Freud Róbert
Gyarmati Edit

SZÁMELMÉLET

Második, javított
és bővített kiadás

Egyetemi-főiskolai tankönyv

Az első kiadás az Oktatási Minisztérium támogatásával,
a Felsőoktatási Pályázatok Irodája által lebonyolított
felsőoktatási tankönyv-támogatási program keretében
jelent meg.

Szakmai bírálók:

Dr. Ruzsa Imre az MTA rendes tagja
(12. fejezet)

Dr. Sárközy András az MTA rendes tagja
(1–12. fejezet)

Dr. Szalay Mihály kandidátus
(1–11. fejezet)

ISBN 963 19 0784 8

A mű más kiadványban való részleges vagy teljes felhasználása, utánközlése,
illetve sokszorosítása tilos!

© Dr. Freud Róbert kandidátus, Dr. Gyarmati Edit PhD,
Nemzeti Tankönyvkiadó Rt., Budapest, 2000, 2006

TARTALOM

Bevezetés **9**

1. Számelméleti alapfogalmak **15**

1.1. Oszthatóság 15
1.2. Maradékos osztás 20
1.3. Legnagyobb közös osztó 25
1.4. Felbonthatatlan szám és prímszám 34
1.5. A számelmélet alaptétele 37
1.6. Kanonikus alak 42

2. Kongruenciák **54**

2.1. Elemi tulajdonságok 54
2.2. Maradékosztályok és maradékrendszerek 60
2.3. Az Euler-féle φ-függvény 67
2.4. Euler–Fermat-tétel 71
2.5. Lineáris kongruenciák 74
2.6. Szimultán kongruenciarendszerek 81
2.7. Wilson-tétel 93
2.8. Műveletek maradékosztályokkal 96

3. Magasabb fokú kongruenciák **102**

3.1. Megoldásszám és redukció 102
3.2. Rend 106
3.3. Primitív gyök 110
3.4. Diszkrét logaritmus (index) 119
3.5. Binom kongruenciák 121
3.6. Chevalley-tétel, Kőnig–Rados-tétel 126
3.7. Prímhatvány modulusú kongruenciák 132

4. Legendre- és Jacobi-szimbólum 137

4.1. Másodfokú kongruenciák 137
4.2. Kvadratikus reciprocitás 141
4.3. Jacobi-szimbólum 147

5. Prímszámok 152

5.1. Klasszikus problémák 152
5.2. Fermat- és Mersenne-prímek 158
5.3. Prímszámok számtani sorozatokban 168
5.4. Becslések $\pi(x)$-re 172
5.5. Hézag a szomszédos prímek között 180
5.6. A prímek reciprokösszege 187
5.7. Prímtesztek 199
5.8. Titkosírás 213

6. Számelméleti függvények 220

6.1. Multiplikativitás, additivitás 220
6.2. Nevezetes függvények 226
6.3. Tökéletes számok 234
6.4. A $d(n)$ függvény vizsgálata 237
6.5. Összegzési és megfordítási függvény 248
6.6. Konvolúció 253
6.7. Átlagérték 260
6.8. Additív függvények karakterizációja 275

7. Diofantikus egyenletek 280

7.1. Lineáris diofantikus egyenlet 281
7.2. Pitagoraszi számhármasok 286
7.3. Néhány elemi módszer 289
7.4. Gauss-egészek 295
7.5. Számok előállítása négyzetösszegként 305
7.6. A Waring-problémakör 314
7.7. A Fermat-sejtés 320
7.8. Pell-egyenlet 334
7.9. Partíciók 340

8. Diofantikus approximáció 349

8.1. Irracionális szám approximációja 349
8.2. Minkowski-tétel 358
8.3. Lánctörtek 365
8.4. A törtrészek eloszlása 372

9. Algebrai és transzcendens számok 377

9.1. Algebrai szám, transzcendens szám 377
9.2. Minimálpolinom és fokszám 381
9.3. Műveletek algebrai számokkal 384
9.4. Algebrai számok approximációja 390
9.5. Az e transzcendens szám 397
9.6. Algebrai egész 403

10. Algebrai számtestek 408

10.1. Testbővítés 408
10.2. egyszerű algebrai bővítés 412
10.3. Másodfokú bővítések 419
10.4. Norma 434
10.5. Egész bázis 439

11. Ideálok 448

11.1. Ideál 448
11.2. Elemi számelméleti kapcsolatok 455
11.3. Alaptételes gyűrű, főideálgyűrű, euklideszi gyűrű 460
11.4. Ideálok oszthatósága 468
11.5. Dedekind-gyűrű 477
11.6. Osztályszám 490

12. Kombinatorikus számelmélet 495

12.1. Csupa különböző összeg 495
12.2. Sidon-sorozatok 506
12.3. Összeghalmazok 517
12.4. Schur tétele 530
12.5. Fedőrendszerek 536
12.6. Additív komplementumok 541

Eredmények és útmutatások **550**

1. Számelméleti alapfogalmak 551
2. Kongruenciák 563
3. Magasabb fokú kongruenciák 578
4. Legendre- és Jacobi-szimbólum 590
5. Prímszámok 594
6. Számelméleti függvények 610
7. Diofantikus egyenletek 631
8. Diofantikus approximáció 654
9. Algebrai és transzcendens számok 659
10. Algebrai számtestek 666
11. Ideálok 672
12. Kombinatorikus számelmélet 679

Megoldások **690**

1. Számelméleti alapfogalmak 690
2. Kongruenciák 699
3. Magasabb fokú kongruenciák 708
4. Legendre- és Jacobi-szimbólum 712
5. Prímszámok 713
6. Számelméleti függvények 724
7. Diofantikus egyenletek 738
8. Diofantikus approximáció 751
9. Algebrai és transzcendens számok 755
10. Algebrai számtestek 758
11. Ideálok 768
12. Kombinatorikus számelmélet 782

Történeti névtár **786**

Táblázatok **792**

Prímszámok (2–3907) 792
Prímtényezős felbontás 794
Mersenne-számok 795
Fermat-számok 796

Tárgymutató **797**

BEVEZETÉS

A könyv szándékaink szerint a következő funkciók betöltésére készült:

(A) Elméleti tankönyv a magyarországi egyetemeken folyó számelmélet-oktatáshoz, elsősorban az egyetemek matematikus, alkalmazott matematikus, matematika tanári és informatika szakos hallgatói részére.

(B) Számelmélet feladatgyűjtemény, szintén elsősorban a fenti hallgatói rétegek számára.

(C) A kötelező és fakultációs anyagon túlmenően a számelmélet egyes fejezeteit, problémaköreit részletesebben tárgyaló „szakkönyv", az ilyen témából szakdolgozatot készítők és más, a terület iránt mélyebben érdeklődők számára.

(D) A(z elemi) számelmélet legfontosabb területeit áttekintő „kézikönyv" matematikusok és matematikatanárok részére.

A könyv felépítése

A fenti célok minél jobb megvalósítása érdekében a tárgyalást teljesen az alapoknál kezdjük és az első két fejezetben csak a középiskolás anyagra támaszkodunk. Ennél a résznél elemi és kevésbé absztrakt segédeszközöket használunk, és a túlzottan tömör indoklások helyett inkább részletes magyarázatokat adunk, hogy a megértést a „kezdő" Olvasók számára is maximálisan megkönnyítsük. Ugyanakkor már itt is nagy súlyt helyezünk az anyag mélyebb összefüggéseit feltáró tételek, a „szép" és nehéz gondolatokat tartalmazó bizonyítások bemutatására.

A későbbi fejezetekben egyre mélyebbre hatolunk a különféle számelméleti témakörök tárgyalásában. Arra törekszünk, hogy a számelmélet rendkívül sokszínű problémavilágából (beleértve a rengeteg régi, de még mindig megoldatlan problémát is) és az ezek kezelésére az évszázadok (sőt évezredek) alatt kidolgozott változatos módszerekből minél többe nyújtsunk betekintést. Ahol lehet, bemutatjuk a számelmélet legújabb eredményeit és alkalmazásait is. Egyes részeknél felhasználjuk a matematika más területeinek tételeit és módszereit is, elsősorban (klasszikus, lineáris és absztrakt) algebrát, analízist és kombinatorikát.

A könyv szerkezetét úgy alakítjuk ki, hogy az az egyes fejezetek egymásra épülését és az anyag rendszerezését minél jobban biztosítsa.

A könyv egészére jellemző, hogy a fogalmakat, állításokat stb. a formális megfogalmazáson túlmenően is alaposan „körbejárjuk", mindig példákkal illusztráljuk, megpróbáljuk a „lényegi" vonásaikat megragadni, bemutatjuk a

korábbi anyaghoz való kapcsolódást, felhívjuk a figyelmet az esetleges buktatókra, elemezzük, mi indokolja az adott fogalom bevezetését stb. Nagy súlyt helyezünk arra, hogy lehetőleg a konkrétból kiindulva haladjunk az általános felé. Igyekszünk a számelméletnek a matematika más területeivel való szoros és sokszínű kapcsolatát minél átfogóbban érzékeltetni.

Feladatok

A fejezeteket alkotó minden egyes pont után feladatok következnek. A feladatok részben az aktuális fogalmak, tételek, módszerek stb. megértését ellenőrzik és ezek elmélyítését segítik elő, részben újabb példákat, összefüggéseket és alkalmazásokat mutatnak be, részben pedig az adott témakörhöz kapcsolódó egyéb problémákat vizsgálnak. Gyakran szerepelnek feladatnak „álcázott" tételek is, amelyek az anyag részletesen nem tárgyalt további érdekes vonatkozásaira, távolabbi összefüggéseire hívják fel a figyelmet.

Ennek megfelelően a feladatok mennyisége és nehézsége igen tág határok között mozog, az éppen sorra kerülő anyag témájától, terjedelmétől és mélységétől függően. A(z általunk) nehezebbnek ítélt feladatokat csillaggal, a kiemelkedően nehéznek tartott feladatokat pedig két csillaggal jelezzük. (Természetesen egy feladat nehézsége mindig relatív; a megoldó képességeitől, érdeklődésétől és általános előismeretétől eltekintve jelentősen függhet — többek között — a korábban megoldott feladatoktól is.)

A feladatok eredményét és/vagy a megoldáshoz vezető (egyik lehetséges) útmutatást — minimális számú kivételtől eltekintve — az „Eredmények és útmutatások" c. fejezetben közöljük. Néhány (elsősorban nehezebb) feladathoz részletes megoldást is adunk a „Megoldások" c. fejezetben, ezeket a feladatokat a kitűzésnél **M** betűvel jelöltük meg.

Az Olvasónak azt tanácsoljuk, hogy lehetőleg csak akkor nézze meg a feladatokhoz adott útmutatást vagy megoldást, ha semmiképpen sem boldogul a feladattal. Térjen inkább vissza többször is ugyanarra a problémára, esetleg oldja meg előbb valamelyik speciális esetet.

Fontos, hogy próbálja meg felderíteni a feladat „mondanivalóját", hátterét, a matematikai környezetben elfoglalt helyét és szerepét. Nagyon hasznos az általánosítás vagy újabb problémák önálló felvetése (még akkor is, ha ezeket nem sikerül megoldani).

Az egyes fejezetek rövid ismertetése

Az első két fejezet bevezető jellegű, ezekben az egész számok oszthatóságával, a legnagyobb közös osztóval, a számelmélet alaptételével (azaz az egyértelmű prímfelbontással), illetve a kongruenciákkal kapcsolatos elemi ismereteket

tárgyaljuk. Ezek biztos elsajátítása elengedhetetlen a további fejezetek tanulmányozásához.

A 3. és 4. fejezetben a kongruenciák elméletét építjük tovább.

Az 5. fejezet témája a prímszámok, amelyek a matematika egyik legegyszerűbben definiált, ugyanakkor talán legtitokzatosabb halmazát jelentik. Ebben a fejezetben Euklidész több mint 2000 éves tételei, valamint azóta is megoldatlan problémái és az utóbbi évtizedek egyik matematikai szenzációját jelentő, a gyors prímtesztelésen és az ehhez képest összemérhetetlenül lassú prímfaktorizáción alapuló nyilvános jelkulcsú titkosírások egyaránt helyet kapnak. Ebben a fejezetben a korábbi számelméleti ismeretek felhasználásán túl számos helyen intenzíven támaszkodunk az elemi analízis eredményeire és módszereire is.

A 6. fejezet a számelméleti függvényekkel foglalkozik. Az egyes fontos függvények bemutatása mellett számos általános konstrukciót és alkalmazást tárgyalunk.

A 7. fejezet a diofantikus egyenletekről szól. A legegyszerűbb problémák (lineáris egyenlet, pitagoraszi számhármasok) bemutatása után ízelítőt nyújtunk többek között a Waring-problémakörből és bebizonyítjuk a Fermat-sejtésnek a köbökre és a negyedik hatványokra vonatkozó speciális esetét. A módszerek közül kiemelnénk a Gauss- és Euler-egészek számelméletét, amelyek általánosítása később a 10. és 11. fejezet egyik központi témáját alkotja.

A 8. fejezet az alkalmazások szempontjából fontos diofantikus approximációval foglalkozik. Röviden bemutatjuk az approximációnak a geometriai számelmélettel, illetve a lánctörtekkel való kapcsolatát is.

A 9–11. fejezetek szoros egységet alkotnak. A 9. fejezetből az algebrai számok és algebrai egészek alaptulajdonságai nélkülözhetetlenek a következő két fejezet megértéséhez. A 10. fejezet a testbővítésekkel, ezen belül is elsősorban a racionális testnek egy algebrai számmal való bővítésében levő algebrai egészek számelméleti vizsgálatával foglalkozik. Ebben a fejezetben intenzíven támaszkodunk az elemi lineáris algebra fogalmaira és tételeire. Végül a 11. fejezetben az ideálok számelméleti vonatkozásait tárgyaljuk. Az ideálok segítségével egyrészt általános gyűrűkben is jól leírhatók a számelmélet alaptételének szükséges és elégséges, illetve elégséges feltételei, másrészt az algebrai számtestek számelméleti vizsgálatánál fontos szerepet játszik, hogy itt az algebrai egészek ideáljaira érvényes az egyértelmű prímfaktorizáció (noha magukra az algebrai egészekre ez általában nem teljesül).

A(z első kiadáshoz képest teljesen új) 12. fejezet néhány érdekes kombinatorikus számelméleti problémát mutat be. Ezek némelyike akár középiskolai szakkörön is tárgyalható, más esetben viszont a megoldáshoz a matematika más ágainak mélyebb módszereit is igénybe kell venni. Reméljük, hogy a való-

gatásunkkal azt is sikerül érzékeltetnünk, milyen nagy szerepet játszottak a témakör fejlődésében Erdős Pál izgalmas problémafelvetései és szellemes bizonyításai.

A könyvben sok helyen kitérünk érdekes matematikatörténeti vonatkozásokra is, és ilyen célt szolgál a könyv végén található rövid „Történeti névtár" is.

Amint a fenti leírásból is kiderül, a számelmélet egyes területei ezer szállal kötődnek egymáshoz és más matematikai ágakhoz egyaránt. Ezért komoly és nem is teljesen áthidalható nehézséget jelent az a kettősség, hogy egyrészt az egyes témakörök tárgyalásánál jól érzékelhető legyen ez a szoros kapcsolat, másrészt az adott témakört bemutató fejezet minél inkább önmagában is érthető és teljes legyen. Igyekeztünk olyan egyensúlyt kialakítani, hogy annak, aki a könyvet folyamatosan dolgozza fel, fokozatosan, összefüggéseiben és minél teljesebben táruljon fel egy probléma- és gondolatgazdag matematikai diszciplína, ugyanakkor a csak néhány fejezetből „csipegető" olvasónak is lehetősége nyíljék érdekes, tartalmas és hasznos ismeretek elsajátítására.

Technikai tudnivalók

Az egyes fejezetek ún. pontokra tagolódnak. A definíciókat, a tételeket és a feladatokat $k.m.n$ típusú módon számoztuk, ahol k a fejezetet, m ezen belül a pontot és n a ponton belüli sorszámot jelenti. A definíciók és a tételek „közös listán" futnak, tehát pl. a 6.2.1 Definíció után a 6.2.2 Tétel következik. Az illusztrációs példák, képletek stb. (sima, egy számmal történő) számozása pontonként újrakezdődik. A definíciók, illetve a tételek megfogalmazásának a végén ♣ áll, a bizonyítások befejezését pedig ■ jelzi.

A jelölések, fogalmak, tételek visszakeresését megkönnyít(het)i a könyv végén található „Tárgymutató", amelyet igyekeztünk nagyon részletesen összeállítani.

Néhány általános jelölés: Megkülönböztetjük a (valós) számok alsó és felső egészrészét, és ezeket $\lfloor\ \rfloor$, illetve $\lceil\ \rceil$ jelöli, így pl. $\lfloor\pi\rfloor = 3$, $\lceil\pi\rceil = 4$, a $[\pi]$ jelölést nem használjuk. A számok törtrészét $\{\ \}$ jelöli, tehát $\{c\} = c - \lfloor c\rfloor$. Az oszthatóságra, a legnagyobb közös osztóra és a legkisebb közös többszörösre a szokásos jelöléseket használjuk, tehát pl. $7 \mid 42$, $(9, 15) = 3$, $[9, 15] = 45$. A $[\ ]$ szögletes zárójel legkisebb közös többszöröst, zárt intervallumot vagy egyszerűen zárójelet jelöl (ez utóbbi különösen a 11. fejezetben jellemző, ahol a $(\ )$ kerek zárójel ideált jelent; a megkülönböztetés érdekében itt a legnagyobb közös osztóra is az $\mathrm{lnko}\{a, b\}$ jelölést használjuk).

A polinomok és függvények jelölésére többnyire az (argumentum nélküli) f, g stb. jelölés szerepel, de helyenként az $f(x)$, $g(x)$ stb. írásmód is előfordul. A polinomok fokszámát (az angol degree szónak megfelelően) „deg"-gel

jelöljük, tehát pl. $\deg(x^3+x)=3$. A szokásos módon $\mathbf{Q}$, $\mathbf{R}$, illetve $\mathbf{C}$ rendre a racionális, a valós, illetve a komplex számok testét, $\mathbf{Z}$, $\mathbf{Z}_m$, illetve $T[x]$ pedig az egész számok, a modulo m maradékosztályok, illetve a T feletti polinomok gyűrűjét jelenti. A testbővítéseknél $\mathbf{Q}(\vartheta)$, illetve $E(\vartheta)$ a racionális test ϑ-val való egyszerű bővítését, illetve (algebrai ϑ esetén) az ebben található algebrai egészek gyűrűjét jelenti, E-vel pedig az összes algebrai egész gyűrűjét jelöljük. A p betűt szinte kizárólag a (pozitív) prímszámok jelölésére tartjuk fenn. A sima (index nélküli) log jelölés a természetes (e alapú) logaritmust jelenti. A (véges vagy végtelen) szorzatok és összegek jelölésére gyakran használjuk a $\prod$ és $\sum$ jeleket, például

$$\prod_{i=1}^{r} p_i^{\alpha_i}, \qquad \prod_{p\le n} p, \qquad \sum_{p} \frac{1}{p^2}$$

rendre a $p_1^{\alpha_1}\dots p_r^{\alpha_r}$ szorzatot, az n-nél nem nagyobb (pozitív) prímszámok szorzatát, illetve a (pozitív) prímszámok négyzetének reciprokösszegét jelenti.

Megemlékezés

A könyvet Turán Pál, Erdős Pál és Gallai Tibor akadémikusok emlékének ajánljuk (akik egyébként egymás jó barátai és közeli munkatársai voltak).

Mindketten abban a szerencsés helyzetben voltunk, hogy szoros kapcsolatban állhattunk a huszadik századi számelmélet két kiemelkedő egyéniségével, Turán Pállal és Erdős Pállal.

Mindketten Turán Pál legendás számelmélet szemináriumain nevelkedtünk, ott kóstoltunk bele először igazán abba, hogyan kell egy-egy probléma lényeges elemeit kibontani, feldolgozni és mindezt mások számára megvilágítani. Turán Páltól tanultuk, hogy a látszólag távoli területek összekapcsolása gyakran új, hatékony megközelítési módot eredményez.

Könyvünk előzményeihez tartozik az a (feladatokat nem tartalmazó) országos Számelmélet jegyzet, amelyet 35 évvel ezelőtt Gyarmati Edit több más forrásmunka mellett Turán Pál előadásainak felhasználásával írt. Az azóta eltelt idő alatt tartott előadásaink tapasztalatai, a hallgatók előismereteinek gyarapodása (pl. lineáris algebra) és az időközben született új eredmények azt indokolták, hogy a már régóta aktuális felfrissítés és átdolgozás helyett egy új könyvet írjunk. Könyvünk szelleme és felépítése természetesen több rokon vonást mutat az említett jegyzettel.

Mindkettőnkre nagy hatással volt Erdős Pál matematikai és emberi nagysága, ahogyan a „szép” matematikai problémák és bizonyítások iránti szenvedélyes szeretetét másokkal megosztotta, ugyanolyan természetes közvetlenséggel

beszélve ezekről (és sok minden másról is) komoly tudósok és kezdő érdeklődők előtt egyaránt. Freud Róbert sok közös matematizálás élményét és szakmai fejlődésének jelentős részét is Erdős Pálnak köszönheti.

Gyarmati Edit pályaválasztásában meghatározó szerepet játszott felejthetetlen középiskolai tanára, Gallai Tibor, a gráfelmélet világhírű kutatója. Gallai Tibor zseniális tanáregyéniség volt, akinek csodálatos gimnáziumi órái és egyetemi előadásai a legjobb hallgatókat sikerrel indították el a matematikai kutatás útján, miközben a gyengébb diákok számára is a megértés és az alkotás élményét nyújtották.

Köszönetnyilvánítás

Nagy köszönettel tartozunk azért a munkáért, amelyet a lektorok, Ruzsa Imre (12. fejezet), Sárközy András (1–12. fejezet) és Szalay Mihály (1–11. fejezet) végeztek. Mindhárman rendkívüli alapossággal nézték át a kéziratot, és igen sok általános, konkrét és stiláris észrevételt tettek, amelyeket szinte kivétel nélkül figyelembe vettünk. Sárközy András koncepcionális megjegyzései nyomán több helyen egységesebb fogalomalkotást, jobban harmonizáló felépítést és további eredményekre történő utalásokat tudtunk megvalósítani. Szalay Mihály a legapróbb részletekbe menően ellenőrizte a kéziratot, és igen gondosan végigszámolta azokat a feladatokat is, amelyek részletes megoldását nem adtuk meg; figyelmét nem kerülte el a legapróbb pontatlanság sem, és konkrétan megfogalmazott módosítási javaslatai sok kisebb-nagyobb hiba, egyenetlenség kijavítását tették lehetővé. Ruzsa Imre az általa átnézett 12. fejezethez fűzött igen értékes megjegyzéseket.

Nagyon köszönjük a Nemzeti Tankönyvkiadó munkatársainak, Palojtay Mária főszerkesztőnek és Balassa Zsófiának, az első kiadás szerkesztőjének kiváló munkáját és segítő együttműködését.

A könyvben a szerzők (és a lektorok) minden igyekezete ellenére bizonyára akadhatnak hibák és hiányosságok. Bárkitől köszönettel fogadjuk az ezzel kapcsolatos észrevételeket.

Budapest, 2006. február Freud Róbert, Gyarmati Edit

Jelen formájában a könyv — néhány új eredmény ismertetésétől, bizonyítások egyszerűsítésétől és sajtóhibák javításától eltekintve — azonos a 2006-os kiadással. Gyarmati Edit, aki nemcsak szerzőtársam, hanem sok évtizeden át nagyszerű feleségem is volt, 2014-ben elhunyt. Remélem, ez a könyv is segít megőrizni az emlékét.

Budapest, 2023. december Freud Róbert, freudro8@gmail.com

ELTE TTK Matematikai Intézet, 1117 Budapest, Pázmány Péter sétány 1c

1. SZÁMELMÉLETI ALAPFOGALMAK

Ebben a fejezetben az egész számok oszthatóságával kapcsolatos néhány alapvető fogalmat, tételt és módszert tekintünk át. A fogalmak bevezetésénél legtöbbször csak általános oszthatósági vonatkozásokra építünk, és minél kevesebbet támaszkodunk az egész számok speciális tulajdonságaira. A páros számok és más példák segítségével igyekszünk rámutatni arra is, hogy az egész számoknál „megszokott" tételek egy része, köztük az egyértelmű prímfelbontás (más néven a számelmélet alaptétele) egyáltalán nem magától értetődő.

A felépítés során úgy jutunk el a számelmélet alaptételéhez, hogy a maradékos osztásból kiindulva az euklideszi algoritmus segítségével megmutatjuk a legnagyobb közös osztó „kitüntetett" tulajdonságát, majd ennek alapján igazoljuk, hogy az egész számok körében a felbonthatatlan számok és a prímszámok egybeesnek. Az alaptételre egy, a maradékos osztástól független, közvetlen indukciós bizonyítást is adunk, majd az alaptétel néhány fontos következményét tárgyaljuk.

1.1. Oszthatóság

Ha a és b racionális számok és $b \neq 0$, akkor a-t b-vel elosztva ismét racionális számot kapunk. Hasonló állítás az egész számok körében nem érvényes. Ezért érdemes bevezetni a következő definíciót:

1.1.1 Definíció **D 1.1.1**

A b egész számot az a egész szám *osztó*jának nevezzük, ha létezik olyan q egész szám, amelyre $a = bq$. ♣

Jelölés: $b \mid a$. Ugyanezt a kapcsolatot fejezi ki más szavakkal, hogy az a *osztható* b-vel, illetve az a *többszöröse* a b-nek. Ha nem létezik olyan q egész, amelyre $a = bq$, akkor a b nem osztója a-nak, ennek jelölése: $b \nmid a$.

A továbbiakban, ha egyéb kikötést nem teszünk, akkor számon mindig egész számot értünk.

A 0 minden számmal osztható (a 0-val is!), hiszen bármely b-re $0 = b \cdot 0$. A másik „végletet" azok a számok alkotják, amelyek minden számnak osztói:

1.1.2 Definíció **D 1.1.2**

Ha egy szám minden számnak osztója, akkor *egység*nek nevezzük. ♣

1.1.3 Tétel **T 1.1.3**

Az egész számok körében két egység van, az 1 és a -1. ♣

Bizonyítás: Az 1 és a -1 valóban egységek: bármely a-ra $\pm 1 \mid a$, hiszen $a = (\pm 1)(\pm a)$.

Megfordítva, ha ε egység, akkor az ε az 1-nek is osztója, azaz alkalmas q-val $1 = \varepsilon q$. Mivel $|\varepsilon| \geq 1$ és $|q| \geq 1$, így csak

$$|\varepsilon| = 1, \qquad \text{azaz} \qquad \varepsilon = \pm 1$$

lehetséges. ■

Megjegyzés: Az oszthatóságot az egészektől különböző számkörökben (sőt általánosabban bármely integritási tartományban, lásd az 1.1.23 feladatot) be lehet vezetni. Tekintsük példaként a páros számokat. Itt $b \mid a$ azt jelenti, hogy létezik olyan q *páros* szám, amelyre $a = bq$. Ennek megfelelően itt $2 \mid 20$, de $2 \not\mid 10$, sőt a 10-nek egyáltalán nincs is osztója. Ebből az is következik, hogy a páros számok körében egyáltalán nincsenek egységek. Ugyanakkor a $c + d\sqrt{2}$ alakú (speciális valós) számok körében, ahol c és d tetszőleges egészek, végtelen sok egység található (lásd az 1.1.22 feladatot). Mindez azt jelenti, hogy az egységek változatos képet mutathatnak, és általában nem (csak) az előjelbeli eltéréssel hozhatók kapcsolatba, mint ahogy azt az 1.1.3 Tétel esetleg tévesen sugallhatná.

1.1.4 Tétel **T 1.1.4**

Ha ε és δ egységek és $b \mid a$, akkor $\varepsilon b \mid \delta a$ is teljesül. ♣

Bizonyítás: Az ε az 1-nek is osztója, azaz alkalmas r-rel $1 = \varepsilon r$. Ha $a = bq$, akkor $\delta a = (\varepsilon b)(\delta q r)$, tehát valóban $\varepsilon b \mid \delta a$. ■

Az 1.1.4 Tétel azt fejezi ki, hogy egy szám és az egységszerese oszthatósági szempontból teljesen azonosan viselkednek; az egységek az oszthatóság szempontjából „nem számítanak”. Ennek alapján nem jelent (majd) megszorítást, ha az egész számok oszthatósági vizsgálatát leszűkítjük a nemnegatív egészekre, sőt (a 0 speciális szerepének tisztázása után) csak a pozitív egészekkel foglalkozunk.

A következő tételben az egész számok oszthatóságának néhány egyszerű, de fontos tulajdonságát foglaljuk össze.

1.1.5 Tétel **T 1.1.5**

(i) Minden a-ra $a \mid a$.

(ii) Ha $c \mid b$ és $b \mid a$, akkor $c \mid a$.

(iii) Az $a \mid b$ és $b \mid a$ oszthatóságok egyszerre akkor és csak akkor teljesülnek, ha az a a b-nek egységszerese.

(iv) Ha $c \mid a$ és $c \mid b$, akkor $c \mid a+b$, $c \mid a-b$, tetszőleges (egész) k-ra $c \mid ka$, és tetszőleges (egész) r, s-re $c \mid ra+sb$. ♣

Az (i)–(iii) tulajdonságok rendre azt fejezik ki, hogy az egész számok oszthatósága reflexív és tranzitív, de nem szimmetrikus reláció. A (iv)-beli állítások közül a legtöbbször az első hármat alkalmazzuk, ezek egyébként valamennyien az utolsónak speciális esetei ($r = s = 1$; $r = 1$, $s = -1$; illetve $r = k$, $s = 0$).

Bizonyítás: Csak (iii)-at igazoljuk, a többi könnyen bizonyítható az oszthatóság definíciójából.

Ha $a = \varepsilon b$, ahol ε egység, akkor $b \mid a$ azonnal adódik. Továbbá $1 = \varepsilon r$ miatt $ra = b$, tehát $a \mid b$ is teljesül.

Megfordítva, ha $a \mid b$ és $b \mid a$, azaz alkalmas q és s egészekkel $b = aq$ és $a = bs$, akkor innen $b = b(qs)$. Ha $b = 0$, akkor szükségképpen $a = 0$, tehát $a = \varepsilon b$. Ha $b \neq 0$, akkor $qs = 1$, azaz s (és q is) egység, tehát ekkor is $a = \varepsilon b$. ■

Feladatok

(Ha más kikötést nem teszünk, a feladatokban értelemszerűen egész számok szerepelnek, a hatványkitevők pedig nemnegatív egészek.)

1.1.1 Írjunk le egy háromjegyű számot kétszer egymás mellé. Mutassuk meg, hogy az így kapott hatjegyű szám osztható 91-gyel.

1.1.2 Lássuk be, hogy két páratlan szám négyzetének a különbsége mindig osztható 8-cal.

1.1.3 Tegyük fel, hogy az (a, b, c számjegyekből álló) $\overline{abc}$ háromjegyű szám osztható 37-tel. Igazoljuk, hogy ekkor a $\overline{bca}$ szám is osztható 37-tel.

1.1.4 Bizonyítsuk be, hogy ha $5a + 9b$ osztható 23-mal, akkor $3a + 10b$ is osztható 23-mal.

1.1.5 Melyek igazak az alábbi állítások közül?

a) $c \mid a+b \Longrightarrow c \mid a,\ c \mid b$.
b) $c \mid a+b,\ c \mid a \Longrightarrow c \mid b$.
c) $c \mid a+b,\ c \mid a-b \Longrightarrow c \mid a,\ c \mid b$.
d) $c \mid 2a+5b,\ c \mid 3a+7b \Longrightarrow c \mid a,\ c \mid b$.
e) $c \mid ab \Longrightarrow c \mid a$ vagy $c \mid b$.
f) $c \mid a,\ d \mid b \Longrightarrow cd \mid ab$.
g) $c \mid a,\ d \mid a \Longrightarrow cd \mid a$.

1.1.6 Igazoljuk az alábbi oszthatóságokat:
(i) $a-b \mid a^n-b^n$; (ii) $a+b \mid a^{2k+1}+b^{2k+1}$; (iii) $a+b \mid a^{2k}-b^{2k}$.

1.1.7 Mely c egészekre lesz $(c^6-3)/(c^2+2)$ is egész szám?

1.1.8 Igazoljuk, hogy minden n természetes számra $133 \mid 11^{n+2}+12^{2n+1}$.

1.1.9 Adjunk meg végtelen sok olyan n-et, amelyre $29 \mid 2^n+5^n$.

1.1.10 Mutassuk meg, hogy $(b-1)^2 \mid b^k-1$ akkor és csak akkor teljesül, ha $b-1 \mid k$.

*1.1.11 Tegyük fel, hogy $2^b-1 \mid 2^a+1$. Lássuk be, hogy $b=1$ vagy 2.

1.1.12 Bizonyítsuk be az alábbi állításokat.

a) Ha $b \mid a$ és $a \neq 0$, akkor $|b| \leq |a|$.
b) Minden nemnulla egész számnak csak véges sok osztója van.

1.1.13 Melyek azok a számok, amelyek felírhatók a) két; b) három (nem feltétlenül különböző) pozitív osztójuk összegeként?

1.1.14 Igazoljuk, hogy egy (tízes számrendszerben felírt természetes) szám akkor és csak akkor osztható

a) 3-mal, illetve 9-cel, ha a számjegyeinek az összege osztható 3-mal, illetve 9-cel;
b) 4-gyel, illetve 25-tel, ha az utolsó két számjegyéből álló szám osztható 4-gyel, illetve 25-tel;
c) 8-cal, illetve 125-tel, ha az utolsó három számjegyéből álló szám osztható 8-cal, illetve 125-tel;
d) 11-gyel, ha a számjegyeinek váltakozó előjellel vett összege osztható 11-gyel.

1.1.15 Létezik-e 2-nek olyan pozitív egész kitevős hatványa, amelyben mind a tíz számjegy ugyanannyiszor fordul elő?

*1.1.16 Létezik-e olyan szám, amelyben csak az 1 és 2 számjegyek fordulnak elő, és amely osztható 2^{1000}-rel?

1.1.17 Mutassuk meg, hogy
a) három szomszédos egész szám szorzata osztható 6-tal;
*b) k szomszédos egész szám szorzata osztható $k!$-sal.

M 1.1.18 Legyen $n > 1$ tetszőleges egész. Csongor megnevezi n-nek egy tetszőleges pozitív osztóját, legyen ez d_1. Ezután Tünde választ egy d_2 pozitív osztót, amely nem lehet osztója d_1-nek. Ismét Csongor választ egy d_3-at, amely nem osztója sem d_1-nek, sem d_2-nek stb. Az veszít, aki magát az n-et kénytelen választani. Kinek van nyerő stratégiája, ha n értéke

a) 16; b) 3^{1111}; c) 10; d) 50; **e) 123 456 789 101 112 131 415?

*1.1.19 Válasszunk ki az $1, 2, \ldots, 2n$ számok közül tetszőlegesen $n + 1$ darabot. Igazoljuk, hogy a kiválasztott számok között biztosan lesz két olyan, hogy az egyik a másiknak osztója.

1.1.20 Mi az oka annak, hogy noha a $0 \mid 0$ *oszthatóság* igaz, a $0/0$ *osztás*nak még sincs értelme?

1.1.21 A páros számok körében melyek azok az elemek, amelyeknek
a) egyáltalán nincs osztója;
b) pontosan két (pozitív vagy negatív) osztója van?

1.1.22 Tekintsük oszthatósági szempontból a $c + d\sqrt{2}$ alakú (speciális valós) számokat, ahol c és d tetszőleges egészek.
a) Döntsük el, hogy $12 - 7\sqrt{2}$ osztható-e $3 + 4\sqrt{2}$-vel.
b) Igazoljuk, hogy az $1 + \sqrt{2}$ egység.
c) Mutassuk meg, hogy végtelen sok egység van.
d) Hány osztója van egy tetszőleges elemnek?
e) Lássuk be, hogy $c + d\sqrt{2}$ akkor és csak akkor egység, ha $|c^2 - 2d^2| = 1$.
M *f) Bizonyítsuk be, hogy az egységek éppen a $\pm(1 + \sqrt{2})^k$ alakú elemek, ahol k tetszőleges egész.
g) Hányszor fordul elő az *egész* számok körében, hogy egy négyzetszám kétszerese eggyel nagyobb, illetve eggyel kisebb egy (másik) négyzetszámnál?

1.1.23 *Integritási tartomány*nak a (legalább kételemű) kommutatív, nullosztómentes gyűrűket nevezzük, azaz amelyekben az összeadás és a szorzás kommutatív és asszociatív, van nullelem, minden elemnek van ellentettje, érvényes a disztributivitás, és két nemnulla elem szorzata sem lehet nulla. (Ez pongyolán fogalmazva azt jelenti, hogy az összeadás, kivonás és szorzás tekintetében az egész számoknál

megszokott „szép” tulajdonságok teljesülnek.) Vezessük be az oszthatóságot és az egység fogalmát az 1.1.1 és 1.1.2 Definíciók szerint, és lássuk be az alábbiakat.

M a) Akkor és csak akkor létezik egység, ha a szorzásnak létezik egységeleme (azaz olyan e elem, amelyre bármely a-val $ea = a$ teljesül).
b) Az egységek éppen az egységelem osztói, illetve más megfogalmazásban azok az elemek, amelyeknek (a szorzásra nézve) létezik inverze.
c) Egy egység minden osztója és két egység szorzata is egység.
d) Vizsgáljuk meg az 1.1.5 Tétel állításait.

1.2. Maradékos osztás

1.2.1 Tétel **T 1.2.1**

Tetszőleges a és $b \neq 0$ egész számokhoz léteznek olyan egyértelműen meghatározott q és r egész számok, melyekre

$$a = bq + r \qquad \text{és} \qquad 0 \leq r < |b|. \ \clubsuit$$

Bizonyítás: Legyen először $b > 0$. A

$$0 \leq r = a - bq < b$$

feltétel pontosan akkor teljesül, ha

$$bq \leq a < b(q+1),$$

azaz

$$q \leq a/b < q + 1.$$

Ilyen q egész szám pedig nyilván pontosan egy létezik; q az a/b (alsó) *egészrésze*, $q = \lfloor a/b \rfloor$, azaz a legnagyobb olyan egész szám, amely még kisebb vagy egyenlő, mint a/b.

Ha $b < 0$, akkor a

$$0 \leq r = a - bq < |b| = -b$$

feltétel

$$q \geq a/b > q - 1$$

teljesülésével ekvivalens, ami ismét pontosan egy q egészre áll fenn (ekkor q az a/b *felső* egészrésze, $q = \lceil a/b \rceil$, azaz a legkisebb olyan egész, amely még nagyobb vagy egyenlő, mint a/b). ■

A maradékos osztásnál kapott q számot *hányados*nak, az r-et pedig (legkisebb nemnegatív) *maradék*nak nevezzük. A $b \mid a$ oszthatóság ($b \neq 0$ esetén) pontosan akkor teljesül, ha a maradék 0.

Gyakran kényelmesebb, ha negatív maradékokat is megengedünk. Erre vonatkozik az 1.2.1 Tétel alábbi variánsa, amely hasonlóan bizonyítható:

1.2.1A Tétel **T 1.2.1A**

Tetszőleges a és $b \neq 0$ egész számokhoz léteznek olyan egyértelműen meghatározott q és r egész számok, melyekre

$$a = bq + r \qquad \text{és} \qquad -\frac{|b|}{2} < r \leq \frac{|b|}{2}\,. \ \clubsuit$$

Ebben az esetben az r-et *legkisebb abszolút értékű maradék*nak nevezzük.

Példa: Legyen $a = 30, b = -8$, ekkor

$$30 = (-8)(-3) + 6 = (-8)(-4) - 2,$$

tehát a legkisebb nemnegatív maradék a 6, a legkisebb abszolút értékű maradék pedig a -2.

Az alábbi tétel bizonyításából látni fogjuk, hogy a maradékos osztás felhasználható a pozitív egész számok ún. *számrendszer*es felírásához is.

1.2.2 Tétel **T 1.2.2**

Legyen $t > 1$ rögzített egész. Ekkor bármely A pozitív egész egyértelműen felírható az alábbi alakban:

$$A = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0, \quad \text{ahol} \quad 0 \leq a_i < t \quad \text{és} \quad a_n \neq 0. \ \clubsuit$$

Bizonyítás: A $0 \leq a_0 < t$ és $t \mid A - a_0$ feltétel miatt a_0 éppen az A-nak a t-vel történő maradékos osztásakor keletkező legkisebb nemnegatív maradék, tehát pontosan egy megfelelő a_0 létezik. Jelöljük a hányadost q_0-lal, ekkor a

$$q_0 = \frac{A - a_0}{t} = a_n t^{n-1} + a_{n-1} t^{n-2} + \ldots + a_2 t + a_1$$

felírásból az előzőkhöz hasonlóan adódik, hogy a_1 éppen a q_0-nak a t-vel történő maradékos osztásakor keletkező legkisebb nemnegatív maradék. Az eljárást folytatva kapjuk a megfelelő a_i-k létezését és egyértelműségét. ■

Az A szám fenti

$$A = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

előállításában az a_i számok az A *számjegy*ei t *alapú számrendszer*ben (ha $t > 10$, akkor a $0, 1, \ldots, 9$ mellett újabb számjegyjeleket is be kell vezetni). A fenti előállítást

$$A = a_n a_{n-1} \ldots a_1 a_{0\,[t]} \qquad \text{vagy} \qquad A = \overline{a_n a_{n-1} \ldots a_1 a_0}_{[t]}$$

alakban jelöljük (a felülvonással szükség esetén azt jelezzük, hogy egymás mellé írt számjegyekről és nem például szorzásról van szó). Ha $t = 10$, akkor a számrendszer alapszámára utaló jelölést legtöbbször elhagyjuk.

Példa: $38 = 38_{[10]} = 123_{[5]}$, hiszen $38 = 1 \cdot 5^2 + 2 \cdot 5 + 3 \cdot 1$.

A mindennapi életben általában a tízes számrendszerrel dolgozunk, de gyakran hasznosabb pl. a kettes számrendszer, többek között a számítógépeknél. Ez utóbbiban csak kétféle számjegy szerepel, a 0 és az 1, az összeadás és a szorzás elvégzéséhez pedig csak az alábbi egyszerű egymegegy, illetve egyszeregy táblát kell tudni (igaz, hogy mindezért cserébe egy szám felírásához jóval több számjegyre van szükség, mint pl. tízes számrendszerben):

$\oplus$	0	1
0	0	1
1	1	10

$\odot$	0	1
0	0	0
1	0	1

A maradékos osztás — egyszerűsége ellenére — mind gyakorlati, mind pedig elméleti szempontból igen jelentős (akár a legkisebb nemnegatív, akár a legkisebb abszolút értékű maradék szerint végezzük). Többek között jól használható oszthatósági kérdések vizsgálatánál, hiszen gyakran „csak a maradék számít”. Legfontosabb alkalmazása talán a maradékos osztások sorozatából álló euklideszi algoritmus, amelyet a következő pontban tárgyalunk.

Feladatok

1.2.1 Ha 10 849-et és 11 873-at ugyanazzal a háromjegyű (tízes számrendszerbeli pozitív egész) számmal maradékosan elosztjuk, mind a kétszer ugyanazt a (nemnegatív) maradékot kapjuk. Mennyi ez a maradék?

1.2.2 Lássuk be, hogy minden m-hez végtelen sok olyan kettőhatvány létezik, amelyek közül bármely kettőnek a különbsége osztható m-mel.

1.2.3 Mutassuk meg, hogy n egész számból mindig kiválasztható néhány (esetleg egy, esetleg az összes), amelyek összege osztható n-nel.

1.2.4 Bizonyítsuk be, hogy minden pozitív egész számnak létezik olyan nemnulla többszöröse, amelyben csak a 0 és 1 számjegyek fordulnak elő (tízes számrendszerben).

*1.2.5 A *Fibonacci-számok* sorozatát a

$$\varphi_0 = 0, \quad \varphi_1 = 1, \quad \varphi_{j+1} = \varphi_j + \varphi_{j-1}, \quad j = 1, 2, \ldots$$

rekurzióval definiáljuk. A sorozat első néhány eleme:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ \ldots$$

Bizonyítsuk be, hogy minden m-hez végtelen sok m-mel osztható Fibonacci-szám létezik.

(*Megjegyzés*: A szakirodalom egy részében a 0-t nem tekintik Fibonacci-számnak, tehát a sorozatot a $\varphi_1 = \varphi_2 = 1$ értékekből kiindulva definiálják a fenti rekurzióval. Ez a kétféleség nem okozhat zavart, ha megegyezünk abban a szóhasználatban, hogy az „n-edik Fibonacci-szám" mindig φ_n-et jelentse.)

1.2.6 Milyen maradékot adhat egy négyzetszám a) 3-mal; b) 4-gyel; c) 5-tel; illetve d) 8-cal osztva?

1.2.7 Mutassuk meg, hogy 12 egymást követő egész szám négyzetének az összege sohasem lehet négyzetszám.

1.2.8 (A feladat tízes számrendszerre vonatkozik.)

a) Van-e olyan (9-nél nagyobb) négyzetszám, amely csupa azonos számjegyből áll?

*b) Adjuk meg a 81-nél nagyobb összes olyan négyzetszámot, amely páros sok jegyű, és az „első fele" is csupa azonos számjegyből áll, valamint a „második fele" is csupa azonos számjegyből áll.

1.2.9 Mutassuk meg, hogy egy egész szám három páratlan kitevőjű hatványának az összege mindig osztható 3-mal.

*1.2.10 Vegyünk nyolc tetszőleges (különböző) természetes számot, és képezzük a páronkénti különbségeik szorzatát. A 2-nek legalább hányadik hatványával osztható ez a szorzat?

1.2.11 Hány olyan legfeljebb 10-jegyű pozitív egész szám van, amely osztható négyzetgyökének (alsó) egészrészével? (Pl. a 12 ilyen, mert $\lfloor\sqrt{12}\rfloor = 3$ osztója a 12-nek, de a 22 nem ilyen, mert $\lfloor\sqrt{22}\rfloor = 4$ nem osztója a 22-nek.)

1.2.12 Milyen kapcsolatban áll $\lfloor a+b\rfloor$ és $\lfloor a\rfloor + \lfloor b\rfloor$?

1.2.13 Elvégezhető-e a maradékos osztás a páros számok körében (azaz érvényes-e az 1.2.1–1.2.1A Tételek megfelelője)?

1.2.14 Mutassuk meg, hogy az 1.1.14 feladatban megismert szabályok értelemszerű átfogalmazásban nemcsak az oszthatóság eldöntésére, hanem az osztási maradék megállapítására is alkalmasak. Hogyan általánosíthatók ezek más alapú számrendszerekre?

1.2.15 Érdekes módon $23+46+12+18 = 99$ és 99 osztója a számok egymás mellé írásával keletkező 23461218-nak. Tényleg a véletlen játékával állunk szemben?

1.2.16 Képezzük az 1223^{1001} szám (tízes számrendszerbeli) számjegyeinek az összegét, majd az így kapott szám számjegyeinek az összegét stb., amíg egyjegyű számhoz nem jutunk. Mi lesz a végeredmény?

1.2.17 Hogyan lehet gyorsan megkapni egy szám 9-es számrendszerbeli felírásából a 3-as számrendszerbeli alakját és viszont? Milyen számrendszerek közötti átváltásnál alkalmazható hasonló gyors eljárás?

1.2.18 Egy n pozitív egész valamely számrendszerben négyjegyű, az eggyel nagyobb alapú számrendszerben pedig kétjegyű. Határozzuk meg n-et.

1.2.19 Az alábbi szorzásban sem a számrendszer alapszámát, sem a $*$-gal jelölt (nem feltétlenül egyforma) számjegyeket nem ismerjük. Határozzuk meg ezeket. (Egyik szám első jegye sem lehet 0.)

$$\begin{array}{cccccccc} 2 & * & * & * & & \cdot & * & * & * & 2 \\ & * & 1 & * & * & & & & & \\ & & * & * & 2 & * & * & & & \\ \hline * & * & * & * & * & * & * & 1 & & \end{array}$$

1.2.20 A 740-et a t alapú számrendszerbe átszámolva olyan négyjegyű számot kapunk, amelynek utolsó jegye 5. Határozzuk meg t értékét.

1.2.21 Egy kétkarú mérleghez tíz darab súlyból álló súlykészletet szeretnénk gyártani, amellyel egy minél nagyobb határig bezárólag minden egész grammnyi súlyt le lehet mérni. Milyen súlyokat válasszunk, ha méréskor

a) csak a mérleg egyik serpenyőjébe tehetünk súlyt;

*b) mindkét serpenyőbe tehetünk súlyt?

1.2.22 Vizsgáljuk meg, hogy körülbelül hányszor annyi számjegy kell egy nagy szám kettes számrendszerbeli felírásához, mint a tízes számrendszerbeli felírásához. Ez pontos megfogalmazásban a következőt jelenti. Jelöljük az n szám számjegyeinek a számát kettes számrendszerben $K(n)$-nel, tízes számrendszerben pedig $T(n)$-nel. Mutassuk meg, hogy a $K(n)/T(n)$ sorozatnak létezik határértéke, és számítsuk ki ezt a határértéket.

1.2.23 *Változó alapú számrendszer.* Legyenek $t_1, t_2, \ldots$ tetszőleges egynél nagyobb egész számok. Mutassuk meg, hogy bármely A pozitív egész egyértelműen felírható

$$A = a_n t_n t_{n-1} \ldots t_1 + a_{n-1} t_{n-1} \ldots t_1 + \ldots + a_1 t_1 + a_0$$

alakban, ahol $0 \leq a_i < t_{i+1}$ és $a_n \neq 0$.

1.3. Legnagyobb közös osztó

1.3.1 Definíció **D 1.3.1**

Az a és b számok *legnagyobb közös osztó*ja d, ha

(i) $d \mid a$, $d \mid b$; és

(ii) ha egy c-re $c \mid a$, $c \mid b$ teljesül, akkor $|c| \leq |d|$. ♣

Jelölés: $d = (a, b)$ vagy $d = \text{lnko}(a, b)$ vagy $d = \text{lnko}\{a, b\}$.

Ha $a = b = 0$, akkor nem létezik legnagyobb közös osztójuk, hiszen minden egész szám közös osztó, és ezek között nincs legnagyobb abszolút értékű.

Minden más esetben viszont (adott a és b mellett) az 1.3.1 Definíciót pontosan két d szám elégíti ki, amelyek egymás ellentettjei. Mivel egy szám és a negatívja oszthatósági szempontból teljesen egyenértékű, ezért a és b összes közös osztóját úgy kapjuk meg, hogy a pozitív közös osztók mellé vesszük azok

negatívjait. A pozitív közös osztók P halmaza nem az üres halmaz, hiszen az 1 biztosan közös osztó, továbbá P-nek csak véges sok eleme lehet, mert egy nemnulla számnak csak véges sok osztója van (lásd az 1.1.12b feladatot). Ennélfogva P elemei között létezik egy legnagyobb, jelöljük h-val. Ekkor nyilván $d = h$ és $d = -h$ kielégítik az 1.3.1 Definíciót, más szám viszont nem.

1.3.2 Definíció **D 1.3.2**

Az a és b számok *kitüntetett közös osztó*ja δ, ha

(i) $\delta \mid a$, $\delta \mid b$; és

(ii') ha egy c-re $c \mid a$, $c \mid b$ teljesül, akkor $c \mid \delta$. ♣

A kitüntetett közös osztó tehát olyan közös osztó, amely minden közös osztónak többszöröse.

A definícióból következik, hogy ha két számnak létezik kitüntetett közös osztója, akkor az egységszerestől eltekintve egyértelmű. Ez részletesen kifejtve azt jelenti, hogy egyrészt egy kitüntetett közös osztó bármely egységszerese is az, másrészt két kitüntetett közös osztó szükségképpen egymás egységszerese. Ennek igazolását az 1.3.10 feladatban tűztük ki.

Ha $a = b = 0$, akkor a kitüntetett közös osztójuk a definíció szerint 0.

A továbbiakban ezzel az esettel egyáltalán nem foglalkozunk, azaz mindig eleve feltesszük, hogy a és b közül legalább az egyik nem nulla.

Megmutatjuk, hogy ha egyáltalán létezik a δ kitüntetett közös osztó, akkor δ csak a legnagyobb közös osztó (valamelyik értéke) lehet. Jelöljük d-vel a δ-val azonos előjelű legnagyobb közös osztót. Ekkor egyrészt (ii) miatt

$$|\delta| \leq |d|\,,$$

másrészt (ii') alapján $d \mid \delta$, amiből

$$|d| \leq |\delta|$$

következik. A két egyenlőtlenségből kapjuk, hogy $|d| = |\delta|$, és így az azonos előjel miatt $\delta = d$.

Egyáltalán nem magától értetődő azonban, hogy a legnagyobb közös osztó valóban rendelkezik a (ii') kitüntetett tulajdonsággal is, vagyis hogy bármely két egész számnak létezik kitüntetett közös osztója.

1.3.3 Tétel **T 1.3.3**

Bármely két egész számnak létezik kitüntetett közös osztója. ♣

Bizonyítás: A kitüntetett közös osztó létezését a matematika egyik legősibb eljárásával, az *euklideszi algoritmus*sal igazoljuk. Az egyik számot maradékosan elosztjuk a másikkal, majd a másik számot a maradékkal stb., mindig az osztót a maradékkal, amíg 0 maradékhoz nem jutunk. Megmutatjuk, hogy az eljárás véges, és az utolsó nemnulla maradék lesz a két szám (egyik) kitüntetett közös osztója.

Nézzük mindezt részletesen. Tegyük fel, hogy (pl.) $b \neq 0$. Ha $b \mid a$, akkor $\delta = b$ megfelel.

Ha $b \nmid a$, akkor alkalmas q_i, r_i egészekkel

$$\begin{aligned}
a &= bq_1 + r_1, && \text{ahol} && 0 < r_1 < |b|,\\
b &= r_1q_2 + r_2, && \text{ahol} && 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && \text{ahol} && 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && \text{ahol} && 0 < r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1} && && (r_{n+1} = 0).
\end{aligned}$$

Az eljárás biztosan befejeződik véges sok lépésben, ugyanis a maradékok nemnegatív egészekből álló szigorúan csökkenő sorozatot alkotnak:

$$|b| > r_1 > r_2 > \dots$$

Most belátjuk, hogy r_n valóban az a és b számok (egyik) kitüntetett közös osztója.

Az algoritmus egyenlőségein alulról felfelé haladva először azt igazoljuk, hogy r_n közös osztója a-nak és b-nek. Az utolsó egyenlőségből $r_n \mid r_{n-1}$. Az utolsó előtti egyenlőségre rátérve

$$r_n \mid r_{n-1},\ \ r_n \mid r_n \Longrightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2}.$$

Ugyanígy folytatva végül $r_n \mid b$, majd (az első egyenlőségből) $r_n \mid a$ adódik.

A kitüntetett tulajdonság igazolásához felülről lefelé haladunk. Legyen $c \mid a,\ c \mid b$, ekkor az első egyenlőségből $c \mid a - bq = r_1$. A második egyenlőségre rátérve

$$c \mid b,\ \ c \mid r_1 \Longrightarrow c \mid b - r_1q_2 = r_2.$$

Ugyanígy folytatva végül az utolsó előtti egyenlőségből kapjuk, hogy $c \mid r_n$. ■

Megjegyzések: 1. Az euklideszi algoritmust a legkisebb nemnegatív maradékok helyett a legkisebb abszolút értékű maradékokkal is végezhetjük; ebben az

esetben a maradékok *abszolút értékei* alkotnak nemnegatív egészekből álló szigorúan csökkenő sorozatot, és így az eljárás ekkor is véges sok lépésben biztosan befejeződik.

2. Szokás a legnagyobb közös osztót eleve pozitívnak definiálni. Mivel azonban egy szám és a negatívja egymás egységszeresei, azaz bármely oszthatósági kérdésnél teljesen azonosan viselkednek, ezért semmi ok sincs arra, hogy a legnagyobb közös osztó fogalmából a negatív számokat eleve kirekesszük. Ezért adtuk meg a legnagyobb közös osztó definícióját úgy, hogy abba a két legnagyobb *abszolút értékű* közös osztó egyenrangúan beleférjen.

3. Az előrebocsátott megjegyzések alapján nem jelent megszorítást, ha a továbbiakban kényelmi okokból a legnagyobb közös osztó, illetve a (vele már bizonyítottan megegyező) kitüntetett közös osztó két értéke közül mindig a pozitívat fogjuk tekinteni. Ezentúl az (a, b), illetve $\mathrm{lnko}(a, b)$ jelölés is ezt a(z egyértelműen meghatározott) pozitív számot fogja jelenteni, és (általában) a kitüntetett közös osztóra is a legnagyobb közös osztó elnevezést fogjuk használni.

4. A legnagyobb közös osztó gyakorlati kiszámításánál az egyszerűen adódó $(a, b) = (b, a - kb)$ összefüggés alapján gyakran kényelmesebb az euklideszi algoritmusnak az

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

alakját használni.

5. Az 1.3.2 Definíciót, az ottani (ii') kitüntetett tulajdonság bevezetését az indokolja, hogy csak oszthatósági relációt használ fel, szemben az 1.3.1 Definícióval, amelyben rendezési reláció (nagyobb–kisebb) is szerepel. Ennélfogva nem meglepő, hogy az egész számok számelméleti vizsgálatainál — amint hamarosan látni fogjuk — mind elméleti, mind pedig gyakorlati szempontból elsősorban a (ii') kitüntetett tulajdonságra tudunk majd támaszkodni. A csak az oszthatóságra épülő fogalomalkotás további előnye, hogy bizonyos számkörökben (illetve általánosabban integritási tartományokban) az 1.3.1 Definíció nem is értelmes. Ennek egyik nyilvánvaló oka az, ha nem definiálható a számkörben (a szokásos „jó" tulajdonságokkal bíró) rendezés, ilyenek pl. a komplex számok bizonyos részhalmazai. Az 1.3.1 Definícióval azonban olyan számkörökben is adódhat probléma, amelyekben van rendezés, például a $c + d\sqrt{2}$ (c, d egészek) számkörben is ez a helyzet. Itt ugyanis a végtelen sok egység miatt bármely két elemnek végtelen sok közös osztója van, és ezek között nincs legnagyobb abszolút értékű. (Ha csak páronként nem egységszeres közös osztókat tekintünk, akkor sincs értelme az 1.3.1 Definíciónak, mert bármely két közös osztó esetén létezik az elsőnek olyan egységszerese,

amely nagyobb a második osztónál.) Ezért a számelmélet további fejezeteiben egyenesen az 1.3.2 Definíció szerint értelmezzük majd a legnagyobb közös osztót.

Most (az egész számok körében) a legnagyobb közös osztó néhány fontos tulajdonságát tárgyaljuk.

1.3.4 Tétel **T 1.3.4**

Ha $c > 0$, akkor $(ca, cb) = c(a, b)$. ♣

Bizonyítás: Tekintsük az (a, b) előállítására szolgáló euklideszi algoritmust, legyen az utolsó nemnulla maradék $r_n = (a, b)$. Szorozzunk meg minden egyenlőséget c-vel, ekkor éppen a (ca, cb)-t előállító euklideszi algoritmushoz jutunk. Ebben az utolsó nemnulla maradék $(ca, cb) = cr_n = c(a, b)$. ■

Az 1.3.4 Tétel egy másik lehetséges bizonyítására vonatkozóan lásd az 1.3.11 feladatot.

1.3.5 Tétel **T 1.3.5**

Az a és b számok legnagyobb közös osztója alkalmas u és v egészekkel kifejezhető $(a, b) = au + bv$ alakban. ♣

Bizonyítás: Az euklideszi algoritmus első egyenlőségéből r_1-et kifejezve

$$r_1 = a - bq_1$$

adódik. Ennek felhasználásával a második egyenlőségből az

$$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a(-q_2) + b(1 + q_1q_2)$$

előállításhoz jutunk, azaz r_2 felírható $aU + bV$ alakban. Hasonlóan továbbhaladva az utolsó előtti egyenlőségből azt kapjuk, hogy $(a, b) = r_n$ is kifejezhető $au + bv$ alakban. ■

Az 1.3.5 Tétel fontos következménye az $ax+by = c$ kétismeretlenes *lineáris diofantikus egyenlet* megoldhatóságára vonatkozó alábbi tétel. Diofantikus egyenletnek általában olyan egész együtthatós algebrai egyenletet nevezünk, melynek a megoldásait is az egész számok körében keressük, ezekkel részletesen a 7. fejezetben foglalkozunk. A fenti $ax + by = c$ egyenletben tehát a, b, c rögzített egész számok, és megoldáson egy x, y egész számpárt értünk.

1.3.6 Tétel **T 1.3.6**

Legyenek a, b, c rögzített egész számok. Az $ax + by = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha $(a, b) \mid c$. ♣

Bizonyítás: Először tegyük fel, hogy létezik x_0, y_0 megoldás. Ekkor $(a, b) \mid a$ és $(a, b) \mid b$ alapján szükségképpen

$$(a, b) \mid ax_0 + by_0 = c.$$

Megfordítva, tegyük fel, hogy $(a, b) \mid c$, vagyis van olyan t egész, amelyre $(a, b)t = c$. Az 1.3.5 Tétel alapján

$$(a, b) = au + bv$$

teljesül alkalmas u, v egészekkel. Ezt az egyenlőséget t-vel beszorozva kapjuk, hogy

$$c = a(ut) + b(vt),$$

azaz $x = ut$, $y = vt$ megoldása az $ax + by = c$ diofantikus egyenletnek. ■

Az 1.3.6 Tételt kiegészíthetjük azzal, hogy megoldhatóság esetén az euklideszi algoritmus egyúttal eljárást is szolgáltat a lineáris diofantikus egyenlet (egyik) megoldásának a megkereséséhez.

A lineáris diofantikus egyenlet további vonatkozásaival (megoldásszám, összes megoldás előállítása, más megoldási módszer) részletesen a 7.1 pontban foglalkozunk, a lineáris kongruenciákkal való kapcsolatát pedig a 2.5 pontban tárgyaljuk.

Több szám legnagyobb közös osztóját rögtön a „kitüntetett” tulajdonsággal definiáljuk; olyan közös osztó, amely minden közös osztónak többszöröse. Az $a_1, a_2, \ldots, a_k$ (nem csupa 0) számok pozitív legnagyobb közös osztóját $(a_1, a_2, \ldots, a_k)$-val jelöljük. Ennek létezését a legegyszerűbben annak alapján igazolhatjuk, hogy két szám közös osztóinak a halmaza megegyezik a két szám legnagyobb közös osztója osztóinak a halmazával. Ebből kapjuk, hogy

$$(a_1, a_2, \ldots, a_k) = ((\ldots((a_1, a_2), a_3), \ldots, a_{k-1}), a_k)\,.$$

1.3.7 Definíció **D 1.3.7**

Az $a_1, a_2, \ldots, a_k$ számok *relatív prím*ek, ha nincs egységtől különböző közös osztójuk, azaz $(a_1, a_2, \ldots, a_k) = 1$. ♣

1.3.8 Definíció **D 1.3.8**

Az $a_1, a_2, \ldots, a_k$ számok *páronként relatív prím*ek, ha közülük semelyik kettőnek sincs egységtől különböző közös osztója, azaz minden $1 \le i \ne j \le k$ esetén $(a_i, a_j) = 1$. ♣

Nyilvánvaló, hogy a páronként relatív prím számok egyúttal relatív prímek is, de ez ($k > 2$ esetén) megfordítva nem igaz (lásd az 1.3.5 feladatot).

Már az 1.1.5e feladatban is láttuk, hogy ha egy szám osztója egy szorzatnak és az egyik tényezőnek nem osztója, akkor ebből **nem** következik, hogy a másik tényezőnek osztója legyen. A helyes feltételt az alábbi tétel adja, amely már Euklidésznél is szerepel, és amely az oszthatósági feladatokban való felhasználhatósága mellett kulcsszerepet játszik a számelmélet alaptételének bizonyításánál is.

1.3.9 Tétel **T 1.3.9**

Ha $c \mid ab$ és $(c, a) = 1$, akkor $c \mid b$. ♣

Bizonyítás: Nyilván elég arra az esetre szorítkoznunk, ha a, b és c pozitív. Ekkor a $c \mid ab$ és $c \mid cb$ oszthatóságokból a legnagyobb közös osztó kitüntetett tulajdonsága, valamint az 1.3.4 Tétel alapján következik, hogy

$$c \mid (ab, cb) = (a, c)b = b. \blacksquare$$

Feladatok

(Ha egy feladatban előfordul valamilyen u, v számpárra az (u, v) jelölés, akkor automatikusan feltesszük, hogy az u és v közül legalább az egyik nem nulla.)

1.3.1 Számítsuk ki $(3794, 2226)$ értékét, és írjuk fel $3794u + 2226v$ alakban.

1.3.2 Mutassuk meg, hogy az alábbi törtek semmilyen n pozitív egész esetén sem egyszerűsíthetők:

$$\text{a) } \frac{3n+5}{7n+12}; \qquad \text{b) } \frac{3n^2+1}{4n^2+3}; \qquad \text{c) } \frac{n!-1}{(n+1)!-1}; \qquad \text{d) } \frac{7^n-2}{7^{n+1}-5}.$$

1.3.3 Adjuk meg $(n^2 + 2, n^4 + 4)$ lehetséges értékeit, ha n végigfut a természetes számokon.

1.3.4 Tegyük fel, hogy $(a, b) = 5$. Számítsuk ki

a) $(a + b, a - b)$; b) $(a + 2b, 4a - b)$

lehetséges értékeit.

1.3.5 Adjunk meg három olyan számot, amelyek relatív prímek, de közülük semelyik kettő sem relatív prím.

1.3.6 Melyek igazak az alábbi állítások közül?

a) Ha $(a, b) = d$, akkor $(\frac{a}{d}, \frac{b}{d}) = 1$.

b) Ha $(a, b) = d$, akkor $(\frac{a}{d}, b) = 1$ és $(a, \frac{b}{d}) = 1$ közül legalább az egyik teljesül.

c) $c \mid ab \iff \frac{c}{(c,a)} \mid b$.

d) $c \mid ab$, $(a, b) = 1 \Longrightarrow c \mid a$ vagy $c \mid b$.

1.3.7 Legyenek a és b pozitív egészek. Hány b-vel osztható szám van az $a, 2a, 3a, \ldots, ba$ számok között?

1.3.8 Legyenek a és b különböző pozitív egészek. Melyek igazak az alábbi állítások közül?

a) Végtelen sok n egészre $(a + n, b + n) = 1$.

b) Végtelen sok n egészre $(a + n, b + n) = (b + n, bn) = 1$.

c) Végtelen sok n egészre $(a + n, bn) = (b + n, bn) = 1$.

1.3.9

a) Hány olyan u, v egész számpár található, amelyre $(a, b) = au + bv$?

b) Az $(a, b) = au + bv$ előállításban mennyi u és v legnagyobb közös osztója?

c) Legyen H az $au + bv$ alakú számok halmaza, ahol u és v végigfut az egész számokon. Mi lesz H legkisebb pozitív eleme?

1.3.10 *A kitüntetett közös osztó egyértelműsége.* Legyen δ az a, b egész számok (egyik) kitüntetett közös osztója. A kitüntetett közös osztó definíciója alapján bizonyítsuk be az alábbiakat.

a) Tetszőleges ε egységre $\varepsilon\delta$ is kitüntetett közös osztója a, b-nek.

b) Ha δ_1 is kitüntetett közös osztója a, b-nek, akkor $\delta_1 = \varepsilon\delta$, ahol ε alkalmas egység.

M 1.3.11 Adjunk az 1.3.4 Tételre új bizonyítást, amely csak a kitüntetett közös osztó fogalmára (és létezésére) támaszkodik, és nem használja fel (közvetlenül) magát az euklideszi algoritmust.

1.3.12 Nevezzük *csupaegy*nek azokat a pozitív egészeket, amelyeknek (tízes számrendszerben) minden számjegye 1-es.
a) Mely számoknak létezik csupaegy többszöröse?
b) A 3^{1000}-nek melyik a legkisebb csupaegy többszöröse?

M* 1.3.13 Mutassuk meg, hogy bármely $n > 0$, $k > 0$ és $a > 1$ egészekre

$$(a^n - 1, a^k - 1) = a^{(n,k)} - 1.$$

1.3.14 Legyen a pozitív egész.
a) Igazoljuk, hogy ha n és k különböző kettőhatványok és a páros szám, akkor $(a^n + 1, a^k + 1) = 1$.
*b) Határozzuk meg általában $(a^n + 1, a^k + 1)$ értékét.

1.3.15 Bizonyítsuk be, hogy a szomszédos Fibonacci-számok (lásd az 1.2.5 feladatot) relatív prímek. Mi a helyzet a másodszomszédokkal? És a harmadszomszédokkal?

**1.3.16 Legyen φ_m az m-edik Fibonacci-szám. Igazoljuk, hogy

$$k \mid n \iff \varphi_k \mid \varphi_n, \qquad \text{sőt} \qquad \varphi_{(k,n)} = (\varphi_k, \varphi_n)\,.$$

1.3.17 *Szakaszok összemérhetősége.* Euklidész „Elemek” c. könyvében egész számok közös osztói mellett foglalkozik szakaszok *közös mérték*ével is. Két szakasz közös mértékén egy olyan szakaszt értünk, amely egész számszor felmérhető (maradék nélkül) mind a két szakaszra. Két szakaszt *összemérhető*nek nevezünk, ha létezik közös mértékük.
a) Bizonyítsuk be, hogy két szakasz akkor és csak akkor összemérhető, ha a hosszaik aránya racionális szám.
b) Két adott összemérhető szakasznak hány közös mértéke létezik?
c) Fogalmazzuk meg a maradékos osztás szakaszokra vonatkozó értelemszerű megfelelőjét, és mutassuk meg, hogy az erre épülő euklideszi algoritmus akkor és csak akkor fejeződik be véges sok lépésben, ha a két kiindulási szakasz összemérhető.
d) Igazoljuk, hogy összemérhető szakaszok esetén létezik a közös mértékeik között legnagyobb, és erre az összes közös mérték egész számszor felmérhető (maradék nélkül).
e) Lássuk be, hogy egy négyzet oldala és átlója esetén az euklideszi algoritmus nem ér véget. (Ezzel a $\sqrt{2}$ irracionalitását geometriai úton igazoltuk.)

1.4. Felbonthatatlan szám és prímszám

Láttuk, hogy oszthatósági szempontból a 0, illetve az egységek különleges szerepet játszanak: a 0-nak minden szám osztója, az egységek pedig minden számot osztanak. Legyen a továbbiakban a tetszőleges, 0-tól és egységtől különböző szám. Az egység definíciója alapján bármely ε egység esetén $\varepsilon \mid a$ és $\varepsilon a \mid a$. Ezeket az *a triviális osztó*inak nevezzük. A továbbiakban fontos szerepet játszanak azok a számok, amelyeknek csak triviális osztóik vannak:

1.4.1 Definíció **D 1.4.1**

A p egységtől (és nullától) különböző számot *felbonthatatlan szám*nak nevezzük, ha **csak** úgy bontható fel két egész szám szorzatára, hogy valamelyik tényező egység. Azaz

$$p = ab \Longrightarrow a \text{ vagy } b \text{ egység.} \ \clubsuit$$

Itt $p \neq 0$-t azért nem szükséges külön kikötni, mert a 0 nemtriviálisan is szorzattá bontható, pl. $0 = 5 \cdot 0$. Megjegyezzük még, hogy a $p = ab$ szorzatban nem lehet mindkét tényező egység, hiszen akkor a szorzatuk, azaz p is egység lenne. (Így az 1.4.1 Definíció végén tulajdonképpen „kizáró vagy" szerepel.)

A felbonthatatlan számok tehát azok az egységtől különböző egészek, amelyek csak triviálisan bonthatók két egész szám szorzatára, vagy más szóval, amelyek csak az egységekkel és saját maguk egységszereseivel oszthatók. Ilyenek például a 2, 3, -17 stb. Ha egy nemnulla számnak triviálistól különböző osztója is van, akkor *összetett szám*nak nevezzük.

A következő fogalom bevezetéséhez emlékeztetünk arra, hogy ha egy c szám osztója egy szorzat valamelyik tényezőjének, akkor c osztója a szorzatnak is, de ennek a megfordítása nem igaz: pl. $c = 6$-ra $6 \mid 3 \cdot 4$, de $6 \nmid 3$, $6 \nmid 4$. Fontos szerepet játszanak azok a c számok, amelyekre a megfordítás is érvényes:

1.4.2 Definíció **D 1.4.2**

A p egységtől és nullától különböző számot *prímszám*nak (vagy röviden *prím*nek) nevezzük, ha **csak** úgy lehet osztója két egész szám szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

$$p \mid ab \Longrightarrow p \mid a \text{ vagy } p \mid b. \ \clubsuit$$

Az 1.4.2 Definíció végén „megengedő vagy" szerepel, hiszen előfordulhat, hogy p a szorzat mindkét tényezőjét osztja. Megjegyezzük még, hogy most

$p \neq 0$-t mindenképpen külön ki kellett kötni, hiszen a 0-ra teljesül az 1.4.2 Definíció további részében megfogalmazott tulajdonság:

$$0 \mid ab \Longrightarrow ab = 0 \Longrightarrow a = 0 \text{ vagy } b = 0 \Longrightarrow 0 \mid a \text{ vagy } 0 \mid b.$$

Az 1.4.2 Definícióból rögtön következik, hogy egy prímszám egy (kettőnél) több tényezős szorzatnak is csak úgy lehet osztója, ha legalább az egyik tényezőnek osztója.

1.4.3 Tétel **T 1.4.3**

Az egész számok körében p akkor és csak akkor prím, ha felbonthatatlan. ♣

Bizonyítás: Nyilván feltehető, hogy p nem nulla és nem egység.

I. Először tegyük fel, hogy p prím, és lássuk be, hogy felbonthatatlan is. Induljunk ki egy $p = ab$ szorzat-előállításból; azt kell igazolnunk, hogy a és b valamelyike egység.

Mivel $p = ab$, így $p \mid ab$ is igaz. Mivel p prím, ezért ebből $p \mid a$ vagy $p \mid b$ következik. Az első esetben $ab \mid a$, tehát ($a \neq 0$ miatt) $b \mid 1$, vagyis b egység, a második esetben pedig ugyanígy kapjuk, hogy a egység.

II. Most tegyük fel, hogy p felbonthatatlan, és lássuk be, hogy prím is. Induljunk ki egy $p \mid ab$ oszthatóságból; azt kell igazolnunk, hogy $p \mid a$ és $p \mid b$ közül legalább az egyik teljesül.

Ha $p \mid a$, akkor készen vagyunk. Ha $p \nmid a$, akkor p felbonthatatlansága és $(p, a) \mid p$ miatt $(p, a) = 1$. A $p \mid ab$ és $(p, a) = 1$ feltételekből az 1.3.9 Tétel alapján $p \mid b$ következik. ■

Ezzel megmutattuk, hogy az egészek körében a felbonthatatlan számok és a prímszámok egybeesnek. Ezért jogosult a felbonthatatlan vagy prím elnevezések bármelyikének a használata, és az is, hogy a középiskolában az egészekre a felbonthatatlan számnak megfelelő tulajdonsággal értelmezik a prímszámot. A továbbiakban a rövidség kedvéért a prím(szám) szót fogjuk általában használni, kivéve, ha hangsúlyozni akarjuk a szám felbonthatatlan tulajdonságát.

A két fogalom azonban sok más számkörben nem ekvivalens. Például a páros számok körében a 6 felbonthatatlan, hiszen egyáltalán nem bontható két páros szám szorzatára, azonban nem prím, mert osztója a $18 \cdot 2$ szorzatnak, de nem osztja egyik tényezőt sem. További példákat látunk majd a 10. fejezetben.

Az egészek körében a prímszámok vizsgálata a számelmélet egyik legfontosabb területe. Már Euklidész bebizonyította, hogy végtelen sok prímszám létezik (5.1.1 Tétel), ugyanakkor a prímszámokkal kapcsolatban rengeteg

az olyan egyszerűen megfogalmazható probléma, amely még ma is megoldatlan. Mindezekkel bővebben az 5. fejezetben foglalkozunk.

Feladatok

A szokásos szóhasználatnak megfelelően az egész számok körében már az alábbiakban is a prím vagy prímszám szót fogjuk használni a felbonthatatlan számra is. Megjegyezzük azonban, hogy az 1.4.1–1.4.7 feladatok mindegyike tulajdonképpen felbonthatatlan számokra vonatkozik.

1.4.1 Adjuk meg az összes olyan n pozitív egészt, amelyre az alábbi számok mindegyike prímszám:

a) n, $n+2$ és $n+4$;
b) n és n^2+8;
c) n, $n+6$, $n+12$, $n+18$ és $n+24$;
d) n, n^3-6 és n^3+6.

1.4.2 Létezik-e végtelen hosszú, nemnulla differenciájú számtani sorozat csupa prímszámból?

1.4.3 Halhatatlan kapitánynak három halhatatlan unokája van, akiknek az életkora három különböző prímszám és ezek négyzetének az összege is prímszám. Hány éves a kapitány legkisebb unokája? (Ne felejtsük el, hogy az unokák halhatatlanok, tehát akár több millió évesek is lehetnek!)

1.4.4 Legyenek a és k egynél nagyobb egészek. Bizonyítsuk be az alábbi állításokat.

a) Ha a^k-1 prím, akkor $a=2$ és k prím.
b) Ha a^k+1 prím, akkor k kettőhatvány.

Megjegyzés: A 2^k-1 alakú prímeket *Mersenne-prím*eknek, a 2^k+1 alakú prímeket pedig *Fermat-prím*eknek nevezzük, ezekkel részletesen az 5.2 pontban foglalkozunk majd.

M 1.4.5 Adjuk meg az összes olyan $t>1$ egészt és $k>0$ *páratlan* számot, amelyre $1^k+2^k+3^k+\ldots+t^k$ prímszám.

1.4.6 Mely n pozitív egészekre lesz prímszám

a) n^3-n+3;
b) n^3-27;
c) $n^8+n^7+n^6+n^5+n^4+n^3+n^2+n+1$;
d) n^4+4;
e) $n^8+n^6+n^4+n^2+1$?

1.4.7 Legyen $n > 1$ egész szám. Bizonyítsuk be az alábbi állításokat.
a) Ha n-nek nem létezik olyan t osztója, amelyre $1 < t \leq \sqrt{n}$, akkor n prímszám.
b) Az n szám 1-nél nagyobb osztói közül a legkisebb szükségképpen prím.
c) Ha n összetett, de nem létezik olyan t osztója, amelyre $1 < t \leq \sqrt[3]{n}$, akkor n két prímszám szorzata.

1.4.8 Bizonyítsuk be, hogy $(n-5)(n+12)+51$ semmilyen n egész esetén sem osztható 289-cel.

1.4.9 Mik lesznek a páros számok körében a felbonthatatlanok, illetve a prímek?

1.4.10 A felbonthatatlan és prím fogalma tetszőleges I integritási tartományban (lásd az 1.1.23 feladatot) értelmezhető. Bizonyítsuk be az alábbi állításokat.
a) Ha I-ben a szorzásnak nincs egységeleme, akkor I-ben nincs prím.
b) Ha I-ben a szorzásnak van egységeleme, akkor I-ben minden prím szükségképpen felbonthatatlan is.

1.5. A számelmélet alaptétele

1.5.1 Tétel (A számelmélet alaptétele) **T 1.5.1**

Minden, a 0-tól és egységektől különböző egész szám felbontható véges sok felbonthatatlan szám szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. (Az egyértelműség azt jelenti, hogy ha

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s \,,$$

ahol a p_i és q_j számok valamennyien felbonthatatlanok, akkor $r = s$, és a p_i és q_j számok párba állíthatók úgy, hogy mindegyik p_i a hozzá tartozó q_j-nek egységszerese.) ♣

Megjegyzések: 1. A 0-t és az egységeket azért kellett kizárni, mert azok egyáltalán nem bonthatók fel felbonthatatlan számok szorzatára: az egységek csak úgy írhatók fel szorzatként, hogy minden tényező egység, a 0 pedig csak úgy, hogy legalább az egyik tényező 0 (és akkor ez a tényező nem felbonthatatlan).

2. Magukra a felbonthatatlan számokra a tétel olyan formában érvényes, hogy ezeket egytényezős szorzatoknak tekintjük.

3. Néhány észrevétel az egyértelműséghez. Tegyük fel, hogy az a szám $a = p_1 p_2 \dots p_r$ alakban előáll felbonthatatlanok szorzataként. Ekkor nyilván a tényezőket tetszőleges más sorrendben összeszorozva ugyancsak a-t kapunk. Emellett legyenek $\varepsilon_1, \dots, \varepsilon_r$ tetszőleges olyan egységek, amelyek szorzata 1, ekkor $\varepsilon_1 p_1, \dots, \varepsilon_r p_r$ is felbonthatatlanok, és ezek szorzata is a-val egyenlő. Az alaptétel egyértelműségi része éppen azt fejezi ki, hogy ezektől a variálási lehetőségektől eltekintve az a másképpen már nem írható fel felbonthatatlanok szorzataként. Például a 12 esetében néhány ilyen felírás

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot (-3) \cdot (-2) = 3 \cdot (-2) \cdot (-2).$$

4. A tétel kimondásánál mindenképpen a felbonthatatlan szám fogalmát érdemes használni, hiszen a tétel éppen azt fejezi ki, hogy ilyen „építőkövekből" lényegében minden szám lényegében egyértelműen „összerakható". A bizonyítás során is meg fogjuk különböztetni a felbonthatatlan és a prím fogalmát. Ezek ekvivalenciája — amint látni fogjuk — szoros összefüggésben áll a számelmélet alaptételének az érvényességével.

5. Sok számkörben (illetve integritási tartományban) nem érvényes a számelmélet alaptétele. Például a páros számok körében a 100-nak két lényegesen különböző felbontása létezik felbonthatatlanok szorzatára: $100 = 2 \cdot 50 = 10 \cdot 10$. További példákat látunk majd a 10. fejezetben.

Most rátérünk az alaptétel igazolására. Az egyértelműségi részre két bizonyítást is adunk.

A felbonthatóság bizonyítása: Tekintsünk egy nullától és egységektől különböző tetszőleges a számot. Ha a felbonthatatlan, akkor készen vagyunk.

Ha a nem felbonthatatlan, akkor létezik nemtriviális felbonthatatlan osztója, mert a legkisebb pozitív nemtriviális osztója szükségképpen felbonthatatlan (lásd az 1.4.7b feladatot). Ekkor $a = p_1 a_1$, ahol p_1 felbonthatatlan és a_1 nem egység.

Ha a_1 felbonthatatlan, akkor készen vagyunk; ha nem, akkor van olyan p_2 felbonthatatlan szám, amellyel $a_1 = p_2 a_2$, ahol a_2 nem egység.

Hasonlóan járunk el a_2-vel stb. Eljárásunk véges sok lépésben be kell hogy fejeződjön, ugyanis az $|a_i|$ számok pozitív egészek, és szigorúan csökkenő sorozatot alkotnak:

$$|a| > |a_1| > |a_2| > \dots,$$

tehát eljutunk egy olyan a_k-hoz, amely már felbonthatatlan, $a_k = p_{k+1}$.

Ekkor az $a = p_1 p_2 \dots p_{k+1}$ előállítást nyerjük. ■

Az egyértelműség első bizonyítása: Ebben a bizonyításban a fő segédeszközünk az lesz, hogy minden felbonthatatlan egyben prím is (1.4.3 Tétel).

Tegyük fel indirekt, hogy valamely a-nak létezik (legalább) két lényegesen különböző felbontása felbonthatatlanok szorzatára:

$$a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s. \tag{1}$$

Ha itt valamelyik p_i egységszerese valamelyik q_j-nek, például $p_1 = \varepsilon q_1$, akkor q_1-gyel egyszerűsítve

$$a' = \frac{a}{q_1} = (\varepsilon p_2) p_3 \dots p_r = q_2 q_3 \dots q_s$$

adódik, vagyis az a' számnak kapjuk két lényegesen különböző felbontását felbonthatatlanok szorzatára.

Az eljárást folytatva így végül egy olyan számhoz jutunk, amelynek a kétféle felbontásában már nincsenek egységszeres tényezők. Az általánosság megszorítása nélkül feltehetjük, hogy az (1)-beli előállítás ilyen, azaz $p_i \neq \varepsilon q_j$.

(1)-ből kapjuk, hogy $p_1 \mid q_1 q_2 \dots q_s$. Mivel p_1 felbonthatatlan, így az 1.4.3 Tétel alapján prím is, ezért p_1 szükségképpen osztója legalább az egyik q_j tényezőnek.

Azonban ha $p_1 \mid q_j$, akkor q_j felbonthatatlansága miatt p_1 vagy egység, vagy pedig a q_j egységszerese, és mindkettő ellentmondás. ■

Az egyértelműség második bizonyítása: Ebben a bizonyításban $|a|$-ra vonatkozó teljes indukciót használunk.

Mivel egy szám és az egységszeresei minden oszthatósági szempontból egyenértékűek, ezért nem jelent megszorítást, ha pozitív egészeknek pozitív felbonthatatlanok szorzatára való felbontásaival foglalkozunk.

Ha $a = 2$, akkor az egyértelműség (a 2 felbonthatatlan volta miatt) igaz.

Tegyük most fel, hogy minden $1 < a < n$ szám egyértelműen bomlik fel felbonthatatlanok szorzatára, és megmutatjuk, hogy ekkor $a = n$ felbontása is egyértelmű. Tegyük fel indirekt, hogy n-nek létezik (legalább) két különböző felbontása felbonthatatlanok szorzatára:

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s. \tag{2}$$

Itt nyilván $r \geq 2, s \geq 2$, továbbá $p_i \neq q_j$, mert ha például $p_1 = q_1$, akkor az $1 < n/p_1 < n$ számnak is két különböző felbontása lenne, ami ellentmond az indukciós feltevésnek.

Tegyük fel, hogy $p_1 < q_1$ és legyen $n_1 = n - p_1 q_2 \dots q_s$. Megmutatjuk, hogy

$$1 < n_1 < n, \tag{3}$$

és

$$n_1\text{-nek is van két különböző felbontása,} \tag{4}$$

ami ellentmondás.

Az $n_1 = n - p_1 q_2 \dots q_s$ kifejezésbe n helyére a (2)-beli felbontásokat beírva kapjuk, hogy

$$n_1 = p_1(p_2 \dots p_r - q_2 \dots q_s) = q_2 \dots q_s(q_1 - p_1). \tag{5}$$

Nyilván $n_1 < n$, továbbá $p_1 < q_1$ miatt

$$n_1 = q_2 \dots q_s(q_1 - p_1) \geq q_2 \cdot 1 = q_2 > 1,$$

amivel (3)-at beláttuk.

Bontsuk fel az n_1 mindkét (5)-beli szorzat-előállításának utolsó tényezőjét felbonthatatlanok szorzatára:

$$p_2 \dots p_r - q_2 \dots q_s = u_1 \dots u_k \qquad \text{és} \qquad q_1 - p_1 = v_1 \dots v_m\,.$$

Ennek alapján az n_1 az alábbi módon áll elő felbonthatatlanok szorzataként:

$$n_1 = p_1 u_1 \dots u_k = q_2 \dots q_s v_1 \dots v_m\,. \tag{6}$$

(Ha esetleg $q_1 - p_1 = 1$, akkor (6) úgy értendő, hogy a v_i-k hiányoznak, a további gondolatmenet ekkor „még inkább" érvényben marad.)

Megmutatjuk, hogy (6) az n_1 két különböző felbontását adja. Az első felbontásban szerepel a p_1. A másodikban viszont nem, ugyanis egyrészt $p_1 \neq q_j$, másrészt, ha valamelyik i-re $p_1 = v_i$, akkor

$$p_1 \mid v_1 \dots v_m = q_1 - p_1 \Longrightarrow p_1 \mid q_1$$

következne, ami lehetetlen. Ezzel (4)-et is beláttuk. ■

Megjegyzések: 1. Az egyértelműség első bizonyítását elemezve megállapíthatjuk, hogy az tulajdonképpen a maradékos osztáson múlott. Ugyanis a maradékos osztásra támaszkodó euklideszi algoritmussal igazoltuk a kitüntetett közös osztó létezését, majd ennek felhasználásával mutattuk meg (az 1.3.9 Tétel segítségével), hogy egy felbonthatatlan szám szükségképpen prím is, és ez volt a bizonyítás kulcslépése.

Általában is igaz, hogy ha egy számkörben (illetve integritási tartományban) létezik a maradékos osztás megfelelője, akkor ott érvényes a számelmélet

alaptétele is. Az egyértelműségi részre az egész számoknál adott gondolatmenetünk az általános esetre is szó szerint átvihető, a felbonthatóságnál esetenként finomabb meggondolásokra is szükség lehet. Erre vonatkozó példák szerepelnek majd a 7. és 10. fejezetben. A 11.3 pontban az ideálok segítségével az általános esetben is egységes bizonyítást adunk arra, hogy a maradékos osztásból következik a számelmélet alaptétele (felbonthatóság és egyértelműség egyaránt).

Megjegyezzük még, hogy a maradékos osztás és az alaptétel kapcsolata nem szimmetrikus; vannak olyan számkörök, amelyekben érvényes a számelmélet alaptétele, noha semmilyen értelemben sem létezik bennük maradékos osztás. Ilyen példát látunk majd a 10. fejezetben.

2. Az egyértelműség második bizonyítása nem támaszkodott az 1.3 és 1.4 pontok tételeire. Ez lehetőséget ad arra, hogy ezeknek a tételeknek egy részére az alaptétel segítségével új bizonyítást adjunk. Ezek közül két fontos tételt külön is kiemelünk: az egyik a kitüntetett közös osztó létezése (1.3.3 Tétel), a másik pedig az, hogy minden felbonthatatlan egyben prím is (az 1.4.3 Tétel „érdemibb" fele). Az előbbinek az alaptételből történő levezetését lényegében az 1.6.4 Tétel bizonyításánál láthatjuk majd, az utóbbira nézve lásd az 1.5.8 feladatot.

Feladatok

1.5.1 Igazoljuk, hogy egy a szám felbonthatatlan számok szorzataként történő előállításában a tényezők száma legfeljebb $\log_2 |a|$.

1.5.2 Tekintsük a páros számok körét.
   a) Mely elemek írhatók fel lényegében egyértelműen felbonthatatlanok szorzataként?
   b) Adjunk meg olyan elemet, amelynek pontosan 1000 lényegesen különböző felbontása van.

1.5.3 Vizsgáljuk meg, hogy az egyértelműségre adott bizonyításaink hol buknak meg a páros számok körében?

1.5.4 Mutassuk meg, hogy a 10-zel osztható egész számok körében nem érvényes a számelmélet alaptétele, sőt itt van olyan elem is, amelynek két különböző felbontásában még a felbonthatatlan tényezők darabszáma sem azonos.

1.5.5 Tekintsük a véges tizedes törtek V halmazát.
   a) Határozzuk meg az egységeket és a felbonthatatlanokat.
   b) Bizonyítsuk be, hogy V-ben érvényes a számelmélet alaptétele.

*c) Lássuk be, hogy V-ben létezik a maradékos osztás megfelelője, azaz minden $c \in V$ elemhez hozzá tudunk rendelni egy $f(c)$ nemnegatív egész számot úgy, hogy $f(c) = 0 \iff c = 0$, továbbá minden $a, b \in V$, $b \neq 0$ esetén létezik olyan $q, r \in V$, hogy $a = bq + r$ és $f(r) < f(b)$.

1.5.6 Az egyértelműségre adott második bizonyításnak sok más változata is elkészíthető. Hol kell módosítani a gondolatmenetet, ha n_1-et $n_1 = n - p_1 q_2$-nek választjuk?

1.5.7 Hányféleképpen írható fel egy egész szám felbonthatatlanok szorzataként, ha most a csak a sorrendben és/vagy egységszeresekben való eltérést is különböző felbontásnak tekintjük?

M 1.5.8 Vezessük le a számelmélet alaptételéből, hogy minden felbonthatatlan egyben prím is.

1.5.9 Keressük meg (az egészek körében) az összes olyan p_1, p_2, p_3 (nem feltétlenül pozitív és nem feltétlenül különböző) prímszámokat, amelyekre

$$\frac{1}{p_1 - p_2 - p_3} = \frac{1}{p_2} + \frac{1}{p_3}\,.$$

M* 1.5.10 Adjuk meg (az egészek körében) az összes olyan pozitív prímszámot, amelynek alkalmas (pozitív egész kitevős) hatványa felírható két pozitív egész szám köbének az összegeként.

1.6. Kanonikus alak

A továbbiakban csak pozitív számok pozitív osztóival foglalkozunk, és prímszámon is pozitív felbonthatatlan számot fogunk érteni. Ebben az esetben a számelmélet alaptétele úgy fogalmazható, hogy minden $n > 1$ egész szám felbontható véges sok (pozitív) prímszám szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű. (Az egységek a pozitivitás miatt most nem játszanak szerepet.)

Az ilyen prímtényezős előállításban az azonos prímek szorzatát általában hatványként jelöljük, vagyis a számot különböző prímek hatványainak a szorzataként írjuk fel. Ekkor a számelmélet alaptételének az alábbi alakját kapjuk:

1.6.1 Tétel **T 1.6.1**

Minden $n > 1$ egész szám felírható

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

alakban, ahol $p_1, \dots, p_r$ *különböző* (pozitív) prímek és $\alpha_i > 0$ egész. Ez a felírás a $p_i^{\alpha_i}$ prímhatványtényezők sorrendjétől eltekintve egyértelmű. ♣

Ezt az előállítást az n szám *kanonikus alak*jának nevezzük.

Látni fogjuk, hogy bizonyos esetekben (például több szám egyidejű vizsgálatánál) kényelmesebb, ha megengedjük, hogy a kanonikus alakban egyes prímek kitevője 0 is lehessen, ekkor az egyértelműség természetesen ezektől a(z esetleges fiktív) tényezőktől eltekintve értendő. Ily módon az 1 számnak is beszélhetünk kanonikus alakjáról (ebben csak 0 kitevővel szerepelnek prímek).

Külön fogjuk jelezni, mikor érdemes a 0 kitevőt is megengedni a kanonikus alakban, a többi esetben automatikusan feltesszük, hogy minden kitevő pozitív (egész).

Először azt mutatjuk meg, hogyan tekinthetők át a kanonikus alak segítségével egy szám osztói, azok száma, két szám legnagyobb közös osztója és legkisebb közös többszöröse.

1.6.2 Tétel **T 1.6.2**

Az

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

kanonikus alakú n számnak egy d pozitív egész akkor és csak akkor osztója, ha d kanonikus alakja

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \quad \text{ahol} \quad 0 \le \beta_i \le \alpha_i, \quad i = 1, 2, \dots, r. \ \clubsuit$$

Az osztók esetében a 0 kitevőt is megengedő módosított kanonikus alakot használtuk.

Az 1, illetve n triviális osztókat abban a két speciális esetben kapjuk meg, amikor (minden i-re) $\beta_i = 0$, illetve $\beta_i = \alpha_i$.

Bizonyítás: Az elégségesség igazolásához tegyük fel, hogy d a fenti alakú. Ekkor a

$$q = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_r^{\alpha_r - \beta_r}$$

szám $\alpha_i \geq \beta_i$ miatt egész, és $n = dq$, vagyis $d \mid n$. (Ennél a résznél nem használtuk ki a kanonikus alak egyértelműségét, sőt azt sem, hogy a p_i-k prímek.)

A szükségességhez tegyük fel, hogy $d \mid n$, azaz van olyan q (pozitív) egész, amellyel $n = dq$. Ekkor n kanonikus alakját a d és a q kanonikus alakjának az összeszorzásából kapjuk meg. Ez azt jelenti, hogy n kanonikus alakjában d minden prímosztója szerepel, éspedig legalább akkora hatványon, mint d-ben, vagyis $\alpha_i \geq \beta_i$. ■

Egy $n > 0$ egész pozitív osztóinak a számát $d(n)$-nel jelöljük.

Példa: $d(1) = 1$, $d(10) = 4$, $d(n) = 2 \iff n$ prím.

1.6.3 Tétel **T 1.6.3**

Az

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

kanonikus alakú n szám pozitív osztóinak a száma

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)\,. \ \clubsuit$$

Bizonyítás: Az 1.6.2 Tétel szerint az n összes pozitív osztóját úgy kapjuk meg, ha a

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

kifejezésben a $\beta_1, \beta_2, \dots, \beta_r$ kitevők egymástól függetlenül végigfutnak a

$$\beta_1 = 0, 1, \dots, \alpha_1, \quad \beta_2 = 0, 1, \dots, \alpha_2, \quad \dots, \quad \beta_r = 0, 1, \dots, \alpha_r$$

értékeken. A β_i kitevő tehát $\alpha_i + 1$-féleképpen választható, és így a $\beta_1, \dots, \beta_r$ kitevők egymástól független megválasztására összesen

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1) \tag{1}$$

lehetőség van. Mivel az n minden pozitív osztója csak egyféleképpen áll elő a fenti alakban (hiszen ennek az osztónak is egyértelmű a prímtényezős felbontása), ezért az (1) képlet valóban az n pozitív osztóinak a számát adja. ■

Most rátérünk két szám legnagyobb közös osztójának a kanonikus alakjára. Itt ismét a módosított kanonikus alakkal dolgozunk: mindkét számnál

kiírjuk azokat a prímszámokat is, amelyek csupán az egyik számnak osztói (a másik szám kanonikus alakjában ezek természetesen 0 kitevővel szerepelnek).

1.6.4 Tétel **T 1.6.4**

Legyen az a és b pozitív egészek kanonikus alakja

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}\,, \qquad \text{ahol} \qquad \alpha_i \geq 0,\ \ \beta_j \geq 0\,.$$

Ekkor

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$$

(ahol $\min(\alpha_i,\beta_i)$ az α_i és β_i számok közül a kisebbiket jelenti, ha $\alpha_i \neq \beta_i$, illetve a közös értéküket, ha $\alpha_i = \beta_i$). ♣

Bizonyítás: Legyen

$$d = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}\,.$$

Azt fogjuk megmutatni, hogy d egyrészt közös osztója a-nak és b-nek, másrészt pedig minden közös osztónak többszöröse. A bizonyításban az 1.6.2 Tételre fogunk támaszkodni.

Mivel $\min(\alpha_i,\beta_i) \leq \alpha_i$ és $\min(\alpha_i,\beta_i) \leq \beta_i$, ezért $d \mid a$ és $d \mid b$, azaz d közös osztó.

Legyen most c az a és b tetszőleges pozitív közös osztója. Ekkor

$$c = \prod_{i=1}^{r} p_i^{\gamma_i}\,, \qquad \text{ahol} \qquad \gamma_i \leq \alpha_i,\ \ \gamma_i \leq \beta_i\,.$$

Ez azt jelenti, hogy $\gamma_i \leq \min(\alpha_i,\beta_i)$, és így $c \mid d$. ■

Példa: Számítsuk ki 4840 és 2156 legnagyobb közös osztóját.

A számok kanonikus alakja: $4840 = 2^3 \cdot 5 \cdot 11^2$, illetve $2156 = 2^2 \cdot 7^2 \cdot 11$. Tehát $(4840, 2156) = 2^2 \cdot 5^0 \cdot 7^0 \cdot 11 = 44$.

Megjegyzés: A legnagyobb közös osztó fenti kiszámítási módja nagyon kényelmesnek tűnik, sajnos azonban nagy számokra általában nem alkalmazható, ugyanis nem ismerünk gyors eljárást nagy számok esetén a kanonikus alak meghatározására. Az euklideszi algoritmus ugyanakkor nagy számok esetén is gyorsan megadja a két szám legnagyobb közös osztóját. Mindezekről (alkalmazásokkal együtt) részletesen az 5.7 és 5.8 pontban lesz szó.

Rátérve a legkisebb közös többszörösre, ez nevének megfelelően a pozitív közös többszörösök közül a legkisebbet jelenti:

1.6.5 Definíció **D 1.6.5**

Az a és b pozitív egészek *legkisebb közös többszöröse* a k pozitív egész, ha

(i) $a \mid k,\ \ b \mid k$; és

(ii) ha egy $c > 0$-ra $a \mid c,\ \ b \mid c$ teljesül, akkor $c \geq k$. ♣

Az a és b legkisebb közös többszörösét $[a, b]$-vel (vagy $\mathrm{lkkt}(a, b)$-vel) jelöljük.

Mivel a két szám szorzata, ab nyilvánvalóan közös többszöröse a-nak és b-nek, így $[a, b]$ meghatározásához elég az ab-nél nem nagyobb véges sok pozitív egész között megkeresni az a és b közös többszörösei közül a legkisebbet. A legkisebb közös többszörös létezése és egyértelműsége tehát nyilvánvaló.

A legnagyobb közös osztónál látottakhoz hasonlóan azonban a legkisebb közös többszörösnél is — a definícióban szereplő „legkisebbség" helyett — inkább egy speciális oszthatósági tulajdonság játszik fontos szerepet: a legkisebb közös többszörös minden közös többszörösnek osztója (szokás a legkisebb közös többszöröst egyenesen ezzel a tulajdonsággal definiálni). Ezt és a legkisebb közös többszörösre vonatkozó további alapvető eredményeket a következő tételben foglaljuk össze:

1.6.6 Tétel **T 1.6.6**

I. Ha az a és b pozitív egészek kanonikus alakja

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}\,, \quad \text{ahol} \quad \alpha_i \geq 0,\ \ \beta_j \geq 0\,,$$

akkor

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_r^{\max(\alpha_r, \beta_r)}$$

(ahol $\max(\alpha_i, \beta_i)$ az α_i és β_i számok közül a nagyobbikat jelenti, ha $\alpha_i \neq \beta_i$, illetve a közös értéküket, ha $\alpha_i = \beta_i$).

II. $a \mid c,\ \ b \mid c \iff [a, b] \mid c$.

III. $(a, b)[a, b] = ab$. ♣

Bizonyítás: I. és II. Egy c pozitív egész akkor és csak akkor közös többszöröse a-nak és b-nek, ha $a \mid c$ és $b \mid c$ egyszerre érvényes. Ez azt jelenti, hogy c kanonikus alakjában mindegyik p_i prím γ_i kitevőjére $\gamma_i \geq \alpha_i$ és $\gamma_i \geq \beta_i$ teljesül, ez pedig azzal ekvivalens, hogy $\gamma_i \geq \max(\alpha_i, \beta_i)$.

Az ilyen c számok közül az a legkisebb, amikor egyrészt $\gamma_i = \max(\alpha_i, \beta_i)$ $(i = 1, 2, \ldots, r)$, másrészt c a p_i-ken kívül más prímekkel egyáltalán nem osztható. Ezzel beláttuk, hogy $[a, b]$ kanonikus alakja valóban az I-beli.

Azt is kaptuk, hogy az összes c közös többszörös kanonikus alakjában a p_i-k kitevője legalább akkora, mint $[a, b]$-ben, és emellett ezekben más prímek is előfordulhatnak, vagyis a c közös többszörösök éppen az $[a, b]$ többszöröseivel egyeznek meg. Ezzel II-t is igazoltuk.

III. Megmutatjuk, hogy $(a, b)[a, b]$ és ab kanonikus alakjában mindegyik p_i prím ugyanakkora kitevővel szerepel, vagyis

$$\min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) = \alpha_i + \beta_i, \qquad i = 1, 2, \ldots, r.$$

Ha például $\alpha_i \leq \beta_i$, akkor itt a bal oldalon $\alpha_i + \beta_i$ áll, ami valóban ugyanaz, mint a jobb oldal. ■

Megjegyzések: 1. A III. összefüggés fontos speciális eseteként kapjuk, hogy $ab = [a, b] \iff (a, b) = 1$.

2. Ne felejtsük el, hogy $a \mid c$ és $b \mid c$ fennállásából **nem** következik $ab \mid c$, például $4 \mid 36$, $6 \mid 36$, azonban $24 \not\mid 36$. A helyes következtetést éppen II-ből kapjuk:

$$a \mid c, \;\; b \mid c \Longrightarrow [a, b] \mid c.$$

Ha a és b relatív prímek, akkor az előző megjegyzés szerint $[a, b] = ab$, és ekkor az alábbi fontos speciális esetet nyerjük:

$$a \mid c, \;\; b \mid c, \;\; (a, b) = 1 \Longrightarrow ab \mid c.$$

Például $72 \mid c$ igazolásához elegendő azt belátni, hogy a c 8-cal és 9-cel is osztható. Általában is, bármely oszthatósági kérdés visszavezethető prím*hatvány*okkal való oszthatóságokra: ha m kanonikus alakja $m = \prod_{i=1}^{r} p_i^{\alpha_i}$ $(\alpha_i > 0)$, akkor

$$m \mid c \iff p_i^{\alpha_i} \mid c, \quad i = 1, 2, \ldots, r.$$

3. A legkisebb közös többszörös fogalma és fő tulajdonságai kettőnél több számra is átvihetők. Kiemeljük, hogy véges sok pozitív egész legkisebb közös többszöröse akkor és csak akkor egyenlő a szorzatukkal, ha páronként relatív prímek. Megjegyezzük még, hogy a III. egyenlőségnek nincs közvetlen egyszerű általánosítása több szám esetére (lásd az 1.6.15 feladatot).

A számelmélet alaptételéből (is) következik, hogy két szám akkor és csak akkor relatív prím, ha nincs közös *prím*osztójuk. Ebből azonnal adódik az alábbi tétel:

1.6.7 Tétel **T 1.6.7**

$$(c, ab) = 1 \iff (c, a) = 1 \text{ és } (c, b) = 1\,. \ \clubsuit$$

Ha két pozitív egész relatív prím, akkor általában az alábbi formában célszerű a kanonikus alakjukat megadni:

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}\,, \quad b = \prod_{j=1}^{s} q_j^{\beta_j}\,, \quad p_i \neq q_j\,.$$

Végül az $n!$ kanonikus alakját tárgyaljuk:

1.6.8 Tétel (Legendre-formula) **T 1.6.8**

Az $n!$ kanonikus alakja

$$n! = \prod_{p \le n} p^{\alpha_p}\,, \qquad \text{ahol} \qquad \alpha_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor\,. \ \clubsuit$$

A fenti képletben $\lfloor x \rfloor$ az x szám (alsó) egészrésze, és a produktum jel alatti p (pozitív) prímet jelent, azaz a szorzatot az *összes* olyan p *prím* szerint kell képezni, amelyre $p \le n$. Ilyen típusú jelölésekkel később is gyakran találkozunk majd, például

$$\sum_{p \le n} \frac{1}{p}, \qquad \prod_{p \le n} p, \qquad \sum_{p \mid n} 1$$

rendre az n-nél nem nagyobb prímek reciprokösszegét, az n-nél nem nagyobb prímek szorzatát, illetve az n különböző prímosztóinak a számát jelenti.

Megjegyezzük még, hogy az 1.6.8 Tételnél az α_p kitevőt előállító összegben elég csak véges sok tagot tekinteni, mert ha $p^k > n$, akkor $\lfloor n/p^k \rfloor = 0$ (a nemnulla tagok száma tehát $\lfloor \log_p n \rfloor$).

Bizonyítás: Mivel az $n! = 1 \cdot 2 \cdot \ldots \cdot n$ szorzat mindegyik tényezője legfeljebb n, ezért n-nél nagyobb prímszám nem fordul elő $n!$ kanonikus alakjában.

Legyen $p \le n$ tetszőleges rögzített prím, és jelölje α_p a p kitevőjét az $n!$ kanonikus alakjában. Azt kell igazolnunk, hogy

$$\alpha_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor\,. \tag{2}$$

Az α_p meghatározásához bontsuk az $1, 2, \ldots, n$ számok mindegyikét prímek szorzatára, és számoljuk össze, hogy összesen hányszor fordul elő ezek között a p.

Minden p-vel osztható számban szerepel legalább egy darab p, először ezeket vesszük számításba. A p-vel osztható számok a következők:

$$p, 2p, \ldots, tp, \quad \text{ahol} \quad tp \le n < (t+1)p\,.$$

Innen

$$t \le \frac{n}{p} < t+1, \qquad \text{vagyis} \qquad t = \left\lfloor \frac{n}{p} \right\rfloor .$$

Ez azt jelenti, hogy az $1, 2, \ldots, n$ egészek között a p-vel oszthatók száma $\lfloor n/p \rfloor$.

A p^2 többszöröseiben legalább két darab p szerepel, ezekből azonban eddig csak egyet vettünk figyelembe. Így a p^2 minden többszöröse egy-egy „újabb" p-t jelent. Ezek száma az előzőkhöz teljesen hasonlóan $\lfloor n/p^2 \rfloor$.

Ugyanígy haladunk tovább. A p^3 többszörösei egy-egy újabb p-t adnak, hiszen az ezekben előforduló legalább három darab p-ből az első két lépésben még csak kettőt vettünk figyelembe. Ez további $\lfloor n/p^3 \rfloor$ darab p-t jelent stb.

Az eljárás véges sok lépésben befejeződik, hiszen ha $p^k > n$, akkor az $1, 2, \ldots, n$ számok egyike sem osztható p^k-nal.

A fenti módon az $n!$-ban szereplő összes p-t pontosan egyszer vettük figyelembe, vagyis α_p valóban a (2)-ben megadott összeggel egyenlő. ■

Feladatok

(A feladatokban számon, osztón, prímszámon stb. mindig pozitív számot értünk.)

1.6.1 Hogyan olvasható le egy szám kanonikus alakjából, hogy négyzetszám, köbszám, illetve általában k-adik hatvány (azaz egy pozitív egész k-adik hatványa)?

1.6.2

a) Mutassuk meg, hogy ha két relatív prím szám szorzata k-adik hatvány, akkor külön-külön is k-adik hatványok.

b) Hogyan kell módosítani ezt az állítást, ha (a pozitív egészek helyett) az összes egész számot tekintjük?

c) Hogyan általánosítható az állítás (kettőnél) több tényezős szorzat esetére?

M 1.6.3 Bizonyítsuk be, hogy a) 2; b) 3; *c) 4 egymást követő (pozitív egész) szám szorzata nem lehet teljes hatvány (azaz egy egész szám egynél nagyobb egész kitevőjű hatványa).

Megjegyzés: Általában is igaz, hogy egymást követő pozitív egészek szorzata sohasem lehet teljes hatvány. Ezt a Catalantól származó és hosszú ideig megoldatlan sejtést Erdős Pál és John Selfridge bizonyították be 1975-ben.

M 1.6.4 Mely p prímszámok esetén lesz $(2^{p-1}-1)/p$ négyzetszám?

1.6.5

a) Bizonyítsuk be, hogy $c \mid ab \iff c = a_1 b_1$, ahol $a_1 \mid a$ és $b_1 \mid b$.

b) Mutassuk meg, hogy ha $(a,b) = 1$, akkor (adott $c \mid ab$-hez) a fenti a_1 és b_1 egyértelmű.

c) Lássuk be, hogy ha $(a,b) \neq 1$, akkor van olyan $c \mid ab$, amely többféleképpen is előáll $c = a_1 b_1$ alakban.

d) Bizonyítsuk be, hogy bármely $c \mid ab$ legfeljebb $d\big((a,b)\big)$-féleképpen áll elő $c = a_1 b_1$ alakban.

e) Mely $c \mid ab$ osztóknak létezik $d\big((a,b)\big)$-féle $c = a_1 b_1$ típusú előállítása?

1.6.6 Tegyük fel, hogy minden k-ra $a^k \mid b^{k+100}$. Bizonyítsuk be, hogy $a \mid b$.

1.6.7 Melyik az a legkisebb pozitív egész, amelynek pontosan
a) 31; b) 33; c) 32
(pozitív) osztója van?

1.6.8 Mely n-ekre lesz $d(n)$ páratlan?

1.6.9 Egy kegyetlen várúr börtönének 400 szűk cellájában egy-egy rab sínylődik. A cellák ajtaján levő zár úgy működik, hogy egy elfordítás esetén nyílik, még egy elfordítás esetén ismét bezárul stb. Jelenleg természetesen minden ajtó zárva van. A várúr a születésnapján elhatározza, hogy nagylelkű lesz, és megparancsolja az egyik őrnek, hogy fordítson egyet valamennyi záron. Közben azonban meggondolja magát, és utánaküld egy másik őrt, akit azzal bíz meg, hogy minden második záron fordítson egyet. Ezt követi a harmadik őr, aki minden harmadik záron változtat stb., végül a négyszázadik őr a négyszázadik cella zárjának az állását módosítja. Azok a rabok szabadulnak ki, akiknek most nyitva áll az ajtaja. Hány rabot bocsátott szabadon a várúr?

M 1.6.10 Egy természetes számot *négyzetmentes*nek nevezünk, ha nem osztható semmilyen egynél nagyobb egész szám négyzetével. Például az 1 vagy a 30 négyzetmentes, a 12 viszont nem. Egy n szám (pozitív) négyzetmentes osztóinak a számát jelöljük $A(n)$-nel, a négyzetszámosztók számát pedig $B(n)$-nel.

a) Bizonyítsuk be, hogy bármely n-re $A(n)B(n) \geq d(n)$.
b) Mely n-ekre áll egyenlőség?

1.6.11 Mutassuk meg, hogy
a) $d(n) \leq n/2 + 1$;
b) $d(n) \leq n/3 + 2$;
c) $d(n) \leq 2\sqrt{n}$.

1.6.12 Mivel egyenlő egy n szám (pozitív) osztóinak a szorzata?

1.6.13 A 10^n osztóiból maximálisan hányat lehet kiválasztani úgy, hogy ezek közül egyik se legyen osztója valamelyik másiknak?

1.6.14
a) Mely a, b számpárokhoz találhatók olyan pozitív egészek, amelyek legnagyobb közös osztója a és legkisebb közös többszöröse b?
b) Hány ilyen számpár létezik, ha $a = 5$ és $b = 35\,000$?
c) Általában is határozzuk meg az ilyen számpárok számát (tetszőleges a, b esetén).

1.6.15 Bizonyítsuk be az alábbi állításokat.
a) $(a, b, c)[a, b, c] \mid abc$, de általában nem áll fenn egyenlőség.
b) $(a, b, c)[a, b, c] = abc \iff a, b, c$ páronként relatív prímek.
c) $(a, b, c)[ab, bc, ac] = abc$.

1.6.16 Melyek igazak az alábbi állítások közül?
a) $(a, b) = (a + b, ab)$.
b) $(a, b) = 1 \iff (a + b, ab) = 1$.
c) $(a, bc) = (a, b)(a, c)$.
d) $(a^3, b^3) = (a, b)^3$.

1.6.17 Bizonyítsuk be az alábbi állításokat.
a) $[a, b] \mid a + b \iff a = b$.
b) $a + b \mid [a, b]$ sohasem teljesül.
c) Van végtelen sok olyan $a \neq b$, amelyre $a + b \mid ab$.
d) $a + b \mid ab \iff a + b \mid (a, b)^2$.

1.6.18 Lássuk be, hogy ha $(a, b^2) = (a^2, b)$, akkor $(a^7, b^{1000}) = (a^{1000}, b^7)$.

1.6.19 Igazoljuk az alábbi „disztributivitási” azonosságokat.
a) $[a, (b, c)] = ([a, b], [a, c])$.
b) $(a, [b, c]) = [(a, b), (a, c)]$.

1.6.20

a) Bizonyítsuk be, hogy az a, b és c pozitív egészekhez akkor és csak akkor létezik olyan x, y és z, amelyekkel

$$(x,y)=a,\quad (y,z)=b\quad \text{és}\quad (z,x)=c\,,$$

ha $(a,b)=(b,c)=(c,a)$.

b) Hány ilyen x, y, z számhármas létezik (adott a, b, c esetén)?

c) Vizsgáljuk meg a „duális" problémát legnagyobb közös osztók helyett legkisebb közös többszörösökre.

1.6.21 Igazoljuk, hogy ha p egy 5-nél nagyobb prím, akkor $240 \mid p^4-1$.

1.6.22 Lássuk be, hogy ha $(ab,42)=1$, akkor $504 \mid a^6-b^6$.

1.6.23 Mutassuk meg, hogy $a^6+85a^4+994a^2$ bármely a esetén osztható 360-tal.

1.6.24 Bizonyítsuk be, hogy $26^{101}-33^{101}+7^{101}$ osztható 606 606-tal.

1.6.25 Hány 0-ra végződik a) 1111!; b) $\binom{125}{60}$?

1.6.26

a) Bizonyítsuk be, hogy ha $c>1$, akkor $c^n \nmid n!$.

b) Adjuk meg azokat az $n>1$ és $c>1$ számokat, amelyekre $c^{n-1} \mid n!$.

1.6.27 Legyen $n\geq 2$ és $1\leq k\leq n-1$.

a) Mutassuk meg, hogy ha k és n relatív prímek, akkor $n \mid \binom{n}{k}$.

b) Igaz-e az a)-beli állítás megfordítása?

c) Melyek azok az n-ek, amelyekre minden $1\leq k\leq n-1$ esetén

$$\text{(c1)}\ \ n \mid \binom{n}{k};\qquad \text{(c2)}\ \ \binom{n}{k}\ \text{páros};\qquad \text{(c3)}\ \ \binom{n}{k}\ \text{páratlan?}$$

d) Van-e olyan n és $1\leq k\leq n-1$, amelyre n és $\binom{n}{k}$ relatív prímek?

M*1.6.28 Egy kerek asztal körül véges sok rozmár ül, és a következő játékot játsszák. Mindegyikük előtt egy tízforintos fekszik az asztalon. Vezényszóra mindegyik rozmár megnézi a jobb oldali szomszédja előtti tízforintost: ha fejet lát, akkor megfordítja a saját tízforintosát; ha írást lát, akkor nem csinál semmit. Ezt addig ismételgetik, amíg mindegyik tízforintos írást nem mutat. Mekkora lehet a rozmárok

száma, ha a tízforintosok tetszőleges kiinduló helyzete esetén a játék előbb-utóbb véget ér?

M*1.6.29 Mutassuk meg, hogy az $n!+1, \ldots, n!+n$ számok mindegyikének van olyan prímosztója, amely a többi $n-1$ szám egyikének sem osztója.

M 1.6.30 Tekintsünk 5000 különböző pozitív egészt, amelyek közül bármely tíznek ugyanaz a legkisebb közös többszöröse. Maximálisan hány szám lehet közöttük, amelyek páronként relatív prímek?

1.6.31 Mely n pozitív egészek rendelkeznek az alábbi tulajdonsággal: $n \mid k^2 \implies n \mid k$ (azaz n egy szám négyzetének csak úgy lehet osztója, ha magának a számnak is osztója)?

1.6.32 Mutassuk meg, hogy ($k > 1$ esetén) két k-adik hatvány különbsége sohasem lehet osztója az összegüknek.

1.6.33 Bizonyítsuk be, hogy a) $\sqrt[5]{100}$; b) $\log_6 18$ irracionális számok.

M*1.6.34 Egy tetszőleges m pozitív egészhez vegyünk minden lehetséges módon olyan $a_1 < a_2 < \ldots < a_t$ egészeket, amelyekre $a_1 = m$ és az $a_1 a_2 \ldots a_t$ szorzat négyzetszám ($t = 1$ is megengedett). Jelöljük $S(m)$-mel a_t lehető legkisebb értékét. Például $S(1) = 1$, $S(2) = 6$, mert $m = 2$ esetén a $2 \cdot 3 \cdot 6$ szorzat a legjobb választás, $S(3) = 8$, $S(4) = 4$ stb.

Bizonyítsuk be, hogy az $S(2), S(3), S(4), \ldots$ sorozatban éppen a pozitív összetett számok szerepelnek, éspedig mindegyik pontosan egyszer fordul elő.

M*1.6.35

a) Létezik-e (nem csupa azonos tagból álló) végtelen hosszú számtani sorozat csupa teljes hatványból?

b) Létezik-e (nem csupa azonos tagból álló) akármilyen hosszú (véges) számtani sorozat csupa teljes hatványból?

2. KONGRUENCIÁK

Ebben a fejezetben a kongruenciákkal kapcsolatos alapvető ismereteket tárgyaljuk. A kongruenciafogalom bevezetése után a maradékosztályokkal és maradékrendszerekkel, valamint az Euler-féle φ-függvénnyel foglalkozunk. Bebizonyítjuk az Euler–Fermat-tételt és a Wilson-tételt, ez utóbbihoz a lineáris kongruenciákat is felhasználjuk. A lineáris kongruenciákhoz kapcsolódóan áttekintjük a szimultán kongruenciarendszereket is. Az ismeretlenes kongruenciák általánosabb vizsgálatára a 3. és 4. fejezetben kerül majd sor.

2.1. Elemi tulajdonságok

oszthatósági kérdések vizsgálatánál gyakran tapasztaljuk, hogy tulajdonképpen csak egy adott számmal való osztási maradék számít, vagyis teljesen egyformán viselkednek azok az egészek, amelyeknek az adott számmal osztva azonos a maradéka. Ez (is) indokolja a következő fogalom bevezetését:

2.1.1 Definíció **D 2.1.1**

Legyenek a és b egész számok és m pozitív egész. Azt mondjuk, hogy a *kongruens* b-vel modulo m, ha $m \mid a-b$. ♣

Jelölés: $a \equiv b \pmod{m}$ vagy röviden $a \equiv b\ (m)$. Az (általában rögzített) m számot *modulus*nak nevezzük.

Mivel $m \mid a-b \iff m \mid b-a$, ezért

$$a \equiv b \pmod{m} \iff b \equiv a \pmod{m},$$

és így helyes az „a és b kongruensek modulo m" szóhasználat is. (A „modulo m" helyett a „mod m" vagy „az m modulusra nézve" vagy „az m modulus szerint" kifejezéseket is szokás mondani.)

Az is világos, hogy a és b akkor és csak akkor kongruensek modulo m, ha a és b az m-mel osztva ugyanazt a maradékot adják. (Itt maradékon a szokásos legkisebb nemnegatív maradékot értjük, de ugyanez érvényes akkor is, ha — mindkét számnál — a legkisebb abszolút értékű maradékról van szó.)

Ha a és b nem kongruensek modulo m, akkor ezt $a \not\equiv b \pmod{m}$ jelöli, és azt mondjuk, hogy a és b *inkongruens*ek modulo m (vagy a inkongruens b-vel modulo m).

Példa: $11 \equiv 5 \pmod 3$; $32 \equiv -1 \ (11)$; $21 \not\equiv 6 \pmod{10}$.

Nyilván bármely két egész szám kongruens az $m = 1$ modulus szerint.

A kongruencia definíciója minden változtatás nélkül kiterjeszthető lenne az $m < 0$ esetre is. Ezzel azonban nem érdemes külön foglalkozni, ugyanis $m \mid a - b \iff -m \mid a - b$.

2.1.2 Tétel **T 2.1.2**

(i) Minden a-ra $a \equiv a \pmod m$.

(ii) $a \equiv b \pmod m \Longrightarrow b \equiv a \pmod m$.

(iii) $a \equiv b \pmod m$, $b \equiv c \pmod m \Longrightarrow a \equiv c \pmod m$.

(iv) $a \equiv b \pmod m$, $c \equiv d \pmod m \Longrightarrow a + c \equiv b + d \pmod m$ és $a - c \equiv b - d \pmod m$.

(v) $a \equiv b \pmod m$, $c \equiv d \pmod m \Longrightarrow ac \equiv bd \pmod m$. ♣

Bizonyítás: Valamennyi állítás könnyen adódik a kongruencia definíciójából és az oszthatóság elemi tulajdonságaiból, ezért mintaként csak az (v) tulajdonságot igazoljuk.

A feltétel szerint $m \mid a - b$ és $m \mid c - d$, amiből

$$m \mid c(a - b) + b(c - d) = ac - bd, \qquad \text{azaz} \qquad ac \equiv bd \pmod m$$

következik. ■

Az (i), (ii) és (iii) tulajdonságok azt fejezik ki, hogy a kongruencia *reflexív*, *szimmetrikus* és *tranzitív* reláció, azaz *ekvivalenciareláció*. Ennek alapján az egész számokat (páronként) diszjunkt halmazok egyesítésére lehet bontani: egy halmazba kerülnek az „egymással kongruens" számok, vagyis azok, amelyek ugyanolyan maradékot adnak m-mel osztva (az idézőjeles kijelentésnek éppen az (i)–(iii) tulajdonságok alapján van egyáltalán értelme). Ezek a halmazok lesznek a modulo m *maradékosztály*ok, amelyekkel részletesen a 2.2 pontban foglalkozunk.

A (iv) és (v) tulajdonságok alapján a(z ugyanazon modulus szerinti) kongruenciák „összeadhatók, kivonhatók és összeszorozhatók." Ezekből azonnal következik, hogy egy kongruencia mindkét oldalához hozzáadhatjuk ugyanazt a számot, és ugyanez vonatkozik a kivonásra és a szorzásra is, továbbá egy kongruenciát önmagával is akárhányszor összeszorozhatunk, vagyis egy kongruenciát szabad (pozitív egész kitevős) hatványra emelni:

(vi) $a \equiv b \pmod{m} \Longrightarrow a + c \equiv b + c \pmod{m}$ és $a - c \equiv b - c \pmod{m}$.

(vii) $a \equiv b \pmod{m} \Longrightarrow ac \equiv bc \pmod{m}$.

(viii) $a \equiv b \pmod{m} \Longrightarrow a^n \equiv b^n \pmod{m}$.

Mindezek ismételt alkalmazásával az alábbi jól használható összefüggést nyerjük:

(ix) Legyen f egy egész együtthatós polinom. Ekkor

$$a \equiv b \pmod{m} \Longrightarrow f(a) \equiv f(b) \pmod{m}.$$

A fentiek alkalmazására néhány egyszerű példát mutatunk.

Példák:

P1 Bizonyítsuk be, hogy bármely n természetes számra

$$17 \mid 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n\,.$$

Megoldás: Azt kell belátni, hogy

$$3^{3n+1}5^{2n+1} + 2^{5n+1}11^n \equiv 0 \pmod{17}.$$

A bal oldalt a fenti tulajdonságok felhasználásával vele kongruens kifejezésekké alakítjuk, amíg 0-t nem kapunk:

$$\begin{aligned} 3^{3n+1}5^{2n+1} + 2^{5n+1}11^n &= 3 \cdot 27^n \cdot 5 \cdot 25^n + 2 \cdot 32^n \cdot 11^n \equiv \\ &\equiv 15(-7)^n 8^n + 2(-2)^n(-6)^n = \\ &= 15(-56)^n + 2(12)^n \equiv 15(-5)^n + 2(-5)^n = \\ &= 17(-5)^n \equiv 0 \pmod{17}. \end{aligned}$$

P2 Igazoljuk (újra) az $a - b \mid a^n - b^n$ oszthatóságot.

Megoldás: Nyilván elég az $a - b > 0$ esetre szorítkozni. alkalmazzuk (viii)-at:

$$a \equiv b \pmod{a-b} \Longrightarrow a^n \equiv b^n \pmod{a-b}.$$

P3 Mutassuk meg, hogy $2^{32}+1$ összetett szám. (Vesd össze az 1.4.4 feladattal és az 5.2 ponttal.)

Megoldás: Azt látjuk be, hogy $641 \mid 2^{32}+1$. Ehhez felhasználjuk, hogy

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1.$$

Ezekből

$$-1 \equiv 5 \cdot 2^7 \pmod{641} \qquad \text{és} \qquad 5^4 \equiv -2^4 \pmod{641}.$$

Az első kongruenciát negyedik hatványra emelve, majd behelyettesítve a másodikat, azt kapjuk, hogy

$$1 = (-1)^4 \equiv 5^4 \cdot 2^{28} \equiv -2^4 \cdot 2^{28} = -2^{32} \pmod{641},$$

azaz $641 \mid 2^{32}+1$.

Láttuk, hogy az összeadás, kivonás és szorzás műveletére vonatkozóan a kongruenciák ugyanúgy viselkednek, mint az egyenlőségek. Az osztás műveleténél azonban jelentős eltérés van, két kongruenciát **nem szabad** egymással elosztani. Először is, osztáskor nem feltétlenül kapunk egész számokat, és ekkor a hányadosok közötti kongruenciának eleve nem is lehet értelme, hiszen a kongruenciákban egész számoknak kell szerepelniük. Azonban még abban az esetben sem lesz általában igaz az osztáskor kapott kongruencia, ha az osztás után mindkét oldalon egész számok maradnak. Például

$$28 \equiv 46 \pmod{6} \quad \text{és} \quad 2 \equiv 2 \pmod{6}, \quad \text{azonban} \quad 14 \not\equiv 23 \pmod{6}.$$

A kongruenciák osztására vonatkozó tilalommal kapcsolatban azt se felejtsük el, hogy a tört is tulajdonképpen osztást jelent. Ezért egy egész értékű tört számlálójába és/vagy nevezőjébe akkor sem szabad vele kongruens számot írni, ha a hányados továbbra is egész marad. Például:

$$45 \equiv 35 \pmod{10} \quad \text{és} \quad 15 \equiv 5 \pmod{10}, \quad \text{de} \quad 3 = \frac{45}{15} \not\equiv \frac{35}{5} = 7 \pmod{10}.$$

A tiltások után térjünk rá arra, hogy ebben a kérdéskörben mi az, ami megengedett. Csak az osztás speciális esetével, az egyszerűsítéssel foglalkozunk. Az alábbi tétel azt mondja ki, hogy az egyszerűsítést csak úgy lehet elvégezni, hogy közben *a modulust is meg kell változtatni*:

2.1.3 Tétel **T 2.1.3**

Legyen $d = (c, m)$. Ekkor

$$ac \equiv bc \pmod{m} \iff a \equiv b \pmod{\frac{m}{d}}\,. \clubsuit$$

Bizonyítás: A kongruencia definíciója alapján

$$ac \equiv bc \pmod{m} \iff m \mid (a-b)c\,,$$

ami tovább ekvivalens az

$$\frac{m}{d} \,\Big|\, (a-b)\frac{c}{d} \tag{1}$$

oszthatósággal. Mivel $(m/d, c/d) = 1$, ezért (1) pontosan akkor teljesül, ha

$$\frac{m}{d} \,\Big|\, a-b\,, \qquad \text{azaz} \qquad a \equiv b \pmod{\frac{m}{d}}\,. \blacksquare$$

A 2.1.3 Tétel fontos speciális eseteként kapjuk, hogy ha c és a modulus relatív prímek, akkor a c-vel történő egyszerűsítés után a kongruencia változatlan modulus mellett érvényben marad:

2.1.3A Tétel **T 2.1.3A**

$$ac \equiv bc \pmod{m},\ \ (c, m) = 1 \Longrightarrow a \equiv b \pmod{m}\,. \clubsuit$$

Feladatok

2.1.1 Bizonyítsuk be, hogy $23 \mid 61^{k+1} + 11^k 7^{2k} 3^{3k} 2^{5k+3}$.

2.1.2 Adjuk meg $999^{777^{888}}$ utolsó három számjegyét (tízes számrendszerben).

2.1.3 Bizonyítsuk be (újra) a 9-cel és a 11-gyel való oszthatósági szabályokat (1.1.14 feladat) és ezek más alapú számrendszerre történő általánosításait (1.2.14 feladat) a kongruenciák segítségével.

2.1.4 Melyek igazak az alábbi állítások közül?

a) $k \mid n,\ \ a \equiv b \pmod{n} \Longrightarrow a \equiv b \pmod{k}$.

b) $k \mid n,\ \ a \equiv b \pmod{k} \Longrightarrow a \equiv b \pmod{n}$.

c) $a \equiv b \pmod{n}$, $a \equiv b \pmod{k} \iff a \equiv b \pmod{kn}$.

d) $a \equiv b \pmod{n}$, $a \equiv b \pmod{k} \iff a \equiv b \pmod{[k, n]}$.

e) $a \equiv b \pmod{n} \iff ka \equiv kb \pmod{kn}$.

f) $a \equiv b \pmod{n}$, $c \equiv d \pmod{k} \implies ac \equiv bd \pmod{kn}$.

g) $a^2 \equiv b^2 \pmod{n} \implies a \equiv \pm b \pmod{n}$.

h) $a^2 \equiv b^2 \pmod{101} \implies a \equiv \pm b \pmod{101}$.

2.1.5 A tízes számrendszerben több olyan számjegy is van, amelyre nem végződhet négyzetszám. Hány ilyen számjegy van a 101 alapú számrendszerben?

2.1.6 Kommentáljuk Butus Maximus professzor alábbi „tételét" és „bizonyítását":
„Tétel: Bármely $n > 3$ egészre $\binom{n}{4} \equiv \binom{n+1}{4} \pmod{4}$.
Bizonyítás: Mivel bármely n egészre $n + 1 \equiv n - 3 \pmod{4}$, ezért

$$\binom{n}{4} = \frac{n(n-1)(n-2)(n-3)}{1 \cdot 2 \cdot 3 \cdot 4} \equiv$$
$$\equiv \frac{n(n-1)(n-2)(n+1)}{1 \cdot 2 \cdot 3 \cdot 4} = \binom{n+1}{4} \pmod{4}."$$

2.1.7 Bizonyítsuk be: $m \mid a - b \implies m^2 \mid a^m - b^m$.

2.1.8 Tegyük fel, hogy $3 \nmid a$, $(6, n) = 1$ és $a^n \equiv b^n \pmod{3^n}$. Mutassuk meg, hogy ekkor $a \equiv b \pmod{3^n}$.

2.1.9 Legyen $p > 2$ prím, $1 \leq k \leq p - 1$. Igazoljuk az alábbi modulo p kongruenciákat:

a) $\binom{p}{k} \equiv 0$; b) $\binom{p-1}{k} \equiv (-1)^k$; c) $\binom{p-2}{k} \equiv (-1)^k(k+1)$.

2.1.10 Határozzuk meg az(oka)t a p prím(ek)et, amelyekre $\binom{3p}{p}$ a p-vel osztva $p - 2$ maradékot ad.

*2.1.11 Legyen p prím. Bizonyítsuk be a következő modulo p kongruenciákat:

a) $\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor$; b) $\binom{n}{kp} \equiv \binom{\lfloor n/p \rfloor}{k}$; c) $\binom{n}{p^k} \equiv \left\lfloor \frac{n}{p^k} \right\rfloor$.

2.2. Maradékosztályok és maradékrendszerek

A modulo m maradékosztály fogalmát már a 2.1.2 Tétel után megemlítettük: azok az egész számok tartoznak egy maradékosztályba, amelyek m-mel osztva azonos maradékot adnak.

2.2.1 Definíció **D 2.2.1**

Rögzített m modulus mellett az a-val kongruens elemek halmazát az a által reprezentált *maradékosztály*nak nevezzük. ♣

Jelölés: $(a)_m$. Ha nem okoz félreértést, akkor a modulusra utaló m indexet elhagyjuk.

Az $(a)_m$ maradékosztály tehát egy „mindkét irányban végtelen számtani sorozat", amelynek egyik eleme a és a differenciája m. A modulo m maradékosztályok száma m, és minden maradékosztálynak végtelen sok eleme van. A definíció alapján $(a)_m = (c)_m \iff a \equiv c \pmod{m}$.

Példa: $(23)_7 = \{\ldots, -5, 2, 9, 16, 23, 30, \ldots\} = (100)_7$.

2.2.2 Definíció **D 2.2.2**

Ha rögzített m modulus mellett minden maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo m *teljes maradékrendszer*nek nevezzük. ♣

Példa: $\{33, -5, 11, -11, -8\}$ teljes maradékrendszer modulo 5.

A leggyakrabban a következő teljes maradékrendszereket használjuk:

(A) legkisebb nemnegatív maradékok: $0, 1, \ldots, m-1$.

(B) legkisebb abszolút értékű maradékok:

$$0,\ \pm1,\ \pm2,\ \ldots,\ \pm\frac{m-1}{2}, \qquad \text{ha } m \text{ páratlan},$$

illetve

$$0,\ \pm1,\ \pm2,\ \ldots,\ \pm\frac{m-2}{2},\ \frac{m}{2}, \qquad \text{ha } m \text{ páros}$$

(nyilván ez utóbbi esetben $m/2$ helyett $-m/2$ is vehető).

Azt, hogy adott számok teljes maradékrendszert alkotnak-e, általában az alábbi egyszerű kritérium alapján tudjuk gyorsan eldönteni:

2.2.3 Tétel **T 2.2.3**

Adott egész számok akkor és csak akkor alkotnak teljes maradékrendszert modulo m, ha

(i) számuk m, és

(ii) páronként inkongruensek modulo m. ♣

Bizonyítás: Legyen T_m egy teljes maradékrendszer modulo m. Mivel a modulo m maradékosztályok száma m, és minden maradékosztályból egy elemet vettünk ki, ezért T_m elemszáma szükségképpen m. Továbbá egyetlen maradékosztályból sem választottunk egynél több elemet, ezért T_m elemei páronként inkongruensek modulo m.

Megfordítva, tekintsünk m darab páronként inkongruens számot modulo m. A páronkénti inkongruencia miatt ezek csupa különböző maradékosztályba tartoznak, és mivel a számuk m, ezért m darab maradékosztályt reprezentálnak, azaz az összeset. Így ezek a számok valóban teljes maradékrendszert alkotnak modulo m. ■

Ha egy teljes maradékrendszert a modulushoz relatív prím számmal végigszorzunk, és ehhez egy tetszőleges egészt hozzáadunk, akkor ismét teljes maradékrendszert kapunk:

2.2.4 Tétel **T 2.2.4**

Legyen $r_1, r_2, \ldots, r_m$ teljes maradékrendszer modulo m, $(a, m) = 1$ és b tetszőleges. Ekkor

$$ar_1 + b,\ ar_2 + b, \ldots, ar_m + b$$

is teljes maradékrendszer modulo m. ♣

Bizonyítás: Mivel az új rendszer elemszáma is m, tehát a 2.2.3 Tétel alapján azt kell még bizonyítani, hogy az elemei páronként inkongruensek mod m.

Tegyük fel, hogy $ar_i + b \equiv ar_j + b \pmod{m}$, megmutatjuk, hogy $i = j$.

Mindkét oldalból b-t kivonva $ar_i \equiv ar_j \pmod{m}$ adódik.

Mivel $(a, m) = 1$, ezért a 2.1.3A Tétel alapján egyszerűsíthetünk a-val: $r_i \equiv r_j \pmod{m}$, és így valóban $i = j$. ■

Megjegyezzük, hogy ha $(a, m) \neq 1$, akkor az $ar_i + b$ számok sohasem alkotnak teljes maradékrendszert, lásd a 2.2.11 feladatot.

Most azt vizsgáljuk meg, hogy a modulushoz relatív prím egészek hogyan helyezkednek el az egyes maradékosztályokban. Megmutatjuk, hogy egy maradékosztálynak vagy az összes eleme relatív prím a modulushoz, vagy pedig

egyetlen eleme sem relatív prím hozzá:

$$\text{Legyen } a \equiv b \pmod{m}. \text{ Ekkor } (a,m) = 1 \iff (b,m) = 1\,.$$

Az alábbi tételben ennél erősebb állítást bizonyítunk:

2.2.5 Tétel **T 2.2.5**

$$a \equiv b \pmod{m} \implies (a,m) = (b,m)\,. \ \clubsuit$$

Bizonyítás: A feltétel szerint $b = a + mc$ teljesül alkalmas c egésszel.

Mivel itt a jobb oldalon a és m is osztható (a,m)-mel, ezért $(a,m) \mid b$. Ez azt jelenti, hogy (a,m) közös osztója b-nek és m-nek, és így $(a,m) \mid (b,m)$.

Ugyanígy adódik a fordított irányú $(b,m) \mid (a,m)$ oszthatóság is, tehát valóban $(a,m) = (b,m)$. ■

Fontos szerepet játszanak azok a maradékosztályok, amelyeknek az elemei relatív prímek a modulushoz:

2.2.6 Definíció **D 2.2.6**

Az $(a)_m$ maradékosztályt modulo m *redukált* maradékosztálynak nevezzük, ha $(a,m) = 1$. ♣

Mint már említettük, a 2.2.5 Tételből következik, hogy ha egy maradékosztálynak van olyan eleme, amely relatív prím a modulushoz, akkor a maradékosztály minden eleme ilyen. Ezért a 2.2.6 Definíció nem függ attól, hogy az $(a)_m$ maradékosztályt melyik elemével reprezentáltuk.

Most bevezetjük a számelmélet egyik legfontosabb függvényét:

2.2.7 Definíció (Euler-féle φ-függvény) **D 2.2.7**

Tetszőleges n pozitív egész esetén $\varphi(n)$ az $1, 2, \ldots, n$ számok közül az n-hez relatív prímek számát jelenti. ♣

Példa: $\varphi(1) = 1, \quad \varphi(10) = 4, \quad \varphi(n) = n - 1 \iff n$ prím.

Világos, hogy $\varphi(n)$ éppen a modulo n redukált maradékosztályok száma.

Az n kanonikus alakjából könnyen kiszámítható $\varphi(n)$ értéke, ezt a képletet a 2.3 pontban tárgyaljuk.

Most a teljes maradékrendszer mintájára a redukált maradékrendszer fogalmát definiáljuk:

2.2.8 Definíció **D 2.2.8**

Ha rögzített m modulus mellett minden *redukált* maradékosztályból egy és csak egy elemet kiveszünk, az így kapott számokat modulo m *redukált maradékrendszer*nek nevezzük. ♣

Példa: $\{17, -5, 11, -11\}$ redukált maradékrendszer modulo 12.

A legegyszerűbben úgy gyárthatunk redukált maradékrendszereket, ha a legkisebb nemnegatív maradékokból, illetve a legkisebb abszolút értékű maradékokból kiválasztjuk a modulushoz relatív prímeket.

A következőkben bebizonyítjuk a 2.2.3 és 2.2.4 Tételeknek a redukált maradékrendszerekre vonatkozó megfelelőit.

2.2.9 Tétel **T 2.2.9**

Adott egész számok akkor és csak akkor alkotnak redukált maradékrendszert modulo m, ha

(i) számuk $\varphi(m)$,
(ii) páronként inkongruensek modulo m, és
(iii) valamennyien relatív prímek m-hez. ♣

Bizonyítás: Legyen R_m egy redukált maradékrendszer modulo m. Mivel a modulo m redukált maradékosztályok száma $\varphi(m)$, és minden maradékosztályból egy elemet vettünk ki, ezért R_m elemszáma szükségképpen $\varphi(m)$. Továbbá egyetlen maradékosztályból sem választottunk egynél több elemet, ezért R_m elemei páronként inkongruensek modulo m. Végül R_m minden eleme relatív prím m-hez, hiszen ezeket redukált maradékosztályokból választottuk.

Megfordítva, tekintsünk $\varphi(m)$ darab, az m-hez relatív prím számot, amelyek páronként inkongruensek modulo m. A páronkénti inkongruencia és az m-hez relatív prímség miatt ezek csupa különböző redukált maradékosztályba tartoznak. Mivel a számuk $\varphi(m)$, ezért $\varphi(m)$ darab redukált maradékosztályt reprezentálnak, azaz az összeset. Így ezek a számok valóban redukált maradékrendszert alkotnak modulo m. ■

2.2.10 Tétel **T 2.2.10**

Legyen $r_1, r_2, \ldots, r_{\varphi(m)}$ redukált maradékrendszer modulo m és $(a, m) = 1$. Ekkor

$$ar_1,\ ar_2, \ldots, ar_{\varphi(m)}$$

is redukált maradékrendszer modulo m. ♣

Bizonyítás: A 2.2.9 Tétel (i)–(iii) kritériumát ellenőrizzük.

(i) Az új rendszer elemszáma is $\varphi(m)$.

(ii) $ar_i \equiv ar_j \pmod m$, $(a,m)=1 \Longrightarrow r_i \equiv r_j \pmod m \Longrightarrow i=j$.

(iii) $(a,m)=1$, $(r_i,m)=1 \Longrightarrow (ar_i,m)=1$. ■

Ha $(a,m)\neq 1$, akkor az ar_i számok sohasem alkotnak redukált maradékrendszert, sőt ezen elemek egyike sem lesz relatív prím az m-hez.

A teljes maradékrendszernél látottakhoz képest jelentős eltérés, hogy a redukált maradékrendszer elemeihez egy b számot hozzáadva már általában nem kapunk redukált maradékrendszert, lásd a 2.2.12 feladatot.

Feladatok

Valamennyi feladatban feltesszük, hogy a modulus $m \geq 2$.

2.2.1 Határozzuk meg az m modulust, ha tudjuk, hogy az alábbi elemek ugyanannak a modulo m redukált maradékosztálynak az elemei:
a) 2 és 14; b) 18, 78 és 178; c) a és $-a$.

2.2.2 Hány olyan
a) teljes; b) redukált
maradékrendszer van modulo m, amelynek minden a_i elemére $0 \leq a_i \leq 5m+1$ teljesül?

2.2.3 Melyek azok a mindkét irányban végtelen számtani sorozatok, amelyekből kiválasztható egy modulo m
a) maradékosztály; b) teljes maradékrendszer?

2.2.4 Milyen $m \geq 2$ esetén létezik olyan teljes maradékrendszer, amelynek elemei
a) páratlan számok;
b) összetett számok;
c) négyzetszámok;
d) (tízes számrendszerben) 1357-re végződő számok;
e) mértani sorozatot alkotnak;
M *f) „csupaegyek” (azaz tízes számrendszerben minden számjegyük 1-es);
M *g) teljes hatványok?

2.2.5 Milyen $m \geq 2$ esetén létezik olyan redukált maradékrendszer, amelynek elemei
a) 15-tel osztható számok;
b) 15-tel nem osztható számok;
c) négyzetszámok;

d) (tízes számrendszerben) 1357-re végződő számok;
e) teljes hatványok?

2.2.6 Melyek igazak az alábbi állítások közül?

a) Ha $r_1, r_2, \ldots, r_k$ redukált maradékrendszer modulo 7, akkor $r_1, r_2, \ldots, r_k$ redukált maradékrendszer modulo 14 is.

b) Ha $r_1, r_2, \ldots, r_k$ redukált maradékrendszer modulo 14, akkor $r_1, r_2, \ldots, r_k$ redukált maradékrendszer modulo 7 is.

2.2.7

a) Milyen maradékot ad m-mel osztva egy modulo m teljes maradékrendszer elemeinek az összege?

b) Legyen m páros, és $a_1, a_2, \ldots, a_m$, valamint $b_1, b_2, \ldots, b_m$ egy-egy teljes maradékrendszer modulo m. Bizonyítsuk be, hogy az $a_1 + b_1, \ldots, a_m + b_m$ elemek *sohasem* alkotnak teljes maradékrendszert modulo m. Mit állíthatunk páratlan m esetén?

c) Vizsgáljuk meg az analóg kérdéseket teljes maradékrendszerek helyett redukált maradékrendszerekre is.

M 2.2.8

a) Egy kör alakú tisztás mentén m fa áll, mindegyiken egy-egy mókus. A mókusok össze szeretnének gyűlni egy fán, de csak úgy változtathatják a helyüket, hogy két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára. Ezt a lépést akárhányszor ismételhetik. Milyen m esetén tudnak összegyűlni a mókusok?

b) Mi a helyzet akkor, ha a megengedett lépést a következőképpen módosítjuk: két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára, azonban ellenkező körüljárási irányba kell ugorniuk.

*2.2.9

a) Mely m-ek esetén alkotnak a $0, 0+1, 0+1+2, \ldots, 0+1+2+\ldots+(m-1)$ számok teljes maradékrendszert modulo m?

b) Mely m-ek esetén létezik olyan $a_1, \ldots, a_m$ teljes maradékrendszer modulo m, amelyre az $a_1, a_1+a_2, a_1+a_2+a_3, \ldots, a_1+a_2+a_3+\ldots+a_m$ számok is teljes maradékrendszert alkotnak modulo m?

2.2.10 Legyen $k \mid m$. Melyek igazak az alábbi állítások közül?

a) Bármely modulo k maradékosztály előáll modulo m maradékosztályok egyesítéseként.

b) Bármely modulo k redukált maradékosztály előáll modulo m redukált maradékosztályok egyesítéseként.

*c) Bármely modulo k redukált maradékosztálynak van olyan részhalmaza, amely egy modulo m redukált maradékosztályt alkot.

d) Bármely modulo k redukált maradékrendszer kiegészíthető egy modulo m redukált maradékrendszerré.

*e) Bármely modulo m redukált maradékrendszerből kiválasztható egy modulo k redukált maradékrendszer.

2.2.11 Legyen $r_1, r_2, \ldots, r_m$ teljes maradékrendszer modulo m, $(a, m) \neq 1$ és b tetszőleges.

a) Bizonyítsuk be, hogy $ar_1 + b, \ldots, ar_m + b$ sohasem alkotnak teljes maradékrendszert modulo m.

b) Összesen hány modulo m maradékosztályt reprezentálnak az $ar_1 + b, \ldots, ar_m + b$ elemek?

M*2.2.12 Legyen $r_1, r_2, \ldots, r_{\varphi(m)}$ redukált maradékrendszer modulo m.

a) Adjuk meg az összes olyan a számot, amelyre az $ar_1, \ldots, ar_{\varphi(m)}$ elemek páronként inkongruensek modulo m.

b) Adjuk meg az összes olyan b számot, amelyre az $r_1 + b, \ldots, r_{\varphi(m)} + b$ elemek is redukált maradékrendszert alkotnak modulo m.

M*2.2.13 Milyen m és k számokhoz létezik olyan $a_1, \ldots, a_m$ teljes maradékrendszer modulo m és $b_1, \ldots, b_k$ teljes maradékrendszer modulo k, hogy az $a_i b_j$ számok teljes maradékrendszert alkotnak modulo mk?

M2.2.14 Legyenek a és b pozitív egészek.

a) Bizonyítsuk be, hogy

$$T = \{ib + ja \mid i = 1, 2, \ldots, a,\ \ j = 1, 2, \ldots, b\}$$

akkor és csak akkor alkot teljes maradékrendszert modulo ab, ha $(a, b) = 1$.

b) Legyen $r_1, \ldots, r_{\varphi(a)}$, illetve $s_1, \ldots, s_{\varphi(b)}$ redukált maradékrendszer modulo a, illetve modulo b. Bizonyítsuk be, hogy

$$R = \{r_i b + s_j a \mid i = 1, 2, \ldots, \varphi(a),\ \ j = 1, 2, \ldots, \varphi(b)\}$$

akkor és csak akkor alkot redukált maradékrendszert modulo ab, ha $(a, b) = 1$.

c) Mutassuk meg, hogy ha $(a, b) = 1$, akkor $\varphi(ab) = \varphi(a)\varphi(b)$.

2.3. Az Euler-féle φ-függvény

Az Euler-féle φ-függvényt a 2.2.7 Definícióban értelmeztük: Tetszőleges n pozitív egész esetén $\varphi(n)$ az $1, 2, \ldots, n$ számok közül az n-hez relatív prímek számát jelenti.

Ebből azonnal következett, hogy $\varphi(m)$ darab modulo m redukált maradékosztály létezik, és egy modulo m redukált maradékrendszer elemeinek a száma is $\varphi(m)$.

Most egy olyan képletet bizonyítunk, amely az n kanonikus alakjának segítségével megadja $\varphi(n)$ értékét:

2.3.1 Tétel **T 2.3.1**

Legyen n kanonikus alakja

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i}\,, \qquad \text{ahol} \qquad \alpha_i > 0\,.$$

Ekkor

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \ldots \left(p_r^{\alpha_r} - p_r^{\alpha_r - 1}\right) = \prod_{i=1}^{r} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)\,. \ \clubsuit$$

Felhívjuk a figyelmet arra, hogy $\varphi(n)$ fenti képlete csak akkor érvényes, ha az n kanonikus alakjában az α_i kitevők valóban pozitívak (szemben például a $d(n)$-re az 1.6.3 Tételben adott képlettel, amely akkor is igaz marad, ha megengedjük, hogy az α_i kitevők között a nulla is előforduljon).

A fenti képlet néhány másik, ekvivalens alakja:

$$\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n \prod_{\substack{p \mid n \\ p \text{ prím}}} \left(1 - \frac{1}{p}\right)\,.$$

A 2.3.1 Tételre két bizonyítást adunk. Egy harmadik bizonyítás leolvasható a 6.5.4b feladatból. Emellett az első bizonyításban döntő fontosságú II. állítás két további igazolási módja is szerepel a 2.2.14, illetve 2.6.10 feladatokban.

Első bizonyítás: A tételt az alábbi két állításra vezetjük vissza:

I. Ha p prím (és $\alpha > 0$), akkor $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
II. Ha $(a, b) = 1$, akkor $\varphi(ab) = \varphi(a)\varphi(b)$.

Ezekből a tétel valóban következik. Ugyanis II-ből a tényezők száma szerinti teljes indukcióval kapjuk, hogy ha az $a_1, \ldots, a_r$ számok *páronként* relatív prímek, akkor $\varphi(a_1 \ldots a_r) = \varphi(a_1) \ldots \varphi(a_r)$. Ha ezt $a_i = p_i^{\alpha_i}$-re alkalmazzuk, és $\varphi(p_i^{\alpha_i})$ helyére az I-ben szereplő értéket beírjuk, akkor éppen a bizonyítandó képlet adódik.

Rátérünk az I. állítás igazolására. Egy szám p^α-hoz akkor és csak akkor relatív prím, ha nem osztható p-vel. Ennélfogva az $1, 2, \ldots, p^\alpha$ egészek közül úgy kapjuk meg a p^α-hoz relatív prímeket, ha elhagyjuk a p-vel oszthatókat. Ez utóbbiak a $p, 2p, \ldots, p^{\alpha-1}p$, és így számuk $p^\alpha/p = p^{\alpha-1}$. Ebből következik, hogy a megmaradók száma $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Nézzük most a II. állítás bizonyítását. (Mint már jeleztük, ennek két másik lehetséges módja szerepel a 2.2.14, illetve 2.6.10 feladatban.)

A $\varphi(ab)$ érték azoknak az ab-nél nem nagyobb pozitív egészeknek a számát jelenti, amelyek relatív prímek ab-hez, azaz relatív prímek a-hoz és b-hez is.

Jelöljük a modulo a redukált maradékosztályok legkisebb pozitív elemeit $r_1, r_2, \ldots, r_{\varphi(a)}$-val, és írjuk fel az ab-nél nem nagyobb pozitív egészek közül azokat, amelyek a-hoz relatív prímek:

$$\begin{array}{rrcr} r_1 & r_2 & \ldots & r_{\varphi(a)} \\ a + r_1 & a + r_2 & \ldots & a + r_{\varphi(a)} \\ 2a + r_1 & 2a + r_2 & \ldots & 2a + r_{\varphi(a)} \\ \vdots & \vdots & & \vdots \\ (b-1)a + r_1 & (b-1)a + r_2 & \ldots & (b-1)a + r_{\varphi(a)} \end{array} \tag{1}$$

Ezek közül kell kiválasztani azokat a számokat, amelyek b-hez is relatív prímek.

Tekintsük evégett az (1) táblázat egy tetszőleges oszlopát. Például az i-edik oszlop elemei a következők:

$$r_i,\ a + r_i,\ 2a + r_i,\ \ldots,\ (b-1)a + r_i\,. \tag{2}$$

Ezek az elemek úgy jöttek létre, hogy a $0, 1, \ldots, b-1$ modulo b teljes maradékrendszer elemeit a b-hez relatív prím a-val megszoroztuk, majd az így kapott számokhoz r_i-t hozzáadtunk. A 2.2.4 Tétel alapján ekkor (2) is teljes maradékrendszer modulo b, vagyis az (1) táblázat minden oszlopában egy-egy modulo b teljes maradékrendszer áll.

Mivel egy modulo b teljes maradékrendszerben $\varphi(b)$ számú b-hez relatív prím elem szerepel, ezért az (1) táblázat minden oszlopában $\varphi(b)$ darab olyan elem van, amely relatív prím b-hez.

Az (1) táblázatban az oszlopok száma $\varphi(a)$, így a táblázatnak összesen $\varphi(a)\varphi(b)$ eleme relatív prím a b-hez.

Ez azt jelenti, hogy az ab-nél nem nagyobb pozitív egészek között $\varphi(a)\varphi(b)$ olyan van, amely a-hoz és b-hez is, vagyis ab-hez relatív prím. Ez a szám másrészt definíció szerint éppen $\varphi(ab)$, tehát valóban $\varphi(ab) = \varphi(a)\varphi(b)$. ■

Második bizonyítás: A logikai szitaformulát alkalmazzuk.

Az $1, 2, \ldots, n$ egészek közül azoknak a számát kell meghatározni, amelyek relatív prímek n-hez, azaz a $p_1, p_2, \ldots, p_r$ prímek egyikével sem oszthatók.

Ehhez az $1, 2, \ldots, n$ közül „ki kell szitálni a rossz tulajdonságúakat", vagyis azokat, amelyek egy vagy több p_j-vel oszthatók.

Tekintsük először azokat az elemeket, amelyek egy adott p_j-vel oszthatók (függetlenül attól, hogy az n többi prímtényezőjével oszthatók-e vagy sem). Ezek száma nyilván n/p_j.

Most nézzük azokat az egészeket, amelyek több, előre megadott p_j-vel oszthatók (ismét nem törődve azzal, oszthatók-e az n fennmaradó prímtényezőivel vagy sem). Egy egész akkor és csak akkor osztható adott prímek mindegyikével, ha osztható ezen prímek szorzatával. Ennélfogva például a p_1-gyel és p_2-vel is osztható elemek száma $n/(p_1p_2)$, a p_1-gyel, p_3-mal és p_7-tel oszthatóké $n/(p_1p_3p_7)$ stb.

Így a logikai szitaformula szerint

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \ldots - \frac{n}{p_r} + \frac{n}{p_1p_2} + \frac{n}{p_1p_3} + \ldots + \frac{n}{p_{r-1}p_r} - \frac{n}{p_1p_2p_3} - \ldots \quad (3)$$

Közvetlen számolással ellenőrizhető, hogy (3) jobb oldala azonos az

$$n\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

szorzattal, ez pedig a tételben megadott képletnek egy másik felírási módja. ■

Feladatok

2.3.1 Mutassuk meg, hogy minden $n > 2$-re $\varphi(n)$ páros szám.

2.3.2 Határozzuk meg azokat az n-eket, amelyekre $\varphi(n)$ értéke
a) 2; b) 4; c) 14; d) 60.

2.3.3 Melyik az a legkisebb n, amelyre $\varphi(n)$ osztható
a) 2^{10}-nel; b) 3^{10}-nel?

2.3.4 Határozzuk meg $\varphi(100n)/\varphi(n)$ összes lehetséges értékét, ha n végigfut a pozitív egészeken.

2.3.5 Bizonyítsuk be a következő állításokat.
a) $k \mid n \implies \varphi(k) \mid \varphi(n)$.
b) $\varphi\big((a,b)\big) \,\big|\, \big(\varphi(a),\varphi(b)\big)$ és $\big[\varphi(a),\varphi(b)\big] \,\big|\, \varphi\big([a,b]\big)$.
c) $\varphi\big((a,b)\big) = \big(\varphi(a),\varphi(b)\big) \iff \big[\varphi(a),\varphi(b)\big] = \varphi\big([a,b]\big)$.

2.3.6 Bizonyítsuk be, hogy $\varphi(a)/\varphi(b) = a/b$ akkor és csak akkor teljesül, ha a és b pontosan ugyanazokkal a prímekkel osztható.

2.3.7 Legyen $n > 2$. Melyek igazak az alábbi állítások közül?
a) Ha $\big(n,\varphi(n)\big) = 1$, akkor n páratlan négyzetmentes szám.
b) Ha n páratlan négyzetmentes szám, akkor $\big(n,\varphi(n)\big) = 1$.

*2.3.8 Bizonyítsuk be, hogy minden k pozitív egészhez létezik olyan n, amelyre $\big(n,\varphi(n)\big) = k$.

2.3.9 Igazoljuk, hogy minden n-re $\varphi(n) + d(n) \le n + 1$. Mely n-ekre áll egyenlőség?

2.3.10
a) Mutassuk meg, hogy ha $(a,b) \ne 1$, akkor $\varphi(ab) > \varphi(a)\varphi(b)$ (tehát ebben az esetben sohasem áll fenn egyenlőség).
b) A 2.3.1 Tétel első bizonyításának döntő része volt a II. állítás, azaz $(a,b) = 1 \implies \varphi(ab) = \varphi(a)\varphi(b)$ igazolása. Hol bukik meg az ott látott gondolatmenet, ha a és b nem relatív prímek?
c) Bizonyítsuk be, hogy bármely a, b esetén

$$\varphi(ab)\varphi\big((a,b)\big) = (a,b)\varphi(a)\varphi(b)\,.$$

2.3.11
a) Bizonyítsuk be, hogy ha n összetett szám, akkor $n - \varphi(n) \ge \sqrt{n}$. Milyen n-ek esetén áll egyenlőség?
b) Határozzuk meg azokat az n-eket, amelyekre $n - \varphi(n)$ értéke
(b1) 1; (b2) 6; (b3) 7; (b4) 10.

2.3.12 Mely *egész* számok szerepelnek az $n/\varphi(n)$ függvény értékkészletében?

2.3.13 Bizonyítsuk be, hogy ha $\varphi(n^2) = \varphi(k^2)$, akkor $n = k$.

2.3.14 Mutassuk meg, hogy $\sum_{d|n} \varphi(d) = n$.

2.3.15 Lássuk be, hogy $\varphi(n) \to \infty$, ha $n \to \infty$.

*2.3.16 Igazoljuk, hogy minden k természetes számhoz található olyan n, amelyre $\varphi(n) = \varphi(n+k)$.

*2.3.17 Adjunk meg 1000 különböző egész számot, amelyekhez a φ-függvény ugyanazt az értéket rendeli.

M*2.3.18 Határozzuk meg az összes olyan n pozitív egészt, amelyhez létezik olyan k, hogy $\varphi(n!) = k!$.

M*2.3.19 Milyen m esetén létezik olyan számtani sorozat, amely redukált maradékrendszert alkot modulo m?

2.4. Euler–Fermat-tétel

2.4.1 Tétel (Euler–Fermat-tétel) **T 2.4.1**

$$(a, m) = 1 \Longrightarrow a^{\varphi(m)} \equiv 1 \pmod{m}\,. \clubsuit$$

Bizonyítás: Legyen $r_1, r_2, \ldots, r_{\varphi(m)}$ redukált maradékrendszer modulo m.

Mivel $(a, m) = 1$, ezért az $ar_1, \ldots, ar_{\varphi(m)}$ elemek is redukált maradékrendszert alkotnak modulo m.

Ez azt jelenti, hogy minden $1 \le i \le \varphi(m)$-hez létezik egy és csak egy olyan $1 \le j \le \varphi(m)$, amelyre $ar_i \equiv r_j \pmod{m}$. Jelöljük ezt az r_j-t s_i-vel:

$$\begin{aligned} ar_1 &\equiv s_1 \pmod{m}\,,\\ ar_2 &\equiv s_2 \pmod{m}\,,\\ &\vdots\\ ar_{\varphi(m)} &\equiv s_{\varphi(m)} \pmod{m}\,. \end{aligned} \tag{1}$$

Itt az $s_1, \ldots, s_{\varphi(m)}$ számok az $r_1, \ldots, r_{\varphi(m)}$ számok egy permutációját alkotják.

Az (1)-beli kongruenciákat összeszorozva azt kapjuk, hogy

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv s_1 s_2 \ldots s_{\varphi(m)} \pmod{m}\,,$$

azaz

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv r_1 r_2 \ldots r_{\varphi(m)} \pmod{m}\,. \tag{2}$$

A (2) kongruenciát $(r_i, m) = 1$ miatt az összes r_i-vel egyszerűsíthetjük, és ekkor a kívánt $a^{\varphi(m)} \equiv 1 \pmod{m}$ adódik. ■

Tekintsük most azt a fontos speciális esetet, amikor a modulus egy p prímszám. Ekkor $\varphi(p) = p - 1$ alapján a következő tételt kapjuk:

2.4.1A Tétel (A „kis" Fermat-tétel egyik alakja) **T 2.4.1A**

Ha p prím és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$. ♣

Megjegyezzük, hogy egy p prím esetén az $(a, p) = 1$, a $p \nmid a$ és az $a \not\equiv 0 \pmod{p}$ feltételek ekvivalensek.

A 2.4.1A Tételből könnyen nyerhető egy olyan kongruencia is, amely már minden a esetén fennáll:

2.4.1B Tétel (A „kis" Fermat-tétel másik alakja) **T 2.4.1B**

Ha p prím, akkor bármely a egész számra $a^p \equiv a \pmod{p}$. ♣

Bizonyítás: Ha $p \nmid a$, akkor a 2.4.1A Tétel alapján $a^{p-1} \equiv 1 \pmod{p}$. Ezt a kongruenciát a-val beszorozva a kívánt $a^p \equiv a \pmod{p}$ adódik.

Ha $p \mid a$, akkor $a \equiv 0 \pmod{p}$. Ezt p-edik hatványra emelve (vagy a^{p-1}-gyel beszorozva) kapjuk, hogy $a^p \equiv 0 \pmod{p}$, és így $a^p \equiv a \pmod{p}$ is teljesül. ■

Megjegyzések: 1. Az Euler–Fermat-tétel (2.4.1 Tétel) megfordítása is igaz, vagyis $(a, m) = 1$ az $a^{\varphi(m)} \equiv 1 \pmod{m}$ kongruencia fennállásának nemcsak elégséges, hanem egyben *szükséges* feltétele is. Sőt, ennél erősebb állítás is igaz: csak akkor létezik egyáltalán olyan $k > 0$ kitevő, amelyre $a^k \equiv 1 \pmod{m}$, ha a és m relatív prímek. Az $a^k \equiv 1 \pmod{m}$ kongruenciából ugyanis a 2.2.5 Tétel szerint $(a^k, m) = (1, m) = 1$ következik, és így $(a, m) = 1$-nek is teljesülnie kell.

2. A kis Fermat-tétel második alakjának (2.4.1B Tétel) nincsen tetszőleges m modulusra vonatkozó „természetes" megfelelője, azaz nincs az általános Euler–Fermat-tételnek olyan „egyszerű" változata, amely minden a esetén érvényes lenne (lásd ezzel kapcsolatban a 2.4.15 feladatot).

3. Mint a név is mutatja, a 2.4.1A és B Tételek Fermat-tól származnak. A kis Fermat-tétel mindkét változata a 2.4.1 Tétel felhasználása nélkül, közvetlenül is bizonyítható: a B variánst (a szerinti) teljes indukcióval igazolhatjuk, és innen az A variáns is könnyen következik (lásd a 2.4.16 feladatot). A 2.4.1 Tételt Euler fedezte fel, éppen a kis Fermat-tétel általánosításaként.

4. A kis Fermat-tételnél a „kis” jelző arra szolgál, hogy megkülönböztesse ezt az eredményt a számelmélet egyik leghíresebb és csak a közelmúltban megoldott problémájától, a „nagy” Fermat-tételtől (vagy más néven Fermat-sejtéstől), amelyről a 7. fejezetben lesz szó.

Feladatok

2.4.1 Bizonyítsuk be, hogy bármely páratlan n-re $n \mid 2^{n!} - 1$.

2.4.2 Határozzuk meg 1793^{8642} utolsó két jegyét (tízes számrendszerben).

2.4.3 Igazoljuk, hogy $n^{20} + 4n^{44} + 8n^{80}$ minden n-re osztható 13-mal.

2.4.4 Mutassuk meg, hogy bármely n esetén $n^6 + 13$ és $n^2 + 21$ közül legalább az egyik összetett szám.

2.4.5 Lássuk be, hogy bármely a egész számra $1\,703\,601\,900 \mid a^{62} - a^2$.

2.4.6 Bizonyítsuk be a következő állításokat:

a) $11 \mid a^{30} + b^{30} + c^{30} \implies 11^{30} \mid a^{30} + b^{30} + c^{30}$.
b) $9 \mid a^{30} + b^{30} + c^{30} \implies 9^{15} \mid a^{30} + b^{30} + c^{30}$.

2.4.7 Mutassuk meg, hogy $a^{88} - b^{88}$ akkor és csak akkor *nem* osztható 23-mal, ha a és b közül pontosan az egyik osztható 23-mal.

2.4.8 Legyen p prím és $r_1, \ldots, r_p$ teljes maradékrendszer modulo p. Bizonyítsuk be, hogy ekkor $r_1^{2p-3}, \ldots, r_p^{2p-3}$ is teljes maradékrendszer modulo p.

2.4.9

a) Legyen p prím, a egész, i, j pozitív egészek és $i \equiv j \pmod{p-1}$. Lássuk be, hogy ekkor $a^i \equiv a^j \pmod{p}$.
b) Hogyan általánosítható az a)-beli állítás (prím helyett) tetszőleges m-re?

2.4.10 Melyek igazak az alábbi állítások közül? (A feladat tízes számrendszerre vonatkozik, és hatványon pozitív egész kitevős hatványt értünk.)

a) 133-nak végtelen sok hatványa végződik 133-ra.
b) 134-nek végtelen sok hatványa végződik 134-re.
c) 136-nak végtelen sok hatványa végződik 136-ra.

2.4.11 Mutassuk meg, hogy az $a, a+d, \ldots, a+kd, \ldots$ (különböző pozitív egészekből álló) végtelen számtani sorozat elemei között akkor és csak akkor szerepel az a-nak végtelen sok (pozitív egész kitevős) hatványa, ha $d/(a,d)$ és a relatív prímek.

2.4.12 Oldjuk meg újra az 1.3.12a feladatot az Euler–Fermat-tétel felhasználásával.

2.4.13 Igazoljuk, hogy egy n^2+1 alakú számnak minden pozitív páratlan osztója $4k+1$ alakú.

2.4.14 Tegyük fel, hogy $a^{40}+b^{40}$ osztható 19-cel. Lássuk be, hogy ekkor a és b is osztható 19-cel.

2.4.15 Bizonyítsuk be a következő állításokat, és vizsgáljuk meg, hogyan kapcsolódnak ezek a kis Fermat-tételhez.
a) Az $a^{\varphi(m)+1} \equiv a \pmod{m}$ kongruencia akkor és csak akkor teljesül minden a-ra, ha m négyzetmentes.
b) Az $a^m \equiv a^{m-\varphi(m)} \pmod{m}$ kongruencia minden m-re és minden a-ra teljesül.
c) Az $a^{1729} \equiv a \pmod{1729}$ kongruencia minden a-ra teljesül.

2.4.16 Adjunk közvetlen bizonyítást a kis Fermat-tétel mindkét alakjára: először igazoljuk indukcióval a 2.4.1B Tételt, majd ebből vezessük le a 2.4.1A Tételt.

2.5. Lineáris kongruenciák

Ebben a pontban az ismeretlenes kongruenciák (vagy kongruenciaegyenletek) legegyszerűbb fajtájával, a lineáris kongruenciákkal foglalkozunk.

2.5.1 Definíció **D 2.5.1**

Legyenek a, b egészek és m pozitív egész. Ekkor az $ax \equiv b \pmod{m}$ kongruenciát *lineáris kongruenciának* nevezzük, és ennek egy *megoldás*án olyan s egész számot értünk, amelyet az x helyére beírva a kongruencia fennáll. ♣

Világos, hogy ha egy s szám megoldás, akkor az $(s)_m$ maradékosztály bármely másik eleme is megoldás. Így az összes megoldás megkereséséhez elegendő egy teljes maradékrendszer elemeit végigpróbálni, melyek adnak közülük megoldást; az összes megoldás ekkor az ezekkel kongruens egészek halmaza lesz.

Ennek alapján a lineáris kongruencia megoldásszámán a *páronként inkongruens* megoldások számát értjük, vagyis azt, hogy hány *maradékosztály*ba tartoznak a megoldások, vagy (ismét kicsit más megfogalmazásban) azt, hogy egy teljes maradékrendszernek hány eleme elégíti ki a kongruenciát. Ugyanez

a helyzet a magasabb fokú kongruenciák esetén is, ezért ezt a definíciót rögtön általánosan is megadjuk.

2.5.2 Definíció **D 2.5.2**

Legyen f egy egész együtthatós polinom. Ekkor az $f(x) \equiv 0 \pmod{m}$ kongruencia *megoldásszám*án egy modulo m teljes maradékrendszer azon s elemeinek a számát értjük, amelyekre $f(s) \equiv 0 \pmod{m}$. ♣

Mivel $u \equiv v \pmod{m} \Longrightarrow f(u) \equiv f(v) \pmod{m}$, ezért a definícióban megadott szám valóban nem függ attól, hogy a modulo m teljes maradékrendszerek közül melyiket választottuk.

Térjünk vissza a lineáris kongruenciákra. Bármely más típusú egyenlethez hasonlóan itt is a következő kérdésekre keressük a választ:

(i) Mi a megoldhatóság szükséges és elégséges feltétele?

(ii) Mennyi a megoldásszám?

(iii) Hogyan lehet az összes megoldást valamilyen értelemben leírni, áttekinteni?

(iv) Milyen megoldási módszerekkel kaphatjuk meg a megoldásokat?

Először a megoldhatóság kérdésével foglalkozunk.

2.5.3 Tétel **T 2.5.3**

Az $ax \equiv b \pmod{m}$ kongruenciának akkor és csak akkor létezik megoldása, ha $(a, m) \mid b$. ♣

Bizonyítás: Az $ax \equiv b \pmod{m}$ kongruencia megoldhatósága azt jelenti, hogy van olyan s egész, amelyre $as \equiv b \pmod{m}$.

Ez tovább ekvivalens azzal, hogy van olyan t egész, amelyre $as + mt = b$ teljesül, vagyis s és t kielégíti az $ax + my = b$ lineáris diofantikus egyenletet.

Ezzel beláttuk, hogy az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha megoldható az $ax + my = b$ lineáris diofantikus egyenlet.

Az utóbbi megoldhatóságának szükséges és elégséges feltétele az 1.3.6 Tétel szerint az, hogy $(a, m) \mid b$ teljesüljön, tehát ugyanez a feltétele az $ax \equiv b \pmod{m}$ kongruencia megoldhatóságának is. ■

A bizonyításból kiderült, hogy az $ax \equiv b \pmod{m}$ lineáris kongruencia és az $ax + my = b$ lineáris diofantikus egyenlet kölcsönösen visszavezethetők

egymásra. (Sőt az $ax + my = b$ diofantikus egyenlet ugyanígy az $my \equiv b \pmod{|a|}$ lineáris kongruenciává is „átalakítható", ha $a \neq 0$.)

Ennek alapján bármely, a lineáris kongruenciákkal kapcsolatos eredmény felhasználható a lineáris diofantikus egyenletek vizsgálatánál és viszont.

Ne feledkezzünk meg azonban a jelentős eltérésekről sem: a lineáris kongruenciák megoldásai egész számok (illetve tulajdonképpen maradékosztályok), a lineáris diofantikus egyenleteké pedig egész szám*pár*ok, egy lineáris kongruencia megoldásszáma véges, egy lineáris diofantikus egyenleté végtelen stb.

A következő tételben meghatározzuk a lineáris kongruenciáknál a megoldásszámot, és egyúttal leírjuk, hogyan kapható meg egy megoldásból az összes többi.

2.5.4 Tétel **T 2.5.4**

I. Ha az $ax \equiv b \pmod{m}$ kongruencia megoldható, akkor a megoldásszáma (a, m).

II. Legyen $(a, m) = d$, $m = dm_1$, és tegyük fel, hogy az s egész szám (az egyik) megoldása az $ax \equiv b \pmod{m}$ kongruenciának. Ekkor az

$$s, \quad s + m_1, \quad s + 2m_1, \quad \ldots, \quad s + (d-1)m_1 \tag{1}$$

számok páronként inkongruensek modulo m, kielégítik a kongruenciát, és az összes megoldás ezek valamelyikével kongruens modulo m. ♣

Bizonyítás: Az I. és II. állításokat egyszerre igazoljuk.
A feltétel szerint az s egész szám megoldás, vagyis

$$as \equiv b \pmod{m}\,. \tag{2}$$

Egy t egész szám akkor és csak akkor megoldás, ha

$$at \equiv b \pmod{m}\,. \tag{3}$$

A (2) feltétel alapján (3) ekvivalens azzal, hogy

$$at \equiv as \pmod{m}\,. \tag{4}$$

A 2.1.3 Tétel alapján (4) tovább ekvivalens

$$t \equiv s \left(\mathrm{mod}\ \frac{m}{(m,a)}\right), \qquad \text{azaz} \qquad t \equiv s \pmod{m_1}$$

teljesülésével. Ezt úgy is írhatjuk, hogy

$$t = s + km_1\,, \tag{5}$$

ahol k egész szám.

Ez azt jelenti, hogy az $ax \equiv b \pmod m$ kongruencia összes megoldását az (5)-ben megadott t értékek szolgáltatják.

Így már csak azt kell igazolnunk, hogy az (5)-beli t értékek d darab különböző maradékosztályba tartoznak modulo m, és (1)-ben éppen ezeknek a maradékosztályoknak egy-egy reprezentánsa szerepel.

Vizsgáljuk meg, mikor esik két ilyen t ugyanabba a maradékosztályba modulo m. Legyen

$$t' = s + k'm_1 \qquad \text{és} \qquad t'' = s + k''m_1\,.$$

Ekkor

$$t' \equiv t'' \pmod m \iff k'm_1 \equiv k''m_1 \pmod m \iff k' \equiv k'' \pmod d\,. \tag{6}$$

Itt az első lépésben a $t' \equiv t'' \pmod m$ kongruenciából kivontunk s-et, majd ismét a 2.1.3 Tétel szabályai szerint egyszerűsítettünk m_1-gyel, ekkor a modulus közben $m/(m_1, m) = m/m_1 = d$-re változott.

(6) azt jelenti, hogy két t pontosan akkor esik ugyanabba a modulo m maradékosztályba, ha a megfelelő két k kongruens modulo d.

Így, ha k végigfut a $0, 1, \ldots, d-1$ számokon, akkor az ezekhez tartozó

$$t = s + km_1, \quad \text{azaz éppen az (1)-beli} \quad s,\ s + m_1,\ \ldots,\ s + (d-1)m_1$$

értékek a keresett modulo m maradékosztályok egy-egy reprezentánsát alkotják. ■

Külön kiemeljük azt a speciális esetet, amikor az $ax \equiv b \pmod m$ lineáris kongruenciában $(a, m) = 1$. Ekkor $(a, m) \mid b$ automatikusan teljesül, tehát a 2.5.3 Tétel szerint a kongruencia biztosan megoldható, és a 2.5.4 Tétel alapján a megoldásszám $(a, m) = 1$. Ezt az eredményt fontossága miatt külön tételként is megfogalmazzuk:

2.5.5 Tétel **T 2.5.5**

Ha $(a, m) = 1$, akkor az $ax \equiv b \pmod m$ kongruencia bármely b esetén megoldható és a megoldásszáma 1. ♣

A megoldási módszerek bemutatása előtt néhány fontos előzetes megjegyzést teszünk.

(A) Általában célszerű előre ellenőrizni a 2.5.3 Tétel kritériuma alapján, hogy a kongruencia egyáltalán megoldható-e.

(B) Ha $(a, m) = 1$, akkor a lineáris kongruenciát csak egyetlen maradékosztály elemei elégítik ki, tehát ha találtunk egy megoldást, akkor készen is vagyunk. Általában is elég egyetlen megoldás megkeresése, mert akkor az összes megoldás megadása már könnyen megy a 2.5.4/II Tétel alapján.

(C) A legtöbb esetben érdemes a megoldandó kongruenciát visszavezetni egy olyan lineáris kongruenciára, amelyben az x együtthatója és a modulus már relatív prímek. Ezt a következőképpen tehetjük meg.

Ha az $ax \equiv b \pmod{m}$ kongruencia megoldható, akkor $(a, m) \mid b$. Így a $d = (a, m)$ jelöléssel

$$a = da_1, \quad m = dm_1, \quad b = db_1 \quad \text{és} \quad (a_1, m_1) = 1\,.$$

Ekkor a kongruenciát „végigoszthatjuk" d-vel (a modulust is beleértve): az $ax \equiv b \pmod{m}$ kongruencia a 2.1.3 Tétel alapján „ekvivalens" az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciával, amelynél már $(a_1, m_1) = 1$. (Ez az átalakítás tulajdonképpen annak felel meg, hogy az $ax \equiv b \pmod{m}$ kongruenciához tartozó $ax + my = b$ diofantikus egyenletet elosztjuk d-vel, és ekkor az $a_1x \equiv b_1 \pmod{m_1}$ kongruenciához tartozó $a_1x + m_1y = b_1$ diofantikus egyenletet kapjuk.)

Az előző bekezdésben az „ekvivalens" szónál az idézőjel arra utal, hogy noha a két kongruenciát ugyanazok az egész számok elégítik ki, azonban ezeket az elsőnél modulo m, a másodiknál pedig modulo m_1 maradékosztályokba kell besorolni. Így például a két kongruencia megoldásszáma sem lesz azonos (ha $d > 1$).

Most rátérünk a lineáris kongruenciák néhány megoldási módszerének az ismertetésére, amelyeket egy-egy példával illusztrálunk.

M1 *Végigpróbálgatás.* Egy modulo m teljes maradékrendszer minden elemére megvizsgáljuk, hogy kielégíti-e a kongruenciát. (Ezt csak nagyon kis modulus esetén érdemes alkalmazni.)

P1 $23x \equiv 11 \pmod{5}$. Az egyszerűbb számolás érdekében a behelyettesítés előtt érdemes az együtthatók helyére velük kongruens, de kisebb (abszolút értékű) számokat írni: $3x \equiv 1 \pmod{5}$ vagy $-2x \equiv 1 \pmod{5}$. Kipróbálva a $0, 1, 2, 3, 4$ (vagy $0, \pm1, \pm2$) értékeket azt kapjuk, hogy az egyetlen megoldást az $x \equiv 2 \pmod{5}$ maradékosztály adja. [Mivel

$(23, 5) = 1$ alapján eleve tudjuk, hogy csak egyetlen megoldás van, így annak megtalálása után a további értékeket természetesen nem kell már kipróbálni.]

M2 *Diofantikus egyenlet.* A lineáris kongruenciát a 2.5.3 Tétel bizonyításában látott módon visszavezetjük egy diofantikus egyenletre, a diofantikus egyenletet megoldjuk, és a kapott megoldásokat „visszaalakítva" megkapjuk a kongruencia megoldásait.

P2 $18x \equiv 38 \pmod{28}$. A megfelelő diofantikus egyenlet $18x + 28y = 38$. Ezt 2-vel leosztva $9x + 14y = 19$ adódik.

Az 1.3.6 Tétel bizonyítását követve állítsuk elő a 9 és a 14 legnagyobb közös osztóját $9u + 14v$ alakban. Az euklideszi algoritmusból vagy némi próbálgatás után kapjuk, hogy $9 \cdot (-3) + 14 \cdot 2 = 1$. Ezt 19-cel beszorozva $9 \cdot (-57) + 14 \cdot 38 = 19$ adódik, vagyis a $9x + 14y = 19$ diofantikus egyenlet egyik megoldása $x = -57$, $y = 38$.

Visszatérve a $18x \equiv 38 \pmod{28}$ kongruenciára, ez azt jelenti, hogy $x = -57$ az egyik megoldás. Az összes megoldást ezután a 2.5.4/II Tétel szerint az $x \equiv -57 \pmod{28}$ és $x \equiv -43 \pmod{28}$ maradékosztályok adják. (Itt a -57 és -43 reprezentánsok helyett írhatunk természetesen például -1-et, illetve 13-at.)

Megjegyezzük, hogy a lineáris diofantikus egyenletek megoldásánál inkább a 7.1 pontban szereplő eljárást érdemes alkalmazni, amely nemcsak egy megoldást szolgáltat, hanem (paraméteres alakban) egyszerre megadja az egyenlet összes megoldását. (Tulajdonképpen az a módszer is az euklideszi algoritmus egy változata.)

M3 *Euler–Fermat-tétel.* Az $ax \equiv b \pmod{m}$ kongruenciát a (C) megjegyzésben látott módon vezessük vissza az $a_1 x \equiv b_1 \pmod{m_1}$ kongruenciára, ahol $(a_1, m_1) = 1$.

Ekkor az Euler–Fermat-tétel szerint $a_1^{\varphi(m_1)} \equiv 1 \pmod{m_1}$. Ennek alapján $x = a_1^{\varphi(m_1)-1} b_1$ megoldása a kongruenciának:

$$a_1 \cdot a_1^{\varphi(m_1)-1} b_1 = a_1^{\varphi(m_1)} b_1 \equiv b_1 \pmod{m_1}.$$

Visszatérve az eredeti kongruenciára, ekkor $x = a_1^{\varphi(m_1)-1} b_1$ annak is megoldása. Az összes megoldást ezután ismét (például) a 2.5.4/II Tételből kaphatjuk meg.

P3 $36x \equiv 81 \pmod{21}$. Itt $(36, 21) = 3$, így a feladatot visszavezethetjük a $12x \equiv 27 \pmod{7}$ kongruenciára. Az együtthatókat redukálva $-2x \equiv -1 \pmod{7}$ adódik. Ennek megoldása $x = (-2)^{6-1}(-1) \equiv 4 \pmod{7}$. Tehát az eredeti kongruencia összes megoldása: $x \equiv 4,\ 11,\ 18 \pmod{21}$.

Természetesen a $12x \equiv 27 \pmod 7$ kongruenciában az együtthatók redukciójánál választhatjuk a legkisebb nemnegatív maradékokat is a legkisebb abszolút értékű maradékok helyett. Ekkor az $5x \equiv 6 \pmod 7$ kongruenciához jutunk és $x \equiv 5^5 \cdot 6 \pmod 7$ adódik.

Mivel $(12, 7) = 1$, ezért a $12x \equiv 27 \pmod 7$ kongruenciának egyetlen megoldása van modulo 7, tehát szükségképpen $5^5 \cdot 6 \equiv 4 \pmod 7$. Ennek a közvetlen igazolásához nem kell az 5^5 értékét ténylegesen kiszámolni, hanem a hatványozáskor mindig vehetjük a modulo 7 maradékokat:

$$5^2 = 25 \equiv 4 \pmod 7, \quad 5^4 \equiv 4^2 \equiv 2 \pmod 7, \quad 5^5 \equiv 5 \cdot 2 \equiv 3 \pmod 7,$$

és így valóban $6 \cdot 5^5 \equiv 6 \cdot 3 \equiv 4 \pmod 7$.

M4 *Ügyeskedések.* A kongruenciát ügyesen választott, a modulushoz relatív prím számokkal szorozva, illetve egyszerűsítve az eredetivel ekvivalens kongruenciákhoz jutunk, míg végül a megoldás(ok) nyilvánvalóan leolvasható(k).

P4 $80x \equiv 32 \pmod{108}$. Itt $(80, 108) = 4$, így a feladatot visszavezethetjük a $20x \equiv 8 \pmod{27}$ kongruenciára.

Mivel $(4, 27) = 1$, ezért a 4-gyel történő egyszerűsítés ekvivalens lépés: $5x \equiv 2 \pmod{27}$.

Most két módszert is mutatunk arra, hogy az $5x \equiv 2 \pmod{27}$ kongruenciában hogyan „szabadulhatunk meg” az 5 együtthatótól.

I. Osztás: Ahhoz, hogy az 5-tel egyszerűsíthessünk, írjuk a jobb oldalon a 2 helyére a vele kongruens -25-öt: $5x \equiv -25 \pmod{27}$. Mivel $(5, 27) = 1$, innen $x \equiv -5 \pmod{27}$ adódik.

II. Szorzás: Olyan szorzót keresünk, hogy a beszorzás után az x együtthatója 1-gyel (vagy -1-gyel) legyen kongruens modulo 27. (Ekkor ez a szorzó biztosan relatív prím a 27-hez, ezért a beszorzás most automatikusan ekvivalens lépést jelent.) Szorozzuk be a $5x \equiv 2 \pmod{27}$ kongruenciát például 11-gyel: ekkor $55x \equiv 22 \pmod{27}$ és $55 \equiv 1 \pmod{27}$ alapján $x \equiv 22 (\equiv -5) \pmod{27}$ adódik.

Az eredeti kongruencia megoldásai tehát: $x \equiv -5, 22, 49, 76 \pmod{108}$.

Az egyes módszereket összehasonlítva első ránézésre talán az M3 vagy az M4 tűnhet a legkényelmesebbnek. Kiderül azonban, hogy nagy modulusok esetén szinte kizárólag az M2 használható. Erről részletesebben az 5.7 pontban lesz szó.

Feladatok

2.5.1 Oldjuk meg a P1–P4 példákat az M2–M4 módszerek mindegyikével.

2.5.2 Oldjuk meg az alábbi kongruenciákat:
a) $24x \equiv 60 \pmod{51}$;
b) $100x \equiv 88 \pmod{116}$;
c) $555x \equiv 5555 \pmod{55\,555}$;
d) $(2^k+1)x \equiv 2^{k+1}+1 \pmod{2^{k+2}+1}$;
e) $10x^{39}+8x^{20}+9x^3+7x \equiv 0 \pmod{19}$;
f) $13x^{41} \equiv 27 \pmod{100}$.

2.5.3 Határozzuk meg azt a két legkisebb pozitív egészt, amelynek 13-szorosát hetes számrendszerben felírva az utolsó előtti jegy 4, az utolsó jegy pedig 3.

2.5.4 Számítsuk ki 3^{279} utolsó két jegyét (tízes számrendszerben).

2.5.5 Az alábbi feltételek mindegyikéről döntsük el, hogy elégséges-e az $ax \equiv b \pmod{m}$ kongruencia megoldhatóságához.
a) $(a,m) \mid (a,b)$.
b) $(a,b) \mid (a,m)$.
c) a,m,b számtani sorozat.
d) a,m,b mértani sorozat.
e) a,b,m számtani sorozat.
f) a,b,m mértani sorozat.

2.5.6 Melyek igazak az alábbi állítások közül?
a) Az $ax \equiv b \pmod{m}$ kongruencia megoldásszáma legfeljebb b, ha $b > 0$.
b) Ha az $ax \equiv b \pmod{m}$ kongruencia megoldható, akkor megoldható az $a^2x \equiv b^2 \pmod{m^2}$ kongruencia is.
c) Ha az $a_1x \equiv b_1 \pmod{m_1}$ és $a_2x \equiv b_2 \pmod{m_2}$ kongruenciák megoldhatók, akkor megoldható az $a_1a_2x \equiv b_1b_2 \pmod{m_1m_2}$ kongruencia is.

M 2.5.7 Legyen a és m rögzített, és jelöljük $f(b)$-vel az $ax \equiv b \pmod{m}$ kongruencia megoldásszámát. Számítsuk ki a $\sum_{b=1}^{m} f(b)$ összeget.

2.6. Szimultán kongruenciarendszerek

Szimultán kongruenciarendszernek azt nevezzük, amikor ugyanarra az ismeretlenre egyidejűleg több, különböző modulus szerinti kongruenciafeltételt is előírunk:

$$f_1(x) \equiv 0 \pmod{m_1}, \quad f_2(x) \equiv 0 \pmod{m_2}, \quad \ldots, \quad f_k(x) \equiv 0 \pmod{m_k},$$

ahol $f_1, \ldots, f_k$ egész együtthatós polinomok.

Egy ilyen rendszer megoldhatóságához nyilván szükséges, hogy minden egyes kongruencia külön-külön megoldható legyen. Az egyes kongruenciákat megoldva így elég az

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}$$

alakú (speciális lineáris) rendszereket vizsgálnunk.

Először a két kongruenciából álló rendszerekkel foglalkozunk.

2.6.1 Tétel **T 2.6.1**

I. Az

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \tag{1}$$

szimultán kongruenciarendszer akkor és csak akkor oldható meg, ha

$$(m_1, m_2) \mid c_1 - c_2 \,.$$

II. Megoldhatóság esetén az összes megoldás egy maradékosztályt alkot modulo $[m_1, m_2]$. Ez más megfogalmazásban azt jelenti, hogy ha az s egész szám a szimultán kongruenciarendszer egy megoldása, akkor az alábbi t értékek adják az összes megoldást:

$$t \equiv s \ \big(\mathrm{mod}\ [m_1, m_2]\big), \quad \text{azaz} \quad t = s + k[m_1, m_2], \ \text{ahol } k \text{ egész. } \clubsuit$$

A tétel bizonyítása egyúttal módszert is szolgáltat a megoldások megkeresésére; kiderül, hogy egy lineáris diofantikus egyenletet (vagy ami ezzel egyenértékű, egy lineáris kongruenciát) kell megoldani.

Bizonyítás: I. A kongruencia definíciója alapján (1) átírható az

$$x = c_1 + z_1 m_1, \quad x = c_2 + z_2 m_2 \tag{2}$$

alakba, ahol z_1 és z_2 egész számok.

A (2) feltétel ekvivalens

$$c_1 + z_1 m_1 = c_2 + z_2 m_2 \tag{3}$$

teljesülésével. (3)-at átrendezve

$$c_1 - c_2 = z_2 m_2 - z_1 m_1 \tag{4}$$

adódik.

Ez azt jelenti, hogy az (1) szimultán kongruenciarendszer a (4) lineáris diofantikus egyenletre vezethető vissza.

Az utóbbi megoldhatóságának szükséges és elégséges feltétele az 1.3.6 Tétel szerint az, hogy $(m_1, m_2) \mid c_1 - c_2$ teljesüljön, tehát ugyanez a feltétele (1) megoldhatóságának is.

Mint a bizonyítás előtt jeleztük, egyúttal módszert is nyertünk a megoldások megkeresésére: a (4) diofantikus egyenletet, vagy egy ennek megfelelő lineáris kongruenciát kell megoldani.

II. Legyen s egy megoldás, azaz

$$\begin{aligned} s &\equiv c_1 \pmod{m_1}, \\ s &\equiv c_2 \pmod{m_2}. \end{aligned} \tag{5}$$

Egy t egész szám definíció szerint pontosan akkor megoldás, ha

$$\begin{aligned} t &\equiv c_1 \pmod{m_1}, \\ t &\equiv c_2 \pmod{m_2}. \end{aligned} \tag{6}$$

(5) alapján a (6) feltétel azzal ekvivalens, hogy

$$\begin{aligned} t &\equiv s \pmod{m_1}, \\ t &\equiv s \pmod{m_2} \end{aligned} \tag{7}$$

teljesül. Írjuk át (7)-et oszthatóságra, és használjuk fel a legkisebb közös többszörös tulajdonságait (1.6.6/II. Tétel):

$$\left.\begin{aligned} m_1 \mid t - s \\ m_2 \mid t - s \end{aligned}\right\} \iff [m_1, m_2] \mid t - s \iff t \equiv s \pmod{[m_1, m_2]}. \quad \blacksquare$$

Külön kiemeljük azt a speciális esetet, amikor az (1) szimultán kongruenciarendszer m_1 és m_2 modulusai relatív prímek. Ekkor az $(m_1, m_2) \mid c_1 - c_2$ feltétel automatikusan teljesül, tehát a 2.6.1 Tétel alapján a kongruenciarendszer biztosan megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo $m_1 m_2$. Ezt az eredményt fontossága miatt külön tételként is megfogalmazzuk:

2.6.1A Tétel **T 2.6.1A**

Ha $(m_1, m_2) = 1$, akkor az

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}$$

szimultán kongruenciarendszer bármilyen c_1 és c_2 egész szám esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo $m_1 m_2$. ♣

A 2.6.1A Tételből következik, hogy ha m_1 és m_2 relatív prímek, akkor hiába tudjuk, hogy mennyi egy számnak az m_1-gyel való osztási maradéka, ez semmilyen támpontot sem jelent az m_2 szerinti osztási maradékkal kapcsolatban: a két modulusra vonatkozó maradék (egy jól meghatározott valószínűségszámítási értelemben) teljesen független egymástól. Így például egy szám utolsó számjegye vagy számjegyei a 10-zel vagy a 10 valamely hatványával való osztási maradékot jelentik, és ennélfogva semmilyen információt sem adhatnak arra vonatkozóan, hogy mi az adott szám maradéka 3-mal, 7-tel vagy 13-mal osztva, hiszen ezek a modulusok relatív prímek a 10-hez.

A több kongruenciából álló szimultán kongruenciarendszerek közül csak azzal az esettel foglalkozunk, amikor a modulusok *páronként* relatív prímek (az általános esetre vonatkozóan lásd a 2.6.13 feladatot). Az idevágó tételt lényegében már Szun Cu kínai matematikus is ismerte közel 2000 évvel ezelőtt(!), ezért ezt kínai maradéktételnek is szokás nevezni.

2.6.2 Tétel (Kínai maradéktétel) **T 2.6.2**

Legyenek az $m_1, \ldots, m_k$ modulusok páronként relatív prímek. Ekkor az

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{8}$$

szimultán kongruenciarendszer bármilyen $c_1, \ldots, c_k$ egészek esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo $m_1 m_2 \ldots m_k$. ♣

Első bizonyítás: A tétel könnyen adódik a 2.6.1A Tételből k szerinti teljes indukcióval.

A $k = 2$ eset éppen maga a 2.6.1A Tétel.

Tegyük fel, hogy $k-1$ kongruenciából álló rendszerekre az állítás igaz, és tekintsük a k kongruenciából álló (8) rendszert. Itt az első $k-1$ kongruenciát kielégítő egész számok az indukciós feltevés szerint egyetlen maradékosztályt alkotnak modulo $m_1 m_2 \dots m_{k-1}$, vagyis az első $k-1$ kongruencia helyett egyetlen $x \equiv c \pmod{m_1 m_2 \dots m_{k-1}}$ kongruencia írható, ahol c alkalmas egész szám. Így (8) ekvivalens az

$$\begin{aligned} x &\equiv c \pmod{m_1 m_2 \dots m_{k-1}} \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{9}$$

szimultán kongruenciarendszerrel. (9)-re ismét a 2.6.1A Tételt alkalmazva éppen a k-ra vonatkozó állítást kapjuk. ■

Második bizonyítás: Csak a megoldhatóságra adunk új bizonyítást, mégpedig a(z egyik) megoldást (valamilyen értelemben) elő is állítjuk.

Az eljárás némileg emlékeztet a Lagrange-féle interpolációs polinomok konstrukciójára.

Először azt a speciális esetet tekintjük, amikor (8)-ban az egyik c_i értéke 1, a többi c_j pedig 0, majd az itt kapott eredményt felhasználjuk az általános eset megoldásához.

Nézzük most mindezt részletesen. Legyen

$$M = m_1 \dots m_k \qquad \text{és} \qquad M_i = \frac{M}{m_i}, \quad i = 1, 2, \dots, k.$$

Mivel az $m_1, \dots, m_k$ modulusok páronként relatív prímek, ezért

$$(M_i, m_i) = 1, \quad i = 1, 2, \dots, k. \tag{10}$$

I. Rögzítsünk egy $1 \le i \le n$ indexet, és oldjuk meg a feladatot először abban a speciális esetben, amikor (8)-ban $c_i = 1$, és $j \neq i$-re $c_j = 0$.

Az $x \equiv 0 \pmod{m_j}$ kongruenciák azt jelentik, hogy x minden $j \neq i$-re osztható m_j-vel. Az m_j modulusok páronként relatív prímek, ezért ez ekvivalens azzal, hogy x osztható az m_j számok szorzatával, vagyis M_i-vel: $x = M_i z$.

Írjuk be ezt x helyére a fennmaradó $x \equiv 1 \pmod{m_i}$ kongruenciában:

$$M_i z \equiv 1 \pmod{m_i}. \tag{11}$$

Ez z-re nézve lineáris kongruencia, amely (10) alapján megoldható.

Legyen a b_i egész szám megoldása (11)-nek. Ekkor az előzőek alapján $x = b_i M_i$ megoldása (8)-nak.

II. Tekintsük most az általános esetet, amikor (8)-ban valamennyi c_i tetszőleges. Megmutatjuk, hogy ekkor

$$x = c_1 b_1 M_1 + \ldots + c_k b_k M_k \quad (\text{ahol } M_i b_i \equiv 1 \pmod{m_i},\ i = 1, \ldots, k) \quad (12)$$

megoldása a (8) szimultán kongruenciarendszernek.

Ellenőrizzük például az $x \equiv c_3 \pmod{m_3}$ kongruencia teljesülését. A (12) összegben M_3 kivételével valamennyi M_j osztható m_3-mal, továbbá $b_3 M_3 \equiv 1 \pmod{m_3}$, ezért valóban

$$c_1 b_1 M_1 + \ldots + c_k b_k M_k \equiv c_3 b_3 M_3 \equiv c_3 \pmod{m_3}\,. \blacksquare$$

A 2.6.2 Tétel fontos következménye, hogy tetszőleges összetett modulusú kongruencia visszavezethető prímhatvány modulusú kongruenciákra. Legyen ugyanis m kanonikus alakja $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Ekkor az

$$f(x) \equiv 0 \pmod{m} \quad (13)$$

kongruencia ekvivalens az

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{\alpha_r}} \end{aligned} \quad (14)$$

szimultán kongruenciarendszerrel.

A (14) rendszerben minden kongruenciát külön-külön megoldunk. Ha valamelyik nem oldható meg, akkor nyilván (13)-nak sincs megoldása. Ha mindegyik megoldható, akkor legyen $h_1, \ldots, h_r$ egy-egy megoldásuk. Ekkor az

$$\begin{aligned} x &\equiv h_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv h_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ x &\equiv h_r \pmod{p_r^{\alpha_r}} \end{aligned}$$

szimultán kongruenciarendszert megoldva az eredeti (13) kongruencia egy megoldásához jutunk. Az összes megoldást úgy kapjuk, ha $h_1, \dots, h_r$ végigfut a (14)-beli kongruenciák összes lehetséges megoldásrendszerén.

P1 példa: Oldjuk meg a

$$10x^{84} + 3x + 7 \equiv 0 \pmod{245} \tag{15}$$

kongruenciát.

Az előzőek alapján (15) ekvivalens a

$$10x^{84} + 3x + 7 \equiv 0 \pmod{5} \tag{16}$$
$$10x^{84} + 3x + 7 \equiv 0 \pmod{49} \tag{17}$$

szimultán kongruenciarendszerrel.

A (16) kongruencia $10 \equiv 0 \pmod 5$ miatt ugyanaz, mint a $3x + 7 \equiv 0 \pmod 5$ lineáris kongruencia. Ennek egyetlen megoldása

$$x \equiv 1 \pmod 5 . \tag{16a}$$

A (17) kongruenciánál a megoldások keresésénél két esetet érdemes megkülönböztetni:

$$\text{(i)} \quad (x, 49) = 1; \qquad \text{(ii)} \quad (x, 49) \neq 1 .$$

Az (i) esetben az Euler–Fermat-tétel szerint

$$x^{84} = x^{2\varphi(49)} \equiv 1 \pmod{49} .$$

Így ebben az esetben (17) ekvivalens a $3x + 17 \equiv 0 \pmod{49}$ lineáris kongruenciával. Ennek egyetlen megoldása

$$x \equiv -22 \pmod{49} . \tag{17a}$$

A (ii) eset azt jelenti, hogy $7 \mid x$. Ekkor $x^{84} \equiv 0 \pmod{49}$. Így ebben az esetben (17) ekvivalens a $3x + 7 \equiv 0 \pmod{49}$ lineáris kongruenciával. Ennek egyetlen megoldása (a $7 \mid x$ feltételt is kielégítő)

$$x \equiv 14 \pmod{49} . \tag{17b}$$

A (15) kongruencia megoldásait ezek szerint az

$$x \equiv \quad 1 \pmod 5 \tag{16a}$$
$$x \equiv -22 \pmod{49}, \tag{17a}$$

illetve az

$$x \equiv \quad 1 \pmod{5} \tag{16a}$$
$$x \equiv 14 \pmod{49} \tag{17b}$$

szimultán kongruenciarendszerek megoldásaiból kapjuk meg.

A megoldásokat meghatározhatjuk a 2.6.1 Tétel bizonyításánál jelzett eljárással, de gyakran kényelmesebb az alábbi módszer.

Az első kongruenciarendszerben a nagyobbik modulus szerinti (17a) kongruenciából

$$x = 49z - 22. \tag{18}$$

Írjuk be (18)-at a (16a) kongruenciába, ekkor

$$49z - 22 \equiv 1 \pmod{5}$$

adódik. Ebből

$$z \equiv 2 \pmod{5}, \qquad \text{azaz} \qquad z = 5w + 2\,. \tag{19}$$

Visszahelyettesítve (19)-et (18)-ba azt kapjuk, hogy $x = 245w + 76$. Ez azt jelenti, hogy az első kongruenciarendszer megoldása $x \equiv 76 \pmod{245}$.

Hasonlóan nyerjük, hogy a második kongruenciarendszer megoldása $x \equiv 161 \pmod{245}$.

Tehát a (15) kongruencia összes megoldása

$$x \equiv 76 \pmod{245} \quad \text{és} \quad x \equiv 161 \pmod{245}\,.$$

Végül a kínai maradéktétel egy számítástechnikai alkalmazását mutatjuk be. Sok olyan művelet van, amelyet a számítógép egész számok összeadásának, kivonásának és szorzásának sorozatából épít fel, azt ilyen alaplépésekre vezeti vissza. Ezért igen lényeges, milyen gyorsan lehet ezeket az alapműveleteket elvégezni.

Tekintsük például az összeadást. A szokásos számrendszeres felírás esetén a számjegyek összeadását nem lehet egymástól függetlenül elvégezni, mert az átvitelek jelentősen befolyásolhatják az eredményt. Az ún. *maradékszámrendszer*ekben viszont az egyes „számjegyekkel" teljesen függetlenül végezhetjük a műveleteket. Ezt elsősorban olyankor szokták alkalmazni, ha sok párhuzamos processzor áll rendelkezésre.

A módszer lényege a következő. Tegyük fel, hogy a számolás során csak N-nél kisebb abszolút értékű egészek fordulhatnak elő. (Ez nem jelent semmiféle megszorítást, hiszen bármely számítógép csak egy adott korlátig képes a számokat ábrázolni és velük műveleteket végezni.) Legyen $m = p_1 \dots p_r$ az első r darab (pozitív) prímszám szorzata, ahol r-et úgy választjuk meg, hogy $m > 2N$ teljesüljön.

Ekkor egy N-nél kisebb abszolút értékű egész szám megegyezik a modulo m legkisebb abszolút értékű maradékával. Ehelyett pedig tekinthetjük a szám modulo p_i maradékainak a rendszerét, ezek lesznek a szám „számjegyei" maradékszámrendszerben.

A „számjegyek" tulajdonképpen egy szimultán kongruenciarendszert jelentenek, ahol a p_i modulusok páronként relatív prímek, és így ezekből a modulo m maradék, vagyis maga a szám egyértelműen rekonstruálható.

Két szám összeadásakor vagy szorzásakor a megfelelő maradékokat (azaz a „számjegyeket") kell összeadni, illetve összeszorozni („átvitel" nincs, a különböző modulusokhoz tartozó műveletek egymástól függetlenül végezhetők), majd az így kapott modulo p_i maradékok rendszeréből kell a modulo m maradékot, vagyis magát a számot meghatározni.

P2 példa: Illusztrációként legyen $N = 1000$, és végezzük el a $27 \cdot 34$ szorzást maradékszámrendszerben.

Ekkor

$$m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$$

megfelel. A 27 maradékai a 2, 3, 5, 7 és 11 prímekkel osztva rendre 1, 0, 2, 6 és 5, tehát a 27 maradékszámrendszeres felírása

$$27 = (1, 0, 2, 6, 5)\,.$$

Hasonlóan

$$34 = (0, 1, 4, 6, 1)\,.$$

A $27 \cdot 34$ szorzás elvégzéséhez összeszorozzuk az egyes „számjegyeket" („átvitel" nincs), a szorzatokat redukáljuk modulo p_i, majd megoldjuk az így adódó szimultán kongruenciarendszert:

$$27 \cdot 34 = (1 \cdot 0,\ \ 0 \cdot 1,\ \ 2 \cdot 4,\ \ 6 \cdot 6,\ \ 5 \cdot 1) = (0, 0, 3, 1, 5)\,,$$

és az

$$x \equiv 0 \pmod 2$$
$$x \equiv 0 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 1 \pmod 7$$
$$x \equiv 5 \pmod{11}$$

szimultán kongruenciarendszer megoldása

$$x \equiv 918 \pmod{2310}.$$

Tehát $27 \cdot 34 = 918$.

Ha több műveletet végzünk, akkor természetesen folyamatosan lehet a maradékszámrendszeres alakkal dolgozni, és csak a végeredményt érdemes „visszaváltani" a számok szokásos alakjába.

Megemlítjük még, hogy a szimultán kongruenciarendszereket hasonló módon lehet alkalmazni (racionális együtthatós) lineáris egyenletrendszerek megoldásánál is. A módszer lényege, hogy az egyenletrendszert különböző prím modulusok szerint tekintjük, majd az így kapott megoldásokból előállítjuk az egyenletrendszer megoldását a modulusok szorzatára nézve, ami megfelelő feltételek esetén magát a keresett megoldást is megadja, ha elég sok modulust választunk. Az eljárás előnye, hogy szemben pl. a hagyományos Gauss-kiküszöböléssel, itt nem keletkeznek túl nagy (vagy túl kicsi) számok, és ezért nem fenyeget a túlcsordulás veszélye.

Feladatok

(Ha más kikötést nem teszünk, akkor a feladatok tízes számrendszerre vonatkoznak.)

2.6.1

a) Egy százlábú meg akarja számolni a lábait. Tudja, hogy legfeljebb 250 lába van. Ha 11-esével számolja őket, akkor 5 marad ki, ha 15-ösével, akkor 3. Hánylábú a százlábú?

b) Egy másik százlábú is megirigyli ezt a módszert. Neki 12-esével számolva 4 marad, 15-ösével számolva pedig 8. Bizonyítsuk be, hogy elszámolta magát.

2.6.2 Egy szám utolsó jegye 20-as alapú számrendszerben „tizenegyes". Mi lehet az utolsó jegye (a) 9-es; (b) 8-as alapú számrendszerben?

2.6.3 Oldjuk meg az alábbi kongruenciákat:

a) $2x^{20} + 3x + 4 \equiv 0 \pmod{176}$;

b) $21x^{66} + 16x^{30} + 11x + 6 \equiv 0 \pmod{333}$;

c) $3x^9 + 5x + 7 \equiv 0 \pmod{105}$.

2.6.4 Legyenek a, b és c páronként relatív prím, 1-nél nagyobb egészek. Milyen maradékot ad

a) ab-vel osztva $a^{\varphi(b)} + b^{\varphi(a)}$;

b) abc-vel osztva $a^{\varphi(bc)} + b^{\varphi(ac)} + c^{\varphi(ab)}$?

2.6.5 Határozzuk meg 1234^{9876} utolsó három számjegyét.

2.6.6 Gondoltam egy egész számot 200 és 2000 között. Ha a szám 501-edik és 201-edik hatványát összeadom, majd ehhez hozzáadom magát a számot, akkor az eredmény 998-ra végződik. Melyik számra gondoltam?

2.6.7 Melyek azok az (a) kétjegyű; (b) háromjegyű pozitív egészek, amelyek négyzete is ugyanerre a két, illetve három számjegyre végződik?

2.6.8

a) Hány olyan huszonegyjegyű pozitív egész létezik, amelynek minden hatványában ugyanaz az utolsó húsz számjegy, mint az eredeti számban volt?

b) Hány olyan huszonegyjegyű pozitív egész létezik, amelynek minden páratlan hatványában ugyanaz az utolsó húsz számjegy, mint az eredeti számban volt?

M 2.6.9 Mennyi lesz a pontos idő (óra/perc) éjfél után $39^{38^{37}}$ perccel?

2.6.10

a) Legyen $(a, b) = 1$ és $r_1, \ldots, r_{\varphi(a)}$, illetve $s_1, \ldots, s_{\varphi(b)}$ redukált maradékrendszer modulo a, illetve modulo b. Jelöljük c_{ij}-vel az

$$x \equiv r_i \pmod{a}$$
$$x \equiv s_j \pmod{b}$$

szimultán kongruenciarendszer (egy) megoldását, $i = 1, \ldots, \varphi(a)$, $j = 1, \ldots, \varphi(b)$. Mutassuk meg, hogy a c_{ij} számok redukált maradékrendszert alkotnak modulo ab. A bizonyítás során csak a redukált maradékrendszer *definíció*ját használjuk (2.2.8 Definíció), és ne támaszkodjunk a 2.2.9 Tételre, illetve a jelen feladat b) részére.

b) Bizonyítsuk be (újra): $(a, b) = 1 \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b)$.

2.6.11 Igazoljuk, hogy a négyzetmentes számok sorozatában tetszőlegesen nagy hézagok is előfordulnak. Pontos megfogalmazásban ez azt jelenti, hogy bármely K-hoz létezik K olyan egymást követő pozitív egész, amelyek egyike sem négyzetmentes.

*2.6.12

a) Bizonyítsuk be, hogy az alábbi két szimultán kongruenciarendszer bármely a, b, c pozitív egész esetén megoldható.

$$\text{(a1)}\quad \begin{aligned} x &\equiv a+b \pmod{c} \\ x &\equiv b+c \pmod{a} \\ x &\equiv c+a \pmod{b} \end{aligned} \qquad\qquad \text{(a2)}\quad \begin{aligned} x &\equiv ab \pmod{c} \\ x &\equiv bc \pmod{a} \\ x &\equiv ca \pmod{b} \end{aligned}$$

b) Mutassuk meg, hogy az

$$x \equiv b \pmod{c}, \qquad x \equiv c \pmod{a}, \qquad x \equiv a \pmod{b}$$

szimultán kongruenciarendszer akkor és csak akkor oldható meg, ha $(a,b) = (b,c) = (c,a)$.

*2.6.13 Mutassuk meg, hogy az

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}$$

szimultán kongruenciarendszer (ahol az m_i modulusok nem feltétlenül páronként relatív prímek) akkor és csak akkor oldható meg, ha minden $1 \le i < j \le k$ esetén $(m_i, m_j) \mid c_i - c_j$ teljesül.

2.6.14 Van-e olyan $f(x)$ egész együtthatós polinom, amelyre az $f(x) \equiv 0 \pmod{30}$ kongruencia megoldásszáma 14?

2.6.15

a) Bizonyítsuk be, hogy akkor és csak akkor léteznek olyan számok, amelyek egyszerre alkotnak teljes maradékrendszert modulo n és redukált maradékrendszert modulo k, ha $\varphi(k) = n$ és $(k,n) = 1$.

**b) Bizonyítsuk be, hogy akkor és csak akkor léteznek olyan számok, amelyek egyszerre alkotnak redukált maradékrendszert modulo n és modulo k is, ha $\varphi(n) = \varphi(k)$.

2.6.16

*a) Bizonyítsuk be, hogy tetszőleges a_1, a_2 és a_3 különböző egész számokhoz végtelen sok olyan n természetes szám létezik, amelyre a_1+n, a_2+n és a_3+n páronként relatív prímek.

b) Adjunk meg olyan a_1, a_2, a_3 és a_4 különböző egészeket, hogy az a_i+n, $i=1,2,3,4$ számok semmilyen n természetes szám esetén se legyenek páronként relatív prímek.

*c) Mutassuk meg, hogy tetszőleges a_1, a_2, a_3 és a_4 különböző egész számokhoz végtelen sok olyan n természetes szám létezik, amelyre minden $i\neq j$ esetén $(a_i+n, a_j+n)\leq 2$.

*d) Igazoljuk, hogy tetszőleges a_1, a_2, a_3 és a_4 különböző egész számokhoz végtelen sok olyan n természetes szám létezik, amelyre minden $1\leq i<j<k\leq 4$ esetén

$$(a_i+n, a_j+n, a_k+n)=1\,.$$

*e) Igazak maradnak-e a c) és d) részben szereplő állítások, ha négy helyett öt, illetve hat a_i számot veszünk?

2.7. Wilson-tétel

T 2.7.1

2.7.1 Tétel (Wilson-tétel) Ha p (pozitív) prím, akkor $(p-1)!\equiv -1 \pmod p$. ♣

Mivel az $1,2,\ldots,p-1$ számok redukált maradékrendszert alkotnak modulo p, és bármely modulo p redukált maradékrendszer elemeinek a szorzata ugyanazt a maradékot adja p-vel osztva, ezért a Wilson-tételt a következő formában is megfogalmazhatjuk:

Ha p (pozitív) prím, akkor egy modulo p redukált maradékrendszer elemeinek a szorzata -1-gyel kongruens modulo p.

Az összetett modulusra vonatkozó általánosításokat a 2.7.1 feladatban, a csoportelméleti vonatkozásokat a 2.8 pontban tárgyaljuk.

Bizonyítás: A tétel $p=2$ és $p=3$ esetén nyilván igaz.

Megmutatjuk, hogy ha $p\geq 5$, akkor a $2,3,\ldots,p-2$ számok párba állíthatók úgy, hogy az egyes párokban az elemek szorzata 1-gyel legyen kongruens modulo p. Ebből a tétel már következik, hiszen ekkor $2\cdot 3\cdot\ldots\cdot(p-2)\equiv 1 \pmod p$, és így

$$(p-1)!=2\cdot 3\cdot\ldots\cdot(p-2)\cdot 1\cdot(p-1)\equiv 1\cdot 1\cdot(p-1)\equiv -1 \pmod p\,.$$

A párba állítást illusztráljuk először $p = 11$-re. A 2 párját a $2x \equiv 1 \pmod{11}$ kongruenciából kapjuk. Ennek egyetlen megoldása $x \equiv 6 \pmod{11}$, azaz a 2 párja a 6. Itt a 2 és a 6 valóban kölcsönösen összetartoznak, „egymás párjai", hiszen $2 \cdot 6 = 6 \cdot 2 \equiv 1 \pmod{11}$.

Hasonlóan továbbhaladva a 3–4, majd az 5–9, végül a 7–8 párokat kapjuk. Ennek alapján

$$10! = (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 1 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) = -1 \pmod{11}\,.$$

Most nézzük mindezt általánosan. A párba állításhoz a következőket kell igazolni:

(i) Minden $2 \le a \le p-2$ egészhez pontosan egy olyan $b = f(a)$ létezik, amelyre
$$ab \equiv 1 \pmod{p} \quad \text{és} \quad 2 \le b \le p-2\,.$$

(ii) Ha $f(a) = b$, akkor $f(b) = a$, azaz a és b valóban „egymás párjai".

(iii) $f(a) \ne a$, azaz „egyik elem párja sem önmaga".

(i) Az $ax \equiv 1 \pmod{p}$ kongruencia $(a, p) = 1$ miatt megoldható, és egyetlen b megoldása van a $0, 1, 2, \ldots, p-1$ teljes maradékrendszerben. Mivel $x = 0$, 1, illetve $p-1$ esetén $ax \equiv 0$, a, illetve $-a \pmod{p}$, így ezekre az x értékekre $ax \not\equiv 1 \pmod{p}$, tehát b valóban a megadott $2 \le b \le p-2$ intervallumba esik.

(ii) Az $f(a) = b$ feltétel azt jelenti, hogy $ab \equiv 1 \pmod{p}$. Az $f(b)$ értéket a $by \equiv 1 \pmod{p}$ kongruencia megoldása adja. Ezt a kongruenciát $y = a$ nyilván kielégíti, továbbá (i)-ből tudjuk, hogy ennek a kongruenciának a $2 \le y \le p-2$ intervallumban pontosan egy megoldása van. Ezért valóban $f(b) = a$.

(iii) A $b = a$ feltétel azt jelentené, hogy $a^2 \equiv 1 \pmod{p}$. Ezt oszthatóságra átírva, majd p prím tulajdonságát felhasználva

$$p \mid (a-1)(a+1) \Longrightarrow p \mid a-1 \text{ vagy } p \mid a+1 \Longrightarrow a \equiv \pm 1 \pmod{p}$$

következik. Ez viszont ellentmond a $2 \le a \le p-2$ feltételnek. ■

A Wilson-tétel egy-egy további bizonyítása szerepel a 3.1.2 Tétel után, valamint a 3.3.6 feladatban.

Feladatok

(Prímszámon végig pozitív prímet értünk.)

2.7.1 *A Wilson-tétel általánosításai összetett modulusra.* Legyen m összetett szám. Milyen maradékot ad m-mel osztva

a) $(m-1)!$; *b) $\big(\varphi(m)\big)!$;

*c) egy redukált maradékrendszer elemeinek a szorzata?

2.7.2 Mely $m > 6$ egészekre teljesül $(m-6)! \equiv 1 \pmod{m}$?

2.7.3 Legyen $m > 2$ és $a_1, \dots, a_m$, illetve $b_1, \dots b_m$ az $1, 2, \dots, m$ számok két tetszőleges permutációja.

a) Mutassuk meg, hogy ha m prím, akkor van olyan $i \neq j$, amelyre

$$m \mid a_i b_i - a_j b_j.$$

*b) Igazoljuk ugyanezt az állítást tetszőleges összetett m-re is.

2.7.4 Legyen p egy $4k-1$ alakú prímszám. Bizonyítsuk be, hogy ekkor

$$\Big(\frac{p-1}{2}\Big)! \equiv \pm 1 \pmod{p}.$$

2.7.5 Lássuk be, hogy bármely p prímszámra

$$p^p \mid (p^2-1)! - p^{p-1}.$$

2.7.6 Legyen $p > 3$ prím. Milyen maradékot ad $3(p-3)!$, ha p-vel maradékosan elosztjuk?

2.7.7 Milyen maradékot ad 99!, ha 10 100-zal maradékosan elosztjuk?

2.7.8 Számítsuk ki $\big(n!+3, (n+2)!+6\big)$ lehetséges értékeit, ha n végigfut a természetes számokon.

2.7.9 Milyen m-ekre létezik

a) teljes; b) redukált

maradékrendszer $k!$ alakú számokból?

2.7.10 Legyen $a_1, \dots, a_{30}$ redukált maradékrendszer modulo 31. Lássuk be, hogy

$$31 \mid (a_1 a_2 a_3)^3 + (a_4 a_5 \dots a_{30})^{27}.$$

2.7.11 Legyen $p > 2$ prím. Képezzünk egy egész számokból álló, $p-1$ tagú számtani sorozatot, és szorozzuk össze az elemeit. Milyen maradékot adhat ez a szorzat p-vel osztva?

2.7.12 Oldjuk meg az $x!(z-x)! \equiv 1 \pmod{z}$ kongruenciát, ahol $0 < x < z$ egész számok.

*2.7.13 Melyek azok a p prímek, amelyekre $(p-1)!+1$ a p-nek (pozitív egész kitevős) hatványa?

2.8. Műveletek maradékosztályokkal

Ebben a pontban a modulo m maradékosztályok között összeadást és szorzást értelmezünk és ezek tulajdonságait vizsgáljuk. Az $m > 1$ modulust végig rögzítettnek tekintjük.

2.8.1 Definíció **D 2.8.1**

Az $(a)_m$ és $(b)_m$ maradékosztályok *összeg*én az $(a+b)_m$, *szorzat*án pedig az $(ab)_m$ maradékosztályt értjük, azaz

$$(a)_m + (b)_m = (a+b)_m \qquad \text{és} \qquad (a)_m(b)_m = (ab)_m\,. \ \clubsuit$$

Be kell látnunk, hogy a fenti módon valóban műveleteket definiáltunk, azaz mind az összeadásnál, mind pedig a szorzásnál bármely két modulo m maradékosztályhoz *egyértelműen* hozzárendeltünk egy modulo m maradékosztályt.

A problémát az jelenti, hogy a maradékosztályokra vonatkozó összeadást és szorzást a reprezentánsok segítségével adtuk meg, és így azt kell igazolni, hogy ez nem függ attól, hogy az egyes maradékosztályokban melyik reprezentánst választottuk.

Nézzük az összeadást. Azt kell megmutatni, hogy ha $(a)_m = (a')_m$ és $(b)_m = (b')_m$, akkor $(a+b)_m = (a'+b')_m$. Ez valóban teljesül, ugyanis

$$\left.\begin{array}{rcl} (a)_m = (a')_m & \Longrightarrow & a \equiv a' \pmod{m} \\ (b)_m = (b')_m & \Longrightarrow & b \equiv b' \pmod{m} \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow a+b \equiv a'+b' \pmod{m} \Longrightarrow (a+b)_m = (a'+b')_m\,.$$

Hasonlóan járhatunk el a szorzás esetében is.

Felhívjuk a figyelmet arra, hogy számos olyan, az egész számokon értelmezett művelet van, amelyek megfelelőit nem lehet a reprezentánsok segítségével a maradékosztályok körében értelmezni. Ennek illusztrálására egy egyszerű példát mutatunk, további példák szerepelnek a 2.8.6 feladatban.

Legyenek a és b egész számok, és jelölje $\max(a,b)$ közülük a nagyobbikat, illetve a közös értéküket, ha $a=b$. Ez a maximumképzés bármely két egész számhoz egyértelműen hozzárendel egy egész számot, tehát művelet az egész számok körében.

Azonban a modulo m maradékosztályok körében a $\max\big((a)_m,(b)_m\big) = \big(\max(a,b)\big)_m$ egyenlőséggel nem tudunk műveletet értelmezni, ugyanis az egyenlőség jobb oldalán más és más maradékosztályt kap(hat)unk, ha az $(a)_m$, illetve $(b)_m$ maradékosztályt egy másik elemével reprezentáljuk. Például legyen a modulus $m=9$, a két maradékosztály pedig $A=(3)_9=(12)_9$ és $B=(10)_9=(1)_9$. Ekkor $\max(A,B)$ egyrészt $\big(\max(3,10)\big)_9=(10)_9$, másrészt $\big(\max(12,1)\big)_9=(12)_9$ lenne, azonban $(10)_9\neq(12)_9$.

Most rátérünk a modulo m maradékosztályok körében értelmezett összeadás és szorzás legfontosabb tulajdonságaira.

Könnyen adódik, hogy az egész számoknál megismert tulajdonságok nagy része a maradékosztályok körében is érvényben marad:

2.8.2 Tétel **T 2.8.2**

A modulo m maradékosztályok körében

— az összeadás *asszociatív* és *kommutatív*;

— a $(0)_m$ *nullelem*, azaz minden $(a)_m$-ra $(0)_m+(a)_m=(a)_m+(0)_m=(a)_m$;

— az $(a)_m$ *ellentett*je $(-a)_m$, azaz $(-a)_m+(a)_m=(a)_m+(-a)_m=(0)_m$;

— a szorzás *asszociatív* és *kommutatív*;

— az $(1)_m$ *egységelem*, azaz minden $(a)_m$-ra $(1)_m(a)_m=(a)_m(1)_m=(a)_m$;

— érvényes a *disztributivitás*. ♣

Bizonyítás: Valamennyi állítás azonnal következik a műveletek definíciójából és az egész számok megfelelő tulajdonságából. Nézzük példaként az összeadás kommutativitását:

$$(a)_m+(b)_m=(a+b)_m=(b+a)_m=(b)_m+(a)_m$$

(az első és a harmadik egyenlőség a maradékosztályok közötti összeadás definíciójából, a második egyenlőség pedig az egész számok összeadásának kommutativitásából adódik). ■

A 2.8.2 Tételben felsorolt tulajdonságok azt jelentik, hogy a modulo m maradékosztályok az összeadásra és szorzásra nézve *egységelemes, kommutatív gyűrű*t alkotnak.

Megjegyezzük, hogy — mint bármely gyűrűben — a maradékosztályok körében a *kivonás* is elvégezhető, azaz bármely $(a)_m$ és $(b)_m$ esetén pontosan egy olyan $(c)_m$ létezik, amelyre $(a)_m = (b)_m + (c)_m$; a keresett $(c)_m$ maradékosztályt az $(a)_m + (-b)_m$ alakban kaphatjuk meg. (A kivonás elvégezhetőségét az egész számok kivonására támaszkodva is beláthatjuk, ekkor $(c)_m = (a-b)_m$ adódik.)

Most megvizsgáljuk, hogy mely maradékosztályoknak létezik a szorzásra nézve *inverze* (multiplikatív inverze, „reciproka"), azaz mely $(a)_m$ esetén létezik olyan $(c)_m$ maradékosztály, amelyre

$$(c)_m(a)_m = (a)_m(c)_m = (1)_m\,. \tag{1}$$

Az (1) feltétel azt jelenti, hogy $(ac)_m = (1)_m$, azaz $ac \equiv 1 \pmod m$, vagyis az $ax \equiv 1 \pmod m$ lineáris kongruencia megoldható. A 2.5.3 Tétel szerint ennek szükséges és elégséges feltétele, hogy $(a, m) \mid 1$, vagyis $(a, m) = 1$ teljesüljön. Ez azzal ekvivalens, hogy $(a)_m$ redukált maradékosztály legyen. Így beláttuk az alábbi tételt:

2.8.3 Tétel **T 2.8.3**

A modulo m maradékosztályok között pontosan a redukált maradékosztályoknak létezik (multiplikatív) inverze. ♣

Megjegyezzük, hogy bármely asszociatív művelet esetén egy elemnek csak egy inverze lehet. Így egy redukált maradékosztály inverze is egyértelmű. (Ez egyébként a 2.5.5 Tételből is következik.)

Kommutatív *test*en egy olyan (legalább kételemű) kommutatív, egységelemes gyűrűt értünk, amelyben a nullelemen kívül minden elemnek létezik inverze. A 2.8.3 Tétel szerint a modulo m maradékosztályok körében ez akkor és csak akkor teljesül, ha minden nemnulla maradékosztály redukált, azaz m prím. Így a következő tételt kaptuk:

2.8.4 Tétel **T 2.8.4**

A modulo m maradékosztályok akkor és csak akkor alkotnak testet, ha m prím. ♣

A modulo m maradékosztályok körében előfordulhat, hogy két nemnulla maradékosztály szorzata a nulla maradékosztály, például $(5)_{10}(4)_{10} = (0)_{10}$. Egy $(a)_m \neq (0)_m$ maradékosztályt — a (kommutatív) gyűrűkben értelmezett általános fogalomnak megfelelően — *nullosztó*nak nevezünk, ha

$$\text{van olyan } (b)_m \neq (0)_m, \text{ amelyre } (a)_m(b)_m = (0)_m. \tag{2}$$

Az előző példa szerint tehát a $(4)_{10}$ maradékosztály nullosztó.

2.8.5 Tétel **T 2.8.5**

Az $(a)_m \neq (0)_m$ maradékosztály akkor és csak akkor nullosztó, ha $(a)_m$ *nem* redukált maradékosztály, azaz $(a, m) \neq 1$. ♣

Az $(a)_m \neq (0)_m$ feltétel az a reprezentánsra vonatkozóan az $m \nmid a$, illetve $(a, m) < m$ kikötést jelenti.

Bizonyítás: A nullosztó (2)-beli definícióját átírva kapjuk, hogy $(a)_m \neq (0)_m$ pontosan akkor nullosztó, ha

$$\text{van olyan } b \not\equiv 0 \pmod{m}, \text{ amelyre } ab \equiv 0 \pmod{m}. \tag{3}$$

Mivel az $ax \equiv 0 \pmod{m}$ kongruenciának $x \equiv 0 \pmod{m}$ mindig megoldása, ezért (3) azzal ekvivalens, hogy az $ax \equiv 0 \pmod{m}$ kongruencia megoldásszáma 1-nél nagyobb. Mivel ez a megoldásszám éppen (a, m), így $(a)_m \neq (0)_m$ valóban akkor és csak akkor nullosztó, ha $(a, m) > 1$. ■

A 2.8.5 Tételből azonnal következik, hogy a modulo m maradékosztályok körében akkor és csak akkor található nullosztó, ha m összetett szám.

Végül röviden kitérünk a maradékosztályok néhány csoportelméleti vonatkozására.

Egy G halmazt akkor nevezünk *csoport*nak, ha értelmezve van G-n egy asszociatív művelet, létezik egységelem és minden elemnek van inverze. Ha a művelet kommutatív, akkor *kommutatív* vagy *Abel*-csoportról beszélünk.

Ennek alapján a modulo m maradékosztályok az összeadásra, a redukált maradékosztályok pedig a szorzásra kommutatív csoportot alkotnak (ez utóbbi abból következik, hogy két redukált maradékosztály szorzata, valamint egy redukált maradékosztály inverze is redukált maradékosztály).

Az Euler–Fermat-tétel a következő általános csoportelméleti tétel speciális esetének tekinthető: Egy véges G csoport bármely a elemére $a^{|G|}$ a csoport egységelemével egyenlő (ahol $|G|$ a csoport elemszámát jelöli). Ez a csoportelméleti tétel kommutatív G esetén az Euler–Fermat-tétel mintájára igazolható (lásd a 2.8.7 feladatot), tetszőleges G-re pedig az ún. *Lagrange-tétel*ből következik.

A Wilson-tétel általánosításaként azt a kérdést lehet megvizsgálni, hogy egy véges kommutatív csoport elemeinek a szorzata a csoport melyik elemével egyenlő (lásd a 2.8.8 feladatot).

Feladatok

2.8.1 Milyen m esetén létezik olyan nemnulla maradékosztály, amely önmagának az ellentettje?

2.8.2 Tekintsük a modulo 100 maradékosztályok gyűrűjét.

a) Mi a (13) maradékosztály multiplikatív inverze?

b) Hány nullosztó van?

c) A (40) maradékosztálynak hány nullosztópárja van, azaz hány olyan $(b) \neq (0)$ maradékosztály létezik, amelyre $(40)(b) = (0)$?

d) Van-e olyan (c) maradékosztály, amelyre $(35)(c) = (90)$?

2.8.3 Hány olyan modulo m maradékosztály van, amelynek önmaga a multiplikatív inverze, ha m értéke

a) 47; b) 30; c) 800; *d) tetszőleges?

2.8.4 Legyen m összetett szám, és tekintsük a modulo m maradékosztályok gyűrűjét.

a) Mutassuk meg, hogy ha (a) nullosztó, akkor tetszőleges (c)-re $(a)(c)$ nullosztó vagy (0).

b) Lássuk be, hogy ha $(a)(c)$ nullosztó, akkor (a) és (c) közül legalább az egyik nullosztó.

c) Melyek azok az m-ek, amelyekre bármely két nullosztó összege is nullosztó vagy (0)?

d) Határozzuk meg az összes nullosztó összegét, illetve szorzatát.

e) Mely m-ek esetén létezik olyan $(a) \neq (0)$, amelyre $(a)^2 = (0)$?

2.8.5

a) Legyen H a modulo 20 maradékosztályok közül a „4-gyel oszthatók” halmaza, azaz

$$H = \{(0)_{20},\ (4)_{20},\ (8)_{20},\ (12)_{20},\ (16)_{20}\}.$$

Bizonyítsuk be, hogy H a maradékosztályok összeadására és szorzására kommutatív testet alkot.

b) Legyen K a modulo 40 maradékosztályok közül a „4-gyel oszthatók” halmaza, azaz

$$K = \{(0)_{40},\ (4)_{40},\ \ldots,\ (36)_{40}\}.$$

Mutassuk meg, hogy K a maradékosztályok összeadására és szorzására kommutatív gyűrűt alkot, amely azonban nem test, a szorzásra nézve nincs egységelem, sőt K minden nemnulla eleme nullosztó.

M *c) Általánosítsuk (minél jobban) a feladatot.

2.8.6 Vizsgáljuk meg minél részletesebben, lehet-e a modulo m maradékosztályokra a pozitív reprezentánsok segítségével értelmezni

a) a legnagyobb közös osztót: $\mathrm{lnko}\big((a)_m,(b)_m\big)=\big(\mathrm{lnko}(a,b)\big)_m$;

b) a köbre emelést: $(a)_m^3=(a^3)_m$;

c) a köbgyökvonást: $\sqrt[3]{(a)_m}=(\sqrt[3]{a})_m$;

d) a számtani közép képzését: $\big((a)_m+(b)_m\big)/2=\big((a+b)/2\big)_m$;

e) a hatványozást: $(a)_m^{(b)_m}=\big(a^b\big)_m$?

2.8.7 *Az Euler–Fermat-tétel általánosítása.* Jelölje a G véges kommutatív csoport elemszámát $|G|$, egységelemét e. Bizonyítsuk be, hogy bármely $a\in G$ elemre $a^{|G|}=e$.

*2.8.8 *A Wilson-tétel általánosítása.* Jelölje S egy G véges kommutatív csoport elemeinek a szorzatát és e az egységelemet. Mutassuk meg, hogy ha G-ben pontosan egy olyan $c\neq e$ elem van, amelyre $c^2=e$, akkor $S=c$, minden más esetben pedig $S=e$.

3. MAGASABB FOKÚ KONGRUENCIÁK

A fejezet elején néhány általános észrevételt teszünk a prím modulusú ismeretlenes kongruenciákra vonatkozóan. Ezután a rend, a primitív gyök és a diszkrét logaritmus legfontosabb tulajdonságait tárgyaljuk, majd ezek felhasználásával a modulo p „gyökvonás" kérdését, azaz a prím modulusú binom kongruenciákat tekintjük át. Szerepeltetjük Kőnig és Rados, valamint Chevalley egy-egy nevezetes tételét is. Végül megmutatjuk, hogyan lehet az összetett modulusú kongruenciákat prímhatvány, illetve prím modulusú kongruenciákra visszavezetni.

3.1. Megoldásszám és redukció

Legyen m rögzített pozitív egész, f tetszőleges egész együtthatós polinom, és tekintsük az $f(x) \equiv 0 \pmod{m}$ ismeretlenes kongruenciát.

A lineáris kongruenciákhoz hasonlóan *megoldás*on egy olyan s egész számot értünk, amelyet az x helyére beírva a kongruencia fennáll. Itt is világos, hogy ha egy s szám megoldás, akkor az $(s)_m$ maradékosztály minden eleme megoldás, hiszen $s \equiv r \pmod{m}$ esetén $f(s) \equiv f(r) \pmod{m}$. Ennek alapján *megoldásszám*on a *páronként inkongruens* megoldások számát értjük, vagyis azt, hogy hány *maradékosztály*ba tartoznak a megoldások (lásd a 2.5.2 Definíciót). Az is nyilvánvaló, hogy f együtthatóira vonatkozóan is csak az számít, hogy melyik maradékosztályokba tartoznak modulo m.

Mindezek alapján gyakran kényelmesebb és természetesebb, ha mind az együtthatókat, mind pedig a megoldásokat (egész számok helyett) modulo m maradékosztályokként kezeljük. Ez más szóval azt jelenti, hogy f-et a modulo m maradékosztályok $\mathbf{Z}_m$ gyűrűje feletti polinomnak tekintjük, és az $f(x) \equiv 0 \pmod{m}$ kongruencia megoldásai az f-hez tartozó polinomfüggvénynek a $\mathbf{Z}_m$-beli gyökei. Ennek megfelelően definiáljuk az f polinom modulo m vett fokszámát is:

3.1.1 Definíció **D 3.1.1**

Az $f = a_0 + a_1x + \ldots + a_nx^n$ polinom modulo m vett *fokszám*a (vagy *fok*a) k, ha $a_k \not\equiv 0 \pmod{m}$, de minden $i > k$ esetén $a_i \equiv 0 \pmod{m}$. Ha minden i-re $a_i \equiv 0 \pmod{m}$, azaz f minden együtthatója 0 mod m, akkor f-nek modulo m nincs foka. ♣

Példa: az $f = 6 + 12x + 15x^2 + 21x^3$ polinomnak modulo 5 a foka 3, modulo 7 a foka 2 és modulo 3 nincs foka.

A pont további részében prím modulusú kongruenciákkal foglalkozunk.

3.1.2 Tétel **T 3.1.2**

Ha p prím és az f polinom modulo p vett foka k, akkor az $f(x) \equiv 0 \pmod{p}$ kongruencia megoldásszáma legfeljebb k. ♣

Bizonyítás: Az előzetes megjegyzések szerint tekintsük f-et a modulo p maradékosztályok $\mathbf{Z}_p$ gyűrűje feletti polinomként, ekkor a kongruencia megoldásszáma az f-hez tartozó polinomfüggvény $\mathbf{Z}_p$-beli gyökeinek a száma.

Mivel $\mathbf{Z}_p$ a 2.8.4 Tétel szerint kommutatív test, ezért a 3.1.2 Tétel állítása azonnal következik az alábbi jól ismert klasszikus algebrai tételből: Ha egy T kommutatív test feletti polinom foka k, akkor a megfelelő polinomfüggvénynek legfeljebb k gyöke lehet T-ben. ■

A 3.1.2 Tétel állítása összetett modulusra nem igaz, pl. a

$$10x - 15 \equiv 0 \pmod{25}$$

elsőfokú kongruencia megoldásszáma 5, az

$$x(x-1)(x-2)(x-3) \equiv 0 \pmod{24}$$

negyedfokú kongruencia megoldásszáma 24 stb.

A 3.1.2 Tétel segítségével újabb bizonyítást nyerhetünk a Wilson-tételre (2.7.1 Tétel): Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.

Az állítás $p = 2$-re nyilvánvaló. Legyen $p > 2$, és tekintsük az

$$f = x^{p-1} - 1 - (x-1)(x-2)\dots(x-(p-1)) = a_0 + a_1 x + \dots + a_{p-2}x^{p-2}$$

polinomot. Az $f(x) \equiv 0 \pmod{p}$ kongruenciának a kis Fermat-tétel szerint az $x = 1, 2, \dots, p-1$ (páronként inkongruens) számok valamennyien megoldásai, tehát a megoldásszám legalább $p-1$. Ha f-nek modulo p létezne foka, akkor ez a fok legfeljebb $p-2$ lehetne, ami ellentmond a 3.1.2 Tételnek. Ebből következik, hogy f-nek modulo p nincs foka, vagyis valamennyi együtthatója 0 modulo p. Speciálisan

$$a_0 = -1 - (-1)^{p-1}(p-1)! = -1 - (p-1)! \equiv 0 \pmod{p},$$

ami éppen a Wilson-tétel állítása. ■

Mivel egy modulo m kongruencia megoldásszáma legfeljebb m, ezért a 3.1.2 Tétel állítása semmitmondó, ha f modulo p vett foka p vagy annál nagyobb. Azonban az $f(x) \equiv 0 \pmod{p}$ kongruencia vizsgálata ebben az esetben is „redukálható" egy legfeljebb $p-1$-edfokú kongruenciára az alábbi értelemben:

3.1.3 Tétel **T 3.1.3**

Bármely p prím és f egész együtthatós polinom esetén létezik olyan g egész együtthatós polinom, hogy

(i) a g modulo p vett foka legfeljebb $p-1$ vagy g minden együtthatója 0 modulo p; és

(ii) minden c egész számra $f(c) \equiv g(c) \pmod{p}$. ♣

Más megfogalmazásban a 3.1.3 Tétel azt jelenti, hogy a $\mathbf{Z}_p$ test felett bármely f polinomhoz található olyan legfeljebb $p-1$-edfokú g polinom (megengedve a nullpolinomot is), hogy a két polinomhoz ugyanaz a polinomfüggvény tartozik.

A tételből nyilvánvalóan következik, hogy az $f(x) \equiv 0 \pmod{p}$ és $g(x) \equiv 0 \pmod{p}$ kongruenciáknak ugyanazok a megoldásai, és így a 3.1.2 Tétel szerint a megoldásszám legfeljebb annyi, mint a g modulo p vett foka.

Első bizonyítás: Írjunk f-ben mindenütt x^p helyére mindaddig x-et, amíg ez csak lehetséges. Így végül egy olyan g polinomhoz jutunk, amelynek (modulo p vett) foka legfeljebb $p-1$ vagy minden együtthatója 0 modulo p. Mivel a kis Fermat-tétel szerint bármely c-re $c^p \equiv c \pmod{p}$, ezért $f(c) \equiv g(c) \pmod{p}$ is teljesül. ■

Második bizonyítás: Osszuk el f-et maradékosan $x^p - x$-szel; mivel $x^p - x$ főegyütthatója 1, ezért a hányados és a maradék is egész együtthatós lesz. Megmutatjuk, hogy a keletkezett maradék megfelel g-nek. Valóban, legyen

$$f = (x^p - x)h + g,$$

ahol g foka legfeljebb $p-1$ vagy g a nullpolinom. Ekkor bármely c egész számra

$$f(c) = (c^p - c)h(c) + g(c) \equiv 0 + g(c) = g(c) \pmod{p}. \blacksquare$$

Megjegyzések: 1. A második bizonyításban a maradékos osztást végezhetjük a $\mathbf{Z}_p$ test feletti polinomok körében is, csak ez kicsit nehézkesebb.

2. Mindkét bizonyítás egyúttal konkrét algoritmust is ad a megfelelő g előállítására (sőt, tulajdonképpen ugyanannak az eljárásnak a kétféle megközelítéséről van szó).

3. Egy harmadik bizonyítást kaphatunk az ún. *interpolációs polinom*ok segítségével, ez azonban g gyakorlati előállítására nemigen alkalmas (lásd a 3.1.8 feladatot).

4. A 3.1.3 Tételt kiegészíthetjük azzal, hogy (megfelelő értelemben tekintve) csak egy ilyen tulajdonságú g polinom létezik (lásd a 3.1.9 feladatot).

Feladatok

3.1.1 Határozzuk meg az alábbi kongruenciák megoldásszámát:
- a) $x^{100} + x \equiv 0 \pmod{101}$;
- b) $x^{100} + x \equiv 0 \pmod{100}$;
- c) $21x^9 + 18x^6 + 15 \equiv 0 \pmod{77}$;
- d) $x(x^2 - 1)(x^2 - 4) \equiv 0 \pmod{60}$.

3.1.2 Bizonyítsuk be, hogy c akkor és csak akkor megoldása az $f(x) \equiv 0 \pmod{m}$ kongruenciának, ha van olyan h egész együtthatós polinom, amelyre az $f-(x-c)h$ polinom minden együtthatója osztható m-mel.

3.1.3 Jelöljük az $f(x) \equiv 0 \pmod{m}$ kongruencia megoldásszámát $N(f, m)$-mel. Melyek igazak az alábbi állítások közül?
- a) $N(fg, m) \leq N(f, m) + N(g, m)$.
- b) $N(fg, m) \leq N(f, m) + N(g, m) + 1000$.
- c) $N(fg, 13) \leq N(f, 13) + N(g, 13)$.
- d) $N(fg, 13) = N(f, 13) + N(g, 13)$.

3.1.4
- a) Adjunk meg olyan f polinomot, amelynek a modulo 37 vett foka 13 és az $f(x) \equiv 0 \pmod{37}$ kongruencia megoldásszáma 12.
- b) Hány olyan f van, amely teljesíti az a)-beli feltételeket és minden együtthatója az $1, 2, \ldots, 37$ számok közül kerül ki?

3.1.5 Legyen p prím, és jelöljük az $f(x) \equiv 0 \pmod{p}$ kongruencia megoldásszámát r-rel. Lássuk be, hogy

$$r \equiv -\sum_{i=1}^{p} f(i)^{p-1} \pmod{p}.$$

3.1.6 Legyen $p > 2$ prím és $1 \leq j \leq p - 2$. Bizonyítsuk be, hogy az $1, 2, \ldots, p - 1$ számokból képezett összes j tényezős szorzat összege osztható p-vel.

3.1.7 Legyen $p > 2$ prím és

$$f = a_0 + a_1 x + \ldots + a_n x^n, \qquad \text{ahol} \qquad a_0 \not\equiv 0 \pmod{p}.$$

Bizonyítsuk be, hogy az $f(x) \equiv 0 \pmod{p}$ kongruencia redukálható egy legfeljebb $p-2$-edfokú kongruencia vizsgálatára az alábbi értelemben: megadható olyan h polinom, amelynek a modulo p vett foka legfeljebb $p-2$ vagy minden együtthatója $\equiv 0 \pmod{p}$, és minden $(c,p) = 1$ esetén $f(c) \equiv h(c) \pmod{p}$ teljesül.

3.1.8 Bizonyítsuk be a 3.1.3 Tételben szereplő g létezését a Lagrange- vagy Newton-féle interpolációs polinomok felhasználásával.

3.1.9 Bizonyítsuk be, hogy a 3.1.3 Tétel követelményeit kielégítő g mint $\mathbf{Z}_p$ feletti polinom egyértelmű, azaz az együtthatói modulo p egyértelműen meg vannak határozva.

3.1.10 Lássuk be, hogy a 3.1.3 Tétel összetett modulus esetén is érvényben marad.

3.2. Rend

Az Euler–Fermat-tételből következik, hogy ha $(a,m) = 1$, akkor van olyan t pozitív egész, amelyre $a^t \equiv 1 \pmod{m}$; ilyen kitevő például a $\varphi(m)$ vagy annak bármely többszöröse. A további vizsgálatokban kitüntetett szerepet játszik a *legkisebb* ilyen tulajdonságú t pozitív egész, amelyet az a *rend*jének nevezünk modulo m:

3.2.1 Definíció **D 3.2.1**

Legyen $(a,m) = 1$. A k pozitív egészt az a *rend*jének nevezzük modulo m, ha $a^k \equiv 1 \pmod{m}$, de bármely $0 < i < k$ esetén $a^i \not\equiv 1 \pmod{m}$. ♣

Az a rendjét $o_m(a)$-val jelöljük. Például $o_7(2) = 3$, $o_{10}(3) = 4$ stb. Ha nem okoz félreértést, akkor a modulusra utaló indexet el is hagyhatjuk. Az „a rendje” helyett — a rend szó latin megfelelőjével — az „ordo a” kifejezést is szokás használni.

Az Euler–Fermat-tételből következik, hogy minden $(a,m) = 1$ esetén létezik az a-nak rendje és $o_m(a) \le \varphi(m)$.

A rend fogalma csak $(a,m) = 1$ esetén értelmezhető: ha $(a,m) \neq 1$, akkor egyáltalán nem létezik olyan $k > 0$ kitevő, amelyre $a^k \equiv 1 \pmod{m}$ teljesülne (lásd a 2.4.1B Tétel utáni 1. megjegyzést).

A rend definíciójából világos, hogy

$$a \equiv b \pmod{m} \Longrightarrow o_m(a) = o_m(b),$$

tehát egy redukált maradékosztály valamennyi elemének ugyanaz a rendje.

Az alábbi tételben összefoglaljuk a rend legfontosabb tulajdonságait.

3.2.2 Tétel **T 3.2.2**

Legyenek t, u, v nemnegatív egészek és $(a, m) = 1$.

(i) $a^t \equiv 1 \pmod{m} \iff o_m(a) \mid t$.

(ii) $a^u \equiv a^v \pmod{m} \iff u \equiv v \pmod{o_m(a)}$.

(iii) Az a-nak $o_m(a)$ darab páronként inkongruens pozitív egész kitevős hatványa létezik modulo m.

(iv) $o_m(a) \mid \varphi(m)$. ♣

Bizonyítás: (i) Ha $t = qo_m(a)$, akkor

$$a^t = \left(a^{o_m(a)}\right)^q \equiv 1^q = 1 \pmod{m}.$$

A megfordításhoz osszuk el a t számot maradékosan $o_m(a)$-val: $t = qo_m(a)+r$, ahol $0 \le r < o_m(a)$. Ekkor

$$1 \equiv a^t = \left(a^{o_m(a)}\right)^q \cdot a^r \equiv 1 \cdot a^r = a^r \pmod{m}.$$

Mivel $r < o_m(a)$, ezért a rend definíciója miatt csak $r = 0$ lehetséges, azaz valóban $o_m(a) \mid t$.

(ii) Legyen $u \ge v$. Ekkor $(a, m) = 1$ és (i) felhasználásával

$$a^u \equiv a^v \pmod{m} \iff a^{u-v} \equiv 1 \pmod{m} \iff$$
$$\iff o_m(a) \mid u - v \iff u \equiv v \pmod{o_m(a)}.$$

(iii) Ez azonnal következik (ii)-ből.

(iv) Az Euler–Fermat-tétel szerint $a^{\varphi(m)} \equiv 1 \pmod{m}$, és így (i) alapján $o_m(a) \mid \varphi(m)$. ■

Példa: Számítsuk ki a 13 rendjét modulo 59.

A 13 és 59 relatív prímek, tehát $o_{59}(13)$ létezik. Mivel $o_{59}(13) \mid \varphi(59)$ és $\varphi(59) = 58$, ezért

$$o_{59}(13) = 1,\ 2,\ 29 \text{ vagy } 58.$$

Nyilván $13 \not\equiv 1 \pmod{59}$, $13^2 \not\equiv 1 \pmod{59}$, és így $o_{59}(13)$ értéke csak 29 vagy 58 lehet. Ennek megfelelően, ha $13^{29} \equiv 1 \pmod{59}$, akkor a rend 29, ha pedig $13^{29} \not\equiv 1 \pmod{59}$, akkor a rend 58.

A 13^{29} maradékát modulo 59 ismételt négyzetre emelések segítségével határozhatjuk meg:

$$\begin{aligned} 13^2 &= 169 \equiv -8 \pmod{59} \\ 13^4 &\equiv (-8)^2 \equiv 5 \pmod{59} \\ 13^8 &\equiv 5^2 = 25 \pmod{59} \\ 13^{16} &\equiv 25^2 \equiv -24 \pmod{59} \end{aligned}$$

és így

$$\begin{aligned} 13^{29} = 13^{16} \cdot 13^8 \cdot 13^4 \cdot 13 &\equiv (-24) \cdot 25 \cdot 5 \cdot 13 = \\ &= (-600) \cdot 65 \equiv (-10) \cdot 6 \equiv -1 \pmod{59}. \end{aligned}$$

Tehát $o_{59}(13) = 58$. (Megjegyezzük, hogy 13^{58} maradékát modulo 59 semmiképpen sem kellett külön kiszámítani, de az Euler–Fermat-tételből eleve is tudtuk, hogy ez a maradék 1.)

Végül megemlítjük, hogy a 3.2.1 Definíció a csoportbeli elemrend fogalmának a speciális esete, és a 3.2.2 Tétel megfelelője is igaz tetszőleges csoportban.

Feladatok

(Ha az index nélküli $o(a)$ jelölést használjuk, akkor ez vagy a feladatban szereplő m, illetve p modulusra, vagy pedig ilyenek hiányában tetszőleges modulusra vonatkozik.)

3.2.1 Számítsuk ki a következő rendeket:

a) $o_{77}(155)$; b) $o_{100}(199)$; c) $o_{65}(2)$; d) $o_{47}(43)$.

3.2.2 Van-e olyan a, amelyre $o_m(a) = 4$, ha m értéke a) 11; b) 12; c) 17?

3.2.3 Melyek azok az m modulusok, amelyekre $o_m(2) = 6$?

3.2.4 Legyen $(a, m) = 1$, $o_m(a) = k$ és $i \geq 0$. Mutassuk meg, hogy

a) $o_m(a^i) \mid k$;

b) $o_m(a^i) = k \iff (i, k) = 1$;

c) $o_m(a^i) = k/(i, k)$.

3.2.5 Mik $o(a)$ lehetséges értékei, ha $o(a^3)$ értéke a) 10; b) 12?

M 3.2.6 Legyen $p > 2$ prím. Igazoljuk: $o_p(a) = o_p(-a) \iff 4 \mid o_p(a)$.

3.2.7 Tegyük fel, hogy a^5, a^{13} és a^{21} pontosan két redukált maradékosztályba tartoznak modulo m. Számítsuk ki $o_m(a)$ értékét.

3.2.8 Tegyük fel, hogy p prím és $o_p(a) = 3$.

a) Lássuk be, hogy $1 + a + a^2 \equiv 0 \pmod{p}$.

b) Számítsuk ki $o_p(1 + a)$ értékét.

M 3.2.9 Tegyük fel, hogy $p > 5$ prím és $a^{2p-10} \equiv -1 \pmod{p}$. Számítsuk ki $o_p(a)$ értékét.

3.2.10

a) Lássuk be, hogy az $a^n \equiv 1 \pmod{m}$ és $a^k \equiv 1 \pmod{m}$ kongruenciák egyidejűleg pontosan akkor teljesülnek, ha $a^{(n,k)} \equiv 1 \pmod{m}$.

b) Az a) rész felhasználásával adjunk új bizonyítást az 1.3.13 feladatra.

3.2.11 Igazoljuk, hogy ha n páratlan, akkor $(a^n - 1, a^k + 1) \leq 2$.

3.2.12 Legyen $p > 2$ prím, $(a, p) = 1$. Mutassuk meg, hogy akkor és csak akkor létezik olyan s, amelyre $a^s \equiv -1 \pmod{p}$, ha $o_p(a)$ páros. Mennyiben változik a helyzet, ha p helyett egy m összetett modulust veszünk?

3.2.13 Bizonyítsuk be, hogy

a) $(a, m) = 1$, $d \mid m \Longrightarrow o_d(a) \mid o_m(a)$;

b) $(a, mn) = 1 \Longrightarrow o_{[m,n]}(a) = [o_m(a), o_n(a)]$.

3.2.14 Az $1, 2, \ldots, 999$ számok között hány másodrendű elem van mod 1000?

*3.2.15 Legyen $o(a) = u$, $o(b) = v$. Igazoljuk, hogy

a) $o(ab) = uv \iff (u, v) = 1$;

b) $\dfrac{[u, v]}{(u, v)} \mid o(ab)$ és $o(ab) \mid [u, v]$.

*3.2.16 Tegyük fel, hogy $a^{o(b)} \equiv b^{o(a)} \pmod{m}$. Lássuk be, hogy $o(a) = o(b)$.

3.2.17 Bizonyítsuk be, hogy $n \mid \varphi(a^n - 1)$ bármely $a > 1$ és $n > 0$ esetén teljesül.

*3.2.18 Legyen $a_1, \ldots, a_{\varphi(m)}$ redukált maradékrendszer modulo m. Mutassuk meg, hogy $\sum_{i=1}^{\varphi(m)} o_m(a_i)$ mindig páratlan szám.

3.2.19 Legyen p prím és $(a,p)=1$. Milyen maradékot ad p-vel osztva az alábbi összeg és szorzat:

$$\text{a) } a+a^2+\ldots+a^{o(a)}\,; \qquad \text{b) } a\cdot a^2\cdot\ldots\cdot a^{o(a)}\,?$$

3.2.20 *Tizedes törtek.* Csak a tizedesvessző után következő jegysorozattal foglalkozunk, ezért elegendő $0<\alpha<1$ számokat tekintenünk. A feladatban kizárjuk azokat a végtelen tizedes törteket, amelyekben egy határtól kezdve minden számjegy 9-es. Egy tizedes tört *véges*, ha csak véges sok jegyből áll; ezt a legrövidebb alakban írjuk fel, azaz az utolsóként szereplő tizedesjegy nem nulla. Egy végtelen tizedes tört *szakaszos*, ha a tizedesjegyek sorozata egy határtól kezdve periodikus, ezen belül *tiszta szakaszos*, illetve *vegyes szakaszos*, attól függően, hogy a periodicitás (azaz az első szakasz) közvetlenül a tizedesvessző után, illetve csak később kezdődik. A racionális számok a/b közönséges tört alakjában feltesszük, hogy $b>0$ és $(a,b)=1$.

a) Mutassuk meg, hogy egy α valós szám tizedestört-alakja akkor és csak akkor véges vagy végtelen szakaszos, ha α racionális.

b) Az a/b racionális szám tizedestört-alakja akkor és csak akkor véges, ha b kanonikus alakjában legfeljebb a 2 és az 5 prímszámok szerepelnek: $b=2^r5^s$. Ekkor a tizedesvessző után szereplő jegyek száma $k=\max(r,s)$, azaz $b\mid 10^k$, de $b\nmid 10^{k-1}$.

c) Az a/b racionális szám tizedestört-alakja akkor és csak akkor tiszta szakaszos, ha $(b,10)=1$. Ekkor a (legkisebb) szakasz hossza $o_b(10)$.

d) Az a/b racionális szám tizedestört-alakja akkor és csak akkor vegyes szakaszos, ha $(b,10)>1$, de a b-nek létezik a 2-től és 5-től különböző prímosztója is: $b=2^r5^st$, ahol $(t,10)=1$, $t>1$ és $k=\max(r,s)>0$. Ekkor a(z első) szakasz a tizedesvessző utáni $k+1$-edik jegyben kezdődik és hossza $o_t(10)$.

3.3. Primitív gyök

Mint láttuk, az Euler–Fermat-tételből következik, hogy bármely $(a,m)=1$ esetén $o_m(a)\le\varphi(m)$. Különösen fontos az az eset, amikor itt egyenlőség teljesül:

3.3.1 Definíció **D 3.3.1**

Egy g számot *primitív gyök*nek nevezünk modulo m, ha $o_m(g)=\varphi(m)$. ♣

A definícióból világos, hogy egy primitív gyök szükségképpen relatív prím az m modulushoz, továbbá egy redukált maradékosztálynak vagy minden eleme primitív gyök, vagy pedig egyetlen eleme sem az.

Példák:

P1 A 3 primitív gyök modulo 10, mert $o_{10}(3) = \varphi(10) = 4$.

P2 A 2 nem primitív gyök modulo 31, mert $o_{31}(2) = 5 < \varphi(31) = 30$.

P3 modulo 12 egyáltalán nem létezik primitív gyök: elég például a $\{\pm 1, \pm 5\}$ redukált maradékrendszer elemeinek a rendjét megvizsgálni, és itt az 1 rendje 1, a többi elemé 2, vagyis mindegyik rend kisebb, mint $\varphi(12) = 4$.

Amikor egy a számról (ahol $(a, m) = 1$) el akarjuk dönteni, hogy primitív gyök-e modulo m, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$ fennállását fölösleges ellenőrizni, hiszen ez az Euler–Fermat-tétel miatt biztosan igaz. Az $o_m(a) \mid \varphi(m)$ összefüggés alapján azt kell megvizsgálni, hogy a $\varphi(m)$ valamely $d < \varphi(m)$ osztójára teljesül-e $a^d \equiv 1 \pmod{m}$; ha van ilyen d, akkor a nem primitív gyök, ha nincs ilyen d, akkor pedig a primitív gyök. Könnyen látszik, hogy a $\varphi(m)$ osztói közül is elég a „maximálisakat" tekinteni, vagyis azokat, amelyek $\varphi(m)/q$ alakúak, ahol q prímszám.

A primitív gyökök alkalmazhatósága elsősorban az alábbi egyszerű tételben megfogalmazott tulajdonságon alapul:

3.3.2 Tétel **T 3.3.2**

Egy g szám akkor és csak akkor primitív gyök az m modulusra nézve, ha $1, g, g^2, \ldots, g^{\varphi(m)-1}$ redukált maradékrendszert alkotnak modulo m. ♣

Bizonyítás: Tegyük fel, hogy g primitív gyök, azaz $o_m(g) = \varphi(m)$. Ekkor a 3.2.2 Tétel (ii) állítása alapján $1, g, g^2, \ldots, g^{\varphi(m)-1}$ páronként inkongruensek modulo m, továbbá számuk $\varphi(m)$ és $(g, m) = 1$ miatt valamennyien relatív prímek m-hez. A 2.2.9 Tétel szerint így valóban redukált maradékrendszert alkotnak mod m.

A megfordításhoz tegyük fel, hogy a fenti g-hatványok redukált maradékrendszert alkotnak mod m. Ekkor $(g, m) = 1$, tehát $o_m(g)$ létezik és az Euler–Fermat-tétel szerint $o_m(g) \leq \varphi(m)$. Továbbá $g, g^2, \ldots, g^{\varphi(m)-1}$ egyike sem lehet kongruens a szintén a megadott redukált maradékrendszerben szereplő 1-gyel, tehát $o_m(g) = \varphi(m)$. ■

A következőkben azt vizsgáljuk meg, milyen m modulus esetén létezik primitív gyök. Megjegyezzük, hogy ezt csoportelméleti terminológiával úgy is

fogalmazhatjuk, hogy mely m esetén lesz a modulo m redukált maradékosztályok multiplikatív csoportja ciklikus.

Először azt igazoljuk, hogy prím modulus esetén mindig létezik primitív gyök:

3.3.3 Tétel **T 3.3.3**

Ha p prím, akkor modulo p létezik primitív gyök. ♣

A 3.3.3 Tétel általánosításaként megmutatható, hogy nemcsak a modulo p maradékosztályok körében, hanem bármely véges elemszámú testben található olyan elem, amelynek a hatványai előállítják a test összes nemnulla elemét.

A 3.3.3 Tételre két bizonyítást adunk. Emellett egy harmadik gondolatmenetet is vázolunk a 3.3.14 feladatban. Mindhárom bizonyítás — értelemszerű módosításokkal — alkalmas az imént említett általánosabb tétel igazolására is.

Első bizonyítás: Ha $p = 2$, akkor $g = 1$ (vagy bármely páratlan szám) primitív gyök.

Legyen $p > 2$ és $p - 1$ összes különböző prímosztója legyen $q_1, \dots, q_s$.

Tegyük fel indirekt, hogy nem létezik primitív gyök, azaz bármely $1 \le i \le p-1$ esetén $o_p(i) = d_i < p - 1$. Mivel $d_i \mid p - 1$, ezért van a $p - 1$-nek olyan q prímosztója, amelyre $d_i \mid (p-1)/q$. Ekkor $i^{(p-1)/q} \equiv 1 \pmod{p}$. Ez azt jelenti, hogy a redukált maradékrendszer bármely eleme gyöke az

$$f = \left(x^{(p-1)/q_1} - 1\right)\left(x^{(p-1)/q_2} - 1\right) \dots \left(x^{(p-1)/q_s} - 1\right) \tag{1}$$

polinommal képzett $f(x) \equiv 0 \pmod{p}$ kongruenciának. Továbbá $f(0) = (-1)^s \not\equiv 0 \pmod{p}$, tehát a kongruencia megoldásszáma pontosan $p - 1$.

Végezzük el (1)-ben a szorzásokat. Ekkor f olyan $\pm x^k$ tagok összegeként áll elő, ahol

a k kitevő különböző $(p-1)/q_j$-knek az (esetleg csak egytagú) összege, (2)

illetve $k = 0$. alkalmazzuk most a 3.1.3 Tétel első bizonyításában szereplő redukciós eljárást: írjunk x^p helyére x-et, amíg ez csak lehetséges. A keletkezett g polinom legfeljebb $p - 1$-edfokú és minden c-re $f(c) \equiv g(c) \pmod{p}$.

Ez azt jelenti, hogy a $g(x) \equiv 0 \pmod{p}$ kongruencia megoldásszáma is pontosan $p - 1$, és így a 3.1.2 Tétel szerint a g polinom modulo p vett foka pontosan $p - 1$ kell hogy legyen.

Ekkor g-ben szükségképpen szerepel x^{p-1}-es tag. A redukciós eljárás során ez a tag csak olyan, az f-ben előforduló x^k tag(ok)ból keletkezhetett, amely(ek)ben

$$\text{a } k \text{ kitevő } k = (p-1)t \text{ alakú, ahol } t > 0 \text{ egész,} \tag{3}$$

hiszen a ($p-1$-nél nagyobb) kitevőket mindig $p-1$-gyel csökkentettük.

A (2) és (3) összevetéséből kapjuk, hogy (mondjuk)

$$t = \frac{1}{q_1} + \frac{1}{q_2} + \ldots + \frac{1}{q_r}\,. \tag{4}$$

A (4) egyenlőséget $q_2 \ldots q_r$-rel beszorozva minden tag egész szám lesz, kivéve a jobb oldal első tagját, és így ellentmondásra jutottunk. ■

Második bizonyítás: Jelölje $h(d)$ az $1, 2, \ldots, p-1$ elemek közül azoknak az i-knek a számát, amelyekre $o_p(i) = d$. Ekkor nyilván $h(d) = 0$, ha $d \nmid p-1$, továbbá

$$\sum_{d \mid p-1} h(d) = p - 1\,. \tag{5}$$

Megmutatjuk, hogy bármely d-re

$$h(d) \le \varphi(d)\,. \tag{6}$$

Ha nincs d-edrendű elem, akkor (6) fennáll, hiszen $0 = h(d) < \varphi(d)$.

Feltehetjük tehát, hogy valamely a-ra $o_p(a) = d$. Ekkor az $a, a^2, \ldots, a^d$ elemek páronként inkongruensek modulo p, és $(a^t)^d = (a^d)^t \equiv 1 \pmod p$ miatt valamennyien gyökei az $x^d \equiv 1 \pmod p$ kongruenciának.

Mivel ennek a kongruenciának a megoldásszáma nem lehet d-nél nagyobb, ezért ha valamely c-re $c^d \equiv 1 \pmod p$ teljesül, akkor a c az $a, a^2, \ldots, a^d$ számok valamelyikével kongruens.

Minden d-edrendű szám is gyöke az $x^d \equiv 1 \pmod p$ kongruenciának, tehát minden d-edrendű szám is $a, a^2, \ldots, a^d$ valamelyikével kongruens. A 3.2.4b feladat szerint $o_p(a^j) = o_p(a) = d$ akkor és csak akkor teljesül, ha $(j, d) = 1$, ennélfogva az $a, a^2, \ldots, a^d$ számok között éppen $\varphi(d)$-nek a rendje lesz d, azaz $h(d) = \varphi(d)$. Ezzel (6)-ot beláttuk.

Felhasználva (5)-öt és (6)-ot, továbbá a 2.3.14 feladatban bizonyított $\sum_{d \mid p-1} \varphi(d) = p - 1$ egyenlőséget azt kapjuk, hogy

$$p - 1 = \sum_{d \mid p-1} h(d) \le \sum_{d \mid p-1} \varphi(d) = p - 1\,,$$

ami nyilván csak úgy teljesülhet, ha minden $d \mid p-1$-re $h(d) = \varphi(d)$.

Ezzel beláttuk, hogy egy mod p redukált maradékrendszerben a d-edrendű elemek száma $\varphi(d)$. Ezt speciálisan $d = p-1$-re alkalmazva adódik, hogy a primitív gyökök száma $\varphi(p-1)$ (tehát létezik primitív gyök). ■

Megjegyzés: A második bizonyításban (látszólag) erősebb állítást bizonyítottunk be: a primitív gyök létezésén túlmenően megkaptuk a (páronként inkongruens) primitív gyökök, sőt még általánosabban bármely adott d-re a d-edrendű elemek számát. Ez a „többleteredmény" azonban könnyen következik a primitív gyök (bármilyen módon igazolt) létezéséből a 3.3.2 Tétel és a 3.2.4b, illetve 3.2.4c feladat felhasználásával (lásd a 3.3.9 feladatot).

Az így adódó eredményeket fontosságuk miatt külön tételként is megfogalmazzuk:

3.3.4 Tétel **T 3.3.4**

Legyen a modulus egy p prímszám.

(i) Egy primitív gyök i-edik hatványa akkor és csak akkor primitív gyök, ha $(i, p-1) = 1$.

(ii) A páronként inkongruens primitív gyökök száma $\varphi(p-1)$.

(iii) Általánosan is igaz, hogy ha $d \mid p-1$, akkor egy mod p redukált maradékrendszer elemei között a d-edrendű elemek száma $\varphi(d)$. ♣

A következő tételben pontosan meghatározzuk, mely m modulusokra létezik primitív gyök:

3.3.5 Tétel **T 3.3.5**

Az $m > 1$ modulusra nézve akkor és csak akkor létezik primitív gyök, ha $m = p^\alpha, 2p^\alpha, 2$ vagy 4, ahol $p > 2$ prím és $\alpha > 0$. ♣

Bizonyítás: Az $m = p$ és $m = 2$ esetet a 3.3.3 Tétel tartalmazza, ha pedig $m = 4$, akkor $g = 3$ primitív gyök. A többi esetre a bizonyítást az alábbi lépésekben végezzük.

(L1) modulo p^2 létezik primitív gyök.

(L2) Ha $\alpha > 2$, akkor modulo p^α létezik primitív gyök.

(L3) modulo $2p^\alpha$ létezik primitív gyök ($\alpha > 0$).

(N1) Ha m osztható 4-gyel és van páratlan prímosztója, vagy ha m-nek van (legalább) két különböző páratlan prímosztója, akkor nem létezik primitív gyök modulo m.

(N2) Ha $m = 2^\alpha$, ahol $\alpha > 2$, akkor nem létezik primitív gyök modulo m.

(L1) Legyen g primitív gyök modulo p. Megmutatjuk, hogy g és $g+p$ közül legalább az egyik primitív gyök lesz modulo p^2 is.

Egyrészt

$$o_{p^2}(g) \mid \varphi(p^2)\,,$$

másrészt a 3.2.13a feladat alapján

$$o_p(g) \mid o_{p^2}(g).$$

A $\varphi(p^2) = p(p-1)$ és $o_p(g) = p-1$ összefüggéseket beírva azt kapjuk, hogy

$$p-1 \mid o_{p^2}(g) \qquad \text{és} \qquad o_{p^2}(g) \mid p(p-1)\,.$$

Így $o_{p^2}(g) = p-1$ vagy $o_{p^2}(g) = p(p-1)$.

A második esetben g (definíció szerint) primitív gyök modulo p^2.

Ha $o_{p^2}(g) = p-1$, akkor megmutatjuk, hogy $g+p$ primitív gyök mod p^2.

Az előző gondolatmenetet g helyett $g+p$-re megismételve adódik, hogy $o_{p^2}(g+p)$ értéke is csak $p-1$ vagy $p(p-1)$ lehet. Így elég azt igazolni, hogy $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$. A hatványozást elvégezve kapjuk, hogy

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} + \binom{p-1}{2} p^2 g^{p-2} + \dots$$

A jobb oldalon az első tag a feltételezésünk szerint 1-gyel kongruens mod p^2, továbbá a harmadiktól kezdve minden tag osztható p^2-tel. Így

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2}\,.$$

(L2) Bebizonyítjuk, hogy ha g primitív gyök modulo p^2, akkor primitív gyök modulo p^α is, tetszőleges $\alpha > 2$-re. Az (L1) részben látott gondolatmenethez hasonlóan elég azt megmutatni, hogy

$$g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}\,.$$

Ezt a következő formában igazoljuk:

$$g^{p^{\alpha-2}(p-1)} = 1 + t_\alpha p^{\alpha-1}, \qquad \text{ahol} \qquad p \nmid t_\alpha\,. \tag{7}$$

A (7) összefüggést α szerinti teljes indukcióval bizonyítjuk.

Az $\alpha = 2$ esetben valóban $g^{p-1} = 1 + t_2 p$ (ez a kis Fermat-tétel), és itt $p \nmid t_2$, mert g primitív gyök modulo p^2.

Tegyük fel most, hogy (7) teljesül valamely $\alpha(\geq 2)$ esetén; belátjuk, hogy ekkor (α helyett) $\alpha+1$-re is fennáll. Emeljük (7)-et p-edik hatványra:

$$g^{p^{\alpha-1}(p-1)} = (1+t_\alpha p^{\alpha-1})^p = 1 + \binom{p}{1} t_\alpha p^{\alpha-1} + \binom{p}{2}(t_\alpha p^{\alpha-1})^2 + \dots \qquad (8)$$

Itt a harmadik tag osztható a p-nek $1+2(\alpha-1) \geq \alpha+1$-edik hatványával, a további tagokban pedig szintén legalább ekkora a p kitevője. Ennélfogva

$$g^{p^{\alpha-1}(p-1)} = 1 + t_\alpha p^\alpha + s p^{\alpha+1} = 1 + t_{\alpha+1} p^\alpha, \qquad \text{ahol} \qquad p \nmid t_{\alpha+1}\,,$$

azaz (7) valóban fennáll $\alpha+1$-re is.

(L3) Legyen g primitív gyök modulo p^α. Jelöljük h-val a g és $g+p^\alpha$ közül azt, amelyik páratlan; belátjuk, hogy h primitív gyök modulo $2p^\alpha$.

Mivel bármely i-re $h^i \equiv 1 \pmod 2$, ezért

$$h^r \equiv 1 \pmod{p^\alpha} \iff h^r \equiv 1 \pmod{2p^\alpha}.$$

Ez azt jelenti, hogy

$$o_{2p^\alpha}(h) = o_{p^\alpha}(h) = \varphi(p^\alpha) = \varphi(2p^\alpha)\,.$$

(N1) Megmutatjuk, hogy tetszőleges $(a,m)=1$ esetén található olyan $0<r<\varphi(m)$, amelyre $a^r \equiv 1 \pmod m$, és így a nem lehet primitív gyök.

A szóban forgó m-ek felírhatók $m=uv$ alakban, ahol $(u,v)=1$ és $u>2, v>2$. Igazolni fogjuk, hogy $r=[\varphi(u),\varphi(v)]$ megfelel.

Az $u>2$, $v>2$ feltétel miatt $\varphi(u)$ és $\varphi(v)$ páros (lásd a 2.3.1 feladatot), tehát $\big(\varphi(u),\varphi(v)\big) \geq 2$. Ebből következik, hogy

$$r = [\varphi(u),\varphi(v)] \leq \frac{\varphi(u)\varphi(v)}{2} = \frac{\varphi(m)}{2}\,.$$

Emellett, $\varphi(u) \mid r$ miatt $a^r \equiv 1 \pmod u$, és ugyanez érvényes mod v is, ezért $a^r \equiv 1 \pmod{[u,v]}$, azaz $\pmod m$ is teljesül.

(N2) Megmutatjuk, hogy ha $\alpha \geq 3$, akkor bármely páratlan a-ra

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}, \quad \text{azaz} \quad o_{2^\alpha}(a) \leq 2^{\alpha-2} < \varphi(2^\alpha)\,. \qquad (8)$$

Az α szerinti teljes indukcióval bizonyítunk. Ha $\alpha=3$, akkor valóban

$$2^3 = 8 \mid a^2-1 = (a-1)(a+1).$$

Tegyük most fel, hogy (8) igaz valamely α-ra; belátjuk, hogy ekkor $\alpha+1$-re is fennáll. Az

$$a^{2^{\alpha-1}} - 1 = \left(a^{2^{\alpha-2}} - 1\right)\left(a^{2^{\alpha-2}} + 1\right)$$

szorzatban az első tényező az indukciós feltevés szerint osztható 2^{α}-val, a második tényező osztható 2-vel, így a szorzat valóban osztható $2^{\alpha+1}$-gyel. ■

Feladatok

3.3.1 Határozzuk meg az összes primitív gyököt modulo m, ha m értéke
a) 7; b) 10; c) 18.

3.3.2 Adjunk meg egy olyan számot, amely egyszerre primitív gyök mod 11 és mod 14 is.

3.3.3 Adjunk meg
a) egy primitív gyököt mod 625;
b) egy olyan primitív gyököt mod 5, amely nem primitív gyök mod 625.

3.3.4 Melyek igazak az alábbi állítások közül?
a) Ha g primitív gyök mod 11, akkor g primitív gyök mod 22.
b) Ha g primitív gyök mod 22, akkor g primitív gyök mod 11.
c) Ha g primitív gyök mod m, akkor g^3 is primitív gyök mod m.
d) Ha g^3 primitív gyök mod m, akkor g is primitív gyök mod m.
e) Ha g primitív gyök mod m, akkor $g^{2\varphi(m)-1}$ is primitív gyök mod m.
f) Ha $(a, 34) = 1$ és $a^8 \not\equiv 1 \pmod{34}$, akkor a primitív gyök mod 34.
g) Ha $(a, 25) = 1$ és $a^{10} \not\equiv 1 \pmod{25}$, akkor a primitív gyök mod 25.

3.3.5 Legyen a modulus egy (tetszőleges, de rögzített) $p > 2$ prímszám.
a) Mutassuk meg, hogy két primitív gyök szorzata sohasem primitív gyök.
b) Bizonyítsuk be, hogy létezik három olyan primitív gyök, amelyeknek a szorzata is primitív gyök.
c) Mely p prímek esetén igaz, hogy bármely három primitív gyök szorzata is primitív gyök?

3.3.6 Adjunk új bizonyítást a Wilson-tételre a primitív gyök felhasználásával.

3.3.7 Legyen $p > 2$ prím. Milyen maradékot ad az $1^k + 2^k + \ldots + (p-1)^k$ összeg p-vel osztva?

3.3.8 Legyen $p > 2$ prím. Milyen maradékot ad p-vel osztva az összes (páronként inkongruens) primitív gyök szorzata? (A primitív gyökök összegére vonatkozóan lásd a 6.5.9c feladatot.)

3.3.9

a) Legyen p prím, $d \mid p-1$, g primitív gyök mod p és $(a,p)=1$. Bizonyítsuk be, hogy

$$o_p(a)=d \iff a \equiv g^j \pmod{p}, \text{ ahol } j=\frac{t(p-1)}{d} \text{ és } (t,d)=1.$$

b) Határozzuk meg az a) rész felhasználásával egy modulo p redukált maradékrendszerben a d-edrendű elemek számát.

M*3.3.10 Legyen $p>2$ prím és $(a,p)=(b,p)=1$. Bizonyítsuk be, hogy $o_p(a)=o_p(b)$ akkor és csak akkor teljesül, ha van olyan r és s pozitív egész, amelyre $a \equiv b^r \pmod{p}$ és $b \equiv a^s \pmod{p}$.

3.3.11 Hogyan általánosítható a 3.3.4 Tétel olyan összetett modulusra, amelyre nézve létezik primitív gyök?

3.3.12 Legyen $m=2^\alpha$, ahol $\alpha \geq 3$. Bizonyítsuk be az alábbi állításokat:

a) $o_m(5)=2^{\alpha-2}$.

b) Az $5^x \equiv -1 \pmod{m}$ kongruencia nem oldható meg.

c) A $\pm 5^k$, $0 \leq k < \varphi(m)/2$ számok redukált maradékrendszert alkotnak modulo m.

Megjegyzés: A 3.3.5 Tételből tudjuk, hogy $m=2^\alpha$, $\alpha \geq 3$ esetén nem létezik primitív gyök. A feladat c) része — kissé pongyolán fogalmazva — azt fejezi ki, hogy az 5 „majdnem" primitív gyök ezekre a modulusokra.

*3.3.13 Legyen az $m>1$ páratlan szám kanonikus alakja $m=p_1^{\alpha_1}\dots p_r^{\alpha_r}$. Mutassuk meg, hogy léteznek olyan $u_1,\dots,u_r$ egészek, hogy az

$$u_1^{k_1}\dots u_r^{k_r}, \qquad 0 \leq k_i < \varphi\big(p_i^{\alpha_i}\big), \qquad i=1,2,\dots,r$$

számok redukált maradékrendszert alkotnak modulo m. Fogalmazzuk meg és bizonyítsuk be a megfelelő állítást páros m-ekre is.

3.3.14 Legyen $p>2$ prím. Adjunk új bizonyítást modulo p primitív gyök létezésére az alábbi gondolatmenet alapján.

a) Mutassuk meg, hogy ha az f egész együtthatós polinomra $f \mid x^{p-1}-1$, akkor az $f(x) \equiv 0 \pmod{p}$ megoldásszáma pontosan az f fokszámával egyenlő.

b) Tegyük fel, hogy $q^\beta \mid p-1$, ahol q prím és $\beta>0$. Bizonyítsuk be, hogy az

$$f_1=x^{q^\beta}-1 \quad \text{és} \quad f_2=x^{q^{\beta-1}}-1$$

polinomokra az $f_1(x) \equiv 0 \pmod{p}$, illetve $f_2(x) \equiv 0 \pmod{p}$ kongruenciák megoldásszáma pontosan q^β, illetve $q^{\beta-1}$.

c) A b) rész jelöléseit és eredményét használva mutassuk meg, hogy van olyan c, amelyre $o_p(c) = q^\beta$.

d) A c) rész és a 3.2.15a feladat felhasználásával igazoljuk, hogy minden $d \mid p-1$ esetén létezik d-edrendű elem modulo p.

3.4. Diszkrét logaritmus (index)

Ebben és a következő pontban feltesszük, hogy a modulus egy p prímszám. Megjegyezzük, hogy az itt szereplő fogalmak és eredmények tetszőleges olyan modulusra is átvihetők, amelyekre nézve létezik primitív gyök.

Legyen g primitív gyök mod p. A 3.3.2 Tétel szerint az $1, g, \ldots, g^{p-2}$ számok redukált maradékrendszert alkotnak mod p, és így bármely $(a,p)=1$ esetén pontosan egy olyan $0 \le k \le p-2$ kitevő létezik, amelyre $a \equiv g^k \pmod{p}$. Mindez lehetővé teszi a „logaritmus" bevezetését:

3.4.1 Definíció **D 3.4.1**

Legyen g primitív gyök mod p és $(a,p)=1$. Ekkor az a-nak a g alapú *diszkrét logaritmus*án vagy *index*én azt a $0 \le k \le p-2$ számot értjük, amelyre $a \equiv g^k \pmod{p}$. ♣

Jelölés: $\operatorname{ind}_{p,g}(a)$. Mivel a p modulus általában rögzített, ezért legtöbbször az erre utaló jelzést elhagyjuk: $\operatorname{ind}_g a$. Ha a g primitív gyök is egyértelmű, akkor simán $\operatorname{ind} a$-t írunk.

Az előzetes megjegyzés szerint $(a,p)=1$ esetén $\operatorname{ind}_g a$ létezik és egyértelmű. Egy a szám diszkrét logaritmusa természetesen függ attól, hogy melyik g primitív gyök szerint vesszük.

Ha $a \equiv b \pmod{p}$, akkor nyilván $\operatorname{ind}_g a = \operatorname{ind}_g b$, tehát (rögzített g mellett) egy redukált maradékosztály minden elemének ugyanaz a diszkrét logaritmusa.

Sokszor fel fogjuk használni a

$$g^s \equiv g^t \pmod{p} \iff s \equiv t \pmod{p-1}$$

összefüggést (amely a 3.2.2 Tétel (ii) állításából következik $m=p$, $a=g$ és $o_p(g)=p-1$ szereposztással).

Ennek megfelelően, ha az összes olyan $j \geq 0$ egészt keressük, amelyre $g^j \equiv a \pmod{p}$, akkor ezek a j értékek éppen egy modulo $p-1$ maradékosztály nemnegatív elemei lesznek. Más megfogalmazásban:

$$g^j \equiv a \pmod{p} \iff j \equiv \operatorname{ind}_g a \pmod{p-1}.$$

(Szokás ennek alapján a diszkrét logaritmust úgy is értelmezni, hogy ezt a modulo $p-1$ maradékosztályt nevezik az a elem g alapú diszkrét logaritmusának.)

A diszkrét logaritmusra is érvényesek a logaritmusazonosságok megfelelői (lásd a 3.4.3–3.4.4 feladatokat).

A diszkrét logaritmus segítségével oldjuk meg a következő pontban a modulo p „gyökvonás" problémáját, emellett egy kriptográfiai alkalmazást is tárgyalunk az 5.8.6 feladatban.

Illusztrációként mellékelünk egy „exponenciális" és egy „logaritmus"-táblázatot (indextáblázatot), amely a $p = 13$ modulusra és a $g = 2$ primitív gyökre vonatkozik.

j	0	1	2	3	4	5	6	7	8	9	10	11
$2^j \pmod{13}$	1	2	4	8	3	6	12	11	9	5	10	7

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 a$	0	1	4	2	9	5	11	3	8	10	7	6

Feladatok

Valamennyi feladatban a g és h primitív gyökök egy $p > 2$ prím modulusra vonatkoznak, a és b relatív prímek p-hez, és ha külön nem jelezzük, akkor g alapú indexről van szó.

3.4.1 Mely p prímekre lesz $\operatorname{ind}_{p,7}(2) = 3$?

3.4.2 Számítsuk ki az alábbi diszkrét logaritmusokat:

a) $\operatorname{ind}_g 1$; b) $\operatorname{ind}_g(-1)$; c) $\operatorname{ind}_g(-g)$.

3.4.3 Bizonyítsuk be az alábbi „logaritmusazonosságokat":

a) $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}$;

b) $\operatorname{ind}(a^k) \equiv k \cdot \operatorname{ind} a \pmod{p-1}$.

3.4.4 Bizonyítsuk be, hogy a g alapú indexről a h alapú indexre az alábbi („szokásos") módon lehet áttérni:

a) $\operatorname{ind}_g h \cdot \operatorname{ind}_h g \equiv 1 \pmod{p-1}$;

b) $\operatorname{ind}_h a \equiv \operatorname{ind}_h g \cdot \operatorname{ind}_g a \pmod{p-1}$.

3.4.5 Melyik az a legkisebb s pozitív egész, amelyre $p-1 \mid s \cdot \operatorname{ind} a$?

3.4.6 Bizonyítsuk be, hogy a akkor és csak akkor primitív gyök mod p, ha $(\operatorname{ind}_g a\,,\ p-1) = 1$.

3.4.7 Bizonyítsuk be az alábbi állításokat.

a) $(\operatorname{ind}_g a\,,\ p-1) = 1 \iff (\operatorname{ind}_h a\,,\ p-1) = 1$.

b) $(\operatorname{ind}_g a\,,\ p-1) = (\operatorname{ind}_h a\,,\ p-1)$.

3.4.8 Legyenek a, b, c tetszőleges primitív gyökök modulo p. Igazoljuk, hogy ekkor

$$a^{\operatorname{ind}_b c}$$

is primitív gyök mod p.

M*3.4.9 Mutassuk meg, hogy $o_p(a) = o_p(b)$ akkor és csak akkor teljesül, ha van olyan g és h primitív gyök, amelyre $\operatorname{ind}_g a = \operatorname{ind}_h b$.

3.4.10 Keressük meg az alábbi prímekhez a legkisebb pozitív primitív gyököt és készítsünk indextáblázatot: a) 7; b) 11; c) 17.

*3.4.11 Bizonyítsuk be, hogy bármely p prímhez és a egészhez végtelen sok olyan k pozitív egész található, amelyre $a \equiv k^k \pmod{p}$.

3.5. Binom kongruenciák

A pozitív valós számok körében a gyökvonás elvégzéséhez a szám logaritmusát elosztjuk a gyökkitevővel, és ezzel megkapjuk a gyök logaritmusát (így vonnak gyököt a kalkulátorok is). Hasonló módon használható a diszkrét logaritmus is a modulo p gyökvonáshoz, azaz az $x^k \equiv a \pmod{p}$ kongruencia megoldásához (ahol p prímszám). Az ilyen kongruenciákat kéttagú vagy *binom* kongruenciáknak nevezzük. Az általános $cx^k \equiv d \pmod{p}$ binom kongruencia, ahol $c \not\equiv 0 \pmod{p}$, szintén ilyen $x^k \equiv a \pmod{p}$ alakra hozható: a megfelelő a értéket a $cy \equiv d \pmod{p}$ lineáris kongruencia (mod p egyértelmű) megoldása szolgáltatja.

Az $(a, p) \neq 1$ esetben $a \equiv 0 \pmod{p}$, azaz az $x^k \equiv 0 \pmod{p}$ kongruenciáról van szó; ennek könnyen láthatóan $x \equiv 0 \pmod{p}$ az egyetlen megoldása.

Így a továbbiakban feltesszük, hogy $(a, p) = 1$.

3.5.1 Tétel **T 3.5.1**

Legyen p prím és $(a,p)=1$. Az

$$x^k \equiv a \pmod{p} \tag{1}$$

kongruencia akkor és csak akkor oldható meg, ha

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}\,. \tag{2}$$

Megoldhatóság esetén a (páronként inkongruens) megoldások száma $(k,p-1)$. A (2) feltétel ekvivalens azzal, hogy

$$(k,p-1) \mid \operatorname{ind}_g a \tag{3}$$

teljesül, ahol g egy tetszőleges primitív gyököt jelent modulo p. ♣

Bizonyítás: A g primitív gyök szerinti diszkrét logaritmust fogjuk használni.

Keressük a megoldást $x \equiv g^{\operatorname{ind} x} \pmod{p}$ alakban. Ekkor az (1) kongruencia átírható a

$$g^{k\,\cdot \operatorname{ind} x} \equiv g^{\operatorname{ind} a} \pmod{p}$$

alakba, amely a már sokszor használt $g^s \equiv g^t \pmod{p} \iff s \equiv t \pmod{p-1}$ összefüggés alapján tovább ekvivalens

$$k \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1} \tag{4}$$

teljesülésével.

A (4) az $\operatorname{ind} x$-re nézve egy lineáris kongruencia, amely a 2.5.3 Tétel szerint akkor és csak akkor oldható meg, ha (3) teljesül, tehát ugyanez az (1) kongruencia megoldhatóságának a szükséges és elégséges feltétele is.

A (4) kongruencia modulo $p-1$ páronként inkongruens megoldásainak az (1) kongruencia modulo p páronként inkongruens megoldásai felelnek meg és viszont, tehát a két kongruenciának ugyanannyi a megoldásszáma: a 2.5.4 Tétel alapján ez $(k,p-1)$.

Végül megmutatjuk a (2) és (3) feltételek ekvivalenciáját. Mivel

$$a^{\frac{p-1}{(k,p-1)}} \equiv \left(g^{\operatorname{ind} a}\right)^{\frac{p-1}{(k,p-1)}} = g^{(p-1)\frac{\operatorname{ind} a}{(k,p-1)}} \pmod{p}\,, \tag{5}$$

ezért $a^{(p-1)/(k,p-1)} \equiv 1 \pmod{p}$ pontosan akkor teljesül, ha (5) utolsó tagjában a g kitevője a $p-1$-nek egész számú többszöröse, azaz ha $(k,p-1) \mid \operatorname{ind} a$. ■

Megjegyzések: 1. A tétel bizonyításából egyúttal megoldási módszert is kaptunk, feltéve, hogy rendelkezésünkre áll egy indextáblázat.

2. A (3)-ban szereplő $\operatorname{ind}_g a$ érték természetesen más és más (lehet), attól függően, hogy melyik g primitív gyököt választottuk. Mivel azonban az (1) kongruencia megoldhatósága nem függ g-től, ezért a (3)-ban megadott feltétel is független a g-től: vagy minden primitív gyökre teljesül, vagy pedig egyikre sem. (Mindez egyébként a 3.4.7b feladatból is következik.)

Példa: Oldjuk meg az $5x^{22} \equiv 6 \pmod{13}$ kongruenciát.

Az $5y \equiv 6 \pmod{13}$ kongruencia (egyetlen) megoldása $y \equiv 9 \pmod{13}$. Ennek megfelelően az $x^{22} \equiv 9 \pmod{13}$ kongruenciát kell megoldanunk.

A 3.5.1 Tétel bizonyításában láttuk, hogy ez a kongruencia a

$$22 \cdot \operatorname{ind} x \equiv \operatorname{ind} 9 \pmod{12}$$

kongruenciával ekvivalens.

A 13 modulusra nézve a 2 primitív gyök, és a megfelelő „exponenciális" és „logaritmus"-táblázatok a 3.4 pont végén találhatók. Innen $\operatorname{ind} 9 = 8$.

Az így nyert

$$22 \cdot \operatorname{ind} x \equiv 8 \pmod{12}$$

lineáris kongruencia $(22, 12) \mid 8$ miatt megoldható és a (páronként inkongruens) megoldások száma $(22, 12) = 2$. A megoldások:

$$\operatorname{ind} x \equiv 2 \pmod{12} \qquad \text{és} \qquad \operatorname{ind} x \equiv 8 \pmod{12}.$$

Az „exponenciális" táblázatot használva ebből

$$x \equiv 4 \pmod{13} \qquad \text{és} \qquad x \equiv 9 \pmod{13}$$

adódik.

Megjegyezzük, hogy nem szükséges az $5y \equiv 6 \pmod{13}$ kongruenciát külön megoldani, hanem rögtön áttérhetünk az indexre:

$$\operatorname{ind} 5 + 22 \cdot \operatorname{ind} x \equiv \operatorname{ind} 6 \pmod{12}, \quad \text{azaz} \quad 9 + 22 \cdot \operatorname{ind} x \equiv 5 \pmod{12}.$$

Ily módon egy lépésben jutottunk el a $22 \cdot \operatorname{ind} x \equiv 8 \pmod{12}$ lineáris kongruenciához.

3.5.2 Definíció **D 3.5.2**

Legyen p prím és $(a,p)=1$. Az a számot (a p-re nézve) k-adik *hatványmaradék*nak nevezzük, ha az $x^k \equiv a \pmod p$ kongruencia megoldható, és k-adik *hatvány-nemmaradék*nak nevezzük, ha az $x^k \equiv a \pmod p$ kongruencia nem oldható meg. ♣

3.5.3 Tétel **T 3.5.3**

Legyen p prím és $(a,p)=1$. Az a szám (a p-re nézve) akkor és csak akkor k-adik hatványmaradék, ha

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod p\,, \qquad \text{illetve} \qquad (k,p-1) \mid \operatorname{ind}_g a\,,$$

ahol g tetszőleges primitív gyök modulo p.
A (páronként inkongruens) k-adik hatványmaradékok száma $(p-1)/(k,p-1)$. ♣

Bizonyítás: Az első állítás a 3.5.1 Tétel (egy részének) átfogalmazása.

A második állítás abból következik, hogy a k-adik hatványmaradékok éppen a

$$z^{\frac{(p-1)}{(k,p-1)}} \equiv 1 \pmod p$$

kongruencia megoldásai, és ennek a kongruenciának a megoldásszáma szintén a 3.5.1 Tétel szerint

$$\left(\frac{p-1}{(k,p-1)}\,,\,p-1\right) = \frac{p-1}{(k,p-1)}\,. \quad \blacksquare$$

Feladatok Valamennyi feladatban a modulus egy $p>2$ prím.

3.5.1 Oldjuk meg az alábbi kongruenciákat. (A 11, 13 és 17 modulusok esetén használjuk fel a 3.4 pont végén, illetve a 3.4.10 feladat útmutatásánál szereplő indextáblázatokat is.)

a) $3x^{50} \equiv 2 \pmod{101}$.

b) $x^{99} \equiv 2 \pmod{101}$.

c) $x^{46} \equiv 50 \pmod{23}$.

d) $5x^{14} \equiv 14x^2 \pmod{17}$.

e) $4x^7 + 7x^4 \equiv 0 \pmod{13}$.

f) $4x^{27} + 5x^{20} + 7x^{17} + 9x^8 + 3 \equiv 0 \pmod{11}$.

3.5.2 Határozzuk meg az alábbi kongruenciák megoldásszámát.

a) $(x^{30}-1)(x^{45}-1) \equiv 0 \pmod{73}$.

b) $1 + x + x^2 + \ldots + x^k \equiv 0 \pmod{31}$.

3.5.3 Mely a számokra oldható meg az

$$1 + x + \ldots + x^{p-2} \equiv a \pmod{p}$$

kongruencia?

3.5.4 Mutassuk meg, hogy ha g primitív gyök, akkor az $x^k \equiv g \pmod{p}$ kongruenciának legfeljebb egy megoldása van.

3.5.5 Jelölje $x^k \equiv 1 \pmod{p}$ összes (páronként inkongruens) megoldását $b_1, \ldots, b_r$. Legyen $(a,p) = 1$ és az $x^k \equiv a \pmod{p}$ kongruencia egy megoldása c. Hogyan kaphatjuk meg az $x^k \equiv a \pmod{p}$ kongruencia összes megoldását?

3.5.6 Határozzuk meg az

a) $p-1$-edik; b) $(p-1)/2$-edik

hatványmaradékokat mod p.

3.5.7 Melyek azok a k értékek, amelyekre a k-adik gyökvonás modulo p egyértelműen elvégezhető, azaz amelyekre az $x^k \equiv a \pmod{p}$ kongruenciának bármely a esetén pontosan egy megoldása van?

3.5.8 Mely prímekre létezik teljes maradékrendszer csupa köbszámból?

3.5.9 Bizonyítsuk be, hogy

a) két k-adik hatványmaradék szorzata mindig k-adik hatványmaradék;

b) egy k-adik hatványmaradék és egy k-adik hatvány-nemmaradék szorzata mindig k-adik hatvány-nemmaradék.

3.5.10 Mi a szükséges és elégséges feltétele annak, hogy létezzen k-adik hatvány-nemmaradék és bármely két k-adik hatvány-nemmaradék szorzata k-adik hatványmaradék legyen?

3.5.11 Milyen maradékot ad p-vel osztva az összes (páronként inkongruens) k-adik hatványmaradék a) összege; b) szorzata?

M 3.5.12 Bizonyítsuk be, hogy a akkor és csak akkor lesz egyszerre 20-adik és 50-edik hatványmaradék modulo p, ha 100-adik hatványmaradék modulo p. Általánosítsuk a feladatot.

3.6. Chevalley-tétel, Kőnig–Rados-tétel

Ebben a pontban prím modulusú kongruenciákra vonatkozó két nevezetes tételt tárgyalunk. Elsőként olyan

$$f_i(x_1, x_2, \ldots, x_t) \equiv 0 \pmod{p}, \qquad i = 1, 2, \ldots, k \tag{1}$$

kongruenciarendszerekkel foglalkozunk, ahol p prím, $k \geq 1$ és

$$f_i(x_1, x_2, \ldots, x_t), \qquad i = 1, 2, \ldots, k$$

olyan egész együtthatós, t-változós polinomok, amelyek konstans tagja 0, azaz

$$f_i(0, 0, \ldots, 0) = 0, \qquad i = 1, 2, \ldots, k. \tag{2}$$

A (2) feltételből azonnal kapjuk, hogy $x_1 \equiv x_2 \equiv \ldots \equiv x_t \equiv 0 \pmod{p}$ kielégíti az (1) kongruenciarendszert, ezt a továbbiakban triviális megoldásnak nevezzük.

Chevalley tétele arra vonatkozik, hogy az f_i polinomok fokszámára tett alkalmas kikötés esetén az (1) rendszernek létezik nemtriviális megoldása is. (Egy $x_1^{n_1} \ldots x_t^{n_t}$ tag fokszáma $n_1 + \ldots + n_t$, egy polinom fokszáma pedig a benne szereplő nemnulla együtthatós tagok fokszámának a maximuma.)

3.6.1 Tétel (Chevalley tétele) **T 3.6.1**

Ha az (1)-ben szereplő f_i polinomokra teljesül (2) és fokszámaik összege kisebb a változók számánál, azaz

$$\sum_{i=1}^{k} \deg f_i < t, \tag{3}$$

akkor (1)-nek létezik nemtriviális megoldása. ♣

Példák: Az

$$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 \equiv 0 \pmod{23}$$
$$x_1^3 + 2x_1x_2 + 3x_2x_3 + 4x_3x_4^2 + 5x_5^2 \equiv 0 \pmod{23}$$

kongruenciarendszernek létezik nemtriviális megoldása, azaz olyan, ahol nem mindegyik x_i osztható 23-mal. (Itt $k = 2$ és $5 = t > 1 + 3 = \deg f_1 + \deg f_2$.)

A 3.6.1 Tételt $k = 1$, azaz egyetlen polinom esetén is jól alkalmazhatjuk: pl. bármely p prím esetén a

$$p \mid x_1^3 + 3x_2^3 + 5x_3^3 + 7x_4^3 + 9x_1x_2 + 11x_3x_4$$

oszthatóság úgy is megvalósul, hogy legalább az egyik x_i nem osztható p-vel. (Most $t = 4$ és $\deg f = 3$.)

Bizonyítás: Tegyük fel indirekt, hogy a kongruenciarendszernek csak triviális megoldása van.

Vezessük be az alábbi két t-változós polinomot:

$$F(x_1, x_2, \ldots, x_t) = \prod_{i=1}^{k} \left(1 - f_i^{p-1}(x_1, x_2, \ldots, x_t)\right),$$

$$G(x_1, x_2, \ldots, x_t) = \prod_{j=1}^{t} (1 - x_j^{p-1}).$$

A kis Fermat-tétel szerint

$$c_j \not\equiv 0 \pmod{p} \Longrightarrow c_j^{p-1} \equiv 1 \pmod{p}.$$

Ebből azonnal következik, hogy G-be tetszőleges $c_1, \ldots, c_t$ egész számokat behelyettesítve

$$G(c_1, c_2, \ldots, c_t) \equiv \begin{cases} 1 \pmod{p}, & \text{ha } c_1 \equiv \ldots \equiv c_t \equiv 0 \pmod{p}; \\ 0 \pmod{p}, & \text{egyébként.} \end{cases} \tag{4}$$

Megmutatjuk, hogy ugyanez érvényes F-re is, azaz

$$F(c_1, c_2, \ldots, c_t) \equiv \begin{cases} 1 \pmod{p}, & \text{ha } c_1 \equiv \ldots \equiv c_t \equiv 0 \pmod{p}; \\ 0 \pmod{p}, & \text{egyébként.} \end{cases} \tag{5}$$

Legyen először

$$c_1 \equiv \ldots \equiv c_t \equiv 0 \pmod{p}.$$

Ekkor (2) alapján minden i-re

$$f(c_1, \ldots, c_t) \equiv 0 \pmod{p},$$

azaz $F(c_1, \ldots, c_t)$ minden tényezője és így maga $F(c_1, \ldots, c_t)$ is 1-gyel kongruens modulo p.

Vegyük most a másik esetet, azaz amikor a $c_1, \ldots, c_t$ számok közül legalább az egyik nem osztható p-vel. Mivel az indirekt feltevés szerint (1)-nek csak triviális megoldása létezik, ezért $c_1, \ldots, c_t$ nem megoldás, vagyis legalább egy i-re

$$f_i(c_1, \ldots, c_t) \not\equiv 0 \pmod{p}.$$

Ebből ismét a kis Fermat-tétel alapján következik, hogy

$$f_i^{p-1}(c_1, c_2, \ldots, c_t) \equiv 1 \pmod{p}.$$

Ez azt jelenti, hogy $F(c_1, \ldots, c_t)$ egyik tényezője, és így maga $F(c_1, \ldots, c_t)$ is osztható p-vel. Ezzel (5) igazolását befejeztük.

A (4) és (5) képletek alapján tetszőleges $c_1, \ldots, c_t$ egész számokra

$$F(c_1, \ldots, c_t) \equiv G(c_1, \ldots, c_t) \pmod{p}. \tag{6}$$

A továbbiakban valamennyi polinomot a modulo p test feletti t-változós polinomnak fogunk tekinteni.

Ekkor (6) azt fejezi ki, hogy az F és G polinomok minden helyettesítési értéke megegyezik (vagyis F-hez és G-hez ugyanaz a polinomfüggvény tartozik; véges test esetén azonban ebből maguknak a polinomoknak, azaz az együtthatóknak az egyenlősége nem következik).

Nevezzük egy H polinom redukált alakjának azt a H^* polinomot, amelyet H-ból úgy kapunk, hogy H-ban mindenhol x_i^p helyére x_i-t írunk, ameddig csak lehetséges. Nyilván H^* minden tagjában bármelyik x_i kitevője legfeljebb $p-1$, továbbá H és H^* minden helyettesítési értéke megegyezik. A változók száma szerinti teljes indukcióval könnyen megmutatható, hogy ha a H és K polinomok minden helyettesítési értéke megegyezik, akkor a H^* és K^* polinomok (formálisan is) egyenlők (azaz H^*-nak és K^*-nak ugyanazok a megfelelő együtthatói).

Láttuk, hogy az F és G polinomok minden helyettesítési értéke megegyezik, ezért az előzőek szerint ekkor az F^* és G^* polinomok egyenlők. Így $\deg G^* = \deg F^*$ is teljesül. Azonban $G = G^*$ és (3) miatt

$$\deg G^* = \deg G = (p-1)t > (p-1)\left(\sum_{i=1}^{k} \deg f_i\right) = \deg F \geq \deg F^*,$$

ami ellentmondás. ■

A pont második részében egy olyan eredményt bizonyítunk, amely az $f(x) \equiv 0 \pmod{p}$ kongruencia megoldásszámára pontos képletet ad az együtthatók segítségével. Ez a Kőnig Gyulától és Rados Gusztávtól származó tétel inkább csak elvi jelentőségű, a megoldásszám gyakorlati kiszámítására nemigen használható.

3.6.2 Tétel (Kőnig–Rados-tétel) **T 3.6.2**

Legyen p prím és

$$f = a_0 + a_1 x + \ldots + a_{p-2} x^{p-2}$$

olyan egész együtthatós polinom, amelyre $a_0 \not\equiv 0 \pmod{p}$. Ekkor az

$$f(x) \equiv 0 \pmod{p}$$

kongruencia megoldásszáma $p-1-r$, ahol $r = r(A)$ az alábbi $(p-1)\times(p-1)$-es A ciklikus mátrixnak a modulo p test feletti rangját jelöli:

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_{p-2} \\ a_{p-2} & a_0 & \ldots & a_{p-3} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix} . \clubsuit$$

Megjegyzések: 1. A tételből azonnal adódik, hogy az $f(x) \equiv 0 \pmod{p}$ kongruencia akkor és csak akkor oldható meg, ha az A mátrix rangja $p-1$-nél kisebb, azaz $\det A \equiv 0 \pmod{p}$.

2. Az f-re tett kikötések nem jelentenek lényeges megszorítást; egy tetszőleges polinom esetén a megoldásszám meghatározását visszavezethetjük a Kőnig–Rados-tételre, lásd a 3.6.11 feladatot.

Bizonyítás: Az alábbi elemi lineáris algebrai tételeket fogjuk felhasználni. Ezek egy T kommutatív test feletti $n \times n$-es mátrixokra vonatkoznak és $r(B)$ jelöli a B mátrix rangját; esetünkben $n = p-1$ és T a modulo p test.

(i) Legyenek $t_1, t_2, \ldots, t_n$ a T test különböző elemei. Ekkor a

$$V = V(t_1, t_2, \ldots, t_n) = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ t_1 & t_2 & t_3 & \ldots & t_n \\ t_1^2 & t_2^2 & t_3^2 & \ldots & t_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_1^{n-1} & t_2^{n-1} & t_3^{n-1} & \ldots & t_n^{n-1} \end{pmatrix}$$

Vandermonde-mátrix rangja $r(V) = n$.

(ii) Ha $r(B) = n$, azaz B invertálható, akkor tetszőleges C-re $r(CB) = r(C)$.

A (ii) összefüggés a bármely M, N mátrixra érvényes

$$r(MN) \le \min\bigl(r(M), r(N)\bigr)$$

egyenlőtlenségből adódik: ennek alapján egyrészt $r(CB) \le r(C)$, másrészt $r(C) = r((CB)B^{-1}) \le r(CB)$.

Rátérve a 3.6.2 Tétel bizonyítására, jelöljük az $f(x) \equiv 0 \pmod p$ kongruencia megoldásszámát s-sel, legyen $V = V(1, 2, \dots, p-1)$, és tekintsük a $D = AV$ mátrixot. Az (i) és (ii) segédtételeink alapján

$$r(D) = r(A) = r\,. \tag{7}$$

Az AV mátrixszorzást elvégezve a D mátrix első sorának j-edik eleme

$$d_{1j} = a_0 + a_1 j + a_2 j^2 + \ldots + a_{p-2} j^{p-2} = f(j)$$

lesz. A második sor j-edik elemének egyszerű felírásához azt is felhasználjuk, hogy $j^{p-1} \equiv 1 \pmod p$:

$$\begin{aligned} d_{2j} &= a_{p-2} + a_0 j + a_1 j^2 + \ldots + a_{p-3} j^{p-2} \equiv \\ &\equiv a_{p-2} j^{p-1} + a_0 j + a_1 j^2 + \ldots + a_{p-3} j^{p-2} = j f(j) \pmod p\,. \end{aligned}$$

Hasonlóan adódik, hogy az i-edik sor j-edik eleme

$$d_{ij} \equiv j^{i-1} f(j) \pmod p\,.$$

Így azt kaptuk (a kongruenciák helyett a modulo p testbeli egyenlőséget írva), hogy

$$D = AV = \begin{pmatrix} f(1) & f(2) & f(3) & \ldots & f(p-1) \\ f(1) & 2f(2) & 3f(3) & \ldots & (p-1)f(p-1) \\ f(1) & 2^2 f(2) & 3^2 f(3) & \ldots & (p-1)^2 f(p-1) \\ \vdots & \vdots & \vdots & & \vdots \\ f(1) & 2^{p-2} f(2) & 3^{p-2} f(3) & \ldots & (p-1)^{p-2} f(p-1) \end{pmatrix}.$$

A D mátrix j-edik oszlopában pontosan akkor lesz minden elem 0, ha $f(j) \equiv 0 \pmod p$, vagyis a D csupa 0 oszlopainak a száma éppen s. A többi oszlop a V különböző oszlopainak a nemnulla skalárszorosa, tehát ezek az (i) segédtétel

szerint lineárisan függetlenek. Ez azt jelenti, hogy $r(D) = p-1-s$. Ezt (7)-tel összevetve éppen a tétel állítását kapjuk. ■

Feladatok

3.6.1 Melyik ismert tételt kapjuk a Chevalley-tételnek abban a speciális esetében, ha mindegyik f_i polinom elsőfokú?

3.6.2 Bizonyítsuk be, hogy az $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ kongruenciának bármely p prím és a, b, c egészek esetén létezik nemtriviális megoldása.

3.6.3

a) Mutassuk meg, hogy bármely $n > 1$-hez található három olyan egész szám, amelyek s négyzetösszegére $n \mid s$, de $n^2 \nmid s$.

b) Lássuk be, hogy $(n, s/n) = 1$ is elérhető.

3.6.4 Mutassuk meg, hogy bármely p prímszámnak létezik olyan (nemnulla) többszöröse, amely kisebb, mint $p^4/4$, és felírható legfeljebb öt egész szám negyedik hatványának az összegeként.

*3.6.5

a) Legyenek $q_1, \ldots, q_k$ különböző prímszámok és $c_1, \ldots, c_t$ olyan különböző pozitív egészek, amelyek egyikének sincs a q_i-ktől különböző prímosztója. Bizonyítsuk be, hogy ha $t \geq 2k + 1$, akkor a c_j számok közül kiválasztható néhány különböző (esetleg csak egy, esetleg az összes) úgy, hogy a szorzatuk köbszám legyen.

b) Általánosítsuk az a) részt köbszámok helyett m-edik hatványokra, ahol m tetszőleges prímszám.

Megjegyzés: A megfelelő állítás (más eszközökkel) igazolható arra az esetre is, amikor m prímhatvány, azonban tetszőleges m egészre a probléma megoldatlan.

*3.6.6 Mutassuk meg, hogy $2n - 1$ egész számból mindig kiválasztható n olyan, amelyek összege osztható n-nel.

3.6.7 Bizonyítsuk be a Chevalley-tétel következő általánosítását. Hagyjuk el a tétel feltételei közül azt, hogy az f_i polinomok konstans tagja 0, a többi feltétel változatlan marad. Ekkor a szóban forgó kongruenciarendszer megoldásaira a következők igazak:

a) Ha van megoldás, akkor legalább két megoldás van.

*b) A megoldásszám osztható p-vel.

3.6.8 Legyen $p > 2$ prím, $(ab, p) = 1$. A Kőnig–Rados-tétel illusztrációjaként határozzuk meg az $f(x) \equiv 0 \pmod{p}$ kongruenciák megoldásszámát az alábbi f polinomok esetén:

a) $ax - b$; b) $1 + x + \ldots + x^{p-2}$; c) $x^{p-2} - a$.

3.6.9 Olvassuk le a Kőnig–Rados-tételből, hogy az alábbi kongruenciák megoldhatók:

a) $x^k \equiv 1 \pmod{p}$, ahol p páratlan prím és $1 \leq k \leq p-2$;

b) $x^2 \equiv -1 \pmod{p}$, ahol p prím és $p \equiv 1 \pmod{4}$.

3.6.10 Legyen $p > 3$ prím, $(a_0, p) = (a_1, p) = (a_{p-2}, p) = 1$ és

$$\begin{aligned} f &= a_0 + a_1 x + \ldots + a_{p-3}x^{p-3} + a_{p-2}x^{p-2}\,, \\ g &= a_1 + a_2 x + \ldots + a_{p-2}x^{p-3} + a_0 x^{p-2}\,, \\ h &= a_{p-2} + a_{p-3}x + \ldots + a_1 x^{p-3} + a_0 x^{p-2}\,. \end{aligned}$$

Bizonyítsuk be, hogy az

$$f(x) \equiv 0 \pmod{p}, \quad g(x) \equiv 0 \pmod{p} \quad \text{és} \quad h(x) \equiv 0 \pmod{p}$$

kongruenciák mindegyikének ugyanannyi a megoldásszáma.

3.6.11 Legyen $g = b_0 + b_1 x + \ldots + b_n x^n$ tetszőleges egész együtthatós polinom. Hogyan vezethetjük vissza a $g(x) \equiv 0 \pmod{p}$ kongruencia megoldásszámának a meghatározását a Kőnig–Rados-tételre az $n > p-2$ és/vagy $b_0 \equiv 0 \pmod{p}$ esetben?

3.7. Prímhatvány modulusú kongruenciák

A 2.6 pontban láttuk, hogy tetszőleges összetett modulusú kongruencia visszavezethető prímhatvány modulusú kongruenciákra a kínai maradéktétel segítségével. Most azzal foglalkozunk, hogyan vezethető vissza alkalmas feltételek teljesülése esetén egy prímhatvány modulusú kongruencia a prím modulusú esetre.

Legyen p prím, k pozitív egész, f egy egész együtthatós polinom, és tekintsük az

$$f(x) \equiv 0 \pmod{p^k} \tag{1}$$

kongruenciát. Ha c megoldása (1)-nek, akkor c nyilván az

$$f(x) \equiv 0 \pmod{p} \tag{2}$$

kongruenciát is kielégíti. Ezért (1) megoldásait a (2) kongruencia megoldásaiból kiindulva fogjuk megkeresni.

3.7.1 Tétel **T 3.7.1**

Legyen c megoldása (2)-nek, és tegyük fel, hogy $f'(c) \not\equiv 0 \pmod{p}$, ahol f' az f polinom deriváltját jelöli. Ekkor (1)-nek pontosan egy olyan $x \equiv c_k \pmod{p^k}$ megoldása létezik, amelyre $c_k \equiv c \pmod{p}$. ♣

A bizonyítás egyúttal eljárást is ad c_k előállítására, és az is kiderül, mi a helyzet akkor, ha $f'(c) \equiv 0 \pmod{p}$.

Bizonyítás: Fel fogjuk használni az alábbi összefüggést:

$$j \geq 1 \Longrightarrow f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}. \tag{3}$$

Ennek igazolásához tekintsük $f(a + tp^j)$ előállítását a Taylor-formula segítségével:

$$f(a + tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + \ldots + t^n p^{nj} \frac{f^{(n)}(a)}{n!}, \tag{4}$$

ahol n az f polinom foka. Itt mindegyik $f^{(r)}(a)/(r!)$ egész szám, ugyanis bármely x^s tag r-edik deriváltja $s(s-1)\ldots(s-r+1)x^{s-r}$ (ha $s \geq r$), és r szomszédos egész szám szorzata mindig osztható $r!$-sal (lásd az 1.1.17b feladatot). Ebből következik, hogy (4) jobb oldalán a harmadik tagtól kezdve minden tag osztható p^{j+1}-gyel, tehát (3) valóban teljesül.

A 3.7.1 Tételt k szerinti teljes indukcióval bizonyítjuk. A $k = 1$ eset (a deriváltra vonatkozó feltétel nélkül is) nyilvánvaló.

Tegyük fel, hogy az állítás $k-1$-re igaz: ez azt jelenti, hogy az

$$f(x) \equiv 0 \pmod{p^{k-1}} \tag{5}$$

kongruenciának $x \equiv c_{k-1} \pmod{p^{k-1}}$ az egyetlen olyan megoldása, amelyre $c_{k-1} \equiv c \pmod{p}$.

Keressük most az (1) kongruenciának a $c_k \equiv c \pmod{p}$ feltételt is teljesítő megoldását. Nyilván c_k kielégíti (5)-öt is, tehát $c_k \equiv c_{k-1} \pmod{p^{k-1}}$, azaz

$$c_k = c_{k-1} + tp^{k-1}. \tag{6}$$

Helyettesítsük be (6)-ot az (1) kongruenciába, és használjuk fel (3)-at ($a = c_{k-1}$, $j = k-1$ szereposztással). Ekkor az

$$f(c_k) = f(c_{k-1} + tp^{k-1}) \equiv f(c_{k-1}) + tp^{k-1} f'(c_{k-1}) \equiv 0 \pmod{p^k} \tag{7}$$

kongruenciához jutunk. Itt az indukciós feltevés miatt $p^{k-1} \mid f(c_{k-1})$. A (7) kongruenciát p^{k-1}-gyel egyszerűsítve és $c_{k-1} \equiv c \pmod p$ felhasználásával

$$\frac{f(c_{k-1})}{p^{k-1}} + tf'(c) \equiv 0 \pmod p \tag{8}$$

adódik. Ez lineáris kongruencia t-re, amelynek az $f'(c) \not\equiv 0 \pmod p$ feltétel miatt pontosan egy $t \equiv t_0 \pmod p$ megoldása létezik. Innen $t = t_0 + sp$, amit (6)-ba visszahelyettesítve kapjuk, hogy

$$c_k = c_{k-1} + t_0 p^{k-1} + sp^k, \quad \text{azaz} \quad c_k \equiv c_{k-1} + t_0 p^{k-1} \pmod{p^k}.$$

Ezzel beláttuk, hogy c_k létezik és mod p^k egyértelmű. ■

A bizonyítás alapján $c = c_1$-ből kiindulva egymás után előállíthatjuk a $c_2, c_3, \ldots$ értékeket, vagyis a c_k meghatározására egy rekurziós módszert kaptunk. (A c_k értékekre akár „képletet" is nyerhetünk, lásd a 3.7.4 feladatot.)

Ha $f'(c) \equiv 0 \pmod p$, akkor a (8) kongruenciának vagy minden t megoldása, vagy pedig egyáltalán nincs megoldása, attól függően, hogy $p^k \mid f(c_{k-1})$ vagy sem. Ez azt jelenti, hogy az (5) kongruencia egy c_{k-1} megoldásából vagy p darab megfelelő c_k értéket kapunk, vagy pedig egyet sem. Ilyenkor tehát a fenti rekurziós típusú eljárás alkalmazása jóval bonyolultabb.

Példa: Oldjuk meg az $x^3 + 2x \equiv 22 \pmod{125}$ kongruenciát.

Először megoldjuk az

$$f(x) = x^3 + 2x - 22 \equiv 0 \pmod 5$$

kongruenciát. A $0, \pm 1, \pm 2$ modulo 5 teljes maradékrendszer elemeit behelyettesítve kapjuk, hogy az összes megoldás

$$\text{(i) } x \equiv 2 \pmod 5 \qquad \text{és} \qquad \text{(ii) } x \equiv -1 \pmod 5.$$

(i) Az $x \equiv 2 \pmod 5$ esetben

$$f'(2) \equiv 3 \cdot 2^2 + 2 \equiv -1 \pmod 5,$$

ezért alkalmazhatjuk a 3.7.1 Tételt.

Az $x^3 + 2x - 22 \equiv 0 \pmod{25}$ kongruenciában az $x = 2 + 5t$ helyettesítést elvégezve a fentiek alapján

$$-10 + (5t) \cdot 14 \equiv 0 \pmod{25}, \quad \text{azaz} \quad -2 - t \equiv 0 \pmod 5$$

adódik, ahonnan $t \equiv -2 \pmod 5$, vagyis $t = 5s - 2$. Innen

$$x = 2 + 5t = 2 + 5(5s - 2) = -8 + 25s.$$

Ez azt jelenti, hogy az

$$x^3 + 2x - 22 \equiv 0 \pmod{25}$$

kongruenciának az $x \equiv 2 \pmod 5$ feltételt is kielégítő egyetlen megoldása $x \equiv -8 \pmod{25}$.

Hasonlóan haladunk tovább az 5^2 modulusról az 5^3 modulusra. Írjuk be az

$$x^3 + 2x - 22 \equiv 0 \pmod{125}$$

kongruenciába x helyére a kapott $x = -8 + 25s$ kifejezést. Ekkor

$$-50 + (25s) \cdot 194 \equiv 0 \pmod{125}$$

adódik. Innen $s \equiv -2 \pmod 5$, tehát

$$x = -8 + 25s = -58 + 125r, \qquad \text{azaz} \qquad x \equiv -58 \pmod{125}.$$

(ii) Az $x \equiv -1 \pmod 5$ esetben $f'(-1) \equiv 0 \pmod 5$, és így a bizonyítás után tett megjegyzés szerint minden lépésben azt kell vizsgálnunk, hogy a (8) kongruenciában a megfelelő $f(c_{k-1})$ érték osztható-e p^k-val vagy sem.

Mivel $f(-1) \equiv 0 \pmod{25}$, ezért minden $x \equiv -1 \pmod 5$ érték kielégíti az $x^3 + 2x - 22 \equiv 0 \pmod{25}$ kongruenciát, azaz a megoldások

$$x \equiv -1,\ 4,\ 9,\ 14 \text{ és } 19 \pmod{25}.$$

Ezek közül csak az utolsó kettőre lesz $f(x)$ osztható 125-tel is, vagyis az $x^3 + 2x - 22 \equiv 0 \pmod{125}$ kongruenciát

$$x \equiv 14 \pmod{25} \qquad \text{és} \qquad x \equiv 19 \pmod{25}$$

elégítik ki (ez $2 \cdot 5 = 10$ maradékosztályt jelent modulo 125).

Összefoglalva, az $x^3 + 2x \equiv 22 \pmod{125}$ kongruencia összes megoldását az alábbi 11 modulo 125 maradékosztály adja:

$$-58, \qquad 14 + 25j \qquad \text{és} \qquad 19 + 25j, \qquad \text{ahol} \qquad 0 \le j \le 4.$$

Feladatok

3.7.1 Határozzuk meg az alábbi kongruenciák megoldásszámát:

a) $x^{80} + x^3 \equiv 8 \pmod{3^{20}}$;

b) $x^{99} + x^3 \equiv 8 \pmod{3^{20}}$;

c) $x^{60} \equiv 1 \pmod{73^{20}}$;

d) $x^{73} \equiv 1 \pmod{73^{20}}$;

e) $x(x-1)(x-2) \equiv 0 \pmod{10^{20}}$.

3.7.2 Legyen p prím, továbbá a és n olyan pozitív egészek, amelyek nem oszthatók p-vel. Bizonyítsuk be, hogy ha az $x^n \equiv a \pmod{p}$ kongruencia megoldható, akkor bármely k esetén megoldható az $x^n \equiv a \pmod{p^k}$ kongruencia is.

3.7.3 Mely, a modulushoz relatív prím a értékek esetén oldhatók meg az alábbi kongruenciák? Határozzuk meg a megoldásszámot is.

a) $x^{10} \equiv a \pmod{11^{50}}$; **M** *b) $x^2 \equiv a \pmod{2^{50}}$.

3.7.4 Tegyük fel, hogy teljesülnek a 3.7.1 Tétel feltételei, és legyen u egy olyan szám, amelyre $uf'(c) \equiv 1 \pmod{p}$. Bizonyítsuk be, hogy a c_k értékek az alábbi rekurzióval állíthatók elő:

$$c_1 = c \quad \text{és} \quad c_k = c_{k-1} - uf(c_{k-1}), \quad \text{ha} \quad k > 1\,.$$

3.7.5 Oldjuk meg az $x^6 + 4x \equiv d \pmod{7^3}$ kongruenciát, ahol d értéke

a) 3; b) 2; c) 72.

4. LEGENDRE- ÉS JACOBI-SZIMBÓLUM

A prím modulusú másodfokú kongruenciák kezelésének alapvető eszköze a Legendre-szimbólum. Ennek tárgyalása során bebizonyítjuk többek között a nevezetes Gauss-lemmát és kvadratikus reciprocitási tételt is. A fejezet végén a Legendre-szimbólum általánosításával, a Jacobi-szimbólummal foglalkozunk.

4.1. Másodfokú kongruenciák

Ebben a pontban végig feltesszük, hogy $p > 2$ prím és $(a, p) = 1$.

A 3.5.2 Definíció $k = 2$ speciális eseteként először definiáljuk a kvadratikus maradék, illetve kvadratikus nemmaradék fogalmát.

4.1.1 Definíció **D 4.1.1**

Legyen $p > 2$ prím és $(a, p) = 1$. Az a számot aszerint nevezzük *kvadratikus maradék*nak, illetve *kvadratikus nemmaradék*nak modulo p, hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldható-e, vagy sem. ♣

Az $a \equiv 0 \pmod{p}$ számokat nem soroljuk sem a kvadratikus maradékok, sem a kvadratikus nemmaradékok közé.

4.1.2 Tétel **T 4.1.2**

(i) Az a szám akkor és csak akkor kvadratikus maradék modulo p, ha $a^{(p-1)/2} \equiv 1 \pmod{p}$. Ezzel ekvivalens, hogy az a (bármely primitív gyök szerinti) indexe páros.

(ii) Az a szám akkor és csak akkor kvadratikus nemmaradék modulo p, ha $a^{(p-1)/2} \equiv -1 \pmod{p}$. Ezzel ekvivalens, hogy az a (bármely primitív gyök szerinti) indexe páratlan.

(iii) A (páronként inkongruens) kvadratikus maradékok száma, illetve kvadratikus nemmaradékok száma egyaránt $(p-1)/2$.

(iv) Ha a kvadratikus maradék, akkor az $x^2 \equiv a \pmod{p}$ kongruenciának két (páronként inkongruens) megoldása van. ♣

Bizonyítás: (i) és (iii) a 3.5.3 Tételnek, (iv) pedig a 3.5.1 Tétel egyik állításának a $k = 2$ speciális esete.

(i) alapján az is adódik, hogy a akkor és csak akkor kvadratikus nemmaradék, ha $a^{(p-1)/2} \not\equiv 1 \pmod{p}$, illetve ha az a indexe páratlan. Így (ii)-höz már csak az

$$a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \tag{1}$$

ekvivalenciát kell igazolni. Mivel $a^{p-1} \equiv 1 \pmod{p}$ és p prím, ezért csak $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ lehetséges. Emellett $p > 2$ miatt $1 \not\equiv -1 \pmod{p}$, és így (1) valóban teljesül. ■

4.1.3 Definíció **D 4.1.3**

Az $\left(\frac{a}{p}\right)$ *Legendre-szimbólum*ot a következőképpen értelmezzük:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ kvadratikus maradék mod } p; \\ -1, & \text{ha } a \text{ kvadratikus nemmaradék mod } p. \end{cases} \clubsuit$$

Megjegyzés: Időnként hasznos a Legendre-szimbólum definícióját a $p \mid a$ esetre is kiterjeszteni, mégpedig az $\left(\frac{a}{p}\right) = 0$ értelmezéssel (lásd például a 4.1.15 feladatot). Ha azonban ezt külön nem jelezzük, akkor a továbbiakban automatikusan az $(a, p) = 1$ feltételre szorítkozunk.

Példa: $\left(\frac{2}{7}\right) = 1$, mert az $x^2 \equiv 2 \pmod{7}$ kongruencia megoldható; az egyik megoldás $x \equiv 3 \pmod{7}$. A megoldhatóságot a

$$2^{\frac{7-1}{2}} = 2^3 \equiv 1 \pmod{7}$$

feltétel ellenőrzésével is beláthatjuk.

A Legendre-szimbólum definícióját a 4.1.2 Tétellel összevetve kapjuk, hogy bármely a esetén

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}\,. \tag{2}$$

A Legendre-szimbólum néhány fontos tulajdonságát az alábbi tételben foglaljuk össze.

T 4.1.4

4.1.4 Tétel

(i) $a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

(iii) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod 4; \\ -1, & \text{ha } p \equiv -1 \pmod 4. \end{cases}$ ♣

Bizonyítás: Mindhárom állítás azonnal adódik (2)-ből, ezt csak (ii)-re részletezzük:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p .$$

Így

$$K = \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

egyrészt osztható $p > 2$-vel, másrészt K értéke csak 0 vagy ± 2 lehet, vagyis valóban $K = 0$. ■

A 4.1.4 Tétel alapján a Legendre-szimbólum számolása visszavezethető a $\left(\frac{2}{p}\right)$ és $\left(\frac{q}{p}\right)$ értékek meghatározására, ahol $q > 2$ a p-től különböző prím. Az erre vonatkozó eredményeket a következő pontban tárgyaljuk.

Feladatok

(A p végig egy 2-nél nagyobb prímszámot jelöl.)

4.1.1 Bizonyítsuk be három különböző módon, hogy $(c, p) = 1$ esetén a c^2 kvadratikus maradék mod p.

4.1.2 Számítsuk ki az alábbi Legendre-szimbólumok értékét:

a) $\left(\frac{39}{19}\right)$; b) $\left(\frac{37}{19}\right)$; c) $\left(\frac{-100}{19}\right)$.

4.1.3 Számítsuk ki az

$$\left(\frac{1}{p}\right),\ \left(\frac{2}{p}\right),\ \ldots,\ \left(\frac{p-1}{p}\right)$$

Legendre-szimbólumok összegét és szorzatát.

4.1.4 Lássuk be, hogy bármely kvadratikus maradék az

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

számok közül pontosan eggyel kongruens modulo p.

4.1.5 Igazoljuk, hogy ha a^2+b^2 osztható 77-tel, akkor osztható 5929-cel is.

4.1.6 Legyen p egy $4k+1$ alakú prím. Bizonyítsuk be, hogy az $x^2 \equiv -1 \pmod{p}$ kongruencia megoldásai

$$x \equiv \pm\Big(\frac{p-1}{2}\Big)! \pmod{p}.$$

4.1.7 Legyen p egy $4k+3$ alakú prím és a kvadratikus maradék mod p. Bizonyítsuk be, hogy az $x^2 \equiv a \pmod{p}$ kongruencia megoldásai

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}.$$

4.1.8

a) Bizonyítsuk be, hogy ha $o_p(a)$ páratlan, akkor a kvadratikus maradék mod p.

b) Mely p prímek esetén igaz a fenti állítás megfordítása?

4.1.9

a) Bizonyítsuk be, hogy egy primitív gyök szükségképpen kvadratikus nemmaradék modulo p.

*b) Mely p prímek esetén igaz a fenti állítás megfordítása?

4.1.10 Tegyük fel, hogy $(c, 97) = 1$, a c kvadratikus nemmaradék és nem primitív gyök mod 97. Számítsuk ki $o_{97}(c)$ értékét.

4.1.11 Bizonyítsuk be, hogy ha

a) $p = 4k-1$; b) $p = 4k+1$,

akkor az $x^2 \equiv k \pmod{p}$ kongruencia megoldható.

4.1.12 Mutassuk meg, hogy bármely p esetén az alábbi mod p kongruenciák közül legalább az egyik biztosan megoldható:

$$x^2 \equiv 30, \quad x^2 \equiv 33, \quad x^2 \equiv 70, \quad x^2 \equiv 105 \quad \text{és} \quad x^2 \equiv 165\,.$$

4.1.13 Oldjuk meg az alábbi kongruenciákat:

M a) $3x^2+5x+5 \equiv 0 \pmod{13}$;

b) $7x^2+8x \equiv 5 \pmod{17}$;

c) $6x^{25}+x^5+5x \equiv 0 \pmod{23}$;

d) $2x^{17}+5x+1 \equiv 0 \pmod{19}$.

4.1.14 Jelöljük $n(p)$-vel a legkisebb olyan pozitív egészt, amely kvadratikus nemmaradék mod p. Például $n(5) = 2, n(7) = 3$. Bizonyítsuk be, hogy

a) $n(p)$ mindig prímszám;

**b) $n(p) < 1 + \sqrt{p}$.

4.1.15 Terjesszük ki a Legendre-szimbólum definícióját a $p \mid a$ esetre az $\left(\frac{a}{p}\right) = 0$ értelmezéssel. Legyen továbbá

$$S(a,p) = \sum_{i=1}^{p} \left(\frac{i(i+a)}{p}\right).$$

Bizonyítsuk be, hogy

a) $S(0,p) = p-1$;

*b) $(a,p) = 1 \Longrightarrow S(a,p) = S(1,p)$;

c) $\sum_{a=0}^{p-1} S(a,p) = 0$;

d) $S(1,p) = -1$.

4.1.16 Jelölje $M(p)$ azoknak az $1 \le a \le p-2$ értékeknek a számát, amelyekre a és $a+1$ is kvadratikus maradék mod p.

a) Bizonyítsuk be, hogy

$$4M(p) = \sum_{a=1}^{p-2} \left(\left(\frac{a}{p}\right) + 1\right)\left(\left(\frac{a+1}{p}\right) + 1\right).$$

b) Mutassuk meg, hogy $M(p)$ „körülbelül” $p/4$: ha $p = 4k \pm 1$, akkor $M(p) = k - 1$.

4.2. Kvadratikus reciprocitás

Ebben a pontban is feltesszük, hogy $p > 2$ prím. A $\left(\frac{2}{p}\right)$ és $\left(\frac{q}{p}\right)$ Legendre-szimbólumokra vonatkozó tételeket fogunk bizonyítani, ahol $q > 2$ a p-től különböző prím. Mindkét eredményhez szükségünk lesz az alábbi lemmára:

4.2.1 Tétel (Gauss-lemma) **T 4.2.1**

Legyen $(a,p) = 1$, és tekintsük az $a, 2a, \ldots, \frac{p-1}{2}a$ számok modulo p vett legkisebb pozitív maradékait. Jelölje v ezek közül a $\frac{p}{2}$-nél nagyobbak számát. Ekkor

$$\left(\frac{a}{p}\right) = (-1)^v. \ \clubsuit$$

Bizonyítás: Az adott $\frac{p-1}{2}$ szám legkisebb pozitív maradékai közül a $\frac{p}{2}$-nél kisebbeket jelölje $r_1, \dots, r_u$, a $\frac{p}{2}$-nél nagyobbakat pedig $p-s_1, \dots, p-s_v$ (ahol $u+v=\frac{p-1}{2}$). Így bármely $1 \le t \le \frac{p-1}{2}$ esetén alkalmas i-vel vagy j-vel

$$ta \equiv \begin{cases} \text{vagy } r_i \\ \text{vagy } p-s_j \end{cases} \pmod{p} \tag{1}$$

teljesül. Itt az r_i és s_j számok valamennyien az $1, 2, \dots, \frac{p-1}{2}$ értékek közül kerülnek ki.

Megmutatjuk, hogy az r_i és s_j számok mind különbözők, és így valamilyen sorrendben az $1, 2, \dots, \frac{p-1}{2}$ számokkal egyeznek meg.

Ha valamely $i \neq k$-ra $r_i = r_k$, akkor alkalmas $1 \le \lambda < \mu \le \frac{p-1}{2}$ számokkal

$$\lambda a \equiv r_i = r_k \equiv \mu a \pmod{p}$$

teljesül. Mivel $(a,p)=1$, ezért a-val egyszerűsítve $\lambda \equiv \mu \pmod{p}$ adódik, ami ellentmondás.

Hasonlóan jutunk ellentmondásra két s_j egyenlőségéből is.

Végül, ha $r_i = s_j$, akkor

$$\lambda a \equiv r_i = s_j \equiv -\mu a \pmod{p},$$

azaz $p \mid a(\lambda+\mu)$. Azonban $(a,p)=1$ és $0 < \lambda+\mu < p$, így egyik tényező sem osztható p-vel, ami ellentmond a p prím voltának.

Szorozzuk most össze az (1) kongruenciákat:

$$\begin{aligned} \Big(\frac{p-1}{2}\Big)! a^{\frac{p-1}{2}} &\equiv r_1 \dots r_u (p-s_1) \dots (p-s_v) \equiv \\ &\equiv (-1)^v r_1 \dots r_u s_1 \dots s_v = (-1)^v \Big(\frac{p-1}{2}\Big)! \pmod{p}. \end{aligned} \tag{2}$$

A (2) kongruenciát a p-hez relatív prím $\big(\frac{p-1}{2}\big)!$-sal egyszerűsítve adódik

$$a^{\frac{p-1}{2}} \equiv (-1)^v \pmod{p}, \quad \text{azaz} \quad \left(\frac{a}{p}\right) = (-1)^v. \ \blacksquare$$

A Gauss-lemma segítségével könnyen meghatározhatjuk, hogy a 2 mely prímekre nézve lesz kvadratikus maradék.

4.2.2 Tétel **T 4.2.2**

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv \pm 1 \pmod 8; \\ -1, & \text{ha } p \equiv \pm 3 \pmod 8. \end{cases} \clubsuit$$

Bizonyítás: A Gauss-lemmát alkalmazzuk $a = 2$-re: megvizsgáljuk, hogy a $2, 4, 6, \ldots, p-1$ számok közül hány nagyobb $\frac{p}{2}$-nél.

A számok száma összesen $\frac{p-1}{2}$, ebből a $\frac{p}{2}$-nél kisebbek száma $\lfloor \frac{p-1}{4} \rfloor$, tehát a keresett v érték

$$v = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor .$$

Ha $p = 8k+1$, akkor így $v = 4k - 2k = 2k$, vagyis $\left(\frac{2}{p}\right) = (-1)^{2k} = 1$.
Hasonlóan kapjuk a tétel állítását a $p = 8k \pm 3$ és $8k-1$ esetekben is. ■

Könnyen ellenőrizhető, hogy a 4.2.2 Tétel a

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

alakban is felírható.

Most rátérünk a Legendre-szimbólumokra vonatkozó legfontosabb eredmény kimondására és igazolására.

4.2.3 Tétel (Kvadratikus reciprocitási tétel) **T 4.2.3**

Ha $p > 2$ és $q > 2$ két különböző prím, akkor

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}, \tag{3}$$

azaz

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{ha } p \equiv q \equiv -1 \pmod 4; \\ \left(\frac{p}{q}\right), & \text{egyébként.} \end{cases} \clubsuit$$

Bizonyítás: Az alábbi két állítást fogjuk igazolni:

(A) Ha $(a,p) = 1$ és a páratlan, akkor

$$\left(\frac{a}{p}\right) = (-1)^w, \qquad \text{ahol} \qquad w = \sum_{t=1}^{\frac{p-1}{2}} \left\lfloor \frac{ta}{p} \right\rfloor . \tag{4}$$

(B) Ha b és c páratlan, 1-nél nagyobb, relatív prím számok, akkor

$$\sum_{\mu=1}^{(c-1)/2} \left\lfloor \frac{\mu b}{c} \right\rfloor + \sum_{\nu=1}^{(b-1)/2} \left\lfloor \frac{\nu c}{b} \right\rfloor = \frac{b-1}{2} \cdot \frac{c-1}{2} \,. \tag{5}$$

Ezekből a 4.2.3 Tétel már következik: (4) alapján

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^z \,, \qquad \text{ahol} \qquad z = \sum_{\mu=1}^{(p-1)/2} \left\lfloor \frac{\mu q}{p} \right\rfloor + \sum_{\nu=1}^{(q-1)/2} \left\lfloor \frac{\nu p}{q} \right\rfloor ,$$

és itt (5) szerint

$$z = \frac{p-1}{2} \cdot \frac{q-1}{2} \,,$$

tehát (3) valóban teljesül.

(A) bizonyításánál a Gauss-lemmára (4.2.1 Tétel) támaszkodunk. Az ottani jelöléseket fogjuk használni. Elég azt igazolnunk, hogy

$$w = \sum_{t=1}^{(p-1)/2} \left\lfloor \frac{ta}{p} \right\rfloor \equiv v \pmod 2. \tag{6}$$

Az (1) kongruenciákat a maradékos osztás alapján a következőképpen írhatjuk át egyenlőséggé:

$$ta = \left\lfloor \frac{ta}{p} \right\rfloor p + \begin{cases} \text{vagy } r_i \\ \text{vagy } p - s_j \,. \end{cases} \tag{7}$$

A (7) egyenlőségeket $t = 1, 2, \ldots, \frac{p-1}{2}$-re összegezve

$$\Big(1 + 2 + \ldots + \frac{p-1}{2}\Big) a = p \sum_{t=1}^{(p-1)/2} \left\lfloor \frac{ta}{p} \right\rfloor + \sum_{i=1}^{u} r_i + \sum_{j=1}^{v} (p - s_j)$$

adódik. Ezt átrendezve, és felhasználva, hogy $r_1, \ldots, r_u, s_1, \ldots, s_v$ az $1, 2, \ldots, \frac{p-1}{2}$ számok egy permutációját alkotják, a következő összefüggést kapjuk:

$$\left(1 + 2 + \ldots + \frac{p-1}{2}\right)(a-1) + 2\sum_{j=1}^{v} s_j = p\left(\sum_{t=1}^{(p-1)/2} \left\lfloor \frac{ta}{p} \right\rfloor + v\right) . \tag{8}$$

Mivel a páratlan, ezért (8) bal oldala páros szám, és így ($p > 2$ miatt) (6) valóban teljesül.

(B) bizonyításához tekintsük a síkon a

$$A = (0\,,\,0), \quad B = \Big(\frac{b}{2}\,,\,0\Big), \quad C = \Big(\frac{b}{2}\,,\,\frac{c}{2}\Big) \quad \text{és} \quad D = \Big(0\,,\,\frac{c}{2}\Big)$$

pontok által meghatározott T téglalapot. Ekkor (5) jobb oldalán nyilván a T belsejébe eső egész koordinátájú pontok (az ún. *rácspont*ok) száma áll.

Megmutatjuk, hogy (5) bal oldala is a fenti rácspontok számával egyenlő. Vágjuk ketté a T téglalapot az A és C csúcsokat összekötő $y = \frac{c}{b}x$ egyenletű átlóval. Magára az átlóra $(b, c) = 1$ miatt nem esik rácspont.

Most megszámoljuk az ABC („alsó") háromszög belsejébe eső rácspontok számát, jelöljük ezt n-nel. Vizsgáljuk meg, hány rácspont helyezkedik el az $x = \nu$ egyenletű („függőleges") egyenesnek a háromszögbe eső részén. Ezeknek a rácspontoknak az első koordinátája ν. A második koordinátát y-nal jelölve az $1 \le y < \frac{c}{b}\nu$ egyenlőtlenségnek kell teljesülnie. Az ilyen y-ok száma tehát $\lfloor \frac{\nu c}{b} \rfloor$. Az ABC háromszög belsejébe eső rácspontok számát innen úgy kapjuk, hogy a $\lfloor \frac{\nu c}{b} \rfloor$ értékeket összegezzük $\nu = 1, 2, \ldots, \frac{b-1}{2}$-re, azaz

$$n = \sum_{\nu=1}^{(b-1)/2} \Big\lfloor \frac{\nu c}{b} \Big\rfloor \,.$$

Ez éppen az (5) bal oldalán szereplő második összeg.

Hasonlóan igazolható, hogy ha az ACD háromszög belsejébe eső rácspontokat az $y = \mu$ („vízszintes") egyenesek mentén számoljuk meg, akkor az (5) bal oldalán szereplő első összeget kapjuk. Ezzel (5)-öt beláttuk, és így a 4.2.3 Tétel bizonyítását befejeztük. ■

Az alábbi példával azt illusztráljuk, hogyan használhatók a 4.1.4, 4.2.2 és 4.2.3 Tételek a Legendre-szimbólum értékének meghatározásánál.

Példa: Megoldható-e az $x^2 \equiv 198 \pmod{1997}$ kongruencia? (Az 1997 prímszám.)

A 198 kanonikus alakja $198 = 2 \cdot 3^2 \cdot 11$, ezért

$$\Big(\frac{198}{1997}\Big) = \Big(\frac{2}{1997}\Big)\Big(\frac{3}{1997}\Big)^2\Big(\frac{11}{1997}\Big) \,.$$

Mivel $1997 \equiv -3 \pmod 8$, így a 4.2.2 Tétel szerint $\big(\frac{2}{1997}\big) = -1$.

Mivel $1997 \equiv 1 \pmod 4$, így a 4.2.3 Tétel, majd $1997 \equiv -5 \pmod{11}$ stb. felhasználásával

$$\left(\frac{11}{1997}\right) = \left(\frac{1997}{11}\right) = \left(\frac{-5}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{5}{11}\right) = (-1)\left(\frac{11}{5}\right) = (-1)\left(\frac{1}{5}\right) = -1\,.$$

Tehát

$$\left(\frac{198}{1997}\right) = (-1)\cdot 1\cdot(-1) = 1,$$

vagyis az $x^2 \equiv 198 \pmod{1997}$ kongruencia megoldható.

Nagyon nagy számok esetén a fenti módszer problematikus pontja az, amikor az eljárás közben keletkező Legendre-szimbólumok „számlálóját" faktorizálni kell, amire nem ismeretes gyors algoritmus. A következő pontban látni fogjuk, hogy ez a probléma a Jacobi-szimbólum segítségével kiküszöbölhető.

Feladatok

4.2.1 Melyek oldhatók meg az alábbi kongruenciák közül:

a) $x^2 \equiv 66 \pmod{191}$; b) $x^2 \equiv 7! \pmod{83}$;
c) $x^2 \equiv 94! \pmod{101}$; d) $x^2 \equiv 30 \pmod{77}$;
e) $x^2 \equiv 38 \pmod{187}$; f) $2x^2 + 3x + 5 \equiv 0 \pmod{101}$.

4.2.2 Milyen $p > 2$ prímekre oldhatók meg az alábbi kongruenciák:

a) $x^2 \equiv -2 \pmod p$; b) $x^2 \equiv 3 \pmod p$;
c) $x^2 \equiv -3 \pmod p$; d) $x^2 \equiv 5 \pmod p$;
e) $x^4 \equiv 4 \pmod p$; *f) $x^4 \equiv -4 \pmod p$;
*g) $x^8 \equiv 16 \pmod p$; *h) $x^8 \equiv 81 \pmod p$.

4.2.3 Bizonyítsuk be, hogy ha $1999 \mid a^2 + 2b^2$, akkor $1999 \mid a$ és $1999 \mid b$.

*4.2.4 Bizonyítsuk be, hogy van olyan c, amelyre $43^{100} \mid 2c^8 + 1$.

4.2.5 Mutassuk meg, hogy

a) egy $8c^2 - 1$ alakú (pozitív) számnak minden prímosztója $8k \pm 1$ alakú és biztosan van $8k - 1$ alakú prímosztója;

b) egy $12c^2 - 1$ alakú (pozitív) számnak minden prímosztója $12k \pm 1$ alakú és biztosan van $12k - 1$ alakú prímosztója;

c) egy $c^2 + 4$ alakú páratlan számnak biztosan van $8k + 5$ és $3 \nmid c$ esetén $12k + 5$ alakú prímosztója is (ez a két prímosztó lehet ugyanaz).

4.2.6 Legyenek p_1, p_2, p_3, p_4, p_5 különböző páratlan prímek, $P = p_1 \dots p_5$ és $a_i = P/p_i$, $i = 1, 2, 3, 4, 5$.

a) Igazoljuk, hogy az

$$x_i^2 \equiv a_i \pmod{p_i}, \qquad i = 1,\ 2,\ 3,\ 4,\ 5$$

kongruenciák közül a megoldhatók száma akkor és csak akkor páros, ha

$$\sum_{i=1}^{5} \left(\frac{-1}{p_i}\right) = \pm 1.$$

b) Tegyük fel, hogy a

$$z_i^2 \equiv p_i \pmod{a_i}, \qquad i = 1,\ 2,\ 3,\ 4,\ 5$$

kongruenciák mindegyike megoldható. Lássuk be, hogy ekkor

$$\sum_{i=1}^{5} \left(\frac{-1}{p_i}\right) \geq 3.$$

4.2.7

a) Bizonyítsuk be, hogy 19 egymást követő egész szám négyzetének az összege nem lehet teljes hatvány.

*b) Mutassuk meg, hogy az a)-beli állítás 19 helyett bármilyen $12k \pm 5$ alakú prímszámra is igaz.

M**4.2.8 Adjunk meg olyan f egész együtthatós polinomot, amelyre az $f(x) = 0$ egyenletnek nincs racionális gyöke, de az $f(x) \equiv 0 \pmod{m}$ kongruencia minden m-re megoldható.

4.3. Jacobi-szimbólum

D 4.3.1

4.3.1 Definíció

Legyen $m > 1$ páratlan szám, $m = p_1 \dots p_r$, ahol a p_i számok (nem feltétlenül különböző) pozitív prímek. Legyen továbbá $(a, m) = 1$. Ekkor az $\left(\frac{a}{m}\right)$ *Jacobi-szimbólum*ot mint az $\left(\frac{a}{p_i}\right)$ Legendre-szimbólumok szorzatát értelmezzük:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right). \ \clubsuit$$

Példa: $\left(\frac{7}{45}\right) = \left(\frac{7}{3}\right)^2 \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$

Ha m prím, akkor a Jacobi-szimbólum megegyezik a Legendre-szimbólummal. Ennélfogva nem okozhat problémát, ha mindkettőt ugyanúgy jelöljük.

A prímeknél tapasztaltakkal szemben összetett m esetén az $x^2 \equiv a \pmod{m}$ kongruencia megoldhatósága nem karakterizálható az $\left(\frac{a}{m}\right)$ Jacobi-szimbólum segítségével (lásd a 4.3.2 feladatot).

A Jacobi-szimbólum ugyanakkor „átörökíti" a Legendre-szimbólumnak a 4.1.4, 4.2.2 és 4.2.3 Tételekben tárgyalt tulajdonságait:

4.3.2 Tétel **T 4.3.2**

Tegyük fel, hogy a szereplő Jacobi-szimbólumok értelmesek, azaz a „nevező" egy 1-nél nagyobb páratlan szám, amely relatív prím a „számlálóhoz" (tehát pl. (v)-ben m és n relatív prím, 1-nél nagyobb páratlan számok).

(i) $a \equiv b \pmod{m} \Longrightarrow \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$

(ii) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right), \qquad \left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right).$

(iii) $\left(\frac{-1}{m}\right) = \begin{cases} 1, & \text{ha } m \equiv 1 \pmod{4}; \\ -1, & \text{ha } m \equiv -1 \pmod{4}. \end{cases}$

(iv) $\left(\frac{2}{m}\right) = \begin{cases} 1, & \text{ha } m \equiv \pm 1 \pmod{8}; \\ -1, & \text{ha } m \equiv \pm 3 \pmod{8}. \end{cases}$

(v) $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), & \text{ha } n \equiv m \equiv -1 \pmod{4}; \\ \left(\frac{n}{m}\right), & \text{egyébként.} \quad \clubsuit \end{cases}$

Bizonyítás: Valamennyi tulajdonság következik a Jacobi-szimbólum definíciójából és a Legendre-szimbólum megfelelő tulajdonságából. Ezt részletesen megmutatjuk (v)-re (azaz a reciprocitási tétel megfelelőjére), a többi hasonlóan igazolható.

Legyen $m = p_1 \dots p_r$, $n = q_1 \dots q_s$ (ahol $p_i \neq q_j$). Ekkor a Jacobi-szimbólum definíciója és a Legendre-szimbólum multiplikativitása (vagy a je-

len tétel (ii) tulajdonságai) alapján

$$\left(\frac{m}{n}\right) = \prod_{\substack{1\le i\le r\\ 1\le j\le s}} \left(\frac{p_i}{q_j}\right), \qquad \left(\frac{n}{m}\right) = \prod_{\substack{1\le i\le r\\ 1\le j\le s}} \left(\frac{q_j}{p_i}\right). \tag{1}$$

Legyen a p_i-k közül u darab, a q_j-k közül v darab $4k-1$ alakú. Erre az uv számú p_i, q_j párra $\left(\frac{p_i}{q_j}\right) = -\left(\frac{q_j}{p_i}\right)$, az összes többi párra pedig $\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right)$. Ezért (1) alapján

$$\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right) \iff uv \text{ páratlan} \iff$$

$$\iff u \text{ és } v \text{ páratlan} \iff m \equiv n \equiv -1 \pmod 4. \ \blacksquare$$

Példa: Megoldható-e az $x^2 \equiv 2342 \pmod{11\,239}$ kongruencia? (A 11 239 prímszám.)

Az $\left(\frac{2342}{11\,239}\right)$ Legendre-szimbólumot Jacobi-szimbólumként, a 4.3.2 Tétel felhasználásával számítjuk ki. Ennek az lesz az előnye, hogy a „számlálókból" mindig csak a legnagyobb kettőhatványokat kell leválasztani, a páratlan részt nem kell faktorizálni, hanem azonnal lehet a reciprocitást alkalmazni.

$$\left(\frac{2342}{11\,239}\right) = \left(\frac{2}{11\,239}\right)\left(\frac{1171}{11\,239}\right) = 1(-1)\left(\frac{11\,239}{1171}\right) = -\left(\frac{-471}{1171}\right) =$$

$$= -\left(\frac{-1}{1171}\right)\left(\frac{471}{1171}\right) = -(-1)(-1)\left(\frac{1171}{471}\right) = -\left(\frac{229}{471}\right) =$$

$$= -\left(\frac{471}{229}\right) = -\left(\frac{13}{229}\right) = -\left(\frac{229}{13}\right) = -\left(\frac{8}{13}\right) = -\left(\frac{2}{13}\right)^3 = 1.$$

A kongruencia tehát megoldható.

Vegyük észre, hogy a fenti eljárás az euklideszi algoritmus egy variánsának tekinthető.

A Jacobi-szimbólum a prímtesztelésnél is fontos szerephez jut (lásd az 5.7.4 Tételt).

Feladatok

4.3.1 Számítsuk ki az alábbi Jacobi-szimbólumokat:

$$\text{a)}\ \left(\frac{1\,234\,567}{225}\right); \qquad \text{b)}\ \left(\frac{31}{95}\right); \qquad \text{c)}\ \left(\frac{589}{1999}\right); \qquad \text{d)}\ \left(\frac{1113}{11\,131}\right).$$

4.3.2 Legyen $m > 1$ páratlan szám és $(a, m) = 1$.

a) Bizonyítsuk be, hogy ha az $x^2 \equiv a \pmod{m}$ kongruencia megoldható, akkor $\left(\frac{a}{m}\right) = 1$.

b) Mutassunk példát, hogy az a)-beli állítás megfordítása nem igaz.

*c) Melyek azok az m-ek, amelyekre az a)-beli állítás megfordítása is igaz?

4.3.3 Bizonyítsuk be, hogy ha p prím és $p = a^2 + b^2$, akkor az

$$x^2 \equiv a \pmod{p} \qquad \text{és} \qquad x^2 \equiv b \pmod{p}$$

kongruenciák közül legalább az egyik megoldható.

4.3.4 Számítsuk ki a Jacobi-szimbólumokból képezett alábbi összegeket:

$$\text{a)}\ \sum_{k=1}^{111} \left(\frac{2}{2k+1}\right); \qquad \text{b)}\ \sum_{k=1}^{111} \left(\frac{k}{2k+1}\right).$$

4.3.5 Legyenek az a, m, n számok 1-nél nagyobbak, m és n páratlan, továbbá $(a, m) = (a, n) = 1$.

a) Bizonyítsuk be, hogy ha $a \equiv 0$ vagy $1 \pmod{4}$, akkor

$$m \equiv n \pmod{a} \Longrightarrow \left(\frac{a}{m}\right) = \left(\frac{a}{n}\right).$$

b) Mutassuk meg, hogy ha $a \equiv 2$ vagy $3 \pmod{4}$, akkor létezik olyan m és n, hogy

$$m \equiv n \pmod{a}, \qquad \text{de} \qquad \left(\frac{a}{m}\right) \neq \left(\frac{a}{n}\right).$$

4.3.6 Legyen $m > 1$ páratlan szám. Számítsuk ki a Jacobi-szimbólumokból képezett alábbi összeget és szorzatot:

$$\text{a)}\ \sum_{\substack{1 \le r \le m \\ (r,m)=1}} \left(\frac{r}{m}\right); \qquad \text{b)}\ \prod_{\substack{1 \le r \le m \\ (r,m)=1}} \left(\frac{r}{m}\right).$$

4.3.7

a) Adjuk meg az összes olyan $m > 1$ páratlan számot, amelyre bármely $(a, m) = 1$ esetén az $\left(\frac{a}{m}\right)$ Jacobi-szimbólum értéke 1.

M *b) Adjuk meg az összes olyan a egészt, amelyre bármely $m > 1$ páratlan szám és $(a, m) = 1$ esetén az $\left(\frac{a}{m}\right)$ Jacobi-szimbólum értéke 1.

5. PRÍMSZÁMOK

A prímszámok a matematika egyik legegyszerűbben megadott, ugyanakkor talán legtitokzatosabb halmazát alkotják. Már Euklidész Elemek című könyvében szerepel annak bizonyítása, hogy végtelen sok prímszám van, azonban ma sem tudjuk, hogy például végtelen sok ikerprím létezik-e. Néhány ilyen híres, egyszerűen megfogalmazható, ugyanakkor reménytelenül nehéz megoldatlan probléma bemutatása után speciális alakú prímekkel foglalkozunk: a Fermat- és Mersenne-prímekkel, illetve számtani sorozatok prímszámaival. A prímszámok eloszlásával kapcsolatban alsó és felső becslést adunk az x-nél nem nagyobb prímszámok számára, továbbá a szomszédos prímek közötti hézagot, valamint a prímek reciprokösszegét vizsgáljuk. Végül azt a kérdéskört tanulmányozzuk, hogyan lehet egy nagy számról a gyakorlatban is eldönteni, hogy prím-e (prímtesztelés), illetve hogyan lehet egy nagy összetett számot tényezőkre bontani (prímfelbontás, faktorizáció). Kiderül, hogy a két feladat alapvetően eltérő időigényű (legalábbis jelenlegi tudásunk szerint), és bemutatjuk az ezen az eltérésen alapuló, széles körben alkalmazott nyilvános jelkulcsú titkosírást, az RSA-sémát.

5.1. Klasszikus problémák

Ebben a fejezetben prímen végig pozitív prímszámot értünk (a „prímszám" szó tulajdonképpen pozitív felbonthatatlan szám értelemben szerepel majd általában), és p-vel mindig (pozitív) prímszámot jelölünk (tehát például $\prod_{p\le n} p$ a $(0,n]$ intervallumba eső prímek szorzatát jelenti).

Először az ókori görög matematika két nevezetes eredményét tárgyaljuk.

5.1.1 Tétel **T 5.1.1**

A prímszámok száma végtelen. ♣

Bizonyítás: Tegyük fel indirekt, hogy csak véges sok prímszám létezik, legyenek ezek $p_1(=2),\dots,p_r$. Tekintsük az $A = p_1 \dots p_r + 1$ számot.

Az A nyilván a $p_1,\dots,p_r$ prímszámok egyikével sem osztható.

Ugyanakkor minden 1-nél nagyobb számnak, így A-nak is létezik prímosztója. Ez szükségképpen különbözik a $p_1,\dots,p_r$ prímektől, ami ellentmond az indirekt feltevésnek. ■

Megjegyzés: A bizonyításból az is leolvasható, hogy

$$p_n < 2^{2^n},$$

ahol p_n az n-edik prímszámot jelöli (5.1.9a feladat). Ennél lényegesen jobb felső becslést fogunk megadni az 5.4 pontban.

Most az *eratoszteneszi szitát* mutatjuk be. Ez egy olyan eljárás, amellyel előállíthatjuk egy adott N számig az összes prímszámot.

5.1.2 Tétel (Eratoszteneszi szita) **T 5.1.2**

Írjuk fel 2-től N-ig az egész számokat. Az első lépésben karikázzuk be a 2-t, majd húzzuk át azokat a számokat, amelyek a 2 többszörösei és 2-nél nagyobbak: $4, 6, 8, \ldots$ Ezután karikázzuk be azt a legkisebb számot, amely még nincs megjelölve (azaz nincs bekarikázva és nincs áthúzva); ez a 3, majd húzzuk át ennek a nála nagyobb többszöröseit: $6, 9, \ldots$ (a 6-ot, 12-t stb. már másodszor húzzuk át).

Ismételjük meg a fentieket mindig a legkisebb még jelöletlen számmal, ha ez a szám még legfeljebb $\sqrt{N}$. Ha már minden $\sqrt{N}$-nél nem nagyobb számot megjelöltünk, akkor álljunk meg.

Ekkor a bekarikázott és a jelöletlen számok együttesen éppen az N-nél nem nagyobb prímszámokat adják (a bekarikázottak lesznek a $\sqrt{N}$-nél nem nagyobb, a jelöletlenek pedig a $\sqrt{N}$ és N közötti prímek). ♣

Bizonyítás: Az áthúzott számok nyilván összetettek, hiszen van egy náluk kisebb, de 1-nél nagyobb osztójuk.

A bekarikázott számokról teljes indukcióval igazoljuk, hogy felbonthatatlanok. Az első bekarikázott szám, a 2 felbonthatatlan. Legyen $s \le \sqrt{N}$ a k-adik bekarikázott szám, és tegyük fel, hogy az első $k-1$ bekarikázott szám alkotja az összes s-nél kisebb felbonthatatlan számot. Ekkor s-nek ezek egyike sem osztója (hiszen s-et egyszer sem húztuk át), tehát s nem osztható egyetlen nála kisebb felbonthatatlan számmal sem, és így s szükségképpen felbonthatatlan.

Legyen végül t egy tetszőleges jelöletlen szám. Ha t összetett lenne, akkor (pl. az 1.4.7a-b feladat szerint) t-nek lenne olyan p felbonthatatlan osztója, amelyre $p \le \sqrt{t} \le \sqrt{N}$. Ez azonban ellentmond annak, hogy t nem osztható a bekarikázott számok, azaz a $\sqrt{N}$-nél nem nagyobb felbonthatatlan számok egyikével sem. ■

Most a prímszámokkal kapcsolatos néhány nevezetes megoldatlan problémát ismertetünk. Ezek egy részével a fejezet további pontjaiban részletesebben is foglalkozunk majd.

Ikerprímek:

$\{3,5\}$, $\{5,7\}$, $\{11,13\}$, $\{17,19\}$, ...: előfordul-e végtelen sokszor, hogy két szomszédos páratlan szám mindegyike prím?

Megjegyzések:

1. A 2023-ban ismert legnagyobb ikerprímpár $2996863034895\cdot 2^{1290000}\pm 1$ (ezek a számok a tízes számrendszerben 388342 jegyűek).

2. A 2 helyett bármilyen más rögzített $2k$ páros számra is megoldatlan, hogy van-e végtelen sok olyan prímpár, amelyben a két prím különbsége éppen $2k$. Azonban óriási áttörést jelentett, amikor Goldston, Pintz és Yildirim eredményeit és módszereit továbbfejlesztve Zhang 2013-ban bebizonyította, hogy létezik ilyen $2k < 70000000$. A Terence Tao által vezetett Polymath8 nemzetközi internetes kutatócsoport 2014-ben ezt leszorította $2k \leq 246$-ra. Jelenleg is ez a legjobb ismert korlát.

3. További általánosításként prímpárok helyett prímhármasokat, prímnégyeseket stb. is vizsgálhatunk: könnyen adódik, hogy $n, n+2$ és $n+4$ mindegyike csak $n=3$ esetén prím, azonban nagyon is elképzelhető, hogy végtelen sok olyan n van, amelyre n, $n+2$ és $n+6$ mindhárman prímek, vagy akár n, $n+2$, $n+6$ és $n+8$ mindegyike prím stb. (Vö. az 1.4.1 és 5.1.1 feladatokkal.)

4. Az ikerprímprobléma úgy is megfogalmazható, hogy a szomszédos prímek különbsége vajon végtelen sokszor lesz-e „nagyon kicsi”. Egy másik irányú nevezetes sejtés, hogy két egymást követő négyzetszám között mindig található prímszám, vagyis a szomszédos prímek különbsége nem nőhet „túl gyorsan”. A szomszédos prímek közötti hézaggal részletesebben az 5.5 pontban foglalkozunk.

5. Az ikerprímek (ha végtelen sokan vannak is) mindenképpen „nagyon ritkán” helyezkednek el a prímek között; például az ikerprímek reciprokösszege konvergens, míg a prímeké divergens (lásd az 5.6 pontot).

6. Egy további érdekes eredmény, hogy végtelen sok olyan p prím létezik, amelyre $p+2$ vagy prím, vagy pedig két prím szorzata (azaz „csak egyetlen lépés” hiányzik az ikerprímprobléma bizonyításához).

Goldbach-sejtés:

$4=2+2$, $6=3+3$, $8=5+3$, $10=7+3$, $12=7+5$, ...: felírható-e 4-től kezdve minden páros szám két prímszám összegeként?

Megjegyzések:

1. A fenti problémát szokás „páros” Goldbach-sejtésnek is nevezni, megkülönböztetésül a „páratlan” Goldbachtól, amely arra vonatkozik, hogy a 7-től kezdve minden páratlan szám felírható három prím összegeként. Ez utóbbi állítás egyrészt azonnal következik a páros Goldbachból (lásd az 5.1.2 feladatot),

másrészt a mindmáig megoldatlan páros esettel ellentétben ezt már sikerült bebizonyítani. Az első lépést Vinogradov tette meg 1937-ben igazolva, hogy minden elég nagy páratlan szám előáll három prím összegeként. A bizonyítás explicit felső korlátot is adott arra, ahonnan kezdve minden páratlan szám biztosan felírható ílyen módon. Így már „csak" a korlát alatti véges sok páratlan számra kellett ellenőrizni a sejtést. Azonban a Vinogradov által talált korlát olyan óriási volt, hogy az elméleti javítások és a szupergyors számítógépek ellenére is ez a befejező lépés egészen a legutóbbi időkig váratott magára. Végül 2013-ban Helfgottnak sikerült teljes egészében belátnia a sejtést.

2. A („páros") Goldbach-sejtéssel kapcsolatos néhány részeredmény:

(A) Minden páros szám legfeljebb 6 prímszám összege. (Az első ilyen típusú tételt a 6 helyett néhány ezerrel Schnirelmann igazolta 1930-ban.)

(B) Minden elég nagy páros szám felírható $p + m$ alakban, ahol p prím és m vagy prím, vagy pedig két prím szorzata. (Az első ilyen típusú tételt, ahol alkalmas rögzített k-val m legfeljebb k darab prím szorzata, Rényi Alfréd igazolta 1947-ben.)

(C) Csak (a megfelelő értelemben vett) „ritka kivételek" lehetnek azok a páros számok, amelyek esetleg nem írhatók fel két prím összegeként. (A „ritka" jelző egyelőre sajnos nem helyettesíthető a „véges sok" kifejezéssel.)

Hosszú számtani sorozatok:

$\{3, 5, 7\}$, $\{5, 11, 17, 23, 29\}$, $\{7, 37, 67, 97, 127, 157\}$, ...: van-e akármilyen hosszú (nemkonstans) számtani sorozat csupa prímszámból?

Itt örömmel számolhatunk be arról, hogy 2004-ben Ben Green és Terence Tao bebizonyították, hogy a válasz igen.

Megjegyzések:

1. A 2023-ben ismert leghosszabb számtani sorozatnak, amely csupa prímszámból áll, 27 tagja van:

$$224584605939537911 + 81292139 \cdot P_{27}k, \qquad k = 0, 1, \ldots, 26,$$

ahol P_n az n-nél kisebb prímek szorzata: $P_{27} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$. Egy n elemű, csupa prímszámból álló számtani sorozat differenciája szükségképpen osztható P_n-nel (lásd az 5.1.5c feladatot).

2. Egy végtelen számtani sorozat már nem állhat csupa prímszámból (lásd az 1.4.2 feladatot), de szerepel benne végtelen sok prím, ha a kezdőtagja és a differenciája relatív prímek (Dirichlet tétele, lásd az 5.3 pontot).

Speciális alakú prímek:

- Létezik-e végtelen sok $2^k - 1$, illetve $2^k + 1$ alakú prím (Mersenne-, illetve Fermat-prímek, lásd az 5.2 pontot)?
- Létezik-e végtelen sok $n^2 + 1$ alakú prím (vö. az 1.4.6 feladattal)?
- Létezik-e végtelen sok prím a (tízes számrendszerben) csupa egyes számjegyet tartalmazó számok, a $333\ldots31$ alakú számok, a Fibonacci-számok stb. között?

Prímképletek:

Megadható-e olyan „gyakorlati szempontból is használható" képlet, amely minden n-re előállítja az n-edik prímszámot, vagy legalábbis olyan, a természetes számokon értelmezett, a gyakorlatban is kiszámítható (végtelen sok értékű) függvény, amelynek minden helyettesítési értéke prím?

Megjegyzések:

1. Általános vélekedés szerint ilyen képletre nemigen van remény. Az 5.1.9b és 5.5.9b feladatokban szereplő képletek éppen a gyakorlati kiszámíthatóság követelményének nem felelnek meg.

2. Már Euler észrevette, hogy n^2+n+41 minden $0 \le n \le 39$ esetén prím (azonban $n = 40$-re összetett). Ebből azonnal adódik, hogy

$$(n-40)^2 + (n-40) + 41 = n^2 - 79n + 1601$$

minden $0 \le n \le 79$ esetén prím. Ha nemcsak egész, hanem racionális együtthatós polinomokat is megengedünk, akkor akármilyen hosszú ilyen prímsorozatot tudunk gyártani (5.1.7 feladat). Másfelől azonban egy (nemkonstans) polinom biztosan nem alkalmas prímképletnek, mert nem vehet fel minden egész helyen prímet (5.1.8 feladat).

3. Meglepő ugyanakkor az alábbi (szintén csak elméleti szempontból jelentős) eredmény: Megadható olyan többváltozós, egész együtthatós polinom, amelynek a változók *nemnegatív* értékein felvett *pozitív* helyettesítési értékei megegyeznek a (pozitív) prímszámok halmazával. (Ez a polinom ugyanazt a prímet több helyen is felveheti, valamint negatív értékeket is felvesz.)

Ilyen polinom létezését először Matijaszevics igazolta 1970-ben. Matijaszevics ekkor oldotta meg Hilbert tizedik problémáját: (mások munkáját betetőzve) bebizonyította, hogy nem létezik olyan általános algoritmus, amely bármelyik diofantikus egyenlet esetén eldönti, hogy annak az egyenletnek van-e megoldása (az egész számok körében) vagy sem. Módszeréből egyúttal a fent jelzett tulajdonságú polinom létezése is kiderült. Az ilyen polinomokra vonatkozó jelenlegi rekordok: (i) a minimális fokszám 5, ekkor 42 változó szerepel; (ii) a minimális változószám 10, ekkor viszont a fokszám kb. $1{,}6 \cdot 10^{45}$.

Feladatok

Lásd az 1.4.1–1.4.7 feladatokat is.

5.1.1 Tegyük fel, hogy az $r_1, \ldots, r_k$ egészekhez végtelen sok olyan n létezik, amelyre az $n + r_1, \ldots, n + r_k$ számok mindegyike prím. Bizonyítsuk be, hogy ekkor az $r_1, \ldots, r_k$ számok semmilyen $m > 1$ modulusra sem tartalmazhatnak teljes maradékrendszert modulo m.

5.1.2 Bizonyítsuk be, hogy

a) a „páros" Goldbach-sejtésből következik a „páratlan", továbbá

b) a „páros" Goldbach-sejtés ekvivalens azzal az állítással, hogy minden $n \geq 6$ egész szám felírható három prím összegeként.

5.1.3 Mely páros számok írhatók fel két (pozitív) összetett szám összegeként? És melyek két *páratlan* (pozitív) összetett szám összegeként?

5.1.4 Határozzuk meg azokat a prímeket, amelyeknek az összege és a különbsége is prímszám.

5.1.5 Tekintsünk egy csupa prímszámból álló számtani sorozatot, jelöljük a tagok számát n-nel, a differenciát pedig d-vel. Bizonyítsuk be, hogy

a) ha $n = 4$, akkor $6 \mid d$;

b) ha $n = 6$, akkor $30 \mid d$;

M c) általában, d osztható az összes n-nél kisebb prímszámmal.

5.1.6 Bizonyítsuk be, hogy a „Speciális alakú prímek" c. résznél felsorolt valamennyi típusú számból végtelen sok összetett szám létezik.

5.1.7 Legyen k tetszőleges pozitív egész. Lássuk be, hogy van olyan f racionális együtthatós polinom, amelyre bármely $1 \leq i \leq k$ esetén $f(i)$ éppen az i-edik prímszám.

5.1.8

a) Legyen f egész együtthatós, egyváltozós, nemkonstans polinom. Mutassuk meg, hogy $f(n)$ nem lehet minden n természetes számra prím.

b) Igazoljuk ugyanezt

(b1) racionális együtthatós;

(b2) komplex együtthatós;

(b3) többváltozós

polinomokra is.

5.1.9 Jelölje p_n az n-edik prímszámot.

a) Bizonyítsuk be, hogy $p_n < 2^{2^n}$.

b) Legyen

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^{2^n}}} = 0{,}000200000000000300\ldots ,$$

azaz c egy olyan tizedes tört, amelyben sorra a prímek tízes számrendszerbeli alakját írjuk le, amelyeket megfelelő számú 0 jeggyel választunk el egymástól (hogy „biztosan ne érjenek egymásba"). Mutassuk meg, hogy

$$p_n = \left\lfloor 10^{2^{2^n}} c \right\rfloor - 10^{2^{2^n} - 2^{2^{n-1}}} \cdot \left\lfloor 10^{2^{2^{n-1}}} c \right\rfloor .$$

c) Miért nem alkalmazható a b)-beli formula p_n tényleges meghatározására?

5.1.10 Adjunk meg olyan K számot, amelyre igaz az alábbi állítás:
A $10^4 \le c \le 10^8$ feltételt kielégítő c számokra c akkor és csak akkor prím, ha $(c, K) = 1$.

5.2. Fermat- és Mersenne-prímek

Ebben a pontban a 2^k+1 és 2^k-1 alakú prímekkel foglalkozunk, az előbbieket *Fermat*-prímeknek, az utóbbiakat *Mersenne*-prímeknek nevezzük. Amint az előző pontban már említettük, megoldatlan, hogy létezik-e végtelen sok Fermat-, illetve Mersenne-prím.

Az 1.4.4 feladatban láttuk, hogy ha $2^k + 1$ prím, akkor k szükségképpen kettőhatvány, ha pedig $2^k - 1$ prím, akkor k maga is prím. Így elég az $F_n = 2^{2^n} + 1$ Fermat-számokat és az $M_p = 2^p - 1$ (ahol p prím) Mersenne-számokat vizsgálnunk.

Először a Fermat-számokkal foglalkozunk. Fermat azt hitte, hogy F_n mindig prímet ad (*nem* ez a híres Fermat-sejtés, azzal a 7. fejezetben foglalkozunk majd). A $0 \le n \le 4$ értékekre F_n valóban prím (ezek a prímek a 3, 5, 17, 257 és 65537), azonban Euler megmutatta, hogy $F_5 = 2^{32} + 1$ már összetett, ugyanis osztható 641-gyel.

2023-ban annyit tudunk, hogy F_n összetett szám $5 \le n \le 32$ és néhány nagyobb n esetén. A rekord $F_{18233954}$ (amely a tízes számrendszerben több, mint $10^{50000000}$ jegyből áll!), ez osztható $7 \cdot 2^{18233956} + 1$-gyel. (Az F_n Fermat-szám minden pozitív osztója $r2^{n+2}k+1$ alakú, ha $n \ge 2$, lásd az 5.2.1 Tételt.) Az $n > 4$ értékekre (egyelőre) nem találtak prímet az F_n számok között. Nem tudjuk, hogy F_{33} prím-e. Nem ismerjük F_{20} és F_{24} egyetlen nemtriviális

osztóját sem (noha tudjuk, hogy összetett számok). F_5, F_6 és F_7 prímtényezős felbontását megadjuk a könyv végén található, a Fermat-számokra vonatkozó táblázatban (rajtuk kívül csak F_8, F_9, F_{10} és F_{11} teljes felbontása ismert).

A Fermat-prímek a szabályos sokszögek szerkesztésénél játszanak szerepet: Gauss tétele szerint egy szabályos N-szög akkor és csak akkor szerkeszthető (euklideszi szerkesztéssel), ha $(3 \leq)N$ kanonikus alakja $N = 2^\alpha p_1 \dots p_r$, ahol $\alpha \geq 0$, $r \geq 0$ és a p_i számok különböző Fermat-prímek. Az első néhány érték $N = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, \dots$

A Fermat-számok vizsgálatában az alábbi két tétel nyújt gyakorlati szempontból is hasznos segítséget. Az 5.2.1 Tétel a Fermat-számok prímosztóinak keresését teszi hatékonyabbá, az 5.2.2 Tétel alapján pedig (viszonylag) gyorsan ellenőrizhető, hogy egy Fermat-szám prím-e vagy összetett.

5.2.1 Tétel **T 5.2.1**

F_n bármely (pozitív) osztója $k2^{n+1}+1$, sőt $n \geq 2$ esetén $r2^{n+2}+1$ alakú. ♣

Feltehetőleg Euler is ezt a tételt használta F_5 összetettségének a kimutatására: F_5 prímosztói csak a $128k+1$ alakú prímek közül kerülhetnek ki. Ezek közül az első kettő a 257 és a 641, és ez utóbbi osztója is F_5-nek.

Bizonyítás: Az állítást először arra az esetre igazoljuk, ha az osztó egy p prímszám. Ekkor $p \mid F_n$ átírható a

$$2^{2^n} \equiv -1 \pmod{p} \tag{1}$$

alakba. Ezt négyzetre emelve

$$2^{2^{n+1}} \equiv 1 \pmod{p} \tag{2}$$

adódik. A 3.2.2(i) Tétel szerint

$$2^j \equiv 1 \pmod{p} \iff o_p(2) \mid j.$$

Ennek megfelelően a (2) kongruenciából azt kapjuk, hogy

$$o_p(2) \mid 2^{n+1},$$

ugyanakkor az (1) kongruencia alapján

$$o_p(2) \nmid 2^n,$$

hiszen nyilván $p > 2$ és így $-1 \not\equiv 1 \pmod{p}$. Ebből következik, hogy

$$o_p(2) = 2^{n+1}.$$

Az $o_p(2) \mid p-1$ összefüggésből kapjuk, hogy $2^{n+1} \mid p-1$, azaz alkalmas k egésszel $p = k2^{n+1}+1$.

Ha $n \geq 2$, akkor az előzőek alapján egyúttal $p = 8s+1$ alakú, és így

$$\left(\frac{2}{p}\right) = 1, \qquad \text{azaz} \qquad 2^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Ebből következik, hogy

$$o_p(2) = 2^{n+1} \,\Big|\, \frac{p-1}{2} \ ,$$

vagyis alkalmas r egésszel $p = r2^{n+2}+1$.

A fenti eredményeket átírhatjuk $p \equiv 1 \pmod{2^{n+1}}$, illetve $n \geq 2$ esetén $p \equiv 1 \pmod{2^{n+2}}$ alakba is.

Legyen végül $d \mid F_n$ tetszőleges. Írjuk fel d-t (nem feltétlenül különböző) prímszámok szorzataként (ha $d > 1$): $d = p_1 \dots p_s$. Az előzőekben azt igazoltuk, hogy mindegyik i-re $p_i \equiv 1 \pmod{2^{n+1}}$. Ezeket a kongruenciákat összeszorozva kapjuk, hogy $d \equiv 1 \pmod{2^{n+1}}$ is teljesül. A 2^{n+2} modulusra vonatkozó állítás ugyanígy bizonyítható. ■

5.2.2 Tétel (Pepin-teszt) **T 5.2.2**

Az $n \geq 1$ esetben F_n akkor és csak akkor prím, ha

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \ \clubsuit \tag{3}$$

Bizonyítás: Tegyük fel először, hogy F_n prím. Ekkor (3) éppen azt jelenti, hogy a 3 kvadratikus nemmaradék modulo F_n, azaz

$$\left(\frac{3}{F_n}\right) = -1.$$

Ennek igazolásához felhasználjuk, hogy $n \geq 1$ miatt $2^{2^n} = 4^t$ alakú, és így

$$F_n \equiv 1 \pmod{4}, \qquad \text{továbbá} \qquad F_n = 4^t + 1 \equiv -1 \pmod{3}.$$

Ezért a kvadratikus reciprocitási tétel alapján

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{-1}{3}\right) = -1\,.$$

A megfordításhoz tegyük fel, hogy (3) teljesül. Ezt négyzetre emelve

$$3^{F_n-1} \equiv 1 \pmod{F_n} \tag{4}$$

adódik. A (4), illetve (3) kongruenciából

$$o_{F_n}(3) \mid F_n - 1, \qquad \text{illetve} \qquad o_{F_n}(3) \nmid \frac{F_n - 1}{2}$$

következik. Mivel $F_n - 1$ kettőhatvány, ezért ebből azt nyerjük, hogy

$$o_{F_n}(3) = F_n - 1.$$

Ez azt is jelenti, hogy $F_n - 1 \mid \varphi(F_n)$. Mivel $\varphi(F_n) \leq F_n - 1$, így csak $F_n - 1 = \varphi(F_n)$ lehetséges, ami azzal ekvivalens, hogy F_n prím. ■

Az 5.2.2 Tétel alapján $F_5 = 2^{32} + 1$ összetettségét a következőképpen lehet kimutatni: $3^{2^{31}}$ modulo F_5 vett maradékát 31 négyzetre emeléssel és az eredményt mindig modulo F_5 redukálva kiszámoljuk, és kiderül, hogy ez a maradék nem -1. Sőt, tulajdonképpen pusztán a kis Fermat-tétel segítségével is célhoz érhetünk: 32 ilyen négyzetre emeléses és redukciós lépéssel kapjuk, hogy

$$3^{F_5-1} = 3^{2^{32}} \not\equiv 1 \pmod{F_5},$$

tehát F_5 nem lehet prím. Így Fermat akár a saját tételével is megcáfolhatta volna a Fermat-számok prím voltára vonatkozó sejtését (az imént jelzett számolás mennyisége nem jelentett volna akadályt, hiszen abban a korban rendszeresen végeztek ennél jóval nagyobb számításokat is papírral és ceruzával).

Az 5.2.2 Tétel általában is hatékony eszközt jelent a Fermat-számok prím vagy összetett voltának az eldöntésére: a (3) feltétel teljesülését ismételt négyzetre emelésekkel (és az eredményt mindig modulo F_n redukálva) gyorsan ellenőrizni tudjuk, összesen $2^{n-1} \approx \log_2 F_n$ ilyen lépést kell végezni. Sajnos, a gyakorlati alkalmazásnak gátat szab az a tény, hogy a Fermat-számok iszonyú sebességgel nőnek, $F_n \approx F_{n-1}^2$, és így a legjobb számítógépek sem képesek megbirkózni már viszonylag kis n értékekkel sem.

Most rátérünk az $M_p = 2^p - 1$ (ahol p prím) Mersenne-számok vizsgálatára. Könnyen látszik, hogy ezek nem lesznek mindig prímek, a legkisebb összetett számot $p = 11$ esetén kapjuk:

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

A Mersenne-prímek jelentőségét többek között a páros tökéletes számokkal való kapcsolatuk adja, lásd a 6.3.2 Tételt. A névadó Mersenne a 17. század jelentős francia „tudományszervezője", Fermat, Descartes és más vezető tudósok intenzív levelezőpartnere volt, aki a minél nagyobb tökéletes számok előállítása reményében keresett ilyen típusú prímeket.

Mersenne jól tudta, hogy nagy számokról igen nehéz eldönteni, hogy prímek-e. 1644-ben megjelent könyvében ezt írja: „Ahhoz, hogy egy 15 vagy 20-jegyű számról megállapítsuk, prím-e vagy sem, egy egész élet ideje sem elég." Néhány oldallal arrébb ennek ellenére az alábbi állítás szerepel: 2^p-1 prím, ha $p=2,3,5,7,13,17,19,31,67,127,257$, de minden más 257-nél kisebb p értékre összetett.

Több mint kétszáz évig senki sem tudta, vajon Mersenne listája helyes-e vagy sem. Az első hibát 1876-ban(!) fedezte fel a szintén francia Lucas: megmutatta, hogy $2^{67}-1$ összetett. Itt külön érdekesség, hogy a számot nem sikerült tényezőkre bontania, csak az összetettség tényét igazolta (a részben róla elnevezett 5.2.4 Tétel segítségével). Végül 1903-ban az amerikai Cole találta meg a

$$193707721 \cdot 761838257287$$

felbontást, miután sok évig minden vasárnap délutánját ennek a problémának szentelte.

Mersenne listájában később további négy hibát találtak: a hiányzó $2^{61}-1$, $2^{89}-1$ és $2^{107}-1$ is prím, ugyanakkor $2^{257}-1$ összetett.

2023-ban 51 Mersenne-prímet ismertünk, ezek az alábbi p kitevőkhöz tartoznak: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609, 57885161, 74207281, 77232917, 82589933. Közülük az utolsó, a 2018-ban felfedezett $2^{82589933}-1$ a legnagyobb ismert prím. Ez a számóriás 24862048 számjegyből áll (tízes számrendszerben).

A könyv végén, a Mersenne-számokra vonatkozó táblázatban megadjuk a 10 és 100 közötti (prím) kitevőkhöz tartozó összetett Mersenne-számok prímtényezős felbontását.

Most az 5.2.1 és 5.2.2 Tételek Mersenne-számokra vonatkozó megfelelőit tárgyaljuk.

5.2.3 Tétel **T 5.2.3**

Legyen $p > 2$ prím. Ekkor M_p bármely (pozitív) osztója egyszerre $2kp+1$ és $8r \pm 1$ alakú. ♣

Példa: Legyen $p = 47$. Ekkor $M_{47} = 2^{47} - 1$ tetszőleges q prímosztója egyrészt $94k + 1$, másrészt $8r \pm 1$ alakú. Az így adódó

$$x \equiv 1 \pmod{94}, \qquad x \equiv \pm 1 \pmod{8}$$

szimultán kongruenciarendszereket megoldva

$$x \equiv 1 \text{ és } 95 \pmod{376}$$

adódik. Az ilyen alakú prímek

$$q = 1129,\ 1223,\ 2351,\ \ldots$$

Ezek közül $2351 \mid M_{47}$, tehát M_{47} összetett.

Könnyen lehet, hogy M_{47}-nek ezt a prímosztóját Mersenne is megtalálta, vagyis tudatosan hagyta ki a $p = 47$ értéket a listájáról (és nem csak arról van szó, hogy szerencsésen tippelt).

Bizonyítás: A Fermat-számoknál látottakhoz hasonlóan most is elég az állítást prímosztókra igazolni.

Tegyük fel, hogy a q prímre

$$q \mid 2^p - 1, \qquad \text{azaz} \qquad 2^p \equiv 1 \pmod{q}.$$

Ekkor $o_q(2) \mid p$, továbbá nyilván $o_q(2) \neq 1$, tehát $o_q(2) = p$.

Innen kapjuk, hogy $p \mid q-1$, azaz $q = tp+1$ alakú. Mivel q és p páratlan, ezért t páros, vagyis $q = 2kp + 1$ alakú.

A $q = 8r \pm 1$ állításhoz azt kell igazolnunk, hogy a 2 kvadratikus maradék mod q. Ez a $2^p \equiv 1 \pmod{q}$ kongruenciából p páratlanságának és a Legendre-szimbólum tulajdonságainak felhasználásával a következőképpen adódik:

$$\left(\frac{2}{q}\right) = \left(\frac{2}{q}\right)^p = \left(\frac{2^p}{q}\right) = \left(\frac{1}{q}\right) = 1\,. \ \blacksquare$$

5.2.4 Tétel (Lucas–Lehmer-teszt) **T 5.2.4**

Legyen $p > 2$ prím, továbbá $a_1 = 4$ és $a_{i+1} = a_i^2 - 2$, ha $i \geq 1$. Ekkor M_p pontosan akkor prím, ha

$$M_p \mid a_{p-1} \,. \ \clubsuit \tag{5}$$

Példa: Legyen $p = 5$. Ekkor

$$a_1 = 4, \quad a_2 = 14, \quad a_3 = 194 \equiv 8 \pmod{31} \quad \text{és} \quad a_4 \equiv 62 \equiv 0 \pmod{31},$$

tehát $M_5 = 31$ prím.

Az (5) feltétel teljesülésének ellenőrzésekor elég mindig az a_i-knek csak a modulo M_p vett maradékát kiszámítani, összesen $p - 2 \approx \log_2 M_p$ négyzetre emelési (valamint kivonási és redukciós) lépést kell végrehajtani.

Bizonyítás: Az $a + b\sqrt{3}$ (a, b egész) alakú számok a szokásos műveletekre egy (kommutatív, egységelemes, nullosztómentes) gyűrűt alkotnak, jelöljük ezt H-val. A bizonyításban a H-beli oszthatóság, kongruencia és rendfogalom elemi tulajdonságait használjuk fel (ezek H-ban is ugyanúgy érvényesek, mint az egész számoknál). Megjegyezzük, hogy H-ban a számelmélet alaptétele is igaz (lásd a 10.3.6 Tételt, illetve a 10.3.1 feladatot), azonban a bizonyítás során erre nem lesz szükségünk.

I. Teljes indukcióval könnyen igazolható, hogy bármely k-ra

$$a_k = (2 + \sqrt{3})^{2^{k-1}} + (2 - \sqrt{3})^{2^{k-1}} \,.$$

Ennek alapján az (5) feltétel ekvivalens az

$$M_p \mid (2 + \sqrt{3})^{2^{p-2}} + (2 - \sqrt{3})^{2^{p-2}} \tag{6}$$

oszthatósággal. A jobb oldalon $(2 - \sqrt{3})^{2^{p-2}}$-t kiemelve (6) átírható az alábbi alakba:

$$M_p \mid (2 - \sqrt{3})^{2^{p-2}} \Big((2 + \sqrt{3})^{2^{p-1}} + 1 \Big) \,. \tag{7}$$

Használjuk fel, hogy a (7)-beli oszthatóság pontosan akkor teljesül az egész számok körében, mint amikor H-ban (lásd az 5.2.10 feladatot), továbbá $(2 - \sqrt{3})(2 + \sqrt{3}) = 1$ miatt a $2 \pm \sqrt{3}$ számok egész kitevős hatványai egységek H-ban. Ennek megfelelően (7) és így (5) is ekvivalens a

$$(2 + \sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p} \tag{8}$$

kongruenciával.

Mindezek alapján az 5.2.4 Tétel átfogalmazható a következő alakba: M_p akkor és csak akkor prím, ha (8) teljesül.

II. Szükségünk lesz a következő lemmára: Ha $q > 3$ tetszőleges prímszám, akkor

$$(a + b\sqrt{3})^q \equiv a + \left(\frac{3}{q}\right) b\sqrt{3} \pmod{q}. \tag{9}$$

A lemma bizonyítása: A binomiális tétel alapján

$$(a + b\sqrt{3})^q = a^q + \binom{q}{1} a^{q-1} b\sqrt{3} + \binom{q}{2} a^{q-2} 3b^2 + \ldots + b^q 3^{(q-1)/2}\sqrt{3}. \tag{10}$$

A kis Fermat-tétel szerint

$$a^q \equiv a \pmod{q} \qquad \text{és} \qquad b^q \equiv b \pmod{q},$$

továbbá

$$\binom{q}{1}, \ \binom{q}{2}, \ \ldots, \ \binom{q}{q-1}$$

mindegyike osztható q-val, és végül

$$3^{(q-1)/2} \equiv \left(\frac{3}{q}\right) \pmod{q}.$$

Ezeket (10)-be beírva éppen (9) adódik.

III. Most megmutatjuk, hogy ha (8) fennáll, akkor M_p prím. A (8) kongruenciát négyzetre emelve kapjuk, hogy

$$(2 + \sqrt{3})^{2^p} \equiv 1 \pmod{M_p}. \tag{11}$$

Legyen q az M_p egy prímosztója (nyilván $q > 3$). Ekkor a (11) és (8) kongruenciák M_p helyett a q modulusra is teljesülnek. Ebből (az 5.2.1 és 5.2.2 Tételek bizonyításánál is használt gondolatmenet szerint) következik, hogy $o_q(2 + \sqrt{3}) = 2^p$.

Ha $\left(\frac{3}{q}\right) = 1$, akkor (9) felhasználásával kapjuk, hogy

$$(2 + \sqrt{3})^{q-1} = (2 - \sqrt{3})(2 + \sqrt{3})^q \equiv (2 - \sqrt{3})(2 + \sqrt{3}) = 1 \pmod{q},$$

és így

$$o_q(2 + \sqrt{3}) = 2^p \leq q - 1.$$

Ez azonban $q \le M_p = 2^p - 1$ miatt lehetetlen.

Ha $\left(\frac{3}{q}\right) = -1$, akkor hasonlóan adódik, hogy

$$(2+\sqrt{3})^{q+1} \equiv (2-\sqrt{3})(2+\sqrt{3}) = 1 \pmod{q},$$

és így

$$o_q(2+\sqrt{3}) = 2^p \le q+1.$$

Ezt a $q \le M_p = 2^p - 1$ egyenlőtlenséggel összevetve kapjuk, hogy $q = M_p$, vagyis M_p prím.

IV. Végül belátjuk, hogy ha M_p prím, akkor (8) teljesül.

Fel fogjuk használni, hogy $M_p \equiv -1 \pmod 8$ miatt

$$\left(\frac{2}{M_p}\right) = 1, \tag{12}$$

továbbá $M_p \equiv 1 \pmod 3$ és $M_p \equiv -1 \pmod 4$ alapján, a reciprocitási tétel felhasználásával

$$\left(\frac{3}{M_p}\right) = -\left(\frac{M_p}{3}\right) = -\left(\frac{1}{3}\right) = -1\,. \tag{13}$$

Induljunk ki a

$$2(2+\sqrt{3}) = (1+\sqrt{3})^2$$

egyenlőségből, és emeljük mindkét oldalt $(M_p+1)/2 = 2^{p-1}$-edik hatványra:

$$2^{(M_p+1)/2} \cdot (2+\sqrt{3})^{2^{p-1}} = (1+\sqrt{3})^{M_p+1}\,. \tag{14}$$

A (14) egyenlőség bal oldalának első tényezőjére (12)-t is felhasználva kapjuk, hogy

$$2^{(M_p+1)/2} = 2 \cdot 2^{(M_p-1)/2} \equiv 2\left(\frac{2}{M_p}\right) = 2 \pmod{M_p}, \tag{15}$$

a (14) jobb oldalán pedig a (9) kongruenciát az $a + b\sqrt{3} = 1 + \sqrt{3}$ és $q = M_p$ szereposztással alkalmazva, valamint (13)-at is felhasználva

$$\begin{aligned}(1+\sqrt{3})^{M_p+1} &= (1+\sqrt{3})(1+\sqrt{3})^{M_p} \equiv (1+\sqrt{3})\left(1+\left(\frac{3}{M_p}\right)\sqrt{3}\right) = \\ &= (1+\sqrt{3})(1-\sqrt{3}) = -2 \pmod{M_p}\end{aligned} \tag{16}$$

adódik. A (15) és (16) összefüggéseket (14)-be beírva azt nyerjük, hogy

$$2(2+\sqrt{3})^{2^{p-1}} \equiv -2 \pmod{M_p}\,. \tag{17}$$

Szorozzuk meg (17)-et 2^{p-1}-gyel. Ekkor $2^p \equiv 1 \pmod{M_p}$ miatt éppen a bizonyítani kívánt (8) kongruenciához jutunk. ■

Feladatok

5.2.1

a) Igazoljuk, hogy $F_{n+1} = F_0F_1 \dots F_n + 2$.

b) Mutassuk meg, hogy a Fermat-számok páronként relatív prímek (vö. az 1.3.14 feladattal).

c) A b) rész felhasználásával adjunk új bizonyítást arra, hogy a prímek száma végtelen.

d) Adjunk új bizonyítást az 5.1.9a feladat állítására.

5.2.2 Bizonyítsuk be, hogy az 5.2.2 Tétel $n \geq 2$ esetén akkor is érvényben marad, ha a (3) képletben a 3 helyére 5-öt vagy 10-et írunk.

5.2.3 Legyen $n \geq 2$. Mutassuk meg, hogy $K_n = 5 \cdot 2^n + 1$ akkor és csak akkor prím, ha

$$3^{(K_n-1)/2} \equiv -1 \pmod{K_n}.$$

5.2.4 Bizonyítsuk be, hogy $\varphi(N)$ akkor és csak akkor kettőhatvány, ha $N = 2^\alpha p_1 \dots p_r$, ahol $\alpha \geq 0$, $r \geq 0$ és a p_i számok különböző Fermat-prímek.

M 5.2.5 Hány olyan k létezik, amelyre szabályos $2^k - 1$-szög szerkeszthető?

5.2.6 Keressük meg az alábbi számok legkisebb prímosztóját:

a) $2^{23} - 1$; b) $2^{29} - 1$; c) $2^{37} - 1$; d) $2^{43} - 1$.

M 5.2.7 Bizonyítsuk be, hogy M_p akkor és csak akkor osztható $2p + 1$-gyel, ha $2p + 1$ prím és $p \equiv 3 \pmod 4$. (Illusztráció: $11 \equiv 3 \pmod 4$, $2 \cdot 11 + 1 = 23$ prím, és valóban $23 \mid 2^{11} - 1$.)

5.2.8 Tegyük fel, hogy egy q prímszámra q^2 osztója egy Fermat-számnak vagy egy Mersenne-számnak. Mutassuk meg, hogy ekkor

$$2^{q-1} \equiv 1 \pmod{q^2}.$$

Megjegyzés: Megoldatlan probléma, hogy a feladat feltétele egyáltalán teljesülhet-e; könnyen elképzelhető ugyanis, hogy valamennyi Fermat- és Mersenne-szám négyzetmentes. Az is megoldatlan, hogy a fenti kongruenciát egyáltalán hány q prím elégíti ki, nem kizárt, hogy a jelenleg ismert 1093-on és 3511-en kívül nincs is több ilyen tulajdonságú q.

M 5.2.9 A 8 és a 9, a 16 és a 17, illetve a 31 és a 32 szomszédos prímhatványok (a prímeket is prímhatványnak tekintjük). Jellemezzük az összes ilyen $n, n + 1$ számpárt.

5.2.10 Jelölje H az $a+b\sqrt{3}$ (a, b egész) alakú számok gyűrűjét (lásd az 5.2.4 Tétel bizonyítását), és legyenek k és n egész számok. Mutassuk meg, hogy a $k \mid n$ oszthatóság akkor és csak akkor teljesül H-ban, ha az egész számok körében is fennáll.

*5.2.11 Az is megoldatlan probléma, hogy a Fermat-számok között végtelen sok összetett szám van-e. Ugyanígy megoldatlan, hogy a $H_n = 6^{2^n}+1$ számok között végtelen sok prím, illetve hogy végtelen sok összetett szám található-e. Mutassuk meg azonban, hogy az F_n és H_n számsorozatok közül legalább az egyikben végtelen sok összetett szám fordul elő.

5.3. Prímszámok számtani sorozatokban

Számtani sorozaton egész számokból álló, pozitív differenciájú, végtelen számtani sorozatot fogunk érteni:

$$a + kd, \qquad \text{ahol } d > 0 \text{ és } a \text{ egészek}, \quad k = 0, 1, 2, \ldots$$

Az 5.1 pontban láttuk, hogy egy ilyen sorozat nem állhat csupa prímszámból. Ha $(a, d) = t > 1$, akkor a sorozat minden eleme osztható t-vel, így a sorozatban legfeljebb egy (pozitív) prím található. Ha azonban $(a, d) = 1$, akkor a sorozatban végtelen sok prím fordul elő:

5.3.1 Tétel (Dirichlet-tétel) **T 5.3.1**

Ha a $d > 0$ és a egészek relatív prímek, akkor az $a + kd$, $k = 0, 1, 2, \ldots$ számtani sorozat végtelen sok prímet tartalmaz. ♣

Ezt a tételt teljes általánosságában nem bizonyítjuk be, csak néhány speciális esetét igazoljuk.

5.3.2 Tétel **T 5.3.2**

A $4k + 3$ alakú prímek száma végtelen. ♣

Bizonyítás: Az 5.1.1 Tétel bizonyításának a gondolatmenetét követjük. Tegyük fel indirekt, hogy csak véges sok ilyen prímszám létezik, legyenek ezek $p_1 = 3, \ldots, p_r$. Tekintsük az $A = 4p_1 \ldots p_r - 1$ számot.

Az A nyilván nem osztható a $p_1, \ldots, p_r$ prímek egyikével sem.

Írjuk fel A-t prímtényezők szorzatatként: $A = q_1 \ldots q_s$ ($s = 1$, illetve $q_i = q_j$ is megengedett). Mivel A páratlan, ezért mindegyik $q_i > 2$. Továbbá

nem lehet minden $q_i \equiv 1 \pmod 4$, ugyanis ezeket a kongruenciákat összeszorozva $A \equiv 1 \pmod 4$ adódna, ami ellentmondás. Ebből következik, hogy a q_i prímek között kell lennie $4k+3$ alakúnak is. Ez szükségképpen különbözik a $p_1, \ldots, p_r$ prímektől, ami ellentmond az indirekt feltevésnek. ■

5.3.3 Tétel **T 5.3.3**

A $4k+1$ alakú prímek száma végtelen. ♣

Bizonyítás: Az euklideszi gondolatmenetet tovább kell finomítanunk. Tegyük fel indirekt, hogy csak véges sok ilyen prímszám létezik, legyenek ezek $p_1 = 5, \ldots, p_r$. Tekintsük az $A = (2p_1 \ldots p_r)^2 + 1$ számot.

Az A nyilván nem osztható a $p_1, \ldots, p_r$ prímek egyikével sem.

Legyen q az A tetszőleges prímosztója. Nyilván $q > 2$. A $q \mid A$ oszthatóságot átírhatjuk a

$$(2p_1 \ldots p_r)^2 \equiv -1 \pmod q$$

alakba. Ebből következik, hogy az $x^2 \equiv -1 \pmod q$ kongruencia megoldható, vagyis $q \equiv 1 \pmod 4$. Így egy újabb $4k+1$ alakú prímet találtunk, ami ellentmondás. ■

A kvadratikus kongruenciák felhasználásával a Dirichlet-tétel számos további speciális esete is elintézhető, lásd az 5.3.3 feladatot.

Most a Dirichlet-tételt tetszőleges olyan számtani sorozatra igazoljuk, amelynek a kezdőtagja 1:

5.3.4 Tétel **T 5.3.4**

Bármely rögzített $m > 0$ esetén az $mk+1$, $k = 0, 1, 2, \ldots$ számok között végtelen sok prím található. ♣

Bizonyítás: Fel fogjuk használni a körosztási polinomokra és a polinomok többszörös gyökeire vonatkozó alábbi összefüggéseket:

(i) Az m-edik körosztási polinom, Φ_m, az az 1 főegyüttható polinom, amelynek gyökei az m-edik primitív komplex egységgyökök. Φ_m fokszáma tehát $\varphi(m)$. Példák:

$$\Phi_4 = x^2 + 1, \qquad \Phi_{11} = x^{10} + x^9 + \ldots + 1.$$

Megmutatható, hogy Φ_m egész együtthatós, továbbá

$$\Phi_m \mid x^m - 1, \quad \text{sőt} \quad x^m - 1 = \prod_{d \mid m} \Phi_d \,. \tag{1}$$

(ii) Legyen T tetszőleges kommutatív test, $f \in T[x]$. Az $\alpha \in T$ elemet az f polinom többszörös gyökének nevezzük, ha $(x-\alpha)^2 \mid f$. Ez pontosan akkor teljesül, ha $f(\alpha) = f'(\alpha) = 0$, ahol f' az f polinom (formálisan képzett) deriváltját jelöli.

Az iménti fogalmak és tételek felhasználásával először az alábbi, önmagában is érdekes lemmát igazoljuk:

Legyen c egész szám és q prímszám. Ekkor

$$o_q(c) = m \iff q \mid \Phi_m(c) \text{ és } q \nmid m. \tag{2}$$

A lemma bizonyítása:

Tegyük fel, hogy $o_q(c) = m$. Ekkor $m \mid q-1$, és így nyilván $q \nmid m$.

Helyettesítsünk (1)-ben x helyére c-t:

$$c^m - 1 = \prod_{d \mid m} \Phi_d(c). \tag{3}$$

Mivel $o_q(c) = m$, ezért $c^m \equiv 1 \pmod q$, és így (3) bal oldala osztható q-val. A q prím, tehát a jobb oldalon is valamelyik $\Phi_d(c)$ tényező osztható q-val. Ekkor $\Phi_d(c) \mid c^d - 1$ miatt $c^d \equiv 1 \pmod q$ valamelyik $d \mid m$-re. Mivel $o_q(c) = m$, ezért csak $d = m$ lehetséges, vagyis valóban $q \mid \Phi_m(c)$.

A megfordításnál a $q \mid \Phi_m(c)$ és $q \nmid m$ feltételekből indulunk ki. Ekkor $\Phi_m(c) \mid c^m - 1$ miatt $c^m \equiv 1 \pmod q$. Tegyük fel indirekt, hogy $o_q(c) = t < m$. Ekkor $t \mid m$ és $c^t \equiv 1 \pmod q$. A (3) összefüggést m helyett t-re alkalmazva azt kapjuk, hogy van olyan $d \mid t$, amelyre $q \mid \Phi_d(c)$. Ez azt jelenti, hogy az eredeti (3) jobb oldalán legalább két tényező osztható q-val.

A továbbiakban az (1)-beli $x^m - 1 = \prod_{d \mid m} \Phi_d$ egyenlőséget a $\mathbf{Z}_q$ modulo q test felett fogjuk tekinteni. Ebben a felfogásban az előző bekezdés utolsó mondata úgy fogalmazható meg, hogy a c (mint $\mathbf{Z}_q$-beli elem) a $\prod_{d \mid m} \Phi_d$ szorzat legalább két tényezőjének gyöke. Mivel ez a szorzat $x^m - 1$-gyel egyenlő, ezért a c legalább kétszeres gyöke az $f = x^m - 1 \in \mathbf{Z}_q[x]$ polinomnak. Ekkor (ii) szerint $f'(c) = mc^{m-1} = 0$ ($\mathbf{Z}_q$-ban).

Mivel $q \nmid m$ és $q \nmid c$, azaz a $\mathbf{Z}_q$ testben $m \neq 0$ és $c \neq 0$, ezért mc^{m-1} sem lehet 0, ami ellentmond az előzőknek. Ezzel a lemma bizonyítását befejeztük.

Rátérve az 5.3.4 Tétel bizonyítására, tegyük fel indirekt, hogy csak véges sok $mk+1$ alakú prím van (esetleg egy sincs), legyenek ezek $p_1, \dots, p_r$. Legyen $c = vmp_1 \dots p_r$, ahol v tetszőleges pozitív egész ($r = 0$-ra $c = vm$). Nyilván elég nagy v esetén $\Phi_m(c) > 1$.

Legyen q a $\Phi_m(c)$ egy tetszőleges prímosztója. Ekkor $\Phi_m(c) \mid c^m - 1$ miatt $(q, c) = 1$, és ennélfogva $q \nmid m$ is teljesül. Így a lemma szerint $o_q(c) = m$.

Ebből következik, hogy $m \mid q-1$, azaz $q = mk+1$ alakú. Végül $(q,c) = 1$ miatt $q \neq p_i$, ami ellentmond annak, hogy $p_1, \ldots, p_r$ az összes $mk+1$ alakú prím. ■

Feladatok

5.3.1 A modulo 9999 maradékosztályok közül hányban található pozitív prímszám?

5.3.2 Miért nem lehet az 5.3.2 Tétel bizonyítását közvetlenül átvinni az 5.3.3 Tételre is, $A = 4p_1 \ldots p_r + 1$-et véve?

5.3.3 Az általános Dirichlet-tétel felhasználása nélkül mutassuk meg, hogy az alábbi számtani sorozatokban végtelen sok prímszám van:

a) $6k+5$; b) $8k+3$; c) $8k+5$; d) $8k+7$;
e) $10k+9$; f) $12k+5$; g) $12k+7$; h) $12k+11$.

5.3.4 Hány olyan prímszám létezik, amelynek tízes számrendszerben az utolsó négy számjegye 4321?

5.3.5 Írjuk le a tizedesvessző után rendre a prímszámokat. Bizonyítsuk be, hogy az így keletkező 0,235 711 131 719 ... szám irracionális.

5.3.6 Mely a, b, c pozitív egészek esetén lesz végtelen sok prím az $a+bk+cn$ alakú számok között, ahol $k = 0, 1, 2, \ldots,\ n = 0, 1, 2, \ldots$?

5.3.7

a) Mutassuk meg, hogy minden $c \neq 0$ egészhez létezik olyan p prím, amelyre a c kvadratikus maradék mod p.

b) Mely c egészekhez létezik olyan p prím, amelyre a c kvadratikus nemmaradék mod p?

5.3.8 Bizonyítsuk be, hogy minden $n > 1$-hez található olyan n-edfokú egész együtthatós f polinom, amely reducibilis a racionális test felett, és alkalmas $v_1, \ldots, v_n$ (különböző) pozitív egészek mindegyikére $f(v_i)$ pozitív prímszám.

5.3.9 Mutassuk meg (az általános Dirichlet-tétel felhasználása nélkül), hogy ha bármely a és d relatív prím pozitív egészek esetén létezik $a+kd$ alakú prím, akkor mindig végtelen sok ilyen prím is létezik. (Ez azt jelenti, hogy az általános Dirichlet-tétel bizonyításánál az igazi nehézséget nem a végtelen sok prím garantálása okozza, hanem az, hogy egyáltalán van a kívánt alakú prímszám.)

5.4. Becslések $\pi(x)$-re

Az x-nél nem nagyobb (pozitív) prímek számát $\pi(x)$-szel jelöljük. Például $\pi(1) = 0$, $\pi(6{,}7) = 3$, $\pi(20) = 8$. Nyilván elég $\pi(x)$-nek a pozitív egész x-eken felvett értékeivel foglalkozni.

Annak ellenére, hogy a prímek igen szabálytalanul helyezkednek el a természetes számok között, a $\pi(x)$ függvény közelítő viselkedése jól leírható. Ez az ún. prímszámtétel, amelyet bizonyítás nélkül közlünk:

5.4.1 Tétel (Prímszámtétel) **T 5.4.1**

Jelölje log a természetes logaritmust. Ekkor

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1\,,$$

azaz $\pi(x)$ és $\frac{x}{\log x}$ aszimptotikusan egyenlők. ♣

Megjegyzések: 1. A prímszámtétel a $\pi(x)$ és $\frac{x}{\log x}$ mennyiségek *arány*ára, és nem a *különbség*ére vonatkozik, ez utóbbi akármilyen nagy is lehet.

2. A prímszámtétel azt fejezi ki, hogy x-ig „körülbelül” $\frac{x}{\log x}$ prím van. Hogy ez „sok” vagy „kevés”, az attól függ, mihez hasonlítjuk. Az összes pozitív egészhez viszonyítva a prímszámok „ritkán” helyezkednek el, hiszen

$$\lim_{x\to\infty} \frac{\pi(x)}{\lfloor x\rfloor} = \lim_{x\to\infty} \frac{\frac{x}{\log x}}{x} = \lim_{x\to\infty} \frac{1}{\log x} = 0\,.$$

Ugyanakkor a prímszámok sokkal „sűrűbben” fordulnak elő, mint például a négyzetszámok, hiszen az utóbbiak száma x-ig $\lfloor\sqrt{x}\rfloor$, és

$$\lim_{x\to\infty} \frac{\pi(x)}{\lfloor\sqrt{x}\rfloor} = \lim_{x\to\infty} \frac{\frac{x}{\log x}}{\sqrt{x}} = \lim_{x\to\infty} \frac{\sqrt{x}}{\log x} = \infty\,.$$

3. A prímszámtételt először a 18. század végén sejtette meg egymástól függetlenül Legendre és Gauss. Gauss ekkor csak 15 éves volt, és az ő sejtésében az $x/\log x$ függvény helyett a

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

logaritmikus integrál szerepelt, amelyről később kiderült, hogy a $\pi(x)$-et az $x/\log x$-nál még sokkal pontosabban közelíti. A prímszámtétel bizonyításához

vezető utat mintegy 70 évvel később Riemann jelölte ki, a bizonyítás pedig először de la Vallée Poussinnek és Hadamard-nak sikerült egymástól függetlenül 1896-ban. 1949-ben Erdős és Selberg talált ún. elemi (azaz mélyebb analízist nem használó) bizonyítást a prímszámtételre.

A prímszámtételből könnyen nyerhetünk aszimptotikát az n-edik prímszámra:

5.4.2 Tétel **T 5.4.2**

Jelölje p_n az n-edik prímszámot. Ekkor

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1\,. \ \clubsuit \tag{1}$$

Bizonyítás: Mivel $\pi(p_n) = n$, így a prímszámtétel szerint

$$\lim_{n\to\infty} \frac{\pi(p_n)}{\frac{p_n}{\log p_n}} = \lim_{n\to\infty} \frac{n \log p_n}{p_n} = 1\,. \tag{2}$$

Az (1) bal oldalán szereplő sorozat reciproka

$$\frac{n \log n}{p_n} = \frac{n \log p_n}{p_n} \cdot \frac{\log n}{\log p_n} \tag{3}$$

alakba írható, ezért (2) alapján (1) igazolásához azt kell megmutatni, hogy (3) jobb oldalán a második tört határértéke is 1, azaz

$$\lim_{n\to\infty} \frac{\log n}{\log p_n} = 1\,. \tag{4}$$

Ha a (2) összefüggést „logaritmáljuk”, akkor

$$\lim_{n\to\infty} \log\left(\frac{n \log p_n}{p_n}\right) = \lim_{n\to\infty} \big(\log n + \log\log p_n - \log p_n\big) = 0 \tag{5}$$

adódik. Mivel $1/(\log p_n)$ korlátos, így (5)-ből kapjuk, hogy

$$\lim_{n\to\infty} \left(\frac{\log n}{\log p_n} + \frac{\log\log p_n}{\log p_n} - 1\right) = 0\,. \tag{6}$$

Itt

$$\lim_{n\to\infty} \frac{\log\log p_n}{\log p_n} = 0\,,$$

ezért (6)-ból következik (4), és így (1) is. ■

A pont hátralevő részében egy, a prímszámtételnél gyengébb eredményt bizonyítunk:

5.4.3 Tétel **T 5.4.3**

Léteznek olyan c_1 és c_2 pozitív konstansok és olyan x_0, hogy minden $x \geq x_0$ esetén

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} . \clubsuit \tag{7}$$

Megjegyzések: 1. Az 5.4.3 Tétel azt fejezi ki, hogy a $\pi(x)$ „nagyságrendje" megegyezik az $x/\log x$ függvény nagyságrendjével. Számos kérdés tisztázásához már ez a tétel is elegendő, lásd például az 5.4.1 Tétel utáni 2. megjegyzésben szereplő sűrűségi összehasonlításokat.

2. Az 5.4.1 és 5.4.3 Tételeket összevetve, a prímszámtétel szerint a $\pi(x)$ és $x/\log x$ függvények hányadosa 1-hez tart, az 5.4.3 Tétel pedig azt állítja, hogy ez a hányados (elég nagy x-ekre) két pozitív konstans közé esik. Ebből rögtön következik, hogy az 5.4.3 Tételben a (7) egyenlőtlenség eleve csak olyan c_1, c_2 konstansokkal lehet igaz, amelyekre $c_1 \leq 1$ és $c_2 \geq 1$. Továbbá, a prímszámtétel éppen azt jelenti, hogy az 5.4.3 Tétel becslései *bármely* $0 < c_1 < 1$ és $c_2 > 1$ konstansokkal fennállnak, azaz *bármely* $0 < c_1 < 1$ és $c_2 > 1$ konstansokhoz található olyan x_0, hogy a (7) egyenlőtlenség minden $x \geq x_0$-ra teljesüljön. (Sőt, azt is bebizonyították, hogy $c_1 = 1$ is választható.)

3. Az 5.4.3 Tételben $x_0 = 2$ is vehető („rosszabb" c_1 és c_2 „árán"), lásd az 5.4.2 feladatot.

4. Az 5.4.3 Tételt először Csebisev bizonyította be 1850-ben. Az alábbiakban az alsó becslésre Erdős, a felső becslésre pedig Erdős és Kalmár közös bizonyítását mutatjuk be.

Bizonyítás: I. Alsó becslés $\pi(x)$-re.

Szükségünk lesz az alábbi segédtételre:

5.4.4 Lemma **L 5.4.4**

Az $\binom{n}{k}$ binomiális együttható bármely prímhatvány osztója kisebb vagy egyenlő, mint n. $\clubsuit$

A lemma bizonyítása: Legyen $\binom{n}{k}$ kanonikus alakja

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \prod_{p \leq n} p^{\beta_p} . \tag{8}$$

Azt kell igazolnunk, hogy $p^{\beta_p} \leq n$, azaz $\beta_p \leq \lfloor \log_p n \rfloor$.

Tekintsünk egy rögzített p prímet, és jelöljük $\lfloor \log_p n \rfloor$ értékét t-vel. A p kitevőjét $n!$-ban, $k!$-ban és $(n-k)!$-ban a Legendre-formulával (1.6.8 Tétel) határozhatjuk meg. Ennek alapján $\binom{n}{k}$-ban a p kitevője

$$\begin{aligned}\beta_p = \quad & \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^t} \right\rfloor - \\ - & \left\lfloor \frac{k}{p} \right\rfloor - \left\lfloor \frac{k}{p^2} \right\rfloor - \ldots - \left\lfloor \frac{k}{p^t} \right\rfloor - \\ & - \left\lfloor \frac{n-k}{p} \right\rfloor - \left\lfloor \frac{n-k}{p^2} \right\rfloor - \ldots - \left\lfloor \frac{n-k}{p^t} \right\rfloor \quad .\end{aligned}$$

Itt mind a t oszlopban az egymás alatt álló tagok előjeles összege $\lfloor a+b \rfloor - \lfloor a \rfloor - \lfloor b \rfloor$ alakú. Könnyen látható, hogy egy ilyen előjeles összeg értéke mindig 0 vagy 1 (lásd az 5.4.1 feladatot), és így $\beta_p \le t$. ■

Most rátérünk $\pi(x)$ alsó becslésének a bizonyítására. A (8) jobb oldalán (legfeljebb) $\pi(n)$ darab prímhatvány szorzata áll, és az 5.4.4 Lemma alapján ezek mindegyike kisebb vagy egyenlő, mint n. Ebből azonnal következik, hogy

$$\binom{n}{k} = \prod_{p \le n} p^{\beta_p} \le n^{\pi(n)} \,. \tag{9}$$

A (9) egyenlőtlenségeket $k = 0, 1, \ldots, n$-re összegezve a

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \le (n+1) n^{\pi(n)}$$

egyenlőtlenséghez jutunk. Ezt logaritmálva

$$n \log 2 \le \log(n+1) + \pi(n) \log n$$

adódik, ahonnan $\pi(n)$-et kifejezve kapjuk, hogy

$$\pi(n) \ge \log 2 \cdot \frac{n}{\log n} - \frac{\log(n+1)}{\log n} \,. \tag{10}$$

Mivel (10) jobb oldalán a második tag korlátos, ezért elég nagy n-re kisebb, mint (például) $0{,}01n/\log n$, és így

$$\pi(n) \; > \; (\log 2 - 0{,}01) \frac{n}{\log n} \,.$$

II. Felső becslés $\pi(x)$-re.

Itt is szükségünk lesz egy segédtételre, amely az n-nél nem nagyobb prímszámok szorzatára ad felső becslést:

5.4.5 Lemma **L 5.4.5**

Tetszőleges $n > 0$ egészre

$$\prod_{\substack{p\le n\\ (p\ \text{prím})}} p \;<\; 4^n\,. \;\clubsuit \tag{11}$$

A lemma bizonyítása: Az állítást teljes indukcióval igazoljuk.

Az $n = 1, 2$ és 3 értékekre (11) nyilván teljesül.

Tegyük fel, hogy az egyenlőtlenség az $n = 1, 2, \ldots, m$ értékek ($m \ge 3$) esetén teljesül, és megmutatjuk, hogy ekkor $n = m + 1$-re is fennáll.

Ha m páratlan, akkor $m+1$ egy 2-nél nagyobb páros szám, tehát összetett. Így az indukciós feltevést $n = m$-re alkalmazva kapjuk, hogy

$$\prod_{p\le m+1} p = \prod_{p\le m} p \;<\; 4^m \;<\; 4^{m+1}\,.$$

Legyen most m páros, $m = 2k$, azaz $m + 1 = 2k + 1$. Ekkor a kérdéses szorzatot a következőképpen bontjuk két részre:

$$\prod_{p\le 2k+1} p = \prod_{p\le k+1} p \;\cdot \prod_{k+2\le p\le 2k+1} p. \tag{12}$$

A (12) jobb oldalán szereplő első tényezőre az $n = k+1$-re vonatkozó indukciós feltevés szerint

$$\prod_{p\le k+1} p \;<\; 4^{k+1}\,. \tag{13}$$

A (12) jobb oldalán levő második tényezőt a $\binom{2k+1}{k}$ binomiális együttható segítségével becsüljük. Mivel

$$\binom{2k+1}{k} = \frac{(2k+1)(2k)\ldots(k+2)}{k!}$$

számlálójában minden $k+2 \le p \le 2k+1$ prímszám szerepel, azonban a nevező ezen prímek egyikével sem osztható, ezért $\binom{2k+1}{k}$ (mely egész szám) osztható ezen prímek mindegyikével, vagyis a szorzatukkal is. Azaz

$$\prod_{k+2\le p\le 2k+1} p \;\Big|\; \binom{2k+1}{k}\,,$$

és így

$$\prod_{k+2\le p\le 2k+1} p \le \binom{2k+1}{k}. \tag{14}$$

Továbbá

$$\binom{2k+1}{k} = \frac{1}{2}\left(\binom{2k+1}{k} + \binom{2k+1}{k+1}\right) < \frac{1}{2}\cdot 2^{2k+1} = 4^k. \tag{15}$$

A (14) és (15) egyenlőtlenségekből

$$\prod_{k+2\le p\le 2k+1} p < 4^k \tag{16}$$

következik. Végül (13)-at és (16)-ot (12)-be beírva kapjuk a kívánt

$$\prod_{p\le 2k+1} p < 4^{2k+1}$$

egyenlőtlenséget. ■

Most rátérünk $\pi(x)$ felső becslésének a bizonyítására. A (11) egyenlőtlenség bal oldalán a tényezők száma $\pi(n)$. Mivel $\pi(n)$-re felső becslést keresünk, az első ötlet az, hogy minden tényező helyére a legkisebb prímet, a 2-t írjuk. Ebből azonban sajnos csak

$$2^{\pi(n)} < \prod_{p\le n} p < 4^n$$

következik, ami a (triviálisnál is rosszabb) $\pi(n) < 2n$ becslést adja.

A javítás kulcsa az, hogy a (11) bal oldalán álló szorzatot úgy csökkentjük, hogy először elhagyjuk a kis prímeket, majd (lényegében) a megmaradó tényezők legkisebbikét írjuk mindegyik tényező helyére:

$$\prod_{p\le n} p \ge \prod_{\sqrt{n}<p\le n} p \ge \sqrt{n}^{\pi(n)-\pi(\sqrt{n})}. \tag{17}$$

A (17) és (11) egyenlőtlenségeket összevetve

$$\sqrt{n}^{\pi(n)-\pi(\sqrt{n})} < 4^n$$

következik. Ezt logaritmálva

$$\big(\pi(n)-\pi(\sqrt{n})\big)\log(\sqrt{n})<n\log 4$$

adódik, ahonnan $\pi(n)$-et kifejezve kapjuk, hogy

$$\pi(n)\;<\;2\cdot\log 4\cdot\frac{n}{\log n}+\pi(\sqrt{n})\,. \tag{18}$$

Végül, mivel $\pi(\sqrt{n})<\sqrt{n}$, és

$$\lim_{n\to\infty}\frac{\sqrt{n}}{\frac{n}{\log n}}=\lim_{n\to\infty}\frac{\log n}{\sqrt{n}}=0\,,$$

ezért elég nagy n-re $\pi(\sqrt{n})$ kisebb, mint (például) $0{,}01n/\log n$, és így (18)-ból

$$\pi(n)<(2\log 4+0{,}01)\frac{n}{\log n}$$

következik. ■

Feladatok

A feladatokban p prímszámot jelöl, p_n az n-edik prímszám, és $u_n\sim v_n$ azt jelenti, hogy u_n és v_n aszimptotikusan egyenlő, azaz $\lim_{n\to\infty}u_n/v_n=1$.

5.4.1 Igazoljuk, hogy az $\lfloor a+b\rfloor-\lfloor a\rfloor-\lfloor b\rfloor$ kifejezés értéke bármely a,b valós szám esetén 0 vagy 1.

5.4.2 Mutassuk meg, hogy az 5.4.3 Tételben $x_0=2$ is vehető, azaz alkalmas c_1' és c_2' pozitív konstansokkal a (7)-nek megfelelő egyenlőtlenség minden $x\geq 2$ valós számra teljesül.

*5.4.3 Milyen alsó és felső becsléseket nyerhetünk p_n-re, ha (az 5.4.1 Tétel helyett) az 5.4.3 Tételt használjuk fel?

5.4.4 Igazoljuk a prímszámtétel felhasználásával a következő becsléseket.

a) $\sum_{p\leq n}\log p\sim n$.

b) Az n-nél nem nagyobb prímek szorzata „körülbelül” e^n az alábbi értelemben (vö. az 5.4.5 Lemmával): Bármely $\varepsilon>0$ esetén létezik olyan n_0, hogy minden $n>n_0$-ra

$$e^{(1-\varepsilon)n}\;<\;\prod_{p\leq n}p\;<\;e^{(1+\varepsilon)n}\,.$$

*5.4.5 Legyen $1 \le a_1 < a_2 < \dots$ a természetes számok tetszőleges részsorozata, és jelölje $A(n)$ a sorozat n-nél nem nagyobb elemeinek a számát, azaz $A(n) = \sum_{a_i \le n} 1$. Bizonyítsuk be, hogy az alábbi négy állítás ekvivalens.

(i) $A(n) \sim n/\log n$.

(ii) $a_n \sim n \log n$.

(iii) $\sum_{a_i \le n} \log a_i \sim n$.

(iv) Bármely $\varepsilon > 0$ esetén létezik olyan n_0, hogy minden $n > n_0$-ra

$$e^{(1-\varepsilon)n} < \prod_{a_i \le n} a_i < e^{(1+\varepsilon)n}.$$

Megjegyzés: A feladat azt mutatja, hogy az 5.4.1 és 5.4.2 Tételekben, valamint az 5.4.4 feladatban szereplő állítások a prímszámok sorozatánál általánosabb sorozatok esetén is szorosan összefüggnek egymással.

*5.4.6 Jelöljük $S(n)$-nel az n-nél nem nagyobb prímszámok összegét, azaz $S(n) = \sum_{p \le n} p$. Bizonyítsuk be az alábbi becsléseket $S(n)$-re:

a) Léteznek olyan c_3 és c_4 pozitív konstansok, hogy minden $n > 1$-re

$$c_3 \frac{n^2}{\log n} < S(n) < c_4 \frac{n^2}{\log n}.$$

b) $S(n) \sim n^2/(2 \log n)$.

5.4.7

a) Mutassuk meg, hogy bármely K-hoz található olyan páros szám, amely legalább K-féleképpen írható fel két prímszám összegeként.

b) Lássuk be a hasonló állítást összeg helyett különbségre is.

5.4.8 Igazoljuk, hogy

$$\pi(n) = \sum_{j=2}^{n} \left(\left\lfloor \frac{(j-1)! + 1}{j} \right\rfloor - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right).$$

alkalmas-e ez a képlet a $\pi(n)$ gyakorlati kiszámítására?

5.5. Hézag a szomszédos prímek között

Először megmutatjuk, hogy a szomszédos prímszámok között tetszőlegesen nagy hézagok is előfordulnak:

5.5.1 Tétel **T 5.5.1**

Bármely K pozitív egészhez meg lehet adni K egymást követő összetett számot. ♣

Bizonyítás: Legyen $N > K$ tetszőleges, és tekintsük az $a_i = N! + i$ számokat, $i = 2, 3, \ldots, K+1$. Ekkor nyilván $i \mid a_i$ és $a_i > i$, tehát valamennyi a_i összetett. ■

Megjegyzés: A bizonyításban $N!$ helyett az N-nél nem nagyobb prímek szorzatát is vehettük volna.

Az 5.5.1 Tételt általánosítva most azt bizonyítjuk be, hogy a szomszédos prímek közötti két egymás utáni hézag is tetszőlegesen nagy lehet, azaz olyan prímek is léteznek, amelyeket mindkét oldalról sok összetett szám vesz körül (az ilyen prímeket *izolált* prímeknek szokták nevezni).

5.5.2 Tétel **T 5.5.2**

Bármely K pozitív egészhez meg lehet adni olyan p prímet, amelyre a $p \pm 1, p \pm 2, \ldots, p \pm K$ számok valamennyien összetettek. ♣

Bizonyítás: Válasszunk egy olyan q prímet, amelyre $q \geq K + 2$, és legyen

$$d = 2 \cdot 3 \ldots (q-2)(q-1)(q+1)(q+2) \ldots (2q-2) = \frac{(2q-2)!}{q}\,.$$

Ekkor $(q, d) = 1$, és így Dirichlet tétele szerint létezik (végtelen sok) olyan $k > 0$, amelyre $p = q + dk$ prímszám. Megmutatjuk, hogy egy ilyen p megfelel a tétel állításának.

Tetszőleges $1 \leq j \leq q - 2$ esetén

$$p \pm j = q + kd \pm j = (q \pm j) + \frac{k(2q-2)!}{q} = (q \pm j)(1 + c_j),$$

ahol c_j pozitív egész, tehát valóban valamennyi $p \pm j$ szám összetett. ■

Most Csebisev nevezetes tételét igazoljuk: egy szám és a kétszerese közé mindig esik prímszám.

5.5.3 Tétel (Csebisev tétele) **T 5.5.3**

Bármely $n \geq 1$ egész esetén létezik olyan p prím, amelyre $n < p \leq 2n$. ♣

A tételből nyilván következik, hogy az állítás (egészek helyett) $n \geq 1$ valós számokra is igaz marad.

A tételt szokás Bertrand-posztulátumnak is nevezni, mert sejtésként először Bertrand fogalmazta meg 1845-ben, abban a hajszálnyival erősebb formában, hogy $n > 3$ esetén létezik olyan p prím, amelyre $n < p \leq 2n - 2$. (Ez az alak is igaz, sőt ennél jóval élesebb eredmények is, lásd az 5.5.4 és 5.5.5 Tételek (A) állításait.) Az 5.5.3 Tételt Csebisev bizonyította be 1852-ben. Az alábbi bizonyítás Erdős Páltól származik.

Bizonyítás: A bizonyítás alapötlete az, hogy az n és $2n$ közötti prímek szorzata szoros kapcsolatban áll a $\binom{2n}{n}$ binomiális együtthatóval. A továbbiakban feltesszük, hogy $n \geq 5$.

I. Írjuk fel $\binom{2n}{n}$ kanonikus alakját, és bontsuk ezt három tényező szorzatára a szereplő prímek nagysága szerint, az alábbi módon:

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\nu_p} = \prod_{p \leq \sqrt{2n}} p^{\nu_p} \cdot \prod_{\sqrt{2n} < p \leq n} p^{\nu_p} \cdot \prod_{n+1 \leq p \leq 2n} p^{\nu_p} . \qquad (1)$$

Jelölje az (1) jobb oldalán álló tényezőket rendre A, B, illetve C. A tétel bizonyításához elég azt igazolni, hogy $C > 1$, hiszen ekkor biztosan létezik az $n + 1 \leq p \leq 2n$ feltételt kielégítő p prím. (Könnyen megmutatható az is, hogy C-ben minden ν_p kitevő értéke 1, azaz C éppen az n és $2n$ közötti prímek szorzata, lásd az 5.5.7a feladatot.)

A $C > 1$ egyenlőtlenség belátásához felső becslést keresünk A-ra és B-re, valamint alsó becslést $\binom{2n}{n}$-re.

II. Alsó becslés $\binom{2n}{n}$-re: Mivel bármely $0 \leq k \leq 2n$ esetén $\binom{2n}{k} \leq \binom{2n}{n}$ (lásd az 5.5.5 feladatot), ezért

$$(2n+1)\binom{2n}{n} > \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n} ,$$

azaz

$$\binom{2n}{n} > \frac{4^n}{2n+1} . \qquad (2)$$

III. Felső becslés A-ra: Az 5.4.4 Lemma alapján $p^{\nu_p} \le 2n$, és így

$$A = \prod_{p \le \sqrt{2n}} p^{\nu_p} \le (2n)^{\pi(\sqrt{2n})} < (2n)^{\sqrt{2n}}\,. \tag{3}$$

IV. Felső becslés B-re: Ismét az 5.4.4 Lemma alapján $p^{\nu_p} \le 2n$, és ebből $p > \sqrt{2n}$ miatt $\nu_p \le 1$ következik.

Megmutatjuk, hogy ($p > 2$ és) $2n/3 < p \le n$ esetén $\nu_p = 0$. Ez azért igaz, mert

$$\binom{2n}{n} = \frac{2n(2n-1)\dots(n+1)}{n!}$$

nevezője és számlálója is egy ilyen p-nek pontosan az első hatványával osztható: a nevezőben csak a p, a számlálóban pedig csak a $2p$ tényezőben szerepel a p.

A fentiek alapján

$$B = \prod_{\sqrt{2n}<p\le n} p^{\nu_p} = \prod_{\sqrt{2n}<p\le 2n/3} p^{\nu_p} \le \prod_{\sqrt{2n}<p\le 2n/3} p\,. \tag{4}$$

A (4) egyenlőtlenség és az 5.4.5 Lemma alapján kapjuk, hogy

$$B < \prod_{p\le 2n/3} p < 4^{2n/3}\,. \tag{5}$$

V. A (2), (3) és (5) becsléseket (1)-be beírva és C-t kifejezve kapjuk, hogy

$$C > \frac{4^n}{(2n+1)(2n)^{\sqrt{2n}}\cdot 4^{2n/3}} > \frac{4^{n/3}}{(2n+1)^{1+\sqrt{2n}}}\,. \tag{6}$$

A $C > 1$ egyenlőtlenség igazolásához elég azt megmutatnunk, hogy a (6) jobb oldalán álló s_n kifejezés logaritmusa pozitív. Mivel

$$\log s_n = \frac{n\log 4}{3} - (1+\sqrt{2n})\log(2n+1) \;\to\; \infty, \quad \text{ha } n\to\infty\,, \tag{7}$$

ezért minden elég nagy n esetén $\log s_n > 0$. Könnyen adódik, hogy például $n > 511$ esetén fennáll a pozitivitás, tehát $n > 511$ esetén $C > 1$.

VI. Végül az $n \le 511$ értékekre közvetlenül ellenőrizhetjük a tétel állítását. Ehhez elegendő a 2-ből kiindulva olyan prímszámsorozatot készítenünk, amelynek bármely eleme kisebb, mint a megelőző elemnek a kétszerese. Egy ilyen sorozat például a következő: 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631. (Az

éppen a Csebisev-tételből következik, hogy ilyen tulajdonságú *végtelen* sorozat is létezik.) ■

A Csebisev-tétellel kapcsolatban felvethetjük a következő általánosabb „hézagfüggvény" problémát:

Milyen $h(n)$ függvényekre igaz, hogy minden elég nagy n természetes szám esetén az $(n, n + h(n))$ nyílt intervallumban található prímszám?

A Csebisev-tétel szerint $h(n) = n$ megfelel, az 5.5.1 Tétel alapján viszont a $h(n)$ nem választható konstans függvénynek, hiszen az $(n, n+K)$ intervallum bármilyen rögzített K esetén végtelen sok n-re „prímmentes".

Megoldatlan probléma, hogy milyen nagyságrendű a „lehető legjobb" $h(n)$. Erre vonatkozóan a következő eredmények ismertek (ezeket bizonyítás nélkül közöljük):

5.5.4 Tétel **T 5.5.4**

(A) Legyen $\theta = 0{,}525$. Ekkor minden elég nagy n-re az $(n, n+n^\theta)$ intervallum tartalmaz prímszámot.

(B) Végtelen sok olyan n pozitív egész létezik, amelyre az

$$\left(n\ ,\ n + \frac{c \cdot \log n \cdot \log\log n \cdot \log\log\log\log n}{\log\log\log n}\right)$$

intervallum nem tartalmaz prímszámot (itt c egy pozitív konstans). ♣

Az 5.5.4 Tétel mindkét állítása igen mély eredmény (például jóval élesebbek, mint a prímszámtételből leolvasható következtetések, lásd az 5.5.5 Tételt), ennek ellenére hatalmas űr tátong közöttük; a $h(n)$ választható n^θ-nak, és nem választható egy $\log n$-nél „nem sokkal nagyobb" függvénynek. Bizonyos valószínűségi megfontolások alapján azt lehet sejteni, hogy a $(\log n)^2$ függvény „környékén" várható a választóvonal.

Érdekességként megjegyezzük, hogy (A)-ból még az az 5.1 pontban már említett, ártatlannak látszó sejtés sem következik, hogy két egymást követő négyzetszám között mindig található prímszám. Ehhez az (A)-beli θ-nak 1/2-re történő leszorítására lenne szükség, amit még az ún. Riemann-sejtés felhasználásával sem sikerült igazolni.

Az alábbiakban azt mutatjuk meg, hogy a prímszámtétel segítségével mennyire élesíthetők az 5.5.3 és 5.5.1 Tételek eredményei.

5.5.5 Tétel **T 5.5.5**

(A) Bármely $\varepsilon > 0$-hoz létezik olyan (ε-tól függő) n_0, hogy minden $n > n_0$ esetén az $\big(n, (1+\varepsilon)n\big)$ intervallum tartalmaz prímszámot.

(B) Bármely $0 < \varepsilon < 1$ esetén végtelen sok olyan n pozitív egész létezik, amelyre az $\big(n, n + (1-\varepsilon)\log n\big)$ intervallum nem tartalmaz prímszámot.

♣

Bizonyítás: Az (A) részhez azt kell igazolnunk, hogy minden elég nagy n-re

$$\pi\big((1+\varepsilon)n\big) - \pi(n) > 0\,. \tag{8}$$

A prímszámtétel szerint minden elég nagy n-re egyrészt

$$\pi(n) < \big(1 + \frac{\varepsilon}{4}\big) \cdot \frac{n}{\log n}\,, \tag{9}$$

másrészt

$$\pi\big((1+\varepsilon)n\big) > \big(1 - \frac{\varepsilon}{4}\big) \cdot \frac{(1+\varepsilon)n}{\log\big((1+\varepsilon)n\big)} \tag{10}$$

teljesül, továbbá nyilván

$$\log\big((1+\varepsilon)n\big) = \log(1+\varepsilon) + \log n < \big(1 + \frac{\varepsilon}{4}\big)\log n\,. \tag{11}$$

(9), (10) és (11) alapján

$$\pi\big((1+\varepsilon)n\big) - \pi(n) > \left(\frac{\big(1-\frac{\varepsilon}{4}\big)\big(1+\varepsilon\big)}{1+\frac{\varepsilon}{4}} - \big(1+\frac{\varepsilon}{4}\big)\right)\frac{n}{\log n}\,. \tag{12}$$

(12) jobb oldalán az $n/\log n$ együtthatója

$$\frac{\big(1-\frac{\varepsilon}{4}\big)\big(1+\varepsilon\big) - \big(1+\frac{\varepsilon}{4}\big)^2}{1+\frac{\varepsilon}{4}} = \frac{\frac{\varepsilon}{4}\big(1-\frac{5\varepsilon}{4}\big)}{1+\frac{\varepsilon}{4}} \;>\; 0$$

(hiszen feltehető, hogy $\varepsilon < 4/5$), és így (12)-ből következik (8).

A (B) állítást indirekt bizonyítjuk. Tegyük fel, hogy van olyan $\varepsilon > 0$ és olyan n_0, hogy minden $n > n_0$ esetén az $\big(n, n + (1-\varepsilon)\log n\big)$ intervallum tartalmaz prímszámot.

Legyen N egy (nagy) rögzített egész, és tekintsük az n_0 és N közötti prímszámokat: $n_0 < p_r < p_{r+1} < \ldots < p_k \le N$. Ekkor az indirekt feltevés alapján az alábbi egyenlőtlenségeket kapjuk:

$$\begin{aligned} p_{r+1} &< p_r \quad + (1-\varepsilon)\log p_r\,, \\ p_{r+2} &< p_{r+1} + (1-\varepsilon)\log p_{r+1}\,, \\ &\vdots \\ p_{k+1} &< p_k \quad + (1-\varepsilon)\log p_k\,. \end{aligned} \tag{13}$$

A (13)-beli egyenlőtlenségeket összeadva a $p_{r+1}, \ldots, p_k$ tagok kiesnek, és

$$p_{k+1} < p_r + (1-\varepsilon)\sum_{j=r}^{k} \log p_j \tag{14}$$

adódik.

A p_k definíciója szerint $p_{k+1} > N$, ezért az ellentmondáshoz elég azt megmutatnunk, hogy (14) jobb oldala viszont kisebb, mint N.

Ehhez (14) jobb oldalát a következőképpen becsüljük felülről:

$$p_r + (1-\varepsilon)\sum_{j=r}^{k} \log p_j < p_r + (1-\varepsilon)\pi(N)\log N\,. \tag{15}$$

A prímszámtétel szerint elég nagy N esetén

$$\pi(N) \;<\; \big(1+\frac{\varepsilon}{4}\big)\frac{N}{\log N}\,, \tag{16}$$

továbbá (elég nagy N-re) nyilván

$$p_r \;<\; \frac{\varepsilon N}{4}\,. \tag{17}$$

A (16) és (17) egyenlőtlenségeket (15)-be beírva azt nyerjük, hogy (14) jobb oldala kisebb, mint

$$\Big(\big(1-\varepsilon\big)\big(1+\frac{\varepsilon}{4}\big)+\frac{\varepsilon}{4}\Big)\,N \;<\; \big(1-\frac{\varepsilon}{2}\big)N \;<\; N\,,$$

amivel megkaptuk a már jelzett ellentmondást. ■

Feladatok

5.5.1 Bizonyítsuk be, hogy $n > 1$ esetén $n!$ nem lehet teljes hatvány.

5.5.2 Igazoljuk, hogy bármely két szomszédos pozitív egész közül legalább az egyik felírható csupa különböző prímszám összegeként (egytagú összeget is megengedünk).

5.5.3 Mutassuk meg, hogy végtelen sok olyan prím van, amelynek (tízes számrendszerben)
a) az első számjegye 1-es;
b) az első ezer számjegye 4-es.

5.5.4 Bizonyítsuk be, hogy ha $1 \le k < n$, akkor az alábbi összegek értéke nem lehet egész szám:

$$\text{a)} \sum_{j=1}^{n} \frac{1}{j}\,; \qquad\qquad \text{b)} \sum_{j=k}^{n} \frac{1}{j}\,.$$

5.5.5 Mutassuk meg, hogy a $\binom{2n}{k}$, $0 \le k \le 2n$, binomiális együtthatók közül $\binom{2n}{n}$ a legnagyobb.

5.5.6 Adjunk még egy bizonyítást az 5.5.2 Tételre az alábbi gondolatmenet alapján: Válasszunk $2K$ darab K-nál nagyobb prímszámot, legyenek ezek $p_1, \dots, p_K, q_1, \dots, q_K$, és tekintsük az

$$x \equiv j \pmod{p_j}, \qquad x \equiv -j \pmod{q_j}, \qquad j = 1, 2, \dots, K$$

szimultán kongruenciarendszert. Mutassuk meg, hogy ennek megoldásai között található (végtelen sok) p prímszám, és ezek kielégítik a tétel feltételeit.

5.5.7
a) Bizonyítsuk be, hogy $\binom{2n}{n}$ minden $n + 1 \le p \le 2n$ prímszámnak pontosan az első hatványával osztható.
b) Mutassuk meg, hogy ha $p > 3$ prím és $2n/5 < p \le n/2$, akkor $\binom{2n}{n}$ nem osztható p-vel. Hogyan általánosítható ez az észrevétel?

5.5.8 Mutassuk meg, hogy ($n \ge 2$ esetén) a Csebisev-tételre adott bizonyításból az alábbi élesebb eredmény is következik: Az n és $2n$ közötti prímek száma nagyobb, mint $cn/\log n$, ahol c alkalmas pozitív konstans.

M 5.5.9

a) Az 5.5.4 Tétel (A) részének a felhasználásával lássuk be, hogy bármely két elég nagy, egymást követő köbszám között található prímszám.

*b) Bizonyítsuk be, hogy létezik olyan $\alpha > 1$ valós szám, amelyre $\lfloor \alpha^{3^n} \rfloor$ minden n pozitív egész esetén prímszám.

c) Miért nem alkalmas a b)-beli képlet nagy prímszámok gyakorlati előállítására?

5.5.10 Vizsgáljuk meg, hogy milyen, az 5.5.5 Tétel (B) állításához hasonló jellegű eredményeket nyerhetünk, ha a prímszámtétel helyett az alábbiakra támaszkodunk:

a) 5.4.3 Tétel;

b) az 5.5.1 Tétel bizonyítása;

c) az 5.5.1 Tétel bizonyítása utáni megjegyzés.

*5.5.11 Bizonyítsuk be, hogy bármely $\varepsilon > 0$-hoz végtelen sok olyan n pozitív egész létezik, amelyre $p_{n+1} - p_n < (1 + \varepsilon) \log n$. (A szokásos módon p_n az n-edik prímszámot jelöli.)

Megjegyzés: Nagyon hosszú ideig ebben a becslésben csak az $1 + \varepsilon$ konstanst sikerült 0,4 körülire javítani. Óriási szenzációt jelentett, amikor 2005-ben Goldston, Motohashi, Pintz János és Yildirim bebizonyították, hogy a $(p_{n+1} - p_n)/\log n$ sorozatnak létezik 0-hoz tartó részsorozata (ami látszólag „alig" erősebb, mint az 5.5.11 feladat állítása). Goldston, Pintz és Yildirim még újabb eredményeit és módszereit továbbfejlesztve 2013-ban Zhang megmutatva, hogy $p_{n+1} - p_n$-nek létezik korlátos(!) részsorozata (lásd részletesebben az Ikerprímek résznél).

5.6. A prímek reciprokösszege

Ebben a pontban bebizonyítjuk, hogy a prímszámok reciprokaiból képzett végtelen sor divergens. Ez azt jelenti, hogy a prímek reciprokai „lassan" fogynak, azaz maguk a prímek lassan növekednek, vagyis a prímek „viszonylag sűrűn" helyezkednek el a pozitív egészek között. Összehasonlításképpen, a négyzetszámok reciprokaiból képzett végtelen sor konvergens, azaz a négyzetszámok a pozitív egészeknek egy „ritka" részsorozatát alkotják (vö. az 5.4.1 Tétel utáni 2. megjegyzéssel).

A prímek reciprokösszegének divergenciájára három bizonyítást adunk. Az első mutatja, hogy ez a tény a prímszámtételből (sőt már az 5.4.3 Tételből

is) következik. A második Erdős Pál szellemes indirekt gondolatmenete. A harmadik Euler bizonyítása, aki először mondta ki és igazolta ezt a tételt.

Végül megmutatjuk, hogy az x-nél nem nagyobb prímek reciprokainak összege nagyon jól közelíthető a $\log\log x$ függvénnyel.

5.6.1 Tétel **T 5.6.1**

A prímek reciprokaiból képzett végtelen sor divergens, azaz

$$\sum_p \frac{1}{p} = \infty\,. \ \clubsuit$$

Első bizonyítás: Azt kell igazolnunk, hogy

$$\lim_{n\to\infty} \sum_{j=1}^{n} \frac{1}{p_j} = \infty\,, \tag{1}$$

ahol p_j a j-edik prímszámot jelöli.

Az 5.4.2 Tétel (vagy az 5.4.3 feladat) szerint létezik olyan c és n_0, hogy minden $j \geq n_0$ esetén $p_j < cj\log j$. Ebből következik, hogy

$$\sum_{j=1}^{n} \frac{1}{p_j} > \frac{1}{c} \sum_{j=n_0}^{n} \frac{1}{j\log j}\,. \tag{2}$$

Rajzoljunk minden $n_0 \leq j \leq n$ egész számhoz egy olyan téglalapot, amelynek az alapja az x tengely $[j, j+1]$ szakasza, magassága pedig $1/(j\log j)$. Ekkor a téglalapok területének összege éppen a (2) jobb oldalán szereplő összeg (az $1/c$ szorzó nélkül).

Mivel az $1/(x\log x)$ függvény ($x > 1$ esetén) monoton csökken, ezért az $[n_0, n+1]$ intervallumon a függvénygörbe a téglalapok alkotta alakzatban halad. Emiatt a függvénygörbe alatti terület kisebb, mint a téglalapok területének az összege, azaz

$$\sum_{j=n_0}^{n} \frac{1}{j\log j} > \int_{n_0}^{n+1} \frac{dx}{x\log x}\,. \tag{3}$$

A (3) jobb oldalán szereplő integrált kiszámítva

$$\int_{n_0}^{n+1} \frac{dx}{x\log x} = \big[\log\log x\big]_{n_0}^{n+1} = \log\log(n+1) - \log\log n_0 \tag{4}$$

adódik.

A (3) és (4) összefüggések felhasználásával a (2) egyenlőtlenségből

$$\sum_{j=1}^{n} \frac{1}{p_j} \;>\; \frac{1}{c}\big(\log\log(n+1) - \log\log n_0\big) \tag{5}$$

következik. Mivel

$$\lim_{n\to\infty} \log\log n = \infty\,,$$

ezért $n \to \infty$ esetén (5)-ben a jobb oldal, és emiatt a bal oldal is a végtelenhez tart, azaz (1) valóban teljesül. ■

Megjegyzés: A bizonyításból az is leolvasható, hogy alkalmas c' konstanssal minden elég nagy n esetén fennáll

$$\sum_{p\le n} \frac{1}{p} \;>\; c' \log\log n\,. \tag{5a}$$

Ugyanígy igazolható

$$\sum_{p\le n} \frac{1}{p} \;<\; c'' \log\log n$$

is, sőt a prímszámtétel (vagy az azzal ekvivalens 5.4.2 Tétel) kicsit ügyesebb alkalmazásával

$$\sum_{p\le n} \frac{1}{p} \;\sim\; \log\log n$$

következik. Ezeknél is élesebb becslést kapunk majd azonban az 5.6.2 Tételben (ráadásul a prímszámtétel felhasználása nélkül), sőt már az 5.6.1 Tételre adott harmadik bizonyítás (13) egyenlőtlensége is sokkal erősebb (5a)-nál.

Második bizonyítás: Tegyük fel indirekt, hogy a prímek reciprokösszege konvergens. Ekkor létezik olyan k, hogy

$$\sum_{j=k+1}^{\infty} \frac{1}{p_j} \;<\; \frac{1}{2}\,. \tag{6}$$

Rögzítsük le k értékét, és osszuk a pozitív egészeket két csoportba: az első csoportba azok a számok kerülnek, amelyeknek van p_k-nál nagyobb prímosztója, a második csoportot pedig azok a számok alkotják, amelyeknek minden prímosztója kisebb vagy egyenlő, mint p_k.

Legyen N (nagy) természetes szám, és tekintsük a $H = \{1, 2, \dots, N\}$ halmazt. Meg fogjuk mutatni, hogy elég nagy N-et választva, a H elemeinek kevesebb, mint a fele tartozik az első csoportba, és ugyancsak kevesebb, mint a fele tartozik a második csoportba, ami nyilvánvaló ellentmondás.

Vizsgáljuk először az első csoportot. Tetszőleges p prím esetén H-ban a p-vel osztható elemek száma $\lfloor \frac{N}{p} \rfloor$. Ebből az első csoportbeli elemek darabszámára a következő felső becslés adódik:

$$\sum_{p_k < p \le N} \left\lfloor \frac{N}{p} \right\rfloor \le \sum_{p_k < p \le N} \frac{N}{p} < N \sum_{j=k+1}^{\infty} \frac{1}{p_j} < \frac{N}{2}$$

(az utolsó lépésben (6)-ot használtuk fel). Ez azt jelenti, hogy H elemeinek kevesebb, mint a fele tartozik az első csoportba.

A második csoport vizsgálatához felhasználjuk, hogy minden pozitív egész (egyértelműen) előállítható egy négyzetszám és egy négyzetmentes szám szorzataként. Ez a számelmélet alaptételéből következik: Válasszuk külön n kanonikus alakjában a páros és páratlan kitevőket:

$$n = q_1^{2\beta_1} \dots q_r^{2\beta_r} q_{r+1}^{2\beta_{r+1}+1} \dots q_s^{2\beta_s+1}$$

(ahol $r = 0$, illetve $r = s$ is megengedett), ekkor

$$n = \left(q_1^{\beta_1} \dots q_r^{\beta_r} q_{r+1}^{\beta_{r+1}} \dots q_s^{\beta_s} \right)^2 \cdot \left(q_{r+1} \dots q_s \right)$$

adja a kívánt előállítást.

Írjuk fel H-nak a második csoportba tartozó elemeit ilyen $a^2 b$ alakban (ahol b négyzetmentes). Ekkor $1 \le a \le \lfloor \sqrt{N} \rfloor$, továbbá b a $p_1, \dots p_k$ prímek közül néhány különbözőnek (akár az összesnek) a szorzata (de b lehet az üres szorzat is, ekkor $b = 1$).

Ebből következik, hogy az a^2 választására $\lfloor \sqrt{N} \rfloor$ lehetőség adódik, a b választására pedig 2^k (ahány részhalmaza van a $\{p_1, \dots, p_k\}$ halmaznak). Ennélfogva az ilyen $a^2 b$ szorzatok száma legfeljebb $\sqrt{N} \cdot 2^k$. Mivel k rögzített, ezért elég nagy N esetén $2^k < \sqrt{N}/2$, tehát $\sqrt{N} \cdot 2^k < N/2$. Ezzel igazoltuk, hogy H elemeinek kevesebb, mint a fele tartozik a második csoportba. ■

Harmadik bizonyítás: Felhasználjuk a következő (analízisbeli) tételeket:

$$\text{(i)} \ \sum_{j=1}^{n} \frac{1}{j} > \log n\,; \qquad \text{(ii)} \ \sum_{j=1}^{\infty} \frac{1}{j^2} < 2\,;$$

$$\text{(iii)} \ \log \frac{1}{1-x} = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots \le x + x^2\,, \quad \text{ha} \quad 0 \le x \le \frac{1}{2}\,.$$

Rátérve a tételünk bizonyítására, tekintsük a következő szorzatot:

$$A_n = \prod_{p \le n} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{\nu_p}}\right) ,$$

ahol $n > 1$ egész és

$$p^{\nu_p} \le n < p^{\nu_p+1} , \qquad \text{azaz} \qquad \nu_p = \lfloor \log_p n \rfloor .$$

Megmutatjuk, hogy

$$A_n \ge \sum_{j=1}^{n} \frac{1}{j} . \tag{7}$$

Legyen először $n = 10$, és írjuk ki az A_{10} tényezőit részletesen:

$$A_{10} = \left(1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3}\right)\left(1 + \frac{1}{3} + \frac{1}{3^2}\right)\left(1 + \frac{1}{5}\right)\left(1 + \frac{1}{7}\right) .$$

Ha $j \le 10$, akkor j kanonikus alakjában csak a 2, 3, 5, 7 prímek fordulhatnak elő, éspedig legfeljebb akkora kitevővel, mint amilyennel az A_{10} egyes tényezőiben szerepelnek. Ezért tetszőleges $j \le 10$ előállítható (ráadásul egyértelműen) ezen prímhatványok szorzataként. Ez azt jelenti, hogy ha elvégezzük a szorzást A_{10}-ben, akkor biztosan megkapjuk minden $j \le 10$ szám reciprokát, és így $A_{10} \ge \sum_{j=1}^{10} 1/j$.

Ugyanezt a meggondolást a 10 helyett tetszőleges n-re végrehajtva a (7) egyenlőtlenséget nyerjük. Ebből (i) felhasználásával

$$A_n > \log n \tag{8}$$

adódik.

Most felső becslést keresünk A_n-re. Az A_n tényezőiben szereplő mértani sorozatokat összegezve kapjuk, hogy

$$A_n = \prod_{p \le n} \frac{1 - \left(\frac{1}{p}\right)^{\nu_p+1}}{1 - \frac{1}{p}} < \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} . \tag{9}$$

A (8) és (9) egyenlőtlenségekből

$$\log n < \prod_{p \le n} \frac{1}{1 - \frac{1}{p}} \tag{10}$$

adódik. (10)-et logaritmálva a

$$\log\log n \;<\; \sum_{p\le n} \log \frac{1}{1-\frac{1}{p}} \tag{11}$$

egyenlőtlenséget kapjuk. A (11) jobb oldalát (iii) szerint felülről becsülve

$$\log\log n \;<\; \sum_{p\le n} \frac{1}{p} + \sum_{p\le n} \frac{1}{p^2} \tag{12}$$

adódik. Végül (ii) miatt a (12) jobb oldalán álló második összeg kisebb, mint 2, és így

$$\sum_{p\le n} \frac{1}{p} \;>\; \log\log n - 2\,, \tag{13}$$

amiből a tétel állítása következik. ■

A harmadik bizonyításból azt is megkaptuk, hogy az n-nél nem nagyobb prímek reciprokösszege nem lehet lényegesen kisebb $\log\log n$-nél (lásd a (13) egyenlőtlenséget). A következőkben ezt tovább élesítjük, és azt igazoljuk, hogy ennek a reciprokösszegnek a $\log\log n$-től való eltérése korlátos:

5.6.2 Tétel **T 5.6.2**

Létezik olyan c konstans, hogy minden $n \ge 3$ egész számra

$$\Big|\sum_{p\le n} \frac{1}{p} \;-\; \log\log n\Big| \;<\; c\,. \;\clubsuit \tag{14}$$

Bizonyítás: A bizonyításhoz szükségünk lesz a $\sum_{p\le n}(\log p)/p$ összeg becslésére:

5.6.3 Tétel **T 5.6.3**

Létezik olyan c' konstans, hogy minden $n \ge 2$ egész számra

$$\Big|\sum_{p\le n} \frac{\log p}{p} \;-\; \log n\Big| \;<\; c'\,. \;\clubsuit \tag{15}$$

Az 5.6.3 Tétel bizonyítása: Induljunk ki az $n!$ kanonikus alakjából (1.6.8 Tétel). Ezt logaritmálva

$$\log n! = \sum_{p\le n} \log p \left(\Big\lfloor \frac{n}{p} \Big\rfloor + \Big\lfloor \frac{n}{p^2} \Big\rfloor + \Big\lfloor \frac{n}{p^3} \Big\rfloor + \dots \right) \tag{16}$$

adódik. Meg fogjuk mutatni, hogy (16) bal oldala „körülbelül" $n \log n$, a jobb oldalon pedig a $\log p$ szorzójában „az egészrész elhagyható és csak az első tag számít", vagyis a jobb oldal „körülbelül" $n \sum_{p \le n} (\log p)/p$. Innen n-nel való osztás után kapjuk a kívánt (15) egyenlőtlenséget.

Nézzük mindezt pontosan és részletesen. A (16) bal oldalán álló $\log n!$ becsléséhez használjuk fel, hogy $n \ge 2$-re

$$\left(\frac{n}{e}\right)^n \;<\; n! \;<\; n^n\,.$$

Itt a felső becslés nyilvánvaló, az alsó becslés pedig könnyen igazolható teljes indukcióval. Ezeket az egyenlőtlenségeket logaritmálva kapjuk, hogy

$$n(\log n - 1) \;<\; \log n! \;<\; n \log n\,. \tag{17}$$

Az $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \dots$ összeget a következőképpen becsülhetjük:

$$\frac{n}{p} - 1 \;<\; \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots \;<\; \frac{n}{p} + \frac{n}{p^2} + \dots \;=\; \frac{n}{p} + \frac{n}{p(p-1)}\,. \tag{18}$$

Jelöljük (16) jobb oldalát J-vel. Ekkor (18) alapján J-re az alábbi becsléseket nyerjük:

$$n \sum_{p \le n} \frac{\log p}{p} \;-\; \sum_{p \le n} \log p \;<\; J \;<\; n \sum_{p \le n} \frac{\log p}{p} \;+\; n \sum_{p \le n} \frac{\log p}{p(p-1)}\,. \tag{19}$$

Az 5.4.5 Lemma alapján

$$\sum_{p \le n} \log p \;=\; \log \prod_{p \le n} p \;<\; \log 4^n \;=\; n \log 4\,, \tag{20}$$

továbbá

$$\sum_{p \le n} \frac{\log p}{p(p-1)} \;<\; \sum_{k=2}^{\infty} \frac{\log k}{k(k-1)}\,, \tag{21}$$

ahol a (21) jobb oldalán álló végtelen sor konvergens, és az is megmutatható, hogy az összege kisebb, mint 4.

A (20) és (21) egyenlőtlenségek felhasználásával (19)-ből kapjuk, hogy

$$\left| \frac{J}{n} - \sum_{p \le n} \frac{\log p}{p} \right| \;<\; 4\,. \tag{22}$$

Ugyanakkor (16) alapján $J = \log n!$, ezért (17)-ből

$$\Big| \frac{J}{n} - \log n \Big| < 1 \tag{23}$$

következik. Végül (22) és (23) miatt (15) is teljesül (például $c' = 5$ megfelel). ■

Az 5.6.2 Tétel bizonyításához kényelmesebb, ha az 5.6.3 Tételt az egész n értékekről tetszőleges $x \geq 2$ valós számra is kiterjesztjük. Ehhez vegyük észre, hogy

$$\sum_{p \leq x} \frac{\log p}{p} = \sum_{p \leq \lfloor x \rfloor} \frac{\log p}{p} \quad \text{és} \quad \big|\log x - \log\lfloor x \rfloor\big| = \log \frac{x}{\lfloor x \rfloor} < \log \frac{3}{2}\ ,$$

és így (15) alapján

$$\Big|\sum_{p \leq x} \frac{\log p}{p} - \log x\Big| \leq \Big|\sum_{p \leq \lfloor x \rfloor} \frac{\log p}{p} - \log\lfloor x \rfloor\Big| + \big|\log\lfloor x \rfloor - \log x\big| < c' + \log \frac{3}{2}\,.$$

Ezzel megmutattuk, hogy tetszőleges $x \geq 2$ valós szám esetén

$$\Big|\sum_{p \leq x} \frac{\log p}{p} - \log x\Big| < 6\,. \tag{24}$$

Vezessük még be a következő jelöléseket tetszőleges $x \geq 2$ valós számra:

$$f(x) = \sum_{p \leq x} \frac{\log p}{p}\,, \quad g(x) = \frac{1}{\log x} \quad \text{és} \quad h(x) = f(x) - \log x\,. \tag{25}$$

Az $f(x)$ és $g(x)$ definíciója alapján $f(2)g(2) = 1/2$, továbbá bármely $k \geq 3$ egész szám esetén

$$\big(f(k) - f(k-1)\big)g(k) = \begin{cases} \frac{1}{k}\,, & \text{ha } k \text{ prím;} \\ 0, & \text{ha } k \text{ nem prím.} \end{cases}$$

Ebből következik, hogy tetszőleges $n \geq 3$ egészre fennáll

$$\sum_{p \leq n} \frac{1}{p} = f(2)g(2) + \sum_{k=3}^{n} \big(f(k) - f(k-1)\big)g(k)\,. \tag{26}$$

(26) jobb oldalát az ún. parciális összegezés (Abel-féle átrendezés) segítségével átalakítva kapjuk, hogy

$$\sum_{p\le n}\frac{1}{p} = f(2)\big(g(2)-g(3)\big)+f(3)\big(g(3)-g(4)\big)+\dots$$
$$\dots+f(n-1)\big(g(n-1)-g(n)\big)+f(n)g(n)\,. \tag{27}$$

Most megmutatjuk, hogy (27) jobb oldalán az összeg egy általános tagja (az utolsó kivételével)

$$f(k)\big(g(k)-g(k+1)\big) = -\int_k^{k+1} f(t)g'(t)\,dt \tag{28}$$

alakba írható. Ez azért igaz, mert a (balról zárt, jobbról nyílt) $[k,k+1)$ intervallumon az $f(t)$ függvény értéke a konstans $f(k)$, továbbá a Newton–Leibniz-szabály szerint

$$\int_k^{k+1} g'(t)dt = g(k+1)-g(k).$$

(28) felhasználásával (27)-ből a következő egyenlőséget nyerjük:

$$\sum_{p\le n}\frac{1}{p} \;=\; f(n)g(n) \;-\; \int_2^n f(t)g'(t)\,dt\,. \tag{29}$$

Most kiszámítjuk a (29) jobb oldalán szereplő integrált az

$$f(t)=\log t+h(t) \quad \text{és} \quad g'(t)=\left(\frac{1}{\log t}\right)'=\frac{-1}{t(\log t)^2}$$

összefüggések felhasználásával:

$$-\int_2^n f(t)g'(t)\,dt \;=\; \int_2^n \frac{dt}{t\log t} \;+\; \int_2^n \frac{h(t)\,dt}{t(\log t)^2}\;. \tag{30}$$

A (30) jobb oldalán szereplő első integrál

$$\int_2^n \frac{dt}{t\log t} = \big[\log\log t\big]_2^n = \log\log n-\log\log 2\,. \tag{31}$$

A (30) jobb oldalán szereplő második integrál becsléséhez felhasználjuk, hogy $|h(t)| < 6$, ez (24)-ből és (25)-ből következik. Innen

$$\left|\int_2^n \frac{h(t)\,dt}{t(\log t)^2}\right| < 6\int_2^n \frac{dt}{t(\log t)^2} = 6\left[\frac{-1}{\log t}\right]_2^n = \frac{6}{\log 2} - \frac{6}{\log n}\,. \tag{32}$$

(32)-t és (31)-et (30)-ba beírva kapjuk, hogy

$$-\int_2^n f(t)g'(t)\,dt = \log\log n + s(n)\,, \quad \text{ahol } s(n) \text{ korlátos.} \tag{33}$$

Most azt igazoljuk, hogy a (29) jobb oldalán álló $f(n)g(n)$ szorzat is korlátos:

$$|f(n)g(n)| = \left|\frac{\log n + h(n)}{\log n}\right| = \left|1 + \frac{h(n)}{\log n}\right| < 1 + 6 = 7\,. \tag{34}$$

Végül (29)-et (33)-mal és (34)-gyel összevetve kapjuk az 5.6.2 Tétel állítását. ■

Megjegyzés: A (32) becslést $[2, n]$ helyett az $[n, N]$ intervallumra megismételve kiderül, hogy $n \to \infty$ esetén a (30) jobb oldalán szereplő második integrálnak létezik határértéke, és az attól való eltérés abszolút értéke legfeljebb $6/\log n$. Ugyanez $f(n)g(n)$-re nyilvánvaló. Így létezik olyan c_1 és c_2 konstans, hogy minden $n \geq 3$ egészre

$$\left|\sum_{p\leq n} \frac{1}{p} - \log\log n - c_1\right| \leq \frac{c_2}{\log n}\,.$$

Feladatok

M 5.6.1 Legyen L rögzített pozitív egész. Tekintsük a pozitív egészek alábbi részsorozatait, és döntsük el, hogy az elemek reciprokaiból álló végtelen sorok konvergensek vagy divergensek-e:

a) az L-lel osztható számok;
b) a teljes hatványok;
c) a négyzetmentes számok;
d) azok a számok, amelyeknek minden prímosztója kisebb, mint L;
e) azok a számok, amelyeknek minden prímosztója nagyobb, mint L;
f) azok a számok, amelyek kanonikus alakjában minden prímszám kitevője legalább 2 (ezeket *négyzetteljes* számoknak szokták hívni).

A c) sorozat kivételével vizsgáljuk meg azt is, hogy nagy n esetén az egyes számsorozatoknak „körülbelül" hány elemük van n-ig; ez pontosabban azt jelenti, hogy ha az $U = \{u_1 < u_2 < \ldots\}$ sorozatról van szó, akkor az $U(n) = \sum_{u_i \le n} 1$ függvényre keresünk aszimptotikát, illetve minél jobb becsléseket. (A négyzetmentes számokra vonatkozó eredményt lásd a 6.7.2 feladatban.)

5.6.2 Az 5.6.1 Tételre adott első bizonyításban alkalmazott „integrálkritérium" segítségével döntsük el, hogy az alábbi végtelen sorok konvergensek vagy divergensek-e:

$$\text{a)}\ \sum_{n=1}^{\infty} \frac{1}{n^{1,01}}\,; \qquad \text{b)}\ \sum_{n=2}^{\infty} \frac{1}{n(\log n)^2}\,; \qquad \text{c)}\ \sum_{n=2}^{\infty} \frac{1}{n \cdot \log n \cdot \log\log n}\,.$$

5.6.3 Az alábbi végtelen sorokban az összegzés a prímek szerint történik. Vizsgáljuk meg a konvergencia, illetve divergencia kérdését:

$$\text{a)}\ \sum_{p} \frac{1}{p \log p}\,; \qquad\qquad \text{b)}\ \sum_{p} \frac{1}{p \log\log p}\,.$$

5.6.4 Tekintsük a pozitív egészek alábbi típusú $a_1 < a_2 < \ldots$ részsorozatait. Mit állíthatunk az elemek reciprokaiból álló végtelen sorokról a konvergencia/divergencia szempontjából? (Lehetséges válaszok: biztosan konvergens — biztosan divergens — lehet konvergens, és lehet divergens is.)

a) Az a_n elemek páronként relatív prím összetett számok.
b) Minden n-re az a_n kanonikus alakjában a prímek kitevőinek az összege legalább $2 \log n$.
c) Minden n-re $a_{n+1} - a_n < 10^{1000}$.
d) Minden n-re $a_{n+1}/a_n < 1{,}00001$.
e) Az a_n elemek között nincs két olyan, amelynek ugyanannyi osztója lenne.

5.6.5 Ha az $A = \{a_1 < a_2 < \ldots\}$ pozitív egészekből álló számsorozatra $\sum_{n=1}^{\infty} 1/a_n < \infty$, akkor ez azt jelenti, hogy az A „ritka". Érdemes-e a ritkaság fogalmát aszerint finomítani, hogy mekkora a $\sum_{n=1}^{\infty} 1/a_n$ összeg?

M 5.6.6 Tetszőleges $s > 1$ valós számra a Riemann-féle zétafüggvényt a következőképpen definiáljuk:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,. \tag{35}$$

Ismeretes (vagy az 5.6.2a feladat mintájára igazolható), hogy a (35) jobb oldalán álló végtelen sor ($s > 1$ esetén) konvergens. Például $\zeta(2) = \pi^2/6$.

Most egy végtelen szorzatot értelmezünk (p a prímeken fut végig):

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \lim_{n\to\infty} \prod_{p\le n} \frac{1}{1-\frac{1}{p^s}}\,. \tag{36}$$

Bizonyítsuk be, hogy $s > 1$ esetén a (36) jobb oldalán szereplő határérték létezik és egyenlő $\zeta(s)$-sel.

5.6.7 Legyen $0 < a_j < 1$, $j = 1, 2, \ldots$ és definiáljuk az alábbi végtelen szorzatot:

$$\prod_{j=1}^{\infty}(1-a_j) = \lim_{n\to\infty} \prod_{j=1}^{n}(1-a_j)\,.$$

Bizonyítsuk be, hogy

$$\sum_{j=1}^{\infty} a_j = \infty \iff \prod_{j=1}^{\infty}(1-a_j) = 0\,.$$

Megjegyzés: Általában egy (nulla tényezőket nem tartalmazó) végtelen szorzatot akkor nevezünk *konvergens*nek, ha a részletszorzatok sorozatának létezik *véges* és *0-tól különböző* határértéke.

*5.6.8 Az 5.6.1 Tétel harmadik bizonyítása során megmutattuk (lásd a (10) egyenlőtlenséget), hogy

$$\log n \;<\; \prod_{p\le n} \frac{1}{1-\frac{1}{p}}\,.$$

Bizonyítsuk be, hogy érvényes az alábbi fordított irányú becslés is: létezik olyan c konstans, amelyre (minden $n \ge 2$ esetén)

$$c\log n \;>\; \prod_{p\le n} \frac{1}{1-\frac{1}{p}}\,.$$

5.6.9 Legyen $n > 1$, és jelölje $p(n)$, illetve $P(n)$ az n legkisebb, illetve legnagyobb prímosztóját. Döntsük el, hogy az alábbi végtelen sorok konvergensek vagy divergensek-e:

a) $\displaystyle\sum_{n=2}^{\infty} \frac{1}{np(n)}$; **b) $\displaystyle\sum_{n=2}^{\infty} \frac{1}{nP(n)}$.

5.7. Prímtesztek

Könnyű-e meghatározni egy szám prímtényezős felbontását? Látszólag igen, hiszen csak meg kell nézni rendre, hogy osztható-e 2-vel, 3-mal, 5-tel stb. Ha találunk egy (prím)osztót, akkor a hányadost kell tovább bontani. Ha pedig a szám négyzetgyökéig elmenve egyáltalán nem találunk ilyen osztót, akkor a szám biztosan prím (lásd az 1.4.7a feladatot).

Ily módon gyorsan fel tudjuk bontani például a 143-at ($= 11 \cdot 13$), vagy be tudjuk látni, hogy a 197 prím (13-ig egyik prímszámmal sem osztható).

Nagy számoknál már nemigen tudjuk megvalósítani, hogy csak a prímeket próbáljuk ki, osztják-e a számot, hiszen a prímek nem állnak eleve rendelkezésünkre. Természetesen ekkor sem érdemes minden számot osztóként kipróbálni: nyilván elég, ha a vizsgált számot annyiszor osztjuk 2-vel, hogy páratlan számhoz jussunk, és ekkor már csak a páratlan számokkal való oszthatóságot kell tekinteni. Ezt a gondolatot tovább is fejleszthetjük: a 2 mellett (például) a 3 és az 5 hatványait is leválaszthatjuk ily módon, és ezután elég csak a 30-hoz relatív prím osztókat keresni.

Igazán nagy számok esetén azonban ezek a „próbaosztásos" módszerek a gyakorlatban teljesen használhatatlanok. A nehézséget az jelenti, hogy olyan sok próbálkozást kellene (számítógéppel) végrehajtani, amihez évmilliárdok sem elegendők. Sőt, a próbaosztásos módszerek továbbfejlesztett változatai, illetve az eddig kidolgozott egyéb faktorizációs algoritmusok is reménytelenül „lassúak". Egy 500-jegyű (összetett) számot, amelynek nincsenek kis prímosztói, vagy nincs valamilyen speciális tulajdonsága, a jelenlegi leggyorsabb számítógépek sem tudnának a Föld kihűlése előtt tényezőkre bontani. (Ez alapvetően megváltozhat, ha a kvantumszámítógépek hatékonyan fognak tudni működni.)

Ugyanakkor léteznek olyan eljárások, amelyek (teljes vagy majdnem teljes biztonsággal) viszonylag gyorsan eldöntik, hogy egy nagy szám prím-e vagy összetett (azonban az utóbbi esetben nem tudják megadni a tényezőket). Az ilyen algoritmusokat nevezik *prímteszt*eknek.

A gyors prímtesztek létezése első hallásra meglepőnek tűnik, különösen azzal összehasonlítva, hogy egy nemtriviális osztó megkeresése (jelenlegi ismereteink szerint) jóval kilátástalanabb feladat, mint egy tűre rálelni a szénakazalban. Ezek az algoritmusok azonban nem osztót keresnek, hanem olyan, gyorsan ellenőrizhető feltételeket vizsgálnak, amelyeket a prímek kielégítenek, az összetett számok viszont gyakorlatilag nem. (A „gyakorlatilag" azt jelenti, hogy a legtöbb módszernél az esetleges „igen ritka" kivételeket, és ezzel együtt a tévedés lehetőségének egy elenyészően csekély mértékű kockázatát meg kell engednünk.)

Speciális alakú számokra már láttunk prímteszteket, ilyen volt a Fermat-, illetve a Mersenne-számok tesztje (5.2.2, illetve 5.2.4 Tétel).

Az általános prímtesztek tárgyalása előtt megmutatjuk, hogy néhány fontos számelméleti feladat megoldására létezik gyors algoritmus.

5.7.1 Tétel **T 5.7.1**

Legyenek a, b, c és m egészek, ahol $b > 1$ és $m > 0$. Ekkor

I. a^b maradéka modulo m;

II. az a és b legnagyobb közös osztója;

III. (páratlan b és $(a, b) = 1$ esetén) az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum;

IV. az $ax + by = c$ lineáris diofantikus egyenlet megoldásai és

V. az $ax \equiv c \pmod{b}$ kongruencia megoldásai

kiszámíthatók legfeljebb $5 \log_2 b$ lépésben, ahol egy lépés két egész szám összeadását, kivonását, szorzását vagy maradékos osztását jelenti. ♣

A fentiek alapján egy 500-jegyű b szám esetén ezek a feladatok legfeljebb

$$5 \log_2 b \approx 2500 \log_2 10 < 9000$$

lépésben megoldhatók. Ezt egy gyors számítógép a másodperc töredéke alatt elvégzi, ráadásul a konkrét eljárásokat ügyesebb szervezéssel még gyorsabbá és automatikusabbá lehet tenni.

Bizonyítás: I. Az a^b szám modulo m vett maradékát az ismételt négyzetre emelések segítségével és minden lépés után az eredményt modulo m redukálva érdemes végeznünk (ez a módszer szerepelt már a 3.2 pontbeli Példában 13^{29} modulo 59 vett maradékának a meghatározásánál, valamint a Fermat-számok tesztjénél, lásd az 5.2.2 Tétel bizonyítása utáni megjegyzéseket).

Legyen $t = \lfloor \log_2 b \rfloor$, és írjuk fel a b kitevőt kettes számrendszerben. A b a számítógépben valószínűleg eleve ebben az alakban van tárolva, de más alapú számrendszerből történő átszámítás is megvalósítható legfeljebb $\log_2 b$ lépésben, hiszen az 1.2.2 Tétel szerint a számjegyeket a 2-vel történő maradékos osztások sorozatával kapjuk meg.

$$b = 2^{i_1} + 2^{i_2} + \ldots + 2^{i_s}\,, \qquad \text{ahol} \qquad 0 \le i_1 < i_2 < \ldots < i_s \le t\,.$$

Ezután ismételt négyzetre emelésekkel (és mindig mod m redukálva) számoljuk ki

$$a^2,\ a^4,\ a^8,\ \ldots,\ a^{2^t}$$

maradékát mod m. Végül az

$$a^b = a^{2^{i_1}} a^{2^{i_2}} \dots a^{2^{i_s}}$$

összefüggés alapján megkapjuk a keresett maradékot.

Például 5^{1000} modulo m kiszámításához először meghatározzuk

$$5^2,\ 5^4,\ 5^8,\ \dots,\ 5^{512}$$

maradékát modulo m, majd ezek közül a megfelelőket összeszorozzuk (és továbbra is minden lépésben csak a szorzat maradékát vesszük modulo m):

$$5^{1000} = 5^8 \cdot 5^{32} \cdot 5^{64} \cdot 5^{128} \cdot 5^{256} \cdot 5^{512}\,.$$

Az a^b modulo m maradék meghatározásához t darab négyzetre emelést és legfeljebb t darab további szorzást (és modulo m redukciót) végeztünk. Így összesen legfeljebb $2t \le 2\log_2 b$ ilyen szorzásra és redukcióra, azaz maradékos osztásra volt szükség. Ehhez hozzávéve a b kettes számrendszerbeli felírásának lépésszámát is, azt kaptuk, hogy a^b modulo m maradékát meg tudjuk kapni legfeljebb $5\log_2 b$ lépésben (ahol egy lépés egy szorzást vagy egy maradékos osztást jelent).

II. A legnagyobb közös osztó kiszámításához a legkisebb abszolút értékű maradékokkal végzett euklideszi algoritmust alkalmazzuk (azaz, amikor a maradékos osztásoknál negatív maradékot is megengedünk, és a maradék abszolút értéke legfeljebb az osztó abszolút értékének a fele, lásd az 1.2.1A Tételt):

$$\begin{aligned}
a &= bq_1 + r_1, && \text{ahol} && |r_1| \le \tfrac{b}{2},\\
b &= r_1q_2 + r_2, && \text{ahol} && |r_2| \le \tfrac{|r_1|}{2} \le \tfrac{b}{4},\\
r_1 &= r_2q_3 + r_3, && \text{ahol} && |r_3| \le \tfrac{|r_2|}{2} \le \tfrac{b}{8},\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && \text{ahol} && |r_n| \le \tfrac{|r_{n-1}|}{2} \le \tfrac{b}{2^n},\\
r_{n-1} &= r_nq_{n+1} && && (r_{n+1} = 0).
\end{aligned}$$

Az euklideszi algoritmus ebben az esetben $n+1$ lépésből áll. Mivel

$$1 \le |r_n| \le \frac{b}{2^n}\,,$$

ezért

$$2^n \le b, \qquad \text{azaz} \qquad n \le \log_2 b\,.$$

Ezzel beláttuk, hogy az euklideszi algorimus legfeljebb $1+\log_2 b$ lépést igényel (ahol egy lépés egy maradékos osztást jelent).

Megjegyezzük, hogy a szokásos módon, a legkisebb nemnegatív maradékokkal végzett euklideszi algoritmus is legfeljebb konstansszor $\log b$ lépésből áll, lásd az 5.7.1 feladatot.

III. A 4.3.2 Tétel alapján a Jacobi-szimbólum kiszámítását a „számlálóban" szereplő kettőhatványok leválasztásával és a reciprocitási tétel ismételt alkalmazásával végezhetjük, ami tulajdonképpen az előbbi euklideszi algoritmus egy variánsa (lásd a 4.3.2 Tétel utáni Példát).

Nézzük mindezt részletesen. Az $\left(\frac{a}{b}\right)$ számolásánál az a-t b-vel maradékosan elosztva azt kapjuk, hogy

$$\left(\frac{a}{b}\right)=\left(\frac{r}{b}\right),\qquad \text{ahol}\qquad |r|<\frac{b}{2}\,.$$

Szükség esetén $\left(\frac{-1}{b}\right)$ felhasználásával azt is elérhetjük, hogy $r>0$ teljesüljön. Ha r páros, akkor a következő lépésben $\left(\frac{2}{b}\right)$ kiemelése után a „számláló" ismét feleződik. Ha r páratlan, akkor a reciprocitási tétel alapján az r a „nevezőbe" kerül, az új „számláló" pedig a b-nek az r szerinti s maradéka, ahol $|s|<r/2$, és ismét elérhető, hogy $s>0$ legyen. Ez azt jelenti, hogy a „számláló" minden lépésben legalábbis feleződik, és így a lépésszám most is legfeljebb $\log_2 b$. Ehhez hozzájön még, hogy $\left(\frac{-1}{v}\right)$ és $\left(\frac{2}{v}\right)$ kiszámításához szükség van a v-nek modulo 4, illetve modulo 8 maradékára, ez egy-egy maradékos osztással megkapható, illetve a v kettes számrendszerbeli alakjának utolsó két, illetve három jegyéből azonnal leolvasható. Hasonlóan egyszerű a „számláló" paritásának a megállapítása, illetve páros esetben a felezése is.

Természetesen $\left(\frac{a}{b}\right)$ csak akkor értelmes, ha $b>1$ páratlan szám és $(a,b)=1$. Ez utóbbi feltétel teljesülését az euklideszi algoritmus segítségével előre is ellenőrizhetjük, azonban erre nincs szükség. Ha ugyanis $(a,b)=d>1$, akkor a fenti eljárást végezve előbb-utóbb egy olyan helyzet adódik, ahol a számláló d, a nevező pedig többszöröse d-nek (lásd az 5.7.2 feladatot), és itt nyilvánvalóan elakadtunk, tehát nem létezik az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum. (Az $(a,b)=1$ esetben ez nem fordulhat elő, akkor az utolsó lépésben egy $\left(\frac{\pm1}{v}\right)$ vagy $\left(\frac{\pm2}{v}\right)$ Jacobi-szimbólumot kell kiszámolnunk.)

IV–V. A 2.5 pontban láttuk, hogy a két probléma ekvivalens. Továbbá az 1.3.6 és 1.3.5 (vagy a 7.1.1) Tételek szerint az $ax+by=c$ diofantikus egyenlet megoldásait az euklideszi algoritmus segítségével állíthatjuk elő, és innen a kívánt lépésszámbecslés is leolvasható. ■

Most rátérünk a prímtesztek tárgyalására. A legegyszerűbb általános prímteszt azonnal következik a kis Fermat-tételből:

Ha egy $n > 2$ számra $2^{n-1} \not\equiv 1 \pmod{n}$, akkor n összetett.

Az 5.7.1 Tétel alapján ez a feltétel valóban gyorsan ellenőrizhető.

Tisztáznunk kell azonban az alábbi fontos kérdést: milyen következtetést vonhatunk le n-re, ha $2^{n-1} \equiv 1 \pmod{n}$?

Sajnos ekkor nem lehetünk teljesen biztosak abban, hogy az n prím, ugyanis végtelen sok olyan n *összetett* szám létezik, amelyre $2^{n-1} \equiv 1 \pmod{n}$. Ezeket 2-es alapú *álprím*eknek vagy *pszeudoprím*eknek nevezzük (a legkisebb a 341).

Megmutatható azonban, hogy a 2-es alapú álprímek *ritkák* a prímekhez képest: az x-nél nem nagyobb álprímek számának és $\pi(x)$-nek a hányadosa $x \to \infty$ mellett (nagyon erősen) 0-hoz tart. (Ezt *illusztrálandó* egy konkrét számpéldát is mutatunk: 10^{10}-ig a 2-es alapú álprímek száma 14 887, a prímek száma pedig 455 052 511, az arányuk körülbelül egy a harmincezerhez.)

Mindezek alapján, ha egy nagy n számra $2^{n-1} \equiv 1 \pmod{n}$ teljesül, akkor azt mondhatjuk, hogy az n „nagy valószínűséggel prím". Ezt a kijelentést úgy kell érteni, hogy ha a tesztet sok, véletlenszerűen választott n-re alkalmazzuk, akkor csak igen ritkán (gyakorlati szempontból nézve szinte sohasem) fordulhat elő, hogy 2^{n-1} maradéka 1, és az n mégis összetett.

Mindezek lényegét az alábbi tételben is összefoglaljuk:

5.7.2 Tétel **T 5.7.2**

Legyen $n > 2$. Ha $2^{n-1} \not\equiv 1 \pmod{n}$, akkor n biztosan összetett. Ha $2^{n-1} \equiv 1 \pmod{n}$, akkor n „majdnem biztosan" prím. A feltétel gyorsan ellenőrizhető, ha a hatványozást ismételt négyzetre emelések segítségével végezzük. ♣

A tesztet többféleképpen is továbbfejleszthetjük: a^{n-1} maradékát modulo n nemcsak az $a = 2$ értékre, hanem (mondjuk) az 1000-nél kisebb összes prímszámra is kiszámítjuk; ha legalább egy a-ra ez a maradék nem 1 (és $n > 1000$), akkor n a kis Fermat-tétel szerint biztosan összetett. Még hatékonyabb, ha az első valahány prím helyett véletlenszerűen választott, n-nel nem osztható számokat veszünk a-nak (lásd az 5.7.13 feladatot).

Ha mindegyik kipróbált a-ra $a^{n-1} \equiv 1 \pmod{n}$, akkor n „még inkább majdnem biztosan" prím, azonban sajnos továbbra sem lehetünk ebben teljesen biztosak. Léteznek ugyanis olyan összetett számok, amelyekre bármely

$(a, n) = 1$ esetén $a^{n-1} \equiv 1 \pmod{n}$, ilyen például az 1729 (lásd a 2.4.15c feladatot). Az ilyen számokat *univerzális álprím*eknek vagy *Carmichael-szám*oknak nevezzük.

Az álprímek „típusait" külön definícióban is összefoglaljuk:

5.7.3 Definíció **D 5.7.3**

Ha egy n összetett számra $a^{n-1} \equiv 1 \pmod{n}$ teljesül, akkor az n-et *a alapú álprím*nek nevezzük.

Ha az n összetett számra a fenti kongruencia minden $(a, n) = 1$ esetén teljesül, akkor az n *univerzális álprím* vagy *Carmichael-szám*. ♣

Minden esetben ugyanúgy használható az „álprím" helyett a „pszeudoprím" elnevezés is.

A Carmichael-számok ekvivalens karakterizációira nézve lásd az 5.7.7 feladatot.

Régóta ismert, hogy bármely $a > 1$ esetén végtelen sok a alapú álprím létezik (lásd az 5.7.5 feladatot). Azt azonban csak 1992-ben sikerült igazolni, hogy az univerzális álprímek száma is végtelen.

Az alábbiakban két olyan prímtesztet tárgyalunk, amelyek már az álprímeket is „leleplezik". Mindkettőben „véletlen" számokat használunk, amin (legalábbis elvileg) azt értjük, hogy egész számoknak egy „nagyméretű", de véges halmazából egymás után „kiveszünk" elemeket úgy, hogy bármely elem kiválasztásának „ugyanannyi a valószínűsége" (mintha egy urnából golyókat húznánk ki visszatevéssel). Például egy kettes számrendszerben 2000-jegyű véletlen számot úgy kaphatunk, hogy az első jegy 1-es, a többi számjegyet pedig 1999 egymás utáni pénzfeldobás eredményeként állapítjuk meg. A gyakorlatban természetesen a számítógép „dobálja a pénzérmét", illetve valójában valamilyen véletlenszám-generátort használ (amely tulajdonképpen általában csak a véletlent nagyon jól „utánzó" ún. „álvéletlen" számsorozatokat produkál.)

5.7.4 Tétel (Solovay–Strassen-prímteszt) **T 5.7.4**

(A) Legyen $n > 1$ páratlan szám, és tekintsük az

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{1}$$

kongruenciát, ahol $\left(\frac{a}{n}\right)$ a Jacobi-szimbólum.

Ha n prím, akkor (1) minden $a \not\equiv 0 \pmod{n}$ esetén teljesül.

Ha n összetett, akkor (1) egy modulo n teljes maradékrendszer elemeinek kevesebb, mint a felére teljesül.

(B) Az (A) kritérium alapján a következőképpen dönthetjük el egy nagy páratlan n-ről, hogy prím-e vagy összetett. Válasszunk (mondjuk) 1000 véletlen $a \not\equiv 0 \pmod{n}$ értéket, és mindegyikre vizsgáljuk meg, hogy az (1) feltétel teljesül-e. Ha legalább egy esetben nem teljesül, akkor az n biztosan összetett. Ha mind az 1000 esetben teljesül, akkor 2^{-1000}-nél kisebb annak a valószínűsége, hogy az n összetett. ♣

Megjegyzések: 1. Ha $(a, n) > 1$, akkor az $\left(\frac{a}{n}\right)$ Jacobi-szimbólum nem értelmes, tehát (1) eleve nem teljesülhet.

2. Az 5.7.1 Tétel alapján az (1) feltétel (akár ezer a-ra is) gyorsan ellenőrizhető.

3. A Solovay–Strassen-teszt is magában hordozza annak a lehetőségét, hogy egy összetett számot tévesen prímnek „nyilvánítunk". Az 5.7.2 Tétel tesztjéhez képest azonban mind elméleti, mind pedig gyakorlati szempontból óriási az előrelépés.

Az 5.7.2 Tétel tesztjénél a 2-es alapú álprímeket egyáltalán nem tudjuk leleplezni, az ilyen számokra a teszt *teljesen* csődöt mond, vagyis egy *konkrét* álprím esetén „száz százalékosan" tévedünk, amikor a teszt alapján prímnek véljük (csak szerencsére ritkán botlunk álprímekbe). Ugyanígy, egy nagy univerzális álprím tesztelésére a továbbfejlesztett változat sem alkalmas, hiába próbálunk ki akár egymillió a értéket is; egy ilyen n-et ismét csak tévesen gondolunk prímnek (hacsak nem került véletlenül egy n-hez nem relatív prím az a-k közé, de ennek gyakorlatilag nulla az esélye).

Ugyanakkor a Solovay–Strassen-teszt elől egyetlen összetett szám sem „bújhat el", erre nézve nincsenek „álprímek"; bármely összetett n esetén rengeteg „tanú" igazolja az n összetettségét. Ez egyben azt is jelenti, hogy a tévedés valószínűségét (a tesztelt számtól függetlenül) tetszőlegesen kicsire tudjuk leszorítani, ha elég sok a értéket próbálunk ki. (Ebből a szempontból az ezer próbánál adódó 2^{-1000}-es hibalehetőség tökéletes biztonságot nyújt.)

Bizonyítás: A (B) rész az (A) rész közvetlen következménye, így elég csak az utóbbit igazolnunk.

Ha n prím, akkor (1) azonnal adódik a 4.1.2 Tételből és a Legendre-szimbólum definíciójából (lásd a 4.1.3 Definíció utáni (2) képletet).

Legyen az n összetett. Mivel (1) eleve csak az n-hez relatív prím a-kra teljesülhet, ezért elegendő azt megmutatni, hogy (1)-et egy modulo n redukált maradékrendszer elemeinek legfeljebb a fele elégíti ki.

Egy n-hez relatív prím a számot nevezzünk *tanú*nak, ha (1) nem teljesül, és *cinkos*nak, ha (1) teljesül. Ezzel a terminológiával élve azt kell igazolnunk, hogy egy redukált maradékrendszer elemeinek legalább a fele tanú.

Első lépésként megmutatjuk, hogy minden páratlan összetett n-hez létezik tanú.

Vizsgáljuk először azt az esetet, amikor az n nem négyzetmentes, tehát van olyan q prím, amelyre $q^2 \mid n$. Jelölje az n különböző prímosztóit $q = q_1, q_2, \ldots, q_s$, legyen g primitív gyök modulo q^2, és legyen v az

$$x \equiv g \pmod{q^2}, \qquad x \equiv 1 \pmod{q_i}, \qquad 2 \le i \le s$$

szimultán kongruenciarendszer egy megoldása (ha $s = 1$, akkor legyen $v = g$). Megmutatjuk, hogy v tanú.

Mivel minden i-re $(v, q_i) = 1$, ezért $(v, n) = 1$. Tegyük fel indirekt, hogy

$$v^{\frac{n-1}{2}} \equiv \left(\frac{v}{n}\right) \pmod{n}. \tag{2}$$

A (2) kongruenciát négyzetre emelve kapjuk, hogy

$$v^{n-1} \equiv \left(\frac{v}{n}\right)^2 = 1 \pmod{n}. \tag{3}$$

Mivel $q^2 \mid n$, ezért a (3) kongruencia akkor is teljesül, ha az n modulus helyett a q^2 modulusra nézzük; ekkor $v \equiv g \pmod{q^2}$-et is felhasználva

$$g^{n-1} \equiv 1 \pmod{q^2} \tag{4}$$

adódik. Mivel a g primitív gyök mod q^2, azaz a rendje $\varphi(q^2) = q(q-1)$, ezért (4) alapján $q(q-1) \mid n-1$. Ugyanakkor $q^2 \mid n$ is igaz, vagyis q az n-nek és az $n-1$-nek is osztója, ami ellentmondás.

Most nézzük azt az esetet, amikor az n négyzetmentes, azaz $n = q_1 \ldots q_s$, ahol a q_i-k különböző prímek és $s \ge 2$.

Legyen a kvadratikus nemmaradék modulo q_1 és t az

$$x \equiv a \pmod{q_1}, \qquad x \equiv 1 \pmod{q_i}, \qquad 2 \le i \le s. \tag{5}$$

szimultán kongruenciarendszer egy megoldása. Megmutatjuk, hogy t tanú.

Indirekt tegyük fel, hogy t-re teljesül (1). Ekkor $(t, n) = 1$ és

$$\left(\frac{t}{n}\right) = \left(\frac{t}{q_1}\right)\left(\frac{t}{q_2}\right)\ldots\left(\frac{t}{q_s}\right) = \left(\frac{a}{q_1}\right)\left(\frac{1}{q_2}\right)\ldots\left(\frac{1}{q_s}\right) = -1.$$

Ezért (1) alapján

$$t^{\frac{n-1}{2}} \equiv -1 \pmod{n}.$$

Mivel $q_2 \mid n$ és az (5) szerint $t \equiv 1 \pmod{q_2}$, így

$$-1 \equiv t^{\frac{n-1}{2}} \equiv 1 \pmod{q_2} \tag{6}$$

ami ellentmondás. Így t valóban tanú.

Ezzel megmutattuk, hogy minden páratlan összetett n-hez létezik tanú.

Végül belátjuk, hogy egy redukált maradékrendszer elemeinek legalább a fele tanú.

Legyen t egy tetszőleges tanú, és legyenek $c_1, c_2, \ldots, c_k$ páronként inkongruens cinkosok. Belátjuk, hogy ekkor $tc_1, \ldots, tc_k$ páronként inkongruens tanúk.

Egyrészt $(t, n) = (c_i, n) = 1$ miatt $(tc_i, n) = 1$ is teljesül, másrészt (ismét $(t, n) = 1$-et is felhasználva kapjuk, hogy) a tc_i elemek is páronként inkongruensek modulo n. Tegyük fel indirekt, hogy valamely i-re tc_i cinkos lenne, azaz

$$(tc_i)^{\frac{n-1}{2}} \equiv \left(\frac{tc_i}{n}\right) \pmod{n} \tag{7}$$

teljesülne. Mivel c_i is cinkos, ezért

$$c_i^{\frac{n-1}{2}} \equiv \left(\frac{c_i}{n}\right) \pmod{n} \tag{8}$$

is igaz. A (7) és (8) kongruenciákat összeszorozva azt kapjuk, hogy

$$t^{\frac{n-1}{2}} c_i^{n-1} \equiv \left(\frac{t}{n}\right)\left(\frac{c_i}{n}\right)^2 \pmod{n}. \tag{9}$$

(8)-at négyzetre emelve

$$c_i^{n-1} \equiv \left(\frac{c_i}{n}\right)^2 = 1 \pmod{n}$$

adódik, és ezt (9)-be beírva azt nyerjük, hogy

$$t^{\frac{n-1}{2}} \equiv \left(\frac{t}{n}\right) \pmod{n},$$

vagyis t is cinkos, ami ellentmondás.

Ezzel beláttuk, hogy ha páronként inkongruens cinkosokat egy tanúval végigszorzunk, akkor páronként inkongruens tanúkat kapunk. Ez viszont azt jelenti, hogy egy redukált maradékrendszer elemei között legalább annyi tanú van, mint cinkos, vagyis az elemeknek legalább a fele tanú. ■

A következő prímteszt kiindulópontja a kis Fermat-tétel, valamint az, hogy ha p prím és $u^2 \equiv 1 \pmod{p}$, akkor csak $u \equiv \pm 1 \pmod{p}$ lehetséges. Ennek megfelelően, ha $p \nmid a$, akkor az

$$a^{p-1},\ a^{\frac{p-1}{2}},\ a^{\frac{p-1}{4}},\ \ldots$$

számok modulo p vett legkisebb abszolút értékű maradékainak sorozata mindenképpen 1-gyel kezdődik és vagy végig 1, vagy pedig az első 1-től különböző maradék szükségképpen -1. Ugyanakkor megmutatjuk, hogy ha p helyett egy tetszőleges n összetett számot veszünk, akkor sok a-ra már nem ilyen maradéksorozatot kapunk. Ennek megfelelően a következő prímtesztet nyerjük (a fenti feltételt technikai okokból kissé módosított alakban, lényegében a „fordított" sorozatra adjuk meg):

5.7.5 Tétel (Miller–Lenstra–Rabin-prímteszt) **T 5.7.5**

Legyen $n > 1$ páratlan szám, $n - 1 = 2^k r$, ahol r páratlan. Az

$$a^r,\ a^{2r},\ a^{4r},\ \ldots,\ a^{2^{k-2}r} = a^{\frac{n-1}{4}},\ a^{2^{k-1}r} = a^{\frac{n-1}{2}} \tag{10}$$

számokat jó sorozatnak nevezzük, ha ezek modulo n vett legkisebb abszolút értékű maradékai között előfordul -1 vagy pedig a^r maradéka 1.

Ha n prím, akkor (10) minden $a \not\equiv 0 \pmod{n}$ esetén jó sorozat.

Ha n összetett, akkor (10) egy modulo n teljes maradékrendszer elemeinek kevesebb, mint a felére alkot jó sorozatot. ♣

Ez a kritérium gyorsan ellenőrizhető: ismételt négyzetre emelések segítségével kiszámítjuk a^r maradékát modulo n, majd ebből a sorozat további elemei egy-egy újabb négyzetre emeléssel adódnak.

A kritérium alapján az 5.7.4 Tétel (B) részéhez hasonlóan megfogalmazhatjuk magát a konkrét eljárást is.

A bizonyítás vázlata: Az 5.7.4 Tétel bizonyításának menetét és (értelemszerűen módosított) tanú-cinkos szóhasználatát követjük.

Ha n prím, akkor az 5.7.5 Tétel kimondása előtt vázoltuk, hogy minden $p \nmid a$ esetén jó sorozatot kapunk.

Ha n összetett és nem négyzetmentes, akkor ugyanúgy kaphatunk tanút, mint az 5.7.4 Tétel bizonyításában.

Ha n összetett és négyzetmentes, akkor tekintsük azt a legnagyobb $0 \le j \le k-1$ számot, amelyhez van olyan $(a,n)=1$, hogy

$$a^{2^j r} \not\equiv 1 \pmod{n}\,. \tag{11}$$

Mivel van olyan j és a, amelyre (11) teljesül, például $j=0$ és $a=-1$ megfelel [hiszen $(-1)^r \not\equiv 1 \pmod{n}$], ezért a jelzett maximális j is valóban létezik.

A (11)-ből következik, hogy az n egyik prímosztójára, mondjuk q_1-re

$$a^{2^j r} \not\equiv 1 \pmod{q_1}\,.$$

Ekkor az 5.7.4 Tétel bizonyításában az (5) kongruenciarendszer szerint gyártott t tanú. Ugyanis az ottani gondolatmenethez hasonlóan kapjuk, hogy

$$t^{2^j r} \not\equiv \pm 1 \pmod{n}\,,$$

ugyanakkor j definíciója szerint ($j < k-1$ esetén)

$$z^{2^{j+1} r} \equiv 1 \pmod{n}\,.$$

Végül, ha *ezt* a t tanút vagy a nem négyzetmentes esetben kapott v tanút páronként inkongruens cinkosokkal megszorozzuk, akkor az 5.7.4 Tétel bizonyításában látott módon páronként inkongruens tanúkat kapunk (a t helyett tetszőleges tanút véve ez nem feltétlenül igaz). Ezzel megmutattuk, hogy összetett n esetén egy redukált maradékrendszer elemeinek legalább a fele tanú. ■

Megjegyzések: 1. A Miller–Lenstra–Rabin-teszt valójában az 5.7.5 Tételben jelzett mértéknél is jóval hatékonyabb: finomabb módszerekkel az is megmutatható, hogy egy redukált maradékrendszer elemeinek *több, mint a háromnegyede* tanú.

2. A Solovay–Strassen- és a Miller–Lenstra–Rabin-tesztet összehasonlítva kiderül, hogy az utóbbi eredményesebben „leplezi le" az összetett számokat, lásd az 5.7.17 feladatot.

Végül megemlítjük, hogy 2002-ben három indiai matematikus, Agrawal, Kayal és Saxena egy olyan gyors prímtesztet talált, amely (nem 99,99999…, hanem) 100 százalékos biztonsággal állapítja meg egy n számról, hogy prím

vagy összetett. Ez a teszt is a kis Fermat-tételből indul ki, mégpedig annak polinomokra vetített változatából. Röviden vázoljuk az alapötletet.

Legyen $(c,n)=1$, és tekintsük az $f_c = x^n - c$ és $g_c = (x-c)^n$ polinomokat $\mathbf{Z}_n$ felett. Ha n prím, akkor $f_c = g_c$ (tehát azonosak a megfelelő együtthatók, ami többet jelent a helyettesítési értékek egyezésénél). Ugyanis a $-c$ és $(-c)^n$ konstans tagokra ez a kis Fermat-tételből következik, a főegyütthatók értéke 1, a g_c többi együtthatója pedig $\binom{n}{k}(-c)^k$, ami n prím volta miatt osztható n-nel (lásd a 2.1.9a feladatot), tehát $\mathbf{Z}_n$-ben 0. Az is könnyen adódik, hogy összetett n esetén van olyan k, amelyre $\binom{n}{k}$ nem osztható n-nel, és így $(c,n)=1$ miatt g_c-ben x^{n-k} együtthatója nem 0, vagyis $f_c \neq g_c$. Ez tehát egy tökéletes prímteszt (pl. $c=1$-gyel), csak sajnos reménytelenül lassú, hiszen g együtthatóinak a kiszámítása a tagok nagy száma miatt még ismételt négyzetre emelésekkel is rengeteg lépést igényel.

Az AKS-teszt nagy ötlete, hogy $f_c = g_c$ helyett csak azt ellenőrizzük, hogy f_c és g_c egy alkalmas $h \in \mathbf{Z}_n[x]$ polinommal osztva azonos maradékot ad-e. Ha h foka (n-hez képest) elég alacsony, akkor ez a számolás már kivitelezhető, hiszen az ismételt négyzetre emeléseknél mindig redukálunk „mod h” is. Ez különösen kényelmes, ha $h = x^r - 1$ alakú polinom, hiszen ekkor csak az x-hatványok kitevőit kell redukálni mod r (vagyis x^j helyére x^{j-r}-et írunk, amíg csak lehetséges).

Ha n prím, akkor természetesen $f_c = g_c$ miatt bármely h szerinti maradékuk is egyenlő. Az AKS-teszt lényege, hogy ha alkalmas r-et választunk, akkor az összetett számok ezt nem teljesítik, vagyis minden összetett n-hez van olyan $c \leq K$ (ahol K az n-hez képest „igen kicsi”), hogy f_c és g_c maradéka nem ugyanaz $x^r - 1$-gyel osztva.

A teszt algoritmusa ennek alapján a megfelelő r kiválasztása után „végigpróbálja” $c = 1, 2, \ldots, K$-ra, hogy $f_c \equiv g_c \pmod{x^r - 1}$ fennáll-e. Ha ez valamelyik c-re nem igaz, akkor n biztosan összetett (ez már a kiinduló meggondolásainkból következik), ha viszont mindegyik c-re igaz, akkor n biztosan prím (ennek belátása a teszt „nehéz” része).

Az r-nek egy „nem túl nagy” és bizonyos tulajdonságokkal rendelkező prímszámot kell választani, ennek létezését egy mély számelméleti tétel biztosítja. Az, hogy ezen r mellett az összetett számok már „néhány” c valamelyikénél is szükségképpen „lelepleződnek”, a véges testekre vonatkozó alapvető tételek felhasználásával igazolható.

Feladatok

5.7.1 Tekintsük az $a > b > 0$ számokra a szokásos euklideszi algoritmust, ahol a keletkező maradékokra $b = r_0 > r_1 > r_2 > \ldots \geq 0$ teljesül.

a) Mutassuk meg, hogy bármely k-ra $r_{k+2} < \frac{r_k}{2}$.

b) Milyen felső becslés adódik innen az algoritmus lépésszámára?

*c) Igazoljuk, hogy ha az algoritmus lépésszáma pontosan s, akkor b lehető legkisebb értéke φ_{s+1}, ahol φ_j a j-edik Fibonacci-szám (a definíciót lásd az 1.2.5 feladatban).

Megjegyzés: A Fibonacci-számok

$$\varphi_j = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^j - \left(\frac{1-\sqrt{5}}{2}\right)^j\right)$$

képlete alapján a c) részből következik, hogy a szokásos euklideszi algoritmus lépésszáma legfeljebb $\log_\gamma b + \delta$, ahol $\gamma = (1+\sqrt{5})/2$ és δ alkalmas konstans, és ez a becslés tovább már nem javítható.

5.7.2 Tekintsük az $\left(\frac{a}{b}\right)$ Jacobi-szimbólum kiszámítására az 5.7.1 Tétel bizonyításának III. pontjában látott eljárást. Mutassuk meg, hogy ha ezt $(a,b) = d > 1$ mellett alkalmazzuk, akkor végül egy olyan helyzethez jutunk, ahol a „számláló" d, a „nevező" pedig többszöröse d-nek. (Ez azt jelenti, hogy ily módon is kiderül, ha a Jacobi-szimbólum nem értelmes, és így a és b relatív prímségét nem kell előre külön ellenőrizni.)

5.7.3 Mutassuk meg, hogy a 341 kettes alapú álprím, de nem hármas alapú álprím.

M 5.7.4 Bizonyítsuk be, hogy ha az n kettes alapú álprím, akkor $2^n - 1$ is az.

5.7.5 Legyen $a > 1$. Bizonyítsuk be, hogy ha a $p > 2$ prím nem osztója $a \pm 1$-nek, akkor az

$$n = \frac{a^{2p} - 1}{a^2 - 1}$$

szám a alapú álprím. (Az $a = 2$, $p = 5$ esetben $n = 341$.)

5.7.6 Igazoljuk, hogy az 561 univerzális álprím.

5.7.7 Bizonyítsuk be, hogy egy n összetett számra az alábbi három feltétel bármelyike ekvivalens.

a) Bármely $(a,n) = 1$ esetén $a^{n-1} \equiv 1 \pmod{n}$.

b) Az n négyzetmentes, továbbá $p \mid n \Longrightarrow p - 1 \mid n - 1$.

c) Bármely a-ra $a^n \equiv a \pmod{n}$.

Megjegyzés: Ennek alapján az univerzális álprím definíciójában a) helyett a c) [vagy a b)] feltételt is választhattuk volna.

5.7.8 Mutassuk meg, hogy egy univerzális álprímnek legalább három prímosztója van.

5.7.9

a) A tárgyalt prímteszteknél a feltétel ellenőrzése előtt nem szükséges külön megnézni, hogy a kipróbált a és a vizsgált n relatív prímek-e. Milyen előny származhat abból, ha mégis kiszámítjuk (a, n) értékét?

b) Ha az n két százjegyű prím szorzata, akkor „nagyjából" mekkora a valószínűsége annak, hogy egy véletlenszerűen választott a szám az n-hez *nem* relatív prím?

5.7.10 Mutassuk meg, hogy ha $a^2 \equiv 1 \pmod{n}$, de $a \not\equiv \pm 1 \pmod{n}$, akkor az n-nek gyorsan meg tudjuk határozni egy nemtriviális osztóját.

*5.7.11 Bizonyítsuk be, hogy ha n-en kívül ismerjük a $\varphi(n)$ egy (nemnulla) többszörösét is, akkor gyorsan elő tudjuk állítani az n kanonikus alakját. (Pontosabban, az eljárásban *elvileg* fennáll annak a lehetősége, hogy mégsem sikerül az n-et prímtényezőkre bontani, de *gyakorlatilag* ez sohasem fordulhat elő.)

5.7.12 Vizsgáljuk meg, alkalmas-e prímtesztnek a Wilson-tétel és megfordítása, azaz ha azt ellenőrizzük, hogy n osztója-e $(n-1)! + 1$-nek.

5.7.13

a) Mutassuk meg, hogy ha az n összetett szám nem univerzális álprím, akkor $a^{n-1} \equiv 1 \pmod{n}$ egy modulo n teljes maradékrendszer elemeinek kevesebb, mint a felére teljesül.

b) Írjuk le az a) részen alapuló konkrét prímtesztet.

5.7.14 Mutassuk meg, hogy az alábbi prímteszt gyors, és a tévedés lehetősége akármilyen pici (előre megadott) korlát alá szorítható.

Az $n > 1$ páratlan számról akarjuk eldönteni, hogy prím-e. Adott darabszámú (de elég sok) véletlen $n \nmid a$-ra megnézzük $a^{(n-1)/2}$ maradékát modulo n. Az n-et akkor „nyilvánítjuk" prímnek, ha az összes vizsgált a-ra a maradék ± 1, de van köztük -1 is.

5.7.15 Legyen $n = 2^k r + 1$, ahol $k \geq 1$, r páratlan és $0 < r < 2^k$. Tegyük fel, hogy egy a egész számra

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}.$$

Lássuk be, hogy ekkor n prím.

5.7.16 Legyen $n > 2$. Mutassuk meg, hogy az alábbi feltételek bármelyikéből következik, hogy az n prím.

a) Van olyan a egész szám, amelyre $a^{n-1} \equiv 1 \pmod{n}$, és az $n-1$ bármely p_i prímosztójára

$$a^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}\,.$$

*b) Az $n-1$ bármely p_i prímosztójához van olyan a_i egész szám, amelyre

$$a_i^{n-1} \equiv 1 \pmod{n} \qquad \text{és} \qquad a_i^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}\,.$$

*c) Létezik az $n-1$-nek egy $\sqrt{n}$-nél nagyobb c osztója a következő tulajdonsággal: a c bármely p_i prímosztójához van olyan a_i egész szám, amelyre

$$a_i^{n-1} \equiv 1 \pmod{n} \qquad \text{és} \qquad \left(a_i^{\frac{n-1}{p_i}} - 1\,,\, n\right) = 1\,.$$

M*5.7.17 Mutassuk meg, hogy a Miller–Lenstra–Rabin-teszt hatékonyabb a Solovay–Strassen-tesztnél az alábbi értelemben. Ha egy adott n-re az a tanú a Solovay–Strassen-tesztnél, akkor ugyanez az a tanú a Miller–Lenstra–Rabin-tesztnél is; vagyis, ha egy a-ra az 5.7.4 Tételnél szereplő (1) feltétel nem teljesül, akkor erre az a-ra az 5.7.5 Tételnél megadott (10) számhalmaz nem alkothat jó sorozatot.

5.8. Titkosírás

A klasszikus titkosírási sémákban A és B előre megegyeznek egy T titkosító kulcsban (például minden betű helyett az ábécé rákövetkező betűjét írják), amelynek az inverze az M megfejtő kulcs (az előző esetben ez minden betű helyett az azt megelőzőt jelenti). Ekkor A az üzenet helyett annak T szerint titkosított változatát küldi el B-nek, aki azt az M segítségével fejti meg.

Ezek a kulcsok nemcsak betűkre, hanem hosszú betűsorozatokra is vonatkozhatnak, és rendkívül bonyolultak is lehetnek. Ezekben a ma már csak számítógéppel kezelhető hatalmas rendszerekben a gép a kulcsok szabályai szerint végzi a titkosítást, illetve a megfejtést, és az üzenettovábbítás is futár helyett elektronikus úton történik.

Ezek a sémák kielégítik azt a két alapkövetelményt, hogy A üzenetét csak B érti meg, továbbá egy harmadik fél nem tud hamis üzenetet küldeni A nevében B-nek. Hátrányt jelent azonban, hogy nehézkes (és veszélyes) a kulcs előzetes egyeztetése; nem dönthetők el az A és B között esetleg felmerülő viták,

hiszen a közös T és M kulcsok birtokában akármelyikük képes a másik nevében „hamis” üzenetet gyártani; továbbá a több féllel történő kapcsolattartásnál (pl. az üzleti életben) minden partnerhez új kulcspár szükséges.

Diffie és Hellman 1975-ben egy forradalmian új elven alapuló titkosírási sémát javasolt. Ebben a T kulcsot nyilvánosságra hozzuk, és csak az M kulcsot tartjuk titokban.

Ez első hallásra képtelen ötletnek hangzik, hiszen ha az egyik irányban ismeri valaki az eljárást, akkor a másik irányban is meg tudja adni. Valóban, legyenek a T és M függvények (amelyek egymás inverzei) például az $\{1, 2, \ldots, N\}$ halmaz bijekciói (látni fogjuk, hogy ez az általánosság megszorítása nélkül mindig feltehető). Ha meg akarjuk határozni (mondjuk) $M(5)$-öt, akkor a nyilvános T kulcs segítségével sorban kiszámítjuk a $T(1), T(2), \ldots$ értékeket, amíg az 5-öt meg nem kapjuk; az $M(5)$ függvényérték az a k lesz, amelyre $T(k) = 5$.

Ez *elvben* szépen hangzik, azonban ha N mondjuk egy 500-jegyű szám, akkor ez az út a *gyakorlatban* már nem járható. Ekkor ugyanis bármely számítógép évmilliárdok alatt is a $T(1), T(2), \ldots$ értékeknek csak egy elenyésző töredékét tudná meghatározni, vagyis majdnem biztos, hogy $M(5)$-öt sohasem találná meg. (A helyzetet megpróbáljuk az alábbi — ma már kissé anakronisztikus — hasonlattal érzékeltetni. Egy nyomtatott angol-magyar szótár elvben használható magyar-angol szótárként is: ha például az „ablak” szó angol megfelelőjét keressük, akkor sorra nézzük az angol-magyar szótár ábécérendben szereplő angol szavait, amíg a magyar jelentések között az „ablak” fel nem bukkan. Ez — meglehetősen hosszú idő múlva — a „window”-nál be is következik. Így ez a módszer a gyakorlatban nem működik.)

Mindezek alapján nem elképzelhetetlen, hogy a T kulcs nyilvános ismerete mellett is az M kulcs egyedül az illetékes személy titka maradjon. Nézzük, hogyan működik az ezen az elven alapuló ún. *nyilvános jelkulcsú titkosírás*.

Minden szereplő elkészít magának egy T, M kulcspárt, amelyek egymás inverzei, a T kulcsot nyilvánosságra hozza, az M kulcsot viszont titokban tartja. Legyen az A kulcspárja T_A, M_A, a B kulcspárja pedig T_B, M_B. Ekkor A az u üzenet helyett a $v = T_B(M_A(u))$ értéket küldi el B-nek, aki ezt a következőképpen fejti meg: $u = T_A(M_B(v))$. Ez valóban igaz, hiszen

$$T_A(M_B(v)) = T_A(M_B(T_B(M_A(u)))) = T_A(M_A(u)) = u\,.$$

(Az A a v kiszámításához szükséges M_A függvényt ismeri, a nyilvános T_B függvényt pedig kikeresi a teletitok–könyvből, a B-nél hasonló a helyzet M_B-vel és T_A-val.)

Most is teljesül az a két alapkövetelmény, hogy A üzenetét csak B érti meg, hiszen senki más nem ismeri a megfejtéshez szükséges M_B-t, továbbá egy

harmadik fél nem tud hamis üzenetet küldeni A nevében B-nek, hiszen csak A ismeri a kódoláshoz szükséges M_A-t.

Emellett nincs szükség előzetes kulcsegyeztetésre, és mindenki használhatja ugyanezeket a kulcsait másokkal történő levelezésben is. Végül A és B között sem merülhet fel vita az üzenetről, mert a hamisíthatatlan „elektronikus aláírásként" működő M_A akár bíróság előtt is egyértelműen bizonyítja a levél valódiságát.

A rendszer megvalósításához tehát olyan T, M kulcspárokra van szükség, hogy a kulcstulajdonos egy alkalmas, csak az ő rendelkezésére álló információ alapján mindkét kulcsot ismerje, azonban mások még a nyilvánosságra hozott T birtokában se legyenek képesek M-et meghatározni.

Korábban láttuk, hogy ilyen „magántitok" például egy nagy szám prímtényezős felbontása, amelyet csak az ismer, aki ezeket a prímtényezőket összeszorozta. Ezt használta fel Rivest, Shamir és Adleman 1976-ban a Diffie–Hellman-féle elv egy konkrét megvalósításához, amelyet ma RSA-sémának nevezünk. (Az elnevezés a felfedezők (vagy feltalálók?) nevének kezdőbetűiből származik.)

Az RSA-séma ismertetése előtt megmutatjuk, hogy tetszőleges titkosírási rendszer visszavezethető arra az esetre, amikor a T és M függvények az $\{1, 2, \ldots, N\}$ halmaz bijekciói (vagyis permutációi), ahol az N egy tetszőleges nagy egész szám. Ennek érdekében a betűket és egyéb jeleket (egy mindenki által ismert módon) számokként kódoljuk, majd az üzenetből ily módon gyártott számsorozatot adott méretű blokkokra vágjuk szét, és az egyes blokkokat (természetes módon) egy-egy (nagy) számnak tekintjük. Az így keletkező számok alkotják majd a T és M függvények értelmezési tartományát és értékkészletét.

A betűknek és jeleknek például az alábbi módon feleltethetünk meg kétjegyű (tízes számrendszerbeli) számokat: A$\mapsto$01, Á$\mapsto$02, B$\mapsto$03, …, Z$\mapsto$35, „pont"$\mapsto$36 stb., és (mondjuk) négy ilyen kétjegyű szám alkosson egy blokkot. Ezzel az üzenetet nyolcjegyű, azaz 1 és $10^8 - 1$ közé eső számokká alakítottuk, vagyis ekkor N vehető $10^8 - 1$-nek.

Nézzük meg, mit kapunk ily módon a „számelmélet" szóból. Az S-nek megfelel a 25, a Z-nek a 35, az Á-nak a 02 stb., vagyis ekkor a

$$25350216|06151607|150626$$

számsorozat keletkezik. Ez a 25350216, 06151607, 15062600 blokkokat jelenti (az utolsó csonka blokkot nullákkal egészítettük ki). Így a titkosírás T (illetve M) kulcsát rendre erre a három számra kell alkalmazni. (Még egyszer hangsúlyozzuk, hogy a szövegnek ez a számokká konvertálási módja mindenki számára ismert, és csak arra szolgál, hogy a titkosírásban szereplő T és M függvényeket egységesebben és kényelmesebben lehessen majd megadni.)

Most rátérünk az RSA-séma szerinti T, M kulcspár konstrukciójára.

Legyen $N = pq$, ahol p és q két nagy prímszám, amelyeket a kulcstulajdonos titokban tart, ugyanakkor N-et teljes nyugalommal nyilvánosságra hozza. Választ továbbá egy olyan $t > 1$ egészt, amelyre $(t\,,\,\varphi(N)) = 1$, és nyilvánosságra hozza, hogy az ő T kulcsa a következő:

$$T(r) = r^t \text{ legkisebb pozitív maradéka } (\mathrm{mod}\ N)\,, \qquad r = 1, 2, \ldots, N\,. \quad (1)$$

Hogyan lehet $M = T^{-1}$-et megkapni? Keressük M-et hasonló alakban:

$$M(s) = s^m \text{ legkisebb pozitív maradéka } (\mathrm{mod}\ N)\,, \qquad s = 1, 2, \ldots, N\,. \quad (2)$$

Ez akkor lesz megfelelő, ha minden r-re

$$r = TM(r) = MT(r) = r^{tm} \text{ legkisebb pozitív maradéka } (\mathrm{mod}\ N)\,,$$

azaz, ha minden r-re

$$r^{tm} \equiv r \pmod{N}\,. \quad (3)$$

A p és q prímekre a kis Fermat-tételt felhasználva könnyen következik, hogy tetszőleges k-val

$$r^{1+k\varphi(N)} \equiv r \pmod{N} \quad (4)$$

minden r-re teljesül (lásd az 5.8.3a feladatot).

A (4) alapján (3)-ban (és így (2)-ben is) megfelelő m-hez jutunk, ha megoldjuk az

$$mt = 1 + k\varphi(N) \quad (5)$$

lineáris diofantikus egyenletet m-re (és k-ra). Mivel $(t\,,\,\varphi(N)) = 1$, ezért van megoldás, és az euklideszi algoritmus segítségével gyorsan megkapható.

Mindezt azonban csak a kulcstulajdonos tudja megcsinálni, mert más nem ismeri $\varphi(N)$ értékét, hiszen ahhoz tudnia kellene, mik az N prímtényezői.

A kulcstulajdonos az eljárás alapját képező p és q prímeket a következőképpen generálja. Sorra választ (mondjuk) 250, illetve 300-jegyű páratlan véletlen számokat, és (például az 5.7 pontban tárgyalt prímtesztek valamelyikével) ellenőrzi, hogy prímek-e. Ezt addig csinálja, amíg egy-egy prímet nem talál. Mivel egyrészt a prímteszt gyors, másrészt „elég sok” 250, illetve 300-jegyű prím van (a prímszámtétel szerint körülbelül minden $\log(10^{300})/2 \approx 345$-ödik 300-jegyű páratlan szám prím), ezért p és q hamar kiválasztható.

Végül, (1) és (2) alapján mind a $T(r)$, mind pedig az $M(s)$ függvényértékek az ismételt négyzetre emelések módszerével gyorsan kiszámolhatók (persze ez utóbbiakat csak a kulcstulajdonos tudja meghatározni).

A p, q és t kiválasztásánál néhány biztonsági szabályt is figyelembe kell venni. Ha például p és q túl közel lenne egymáshoz, akkor könnyebb lenne az N-et faktorizálni, ezért kellett a p és q választásánál különböző nagyságú véletlen számokat tesztelni. Hasonló okokból szükséges az is, hogy $p-1$-nek és $q-1$-nek legyenek nagy prímtényezői stb. Ezekkel a technikai részletekkel nem foglalkozunk.

Mennyire biztonságos ez az eljárás? Úgy tűnik, hogy (az óvatossági rendszabályok maximális betartása esetén) nincs okunk aggodalomra. Nincs azonban kizárva, hogy valaki talál egy olyan módszert, amellyel gyorsan tud nagy számokat is prímtényezőkre bontani, és akkor hozzáfér az M kulcshoz. Az is elképzelhető, hogy valamilyen egészen másféle formában képes előállítani az M függvényt. Mindez azonban jelenleg meglehetősen valószínűtlen. Ahogy azonban az 5.7 pont elején is jeleztük, a helyzet alapvetően megváltozhat, ha a kvantumszámítógépek hatékonyan fognak tudni működni.

Az RSA-séma lényegét az alábbi tételben foglaljuk össze:

5.8.1 Tétel (RSA-séma) **T 5.8.1**

Legyen p, q két nagy prím, $N = pq$ és $(t, \varphi(N)) = 1$. Definiáljuk a T, M kulcspárt (1), illetve (2) alapján, ahol m-re teljesül (5). Nyilvános: N, t és T, titkos: p, q, $\varphi(N)$, m és M. Ekkor $M = T^{-1}$, és M a T ismeretében sem határozható meg.

A p és q prímeket a kulcstulajdonos véletlen számok prímtesztelésével nyeri, ezek segítségével m-et gyorsan meg tudja határozni. Az $M(s)$ függvényértékeket a kulcstulajdonos, a $T(r)$ függvényértékeket pedig bárki gyorsan ki tudja számítani. ♣

Feladatok

5.8.1 Milyen problémát jelenthet, ha a Diffie–Hellman-sémában az A az u üzenet helyett nem a $v = T_B(M_A(u))$, hanem csak a $v' = T_B(u))$ értéket küldi el B-nek?

5.8.2 Bizonyítsuk be, hogy az (1) által definiált T függvénynek akkor és csak akkor létezik inverze, ha $(t\,,\,\varphi(N)) = 1$.

5.8.3 Legyen $N = pq$, ahol p és q különböző prímek.
a) Bizonyítsuk be, hogy $r^{1+k\varphi(N)} \equiv r \pmod{N}$ minden r-re teljesül.
b) Adjuk meg az összes olyan $v > 0$ egészt, amellyel $r^v \equiv r \pmod{N}$ minden r-re teljesül.

5.8.4 Tegyük fel, hogy az RSA-sémához (a prímtesztelés tökéletlensége folytán) olyan p számot használunk fel, amely nem prím, hanem uni-

verzális álprím (és ezt persze nem is tudjuk). Gondot okoz-e ez az RSA-sémában?

*5.8.5 Mutassuk meg, hogy az RSA-séma nem biztonságos, ha olyan t kitevőt választunk, amelynek a modulo $\varphi(N)$ vett rendje kicsi.

5.8.6 Legyen p nagy prím és g egy primitív gyök modulo p. Jelenlegi tudásunk szerint a g alapú diszkrét logaritmus, vagyis $\operatorname{ind}_g a$ meghatározása reménytelen feladat, erre nem ismerünk gyors algoritmust. Ez azt jelenti, hogy bármely k-ra a g^k mod p vett a maradékát gyorsan ki tudjuk számítani, azonban a-ból k értékét más nem tudja előállítani.

A és B választ egy-egy ilyen k_A, illetve k_B kitevőt, amelyet titokban tartanak, azonban g^{k_A}, illetve g^{k_B} modulo p maradékát nyilvánosságra hozzák. Mutassuk meg, hogy ekkor a $g^{k_A k_B}$ szám modulo p maradékát mind A, mind pedig B ki tudja számítani, rajtuk kívül más azonban (remélhetőleg) nem. (Ez azt jelenti, hogy ily módon A és B külön egyeztetés nélkül meg tudnak állapodni egy közös jelszóban vagy számkulcsban, anélkül hogy a titkos k_A, illetve k_B értéküket egymás tudomására kellene hozniuk).

5.8.7 Hosszú ideig úgy tűnt, hogy az alább ismertetett séma, az ún. moduláris hátizsák- vagy részösszegprobléma is felhasználható nyilvános jelkulcsú titkosírásra, később azonban kiderült, hogy ez nem biztonságos.

a) A pozitív egészekből álló $C = \{c_0, c_1, \ldots, c_{k-1}\}$ sorozatot nevezzük (házi használatra) *összeginjektív*nek, ha a különböző c_i-kből képzett akárhány tagú összegek mind különbözők.

Bizonyítsuk be, hogy ha a C sorozat „szupernövekedő”, azaz

$$c_i > \sum_{j=0}^{i-1} c_j\,, \qquad i = 1, 2, \ldots, k-1\,, \tag{6}$$

akkor C összeginjektív.

b) Legyen C összeginjektív, $m > \sum_{i=0}^{k-1} c_i$ és $(r, m) = 1$, továbbá

$$d_i = rc_i \text{ legkisebb pozitív maradéka (mod } m), \;\; i = 0, 1, \ldots, k-1. \tag{7}$$

Mutassuk meg, hogy ekkor a $d_0, \ldots, d_{k-1}$ sorozat is összeginjektív.

c) Legyen $0 \le u < 2^k$, és írjuk fel az u számot kettes számrendszerben:

$$u = \sum_{i=0}^{k-1} \delta_i 2^i\,, \qquad \text{ahol} \qquad \delta_i = 0 \text{ vagy } 1,\ \ i = 0, 1, \ldots, k-1\,.$$

Bizonyítsuk be, hogy ha H összeginjektív, akkor a

$$v = \sum_{i=0}^{k-1} \delta_i h_i$$

szám ismeretében u *elvileg* meghatározható.

d) Mutassuk meg, hogy a (6) és a belőle gyártott (7) típusú sorozatokra az u a v-ből *gyakorlatilag* is gyorsan meghatározható.

Mindezek alapján vegyünk egy (6) típusú C sorozatot, és készítsünk ebből egy (7) típusú D sorozatot. Magát a D-t hozzuk nyilvánosságra, azonban a c_i, m és r értékeket tartsuk titokban. Ekkor *bárki* gyorsan ki tudja számítani az u-ból a v-t, és *mi* ezt C, m és r ismeretében visszafelé is meg tudjuk csinálni. Mivel egy általános összeginjektív sorozat esetén a v-ből az u *konkrét* előállítása igen nehéz, ezért úgy tűnt, hogy a (7) típusú sorozatoknál is ez a helyzet, ha valaki nem ismeri a c_i, m és r értékeket. Mint említettük, ez a vélekedés tévesnek bizonyult.

6. SZÁMELMÉLETI FÜGGVÉNYEK

Számelméleti függvényen a pozitív egészeken értelmezett komplex értékű függvényt értünk. Ezek közül elsősorban azok lesznek érdekesek számunkra, amelyek a pozitív egészek valamilyen aritmetikai tulajdonságával kapcsolatosak. Ilyen például az n pozitív osztóinak számát jelölő $d(n)$ és a kongruenciáknál nélkülözhetetlen Euler-féle $\varphi(n)$, amelyekkel már az 1., illetve 2. fejezetben találkoztunk. További fontos példák az n pozitív osztóinak összegét jelentő $\sigma(n)$, amely a tökéletes számokhoz is kapcsolódik, valamint a $\mu(n)$ Möbius-függvény, amely az összegzési és megfordítási függvénynél játszik alapvető szerepet. A $d(n)$ példáján keresztül bemutatjuk azt a sok számelméleti függvényre jellemző kétarcúságot, amely egyfelől a függvényértékek szeszélyes ingadozását, másfelől az „átlagos" értelemben vett szabályos viselkedést jelenti. Az átlagértékek vizsgálatát a konvolúció felhasználásával kiterjesztjük a $\sigma(n)$-re és a $\varphi(n)$-re is. Ez utóbbi eredmény egyúttal megadja, mi a (pontosan definiálható értelemben vett) valószínűsége annak, hogy két szám relatív prím. (Ez a valószínűség meglepően nagynak bizonyul: $6/\pi^2 \approx 0{,}61$.) Különösen érdekes az n különböző (pozitív) prímosztóinak számát jelentő $\omega(n)$ függvény vizsgálata, amelyről kiderül, hogy (ellentétben például a $d(n)$-nel) legtöbbször az átlagértékéhez közeli függvényértékeket vesz fel. Hardy és Ramanujan ezen híres tételére Turán Pál adott egyszerű bizonyítást, amely később a valószínűségi számelmélet kiindulópontjává vált. Végül abból az Erdős által elindított témakörből adunk ízelítőt, amely azt vizsgálja, milyen feltételekkel karakterizálható az additív függvények közül a logaritmusfüggvény.

6.1. Multiplikativitás, additivitás

6.1.1 Definíció **D 6.1.1**

*Számelméleti függvény*eknek a pozitív egészeken értelmezett komplex értékű függvényeket nevezzük. ♣

Példák:

$d(n)$ az n pozitív osztóinak a száma (lásd az 1.6.3 Tételt);

az Euler-féle φ-függvény (lásd a 2.2.7 Definíciót és a 2.3.1 Tételt);

$f(n) = (-1)^n$, $g(n) = \sqrt{n^2+5} + i \sin n$ stb.

Néhány fontos számelméleti függvényt a 6.2 pontban fogunk ismertetni.

A számelméleti függvények vizsgálatánál gyakran lényeges szerepet játszanak az alábbi tulajdonságok:

6.1.2 Definíció **D 6.1.2**

Az f számelméleti függvény *multiplikatív*, ha bármely $(a, b) = 1$ esetén $f(ab) = f(a)f(b)$ teljesül. ♣

6.1.3 Definíció **D 6.1.3**

Az f számelméleti függvény *teljesen multiplikatív* (vagy *totálisan multiplikatív*), ha minden a, b esetén $f(ab) = f(a)f(b)$ teljesül. ♣

Példák:

Az Euler-féle φ-függvény multiplikatív (ezt a 2.3.1 Tétel első bizonyításában igazoltuk), de nem teljesen multiplikatív, mert például $\varphi(8) \neq \varphi(2)\varphi(4)$. Hasonló a helyzet a $d(n)$-nel (lásd a 6.1.1 feladatot).

Az $f(n) = n^\alpha$ függvény, ahol α rögzített valós szám, teljesen multiplikatív (és így multiplikatív is).

A $g(n) = 3n - 2$ függvény nem multiplikatív, mert például $(2, 3) = 1$, de $g(6) \neq g(2)g(3)$.

Ha a függvényértékek szorzata helyett az összegükre követelünk meg a fentiekhez hasonló feltételeket, akkor az additív, illetve teljesen additív függvény fogalmához jutunk:

6.1.4 Definíció **D 6.1.4**

Az f számelméleti függvény *additív*, ha bármely $(a, b) = 1$ esetén $f(ab) = f(a) + f(b)$ teljesül. ♣

6.1.5 Definíció **D 6.1.5**

Az f számelméleti függvény *teljesen additív* (vagy *totálisan additív*), ha minden a, b esetén $f(ab) = f(a) + f(b)$ teljesül. ♣

Külön is felhívjuk a figyelmet arra, hogy a feltétel az additív, illetve teljesen additív függvény definíciójában is az $f(ab)$ (és nem az $f(a+b)$) függvényértékre vonatkozik.

Példák:

A (bármilyen alapú) logaritmusfüggvény teljesen additív.

$f(n) = 1 + (-1)^n$ additív, de nem teljesen additív.

$g(n) = 1 + \log_2 n$ nem additív (és így nem lehet teljesen additív sem).

Az $f = 0$ (azaz az azonosan nulla) függvény mind teljesen multiplikatív, mind pedig teljesen additív, de más függvény nem lehet egyszerre multiplikatív és additív (ez leolvasható például a 6.1.6 Tételből).

Először megmutatjuk, hogy egy additív, illetve egy $\neq 0$ multiplikatív függvény az 1 helyen csak speciális értéket vehet fel:

6.1.6 Tétel **T 6.1.6**

Ha f multiplikatív és $f \neq 0$, akkor $f(1) = 1$.

Ha g additív, akkor $g(1) = 0$. ♣

Bizonyítás: Legyen a olyan pozitív egész, amelyre $f(a) \neq 0$. Ekkor $(a, 1) = 1$ miatt $f(a) = f(a \cdot 1) = f(a)f(1)$, ahonnan $f(a) \neq 0$-val történő egyszerűsítés után $1 = f(1)$ adódik.

A másik állítás is hasonlóan bizonyítható. ■

A 6.1.6 Tétel tehát az additivitásnak, illetve multiplikativitásnak egy szükséges (de nem elégséges) feltételét adja.

Az additivitás, illetve multiplikativitás definíciójából azonnal következik, hogy egy additív, illetve ($\neq 0$) multiplikatív függvényt a prímhatvány helyeken felvett értékei már egyértelműen meghatároznak:

6.1.7 Tétel **T 6.1.7**

Legyen f multiplikatív, g additív és $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ az $n > 1$ szám kanonikus alakja . Ekkor

$$f(n) = f(p_1^{\alpha_1}) \dots f(p_r^{\alpha_r}) \qquad \text{és} \qquad g(n) = g(p_1^{\alpha_1}) + \dots + g(p_r^{\alpha_r})\,. \ \clubsuit$$

Ezt a tényt használtuk fel a $\varphi(n)$ képletének levezetésekor is (a 2.3.1 Tétel első bizonyításában).

A teljesen additív, illetve ($\neq 0$) teljesen multiplikatív esetben a függvényt már a prím helyeken felvett értékei is egyértelműen meghatározzák:

6.1.8 Tétel **T 6.1.8**

Legyen f teljesen multiplikatív, g teljesen additív és $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ az $n > 1$ szám kanonikus alakja. Ekkor

$$f(n) = f(p_1)^{\alpha_1} \dots f(p_r)^{\alpha_r} \qquad \text{és} \qquad g(n) = \alpha_1 g(p_1) + \dots + \alpha_r g(p_r)\,. \ \clubsuit$$

A 6.1.7 Tételt kiegészíthetjük azzal, hogy a prímhatvány helyeken felvett értékekre a multiplikativitás, illetve additivitás már semmilyen megszorítást sem jelent, ezek „szabadon megválaszthatók”. Ezen pontosan a következőt kell érteni: akárhogyan írjuk elő a prímhatvány helyeken felveendő értékeket, biztosan létezik olyan multiplikatív, illetve additív függvény, amely ezeken a helyeken az előírt értékeket veszi fel. A teljesen multiplikatív, illetve teljesen additív esetben hasonló értelmű állítás érvényes a prímhatványok helyett a prímekre. (Minderre vonatkozólag lásd a 6.1.4 feladatot.)

Feladatok

6.1.1 Mutassuk meg, hogy a $d(n)$ függvény multiplikatív, de nem teljesen multiplikatív.

6.1.2 Az alábbi függvények közül melyek multiplikatívak, illetve teljesen multiplikatívak, és melyek additívak, illetve teljesen additívak?

a) $f(n) = \begin{cases} 0, & \text{ha } 6 \mid n; \\ 1, & \text{ha } 6 \nmid n. \end{cases}$ b) $g(n) = \begin{cases} 0, & \text{ha } 3 \mid n; \\ 1, & \text{ha } 3 \nmid n. \end{cases}$

c) $h(n) = \begin{cases} 0, & \text{ha } 3 \mid n; \\ 2, & \text{ha } 3 \nmid n. \end{cases}$ d) $k(n) = \begin{cases} 2, & \text{ha } 3 \mid n; \\ 0, & \text{ha } 3 \nmid n. \end{cases}$

6.1.3 Van-e olyan h additív, illetve multiplikatív függvény, amelyre $h(6) = 0$, $h(10) = 1$ és $h(15) = 3$?

6.1.4 Legyen $p_1, p_2, \ldots = 2, 3, 5, 7, \ldots$ a prímszámok, $q_1, q_2, \ldots = 2, 3, 4, 5, 7, 8, 9, 11, \ldots$ pedig a prímhatványok sorozata, és legyenek $c_1, c_2, \ldots$ tetszőleges komplex számok.

a) Bizonyítsuk be, hogy pontosan egy olyan $f \neq 0$ multiplikatív, illetve g additív függvény létezik, amelyre

$$f(q_i) = g(q_i) = c_i, \qquad i = 1, 2, \ldots$$

b) Bizonyítsuk be, hogy pontosan egy olyan $s \neq 0$ teljesen multiplikatív, illetve t teljesen additív függvény létezik, amelyre

$$s(p_i) = t(p_i) = c_i, \qquad i = 1, 2, \ldots$$

6.1.5 Ha g csak pozitív egész értékeket vesz fel, akkor tetszőleges f-re definiálhatjuk a $h(n) = (f \circ g)(n) = f(g(n))$ összetett függvényt. Melyek igazak az alábbi állítások közül?

a) Ha f és g teljesen multiplikatív, akkor h is teljesen multiplikatív.

b) Ha f és g teljesen additív, akkor h is teljesen additív.

c) Ha f multiplikatív és g teljesen multiplikatív, akkor h is multiplikatív.

d) Ha f teljesen multiplikatív és g multiplikatív, akkor h is multiplikatív.

6.1.6

a) Legyen f teljesen additív. Melyek azok a k pozitív egészek, amelyekre a $g(n) = f(kn)$ függvény is teljesen additív?

b) Oldjuk meg a feladatot arra az esetre is, ha a teljes additivitás helyett (mind f-re, mind pedig g-re) csak additivitást követelünk meg.

c) Vizsgáljuk meg a kérdés teljesen multiplikatív, illetve multiplikatív változatát is.

M 6.1.7

a) Bizonyítsuk be, hogy ha f teljesen additív, akkor

$$\text{minden } a,b\text{-re } \ f(a)+f(b)=f((a,b))+f([a,b]). \qquad (\nabla)$$

b) Mutassuk meg, hogy (∇) akkor is érvényes, ha f-ről csak additivitást teszünk fel.

*c) Adjuk meg az összes olyan f-et, amelyre (∇) fennáll.

*d) Vizsgáljuk meg a problémakörnek az $f(a)f(b) = f((a,b))f([a,b])$ egyenlőségre vonatkozó megfelelőjét is.

6.1.8 Legyen f valós értékű és $g(n) = 2^{f(n)}$. Mutassuk meg, hogy g akkor és csak akkor multiplikatív, ha f additív.

Megjegyzés: Ennek alapján a valós értékű additív függvények és a pozitív értékű multiplikatív függvények vizsgálata kölcsönösen visszavezethető egymásra.

6.1.9

a) Bizonyítsuk be, hogy két additív, illetve két teljesen additív függvény összege és különbsége is additív, illetve teljesen additív.

b) Bizonyítsuk be, hogy két teljesen additív függvény szorzata sohasem teljesen additív, kivéve azt a triviális esetet, amikor a két függvény közül legalább az egyik a 0 függvény.

c) Mutassunk olyan példát, amikor két $\neq 0$ additív függvény szorzata is additív, és olyat is, amikor a szorzatuk nem additív.

M *d) Adjuk meg az összes olyan additív függvénypárt, amelyek szorzata is additív.

e) Mutassuk meg, hogy két multiplikatív, illetve két teljesen multiplikatív függvény szorzata is multiplikatív, illetve teljesen multiplikatív.

f) Bizonyítsuk be, hogy két különböző $\neq 0$ multiplikatív függvény összege, illetve különbsége sohasem multiplikatív.

6.1.10

a) Bizonyítsuk be, hogy két additív, illetve két teljesen additív függvény számtani közepe is additív, illetve teljesen additív.

b) Bizonyítsuk be, hogy ha két teljesen multiplikatív függvény számtani közepe is teljesen multiplikatív, akkor a két függvény egyenlő. Mi a helyzet, ha (mindhárom függvényre) a teljes multiplikativitás helyett csak multiplikativitást követelünk meg?

6.1.11 Tegyük fel, hogy f multiplikatív, g additív és $f+g$ konstans. Mutassuk meg, hogy ekkor $f^{1000}+g^{1000}$ multiplikatív és $f^{1000}g^{1000}$ additív.

*6.1.12

a) Tegyük fel, hogy a h additív függvény előáll két multiplikatív függvény különbségeként. Bizonyítsuk be, hogy ha a, b és c páronként relatív prímek, akkor $h(a)h(b)h(c) = 0$.

b) Tegyük fel, hogy a h additív függvény a triviális $1 \cdot h = h$ előállításon kívül másképp is felírható egy multiplikatív és egy additív függvény szorzataként. Bizonyítsuk be, hogy ha a, b és c páronként relatív prímek, akkor $h(a)h(b)h(c) = 0$.

6.1.13

M a) Tegyük fel, hogy egy additív függvény értékkészlete csak véges sok számból áll. Igazoljuk, hogy akkor ezen értékek mindegyikét a függvénynek végtelen sok helyen kell felvennie.

b) Mutassunk példát arra, hogy az a) rész állítása multiplikatív függvényekre általában nem igaz.

c) Tegyük fel, hogy egy f multiplikatív függvény értékkészlete csak véges sok számból áll, és van olyan érték, amelyet a függvény csak véges sokszor vesz fel. Bizonyítsuk be, hogy ekkor létezik olyan K, hogy ha n-nek van K-nál nagyobb prímosztója, akkor $f(n) = 0$.

6.1.14 Melyek igazak az alábbi állítások közül?

a) Ha f additív, és van olyan a, b számpár, amelyre $(a, b) \neq 1$ és $f(ab) = f(a) + f(b)$, akkor f teljesen additív.

b) Ha f additív, és van olyan a, b számpár, amelyre $(a,b) \neq 1$ és $f(ab) = f(a) + f(b)$, akkor végtelen sok ilyen számpár is létezik.

c) Ha f additív, de nem teljesen additív, akkor $(a,b) \neq 1$-ből következik, hogy $f(ab) \neq f(a) + f(b)$.

d) Ha f additív, de nem teljesen additív, akkor végtelen sok olyan a, b számpár létezik, amelyre $f(ab) \neq f(a) + f(b)$.

e) Ha f multiplikatív, de nem teljesen multiplikatív, akkor végtelen sok olyan a, b számpár létezik, amelyre $f(ab) \neq f(a)f(b)$.

M*6.1.15 Jelölje $\varphi_2(n)$ az $1, 2, \ldots, n$ számok közül azoknak az i-knek a számát, amelyekre $(i,n) = (i+1,n) = 1$. Adjunk képletet $\varphi_2(n)$-re az n kanonikus alakjának alapján.

*6.1.16 Bizonyítsuk be:

$$\sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} (k-1,n) = \varphi(n)d(n)\,.$$

6.2. Nevezetes függvények

Ebben a pontban néhány fontos számelméleti függvényt vezetünk be, ezek a $\sigma(n), \mu(n), \omega(n), \Omega(n)$ és $d_k(n)$.

D 6.2.1

6.2.1 Definíció

$\sigma(n)$ az n pozitív osztóinak az összege. ♣

Példa: $\sigma(1) = 1$, $\sigma(10) = 18$; $\sigma(n) = n+1 \iff n$ prím.

Osztón a fejezet további részében mindig pozitív osztót fogunk érteni.

T 6.2.2

6.2.2 Tétel

Ha az n kanonikus alakja $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, akkor

$$\sigma(n) = \prod_{i=1}^{r} (1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}\,. \ \clubsuit$$

Bizonyítás: Ugyanazt a gondolatmenetet követjük, amelyet a $d(n)$ képletének levezetésénél használtunk (1.6.3 Tétel).

Az 1.6.2 Tétel szerint az n összes (pozitív) osztóját úgy kapjuk meg, ha a

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} \tag{1}$$

kifejezésben a $\beta_1, \beta_2, \dots, \beta_r$ kitevők egymástól függetlenül végigfutnak a

$$\beta_1 = 0, 1, \dots, \alpha_1, \quad \beta_2 = 0, 1, \dots, \alpha_2, \quad \dots, \quad \beta_r = 0, 1, \dots, \alpha_r$$

értékeken, továbbá az n minden osztója csak egyféleképpen áll elő a fenti alakban. Ennek megfelelően a $\sigma(n)$ az összes ilyen d összege.

Másrészt nyilván ugyanezt az összeget kapjuk, ha a

$$\prod_{i=1}^{r} (1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}) \tag{2}$$

szorzást elvégezzük; az (1) szorzat akkor keletkezik, amikor (2) első tényezőjéből a $p_1^{\beta_1}$ tagot, a második tényezőből a $p_2^{\beta_2}$ tagot stb. szorozzuk össze.

Ezzel beláttuk a tétel állításában szereplő első egyenlőséget.

A második egyenlőség a véges mértani sorozatok jól ismert összegképletéből adódik. ■

A 6.2.2 Tétel egy másik lehetséges bizonyítására nézve lásd a 6.2.1 feladatot.

6.2.3 Definíció **D 6.2.3**

A $\mu(n)$ *Möbius-függvény*t a következő módon értelmezzük:

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1; \\ (-1)^r, & \text{ha } n = p_1 \dots p_r, \text{ ahol a } p_j\text{-k különböző prímek;} \\ 0, & \text{ha van olyan } p \text{ prím, amelyre } p^2 \mid n. \ \clubsuit \end{cases}$$

Példa: $\mu(10) = 1$, $\mu(20) = 0$, $\mu(30) = -1$.

A μ-függvény későbbi fontos szerepe elsősorban az alábbi egyszerű tulajdonságán múlik:

6.2.4 Tétel **T 6.2.4**

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1. \ \clubsuit \end{cases}$$

Bizonyítás: Ha $n = 1$, akkor $\sum_{d|1} \mu(d) = \mu(1) = 1$.

Ha $n > 1$, akkor legyen az n kanonikus alakja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Mivel a nem négyzetmentes számokra a μ-függvény értéke 0, ezért elég az összegzést az n négyzetmentes osztóira elvégezni. Ennélfogva

$$\begin{aligned}\sum_{d|n} \mu(d) =& \mu(1) + \mu(p_1) + \ldots + \mu(p_r) + \\ &+ \mu(p_1p_2) + \mu(p_1p_3) + \ldots + \mu(p_{r-1}p_r) + \ldots + \mu(p_1p_2\dots p_r) = \\ =& 1 - r + \binom{r}{2} - \binom{r}{3} + \ldots + (-1)^r \binom{r}{r} = (1-1)^r = 0. \ \blacksquare\end{aligned}$$

6.2.5 Definíció **D 6.2.5**

$\omega(n)$ az n különböző (pozitív) prímosztóinak a száma.

$\Omega(n)$ az n „összes" (pozitív) prímosztóinak a száma, tehát amikor a prímeket a kanonikus alakban szereplő kitevő szerinti multiplicitással számoljuk.

Képlettel: $\omega(1) = \Omega(1) = 0$, és ha az n kanonikus alakja

$$n = p_1^{\alpha_1} \dots p_r^{\alpha_r} \qquad \text{(ahol minden } \alpha_i > 0\text{)},$$

akkor

$$\omega(n) = r \qquad \text{és} \qquad \Omega(n) = \alpha_1 + \ldots + \alpha_r \,. \ \clubsuit$$

Példa: $\omega(500) = 2$, $\Omega(500) = 5$; $\omega(n) = \Omega(n) \iff n$ négyzetmentes.

6.2.6 Definíció **D 6.2.6**

Legyen k rögzített pozitív egész. Ekkor $d_k(n)$ az $n = x_1x_2 \dots x_k$ egyenlet pozitív egész megoldásainak a számát jelenti, ahol két megoldást akkor is különbözőnek tekintünk, ha csak a tényezők sorrendjében térnek el egymástól. $\clubsuit$

Nyilván $d_1(n) = 1$, $d_k(1) = 1$, továbbá $d_2(n) = d(n)$ (a $d_k(n)$ függvény tehát a $d(n)$ általánosításának tekinthető).

6.2.7 Tétel **T 6.2.7**

Ha az n kanonikus alakja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, akkor

$$d_k(n) = \prod_{i=1}^{r} \binom{\alpha_i + k - 1}{k - 1} \,. \ \clubsuit$$

Bizonyítás: Az x_i számok prímosztói is a $p_1, \ldots, p_r$ prímek közül kerülnek ki, ezért az x_i számok kanonikus alakja

$$x_1 = p_1^{\beta_{11}} \ldots p_r^{\beta_{r1}}, \quad \ldots, \quad x_k = p_1^{\beta_{1k}} \ldots p_r^{\beta_{rk}},$$

ahol

$$0 \le \beta_{ij} \le \alpha_i, \qquad i = 1, 2, \ldots, r, \qquad j = 1, 2, \ldots k\,.$$

(A kitevőkben az első index a prím, a második index pedig az ismeretlen sorszámát jelenti.)

Ekkor az $n = x_1 x_2 \ldots x_k$ egyenlet pontosan akkor teljesül, ha

$$\alpha_1 = \beta_{11} + \beta_{12} + \ldots + \beta_{1k}, \quad \ldots, \quad \alpha_r = \beta_{r1} + \beta_{r2} + \ldots + \beta_{rk}\,. \tag{3}$$

A (3) egyenletrendszer r darab

$$\alpha = y_1 + y_2 + \ldots + y_k, \qquad y_i \ge 0 \text{ egész} \tag{4}$$

típusú egyenletet tartalmaz.

Vizsgáljuk meg, hogy egy ilyen egyenletnek hány megoldása van.

Más megfogalmazásban (4) megoldásszáma azt jelenti, hányféleképpen lehet az α számot k darab nemnegatív egész összegeként előállítani, ha az összeadandók sorrendje is számít, vagyis ha két előállítást akkor is különbözőnek tekintünk, ha csak az összeadandók sorrendjében térnek el egymástól.

Vegyünk egy α hosszúságú szakaszt, és mérjük fel rá sorban az $y_1, \ldots, y_k$ hosszúságú szakaszokat (beleértve a 0 hosszúságúakat is). Ezt úgy is interpretálhatjuk, hogy leírunk y_1 darab 1-est, majd egy $*$ jellel jelezzük, hogy ennek a szakasznak vége, ezután leírunk y_2 darab 1-est, amelyet ismét egy $*$ elválasztójel követ stb., végül y_k darab 1-es zárja a sort.

Például, ha $\alpha = 7$ és $k = 4$, akkor a $7 = 4 + 0 + 1 + 2$ előállításnak az $1111 * *1 * 11$ jelsorozat felel meg. Megfordítva a $*1111 * 111*$ jelsorozat a $7 = 0 + 4 + 3 + 0$ előállításból származott.

Ennek megfelelően a (4) egyenlet megoldásszáma megegyezik az ilyen jelsorozatok számával. Egy jelsorozat α darab 1-est és $k - 1$ darab $*$ elválasztójelet tartalmaz, tetszőleges sorrendben. Ennélfogva az ilyen jelsorozatok száma

$$\binom{\alpha + k - 1}{k - 1}. \tag{5}$$

Az (5) képlet alapján a (3)-ban szereplő egyenletek megoldásszáma rendre

$$\binom{\alpha_1 + k - 1}{k - 1}, \ \binom{\alpha_2 + k - 1}{k - 1}, \ \ldots, \ \binom{\alpha_r + k - 1}{k - 1}. \tag{6}$$

Mivel az egyes egyenletek egymástól teljesen függetlenek, ezért a (3) rendszer megoldásszámát az egyes egyenletek megoldásszámainak, azaz a (6)-ban felsorolt számoknak a szorzata adja. ■

Megjegyezzük, hogy a $\sigma(n)$, $\Omega(n)$, $d_k(n)$ (és így speciálisan $d(n)$) függvényekre adott képlet akkor is igaz marad, ha megengedjük, hogy az n kanonikus alakjában az α_i kitevők között a nulla is előforduljon, azonban $\varphi(n)$ és $\omega(n)$ képlete csak úgy érvényes, ha a kanonikus alakban minden kitevő valóban pozitív.

Végül megvizsgáljuk a megismert függvényeket multiplikativitás, illetve additivitás szempontjából.

6.2.8 Tétel **T 6.2.8**

$\varphi(n)$, $\sigma(n)$, $\mu(n)$ és $d_k(n)$ multiplikatív, de nem teljesen multiplikatív (a $d_1(n) = 1$ triviális esettől eltekintve).

$\omega(n)$ additív, de nem teljesen additív.

$\Omega(n)$ teljesen additív. ♣

Bizonyítás: $\varphi(n)$ multiplikativitása szerepelt a 2.3.1 Tétel első bizonyításában (valamint a 2.2.14 és 2.6.10 feladatokban is). Továbbá például

$$6 = \varphi(9) \neq \varphi(3)\varphi(3) = 4,$$

tehát $\varphi(n)$ nem teljesen multiplikatív. (Sőt, $(a, b) \neq 1$ esetén $\varphi(ab) = \varphi(a)\varphi(b)$ *sohasem* teljesül, lásd a 2.3.10a feladatot.)

A $\sigma(n)$ multiplikativitásához a 6.2.2 Tételben bizonyított képletet használjuk fel (egy másik bizonyítást kaphatunk az 1.6.5a-b feladat alapján, lásd a 6.2.1 feladatot).

Ha $a = 1$ vagy $b = 1$, akkor $\sigma(ab) = \sigma(a)\sigma(b)$ nyilván teljesül.

Ha $(a, b) = 1$ és a kanonikus alakjuk

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r}\,, \qquad b = q_1^{\beta_1} \dots q_s^{\beta_s}\,,$$

ahol a relatív prímség miatt $p_i \neq q_j$, akkor ab kanonikus alakja

$$ab = p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}\,,$$

és így a σ képletét a-ra, b-re és ab-re alkalmazva kapjuk, hogy

$$\sigma(a)\sigma(b) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1}-1}{p_r-1} \cdot \frac{q_1^{\beta_1+1}-1}{q_1-1} \cdot \ldots \cdot \frac{q_s^{\beta_s+1}-1}{q_s-1} = \sigma(ab)\,.$$

Továbbá például

$$36 = \sigma(2)\sigma(6) \neq \sigma(12) = 28,$$

tehát $\sigma(n)$ nem teljesen multiplikatív. (Sőt, $(a,b) \neq 1$ esetén $\sigma(ab) = \sigma(a)\sigma(b)$ *sohasem* teljesül, lásd a 6.2.2 feladatot.)

A $\mu(n)$ multiplikativitását a függvény 6.2.3 Definíciója alapján igazoljuk. Ha $a = 1$ vagy $b = 1$, akkor $\mu(ab) = \mu(a)\mu(b)$ nyilván teljesül. Ha a és b közül legalább az egyik nem négyzetmentes, akkor a szorzatuk sem az, és így $\mu(ab) = \mu(a)\mu(b) = 0$. Végül, ha mindketten négyzetmentesek és $(a,b) = 1$, akkor a szorzatuk is négyzetmentes;

$$a = p_1 \dots p_r, \qquad b = q_1 \dots q_s, \qquad ab = p_1 \dots p_r q_1 \dots q_s,$$

és így

$$\mu(a)\mu(b) = (-1)^r(-1)^s = (-1)^{r+s} = \mu(ab)\,.$$

Továbbá például

$$-1 = \mu(5)\mu(15) \neq \mu(75) = 0,$$

tehát $\mu(n)$ nem teljesen multiplikatív.

(Megjegyezzük, hogy a $\mu(n)$ esetében — szemben a $d(n)$, $\varphi(n)$ és $\sigma(n)$ függvényeknél tapasztaltakkal — olyan a, b számpárokból is végtelen sok van, amelyekre $(a,b) \neq 1$ és mégis $\mu(a)\mu(b) = \mu(ab)$; legyen például $a = 4$ és b tetszőleges páros szám.)

A $d_k(n)$-re vonatkozó állítást a $\sigma(n)$-nél látottakhoz hasonlóan igazolhatjuk.

Végül, az $\omega(n)$-re és $\Omega(n)$-re vonatkozó állítás azonnal következik a függvények 6.2.5 Definíciójából. ■

Feladatok

6.2.1 Bizonyítsuk be a $\sigma(n)$ multiplikativitását az 1.6.5a-b feladat felhasználásával, majd ennek alapján vezessük le a $\sigma(n)$ képletét.

6.2.2 Mutassuk meg, hogy ha $(a,b) \neq 1$, akkor $\sigma(ab) < \sigma(a)\sigma(b)$, továbbá $k > 1$ esetén $d_k(ab) < d_k(a)d_k(b)$.

6.2.3 Tegyük fel, hogy $n\varphi(n)\sigma(n)$ nem osztható 3-mal. Bizonyítsuk be, hogy ekkor n négyzetszám.

6.2.4 Bizonyítsuk be, hogy minden n-hez végtelen sok olyan k létezik, amelyre $\sigma(n) \mid \sigma(n^k)$.

6.2.5 Egy n szám (pozitív) osztóinak az összegét elosztjuk az n (pozitív) osztói reciprokainak az összegével. Mit kapunk eredményül?

6.2.6 Határozzuk meg az összes olyan n-et, amelyre $\sigma(n)$
a) páratlan; b) kettőhatvány.

M*6.2.7 Bizonyítsuk be, hogy a $\sigma(n)$ függvény értékkészletéből végtelen sok természetes szám kimarad.

M*6.2.8 Határozzuk meg az összes olyan n pozitív egészt, amelyhez létezik olyan k, hogy $\sigma(n!) = k!$.

6.2.9 Mutassuk meg, hogy bármely n összetett számra $\sigma(n) \geq n + \sqrt{n} + 1$. Mikor áll egyenlőség?

6.2.10 Tekintsük a $\sigma(n) = n + c$ egyenletet, ahol az n az ismeretlen és a c rögzített pozitív egész.

a) Oldjuk meg az egyenletet, ha c értéke
(a1) 1; (a2) 5; (a3) 8; (a4) 11.

b) Mely c értékek esetén van az egyenletnek végtelen sok megoldása?

c) Tegyük fel, hogy a páros Goldbach-sejtés abban a kicsit erősebb értelemben igaz, hogy minden 6-nál nagyobb páros szám előáll két *különböző* prímszám összegeként. Mutassuk meg, hogy ekkor a fenti egyenletnek minden $c \neq 5$ páratlan szám esetén létezik megoldása.

Megjegyzés: Sokáig megoldatlan probléma volt, hogy végtelen sok olyan c pozitív egész létezik-e, amelyre egyáltalán nincs megoldás. Erdős megmutatta, hogy valóban végtelen sok ilyen (páros) c van.

6.2.11 Tekintsük a $\sigma(n) - \varphi(n) = c$ egyenletet, ahol az n az ismeretlen és a c rögzített pozitív egész.

a) Oldjuk meg az egyenletet, ha c értéke
(a1) 2; (a2) 4; (a3) 5; (a4) 10.

b) Mely c értékek esetén van az egyenletnek végtelen sok megoldása?

c) Tegyük fel, hogy a páros Goldbach-sejtés abban a kicsit erősebb értelemben igaz, hogy minden 6-nál nagyobb páros szám előáll két *különböző* prímszám összegeként. Adjunk meg ennek alapján végtelen sok olyan c értéket, amelyre a fenti egyenletnek létezik megoldása.

6.2.12 Hány olyan $a \neq b$ számpár létezik, ahol a és b is összetett és
a) $a + \varphi(b) = b + \varphi(a)$; *b) $a + \sigma(b) = b + \sigma(a)$?

6.2.13 Bizonyítsuk be, hogy az alábbi egyenlőtlenségek minden n-re teljesülnek, és határozzuk meg, mikor áll egyenlőség.

a) $\sigma(n) \le \dfrac{(n+1)d(n)}{2}$;

b) $\sigma(n) \le \dfrac{nd(n)}{2} + 1$;

c) $\sigma(n) \ge n + 2d(n) - 3$.

*6.2.14 Oldjuk meg a $2\sigma(n) = nd(n)$ egyenletet.

6.2.15

a) Bizonyítsuk be, hogy az alábbi egyenlőtlenségek minden $n > 1$ számra teljesülnek, és határozzuk meg, mikor áll egyenlőség.

(a1) $\sigma(n)\varphi(n) \le n^2 - 1$; (a2) $\sigma(n) + \varphi(n) \ge 2n$.

*b) Igazoljuk, hogy

(b1) $\sigma(n)\varphi(n) > \dfrac{n^2}{2}$; (b2) $\inf \dfrac{\sigma(n)\varphi(n)}{n^2} = \dfrac{6}{\pi^2}$.

*6.2.16 Bizonyítsuk be:

$$\varphi(n) \mid n\sigma(n) - 2 \iff n \text{ prím vagy } n = 1,\ 4,\ 6,\ 22.$$

6.2.17 Milyen értékeket vesznek fel az alábbi függvények?

a) $f(n) = \mu(n) + \mu(2n) + \mu(5n) + \mu(10n)$;

M b) $g(n) = \displaystyle\sum_{k \mid 100!} \mu(kn)$.

6.2.18

a) Hány olyan egymást követő szám adható meg, hogy $\mu(n)$ azok egyikén sem nulla?

b) Hány olyan egymást követő szám adható meg, hogy $\mu(n)$ azok mindegyikén nulla?

*6.2.19 Igazoljuk, hogy a primitív komplex n-edik egységgyökök összege $\mu(n)$.

6.2.20 Adjuk meg egyszerűbb alakban a $\mu(n)\big(\Omega(n) - \omega(n)\big)$ függvényt.

6.2.21

a) Bizonyítsuk be, hogy

$$2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}$$

minden n-re teljesül. Mikor áll egyenlőség?

b) Hogyan általánosítható az a) rész $d(n)$-ről $d_k(n)$-re?

6.2.22 Melyek igazak az alábbi állítások közül?
a) Ha n négyzetszám, akkor $d(n) \mid d_3(n)$.
b) Ha $d(n) \mid d_3(n)$, akkor n négyzetszám.

6.2.23 Legyen ν tetszőleges valós szám és definiáljuk a $\sigma_\nu(n)$ függvényt, mint az n pozitív osztói ν-edik hatványainak az összegét:

$$\sigma_\nu(n) = \sum_{d|n} d^\nu .$$

Speciálisan: $\sigma_1(n) = \sigma(n)$ és $\sigma_0(n) = d(n)$.
Adjunk képletet $\sigma_\nu(n)$-re, és lássuk be, hogy $\sigma_\nu(n)$ multiplikatív.

6.3. Tökéletes számok

A régi görögök számmisztikájának fontos eleme, hogy egy szám osztóját (kivéve magát a számot) a szám részének tekintették, és tökéletesnek nevezték azokat a számokat, amelyek a „részeikből összeállnak". Ilyen például a $6 = 1 + 2 + 3$ és a $28 = 1 + 2 + 4 + 7 + 14$. Euklidész Elemek című könyvében szerepel az alábbi általános konstrukció is (bizonyítással együtt!):

„Ha az egységtől kezdve kétszeres arányban képezünk egy mértani sorozatot, amíg a sorösszeg prím nem lesz, és az összeggel megszorozzuk az utolsó tagot, akkor a szorzat tökéletes szám lesz."

Mai terminológiával a tökéletes számok éppen azok, amelyekre $\sigma(n) = 2n$ (hiszen magát az n-et is az osztók közé számítjuk), és Euklidész tétele szerint az

$$(1 + 2 + 2^2 + \ldots + 2^k)2^k = (2^{k+1} - 1)2^k$$

szám tökéletes, ha $2^{k+1} - 1$ prím. A $k = 1$ és $k = 2$ esetekben éppen a 6-ot és a 28-at kapjuk.

A $2^s - 1$ alakú prímek a Mersenne-prímek (lásd az 5.2 pontot), és tudjuk, hogy ekkor s is szükségképpen prím. Mint az 5.2 pontban már említettük, Mersenne (másokhoz hasonlóan) éppen a minél nagyobb tökéletes számok előállítása céljából foglalkozott az ilyen alakú prímekkel.

Euler bebizonyította, hogy minden *páros* tökéletes szám az euklideszi konstrukcióval nyerhető. Ebből következik, hogy a páros tökéletes számok száma megegyezik a Mersenne-prímek számával. Mivel megoldatlan, hogy végtelen sok Mersenne-prím létezik-e, így azt sem tudjuk, vajon páros tökéletes számból végtelen sok van-e. További megoldatlan probléma, hogy a páratlan számok között található-e egyáltalán tökéletes szám. Ezek az igen egyszerűen

hangzó, több mint kétezer éves kérdések a matematika talán legrégibb megoldatlan problémái.

Most megismételjük a tökéletes szám definícióját, és bebizonyítjuk a páros tökéletes számok leírását megadó Euklidész–Euler-tételt.

6.3.1 Definíció **D 6.3.1**

Az n pozitív egész *tökéletes szám*, ha $\sigma(n) = 2n$. ♣

6.3.2 Tétel **T 6.3.2**

Egy n páros szám akkor és csak akkor tökéletes, ha $n = 2^{p-1}(2^p - 1)$ alakú, ahol $2^p - 1$ (Mersenne-)prím (és így p is szükségképpen prím). ♣

Bizonyítás: Először megmutatjuk, hogy az ilyen alakú számok valóban tökéletesek. Mivel $2^p - 1$ prím, ezért a megadott alak egyben az n kanonikus alakja, és így a 6.2.2 Tétel szerint kapjuk, hogy

$$\sigma(n) = (1 + 2 + \ldots + 2^{p-1})(1 + (2^p - 1)) = (2^p - 1)2^p = 2n\,.$$

A megfordításhoz tegyük fel, hogy n páros és tökéletes, azaz

$$n = 2^k t, \text{ ahol } k \geq 1 \text{ és } t \text{ páratlan, továbbá } \sigma(n) = 2n\,. \tag{1}$$

Mivel $(2^k, t) = 1$, ezért a σ-függvény multiplikativitását és a $\sigma(2^k)$-ra vonatkozó képletet felhasználva (1)-ből

$$2^{k+1}t = 2n = \sigma(n) = \sigma(2^k)\sigma(t) = (2^{k+1} - 1)\sigma(t) \tag{2}$$

adódik.

Vonjuk ki (2)-ből (pontosabban az egyenlőségsor első és utolsó tagjából) a $(2^{k+1} - 1)t$ értéket, ekkor a t számot szorzattá tudjuk bontani:

$$t = (2^{k+1} - 1)(\sigma(t) - t)\,. \tag{3}$$

A (3)-ból következik, hogy a t osztói között szerepel a $\sigma(t) - t$. Emellett $k \geq 1$ miatt $2^{k+1} - 1 > 1$, ezért (3) alapján $\sigma(t) - t \neq t$.

Mivel $\sigma(t) - t$ és t különböző osztói t-nek, továbbá ezek összege egyenlő $\sigma(t)$-vel, vagyis a t összes osztójának az összegével, ezért a t-nek nem lehet több osztója. Ez azt jelenti, hogy t prím, és így $\sigma(t) - t = 1$.

Ezt (3)-ba, majd (1)-be visszahelyettesítve kapjuk, hogy

$$n = 2^k(2^{k+1} - 1), \quad \text{ahol} \quad 2^{k+1} - 1 \text{ prím},$$

ami (a $p = k + 1$ helyettesítés után) éppen az n keresett előállítását adja. ■

Feladatok

6.3.1 Mutassuk meg, hogy minden páros tökéletes szám utolsó számjegye 6 vagy 8 (a tízes számrendszerben).

6.3.2 Bizonyítsuk be, hogy ha létezik egy páratlan n tökéletes szám, akkor szükségképpen

a) $n = s^2p$, ahol p egy $4k + 1$ alakú prím;

b) $n \equiv 1 \pmod{12}$ vagy $n \equiv 9 \pmod{36}$.

6.3.3 Egy természetes számot a régi görögök nyomán *hiányos*nak nevezünk, ha nagyobb, mint a nála kisebb pozitív osztóinak az összege (azaz „a részei együttesen kevesebbet tesznek ki nála"). *Bővelkedő* egy szám, ha ez az összeg nagyobb magánál a számnál (azaz „a részei együttesen többet tesznek ki nála"). Például a 10 hiányos, mert $1 + 2 + 5 < 10$, a 12 viszont bővelkedő, mert $1 + 2 + 3 + 4 + 6 > 12$.
Igazoljuk az alábbi állításokat.

a) Minden prímhatvány hiányos szám.

b) Ha egy n páratlan számnak csak két különböző prímosztója van, akkor n hiányos.

c) Minden $k \geq 3$ esetén végtelen sok olyan páratlan bővelkedő szám és végtelen sok olyan páratlan hiányos szám létezik, amelynek pontosan k különböző prímosztója van.

d) Egy bővelkedő szám minden többszöröse is bővelkedő.

e) Bármely hiányos számnak végtelen sok bővelkedő többszöröse és végtelen sok hiányos többszöröse van.

*6.3.4 Ha az osztók közül magán a számon kívül az 1-et is kihagyjuk, és a többi osztóból akarjuk a számot összeállítani, akkor a $\sigma(n) = 2n + 1$ feltételhez jutunk. Bizonyítsuk be, hogy egy ilyen tulajdonságú szám szükségképpen egy páratlan szám négyzete.

Megjegyzés: Ezeket a számokat *kvázitökéletes* számoknak nevezzük. Megoldatlan probléma, hogy egyáltalán létezik-e kvázitökéletes szám.

M*6.3.5 Az n pozitív egészt *szupertökéletes*nek nevezzük, ha $\sigma(\sigma(n)) = 2n$. Bizonyítsuk be az alábbi állításokat.

a) Egy n páros szám akkor és csak akkor szupertökéletes, ha $n = 2^{p-1}$ alakú, ahol $2^p - 1$ (Mersenne-)prím.

b) Egy páratlan szupertökéletes szám szükségképpen négyzetszám.

c) Egy páratlan prímszám hatványa nem lehet szupertökéletes.

Megjegyzés: Az a) rész szerint a páros szupertökéletes számok száma megegyezik a Mersenne-prímek számával, és így megoldatlan, hogy végtelen sok páros szupertökéletes szám létezik-e. Szintén megoldatlan, hogy a páratlan számok között található-e egyáltalán szupertökéletes szám.

6.3.6 Az n pozitív egészt *harmonikus szám*nak (vagy *Ore-szám*nak) nevezzük, ha a pozitív osztóinak a harmonikus közepe egész szám. Bizonyítsuk be az alábbi állításokat.

a) Az n akkor és csak akkor harmonikus, ha $\sigma(n) \mid nd(n)$.

b) Minden tökéletes szám egyben harmonikus is.

c) Egy prímhatvány nem lehet harmonikus.

d) A négyzetmentes számok közül egyedül a 6 harmonikus.

Megjegyzés: Léteznek a tökéletes számokon kívül is harmonikus számok, ilyen például az 1 és a 140. Megoldatlan probléma, hogy végtelen sok harmonikus szám van-e, és hogy az 1-nél nagyobb páratlan számok között található-e egyáltalán harmonikus szám.

6.3.7 Az $a \neq b$ pozitív egészek *barátságos* számpárt alkotnak, ha $\sigma(a) = \sigma(b) = a + b$. Ilyen számpár például a 220 és a 284.

a) Mutassuk meg, hogy egy barátságos számpár egyik tagja hiányos, a másik tagja pedig bővelkedő szám (a definíciókat lásd a 6.3.3 feladatban).

b) Igazoljuk, hogy egy barátságos számpár egyik eleme sem lehet kettőhatvány.

Megjegyzés: A barátságos számok fogalma is a régi görögöktől ered: „az egyik szám részeiből, azaz nála kisebb pozitív osztóiból éppen összeáll a másik szám, és viszont”. Megoldatlan probléma, hogy létezik-e végtelen sok barátságos számpár, továbbá, hogy létezik-e egyáltalán olyan barátságos számpár, amelynek elemei relatív prímek, illetve ellenkező paritásúak.

6.4. A $d(n)$ függvény vizsgálata

Először megmutatjuk, hogy a $d(n)$ függvény értékei szeszélyesen ingadoznak, a függvény „grafikonjában” tetszőlegesen mély „völgyek” és tetszőlegesen magas „hegyek” találhatók.

6.4.1 Tétel (Völgytétel) **T 6.4.1**

Tetszőleges K pozitív egészhez végtelen sok olyan n található, amelyre

$$d(n-1)-d(n)>K \qquad \text{és} \qquad d(n+1)-d(n)>K \tag{1}$$

egyidejűleg teljesül. ♣

Bizonyítás: Az n-et alkalmas prímszámoknak fogjuk választani, ekkor $d(n)=2$.

Az (1) feltétel így azt jelenti, hogy $n-1$-nek és $n+1$-nek is legalább $K+3$ osztója van. Ez biztosan teljesül, ha például $2^{K+2} \mid n-1$ és $3^{K+2} \mid n+1$, azaz ha az n megoldása az

$$x \equiv 1 \pmod{2^{K+2}}, \qquad x \equiv -1 \pmod{3^{K+2}} \tag{2}$$

szimultán kongruenciarendszernek.

A (2) rendszer $(2^{K+2}, 3^{K+2})=1$ miatt biztosan megoldható, és az összes (pozitív) megoldás $x \equiv x_0 \pmod{6^{K+2}}$, azaz

$$x = x_0 + t6^{K+2}, \quad t=0,1,2,\dots \tag{3}$$

alakba írható.

Azt kell még igazolnunk, hogy a (3) számtani sorozatban végtelen sok prím található. Ez Dirichlet tétele (5.3.1 Tétel) szerint akkor teljesül, ha $(x_0, 6^{K+2})=1$. Mivel x_0 kielégíti (2)-t, ezért x_0 relatív prím a 2-höz és a 3-hoz, és így 6^{K+2}-höz is. ■

6.4.2 Tétel (Hegytétel) **T 6.4.2**

Tetszőleges K pozitív egészhez végtelen sok olyan n található, amelyre

$$d(n)-d(n-1)>K \qquad \text{és} \qquad d(n)-d(n+1)>K \tag{4}$$

egyidejűleg teljesül. ♣

Bizonyítás: Az n-et az első r prímszám szorzatának fogjuk választani:

$$n = p_1 \dots p_r, \qquad \text{ekkor} \qquad d(n)=2^r. \tag{5}$$

Meg fogjuk mutatni, hogy

$$d(n-1) \le 2^{r-1} \qquad \text{és} \qquad d(n+1) \le 2^{r-1}. \tag{6}$$

Így (5)-ből és (6)-ból már következik, hogy

$$d(n) - d(n-1) \geq 2^{r-1} \qquad \text{és} \qquad d(n) - d(n+1) \geq 2^{r-1}\,,$$

azaz $2^{r-1} > K$ esetén (4) is teljesül.

A (6)-beli egyenlőtlenségek közül a $d(n+1)$-re vonatkozót bizonyítjuk, a másik igazolása ugyanúgy történhet.

Írjuk fel $n+1$-et prímek szorzataként: $n+1 = q_1 \dots q_s$ (itt $q_i = q_j$ is előfordulhat). Mivel n az első r prímszám szorzata és $(n+1, n) = 1$, ezért bármely i esetén $q_i > p_r$ (ahol p_r az r-edik prímszám).

Az $n+1$ összes osztóját úgy kapjuk meg, hogy valahány q_j-t kiválasztunk, és ezeket összeszorozzuk (például az 1, illetve az $n+1$ akkor adódik, ha egyetlen q_j-t sem választunk, illetve az összes q_j-t vesszük). Ha a q_j-k nem mind különbözők, akkor ugyanazt az osztót többféleképpen is megkapjuk. Ennek alapján $d(n+1) \leq 2^s$. A (6)-beli $d(n+1) \leq 2^{r-1}$ egyenlőtlenséghez így elég azt megmutatnunk, hogy $s \leq r-1$.

Tegyük fel indirekt, hogy $s \geq r$. Ekkor ($r \geq 2$ esetén) az alábbi módon jutunk ellentmondásra:

$$n+1 = q_1 \dots q_s \geq q_1 \dots q_r \geq p_r^r + 1 \geq p_1 \dots p_r + 2 = n+2\,. \quad \blacksquare$$

Az imént bizonyított hegy- és völgytétel is illusztrálja, hogy a $d(n)$ függvény igen szabálytalanul viselkedik. A következőkben az első n helyen felvett függvényértékek átlagát fogjuk vizsgálni, és kiderül, hogy ez az *átlagérték*függvény (vagy *középérték*függvény) már igen „szép” képet mutat.

6.4.3 Tétel **T 6.4.3**

Legyen

$$D(n) = \sum_{i=1}^{n} d(i).$$

Ekkor bármely n-re

$$\left| \frac{D(n)}{n} - \log n \right| \leq 1\,. \ \clubsuit \tag{7}$$

Bizonyítás: Fel fogjuk használni, hogy bármely n-re

$$\log n < \sum_{j=1}^{n} \frac{1}{j} \leq 1 + \log n\,. \tag{8}$$

(A (8) egyenlőtlenség az 5.6.1 Tétel első bizonyításában alkalmazott integrálos terület-összehasonlítás segítségével igazolható.)

Készítsünk egy $n \times n$-es táblázatot (mátrixot), amelyben az i-edik sor j-edik eleme, a_{ij} aszerint 1 vagy 0, hogy a j osztója-e az i-nek vagy sem:

$$a_{ij} = \begin{cases} 1, & \text{ha } j \mid i; \\ 0, & \text{ha } j \nmid i. \end{cases}$$

Például $n = 6$-ra a következő táblázatot kapjuk:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

A bizonyítás alapgondolata, hogy kétféleképpen is meghatározzuk a táblázat összes elemének az összegét (vagyis a táblázatban szereplő 1-esek számát).

Az i-edik sorban annyi 1-es szerepel, ahányszor $j \mid i$ teljesül, vagyis az i-edik sor elemeinek az összege $d(i)$. Innen soronkénti összegzéssel azt kapjuk, hogy a táblázat elemeinek az összege

$$D(n) = \sum_{i=1}^{n} d(i). \tag{9}$$

A j-edik oszlopban pontosan a

$$j,\ 2j,\ \ldots,\ \left\lfloor \frac{n}{j} \right\rfloor j$$

sorszámú helyeken áll 1-es, tehát a j-edik oszlop elemeinek az összege $\lfloor n/j \rfloor$. Innen oszloponkénti összegzéssel az adódik, hogy a táblázat elemeinek az összege

$$\sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor. \tag{10}$$

Mivel (9) és (10) is a táblázat elemeinek az összege, ezért

$$D(n) = \sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor . \tag{11}$$

Az

$$\frac{n}{j} - 1 < \left\lfloor \frac{n}{j} \right\rfloor \le \frac{n}{j}$$

egyenlőtlenség és (8) felhasználásával (11)-ből egyrészt

$$D(n) \le \sum_{j=1}^{n} \frac{n}{j} = n \sum_{i=1}^{n} \frac{1}{j} \le n(1 + \log n) , \tag{12a}$$

másrészt

$$D(n) > \sum_{j=1}^{n} \Big(\frac{n}{j} - 1 \Big) = \Big(n \sum_{j=1}^{n} \frac{1}{j} \Big) - n > n(-1 + \log n) \tag{12b}$$

adódik. A (12a) és (12b) egyenlőtlenségeket n-nel osztva éppen a bizonyítandó (7) egyenlőtlenséget kapjuk. ■

A 6.4.3 Tétel állítását $|D(n) - n \log n| \le n$ alakba is írhatjuk. Az alábbi tételben a $D(n)$ és az $n \log n$ függvények eltérésére (azaz a „hibatagra") ennél erősebb becslést adunk.

Ehhez szükségünk lesz a $\sum_{j=1}^{n} 1/j$ összegnek a (8)-nál pontosabb, következő becslésére is: A $\sum_{j=1}^{n} 1/j - \log n$ sorozat konvergens, a határértéke $\gamma = 0{,}577\ldots$ az ún. Euler-konstans, és bármely n-re

$$\Big| \sum_{j=1}^{n} \frac{1}{j} - \log n - \gamma \Big| \le \frac{10}{n} . \tag{13}$$

6.4.4 Tétel **T 6.4.4**

Létezik olyan c konstans, hogy bármely n-re

$$|D(n) - n \log n - (2\gamma - 1)n| < c\sqrt{n} . \ \clubsuit \tag{14}$$

Bizonyítás: A $d(i)$ azoknak az x, y pozitív egész számpároknak a száma, amelyekre $xy = i$ (az x és y sorrendje is számít). Ennélfogva $D(n) = \sum_{i=1}^{n} d(i)$ azoknak az x, y pozitív egész számpároknak a száma, amelyekre $xy \le n$.

Ez azt jelenti, hogy $D(n)$ a síkon azoknak az (x, y) egész koordinátájú pontoknak, azaz rácspontoknak a száma, amelyek az első síknegyedben az $xy = n$ hiperbola és a koordinátatengelyek közé esnek, beleértve a hiperbolán levő rácspontokat, de nem számítva a koordinátatengelyek rácspontjait. Most megszámoljuk ezeket a rácspontokat.

Legyen $A(n)$ azoknak az (x, y) rácspontoknak a száma, amelyekre $x \le \sqrt{n}$. Mivel a rácspontok elhelyezkedése szimmetrikus az $y = x$ egyenesre nézve, ezért azoknak a rácspontoknak a száma is $A(n)$, amelyekre $y \le \sqrt{n}$.

Ezzel minden rácspontot figyelembe vettünk, de kétszer számoltuk azokat a rácspontokat, amelyekre $x \le \sqrt{n}$ és $y \le \sqrt{n}$ is teljesül. Ezek éppen annak a négyzetnek a rácspontjai, amelynek egyik átlója az origót és a $(\sqrt{n}, \sqrt{n})$ pontot összekötő szakasz. Így ezeknek a rácspontoknak a száma $\lfloor\sqrt{n}\rfloor^2$.

Ez azt jelenti, hogy az összes rácspontok száma

$$D(n) = 2A(n) - \lfloor\sqrt{n}\rfloor^2. \tag{15}$$

Most meghatározzuk $A(n)$-et. Mivel a j abszcisszájú rácspontok száma $\lfloor n/j \rfloor$, ezért

$$A(n) = \sum_{j=1}^{\lfloor\sqrt{n}\rfloor} \left\lfloor \frac{n}{j} \right\rfloor. \tag{16}$$

A (16) jobb oldalán álló összeget a 6.4.3 Tétel bizonyításában látott módon becsülve azt kapjuk, hogy

$$A(n) = n \sum_{j=1}^{\lfloor\sqrt{n}\rfloor} \frac{1}{j} + f(n), \qquad \text{ahol} \quad |f(n)| < \sqrt{n}\,. \tag{17}$$

alkalmazzuk most a (17)-beli összegre (13)-at:

$$\sum_{j=1}^{\lfloor\sqrt{n}\rfloor} \frac{1}{j} = \log\lfloor\sqrt{n}\rfloor + \gamma + g(n), \qquad \text{ahol} \quad |g(n)| \le \frac{10}{\lfloor\sqrt{n}\rfloor}\,. \tag{18}$$

Ezt (17)-be beírva azt kapjuk, hogy

$$A(n) = n \log\lfloor\sqrt{n}\rfloor + \gamma n + h(n), \tag{19a}$$

ahol

$$|h(n)| = |ng(n) + f(n)| < \frac{10n}{\lfloor\sqrt{n}\rfloor} + \sqrt{n} < \frac{10n}{\frac{\sqrt{n}}{2}} + \sqrt{n} = 21\sqrt{n}\,. \tag{19b}$$

Most (19a) további átalakításához megbecsüljük a $\frac{\log n}{2} - \log\lfloor\sqrt{n}\rfloor$ különbséget.

Mivel $(\log x)' = 1/x$, ezért a Lagrange-féle középértéktétel szerint bármely $a > 1$-hez létezik olyan u, amelyre $a-1 < u < a$ és

$$\log a - \log(a-1) = \frac{\log a - \log(a-1)}{a-(a-1)} = \frac{1}{u} < \frac{1}{a-1}\,.$$

Ennélfogva $n \geq 4$-re

$$0 \leq \frac{\log n}{2} - \log\lfloor\sqrt{n}\rfloor < \log\sqrt{n} - \log(\sqrt{n}-1) < \frac{1}{\sqrt{n}-1} \leq \frac{2}{\sqrt{n}}\,. \tag{20}$$

A (20) alapján (19a) és (19b) átírható a következő alakba:

$$A(n) = \frac{n\log n}{2} + \gamma n + k(n), \qquad \text{ahol} \quad |k(n)| < 23\sqrt{n}\,. \tag{21}$$

Szükségünk lesz még $n - \lfloor\sqrt{n}\rfloor^2$ becslésére:

$$\begin{aligned} 0 \leq n - \lfloor\sqrt{n}\rfloor^2 &= (\sqrt{n})^2 - \lfloor\sqrt{n}\rfloor^2 = \\ &= (\sqrt{n} - \lfloor\sqrt{n}\rfloor)(\sqrt{n} + \lfloor\sqrt{n}\rfloor) < 1(\sqrt{n}+\sqrt{n}) = 2\sqrt{n}\,. \end{aligned} \tag{22}$$

Végül (21)-et és (22)-t (15)-be beírva azt kapjuk, hogy

$$D(n) = n\log n + (2\gamma - 1)n + \ell(n), \qquad \text{ahol} \quad |\ell(n)| < 48\sqrt{n}\,. \ \blacksquare$$

Megjegyzések: 1. A számelmélet egyik sokat vizsgált és nehéz problémája, hogy a 6.4.4 Tételben a hibatagra adott (14) becslés mennyire javítható. Bebizonyították, hogy az állítás akkor is érvényes, ha $\sqrt{n}$ helyére $n^{0{,}32}$-t írunk, azonban $n^{0{,}25}$-nel már nem marad igaz.

2. Mivel

$$\log 1 + \log 2 + \ldots + \log n \sim n\log n$$

(a két függvény aszimptotikusan egyenlő, azaz a hányadosuk 1-hez tart), ezért a 6.4.3 (vagy 6.4.4) Tételből az is következik, hogy

$$d(1) + d(2) + \ldots + d(n) \sim \log 1 + \log 2 + \ldots + \log n\,. \tag{23}$$

A (23) összefüggés úgy értelmezhető, hogy a $d(n)$ függvény „átlagos nagyságrendje" $\log n$.

Ez azonban nem jelenti azt, hogy egy „tipikus” n-nek „körülbelül” $\log n$ osztója lenne; a 6.7 pontban bebizonyítjuk (lásd a 6.7.6 feladatot), hogy az osztók száma általában ennél kevesebb, a „legtöbb” n-re $d(n)$ értéke „körülbelül”

$$(\log n)^{\log 2} = (\log n)^{0,69\ldots}\,.$$

A $\log n$-es átlag a ritkán előforduló, de kirívóan sok osztóval rendelkező számoknak köszönhető.

Végül a $d(n)$ függvény értékkészletének néhány további tulajdonságát vizsgáljuk.

A $d(n)$ függvény minden $k \geq 2$ egész számot végtelen sokszor felvesz, hiszen bármely p prímre $d(p^{k-1}) = k$.

Az 1.6.11 feladatban több egyszerű felső becslést adtunk $d(n)$-re az n függvényében. Az alábbi tételben ezeket élesítjük:

6.4.5 Tétel **T 6.4.5**

Bármely rögzített $\delta > 0$ esetén

$$\lim_{n\to\infty} \frac{d(n)}{n^{\delta}} = 0\,. \ \clubsuit$$

A bizonyításhoz az alábbi segédtételt használjuk fel:

6.4.6 Tétel **T 6.4.6**

Legyen

$$\{q_1 < q_2 < \ldots\} = \{2, 3, 4, 5, 7, 8, 9, 11, \ldots\}$$

a prímhatványok sorozata és f egy tetszőleges multiplikatív számelméleti függvény. Ekkor

$$\lim_{j\to\infty} f(q_j) = 0 \implies \lim_{n\to\infty} f(n) = 0\,. \ \clubsuit$$

A 6.4.6 Tétel bizonyítása: A feltétel szerint van olyan H és k, hogy

$$|f(q_j)| \leq H \text{ minden } j\text{-re}, \qquad \text{és} \qquad |f(q_j)| \leq 1, \ \text{ ha } \ j > k\,. \tag{24}$$

Először megmutatjuk, hogy bármely m-re

$$|f(m)| \leq H^k\,. \tag{25}$$

Ha m kanonikus alakja $m = \prod_{i=1}^{r} p_i^{\alpha_i}$, akkor az f multiplikativitása miatt

$$|f(m)| = \prod_{i=1}^{r} |f(p_i^{\alpha_i})| \,. \tag{26}$$

A (26) jobb oldalán szereplő tényezők közül (24) szerint legfeljebb k darab nagyobb, mint 1, és ezek értéke is legfeljebb H, azaz (25) valóban teljesül.

Legyen $\varepsilon > 0$ tetszőleges. Be kell látni, hogy létezik olyan $n_0 = n_0(\varepsilon)$, hogy minden $n > n_0$ esetén $|f(n)| < \varepsilon$.

A feltétel szerint létezik olyan $s = s(\varepsilon)$, hogy

$$|f(q_j)| < \frac{\varepsilon}{H^k} \,, \qquad \text{ha } j > s \,. \tag{27}$$

Megmutatjuk, hogy $q_1 \dots q_s$ megfelel n_0-nak.

Ha $n > q_1 \dots q_s$, akkor az n kanonikus alakjában szerepelnie kell egy q_s-nél nagyobb q_j prímhatványnak: $n = q_j m$, ahol $(q_j, m) = 1$.

Ekkor (27) alapján $|f(q_j)| < \varepsilon / H^k$, továbbá (25) alapján $|f(m)| \le H^k$, és így

$$|f(n)| = |f(q_j)| \cdot |f(m)| < \frac{\varepsilon}{H^k} \cdot H^k = \varepsilon \,. \quad \blacksquare$$

A 6.4.5 Tétel bizonyítása: A 6.4.6 Tételt az

$$f(n) = \frac{d(n)}{n^\delta}$$

függvényre fogjuk alkalmazni. Ehhez azt kell megmutatni, hogy

$$\lim_{j \to \infty} \frac{d(q_j)}{q_j^\delta} = 0 \,. \tag{28}$$

Legyen $q_j = p^\alpha$ (ahol p prím). Ekkor

$$d(q_j) = d(p^\alpha) = \alpha + 1 \le 2\alpha = \frac{2 \log(p^\alpha)}{\log p} \le \frac{2 \log q_j}{\log 2} \,,$$

tehát

$$\frac{d(q_j)}{q_j^\delta} \le \frac{2}{\log 2} \cdot \frac{\log q_j}{q_j^\delta} \,. \tag{29}$$

Mivel

$$\lim_{x \to \infty} \frac{\log x}{x^\delta} = 0 \,,$$

ezért (29)-ben a jobb oldal, és így a bal oldal is 0-hoz tart. $\blacksquare$

Megjegyzés: Megmutatható, hogy a $d(n)$ függvény „maximális" nagyságrendje körülbelül

$$n^{\frac{\log 2}{\log\log n}}\,.$$

Ez pontosan a következőket jelenti:

(i) Bármely $\varepsilon > 0$-hoz létezik olyan $n_0 = n_0(\varepsilon)$, hogy minden $n > n_0$ esetén

$$d(n) < n^{\frac{(1+\varepsilon)\log 2}{\log\log n}}\,.$$

(ii) Bármely $\varepsilon > 0$-hoz végtelen sok olyan n létezik, amelyre

$$d(n) > n^{\frac{(1-\varepsilon)\log 2}{\log\log n}}\,.$$

A (ii) állítás bizonyítását a 6.4.3b feladatban tűztük ki.

Feladatok

*6.4.1 Mutassuk meg, hogy a 6.4.1 és 6.4.2 Tételek állítása a $d(n)$ helyett a $\sigma(n)$, $\varphi(n)$, $\Omega(n)$, $\omega(n)$ és $k > 1$ esetén a $d_k(n)$ függvényekre is érvényes.

6.4.2 Bizonyítsuk be, hogy bármely rögzített $\delta > 0$ és k pozitív egész esetén

$$\lim_{n\to\infty} \frac{d_k(n)}{n^\delta} = 0\,.$$

6.4.3 Legyen $\varepsilon > 0$ tetszőleges. Mutassuk meg, hogy végtelen sok olyan n létezik, amelyre

a) $d(n) > (\log n)^{100}$; *b) $d(n) > n^{\frac{(1-\varepsilon)\log 2}{\log\log n}}$.

6.4.4 Mutassuk meg, hogy bármely n-re $\Omega(n) \le \log_2 n$. Mikor áll egyenlőség?

*6.4.5 Legyen $\varepsilon > 0$ tetszőleges. Igazoljuk az alábbi állításokat.

a) Minden elég nagy n-re

$$\omega(n) < \frac{(1+\varepsilon)\log n}{\log\log n}\,.$$

b) Végtelen sok n-re

$$\omega(n) > \frac{(1-\varepsilon)\log n}{\log\log n}\,.$$

6.4.6 Bizonyítsuk be, hogy minden elég nagy n esetén

$$\text{a) } \varphi(n) > n^{0,99}; \qquad \text{b) } \varphi(n) > \frac{n}{2\log n}; \qquad {}^*\text{c) } \varphi(n) > \frac{n}{C\log\log n};$$

és

$$\text{d) } \sigma(n) < n^{1,01}; \qquad \text{e) } \sigma(n) < 2n\log n; \qquad {}^*\text{f) } \sigma(n) < Cn\log\log n$$

(ahol a c) és f) részben C egy alkalmas abszolút konstans).

6.4.7 Igazoljuk az alábbi állításokat.

a) A $\varphi(n)/n$ függvény értékkészlete mindenütt sűrű a $[0,1]$ intervallumban.

b) A $\sigma(n)/n$ függvény értékkészlete mindenütt sűrű $[1,\infty]$-ben.

*6.4.8 A Dirichlet-tétel azt mondja ki, hogy ha az a és d pozitív egészek relatív prímek, akkor az $a + kd$, $k = 0, 1, 2, \ldots$ számtani sorozat végtelen sok prímet tartalmaz. Ez a tétel jelentősen élesíthető:

(i) Ezeknek a prímeknek a reciprokösszege divergens.

(ii) Az n-nél kisebb ilyen prímek száma rögzített d mellett $n \to \infty$-re

$$\sim \frac{n}{\varphi(d)\log n}.$$

Ezek az eredmények az 5.6.1, illetve 5.4.1 Tételek általánosításai.

a) Legyen k tetszőleges, rögzített pozitív egész. Mutassuk meg (i) felhasználásával, hogy $k \mid \varphi(n)$ majdnem minden n-re teljesül. Ez pontosan a következőt jelenti. Legyen $F(N)$ azon $x \le N$ egészeknek a száma, amelyekre $k \mid \varphi(x)$. Ekkor $\lim_{N\to\infty} F(N)/N = 1$.

M b) Lássuk be, hogy a φ-függvény értékkészletéből majdnem minden pozitív egész hiányzik. (Az előzőkhöz hasonlóan ezen a következőt kell érteni. Legyen $G(N)$ azon $y \le N$ értékeknek a száma, amelyek előfordulnak a φ-függvény értékkészletében. Ekkor $\lim_{N\to\infty} G(N)/N = 0$.)

*6.4.9 Mutassuk meg, hogy az előző feladat állításai a φ helyett a σ-függvényre is érvényesek.

6.5. Összegzési és megfordítási függvény

6.5.1 Definíció **D 6.5.1**

Az f számelméleti függvény osztókra vonatkozó *összegzési függvényén* az

$$f^+(n) = \sum_{d|n} f(d)$$

függvényt értjük. ♣

Példák:

Az $f(n) = 1$ függvény összegzési függvénye $f^+(n) = d(n)$, a $g(n) = n$ függvényé pedig $g^+(n) = \sigma(n)$.

A 2.3.14 feladat szerint $\varphi^+(n) = n$, a 6.2.4 Tétel alapján $\mu^+(n) = e(n)$, ahol

$$e(n) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1. \end{cases} \tag{1}$$

6.5.2 Tétel **T 6.5.2**

Bármely f számelméleti függvényhez pontosan egy olyan függvény található, amelynek az összegzési függvénye f. Ezt az egyértelműen meghatározott függvényt az f *megfordítási függvényének* nevezzük, és $\tilde{f}$-mal jelöljük. ♣

Bizonyítás: Írjuk fel minden n-re a megfordítási függvénytől megkövetelt

$$f(n) = \sum_{d|n} \tilde{f}(d)$$

egyenlőségeket:

$$\begin{aligned}
f(1) &= \tilde{f}(1) \\
f(2) &= \tilde{f}(1) + \tilde{f}(2) \\
f(3) &= \tilde{f}(1) + \tilde{f}(3) \\
f(4) &= \tilde{f}(1) + \tilde{f}(2) + \tilde{f}(4) \\
f(5) &= \tilde{f}(1) + \tilde{f}(5) \\
f(6) &= \tilde{f}(1) + \tilde{f}(2) + \tilde{f}(3) + \tilde{f}(6) \\
&\vdots
\end{aligned}$$

Azt kell belátni, hogy ez a végtelen sok egyenletből álló és a végtelen sok $\tilde{f}(1), \tilde{f}(2), \ldots$ ismeretlenre vonatkozó „egyenletrendszer" egyértelműen megoldható.

Az első egyenlet pontosan akkor teljesül, ha

$$\tilde{f}(1) = f(1)\,.$$

Az első és második egyenlet együttesen pontosan akkor teljesül, ha $\tilde{f}(1)$ az első egyenletből kapott érték és

$$\tilde{f}(2) = f(2) - \tilde{f}(1)\,.$$

Ugyanígy haladhatunk tovább indukcióval. Tegyük fel, hogy az első $m-1$ egyenletből álló egyenletrendszernek pontosan egy $\tilde{f}(1), \ldots, \tilde{f}(m-1)$ megoldása van, és tekintsük most az első m egyenletből álló rendszert. Mivel az $\tilde{f}(m)$ „ismeretlen" először az m-edik egyenletben fordul elő, így az első m egyenlet együttesen pontosan akkor teljesül, ha $\tilde{f}(1), \ldots, \tilde{f}(m-1)$ az első $m-1$ egyenletből (az indukció szerint) egyértelműen adódó érték és

$$\tilde{f}(m) = f(m) - \sum_{\substack{d|m \\ d<m}} \tilde{f}(d)\,. \tag{2}$$

Ezzel az $\tilde{f}$ függvény létezését és egyértelműségét beláttuk. (A (2) képlet az $\tilde{f}$ függvény értékeinek egy rekurzív előállítását jelenti). ■

Példák: A 6.5.1 Definíció utáni példákat „visszafelé olvasva" (és az ottani jelöléseket használva) azt kapjuk, hogy

$$\tilde{d}(n) = 1; \qquad \tilde{\sigma}(n) = n; \qquad \tilde{g}(n) = \varphi(n); \qquad \tilde{e}(n) = \mu(n)\,.$$

Az alábbiakban a megfordítási függvényt „képlet" alakban is előállítjuk:

6.5.3 Tétel (Möbius-féle megfordítási formula) **T 6.5.3**

$$\tilde{f}(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})\,. \ \clubsuit \tag{3}$$

Bizonyítás: Mivel a 6.5.2 Tétel szerint $\tilde{f}$ egyértelműen létezik, így elég megmutatni, hogy a (3) jobb oldalán megadott

$$h(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{cd=n} \mu(d) f(c)$$

függvény $h^+(n)$ összegzési függvénye éppen $f(n)$. Ezt a szereplő összegek megfelelő átrendezésével és (1) felhasználásával igazolhatjuk:

$$h^+(n) = \sum_{k|n} h(k) = \sum_{k|n} \sum_{cd=k} \mu(d) f(c) = \sum_{cd|n} \mu(d) f(c) =$$
$$= \sum_{c|n} f(c) \Big(\sum_{d|\frac{n}{c}} \mu(d) \Big) = \sum_{c|n} f(c) \mu^+(\frac{n}{c}) = \sum_{c|n} f(c) e(\frac{n}{c}) = f(n)\,. \ \blacksquare$$

Végül a megfordítási függvény egy érdekes alkalmazását, az ún. Smith-féle determinánst mutatjuk be:

6.5.4 Tétel **T 6.5.4**

Legyen f tetszőleges számelméleti függvény, és képezzük az $n \times n$-es

$$A = \begin{pmatrix} f\big((1,1)\big) & f\big((1,2)\big) & \dots & f\big((1,n)\big) \\ f\big((2,1)\big) & f\big((2,2)\big) & \dots & f\big((2,n)\big) \\ \vdots & \vdots & \ddots & \vdots \\ f\big((n,1)\big) & f\big((n,2)\big) & \dots & f\big((n,n)\big) \end{pmatrix}$$

mátrixot, ahol (i,j) az i és j számok legnagyobb közös osztóját jelenti. Ekkor az A mátrix determinánsa

$$\det A = \tilde{f}(1)\tilde{f}(2)\dots\tilde{f}(n)\,. \ \clubsuit$$

Bizonyítás: Tekintsük azt az $n \times n$-es B, illetve C mátrixot, amelyben az i-edik sor j-edik eleme b_{ij}, illetve c_{ij}, ahol

$$b_{ij} = \begin{cases} 1, & \text{ha } j \mid i; \\ 0, & \text{ha } j \nmid i, \end{cases}$$

és

$$c_{ij} = b_{ij}\tilde{f}(j)\,, \qquad \text{azaz} \qquad c_{ij} = \begin{cases} \tilde{f}(j), & \text{ha } j \mid i; \\ 0, & \text{ha } j \nmid i. \end{cases}$$

Mindkét mátrixban a főátló fölött csupa 0 áll, tehát a determinánsuk a főátlóbeli elemek szorzata. A B mátrix főátlójában minden elem 1-es, a C mátrix főátlójában pedig az $\tilde{f}(1), \dots, \tilde{f}(n)$ elemek szerepelnek, ezért

$$\det B = 1 \qquad \text{és} \qquad \det C = \tilde{f}(1)\tilde{f}(2)\dots\tilde{f}(n)\,. \tag{4}$$

Most vizsgáljuk meg a $D = BC^T$ szorzatmátrixot, ahol C^T a C mátrix transzponáltját jelöli. Ekkor D-ben az i-edik sor j-edik eleme

$$\begin{aligned} d_{ij} &= b_{i1}c_{j1} + b_{i2}c_{j2} + \ldots + b_{in}c_{jn} = \\ &= b_{i1}b_{j1}\tilde{f}(1) + b_{i2}b_{j2}\tilde{f}(2) + \ldots + b_{in}b_{jn}\tilde{f}(n)\,. \end{aligned} \tag{5}$$

Itt

$$b_{ik}b_{jk}\tilde{f}(k) = \begin{cases} \tilde{f}(k), & \text{ha } k \mid i \text{ és } k \mid j; \\ 0, & \text{egyébként,} \end{cases}$$

azaz

$$b_{ik}b_{jk}\tilde{f}(k) = \begin{cases} \tilde{f}(k), & \text{ha } k \mid (i,j); \\ 0, & \text{ha } k \nmid (i,j). \end{cases} \tag{6}$$

A (6)-ot (5)-be beírva és $\tilde{f}$ definícióját felhasználva azt kapjuk, hogy

$$d_{ij} = \sum_{k \mid (i,j)} \tilde{f}(k) = f\big((i,j)\big)\,,$$

tehát $D = A$.

Végül a determinánsok szorzástétele és (4) alapján

$$\det A = \det D = (\det B)(\det C) = \tilde{f}(1)\tilde{f}(2)\ldots\tilde{f}(n)\,. \quad \blacksquare$$

Feladatok

6.5.1 Mutassuk meg, hogy $d_k^+(n) = d_{k+1}(n)$.

6.5.2 Bizonyítsuk be az alábbi állításokat:

a) f multiplikatív $\iff$ f^+ multiplikatív.

b) f multiplikatív $\iff$ $\tilde{f}$ multiplikatív.

Megjegyzés: A 6.5.2 feladatból azonnal következik például a $d(n)$, $\sigma(n)$, illetve $\varphi(n)$ függvények multiplikativitása.

6.5.3

a) Melyek azok a teljesen multiplikatív függvények, amelyeknek az összegzési függvénye is teljesen multiplikatív?

b) Melyek azok az additív függvények, amelyeknek az összegzési függvénye is additív?

6.5.4 Legyen n kanonikus alakja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Bizonyítsuk be az alábbi állításokat.

a) Ha f multiplikatív és $f \neq 0$, akkor

$$f^+(n) = \prod_{i=1}^{r} \big(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i})\big)$$

és

$$\tilde{f}(n) = \prod_{i=1}^{r} \big(f(p_i^{\alpha_i}) - f(p_i^{\alpha_i - 1}\big).$$

b) Ha f teljesen multiplikatív, és egyetlen prím helyen sem veszi fel a 0 vagy 1 értéket, akkor

$$f^+(n) = \prod_{i=1}^{r} \frac{f(p_i)^{\alpha_i+1} - 1}{f(p_i) - 1} \quad \text{és} \quad \tilde{f}(n) = f(n) \prod_{i=1}^{r} \big(1 - \frac{1}{f(p_i)}\big)\,.$$

Mely függvények képlete adódik az $f(n) = n$ speciális esetben?

6.5.5 Adjuk meg az alábbi függvények megfordítási függvényét:

a) $f(n) = c$ (konstans függvény); b) $g(n) = \dfrac{(-1)^n + 1}{2}$;

c) $\Omega(n)$; d) $\omega(n)$.

6.5.6 Bizonyítsuk be, hogy ha f additív és $\omega(n) \geq 2$, akkor $\tilde{f}(n) = 0$.

6.5.7 Adjuk meg egyszerűbb alakban a

$$\sum_{ab=n} \sigma(a)\mu(b)$$

összeget.

6.5.8 Bizonyítsuk be, hogy

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}\,.$$

6.5.9 Igazoljuk az alábbi állításokat.

a) A primitív komplex n-edik egységgyökök összege $\mu(n)$.

*b) A primitív komplex n-edik egységgyökök k-adik hatványainak összege

$$\frac{\mu(n')\varphi(n)}{\varphi(n')}\,, \qquad \text{ahol} \qquad n' = \frac{n}{(n,k)}\,.$$

c) Ha p prím, akkor a modulo p páronként inkongruens primitív gyökök összege $\mu(p-1)$-gyel kongruens modulo p.

6.5.10 Számítsuk ki azokat az $n \times n$-es determinánsokat, ahol az i-edik sor j-edik eleme

$$\text{a) } (i,j)\,; \qquad \text{b) } \sigma\big((i,j)\big)\,; \qquad \text{c) } d\big((i,j)\big)\,; \qquad \text{d) } \omega\big((i,j)\big)\,.$$

6.5.11 Legyenek $s_1, \ldots, s_n$ tetszőleges olyan különböző pozitív egészek, amelyekre mindegyik s_i-nek minden osztója is szerepel az s_j-k között. Mutassuk meg, hogy a 6.5.4 Tétel megfelelője akkor is érvényben marad, ha az $1, 2, \ldots, n$ számok helyére mindenhol az $s_1, \ldots, s_n$ számokat írjuk.

6.6. Konvolúció

6.6.1 Definíció **D 6.6.1**

Az f és g számelméleti függvények *konvolúció*ján az

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{cd=n} f(d)g(c)$$

függvényt értjük. ♣

Az összegzési, illetve megfordítási függvény képzése a konvolúció speciális esete: f^+ definíció szerint az f és a konstans 1 függvény konvolúciója, $\tilde{f}$ pedig a Möbius-féle megfordítási formula alapján az f és μ konvolúciója, azaz

$$f^+ = f * 1 \qquad \text{és} \qquad \tilde{f} = f * \mu\,.$$

Most megvizsgáljuk a konvolúció művelet tulajdonságait.

6.6.2 Tétel **T 6.6.2**

A konvolúció asszociatív és kommutatív, az egységelem

$$e(n) = \begin{cases} 1, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1, \end{cases}$$

és pontosan azoknak az f-eknek létezik inverze, amelyekre $f(1) \neq 0$. ♣

Bizonyítás: Kommutativitás: közvetlenül következik a definícióból.
Asszociativitás:

$$\big(f * (g * h)\big)(n) = \sum_{bk=n} f(b)\big(\sum_{cd=k} g(c)h(d)\big) = \sum_{bcd=n} f(b)g(c)h(d)\,,$$

és ugyanerre az alakra hozható $\big((f * g) * h\big)(n)$ is.
Egységelem:

$$(e * f)(n) = \sum_{d|n} e(d) f(\frac{n}{d}) = 1 \cdot f(n) + \sum_{1<d|n} 0 \cdot f(\frac{n}{d}) = f(n)\,.$$

Inverz: A 6.5.2 Tétel bizonyításához hasonlóan járhatunk el. Az f függvény g inverzének az $e = f * g$ feltételt, vagyis az alábbi egyenlőségeket kell kielégítenie:

$$\begin{aligned}
1 &= e(1) = f(1)g(1) \\
0 &= e(2) = f(1)g(2) + f(2)g(1) \\
0 &= e(3) = f(1)g(3) + f(3)g(1) \\
0 &= e(4) = f(1)g(4) + f(2)g(2) + f(4)g(1) \\
0 &= e(5) = f(1)g(5) + f(5)g(1) \\
0 &= e(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1) \\
&\vdots
\end{aligned}$$

Ebben a végtelen sok egyenletből álló egyenletrendszerben $g(1), g(2), \ldots$ az ismeretlenek. Az első m egyenletben csak a $g(1), \ldots, g(m)$ ismeretlenek szerepelnek, a $g(m)$ először az m-edik egyenletben fordul elő.

Ha $f(1) = 0$, akkor az első egyenlet nem oldható meg, tehát $f(1) \neq 0$ az inverz létezésének szükséges feltétele. Az elégségességhez azt kell megmutatni, hogy $f(1) \neq 0$ esetén az egyenletrendszer (egyértelműen) megoldható.

Az első egyenlet pontosan akkor teljesül, ha

$$g(1) = \frac{1}{f(1)}\,.$$

Az első és második egyenlet együttesen pontosan akkor teljesül, ha $g(1)$ az első egyenletből egyértelműen adódó érték és

$$g(2) = \frac{-f(2)g(1)}{f(1)}\,.$$

Ugyanígy haladhatunk tovább indukcióval. Tegyük fel, hogy az első $m-1$ egyenletből álló egyenletrendszernek pontosan egy $g(1), \ldots, g(m-1)$ megoldása van, és tekintsük most az első m egyenletből álló rendszert. Mivel a $g(m)$ „ismeretlen" először az m-edik egyenletben fordul elő, így az első m egyenlet együttesen pontosan akkor teljesül, ha $g(1), \ldots, g(m-1)$ az első $m-1$ egyenletből (az indukció szerint) egyértelműen adódó érték és

$$g(m) = \frac{-1}{f(1)} \sum_{\substack{d|m \\ d<m}} g(d) f(\frac{m}{d})\,.$$

A g függvénynek ezzel a rekurzív definíciójával megadtuk az f inverzét. ■

Most a konvolúció segítségével egy egyszerű bizonyítást adunk a Möbius-féle megfordítási formulára, és ebből egyúttal az is világosabbá válik, mi az „oka" a μ függvény kitüntetett szerepének.

A megfordítási függvény definícióját a konvolúció segítségével az

$$\tilde{f} * 1 = f \tag{1}$$

egyenlőséggel írhatjuk fel, és ebből kell $\tilde{f}$-ot kifejezni. Jelöljük az 1 függvény inverzét g-vel, és „szorozzuk be" (1)-et g-vel (azaz vegyük mindkét oldalnak a g-vel való konvolúcióját). Ekkor (a konvolúció műveleti tulajdonságait is felhasználva) kapjuk, hogy

$$\tilde{f} = f * g\,. \tag{2}$$

Itt a g az 1 függvény inverze, ami azt jelenti, hogy $1 * g = e$, azaz $g^+ = e$, vagy más szóval $g = \tilde{e} = \mu$. Ezt (2)-be beírva

$$\tilde{f} = f * \mu$$

adódik, ami éppen a Möbius-féle megfordítási formula.

A számelméleti függvények vizsgálatánál igen fontos szerepet játszik a függvényekhez rendelt *Dirichlet-sor*:

6.6.3 Definíció **D 6.6.3**

Legyen f számelméleti függvény és S azoknak az s valós számoknak a halmaza, amelyekre a

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \tag{3}$$

végtelen sor konvergens. Ekkor az f-hez tartozó *Dirichlet-sor*on az

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

végtelen sorral értelmezett $F : S \to \mathbf{C}$ függvényt értjük. ♣

Az F függvény értelmezési tartománya tehát azoknak az s valós számoknak a halmaza, amelyekre a (3) végtelen sor konvergens.

Könnyen adódik (lásd a 6.6.6 feladatot), hogy ha (3) egy s_0 helyen konvergens, akkor minden $s > s_0 + 1$ helyen abszolút konvergens. A továbbiakban az $F(s)$ függvényt csak olyan s helyeken fogjuk tekinteni, amelyekre a (3) sor *abszolút konvergens*. Ennek az lesz az előnye, hogy felhasználhatjuk az abszolút konvergens sorokra vonatkozó tételeket, amelyeket úgy foglalhatunk össze, hogy abszolút konvergens sorokkal „ugyanúgy" számolhatunk, mint a véges sok tagból álló összegekkel. Ez többek között azt jelenti, hogy egy abszolút konvergens sor tagjait tetszőlegesen átrendezve és csoportosítva ismét abszolút konvergens sort kapunk, amelynek az összege megegyezik az eredeti sor összegével, és két abszolút konvergens sort a „minden tagot minden taggal" „szabály" szerint összeszorozva (és az így keletkező szorzatokat tetszőlegesen átrendezve és csoportosítva) egy olyan abszolút konvergens sort kapunk, amelynek az összege az eredeti két sor összegének a szorzata.

Megjegyezzük, hogy a Dirichlet-sort lehet (valós helyett) komplex változós függvényként, illetve a konvergenciát egyáltalán nem vizsgáló „formális sorként" is tekinteni, ezzel azonban nem foglalkozunk.

Az egyik legfontosabb Dirichlet-sor az $f = 1$ függvényhez tartozó *Riemann-féle zétafüggvény*:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,, \tag{4}$$

amelyet már az 5.6.6 feladatban definiáltunk. A (4) sor $s > 1$-re abszolút konvergens, és az 5.6.6 feladat szerint felírható az alábbi végtelen szorzatként is:

$$\zeta(s) = \prod_{p} \frac{1}{1 - \frac{1}{p^s}} = \lim_{n\to\infty} \prod_{p\le n} \frac{1}{1 - \frac{1}{p^s}}\,. \tag{5}$$

Az Eulertől származó (5) összefüggés alapján nem meglepő, hogy a prímszámok eloszlásának vizsgálata szoros kapcsolatba hozható a ζ-függvény viselkedésével. Így például a prímszámokra vonatkozóan különösen fontos tételeket nyerhetnénk, ha beigazolódna a híres *Riemann-sejtés*, amely azt állítja, hogy a komplex változóra megfelelően kiterjesztett ζ-függvény bármely nem valós gyökének a valós része $1/2$.

Az alábbi tétel a Dirichlet-sor és a konvolúció kapcsolatáról szól:

6.6.4 Tétel **T 6.6.4**

Jelölje az f, g, illetve h számelméleti függvényekhez tartozó Dirichlet-sorokat $F(s), G(s)$, illetve $H(s)$, és tegyük fel, hogy ezek abszolút konvergensek, továbbá $h = f * g$. Ekkor $H(s) = F(s)G(s)$. ♣

Bizonyítás: Az abszolút konvergens sorok szorzásának tulajdonságait felhasználva

$$F(s)G(s) = \Big(\sum_{k=1}^{\infty} \frac{f(k)}{k^s}\Big)\Big(\sum_{m=1}^{\infty} \frac{g(m)}{m^s}\Big) = \sum_{k=1}^{\infty}\sum_{m=1}^{\infty} \frac{f(k)g(m)}{(km)^s} =$$

$$= \sum_{n=1}^{\infty} \frac{\sum_{km=n} f(k)g(m)}{n^s} = \sum_{n=1}^{\infty} \frac{h(n)}{n^s} = H(s)\,. \blacksquare$$

A 6.6.4 Tétel alapján könnyen meghatározhatjuk például a Möbius-függvény

$$M(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

Dirichlet-sorát. Ez a sor $|\mu(n)| \le 1$ miatt $s > 1$-re abszolút konvergens. Mivel $\mu * 1 = e$, ezért

$$M(s)\zeta(s) = \sum_{n=1}^{\infty} \frac{e(n)}{n^s} = \frac{1}{1^s} + \sum_{n=2}^{\infty} \frac{0}{n^s} = 1\,,$$

tehát

$$M(s) = \frac{1}{\zeta(s)}\,, \qquad \text{azaz} \qquad \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\sum_{n=1}^{\infty} \frac{1}{n^s}}\,. \tag{6}$$

Speciálisan $s = 2$-re ebből azt kapjuk, hogy

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}\,. \tag{7}$$

Feladatok

6.6.1 Melyik (ismert) függvényt kapjuk, ha az $f = 1$ függvénynek a konvolúció szerinti k-adik hatványát (azaz a k-tényezős $1 * 1 * \ldots * 1$ konvolúciót) képezzük?

6.6.2 Bizonyítsuk be, hogy a számelméleti függvények az összeadás és a konvolúció műveletére kommutatív, nullosztómentes, egységelemes gyűrűt alkotnak.

6.6.3 Legyen f olyan (komplex értékű) számelméleti függvény, amelyre $f(1) \neq 0$. Hány k-adik gyöke van f-nek a konvolúcióra nézve?

6.6.4

a) Bizonyítsuk be, hogy két multiplikatív függvény konvolúciója is multiplikatív.

b) Legyen f és g teljesen multiplikatív. Mutassuk meg, hogy $f * g$ akkor és csak akkor teljesen multiplikatív, ha minden $n > 1$-re $(fg)(n) = 0$.

6.6.5 Igazoljuk, hogy

$$\sum_{d|n} \sigma(d)\varphi(\frac{n}{d}) = nd(n)\,.$$

6.6.6 Bizonyítsuk be, hogy ha a

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

végtelen sor $s = s_0$-ra konvergens, akkor minden $s > s_0 + 1$ esetén abszolút konvergens.

6.6.7 Jelölje az f, f^+, illetve $\tilde{f}$ számelméleti függvényekhez tartozó Dirichlet-sorokat rendre $F(s), F^+(s)$, illetve $\tilde{F}(s)$. Bizonyítsuk be, hogy abszolút konvergencia és $s > 1$ esetén

$$F^+(s) = f(s)\zeta(s) \qquad \text{és} \qquad \tilde{F}(s) = \frac{F(s)}{\zeta(s)}\,.$$

6.6.8 Bizonyítsuk be, hogy $s > 1$ esetén

a) $\displaystyle\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta^2(s)\,;$ b) $\displaystyle\sum_{n=1}^{\infty} \frac{d_k(n)}{n^s} = \zeta^k(s)\,.$

6.6.9 Bizonyítsuk be, hogy $s > 2$ esetén

$$\text{a)}\ \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} = \zeta(s)\zeta(s-1)\,; \qquad \text{b)}\ \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}\,.$$

6.6.10 Ebben a feladatban a ζ-függvényre adott szorzat-előállítást általánosítjuk multiplikatív, illetve teljesen multiplikatív függvényekre. A prímek szerint vett végtelen szorzatokat az 5.6.6 feladatban (illetve az ebben a pontban az (5) képletben) látott módon értelmezzük, és feltesszük, hogy valamennyi végtelen sor abszolút konvergens.

a) Bizonyítsuk be, hogy ha f multiplikatív, akkor

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \Big(\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}\Big)\,.$$

b) Mutassuk meg, hogy ha $f \neq 0$, f teljesen multiplikatív és bármely p prímre $|f(p)| < p^s$, akkor

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - \frac{f(p)}{p^s}}\,.$$

6.6.11 Bizonyítsuk be, hogy $s > 1$ esetén

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p \Big(1 - \frac{1}{p^s}\Big)\,.$$

M 6.6.12 Számítsuk ki az alábbi végtelen sorok összegét:

$$\text{a)}\ \sum_{n=1}^{\infty} \frac{d(n)}{n^2}\,; \qquad {}^{**}\text{b)}\ \sum_{n=1}^{\infty} \Big(\frac{d(n)}{n}\Big)^2\,.$$

*6.6.13 Határozzuk meg a négyzetmentes számok reciprokainak négyzetösszegét.

6.6.14

a) Bizonyítsuk be, hogy ha $|x| < 1$ és a

$$\sum_{n=1}^{\infty} \frac{f(n)x^n}{1-x^n} = \sum_{k=1}^{\infty} f^+(k)x^k$$

egyenlőség két oldalán szereplő végtelen sorok abszolút konvergensek, akkor az egyenlőség teljesül.

b) Számítsuk ki az alábbi végtelen sorok összegét:

$$\text{(b1)}\ \sum_{n=1}^{\infty}\frac{\mu(n)}{2^n-1}\,; \qquad \text{(b2)}\ \sum_{n=1}^{\infty}\frac{\varphi(n)}{2^n-1}\,.$$

6.7. Átlagérték

A 6.4 pontban bebizonyítottuk, hogy noha a $d(n)$ függvény értékei igen erős ingadozást mutatnak, az első n helyen felvett függvényértékek átlaga már kiegyenlítetten viselkedik. Ebben a pontban más nevezetes függvények, a σ, φ és ω átlagértékfüggvényeit fogjuk vizsgálni.

6.7.1 Definíció **D 6.7.1**

Legyen f számelméleti függvény és $F(n)=f(1)+f(2)+\ldots+f(n)$. Az f függvény *átlagérték*függvényén vagy *középérték*függvényén az

$$\frac{F(n)}{n}=\frac{f(1)+f(2)+\ldots+f(n)}{n}$$

függvényt értjük. ♣

Az átlagértékfüggvény kiszámításánál többször szükségünk lesz az alábbi tételre:

6.7.2 Tétel **T 6.7.2**

Ha $f=g*h$, akkor

$$F(n)=\sum_{i=1}^{n}f(i)=\sum_{j=1}^{n}g(j)\Big(\sum_{k=1}^{\lfloor n/j\rfloor}h(k)\Big)\,. \ \clubsuit \tag{1}$$

Bizonyítás: A konvolúció definíciója alapján

$$\sum_{i=1}^{n}f(i)=\sum_{i=1}^{n}\sum_{jk=i}g(j)h(k)=\sum_{j=1}^{n}g(j)\Big(\sum_{k=1}^{\lfloor n/j\rfloor}h(k)\Big)\,. \ \blacksquare$$

A 6.7.2 Tétel legegyszerűbb speciális esete, ha $f = g^+ = g * 1$. Ekkor

$$\sum_{i=1}^{n} f(i) = \sum_{j=1}^{n} g(j)\Big(\sum_{k=1}^{\lfloor n/j \rfloor} 1\Big) = \sum_{j=1}^{n} g(j)\Big\lfloor \frac{n}{j} \Big\rfloor . \tag{2}$$

Az $f(n) = d(n)$ esetben $g = 1$, és így (2) a

$$D(n) = \sum_{j=1}^{n} \Big\lfloor \frac{n}{j} \Big\rfloor$$

alakot ölti, ami megegyezik a 6.4.3 Tétel bizonyításában szereplő (11) egyenlőséggel.

Elsőként a σ átlagértékfüggvényével foglalkozunk.

6.7.3 Tétel **T 6.7.3**

Legyen $\Sigma(n) = \sigma(1) + \sigma(2) + \ldots + \sigma(n)$. Ekkor

$$\Sigma(n) \sim \frac{\pi^2}{12} n^2 , \tag{3}$$

ahol $\sim$ az aszimptotikus egyenlőséget jelöli.

A (3) összefüggés két másik ekvivalens alakja

$$\frac{\Sigma(n)}{n} \sim \frac{\pi^2}{12} n , \tag{4}$$

illetve

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) \sim \frac{\pi^2}{6} \cdot 1 + \frac{\pi^2}{6} \cdot 2 + \ldots + \frac{\pi^2}{6} n \,. \ \clubsuit \tag{5}$$

(4) azt jelenti, hogy a σ középértékfüggvénye jól közelíthető az $n\pi^2/12$ függvénnyel, (5)-öt pedig úgy értelmezhetjük, hogy a σ *átlagos nagyságrend*je $n\pi^2/6$.

Bizonyítás: Próbálkozzunk először a $d(n)$-nél használt módszer értelemszerű módosításával. Mint az imént láttuk, ez tulajdonképpen a 6.7.2 Tétel következményeként kapott (2) egyenlőség alkalmazását jelenti. Ennek megfelelően a $v(n) = n$ jelöléssel $\sigma = v^+ = v * 1$, és így

$$\Sigma(n) = \sum_{i=1}^{n} \sigma(i) = \sum_{j=1}^{n} j \Big\lfloor \frac{n}{j} \Big\rfloor . \tag{6}$$

(6) jobb oldalát a szokásos módon $a-1<\lfloor a\rfloor\le a$ felhasználásával becsülve

$$n^2-\frac{n(n+1)}{2}<\Sigma(n)\le n^2$$

adódik, amiből nem kapunk aszimptotikát $\Sigma(n)$-re.

Ezen úgy segíthetünk, ha a 6.7.2 Tételt a $\sigma=1*v$ konvolúcióra, azaz $g=1$ és $h=v$ szereposztással alkalmazzuk (ahol $v(n)=n$):

$$\Sigma(n)=\sum_{j=1}^{n}\sum_{k=1}^{\lfloor n/j\rfloor}k=\sum_{j=1}^{n}\frac{\lfloor\frac{n}{j}\rfloor(\lfloor\frac{n}{j}\rfloor+1)}{2}\,. \tag{7}$$

(7) jobb oldalának becsléséhez használjuk fel, hogy $a>0$ esetén

$$a^2-a=(a-1)a<\lfloor a\rfloor(\lfloor a\rfloor+1)\le a(a+1)=a^2+a\,,$$

és így

$$\bigl|\lfloor a\rfloor(\lfloor a\rfloor+1)-a^2\bigr|\le a\,. \tag{8}$$

(8)-at $a=n/j$-re alkalmazva (7)-ből azt kapjuk, hogy

$$\Bigl|\Sigma(n)-\sum_{j=1}^{n}\frac{n^2}{2j^2}\Bigr|\le\sum_{j=1}^{n}\frac{n}{2j}\le\frac{n(1+\log n)}{2}\,,$$

azaz $n\ge 3$-ra

$$\Sigma(n)=\frac{n^2}{2}\sum_{j=1}^{n}\frac{1}{j^2}+U(n),\quad\text{ahol}\quad|U(n)|<n\log n\,. \tag{9}$$

(9)-et n^2-tel osztva

$$\frac{\Sigma(n)}{n^2}=\frac12\sum_{j=1}^{n}\frac{1}{j^2}+\frac{U(n)}{n^2} \tag{10}$$

adódik. Ha $n\to\infty$, akkor (10) jobb oldalán az első tag határértéke

$$\frac12\sum_{j=1}^{\infty}\frac{1}{j^2}=\frac{\pi^2}{12}\,,$$

a második tag pedig 0-hoz tart, vagyis

$$\lim_{n\to\infty}\frac{\Sigma(n)}{n^2}=\frac{\pi^2}{12}\,.$$

Ez ekvivalens a bizonyítandó (3) állítással. ■

Hasonló módszerekkel kezelhető a φ középértékfüggvénye is:

6.7.4 Tétel **T 6.7.4**

Legyen $\Phi(n) = \varphi(1) + \varphi(2) + \ldots + \varphi(n)$. Ekkor

$$\Phi(n) \sim \frac{3}{\pi^2} n^2 \,, \tag{11}$$

ahol $\sim$ az aszimptotikus egyenlőséget jelöli.

A (11) összefüggés két másik ekvivalens alakja

$$\frac{\Phi(n)}{n} \sim \frac{3}{\pi^2} n \,, \tag{12}$$

illetve

$$\varphi(1) + \varphi(2) + \ldots + \varphi(n) \sim \frac{6}{\pi^2} \cdot 1 + \frac{6}{\pi^2} \cdot 2 + \ldots + \frac{6}{\pi^2} n \,. \ \clubsuit \tag{13}$$

(12) azt jelenti, hogy a φ középértékfüggvénye jól közelíthető az $3n/\pi^2$ függvénnyel, (13)-at pedig úgy értelmezhetjük, hogy a φ átlagos nagyságrendje $6n/\pi^2$.

Bizonyítás: A 6.7.2 Tételt most a $\varphi = \mu * v$ konvolúcióra, azaz $g = \mu$ és $h = v$ szereposztással alkalmazzuk (ahol $v(n) = n$):

$$\Phi(n) = \sum_{j=1}^{n} \mu(j) \sum_{k=1}^{\lfloor n/j \rfloor} k = \sum_{j=1}^{n} \mu(j) \frac{\lfloor \frac{n}{j} \rfloor (\lfloor \frac{n}{j} \rfloor + 1)}{2} \,. \tag{14}$$

A további lépések teljesen a 6.7.3 Tétel bizonyításának mintájára végezhetők (a hibatag becslésénél $|\mu(j)| \leq 1$-et kell felhasználnunk). Végül a (10)-nek megfelelő

$$\frac{\Phi(n)}{n^2} = \frac{1}{2} \sum_{j=1}^{n} \frac{\mu(j)}{j^2} + \frac{U(n)}{n^2} \tag{15))}$$

becsléshez jutunk. Ha $n \to \infty$, akkor (15) jobb oldalán a második tag 0-hoz tart, az első tag határértéke pedig

$$\frac{1}{2} \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} \,.$$

Mivel a 6.6.4 Tétel utáni (7) képlet szerint

$$\sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} = \frac{6}{\pi^2} ,$$

ezért

$$\lim_{n\to\infty} \frac{\Phi(n)}{n^2} = \frac{3}{\pi^2} . \blacksquare$$

A 6.7.4 Tétel alapján egyúttal arra is választ kaphatunk, mennyi annak a valószínűsége, hogy két szám relatív prím. Más megfogalmazásban ez azt jelenti, hogy milyen valószínűséggel látszik egy P rácspont az origóból (hiszen pontosan akkor nem esik az origót P-vel összekötő szakasz belsejébe további rácspont, ha P koordinátái relatív prímek).

Először a fenti valószínűség pontos értelmezésére van szükség. Megvizsgáljuk, hogy mennyi a relatív prímek aránya azon rendezett számpárok között, amelyek mindkét eleme pozitív és $\leq n$, majd vesszük ennek az aránynak a határértékét, ha $n \to \infty$:

$$\lim_{n\to\infty} \frac{H(n)}{n^2} , \quad \text{ahol} \quad H(n) = \sum_{\substack{1\leq a\leq n, 1\leq b\leq n \\ (a,b)=1}} 1 . \tag{16}$$

Meg fogjuk mutatni, hogy ez a határérték valóban létezik, és ezt a határértéket nevezzük a szóban forgó valószínűségnek.

A rácspontos megfogalmazásban ez a következőket jelenti: az első síknegyedben vesszük azt az n oldalhosszúságú Q_n négyzetet, amelynek egyik csúcsa az origó és két oldala a koordinátatengelyekre esik, és megvizsgáljuk, hogy Q_n rácspontjai között (a tengelyeken levő pontokat nem számítva) mennyi az origóból láthatók aránya, majd a Q_n négyzet oldalhosszával a végtelenhez tartva tekintjük ennek az aránynak a határértékét.

6.7.5 Tétel **T 6.7.5**

Két szám relatív prímségének a valószínűsége (a (16)-beli értelemben) $6/\pi^2$. ♣

A tétel állításának természetesen az is része, hogy ez a valószínűség, vagyis a (16)-beli határérték egyáltalán létezik.

Mint jeleztük, ez a valószínűség szoros kapcsolatban van a φ átlagértékfüggvényével. Ennek alapján a 6.7.5 Tétel azonnal következni fog a 6.7.4

Tételből. A 6.7.5 Tételre egy másik bizonyítást is adunk a logikai szitaformula segítségével (és ebből tulajdonképpen a 6.7.4 Tételre is egy újabb bizonyítást nyerünk).

Első bizonyítás: Megmutatjuk, hogy

$$\Phi(n) = \sum_{i=1}^{n} \varphi(i) \qquad \text{és} \qquad H(n) = \sum_{\substack{1 \le a \le n, 1 \le b \le n \\ (a,b)=1}} 1$$

között az alábbi összefüggés érvényes:

$$H(n) = 2\Phi(n) - 1\,. \tag{17}$$

Ennek igazolásához tekintsük a 6.7.5 Tétel kimondása előtt definiált Q_n négyzetet, és bontsuk ezt az origóból kiinduló átlója segítségével két háromszögre. $H(n)$ éppen azoknak a Q_n-beli rácspontoknak a száma (a tengelyeken levő pontokat nem számítva), amelyekben a két koordináta relatív prím. Ezek a rácspontok az origóból kiinduló átlóra nézve szimmetrikusan helyezkednek el. Az átló alatti háromszögben az i abszcisszájú pontok közül azok a rácspontok felelnek meg, amelyek t ordinátájára $1 \le t \le i$ és $(i,t) = 1$ teljesül. Az ilyen rácspontok száma $\varphi(i)$, és így az alsó háromszögben a keresett rácspontok száma

$$\sum_{i=1}^{n} \varphi(i) = \Phi(n)\,.$$

A szimmetria miatt ugyanennyi rácspont teljesíti a feltételt a felső háromszögben is. Ekkor kétszer számoltuk az átlón levő rácspontokat, magán az átlón azonban csak egyetlen ilyen rácspont, az $(1,1)$ található. Ennek megfelelően az origóból látható rácspontok száma valóban $2\Phi(n) - 1$.

A (17) egyenlőségből a 6.7.4 Tétel alapján kapjuk, hogy

$$\lim_{n\to\infty} \frac{H(n)}{n^2} = 2 \lim_{n\to\infty} \frac{\Phi(n)}{n^2} = \frac{6}{\pi^2}\,. \quad \blacksquare$$

Második bizonyítás: $H(n)$-et a logikai szitaformula segítségével fogjuk meghatározni.

Az $\{(a,b) \mid 1 \le a \le n,\ 1 \le b \le n\}$ rendezett számpárok közül azoknak a számát kell megadni, amelyekre a és b relatív prím.

Ehhez „ki kell szitálni a rossz tulajdonságúakat”, vagyis azokat, amelyekre a-nak és b-nek van (egy vagy több) közös prímosztója.

Tekintsük először azokat a számpárokat, amelyek mindkét koordinátája osztható egy adott p prímmel (függetlenül attól, hogy van-e további közös prímosztójuk vagy sem). Ezeknek a számpároknak a száma nyilván $\lfloor n/p \rfloor^2$.

Most nézzük azokat a számpárokat, amelyek koordinátái több, előre megadott p_j prímmel oszthatók (ismét nem törődve azzal, oszthatók-e további prímekkel vagy sem). Egy egész akkor és csak akkor osztható adott prímek mindegyikével, ha osztható ezen prímek szorzatával. Ennélfogva például

$$\Big\lfloor \frac{n}{p_1 p_2} \Big\rfloor^2$$

azoknak a számpároknak a száma, amelyek mindkét koordinátája osztható p_1-gyel és p_2-vel is, ahol $p_1 < p_2$ különböző prímek stb.

Így a logikai szitaformula szerint

$$H(n) = n^2 - \sum_{p \le n} \Big\lfloor \frac{n}{p} \Big\rfloor^2 + \sum_{p_1 p_2 \le n} \Big\lfloor \frac{n}{p_1 p_2} \Big\rfloor^2 \mp \dots \tag{18}$$

Vegyük észre, hogy (18) jobb oldalán éppen a

$$\mu(j) \Big\lfloor \frac{n}{j} \Big\rfloor^2, \qquad j = 1, 2, \dots, n$$

alakú tagok összege áll, azaz

$$H(n) = \sum_{j=1}^{n} \mu(j) \Big\lfloor \frac{n}{j} \Big\rfloor^2 . \tag{19}$$

(19) jobb oldalának becsléséhez használjuk fel, hogy $a > 0$ esetén

$$0 \le a^2 - \lfloor a \rfloor^2 = (a - \lfloor a \rfloor)(a + \lfloor a \rfloor) < 2a \,,$$

és így

$$\big| \lfloor a \rfloor^2 - a^2 \big| < 2a \,. \tag{20}$$

alkalmazzuk (20)-at $a = n/j$-re, ekkor $|\mu(j)| \le 1$-et is figyelembe véve (19)-ből azt kapjuk, hogy

$$\Big| H(n) - \sum_{j=1}^{n} \mu(j) \big(\frac{n}{j}\big)^2 \Big| < 2 \sum_{j=1}^{n} \frac{n}{j} < 2n(1 + \log n) \,,$$

azaz $n \geq 3$-ra

$$H(n) = n^2 \sum_{j=1}^{n} \frac{\mu(j)}{j^2} + V(n), \quad \text{ahol} \quad |V(n)| < 4n \log n \,. \tag{21}$$

(21)-et n^2-tel osztva a

$$\frac{H(n)}{n^2} = \sum_{j=1}^{n} \frac{\mu(j)}{j^2} + \frac{V(n)}{n^2}$$

becsléshez jutunk, ahonnan a 6.7.4 Tétel bizonyításának végéhez hasonló módon

$$\lim_{n\to\infty} \frac{H(n)}{n^2} = \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} = \frac{6}{\pi^2}$$

adódik. ■

Most rátérünk az ω középértékfüggvényének a vizsgálatára:

6.7.6 Tétel **T 6.7.6**

Az ω középértékfüggvényének a $\log\log n$ függvénytől való eltérése korlátos. Más szóval, ha $z(n) = \omega(1) + \omega(2) + \ldots + \omega(n)$, akkor létezik olyan C konstans, hogy minden $n \geq 3$ egész számra

$$\left| \frac{z(n)}{n} - \log\log n \right| < C \,. \ \clubsuit$$

Bizonyítás: alkalmazzuk a 6.7.2 Tételt az $\omega = \tilde{\omega} * 1$ konvolúcióra (ekkor $g = \tilde{\omega}$ és $h = 1$):

$$z(n) = \sum_{i=1}^{n} \omega(i) = \sum_{j=1}^{n} \tilde{\omega}(j) \left\lfloor \frac{n}{j} \right\rfloor . \tag{22}$$

Könnyen ellenőrizhető (lásd például a 6.5.5d feladatot), hogy

$$\tilde{\omega}(j) = \begin{cases} 1, & \text{ha } j \text{ prím;} \\ 0, & \text{egyébként.} \end{cases} \tag{23}$$

A (23)-at (22)-be beírva

$$z(n) = \sum_{p \leq n} \left\lfloor \frac{n}{p} \right\rfloor \tag{24}$$

adódik. Az

$$a - 1 < \lfloor a \rfloor \leq a$$

egyenlőtlenséget $a = n/p$-re felhasználva (24)-ből a szokásos módon azt kapjuk, hogy

$$z(n) = n \sum_{p \leq n} \frac{1}{p} + W(n), \quad \text{ahol} \quad |W(n)| \leq \pi(n) < n\,,$$

azaz

$$\Big| \frac{z(n)}{n} - \sum_{p \leq n} \frac{1}{p} \Big| < 1\,. \tag{25}$$

Mivel az 5.6.2 Tétel szerint ($n \geq 3$-ra)

$$\sum_{p \leq n} \frac{1}{p} - \log\log n$$

korlátos, ezért (25)-ből következik az állítás. ■

Könnyen igazolható, hogy

$$\sum_{i=2}^{n} \log\log i \sim n \log\log n\,,$$

ezért a 6.7.6 Tételből az is következik, hogy

$$\omega(2) + \ldots + \omega(n) \sim \log\log 2 + \log\log 3 + \ldots + \log\log n\,. \tag{26}$$

A (26) összefüggést úgy értelmezhetjük, hogy az ω átlagos nagyságrendje is $\log\log n$.

Általában nem igaz, hogy egy számelméleti függvény a legtöbbször a középértéke vagy az átlagos nagyságrendje körüli értékeket vesz fel. Legyen például

$$f(n) = \begin{cases} n, & \text{ha } n \text{ négyzetszám;} \\ 0, & \text{egyébként.} \end{cases}$$

Ekkor

$$F(n) = \sum_{i=1}^{n} f(i) = \sum_{k \leq \sqrt{n}} k^2 \sim \frac{n^{3/2}}{3}\,,$$

ahonnan azt kapjuk, hogy f középértékfüggvénye

$$\frac{F(n)}{n} \sim \frac{\sqrt{n}}{3}\,,$$

és az is könnyen adódik, hogy $f(n)$ átlagos nagyságrendje $\sqrt{n}/2$. Ugyanakkor $f(n)$ értéke majdnem minden n-re 0.

Hardy és Ramanujan nevezetes tétele azt mondja ki, hogy az ω függvény a legtöbbször a középértékfüggvényéhez közeli értéket vesz fel, azaz a legtöbb n-re az n számnak körülbelül $\log\log n$ különböző prímosztója van. A tételre Turán Pál bizonyítását közöljük, amely kiindulópontja lett a valószínűségszámítás számelméleti alkalmazásainak.

6.7.7 Tétel (Hardy–Ramanujan-tétel) **T 6.7.7**

Legyen $\delta > 1/2$ tetszőleges rögzített valós szám, $n \geq 3$, és jelöljük $k(n)$-nel azoknak az i egészeknek a számát, amelyekre $3 \leq i \leq n$ és

$$|\omega(i) - \log\log i| < (\log\log i)^{\delta}\,. \tag{27}$$

Ekkor

$$\lim_{n\to\infty} \frac{k(n)}{n} = 1\,. \ \clubsuit$$

Mivel ($\delta < 1$-re)

$$\lim_{i\to\infty} \frac{(\log\log i)^{\delta}}{\log\log i} = 0\,,$$

ezért a 6.7.7 Tételből következik, hogy egy „ritka” részsorozattól eltekintve

$$\omega(i) \sim \log\log i\,.$$

A 6.7.7 Tételt az alábbi véges változatából fogjuk levezetni:

6.7.7A Tétel **T 6.7.7A**

Bármely $\varepsilon > 0$-hoz létezik olyan (az ε-tól függő) T, hogy tetszőleges $n \geq 3$ esetén az $1, 2, \ldots, n$ számok között legalább $(1-\varepsilon)n$ darab olyan i található, amelyre

$$|\omega(i) - \log\log n| < T\sqrt{\log\log n}\,. \ \clubsuit \tag{28}$$

Felhívjuk a figyelmet arra az eltérésre, hogy a $\log\log$ függvénynek (27)-ben az i helyen, (28)-ban pedig az n helyen felvett helyettesítési értéke szerepel.

Mivel azonban a log log függvény igen lassan változik, ezért a legtöbb i-re ez alig jelent különbséget (lásd majd a (41) képletet).

Először a 6.7.7A Tételt bizonyítjuk, és utána megmutatjuk, hogyan következik ebből a 6.7.7 Tétel.

A 6.7.7A Tétel bizonyítása: A bizonyítás alapgondolata a következő: belátjuk, hogy az

$$U = \sum_{i=1}^{n} \big(\omega(i) - \log\log n\big)^2 \tag{29}$$

négyzetösszeg „viszonylag kicsi", és így a tagok nemnegativitása miatt csak kevés i-re lehet $|\omega(i) - \log\log n|$ „nagy".

Nézzük mindezt részletesen. Megmutatjuk, hogy alkalmas c konstanssal bármely $n \geq 3$-ra fennáll

$$U = \sum_{i=1}^{n} \big(\omega(i) - \log\log n\big)^2 < cn \log\log n\,. \tag{30}$$

Ehhez fel fogjuk használni, hogy a 6.7.6 Tétel szerint ($n \geq 3$-ra)

$$z(n) = \sum_{i=1}^{n} \omega(i) = n\log\log n + nA(n), \qquad \text{ahol } A(n) \text{ korlátos,} \tag{31}$$

továbbá az 5.6.2 Tétel szerint ($n \geq 3$-ra)

$$\sum_{p \leq n} \frac{1}{p} = \log\log n + B(n), \qquad \text{ahol } B(n) \text{ korlátos.} \tag{32}$$

Végezzük el (29)-ben a négyzetre emeléseket:

$$U = \sum_{i=1}^{n} \omega^2(i) - 2\log\log n \sum_{i=1}^{n} \omega(i) + n(\log\log n)^2\,.$$

Innen (31) alapján azt nyerjük, hogy

$$\begin{aligned} U &= \sum_{i=1}^{n} \omega^2(i) - 2\log\log n\big(n\log\log n + nA(n)\big) + n(\log\log n)^2 = \\ &= \sum_{i=1}^{n} \omega^2(i) - n(\log\log n)^2 - 2nA(n)\log\log n\,. \end{aligned} \tag{33}$$

Az U felső becsléséhez így a

$$V = \sum_{i=1}^{n} \omega^2(i) \tag{34}$$

összeget kell felülről becsülnünk.

Az $\omega(i)$ definícióját (részben) beírva a szokásos összegátrendezés után

$$V = \sum_{i=1}^{n} \omega^2(i) = \sum_{i=1}^{n} \omega(i) \sum_{p|i} 1 = \sum_{p\le n} \sum_{k=1}^{\lfloor n/p \rfloor} \omega(pk) \tag{35}$$

adódik. Mivel

$$\omega(pk) = \begin{cases} \omega(k), & \text{ha } p \mid k; \\ 1+\omega(k), & \text{ha } p \nmid k, \end{cases}$$

ezért (35)-ből azt kapjuk, hogy

$$V \le \sum_{p\le n} \sum_{k=1}^{\lfloor n/p \rfloor} \big(1+\omega(k)\big) = \sum_{p\le n} \Big\lfloor \frac{n}{p} \Big\rfloor + \sum_{p\le n} \sum_{k=1}^{\lfloor n/p \rfloor} \omega(k)\,. \tag{36}$$

Jelöljük a (36) jobb oldalán szereplő első összeget K-val, a második, kettős összeget pedig L-lel.

Ekkor K-ra (32) alapján a következő felső becslést nyerjük:

$$K = \sum_{p\le n} \Big\lfloor \frac{n}{p} \Big\rfloor \le n \sum_{p\le n} \frac{1}{p} = n\big(\log\log n + B(n)\big)\,. \tag{37}$$

Az L felső becsléséhez beírjuk $\omega(k)$ definícióját és a szokásos összegátrendezést alkalmazzuk (itt p' is azt jelzi, hogy az összegzés prímekre történik), majd felhasználjuk (32)-t:

$$\begin{aligned} L = \sum_{p\le n} \sum_{k=1}^{\lfloor n/p \rfloor} \omega(k) = \sum_{p\le n} \sum_{k=1}^{\lfloor n/p \rfloor} \sum_{p'|k} 1 = \sum_{p\le n} \sum_{p'\le n/p} \Big\lfloor \frac{n}{pp'} \Big\rfloor \le \\ \le n \sum_{pp'\le n} \frac{1}{pp'} \le n\Big(\sum_{p\le n} \frac{1}{p}\Big)\Big(\sum_{p'\le n} \frac{1}{p'}\Big) = n\big(\log\log n + B(n)\big)^2\,. \end{aligned} \tag{38}$$

A (37) és (38) becsléseket (36)-ba beírva azt kapjuk, hogy

$$V \le n\big(\log\log n + B(n)\big) + n\big(\log\log n + B(n)\big)^2\,. \tag{39}$$

Végül, ha a $V = \sum_{i=1}^{n} \omega(i)^2$-re ily módon nyert (39) becslést (33)-ba behelyettesítjük, akkor az $n(\log\log n)^2$ tagok kiejtik egymást, és

$$U \le \big(1 + 2B(n) - 2A(n)\big)n \log\log n + \big(B(n) + B^2(n)\big)n < cn \log\log n$$

adódik, amivel (30)-at bebizonyítottuk.

Most már csak a bizonyítás elején jelzett gondolatmenetnek azt a részét kell pontosítani, hogy ha a (29) négyzetösszeg „kicsi", akkor ebben csak kevés „nagy" tag szerepelhet.

Jelöljük s-sel a (28)-at nem teljesítő (azaz „rossz") $1 \le i \le n$ számoknak a számát. A tétel állítását kicsit átfogalmazva, azt kell belátnunk, hogy bármely $\varepsilon > 0$-hoz található olyan T, amelyre $s < \varepsilon n$ teljesül.

Csökkentsük (30) bal oldalát úgy, hogy írjunk $\big(\omega(i) - \log\log n\big)^2$ helyére ennél az s darab „rossz" i-nél $T^2 \log\log n$-et, a többi i-nél pedig 0-t. Ekkor (30) alapján azt kapjuk, hogy

$$sT^2 \log\log n < cn \log\log n, \quad \text{azaz} \quad s < \frac{c}{T^2} n\,.$$

Ha most T értékét a

$$\frac{c}{T^2} < \varepsilon \tag{40}$$

feltételnek megfelelően választjuk, akkor éppen a kívánt $s < \varepsilon n$ becslés adódik. ■

A 6.7.7 Tétel bizonyítása: Azt kell igazolni, hogy bármely $\varepsilon > 0$-hoz létezik olyan (az ε-tól függő) n_0, hogy minden $n > n_0$ esetén a $3, 4, \dots, n$ számok között legfeljebb εn darab olyan i található, amelyre (27) nem teljesül.

Amint korábban is jeleztük, a már bizonyított 6.7.7A Tétel esetén a (28) képletben $\log\log n$ szerepel, míg a bizonyítandó 6.7.7 Tétel esetén a (27) képletben $\log\log i$-ről van szó. A bizonyításhoz tulajdonképpen ezt az eltérést kell áthidalni.

A bizonyítás lényege az alábbi észrevétel: a log log függvény olyan lassan változik, hogy $\sqrt{n}$ és n között „majdnem" konstansnak tekinthető, a $\sqrt{n}$-nél kisebb i értékek pedig olyan kevesen vannak, hogy az belefér a megengedett kivételek halmazába.

Nézzük mindezt részletesen. alkalmazzuk a 6.7.7A Tételt ε helyett $\varepsilon/2$-re. Ekkor a $\sqrt{n}$ és n közé eső számok között legfeljebb $\varepsilon n/2$ olyan i van, amelyre (28) *nem* teljesül. Mivel $\sqrt{n} \le i \le n$ esetén

$$\log\log n - \log 2 = \log\log\sqrt{n} \le \log\log i \le \log\log n\,, \tag{41}$$

ezért az előbbi kijelentés akkor is igaz marad, ha (28)-ban a $\log\log n$ helyett mindkétszer $\log\log i$ szerepel, ehhez csak T értékét kell (a (40)-ben előírtnál) megfelelően nagyobbra választani. Ha n elég nagy, akkor a $\sqrt{n}$-nél kisebb i értékek száma kevesebb, mint $\varepsilon n/2$, vagyis azt kaptuk, hogy alkalmas T és elég nagy n esetén a $3, 4, \ldots, n$ számok között legalább $(1-\varepsilon)n$ darab olyan i található, amelyre

$$|\omega(i) - \log\log i| < T\sqrt{\log\log i}\,. \tag{42}$$

Mivel $\delta > 1/2$, ezért minden, a T-től és δ-tól függően elég nagy i-re

$$T\sqrt{\log\log i} < (\log\log i)^{\delta}\,,$$

és így (42)-ből következik a 6.7.7 Tétel állítása. ■

Megjegyzés: A 6.7.7A Tétel bizonyításának a valószínűségszámítási tartalma a következő. Legyen n rögzített, és tekintsük az ω-t valószínűségi változónak, amely egyforma, azaz $1/n$ valószínűséggel veszi fel az $\omega(1), \omega(2), \ldots, \omega(n)$ értékeket. Ennek a valószínűségi változónak az E várható értéke definíció szerint az ω középértékfüggvényének az n helyen felvett értéke, ami körülbelül $\log\log n$. A (29)-ben megadott U pedig körülbelül nD^2, ahol D az ω szórása. A 6.7.7A Tétel állítása ezután a D-re adott felső becslésből (lásd (30)) és a

$$P(|\omega - E| > rD) < \frac{1}{r^2} \tag{43}$$

Csebisev-egyenlőtlenségből következett (ahol P az esemény valószínűségét jelöli).

A 6.7.6, 6.7.7 és 6.7.7A Tételek az ω helyett a Ω függvényre is igazak, lásd a 6.7.5b feladatot. Ezekből a

$$2^{\omega(n)} \le d(n) \le 2^{\Omega(n)}$$

egyenlőtlenség segítségével igazolható az a 6.4 pontban már jelzett érdekesség is, hogy a legtöbb n esetén a $d(n)$ függvény értéke „körülbelül”

$$(\log n)^{\log 2} = (\log n)^{0{,}69\ldots}\,,$$

ami lényegesen kisebb, mint a $d(n)$ középértékének megfelelő $\log n$-es nagyságrend (lásd a 6.7.6 feladatot).

Feladatok

6.7.1 Számítsuk ki a

$$\sum_{j=1}^{n} \mu(j) \left\lfloor \frac{n}{j} \right\rfloor$$

összeget.

6.7.2 Mi a valószínűsége annak, hogy egy pozitív egész szám négyzetmentes legyen?

*6.7.3 Bizonyítsuk be az alábbi aszimptotikus egyenlőségeket a $d_3(n)$ függvény, illetve rögzített $\nu > 0$ esetén a 6.2.23 feladatban definiált $\sigma_\nu(n)$ függvény középértékfüggvényére:

$$\text{a)} \quad \frac{D_3(n)}{n} = \frac{d_3(1) + d_3(2) + \ldots + d_3(n)}{n} \sim \frac{\log^2(n)}{2} \,;$$

$$\text{b)} \quad \frac{\Sigma_\nu(n)}{n} = \frac{\sigma_\nu(1) + \sigma_\nu(2) + \ldots + \sigma_\nu(n)}{n} \sim \frac{n^\nu \zeta(\nu+1)}{\nu+1} \,.$$

M*6.7.4 Igazoljuk, hogy bármely k esetén léteznek olyan $n_1, \ldots, n_k$ különböző egész számok, amelyekre $\sigma(n_1) = \ldots = \sigma(n_k)$.

6.7.5

a) Bizonyítsuk be, hogy

$$0 \le \sum_{i=1}^{n} \big(\Omega(i) - \omega(i)\big) < n \,.$$

b) Mutassuk meg, hogy a 6.7.6, 6.7.7 és 6.7.7A Tételek állításai az ω helyett a Ω függvényre is igazak.

6.7.6 Mutassuk meg, hogy a legtöbb n-re az n számnak körülbelül

$$(\log n)^{\log 2}$$

osztója van a következő értelemben. Legyen $\varepsilon > 0$ tetszőleges, és jelöljük $k(n)$-nel azoknak az $1 \le i \le n$ számoknak a számát, amelyekre

$$(\log n)^{\log 2 - \varepsilon} < d(i) < (\log n)^{\log 2 + \varepsilon} \,.$$

Ekkor

$$\lim_{n\to\infty} \frac{k(n)}{n} = 1 \,.$$

*6.7.7 Jelölje $h(n)$ azoknak az $1 \le i \le n$ számoknak a számát, amelyek felírhatók két $\sqrt{n}$-nél kisebb pozitív egész szorzataként. Számítsuk ki a

$$\lim_{n\to\infty} \frac{h(n)}{n}$$

határértéket.

6.7.8 Fogalmazzuk meg pontosan és bizonyítsuk be a Hardy–Ramanujan-tétel következő általánosítását:

Tegyük fel, hogy az f valós értékű additív függvény rendelkezik az alábbi tulajdonságokkal.

(i) Létezik olyan K, hogy minden p prímre $0 \le f(p) \le K$.

(ii) Minden p prímre és $\alpha > 0$ egészre $f(p^\alpha) = f(p)$.

(iii) A $\sum_p f(p)/p$ végtelen sor divergens.

Ekkor majdnem minden n-re

$$f(n) \sim \sum_{p\le n} \frac{f(p)}{p}\,.$$

6.8. Additív függvények karakterizációja

Láttuk, hogy a legtöbb számelméleti függvényre a függvényértékek ingadozása jellemző. Az alábbi, Erdős Páltól származó tétel azt mutatja, hogy az additív függvények körében ez alól teljes mértékben csak a logaritmusfüggvény jelent kivételt:

6.8.1 Tétel **T 6.8.1**

Legyen f valós értékű additív függvény, és tegyük fel, hogy

(i) $f(n)$ monoton,

vagy

(ii) $f(n+1) - f(n) \to 0$, ha $n \to \infty$.

Ekkor alkalmas c konstanssal $f(n) = c \log n$. ♣

Bizonyítás: Azt a kicsit erősebb eredményt fogjuk igazolni, hogy ha egy f valós értékű additív függvényre a

$$\liminf_{n\to\infty} \big(f(n+1) - f(n)\big) \ge 0 \tag{1}$$

feltétel teljesül, akkor $f(n) = c \log n$.

Ebből a 6.8.1 Tétel valóban következik: ha f a (ii) tulajdonsággal rendelkezik, vagy f monoton növő, akkor f nyilván kielégíti (1)-et, ha pedig f monoton fogyó, akkor f helyett $-f$ teljesíti (1)-et, és így $(-f)(n) = c\log n$, azaz $f(n) = -c\log n$ adódik.

A bizonyítás alapgondolata a következő. Legyen $k > 1$ rögzített egész, és írjunk fel egy tetszőleges n-et k alapú számrendszerben:

$$n = a_s k^s + \ldots + a_2 k^2 + a_1 k + a_0\,, \qquad s = \lfloor \log_k n \rfloor\,. \tag{2}$$

Az n utolsó számjegyét elhagyva és az utolsó előtti számjegyet alkalmasan megváltoztatva, az n-hez „viszonylag közel" találunk egy olyan

$$n' = a_s k^s + \ldots + a_2 k^2 + a_1' k \tag{3}$$

számot, amelyre $(a_1', k) = 1$. Ekkor a feltételek alapján $f(n)$ „nem sokkal tér el" az

$$f(n') = f(k) + f(a_s k^{s-1} + \ldots + a_2 k + a_1') \tag{4}$$

függvényértéktől. Az eljárást a (4) jobb oldalán levő második tagra megismételve stb. végül azt kapjuk, hogy

$$f(n) \sim s f(k) \sim \frac{f(k)\log n}{\log k}\,, \qquad \text{azaz} \qquad \lim_{n\to\infty} \frac{f(n)}{\log n} = \frac{f(k)}{\log k}\,,$$

tehát $f(k)/\log k$ konstans.

Nézzük mindezt pontosan és részletesen. Legyen $\varepsilon > 0$ tetszőleges. Ekkor az (1) feltétel szerint van olyan (az ε-tól függő) n_0, hogy minden $n > n_0$ esetén

$$f(n+1) - f(n) \geq -\varepsilon\,, \quad \text{azaz} \quad f(n) \leq f(n+1) + \varepsilon. \tag{5}$$

(A technikai lépések kényelmesebb leírása érdekében feltesszük, hogy $n_0 > k^2$.)

Ha (5)-ben n helyére rendre az $n+1, n+2, \ldots, n+t-1$ értékeket írjuk, akkor

$$f(n+1) \leq f(n+2)+\varepsilon,\ f(n+2) \leq f(n+3)+\varepsilon,\ \ldots,\ f(n+t-1) \leq f(n+t)+\varepsilon,$$

és így

$$f(n) \leq f(n+1) + \varepsilon \leq f(n+2) + 2\varepsilon \leq \ldots \leq f(n+t) + t\varepsilon \tag{6}$$

adódik.

Legyen n „sokkal nagyobb” n_0-nál, és tekintsük (rögzített $k > 1$ mellett) a (2) előállítást. Válasszuk a (3)-nak megfelelő legkisebb olyan n' számot, amelyre $n' > n$ és $(a_1', k) = 1$. Ez azt jelenti, hogy n utolsó számjegyét elhagyjuk, és az utolsó előtti a_1 számjegy helyett egy nála nagyobb a_1'-t veszünk (esetleg $a_1' = k + 1$ is előfordulhat). Jelöljük az n' és n különbségét t-vel:

$$t = n' - n = (a_1' - a_1)k - a_0\,. \tag{7}$$

Ha $a_1 = 0$, akkor $a_1' = 1$, ha pedig $a_1 \geq 1$, akkor $1 \leq a_1 < a_1' \leq k + 1$, ezért (7) alapján mindenképpen

$$0 < t \leq k^2 \tag{8}$$

teljesül. Rendre a (6), majd a (7) és (8), végül a (4) összefüggéseket alkalmazva, azt kapjuk, hogy $n > n_0$ esetén

$$f(n) \leq f(n+t)+t\varepsilon \leq f(n')+k^2\varepsilon = f(k)+f(a_s k^{s-1}+\ldots+a_2 k+a_1')+k^2\varepsilon\,. \tag{9}$$

Tekintsük most a (9) jobb oldalán szereplő középső tagban előforduló

$$n_1 = a_s k^{s-1} + \ldots + a_2 k + a_1'$$

számot. Ha ebben $a_1' = k + 1$, akkor írjuk át n_1-et a szokásos számrendszeres alakba (ahol tehát minden k-hatvány együtthatója k-nál kisebb; ekkor az utolsó számjegy 1-es lesz, az utolsó előtti 1-gyel nő, illetve ha az $k - 1$ volt, akkor további változások is történhetnek).

Most ismételjük meg az egész eddigi eljárást n helyett n_1-re. Ekkor azt kapjuk, hogy

$$f(a_s k^{s-1} + \ldots + a_2 k + a_1') = f(n_1) \leq f(k) + f(a_s k^{s-2} + \ldots + a_2') + k^2\varepsilon\,,$$

amit (9)-be beírva

$$f(n) \leq 2f(k) + f(a_s k^{s-2} + \ldots + a_2') + 2k^2\varepsilon$$

adódik. Hasonlóan haladhatunk tovább mindaddig, amíg n_0-nál nagyobb helyeken felvett függvényértékek keletkeznek. Végül azt nyerjük, hogy

$$f(n) \leq (s - s_0)f(k) + (s - s_0)k^2\varepsilon + M_0\,, \tag{10}$$

ahol $s - s_0$ a lépések száma és M_0 az n_0-ig terjedő függvényértékek maximuma. Itt M_0 csak ε-tól, s_0 pedig ε-tól és (a rögzített) k-tól függ, ezért (10) átírható az

$$f(n) \leq sf(k) + sk^2\varepsilon + M_1 \tag{11}$$

alakba, ahol M_1 az ε-tól és k-tól függő konstans.

Hasonlóan nyerhetünk alsó becslést is $f(n)$-re. Ehhez n'-t most is az n-hez közel és az $(a_1', k) = 1$ feltételnek megfelelően kell választanunk, azonban most a minimális $n' > n$ helyett a maximális $n' < n$ követelményt írjuk elő (most $a_1' = -1$ is lehet). A felső becslés lépéseit csak annyiban kell módosítani, hogy a t értékét $n - n'$-nek vesszük, és (6) helyett az

$$f(n) \geq f(n-t) - t\varepsilon$$

egyenlőtlenséget alkalmazzuk. Ekkor az előzőkhöz teljesen hasonlóan az adódik, hogy alkalmas M_2-vel

$$f(n) \geq sf(k) - sk^2\varepsilon - M_2 \tag{12}$$

teljesül.

A (11) és (12) egyenlőtlenségekből $s = \lfloor \log_k n \rfloor$-nel történő osztás után azt kapjuk, hogy

$$\left| \frac{f(n)}{\lfloor \log_k n \rfloor} - f(k) \right| \leq k^2\varepsilon + \frac{M}{\lfloor \log_k n \rfloor}\,. \tag{13}$$

Ha $n \to \infty$, akkor (13) jobb oldala $k^2\varepsilon$-hoz tart. Mivel azonban ε tetszőleges volt, ezzel beláttuk, hogy

$$\lim_{n\to\infty} \frac{f(n)}{\lfloor \log_k n \rfloor} = f(k)\,. \tag{14}$$

A (14)-ből nyilván következik, hogy

$$\lim_{n\to\infty} \frac{f(n)}{\log_k n} = f(k)\,,$$

azaz

$$\lim_{n\to\infty} \frac{f(n)}{\log n} = \frac{f(k)}{\log k}\,. \tag{15}$$

Jelöljük a (15)-beli határértéket c-vel; mivel c nem függ a (jobb oldalon szereplő) k-tól, ez éppen azt jelenti, hogy bármely $k > 1$-re

$$\frac{f(k)}{\log k} = c\,,$$

azaz

$$f(k) = c \log k\,. \tag{16}$$

Végül, mivel $f(1) = \log 1 = 0$, ezért (16) teljesül $k = 1$-re is. ■

Feladatok

6.8.1 Bizonyítsuk be, hogy ha egy f komplex értékű teljesen additív függvény korlátos, akkor $f = 0$.

6.8.2 Mutassuk meg, hogy ha egy f komplex értékű additív függvényre az $f(n)$ függvényértékek sorozata konvergens, akkor $f = 0$.

6.8.3 Melyek a valós értékű monoton multiplikatív függvények?

6.8.4 Bizonyítsuk be, hogy ha egy f valós értékű additív függvényre

$$\limsup_{n\to\infty}\bigl(f(n) - f(n-1)\bigr) \le 0\,,$$

akkor $f(n) = c\log n$.

6.8.5 Mutassuk meg, hogy ha egy *komplex* értékű f additív függvényre

$$\lim_{n\to\infty}\bigl(f(n) - f(n-1)\bigr) = 0\,,$$

akkor $f(n) = c\log n$, ahol c alkalmas komplex konstans.

6.8.6 Bizonyítsuk be az alábbi állításokat.

a) Létezik a természetes számoknak akármilyen ritka olyan a_n részsorozata, hogy ha egy f valós értékű additív függvényre $f(a_n)$ monoton, akkor $f(n) = c\log n$.

b) Létezik a természetes számoknak akármilyen ritka olyan a_n részsorozata, hogy ha egy f valós értékű additív függvényre

$$\lim_{n\to\infty}\bigl(f(a_n) - f(a_{n-1})\bigr) = 0\,,$$

akkor $f = 0$.

(Az akármilyen ritka azt jelenti, hogy bármilyen előre megadott b_n sorozathoz található olyan a_n sorozat, amely rendelkezik az előírt tulajdonsággal, és $a_n > b_n$.)

7. DIOFANTIKUS EGYENLETEK

Diofantikus (vagy diofantoszi) egyenletnek általában olyan egész együtthatós algebrai egyenletet nevezünk, melynek a megoldásait is az egész (esetenként a racionális) számok körében keressük. Diophantosz görög matematikus az i.sz. III. században élt Alexandriában, és sokféle ilyen egyenlettel foglalkozott. (Akkoriban teljesen természetes volt, hogy egész, illetve racionális megoldásokat kerestek, hiszen az irracionális számok annak ellenére sem nyertek igazán polgárjogot, hogy a görögök bebizonyították ezek létezését.) A diofantikus egyenletek története egyébként még ennél is sokkal régebbre nyúlik vissza; közel négyezer éves kőtáblák tanúsága szerint már a babiloniaiak is ismerték az ún. pitagoraszi számhármasok előállítási módját.

A diofantikus egyenletek megoldása igen változatos módszereket igényel, univerzális megoldási módszer nem létezik (sőt, mint az 5.1 pontban már említettük, annak az egyszerűbb kérdésnek a megválaszolására sem létezik általános algoritmus, hogy egy tetszőlegesen adott diofantikus egyenletnek egyáltalán van-e megoldása vagy sem). Egy-egy konkrét egyenlet esetén is gyakran igen nehéz eldönteni a megoldhatóságot, a megoldásszámról, illetve az összes megoldás meghatározásáról nem is beszélve. Ez a témakör is bővelkedik híres megoldatlan problémákban.

A már az 1. fejezetben is szerepelt lineáris diofantikus egyenletek részletes tárgyalása után a pitagoraszi számhármasokkal foglalkozunk, majd néhány jól használható elemi módszert mutatunk be diofantikus egyenletek megoldására. A továbbiakban olyan diofantikus problémák következnek, amelyek kezeléséhez látszólag egészen más jellegű matematikai eszközöket érdemes bevetni: a két négyzetszám összegéből történő előállíthatósághoz a Gauss-egészeket, a Fermat-sejtés köbszámokra vonatkozó speciális eseténél az Euler-egészeket és a Pell-egyenletnél a diofantikus approximációt. Ezeknek a „segédeszközöknek” a kialakulását és önálló elméletté terebélyesedését éppen a diofantikus egyenleteknél való alkalmazhatóságuk segítette elő. Az ezekből kifejlődött területeknek a részletes bemutatására a 8–11. fejezetekben kerül majd sor. Végül, a jelen fejezet utolsó pontjában a fentiektől mind a probléma jellegében, mind pedig a megoldási módszerekben alapvetően eltérő partíciós kérdéseket tárgyalunk.

7.1. Lineáris diofantikus egyenlet

Először az $ax+by=c$ kétismeretlenes lineáris diofantikus egyenlettel foglalkozunk. Itt a, b, c rögzített egész számok, ahol az $a=b=0$ esetet eleve kizárjuk, és megoldáson x, y egész számokból álló számpárt értünk.

A megoldhatóság szükséges és elégséges feltételét az 1.3.6 Tételben, az egyenletnek a lineáris kongruenciákkal való kapcsolatát a 2.5.3 Tétel bizonyítása során tárgyaltuk. Az 1.3.6 Tétel bizonyításából azt is leolvastuk, hogy az egyenlet egy megoldását az euklideszi algoritmus segítségével kaphatjuk meg. Ebből az 5.7.1 Tétel szerint következett, hogy az egyenlet egy megoldását nagy számok esetén is „gyorsan" meg tudjuk határozni; ezt a tényt az RSA-sémában (5.8.1 Tétel) is felhasználtuk.

Most megadjuk a megoldásszámot és az összes megoldás leírását. A teljesség kedvéért a tétel állításában a megoldhatóságról és a megoldási módszerről korábban bizonyított állításokat is összefoglaljuk.

7.1.1 Tétel **T 7.1.1**

Legyenek a, b és c rögzített egész számok, ahol a és b közül legalább az egyik nem nulla, és tekintsük az $ax+by=c$ diofantikus egyenletet.

(i) Az egyenlet akkor és csak akkor oldható meg, ha $(a,b) \mid c$.

(ii) Megoldhatóság esetén végtelen sok megoldás van. Ha x_0, y_0 (egy rögzített) megoldás, akkor az összes x', y' megoldást az alábbi képlet szolgáltatja:

$$x' = x_0 + t\frac{b}{(a,b)}\,, \quad y' = y_0 - t\frac{a}{(a,b)}\,, \quad \text{ahol} \quad t = 0, \pm 1, \pm 2, \ldots \qquad (1)$$

(iii) Az egyenlet egy megoldását az euklideszi algoritmus segítségével kaphatjuk meg. ♣

Bizonyítás: Mint már említettük, (i)-et és (iii)-at az 1.3.6 Tételben igazoltuk.

Rátérve (ii)-re, először azt mutatjuk meg, hogy az (1)-ben megadott x', y' számok valóban az egyenlet egy megoldását szolgáltatják. Mivel x_0, y_0 megoldás, azaz $ax_0+by_0=c$, így

$$ax' + by' = a\left(x_0 + t\frac{b}{(a,b)}\right) + b\left(y_0 - t\frac{a}{(a,b)}\right) = ax_0 + by_0 = c\,.$$

A megfordításhoz tegyük fel, hogy x', y' egy tetszőleges megoldás, és belátjuk, hogy x' és y' a kívánt alakú.

A feltétel szerint

$$ax_0 + by_0 = c \qquad \text{és} \qquad ax' + by' = c\,.$$

A két egyenlőséget egymásból kivonva

$$a(x' - x_0) + b(y' - y_0) = 0$$

adódik. Rendezés és (a, b)-vel történő osztás után azt kapjuk, hogy

$$\frac{a}{(a,b)}(x' - x_0) = \frac{b}{(a,b)}(y_0 - y')\,. \tag{2}$$

Mivel

$$\left(\frac{b}{(a,b)}, \frac{a}{(a,b)}\right) = 1\,,$$

ezért (2)-ből

$$\frac{b}{(a,b)} \mid x' - x_0,$$

azaz alkalmas t egésszel

$$x' = x_0 + t\frac{b}{(a,b)} \tag{3}$$

következik. A (3)-at (2)-be visszahelyettesítve kapjuk, hogy

$$y' = y_0 - t\frac{a}{(a,b)}\,.$$

Ezzel megmutattuk, hogy x' és y' valóban az (1)-ben előírt alakú. ■.

A diofantikus egyenletek tényleges megoldásakor az euklideszi algoritmusnak egy olyan variánsát érdemes alkalmazni, amelynek segítségével (nemcsak egy megoldáshoz jutunk el, hanem) egyszerre tudjuk az összes megoldást (paraméteres alakban) előállítani. Ezt az eljárást egy konkrét példán keresztül mutatjuk be.

Példa: Oldjuk meg a $43x + 25y = 98$ diofantikus egyenletet.

Fejezzük ki az egyenletből azt az ismeretlent, amelynek az együtthatója kisebb abszolút értékű, és a törtből válasszunk le olyan részeket, amelyek biztosan egész értékűek:

$$y = \frac{98 - 43x}{25} = 4 - 2x + \frac{7x - 2}{25}\,. \tag{A1}$$

Ekkor az (A1) jobb oldalán álló $(7x-2)/25$ tört is egész szám kell hogy legyen, jelöljük ezt u-val. Innen $7x-2=25u$. Ez egy hasonló diofantikus egyenlet, mint az eredeti, csak itt az x együtthatójának kisebb az abszolút értéke, mint az eredeti egyenletben y együtthatójáé volt.

Ismételjük meg most az előző eljárást a $7x-2=25u$ egyenletre, fejezzük ki x-et, és válasszuk le a garantáltan egész értékű kifejezéseket:

$$x=\frac{25u+2}{7}=4u+\frac{2-3u}{7}\,. \tag{A2}$$

Az (A2) jobb oldalán szereplő $(2-3u)/7$ tört egész szám kell hogy legyen, jelöljük v-vel, ekkor $2-3u=7v$. Hasonlóan tovább haladva kapjuk, hogy

$$u=\frac{2-7v}{3}=-2v+\frac{2-v}{3}\,. \tag{A3}$$

A $(2-v)/3$ egész számot w-vel jelölve $2-v=3w$, azaz

$$v=2-3w. \tag{A4}$$

Mivel (A4)-ben már nem szerepel tört, most elindulunk „visszafelé”, és rendre (A3), (A2) és (A1) felhasználásával u, x és y értékét kifejezzük a w paraméter segítségével:

$$u=-2v+w=-2(2-3w)+w=-4+7w; \tag{B3}$$

$$x=4u+v=4(-4+7w)+(2-3w)=-14+25w; \tag{B2}$$

$$y=4-2x+u=4-2(-14+25w)+(-4+7w)=28-43w. \tag{B1}$$

A módszerből világos, hogy a (B2)–(B1) képletpár szolgáltatja a $43x+25y=98$ diofantikus egyenlet összes megoldását, ahol a w paraméter tetszőleges egész szám. Ugyanis egyrészt, ha egy x,y egész számpár megoldás, akkor az (A1)–(A3) lépéseken végighaladva eljutunk w-hez, majd ennek segítségével x-re és y-ra a (B2)–(B1) képletpár adódik, másrészt tetszőleges egész w-re az így képzett x és y számok egészek lesznek és kielégítik az egyenletet.

Megjegyzések: 1. Nézzük az eljárás lépései során keletkező együtthatópárokat:

$$\{43,25\};\quad \{25,7\};\quad \{7,3\};\quad \{3,1\}.$$

Ezek rendre úgy keletkeztek, hogy a 43-at a 25-tel osztva -7 volt a (legkisebb abszolút értékű) maradék, a 25-öt a 7-tel osztva -3 stb. Ez azt jelenti, hogy

itt valóban az euklideszi algoritmus egy variánsáról van szó, és ebből az is következik, hogy a diofantikus egyenlet megoldásait ily módon „gyorsan" meg tudjuk határozni.

2. A fenti módszer lényege, hogy az *ismeretlenek együtthatói*nak az abszolút értékeit megfelelően csökkentve végül a törteket teljesen kiküszöböljük. Ebből a szempontból mellékes, hogy a „*konstans*" tag abszolút értékét csökkentjük-e vagy sem. Akár végrehajtunk ilyen átalakítást (mint a fenti példában), akár nem, ez az eljárás lépésszámát nem befolyásolja, legfeljebb „kényelmesebb", ha kisebb számokkal dolgozunk.

3. Nem szükséges a megoldhatóság feltételét előre külön ellenőrizni, az eljárásból is automatikusan kiderül, ha nincs megoldás: ekkor egy olyan törthöz jutunk, amelyben már nem szerepel ismeretlen, azonban a tört értéke nem egész szám.

4. A (B2)–(B1) képlet összhangban van a 7.1.1 Tételnek az összes megoldást leíró (1) előállításával: most $x_0 = -14$, $y_0 = 28$, és a t szerepét w játssza. Ez az észrevétel esetleges számolási hibák kiszűrésére is alkalmas: a végeredményként kapott képletet mindig érdemes ilyen szempontból (1)-gyel összevetni.

Kettőnél több ismeretlenes lineáris diofantikus egyenletekre is a kétismeretlenes esethez hasonló állítások érvényesek. Ezeket az alábbi tételben foglaljuk össze, a bizonyításokat a 7.1.8 feladatban tűztük ki.

7.1.2 Tétel **T 7.1.2**

Legyen $k \geq 2$, $a_1, \ldots, a_k$ nem csupa 0 egész számok, c tetszőleges egész, és tekintsük az

$$a_1x_1 + \ldots + a_kx_k = c$$

diofantikus egyenletet (azaz megoldáson egy egészekből álló $x_1, \ldots, x_k$ számk-ast értünk).

(i) Az egyenlet akkor és csak akkor oldható meg, ha $(a_1, \ldots, a_k) \mid c$.

(ii) Megoldhatóság esetén végtelen sok megoldás van. Az összes megoldás $k-1$ egész paraméter segítségével adható meg. A megoldások meghatározása a két ismeretlen esetén látott módszer értelemszerű általánosításával történik. ♣

Feladatok

7.1.1 Bolondóciában csak 47 és 79 forintos bankjegyek léteznek. Hányféleképpen lehet pontosan 10 000 forintot kifizetni?

7.1.2 Egy szigeten 7- és 11-fejű sárkányok élnek. Hány sárkány él a szigeten, ha összesen 118 fejük van?

7.1.3 Egy üzletben háromféle csokoládé kapható, 70, 130, illetve 150 forintos egységárban. Hányféleképpen lehet (pontosan) 5000 forintért (pontosan) 50 darab csokoládét vásárolni?

M 7.1.4 Valamikor a huszadik században a 99 évnél nem idősebb és különböző korú Alexander és Bernát mindketten éppen annyi idősek, mint amennyi a születési évszámukban a számjegyek összege. Hány év közöttük a korkülönbség?

7.1.5 Mutassuk meg, hogy a 7.1.1 Tétel (ii) állítása a 2.5.4 Tételből (illetve az arra adott bizonyításból) is következik.

7.1.6 A síkon hány rácspontot tartalmazhat egy
a) racionális; b) irracionális
meredekségű egyenes?

7.1.7 Adjuk meg a $6x + 10y + 15z = 7$ diofantikus egyenlet összes megoldását.

7.1.8 Igazoljuk a 7.1.2 Tétel állításait.

7.1.9 Bizonyítsuk be, hogy az $a_1x_1 + \ldots + a_kx_k = c$ diofantikus egyenletnek akkor és csak akkor létezik megoldása, ha minden m pozitív egész esetén megoldható az $a_1x_1 + \ldots + a_kx_k \equiv c \pmod{m}$ kongruencia.

*7.1.10 Mely $a_1, \ldots, a_k$ egészek esetén igaz, hogy az $a_1x_1 + \ldots + a_kx_k = c$ diofantikus egyenletnek minden elég nagy c esetén létezik *pozitív* egészekben megoldása?

*7.1.11 Legyenek a és b rögzített, relatív prím, 1-nél nagyobb egészek. Nevezzünk (házi használatra) egy c pozitív egészt (a-ból és b-ből) „összerakhatónak", ha c felírható $c = ax + by$ alakban, ahol x és y *nemnegatív* egészek.

a) Mutassuk meg, hogy ha $c > ab - a - b$, akkor c összerakható, azonban $c = ab - a - b$ nem összerakható.

b) Hány nem összerakható pozitív egész létezik?

Megjegyzés: A feladat a) részét több változóra a következőképpen általánosíthatjuk. Legyenek $a_1, \ldots, a_k$ relatív prím, 1-nél nagyobb egészek. Keressük azt a maximális $F = F(a_1, \ldots, a_k)$ egészt, amelyre az $a_1x_1 + \ldots + a_kx_k = F$ diofantikus egyenlet nem oldható meg nemnegatív egészekben. Ezt a kérdést *Frobenius-problémá*nak nevezik. A $k > 2$ eset vizsgálata igen nehéz.

*7.1.12

a) Mutassuk meg, hogy minden elég nagy n esetén létezik n darab olyan (nem feltétlenül egybevágó) kocka, amelyekből (mindegyiket egyszer felhasználva) összeállítható egy (nagyobb) kocka.

b) Igazoljuk ugyanezt minden $n \geq 48$-ra.

Megjegyzés: Megoldatlan probléma, hogy az állítás igaz-e $n = 47$-tel is.

7.2. Pitagoraszi számhármasok

*Pitagoraszi számhármas*oknak az $x^2 + y^2 = z^2$ egyenlet pozitív egész megoldásait nevezzük. Geometriai megfogalmazásban a pitagoraszi számhármasok azoknak a derékszögű háromszögeknek az oldalhosszait jelentik, amelyekben mindhárom oldal hossza egész szám.

Azonnal látszik, hogy az egyenlet megoldható (például a 3, 4, 5 számhármas megoldás), sőt egy x, y, z megoldást tetszőleges d pozitív egésszel beszorozva a kapott dx, dy, dz számhármas is nyilván megoldás. Ezért külön érdemes azokat a megoldásokat vizsgálni, ahol $(x, y, z) = 1$, ezeket *alapmegoldás*oknak vagy *primitív* pitagoraszi számhármasoknak nevezzük.

Megmutatjuk, hogy alapmegoldásból is végtelen sok van, sőt elő tudjuk állítani az összes alapmegoldást és így az összes megoldást is alkalmas paraméterek segítségével:

7.2.1 Tétel **T 7.2.1**

(i) Az

$$x^2 + y^2 = z^2 \tag{1}$$

egyenletnek az

$$(x, y, z) = 1 \tag{2}$$

feltételt kielégítő összes pozitív egész megoldását (azaz az alapmegoldásokat, vagy más néven a primitív pitagoraszi számhármasokat) a következő képlet szolgáltatja (itt az x és y felcseréléséből adódó megoldásokat azonosnak tekintjük):

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2, \tag{3}$$

ahol az m és n paraméterek tetszőleges olyan pozitív egészek, amelyekre

$$m \text{ és } n \text{ különböző paritású}, \qquad m > n \qquad \text{és} \qquad (m, n) = 1. \tag{4}$$

(ii) Az (1) egyenlet összes pozitív egész megoldását (azaz az összes pitagoraszi számhármast) az alapmegoldások többszöröseiként kapjuk meg, tehát

$$x = 2mnd, \qquad y = (m^2 - n^2)d, \qquad z = (m^2 + n^2)d, \tag{5}$$

ahol d tetszőleges pozitív egész, az m és n pozitív egészekre pedig teljesül (4). ♣

Bizonyítás: Végig valamennyi változó pozitív egészt jelöl.

(i) Először azt mutatjuk meg, hogy ha x, y, z alapmegoldás (azaz eleget tesz (1)-nek és (2)-nek), akkor x, y és z szükségképpen a (3)-ban és (4)-ben előírt alakú.

Első lépésként belátjuk, hogy x, y és z páronként is relatív prímek. Nézzük például $(x, z) = 1$-et, a másik két eset ugyanígy igazolható. Tegyük fel indirekt, hogy egy p prímre $p \mid x$ és $p \mid z$ fennáll. Ekkor ebből $p \mid z^2 - x^2 = y^2$, és így p prím volta miatt $p \mid y$ következik. Ez azt jelenti, hogy p közös osztója az x, y és z számoknak, ami ellentmond (2)-nek.

Most megmutatjuk, hogy x és y közül az egyik páros, a másik páratlan. Mindkettő nem lehet páros, hiszen $(x, y) = 1$. Ha mindkettő páratlan, akkor a négyzetük 1 maradékot ad 4-gyel osztva, vagyis $x^2 + y^2 = z^2$ bal oldala 2 maradékot ad 4-gyel osztva, a jobb oldal viszont 0-t vagy 1-et, ami ellentmondás.

Feltehetjük, hogy x páros és y páratlan. Ekkor (1)-et átrendezve, 4-gyel elosztva és szorzattá bontva az

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2} \tag{6}$$

alakhoz jutunk.

Belátjuk, hogy a (6) jobb oldalán szereplő két tényező relatív prím. Tegyük fel, hogy k közös osztója $(z+y)/2$-nek és $(z-y)/2$-nek. Ekkor

$$k \mid \frac{z+y}{2} + \frac{z-y}{2} = z \qquad \text{és} \qquad k \mid \frac{z+y}{2} - \frac{z-y}{2} = y\,.$$

Mivel $(y, z) = 1$, ezért $k \mid 1$, tehát valóban

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1\,. \tag{7}$$

Az 1.6.2a feladat alapján (6)-ból és (7)-ből következik, hogy a (6) jobb oldalán szereplő két pozitív tényező külön-külön is négyzetszám, azaz alkalmas m és n pozitív egésszel

$$\frac{z+y}{2} = m^2 \qquad \text{és} \qquad \frac{z-y}{2} = n^2\,. \tag{8}$$

A (8) egyenlőségeket összeadva, illetve kivonva, valamint (6)-ba visszahelyettesítve éppen a kívánt (3) előállítást kapjuk z-re, y-ra és x-re.

A (4) feltételek is teljesülnek; ezek rendre z (vagy y) páratlanságából, $y > 0$-ból, illetve (7)-ből következnek.

Rátérve a megfordításra, most azt igazoljuk, hogy a (3)–(4) képlet mindig primitív pitagoraszi számhármast definiál.

Az így megadott x, y és z számok az $m > n > 0$ feltétel miatt pozitív egészek, és egyszerű behelyettesítéssel ellenőrizhető, hogy kielégítik az (1) egyenletet.

Azt kell még megmutatni, hogy $(x, y, z) = 1$. Ehhez elég belátni, hogy (például) y és z relatív prímek.

Tegyük fel indirekt, hogy van olyan p prím, amelyre $p \mid y$ és $p \mid z$. Ekkor $p \mid z + y$ és $p \mid z - y$ is teljesül, azaz

$$p \mid (m^2+n^2)+(m^2-n^2) = 2m^2 \qquad \text{és} \qquad p \mid (m^2+n^2)-(m^2-n^2) = 2n^2\,. \quad (9)$$

Mivel p prím, ezért (9)-ből következik, hogy $p = 2$, vagy $p \mid m^2$ és $p \mid n^2$.

A $p = 2$ eset nem lehetséges, mert m és n ellenkező paritása miatt $z = m^2 + n^2$ páratlan.

A másik esetben pedig (ismét felhasználva, hogy p prím) azt kapjuk, hogy $p \mid m$ és $p \mid n$, ami ellentmond az $(m, n) = 1$ feltételnek.

(ii) Mint már említettük, egy alapmegoldást (vagy bármilyen megoldást) d-vel végigszorozva nyilván ismét megoldást kapunk. Megfordítva, egy tetszőleges x, y, z megoldás előáll az x/d, y/d, z/d alapmegoldás d-szereseként, ahol $d = (x, y, z)$. ■

Feladatok

7.2.1 Mutassuk meg, hogy ha egy derékszögű háromszög oldalai egész számok, akkor az oldalhosszak szorzata osztható 60-nal.

7.2.2 Számítsuk ki a derékszögű háromszög oldalait, ha tudjuk, hogy az oldalak egész számok és a háromszög területe 60.

7.2.3 Adjuk meg az összes olyan derékszögű háromszöget, amelynek az oldalai egész számok és a kerület és terület mérőszáma megegyezik.

7.2.4 Mely k egészekre létezik olyan egész oldalú derékszögű háromszög, amelynek az egyik oldala k?

7.2.5 Mutassuk meg, hogy végtelen sok olyan háromtagú számtani sorozat létezik, amelynek tagjai relatív prímek és mindhárom elem négyzetszám.

7.3. Néhány elemi módszer

Az alábbiakban néhány tipikus módszert mutatunk be, amelyek gyakran alkalmazhatók diofantikus egyenletek vizsgálatánál.

I. *„Szorzat = szám"*

A 7.2.2 és 7.2.3 feladatokhoz fűzött két-két útmutatás mindegyikében a megoldás kulcsát egy-egy olyan diofantikus egyenlet szolgáltatta, ahol az egyik oldalon egy $c \neq 0$ egész szám, a másik oldalon pedig egy szorzat állt:

$$d^2mn(m-n)(m+n) = 60, \qquad (x-4)(y-4) = 8 \qquad \text{stb.}$$

Ilyen típusú szorzattá bontás segítségével most azt a problémát vizsgáljuk meg, hogy mely pozitív egészek állnak elő és hányféleképpen két négyzetszám különbségeként.

7.3.1 Tétel **T 7.3.1**

Tekintsük az $x^2 - y^2 = n$ diofantikus egyenletet, ahol n rögzített pozitív egész.

(i) Az egyenlet akkor és csak akkor oldható meg, ha $n \not\equiv 2 \pmod 4$.

(ii) A megoldásszám $2d(n)$, ha n páratlan, és $2d(\frac{n}{4})$, ha $4 \mid n$ (ahol $d(k)$ a k pozitív osztóinak a száma). ♣

Itt a csak az előjelben eltérő megoldásokat is külön megoldásoknak tekintjük. A tétel alapján könnyen megkaphatjuk a „lényegesen különböző" megoldások számát is, lásd a 7.3.1 feladatot.

Bizonyítás: Az $(x+y)(x-y) = n$ egyenlőség pontosan akkor teljesül, ha $x+y$ és $x-y$ az n két komplementer osztója, azaz

$$x + y = d_1, \quad x - y = d_2, \quad \text{ahol} \quad d_1 d_2 = n\,. \tag{1}$$

Az (1) egyenletrendszert megoldva

$$x = \frac{d_1 + d_2}{2}, \qquad y = \frac{d_1 - d_2}{2}$$

adódik. Itt x-re és y-ra pontosan akkor kapunk egész értéket, ha d_1 és d_2 azonos paritású.

Ennek megfelelően az $x^2 - y^2 = n$ diofantikus egyenlet akkor és csak akkor oldható meg, ha az n felírható két azonos paritású osztója szorzataként, a megoldások száma pedig az ilyen azonos paritású osztópárok száma (ahol a két osztó sorrendje is számít és a negatív osztókat is figyelembe kell venni).

Ha n páratlan, akkor minden osztója is páratlan, tehát minden osztópár megfelel. Ennek megfelelően (az egyenlet megoldható és) a megoldások száma az n összes (pozitív és negatív) osztóinak a száma, vagyis $2d(n)$.

Ha n páros, de nem osztható 4-gyel, akkor n nem írható fel két azonos paritású szám szorzataként, hiszen két páratlan szám szorzata páratlan, két páros szám szorzata pedig osztható 4-gyel. Ez azt jelenti, hogy az egyenlet ilyen n-ekre nem oldható meg.

Ha $4 \mid n$, akkor azok az osztópárok felelnek meg, amelyekben mindkét osztó páros szám: $n = (2k_1)(2k_2)$. Mivel ez ekvivalens az $n/4 = k_1k_2$ feltétellel, ezért (az egyenlet megoldható és) a megoldásszám az $n/4$ összes (pozitív és negatív) osztóinak a száma, vagyis $2d(n/4)$. ■

II. *„Szorzat = hatvány"*

A számelmélet alaptételéből következik, hogy ha egy k-adik hatvány két relatív prím tényező szorzata, akkor egységszorzóktól eltekintve a tényezők maguk is k-adik hatványok (lásd az 1.6.2 feladatot). Ez a tény fontos szerepet játszott a 7.2.1 Tétel bizonyításánál (lásd az ottani (6), (7) és (8) képleteket), valamint az 1.6.3 feladat megoldásánál. A következő példával azt illusztráljuk, hogy ilyen típusú meggondolások gyakran akkor is alkalmazhatók, ha a tényezők nem feltétlenül relatív prímek.

Példa: Oldjuk meg az $x^3 + 7x = y^3$ diofantikus egyenletet.

Az $x = y = 0$ nyilván megoldás, továbbá ha x, y megoldás, akkor $-x, -y$ is az, ezért a továbbiakban feltehetjük, hogy x (és így y is) pozitív.

Az egyenlet bal oldalát bontsuk szorzattá:

$$x(x^2 + 7) = y^3, \tag{2}$$

és vizsgáljuk meg a két tényező legnagyobb közös osztójának lehetséges értékeit. Legyen $d = (x, x^2 + 7)$, ekkor

$$d \mid (x^2 + 7) - x \cdot x = 7,$$

azaz csak $d = 1$ és $d = 7$ jöhet szóba.

Ha $d = 1$, akkor x és $x^2 + 7$ külön-külön is köbszámok, azaz alkalmas u, v (pozitív) egészekkel

$$x = u^3 \qquad \text{és} \qquad x^2 + 7 = v^3\,. \tag{3}$$

A második egyenlőségben x helyére u^3-t beírva

$$v^3 - u^6 = 7 \tag{4}$$

adódik. Két pozitív köbszám különbsége csak a $(8, 1)$ pár esetén lehet 7: ha $a > b > 0$, akkor

$$a^3 - b^3 \geq (b+1)^3 - b^3 = 3b^2 + 3b + 1 \geq 7,$$

és egyenlőség csak a $b = 1$, $a = b + 1 = 2$ értékekre áll fenn. (Másik indoklási lehetőség: a

$$7 = a^3 - b^3 = (a-b)(a^2 + ab + b^2)$$

szorzat-előállításban a tényezők eleve csak ± 1 és ± 7 lehetnek megfelelő párosításban.)

(3) és (4) alapján így az $x = 1$, $y = 2$ megoldást kapjuk.

Nézzük most a $d = 7$ esetet. Ekkor $7 \mid x$ és $x \mid y^3$ alapján $7 \mid y^3$, és így a 7 prím volta miatt $7 \mid y$ következik. Vizsgáljuk meg, hogy a 7 hányadik hatványával osztható (2) jobb oldala, illetve a bal oldal két tényezője. A jobb oldalon y^3-ban a 7 kitevője legalább 3, ugyanakkor a bal oldal második tényezőjére ($7^2 \mid x^2$ miatt) $7^2 \nmid x^2 + 7$. Ennélfogva a bal oldal első tényezőjében a 7 kitevője legalább $3 - 1 = 2$, azaz szükségképpen $7^2 \mid x$.

A fentiekből adódó $x = 7^2 r$ és $y = 7s$ összefüggéseket (2)-be beírva és 7^3-nal egyszerűsítve azt kapjuk, hogy

$$r(7^3 r^2 + 1) = s^3\,. \tag{5}$$

Az (5) bal oldalán álló két tényező relatív prím, tehát külön-külön is köbszámok:

$$r = w^3 \qquad \text{és} \qquad 7^3 r^2 + 1 = 7^3 w^6 + 1 = z^3\,.$$

Az utolsó egyenlőség szerint $z^3 - (7w^2)^3 = 1$, ez azonban nemnulla köbszámok esetén nem lehetséges.

Ez azt jelenti, hogy a $d = 7$ eset nem valósulhat meg.

Összefoglalva, az egyenletnek három megoldása van:

$$x = y = 0; \qquad x = 1,\ y = 2; \qquad x = -1,\ y = -2.$$

Ugyanennél az egyenletnél egy másik eljárás is célhoz vezet, lásd alább a IV. módszert.

III. *Megoldhatatlanság bizonyítása kongruencia segítségével*

Ha egy diofantikus egyenlet esetén az egyenlet két oldala valamely alkalmas modulus szerint sohasem lehet kongruens egymással, akkor az egyenlőség biztosan nem teljesülhet (ez fordított irányban nem igaz!).

Példa: Oldjuk meg az $x^4 + 5y^4 = 4z^4$ diofantikus egyenletet.

Az egyenletnek nyilván megoldása $x = y = z = 0$. Megmutatjuk, hogy más megoldás nincs.

Tegyük fel indirekt, hogy létezik olyan megoldás, ahol x, y, z nem mindegyike 0. Ekkor azt is feltehetjük, hogy x, y és z relatív prímek. Ha ugyanis $(x, y, z) = d > 1$, akkor az egyenletet d^4-nel elosztva kapjuk, hogy x/d, y/d, z/d is megoldás, és ez a három szám már relatív prím is.

Mivel $x^4 + 5y^4 = 4z^4$, ezért

$$x^4 + 5y^4 \equiv 4z^4 \pmod 5 \tag{6}$$

is teljesül. A kis Fermat-tétel szerint bármely a egész számra

$$a^4 \equiv \begin{cases} 1 \pmod 5, & \text{ha } 5 \nmid a; \\ 0 \pmod 5, & \text{ha } 5 \mid a. \end{cases} \tag{7}$$

Ha $5 \nmid x$, akkor (7) alapján (6) bal oldala 1-gyel, a jobb oldal viszont 0-val vagy 4-gyel kongruens modulo 5, ami lehetetlen. Az $5 \nmid z$ eset ugyanígy ellentmondásra vezet. Ebből következik, hogy $5 \mid x$ és $5 \mid z$.

Legyen $x = 5x_1$, $z = 5z_1$, ezt az eredeti egyenletbe beírva

$$5^4 x_1^4 + 5y^4 = 4 \cdot 5^4 z_1^4, \qquad \text{azaz} \qquad 5^3 x_1^4 + y^4 = 4 \cdot 5^3 z_1^4$$

adódik. Ennélfogva $5 \mid y^4$, és így az 5 prím volta miatt $5 \mid y$ is teljesül. Ez azonban ellentmond az $(x, y, z) = 1$ feltételnek.

Megjegyzések: 1. A fenti egyenletet modulo 5 helyett modulo 16 vizsgálva is hasonló módon ellentmondásra juthatunk.

2. Általában olyan modulussal érdemes próbálkozni, amely osztója az egyenlet valamelyik együtthatójának vagy amelyre nézve az egyenletben előforduló hatványok kevés maradékosztályba eshetnek csak. Például a négyzetszámok 8-cal osztva csak 0, 1 vagy 4, a negyedik hatványok 16-tal osztva csak 0 vagy 1 maradékot adhatnak, ezért gyakran érdemes modulusnak a 8-at, illetve a 16-ot választani.

3. Ha valamilyen modulus esetén nem jutunk ellentmondásra, ez csak annyit jelent, hogy a megfelelő kongruencia megoldható, ebből azonban nem

következik, hogy az egyenletnek is van megoldása (és persze az sem következik, hogy az egyenletnek nincs megoldása). Például a fenti egyenletnél az $m = 3$ vagy az $m = 7$ modulus nem segített volna, hiszen az $x^4 + 5y^4 \equiv 4z^4 \pmod 3$, illetve (mod 7) kongruenciáknak létezik nemtriviális megoldása:

$$(\pm 1)^4 + 5(\pm 1)^4 \equiv 4 \cdot 3^4 \pmod 3 \quad \text{és} \quad (\pm 1)^4 + 5(\pm 2)^4 \equiv 4(\pm 1)^4 \pmod 7 .$$

4. Még egyszer hangsúlyozzuk, hogy ez a módszer lényegében csak akkor vezethet (önmagában) eredményre, ha a diofantikus egyenletnek nincs megoldása, illetve csak „triviális" megoldása van (mint a fenti egyenletnél $x = y = z = 0$). Ha ugyanis létezik az egyenletnek (nemtriviális) megoldása, akkor az tetszőleges m modulus esetén kielégíti a megfelelő kongruenciát is, tehát egyetlen modulusnál sem jutunk ellentmondásra. (Az természetesen igaz, hogy az ilyen jellegű kongruenciás megfontolások bármely diofantikus egyenlet esetén segíthetnek *bizonyos típusú* megoldások kizárásában.)

5. A diofantikus egyenlet megoldhatatlansága esetén sem biztos, hogy ez a módszer célhoz vezet. Egyrészt nem biztos, hogy rátalálunk egy olyan modulusra, amely kihozza a keresett ellentmondást, másrészt lehet, hogy nincs is ilyen modulus: a 4.2.8 feladatban láttuk, hogy van olyan egyenlet, amelynek nincs egész vagy racionális megoldása, ugyanakkor a megfelelő kongruencia bármely m modulus esetén megoldható.

IV. *Egyenlőtlenségek alkalmazása*

Tekintsünk egy $f(x) = y^k$ típusú diofantikus egyenletet. Ha van olyan c, hogy minden c-nél nagyobb abszolút értékű x egész számra az $f(x)$ két egymást követő k-adik hatvány közé esik (az egyenlőséget nem megengedve), akkor világos, hogy csak olyan megoldások jöhetnek szóba, ahol $|x| \leq c$. Az így megmaradt véges sok x-et végigpróbálva megkaphatjuk az egyenlet összes megoldását.

Az eljárást a (II. módszerrel már vizsgált) $x^3 + 7x = y^3$ diofantikus egyenleten mutatjuk be.

Mint láttuk, elegendő az $x > 0$ esetre szorítkozni, továbbá $x = 1$, $y = 2$ megoldás.

egyszerű számolással adódik, hogy ha $x > 1$, akkor

$$x^3 < x^3 + 7x < (x + 1)^3 ,$$

tehát $x > 1$ esetén $x^3 + 7x$ nem lehet köbszám.

Mindezek alapján az egyenlet összes megoldása a II. módszernél megadott három számpár.

Feladatok

7.3.1 Legyen n rögzített pozitív egész. Hány „lényegesen különböző módon" írható fel az n két négyzetszám különbségeként, azaz hány megoldása van az $x^2 - y^2 = n$ egyenletnek a *nemnegatív* egészek körében?

7.3.2 Egy háziasszony egy tepsi süteményt úgy akar (egyforma téglalap alakú darabokra) felvágni, hogy ugyanannyi „égett", azaz a tepsi falával legalább egy oldalon érintkező, mint „nem égett", azaz a tepsi falával nem érintkező szelet keletkezzen. Hogyan végezze a szeletelést?

7.3.3 Ottlik Géza, a kiváló prózaíró, matematikai tanulmányokat is folytatott. Ezzel kapcsolatos visszaemlékezéseiben szerepel az alábbi feladat: Bizonyítsuk be, hogy bármely $p > 2$ prím esetén a $2/p$ szám pontosan egyféleképpen írható fel két különböző pozitív egész reciprokának összegeként. (Az összeadandók sorrendjére nem vagyunk tekintettel.)

*7.3.4 Mely 4 számlálójú törtek írhatók fel két természetes szám reciprokának az összegeként?

7.3.5 Mutassuk meg, hogy ha az n pozitív egész *nem* $24k+1$ alakú, akkor $4/n$ felírható három természetes szám reciprokának az összegeként.

Megjegyzés: Erdős és Straus egy nevezetes, máig bizonyítatlan sejtése szerint minden n pozitív egész rendelkezik a fenti tulajdonsággal.

7.3.6 Bizonyítsuk be, hogy minden pozitív racionális szám végtelen sokféleképpen áll elő véges sok különböző pozitív egész reciprokának az összegeként.

Megjegyzés: A pozitív egészek reciprokait, azaz az 1 számlálójú (és pozitív nevezőjű) törteket *egyiptomi tört*eknek nevezzük, mert az ókori Egyiptomban a racionális számokat általában ilyen törtek összegeként írták fel.

7.3.7 Van-e olyan negyedik hatvány, amely 4-gyel nagyobb egy ötödik hatványnál?

M 7.3.8 Adjuk meg az alábbi egyenletrendszer összes olyan megoldását, ahol x, y, s és t racionális számok:

$$t^2 + (s+x)^2 = s^2 + y^2 = (y+t)^2 + x^2\,.$$

7.3.9 Bizonyítsuk be, hogy 99 egymást követő négyzetszám összege nem lehet teljes hatvány.

M 7.3.10 Adjuk meg az összes olyan egész számot, amelynek a köbe előáll nyolc szomszédos egész szám köbének az összegeként.

*7.3.11 Bizonyítsuk be, hogy 6 egymást követő természetes szám nem osztható két (diszjunkt) csoportra úgy, hogy az egyik csoport elemeinek a szorzata megegyezzék a másik csoport elemeinek a szorzatával. Igazoljuk ugyanezt az állítást 6 helyett 106-ra is.

7.3.12 Adott m pozitív egészhez adjuk meg az összes olyan n, x, y pozitív egészt, amelyre

$$(n, m) = 1 \qquad \text{és} \qquad (x^2 + y^2)^m = (xy)^n .$$

7.3.13 Oldjuk meg a következő diofantikus egyenleteket:

a) $xy + 3x + 5y = 7$;
b) $x^2 - 2y^2 + 363z^2 = 77$;
c) $2x^2 + 3y^2 = z^2$;
d) $x^2 - 230y^2 = 7z^2$;
*e) $x^5 + 3y^5 = 5z^5$;
f) $(x^2 - 2)(x^2 + 7) = z^3$;
M *g) $x^2 - 2y^4 = 1$;
M h) $x^y = y^x$ (x és y pozitív egész);
M *i) $2^x - y^5 = 31$.

7.3.14 Milyen alapú számrendszerekben igaz, hogy az alábbi alakú számok négyzetszámok?
a) 111; *b) 11111; c) 111111.
(A „kimaradt” 1111-re vonatkozóan lásd a 7.7.7 feladatot.)

7.4. Gauss-egészek

A 7.3.1 Tételben pontos választ adtunk arra, mely pozitív egészek állnak elő és hányféleképpen két négyzetszám különbségeként. Most azt a rokon kérdést vetjük fel, hogy mi a helyzet különbség helyett összegre, azaz mely pozitív egészek állnak elő és hányféleképpen két négyzetszám összegeként.

Az $x^2 - y^2 = n$ diofantikus egyenlet megoldásánál a bal oldal szorzattá bontása volt a kulcslépés. Az $x^2 + y^2 = n$ esetben ilyen szorzattá bontás az egész (vagy akár valós) számok keretén belül maradva nem létezik, azonban a komplex számok körében már igen: $(x + yi)(x - yi) = n$. Ezért ígéretesnek tűnik az olyan $a + bi$ komplex számok számelméletének a kiépítése, ahol a és b egész számok. Az ilyen komplex számokat nevezzük *Gauss-egész*eknek.

Az egész számok mintájára a Gauss-egészek körében is definiáljuk a megfelelő számelméleti fogalmakat (oszthatóság, egység, legnagyobb közös osztó, felbonthatatlan, prím), majd megmutatjuk, hogy a Gauss-egészekre is érvényes a számelmélet alaptétele, ezután pedig az összes Gauss-felbonthatatlan „áttekintése" következik. Mindezek birtokában a következő pontban visszatérünk majd a kiindulási problémánkra, az $x^2 + y^2 = n$ diofantikus egyenletre.

7.4.1 Definíció **D 7.4.1**

*Gauss-egész*eknek azokat az $\alpha = a + bi$ komplex számokat nevezzük, ahol a és b egész szám. ♣

Az egyértelmű megkülönböztetés érdekében ebben a pontban az egész számokat latin betűkkel, míg a Gauss-egészeket görög betűkkel jelöljük.

A Gauss-egészek a komplex számok összeadására és szorzására kommutatív, egységelemes, nullosztómentes gyűrűt alkotnak.

A Gauss-egészek számelméleti vizsgálatánál kulcsszerepet játszik a norma fogalma:

7.4.2 Definíció **D 7.4.2**

Az $\alpha = a + bi$ Gauss-egész *normá*jának nevezzük és $N(\alpha)$-val jelöljük az α abszolút értékének négyzetét:

$$N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2 \,. \ \clubsuit$$

A Gauss-egészek definíciójából és a komplex számok abszolút értékének tulajdonságaiból azonnal adódnak az alábbi egyszerű, de fontos állítások:

7.4.3 Tétel **T 7.4.3**

Tetszőleges α, β Gauss-egészek esetén

(i) $N(\alpha)$ nemnegatív egész szám;

(ii) $N(\alpha) = 0 \iff \alpha = 0$;

(iii) $N(\alpha\beta) = N(\alpha)N(\beta)$. ♣

A Gauss-egészek számelméletének kiépítéséhez az egész számokra az 1. fejezetben látott utat követjük: a fogalmak definiálása és a számelmélet alaptételének bizonyítása az ottani mintára történik. Egyedül a maradékos osztás tételének a Gauss-egészekre vonatkozó megfelelője (7.4.8 Tétel) mutat komolyabb formai eltérést, ettől eltekintve szinte „lemásoljuk" az egész számoknál szereplő felépítést.

7.4.4 Definíció **D 7.4.4**

A β Gauss-egészt az α Gauss-egész *osztó*jának nevezzük, ha létezik olyan γ Gauss-egész, amelyre $\alpha = \beta\gamma$. ♣

Akárcsak az egész számoknál, ugyanezt jelenti az „α *osztható* β-val", illetve az „α *többszöröse* a β-nak" kifejezés is, és a Gauss-egészeknél is a $\beta \mid \alpha$ jelölést használjuk.

A $\beta \neq 0$ esetben $\beta \mid \alpha$ pontosan akkor teljesül, ha az $\dfrac{\alpha}{\beta}$ komplex szám Gauss-egész.

Példák:

$$2+i \mid 7+i, \quad \text{mert} \quad \frac{7+i}{2+i} = 3-i;$$

$$4+i \not\mid 4-i, \quad \text{mert} \quad \frac{4-i}{4+i} = \frac{15}{17} - \frac{8}{17}i.$$

A Gauss-egészek és az egész számok számelmélete között fontos híd az alábbi (egyirányú) kapcsolat:

7.4.5 Tétel **T 7.4.5**

Ha $\beta \mid \alpha$ (a Gauss-egészek körében), akkor $N(\beta) \mid N(\alpha)$ (az egész számok körében). ♣

Bizonyítás: Az állítás a 7.4.4 Definícióból és a 7.4.3/(iii) Tételből következik. ■

A 7.4.5 Tétel megfordítása nem igaz, amint azt a tétel fölött megadott második példa is mutatja.

7.4.6 Definíció **D 7.4.6**

Az ε Gauss-egész *egység*, ha minden Gauss-egésznek osztója. ♣

Az egységek sokféle ekvivalens jellemzéséről szól a következő tétel:

7.4.7 Tétel **T 7.4.7**

Egy ε Gauss-egészre az alábbi feltételek ekvivalensek:

(i) ε egység.

(ii) $\varepsilon \mid 1$.

(iii) $N(\varepsilon) = 1$.

(iv) $\varepsilon = 1, -1, i$ vagy $-i$. ♣

Bizonyítás: (i) $\Longrightarrow$ (ii): Ha ε minden Gauss-egésznek osztója, akkor speciálisan az 1-nek is osztója.

(ii) $\Longrightarrow$ (iii): A 7.4.5 Tételből következik.

(iii) $\Longrightarrow$ (iv): A $N(a+bi) = a^2 + b^2 = 1$ egyenlőség egész a, b mellett csak $a = \pm 1, b = 0$, illetve $a = 0, b = \pm 1$ esetén teljesülhet.

(iv) $\Longrightarrow$ (i): Bármely α Gauss-egészre

$$\alpha = 1\alpha = (-1)(-\alpha) = i(-i\alpha) = (-i)(i\alpha). \blacksquare$$

Most rátérünk a maradékos osztás Gauss-egészekbeli megfelelőjére:

7.4.8 Tétel **T 7.4.8**

Tetszőleges α és $\beta \neq 0$ Gauss-egészekhez léteznek olyan γ és ϱ Gauss-egészek, melyekre

$$\alpha = \beta\gamma + \varrho \qquad \text{és} \qquad N(\varrho) < N(\beta). \ \clubsuit \tag{1}$$

Bizonyítás: Az (1) feltétel ekvivalens

$$\frac{\alpha}{\beta} - \gamma = \frac{\varrho}{\beta} \qquad \text{és} \qquad |\varrho| < |\beta|, \quad \text{azaz} \quad \left|\frac{\varrho}{\beta}\right| < 1$$

teljesülésével. Ez azt jelenti, hogy olyan γ Gauss-egészt kell keresni, amelyre

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1\,. \tag{2}$$

A Gauss-egészek a komplex számsíkon a szokásos egységnyi oldalú négyzetrács pontjait alkotják. A (2) feltétel így átfogalmazható arra, hogy a síkon az α/β-nak megfelelő (racionális koordinátájú) pont a γ rácsponttól 1-nél kisebb távolságra esik, azaz benne van a γ körül rajzolt egységkör belsejében.

Tekintsünk egy olyan rácsnégyzetet, amely az α/β pontot (a belsejében vagy a határán) tartalmazza (akkor létezik több ilyen rácsnégyzet, ha α/β-nak legalább az egyik koordinátája egész szám). A rácsnégyzet két átellenes csúcsa köré rajzoljunk egy-egy egységkört; ezeknek a köröknek a belseje a két másik csúcs kivételével az egész négyzetet lefedi. Ez azt jelenti, hogy a sík bármely pontjához található tőle 1-nél kisebb távolságra levő rácspont, vagyis bármely α/β-hoz található legalább egy megfelelő γ.

Ezután ϱ értéke a $\varrho = \alpha - \beta\gamma$ összefüggésből adódik. ■

Megjegyzések: 1. A bizonyításból az is leolvasható, hogy a γ hányados és a ϱ maradék általában nem egyértelmű. Az egyértelműség csak akkor teljesül, ha α/β maga is rácspont, azaz $\beta \mid \alpha$ (ekkor a maradék 0). Minden más esetben, α/β elhelyezkedésétől függően 2, 3 vagy 4 megfelelő γ, ϱ pár létezik.

2. A bizonyítás egyúttal algoritmust is ad γ és ϱ megkeresésére: az α/β-hoz legközelebbi rácspontot érdemes γ-nak választani. Ez geometriamentesen is megfogalmazható: Ha $\alpha/\beta = r + si$, akkor legyen $\gamma = u + vi$, ahol u, illetve v az r, illetve s (racionális) számhoz legközelebb eső egész szám. Ekkor

$$\left|\frac{\alpha}{\beta} - \gamma\right|^2 = (r-u)^2 + (s-v)^2 \le \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}\,.$$

A Gauss-egészeknél a legnagyobb közös osztó fogalmát eleve a kitüntetett közös osztó mintájára értelmezzük: olyan közös osztó, amely minden közös osztónak többszöröse.

7.4.9 Definíció **D 7.4.9**

Az α és β Gauss-egészek *legnagyobb közös osztó*ja δ, ha

(i) $\delta \mid \alpha$, $\delta \mid \beta$; és

(ii) ha egy γ-ra $\gamma \mid \alpha$, $\gamma \mid \beta$ teljesül, akkor $\gamma \mid \delta$. ♣

Most is feltesszük, hogy α és β közül legalább az egyik nem nulla.

A legnagyobb közös osztó létezése az 1.3.3 Tétel bizonyításához hasonlóan az euklideszi algoritmusból következik (az eljárás a Gauss-egészeknél is véges sok lépésben befejeződik, hiszen a maradékok *normái* nemnegatív egészek és szigorúan csökkenő sorozatot alkotnak). Az euklideszi algoritmus a legnagyobb közös osztó gyakorlati meghatározására is alkalmas.

A legnagyobb közös osztó egységszerestől eltekintve egyértelmű, azaz ha δ az α és β Gauss-egészek egyik legnagyobb közös osztója, akkor az összes legnagyobb közös osztót a δ egységszeresei adják. (Ez a legnagyobb közös osztó definíciójából következik.)

Mindezek alapján bármely két Gauss-egésznek (amelyek közül legalább az egyik nem nulla) pontosan négy legnagyobb közös osztója van. Mivel ezek oszthatósági szempontból teljesen egyformán viselkednek, valamint egyikük előtérbe helyezését sem támasztja alá olyan természetes kiválasztási elv, mint az egész számoknál a pozitivitás, ezért közöttük semmilyen formában nem teszünk különbséget, és az (α, β) jelölés közülük akármelyiket jelentheti.

A legnagyobb közös osztóra vonatkozó, az 1.3 pontban szereplő további tételek és definíciók megfelelői a Gauss-egészek körében is ugyanúgy érvényesek.

Most a Gauss-felbonthatatlan és a Gauss-prím fogalmát definiáljuk az 1.4.1, illetve 1.4.2 Definíciók mintájára.

7.4.10 Definíció **D 7.4.10**

A π egységtől (és nullától) különböző Gauss-egészt *Gauss-felbonthatatlan*nak nevezzük, ha **csak** úgy bontható fel két Gauss-egész szorzatára, hogy valamelyik tényező egység. Azaz

$$\pi = \alpha\beta \Longrightarrow \alpha \text{ vagy } \beta \text{ egység. } \clubsuit$$

7.4.11 Definíció **D 7.4.11**

A π egységtől és nullától különböző Gauss-egészt *Gauss-prím*nek nevezzük, ha **csak** úgy lehet osztója két Gauss-egész szorzatának, ha legalább az egyik tényezőnek osztója. Azaz

$$\pi \mid \alpha\beta \Longrightarrow \pi \mid \alpha \text{ vagy } \pi \mid \beta. \clubsuit$$

A Gauss-egészek körében is érvényes az 1.4.3 Tétel megfelelője, és az arra adott bizonyítás is szó szerint átvihető:

7.4.12 Tétel **T 7.4.12**

Egy Gauss-egész pontosan akkor Gauss-prím, ha Gauss-felbonthatatlan. $\clubsuit$

A továbbiakban ennek megfelelően általában a Gauss-felbonthatatlan helyett is a (rövidebb) Gauss-prím elnevezést fogjuk használni.

Most már minden készen áll az 1.5.1 Tétel megfelelőjének a kimondásához és bizonyításához:

7.4.13 Tétel (A számelmélet alaptétele) **T 7.4.13**

Minden, a 0-tól és egységektől különböző Gauss-egész felbontható véges sok Gauss-felbonthatatlan szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű. ♣

Bizonyítás: Az egyértelműségre az egész számoknál adott első bizonyítás szó szerint átvihető a Gauss-egészekre is (a második bizonyítás megfelelőjére nézve lásd a 7.4.11 feladatot).

A felbonthatóság bizonyításához is lényegében az egész számoknál szereplő gondolatmenetet alkalmazhatjuk, azzal a két apró módosítással, hogy „a legkisebb pozitív nemtriviális osztója" helyett „a(kármelyik) legkisebb normájú nemtriviális osztója", illetve $|a_i|$ helyett $N(\alpha_i)$ veendő. A részletek végiggondolását az Olvasóra bízzuk. ■

Megjegyzés: Összefoglalva megállapíthatjuk, hogy az egész számoknál és a Gauss-egészeknél szinte azonos módon jutottunk el a számelmélet alaptételéhez. A felbonthatóság bizonyítása mindkét számkörben közvetlenül történt (hasonló gondolatmenettel), az egyértelműség bizonyításához vezető út lépései pedig a következők voltak:

Maradékos osztás ⇒ létezik legnagyobb közös osztó (a „kitüntetett" értelemben) ⇒ minden felbonthatatlan egyben prím is ⇒ a számelmélet alaptételének az egyértelműségi része.

Később megmutatjuk, hogy a (megfelelő értelemben vett) maradékos osztás elvégezhetőségéből mindig következik a számelmélet alaptétele, de ez fordítva nem igaz (lásd a 11.3 pontot).

A továbbiakban célunk az összes Gauss-prím jellemzése, áttekintése. Ennek előkészítéseként kapcsolatot keresünk a Gauss-prímek és a ($\mathbf{Z}$-beli) prímszámok között:

7.4.14 Tétel **T 7.4.14**

(i) Minden π Gauss-prímhez pontosan egy olyan p pozitív prímszám létezik, amelyre $\pi \mid p$.

(ii) Minden p pozitív prímszám vagy maga is Gauss-prím, vagy pedig pontosan két Gauss-prímnek a szorzata, amelyek normája p, és amelyek egymás konjugáltjai. ♣

Bizonyítás: (i) Mivel $\pi \neq 0$ és π nem egység, ezért $N(\pi) > 1$, és így $N(\pi)$ felbontható pozitív prímszámok szorzatára: $N(\pi) = p_1 p_2 \dots p_r$. Ekkor

$$\pi \mid \pi\overline{\pi} = N(\pi) = p_1 p_2 \dots p_r,$$

továbbá π Gauss-prím, tehát π szükségképpen osztója valamelyik p_i-nek is.

Az egyértelműség igazolásához tegyük fel indirekt, hogy $p \neq q$ olyan pozitív prímszámok, amelyekre $\pi \mid p$ és $\pi \mid q$. Mivel p és q (az egész számok körében) relatív prímek, ezért alkalmas u és v egész számokkal $1 = pu + qv$ teljesül. Ekkor $\pi \mid p$ és $\pi \mid q$ miatt $\pi \mid pu + qv$, azaz $\pi \mid 1$ is fennáll, ami ellentmondás.

(ii) Ha a $p > 0$ prímszám nem Gauss-prím, akkor (a számelmélet alaptétele szerint) felírható legalább két Gauss-prím szorzataként:

$$p = \pi_1 \dots \pi_r, \qquad \text{ahol} \qquad r \geq 2. \tag{3}$$

A normákra áttérve, (3)-ból

$$p^2 = N(p) = N(\pi_1) \dots N(\pi_r) \tag{4}$$

következik. Mivel π_i nem egység, ezért $N(\pi_i) > 1$. A p^2 azonban csak egyféleképpen bontható 1-nél nagyobb egész számok szorzatára: $p^2 = p \cdot p$. Ebből következik, hogy (4), és így (3) jobb oldalán is csak két tényező szerepelhet:

$$p = \pi_1 \pi_2, \qquad \text{ahol} \qquad N(\pi_1) = N(\pi_2) = p.$$

Végül a

$$p = \pi_1 \pi_2 \qquad \text{és} \qquad p = N(\pi_1) = \pi_1 \overline{\pi_1}$$

egyenlőségekből kapjuk, hogy $\pi_2 = \overline{\pi_1}$. ■

És most lássuk a Gauss-prímek „listáját”:

7.4.15 Tétel **T 7.4.15**

Az alábbi Gauss-egészek adják az összes Gauss-prímet (ε tetszőleges egységet jelöl):

(A) $\varepsilon(1 + i)$;

(B) εq, ahol q pozitív $4k - 1$ alakú prímszám;

(C) π, ahol $N(\pi)$ egy pozitív $4k + 1$ alakú prímszám; minden ilyen prímszámhoz egységszerestől eltekintve két Gauss-prím tartozik, amelyek egymás konjugáltjai, de nem egymás egységszeresei. ♣

Példák:

A $-1+i=i(1+i)$ és $-7i$ Gauss-prímek.

Szintén Gauss-prím a $2-5i$, mert $(2-5i)(2+5i)=29$, és a 29 egy $4k+1$ alakú pozitív prímszám.

A $2+5i$ is Gauss-prím, amely nem egységszerese a $2-5i$-nek.

A $29=(5-2i)(5+2i)$ felbontás tényezői viszont (a számelmélet alaptétele szerint) már csak az előzők egységszeresei lehetnek, és valóban $5-2i=$ $=(-i)(2+5i)$, illetve $5+2i=i(2-5i)$.

Nem Gauss-prím a -37, mert a 37 (ugyan prímszám, de) nem $4k-1$ alakú.

A $9+2i$ sem Gauss-prím, mert $(9+2i)(9-2i)=85$ nem prímszám.

Bizonyítás: A 7.4.14 Tétel szerint az összes Gauss-prímet a pozitív prímszámoknak a Gauss-prímek szorzatára történő felbontásaiból kaphatjuk meg. Más és más típusú felbontást kapunk attól függően, hogy ez a pozitív prímszám (A) a 2; (B) $4k-1$ alakú; illetve (C) $4k+1$ alakú.

(A) Mivel $2=(1+i)(1-i)=(-i)(1+i)^2$, ezért a 2-nek egységszerestől eltekintve egyetlen Gauss-prím osztója van, az $1+i$.

(B) Legyen q pozitív $4k-1$ alakú prímszám. Tegyük fel indirekt, hogy q nem Gauss-prím. Ekkor a 7.4.14 Tétel (ii) állítása szerint van olyan $\pi=a+bi$ Gauss-prím, amelyre $q=N(\pi)=a^2+b^2$. Ez azonban lehetetlen, mert két négyzetszám összege nem lehet $4k-1$ alakú.

(C) Legyen p pozitív $4k+1$ alakú prímszám. Először azt igazoljuk, hogy p nem Gauss-prím.

A 4.1.4 Tétel szerint az $x^2\equiv -1 \pmod p$ kongruencia megoldható, azaz létezik olyan c egész szám, amelyre $p\mid c^2+1$. Ennek megfelelően a p a Gauss-egészek körében osztója a $(c+i)(c-i)$ szorzatnak. Ugyanakkor

$$\frac{c\pm i}{p}=\frac{c}{p}\pm\frac{1}{p}i$$

nem Gauss-egészek (mert például a képzetes részük nem egész szám), tehát a $c+i$ és $c-i$ tényezők egyike sem osztható p-vel. Ebből (a Gauss-prím definíciója szerint) következik, hogy a p nem Gauss-prím.

A 7.4.14 Tétel alapján ekkor $p=\pi\overline{\pi}$, ahol π és $\overline{\pi}$ Gauss-prímek. A számelmélet alaptétele szerint a p-nek egységszeresektől eltekintve ez az egyetlen felbontása Gauss-prímek szorzatára, így már csak azt kell igazolnunk, hogy $\pi\neq\varepsilon\overline{\pi}$, ahol ε egység. Ez egyszerű számolással adódik a $\pi=a+bi$ alakból az $\varepsilon=1$, -1, i és $-i$ esetek végigpróbálásával (valamint következik a 7.4.3 feladatból is). ■

Feladatok ($\alpha, \beta, a+bi$ stb. végig Gauss-egészt jelölnek.)

7.4.1 Mely Gauss-egészek oszthatók $1+i$-vel?

7.4.2 Igazoljuk az alábbi állításokat:

a) $\gamma \mid \alpha \iff \overline{\gamma} \mid \overline{\alpha}$;

b) $(\overline{\alpha}, \overline{\gamma}) = \overline{(\alpha, \gamma)}$;

c) α Gauss-prím $\iff$ $\overline{\alpha}$ Gauss-prím.

7.4.3 Legyen $\alpha = a+bi$. Mutassuk meg, hogy

$$\alpha \mid \overline{\alpha} \iff |a| = |b| \text{ vagy } ab = 0.$$

7.4.4 Ha a és $b \neq 0$ két egész szám, akkor a $b \mid a$ oszthatóságnál, illetve az (a, b) legnagyobb közös osztónál tulajdonképpen meg kellene mondani, hogy a-t és b-t most egész számoknak vagy pedig Gauss-egészeknek tekintjük. Bizonyítsuk be, hogy ez a megkülönböztetés fölösleges:

a) $b \mid a$ pontosan akkor igaz a Gauss-egészek körében, ha **Z**-ben igaz;

b) az a és b számok **Z**-beli legnagyobb közös osztója (egységszerestől eltekintve) megegyezik a Gauss-egészek körében vett legnagyobb közös osztóval.

7.4.5 Melyek igazak az alábbi állítások közül?

a) $\big(N(\alpha), N(\beta)\big) = 1 \Longrightarrow (\alpha, \beta) = 1$.

b) $(\alpha, \beta) = 1 \Longrightarrow \big(N(\alpha), N(\beta)\big) = 1$.

c) $(\alpha, \beta) = (\overline{\alpha}, \beta) = 1 \Longrightarrow \big(N(\alpha), N(\beta)\big) = 1$.

7.4.6 Számítsuk ki α és β legnagyobb közös osztóját, ahol

a) $\alpha = 8+i$ és $\beta = 11-3i$;

b) $\alpha = 39(1-i)^3$ és $\beta = 62(2+i)^3$;

c) $\alpha = (4+i)^{10} + (2+i)^{11}$ és $\beta = (4+i)^{10} - (2+i)^{11}$.

7.4.7 Legyen $\alpha = a+bi$.

a) Melyek igazak az alábbi állítások közül?

(a1) $(\alpha, \overline{\alpha}) = 1 \Longrightarrow (a, b) = 1$.

(a2) $(a, b) = 1 \Longrightarrow (\alpha, \overline{\alpha}) = 1$.

b) Milyen kapcsolatban áll egymással általában $(\alpha, \overline{\alpha})$ és (a, b)?

7.4.8 Nevezzük az α és β Gauss-egészeket barátoknak, ha relatív prímek, és egy („közönséges") egész szám pontosan akkor többszöröse α-nak, amikor β-nak.

a) Bizonyítsuk be, hogy $a+bi$-nek akkor és csak akkor létezik barátja, ha $(a,b)=1$ és $a \not\equiv b \pmod 2$.
b) Hány barátja van $a+bi$-nek ebben az esetben?

7.4.9 Bontsuk fel a $270+2610i$ Gauss-egészt Gauss-prímek szorzatára.

7.4.10 Melyek igazak az alábbi állítások közül?

a) Ha α Gauss-prím, akkor $N(\alpha)$ prímszám.
b) Ha $N(\alpha)$ prímszám, akkor α Gauss-prím.
c) Ha α egy Gauss-egész köbe, akkor $N(\alpha)$ egy nemnegatív egész szám köbe.
d) Ha $N(\alpha)$ egy nemnegatív egész szám köbe, akkor α egy Gauss-egész köbe.
e) Ha $\alpha \mid \overline{\alpha}$, akkor $N(\alpha)$ négyzetszám vagy egy négyzetszám kétszerese.
f) Ha $N(\alpha)$ négyzetszám vagy egy négyzetszám kétszerese, akkor $\alpha \mid \overline{\alpha}$.

*7.4.11 Bizonyítsuk be a számelmélet alaptételének egyértelműségi részét az 1.5.1 Tételben látott második bizonyítás mintájára.

7.5. Számok előállítása négyzetösszegként

Ebben a pontban azt vizsgáljuk meg, hogy mely pozitív egészek állnak elő két, három, illetve négy négyzetszám összegeként (összeadandóként a 0-t is megengedve).

7.5.1 Tétel (Két-négyzetszám-tétel) **T 7.5.1**

Legyen az n pozitív egész kanonikus alakja

$$n = 2^{\alpha} p_1^{\beta_1} \dots p_r^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s} \,, \tag{1}$$

ahol a p_μ prímek $4k+1$, a q_ν prímek $4k-1$ alakúak, és a szereplő α, β_μ, γ_ν kitevők nemnegatív egészek.

Az

$$x^2 + y^2 = n \tag{2}$$

diofantikus egyenlet akkor és csak akkor oldható meg, ha minden γ_ν páros, és ebben az esetben a megoldásszám

$$4 \prod_{\mu=1}^{r} (\beta_\mu + 1) \,. \ \clubsuit$$

A 7.3.1 Tételhez hasonlóan, a csak az előjelben eltérő megoldásokat is külön megoldásoknak tekintjük. Ebből most is könnyen megkaphatjuk a „lényegesen különböző" megoldások számát, lásd a 7.5.1 feladatot.

Példa: Legyen $n = 4050$. A 4050 kanonikus alakja $2 \cdot 3^4 \cdot 5^2$. Itt a 3 kitevője páros, tehát van megoldás, és a megoldásszám az 5 kitevőjéből $4(2+1) = 12$. A megoldások:

$$4050 = (\pm 45)^2 + (\pm 45)^2 = (\pm 9)^2 + (\pm 63)^2 = (\pm 63)^2 + (\pm 9)^2 .$$

Bizonyítás: Az $x^2 + y^2 = n$ egyenlet átírható az

$$(x + yi)(x - yi) = n \tag{3}$$

alakba. Ennek megfelelően azt kell megállapítani, hogy mely n-ek és hányféleképpen írhatók fel két olyan Gauss-egész szorzataként, amelyek egymás konjugáltjai.

Ehhez először meghatározzuk az n „kanonikus alakját" a Gauss-egészek körében. Ezen olyan

$$\varepsilon \varrho_1^{\kappa_1} \dots \varrho_t^{\kappa_t}$$

előállítást értünk, ahol a szereplő ϱ_j Gauss-prímek közül semelyik kettő sem egységszerese egymásnak és ε egység. Például a 4 kanonikus alakja $(-1)(1+i)^4$ vagy $(-1)(-1+i)^4$ stb. (A „külön" egységtényezőre az egész számok körében is szükség lehet, ha a kanonikus alakot a negatív egészekre is ki akarjuk terjeszteni: például -9 csak $(-1)3^2$ vagy $(-1)(-3)^2$ alakban írható fel ily módon.)

A 7.4.15 Tétel alapján az n (egyik) kanonikus alakja a Gauss-egészek körében

$$n = (-i)^\alpha (1+i)^{2\alpha} \pi_1^{\beta_1} \overline{\pi_1}^{\beta_1} \dots \pi_r^{\beta_r} \overline{\pi_r}^{\beta_r} q_1^{\gamma_1} \dots q_s^{\gamma_s} , \tag{4}$$

ahol $\pi_\mu \overline{\pi_\mu} = p_\mu$. (A (4) jobb oldalán szereplő Gauss-prímek közül semelyik kettő sem egységszerese egymásnak.)

Mivel $x + yi \mid n$, ezért (a számelmélet alaptétele szerint) $x + yi$ kanonikus alakja

$$x + yi = \varepsilon (1+i)^{\alpha'} \prod_{\mu=1}^{r} \left(\pi_\mu^{\beta'_\mu} \overline{\pi_\mu}^{\beta''_\mu} \right) \prod_{\nu=1}^{s} q_\nu^{\gamma'_\nu} , \tag{5}$$

ahol ε egység és minden Gauss-prím kitevője legfeljebb akkora, mint (4)-ben.

Az (5) egyenlőség konjugálásával és $1-i=(-i)(1+i)$ felhasználásával $x-yi$-ra az alábbi kanonikus alakot kapjuk:

$$x-yi=\left(\overline{\varepsilon}(-i)^{\alpha'}\right)(1+i)^{\alpha'}\prod_{\mu=1}^{r}\left(\pi_\mu^{\beta''_\mu}\,\overline{\pi_\mu}^{\beta'_\mu}\right)\prod_{\nu=1}^{s}q_\nu^{\gamma'_\nu}\,. \tag{6}$$

A számelmélet alaptétele szerint (3) pontosan akkor teljesül, ha (4)-ben minden Gauss-prím kitevője megegyezik az (5)- és (6)-beli megfelelő kitevők összegével, továbbá a (4)-beli „külön" egységtényező egyenlő az (5)- és (6)-beli ilyen egységtényezők szorzatával.

Ez az alábbi egyenlőségek teljesülését jelenti:

$1+i$ kitevője: $$2\alpha=\alpha'+\alpha' \tag{7a}$$

π_μ kitevője: $$\beta_\mu=\beta'_\mu+\beta''_\mu \tag{7b}$$

$\overline{\pi_\mu}$ kitevője: $$\beta_\mu=\beta''_\mu+\beta'_\mu \tag{7c}$$

q_ν kitevője: $$\gamma_\nu=\gamma'_\nu+\gamma'_\nu \tag{7d}$$

egység: $$(-i)^{\alpha}=\varepsilon\overline{\varepsilon}(-i)^{\alpha'} \tag{7e}$$

A (7a) egyenlőségből kapjuk, hogy $\alpha'=\alpha$, és ekkor (7e) is automatikusan teljesül tetszőleges ε esetén. A (7b) és (7c) ugyanazt jelentik, és pontosan akkor állnak fenn, ha

$$\beta'_\mu=0,1,\dots,\beta_\mu \quad \text{és} \quad \beta''_\mu=\beta_\mu-\beta'_\mu, \quad \mu=1,2,\dots,r.$$

Végül (7d) akkor és csak akkor elégíthető ki, ha γ_ν páros, és ekkor $\gamma'_\nu=\gamma_\nu/2$.

A fentiekből következik, hogy (2) akkor és csak akkor oldható meg, ha mindegyik γ_ν páros.

A megoldásszám azoknak a lehetőségeknek a száma, ahányféleképpen az ε, α', β'_μ, β''_μ és γ'_μ értékek megválaszthatók. A felsorolt ötféle „ismeretlen" választására egymástól függetlenül rendre 4, 1, $\beta_\mu+1$, 1, 1 lehetőség van, így (2) megoldásszáma ezek szorzata, azaz $4\prod_{\mu=1}^{r}(\beta_\mu+1)$. ■

7.5.2 Tétel (Három-négyzetszám-tétel) **T 7.5.2**

Az n pozitív egész akkor és csak akkor **nem** áll elő három négyzetszám összegeként, ha

$$n=4^k(8m+7) \tag{8}$$

alakú. ♣

Bizonyítás: Az állításnak csak azt a könnyebben adódó részét igazoljuk, hogy a (8)-beli számok nem állnak elő három négyzetszám összegeként, a másik irány igazolása jóval nehezebb.

A k szerinti teljes indukcióval bizonyítunk.

A $k = 0$ esetben azt kell megmutatni, hogy a $8m + 7$ alakú számok nem írhatók fel három négyzetszám összegeként. Ez abból következik, hogy egy négyzetszám 0, 1 vagy 4 maradékot ad 8-cal osztva, és három ilyen maradék összegeként sohasem kaphatunk 7 maradékot.

Tegyük most fel, hogy az állítás valamely k-ra igaz, és lássuk be, hogy ekkor $k + 1$-re is teljesül. Indirekt feltesszük, hogy léteznek olyan a, b és c egész számok, amelyekre

$$4^{k+1}(8m + 7) = a^2 + b^2 + c^2 \,. \tag{9}$$

A (9) bal oldala osztható 4-gyel. Egy négyzetszám 4-gyel osztva 0-t vagy 1-et ad maradékul, attól függően, hogy páros, illetve páratlan számot emeltünk négyzetre. Ezért a jobb oldal csak úgy lehet osztható 4-gyel, ha a, b és c mindegyike páros, tehát $a/2$, $b/2$ és $c/2$ egész számok. Így (9)-et 4-gyel elosztva

$$4^k(8m + 7) = \left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{c}{2}\right)^2$$

adódik, ami ellentmond az indukciós feltevésnek. ■

7.5.3 Tétel (Négy-négyzetszám-tétel) **T 7.5.3**

Minden pozitív egész felírható négy négyzetszám összegeként. ♣

Bizonyítás: Szükségünk lesz az alábbi két segédtételre:

7.5.4 Lemma **L 7.5.4**

Ha két szám felírható négy négyzetszám összegeként, akkor a szorzatuk is, nevezetesen

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \\ = (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 + \\ + (a_1b_3 - a_3b_1 - a_2b_4 + a_4b_2)^2 + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2 \,. \ \clubsuit\end{aligned} \tag{10}$$

7.5.5 Lemma **L 7.5.5**

Az

$$1 + x^2 + y^2 \equiv 0 \pmod{p} \tag{11}$$

kongruencia bármely p prímre megoldható. ♣

A 7.5.4 Lemma bizonyítása: A (10) azonosság egyszerű számolással ellenőrizhető. ■

Megjegyezzük, hogy (10) „természetes" módon adódik a *kvaterniók* felhasználásával: ha az α és β kvaterniók

$$\alpha = a_1 + a_2 i + a_3 j + a_4 k \qquad \text{és} \qquad \beta = b_1 + b_2 i + b_3 j + b_4 k\,,$$

akkor (10) éppen a (kvaternió)normákra vonatkozó $N(\alpha)N(\beta) = N(\beta\overline{\alpha})$ azonosság kifejtett alakja. (Természetesen $N(\alpha)N(\beta) = N(\alpha\beta)$ is alkalmas lett volna a 7.5.4 Lemma „szöveges" részének az igazolására, azonban ekkor (10) helyett egy másik azonosságot kaptunk volna, ugyanakkor a 7.5.3 Tétel bizonyításában magára a (10) képletre is szükségünk lesz.)

A 7.5.5 Lemma bizonyítása: Az állítás $p = 2$-re nyilvánvaló.

Tegyük fel indirekt, hogy valamely $p > 2$ prímre a (11) kongruenciának nincs megoldása, azaz bármely x és y egész esetén

$$x^2 \not\equiv -1 - y^2 \pmod{p}\,. \tag{12}$$

Ha x végigfut egy modulo p teljes maradékrendszer elemein, akkor az x^2 értékek a modulo p kvadratikus maradékokat és a 0 maradékosztály egy reprezentánsát adják. A 4.1.2 Tétel alapján így x^2-re

$$\frac{p-1}{2} + 1 = \frac{p+1}{2}$$

páronként inkongruens értéket kapunk.

Ugyanez érvényes y^2-re, és így $-1 - y^2$-re is. Ebből (12) alapján az következik, hogy megadható $2\frac{p+1}{2} = p + 1$ olyan szám, amelyek páronként inkongruensek modulo p, ami nyilvánvaló ellentmondás. ■

Megjegyezzük, hogy a 7.5.5 Lemma Chevalley tételéből (3.6.1 Tétel), illetve a 3.6.2 feladatból is könnyen levezethető (lásd a 7.5.19 feladatot).

Rátérünk a 7.5.3 Tétel bizonyítására. Nevezzünk a rövidség kedvéért egy pozitív egészt „szép”-nek, ha felírható négy négyzetszám összegeként.

Mivel az 1 és a 2 nyilván szép, ezért a 7.5.4 Lemma alapján elég azt megmutatni, hogy minden $p > 2$ prím is szép.

A p-nek létezik szép többszöröse, például a $4p^2$. Vegyük a legkisebb pozitív m-et, amelyre mp szép, legyen

$$mp = a_1^2 + a_2^2 + a_3^2 + a_4^2 \,. \tag{13}$$

Azt kell igazolnunk, hogy $m = 1$. Meg fogjuk mutatni, hogy $m > 1$ esetén létezik olyan m_1, amelyre $0 < m_1 < m$, és $m_1 p$ is szép. Ez azonban ellentmond m minimalitásának, és így valóban $m = 1$.

Először azt bizonyítjuk be, hogy $m < p$, azaz a p-nek létezik p^2-nél kisebb szép többszöröse. A 7.5.5 Lemma alapján a (11) kongruencia megoldható, és a modulo p legkisebb abszolút értékű maradékok rendszerét véve olyan x, y megoldást kapunk, amelyre $|x| < \frac{p}{2}$ és $|y| < \frac{p}{2}$. Ekkor

$$v = 1^2 + x^2 + y^2 + 0^2 \text{ szép}, \qquad p \mid v \qquad \text{és} \qquad 0 < v < 2\Big(\frac{p}{2}\Big)^2 + 1 < p^2 \,.$$

Most belátjuk, hogy m szükségképpen páratlan. Ellenkező esetben (13)-ból következik, hogy két-két a_ν, mondjuk a_1 és a_2, illetve a_3 és a_4 azonos paritású. Ekkor

$$\Big(\frac{m}{2}\Big)p = \Big(\frac{a_1 + a_2}{2}\Big)^2 + \Big(\frac{a_1 - a_2}{2}\Big)^2 + \Big(\frac{a_3 + a_4}{2}\Big)^2 + \Big(\frac{a_3 - a_4}{2}\Big)^2 \,,$$

ami ellentmond m minimalitásának.

A (13) egyenlőséget most modulo m fogjuk tekinteni. Legyen b_1, b_2, b_3, b_4 rendre az a_1, a_2, a_3, a_4 számok modulo m szerinti legkisebb abszolút értékű maradéka, azaz

$$b_\nu \equiv a_\nu \pmod{m}, \qquad |b_\nu| \le \frac{m-1}{2}, \qquad \nu = 1, 2, 3, 4. \tag{14}$$

Ekkor

$$b_1^2 + b_2^2 + b_3^2 + b_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m} \,,$$

azaz alkalmas m_1 egésszel

$$mm_1 = b_1^2 + b_2^2 + b_3^2 + b_4^2 \tag{15}$$

teljesül. Megmutatjuk, hogy (15)-ben $0 < m_1 < m$.

Ha $m_1 = 0$, akkor mindegyik $b_\nu = 0$, azaz mindegyik a_ν osztható m-mel. Ebből következik, hogy

$$m^2 \mid a_1^2 + a_2^2 + a_3^2 + a_4^2 = mp, \qquad \text{tehát} \qquad m \mid p\,,$$

ami $1 < m < p$ miatt lehetetlen.

Az $m_1 < m$ egyenlőtlenség az

$$mm_1 = \sum_{\nu=1}^{4} b_\nu^2 \le 4\Big(\frac{m-1}{2}\Big)^2 < 4\Big(\frac{m}{2}\Big)^2 = m^2$$

összefüggésből következik.

A (13) és (15) egyenlőségeket összeszorozva és (10)-et felhasználva azt kapjuk, hogy

$$m^2 m_1 p = c_1^2 + c_2^2 + c_3^2 + c_4^2\,, \tag{16}$$

ahol a c_ν számok (10)-ből olvashatók le.

Belátjuk, hogy mindegyik c_ν osztható m-mel. Mivel $b_\nu \equiv a_\nu \pmod m$, ezért

$$c_1 = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 = mp \equiv 0 \pmod m\,,$$

és hasonlóan adódik az m-mel való oszthatóság a többi c_ν-re is.

Így (16)-ot m^2-tel elosztva azt nyerjük, hogy m_1p is felírható négy négyzetszám összegeként, ami $0 < m_1 < m$ miatt ellentmond m minimalitásának. ■

Megjegyzés: A bizonyítás során használt módszer az ún. *végtelen leszállás* egyik változata volt. Az elnevezés magyarázata világosabbá válik a gondolatmenetünk alábbi átfogalmazásából: Ha maga a p nem szép, akkor tekintve a p-nek egy szép mp (pozitív) többszörösét, találunk egy másik szép m_1p többszöröst, ahol $0 < m_1 < m$, majd ugyanígy ehhez is találunk egy szép m_2p többszöröst, ahol $0 < m_2 < m_1$ stb. Ez azt jelenti, hogy pozitív egészekből egy végtelen, szigorúan monoton fogyó sorozatot kapunk (vagyis a pozitív egészek körében egy „végtelen leszállást" hajtunk végre), ami nyilván lehetetlen.

A végtelen leszállás a pozitív egészekre nézve leginkább egy indirekt teljes indukciós bizonyításhoz hasonlít. Az 1.5.1 Tételnél az egyértelműségi rész második bizonyítása is tulajdonképpen egy végtelen leszállást takart.

A teljes indukcióval való rokonsága ellenére a végtelen leszállás más elven alapul: az ún. *jólrendezési* tulajdonságot használja fel, vagyis azt, hogy bármely részhalmaznak van minimális eleme, tehát nem képezhető végtelen

leszálló sorozat. Így ha valamilyen tulajdonság ilyen végtelen leszállással öröklődik, akkor egy jólrendezett halmaz egyetlen eleme sem rendelkezhet ezzel a tulajdonsággal.

Mivel a *kiválasztási axiómá*ból következik, hogy bármely halmaz jólrendezhető, ezért a végtelen leszállás a halmazok jóval szélesebb körében alkalmazható, mint a teljes indukció.

Feladatok

7.5.1 Hány „lényegesen különböző módon" állítható elő egy adott pozitív egész két négyzetszám összegeként? (A 7.5.1 Tétel utáni példában szereplő 4050 kétféleképpen: $4050 = 45^2 + 45^2 = 9^2 + 63^2$.)

7.5.2 Hány olyan Gauss-egész létezik, amelynek a normája 98 000?

7.5.3 Melyik az a legnagyobb r, amelyre igaz, hogy végtelen sokszor előfordul r egymást követő szám, amelyek mindegyike felírható két négyzetszám összegeként vagy különbségeként?

7.5.4 Adjunk új bizonyítást a 4.1.5 feladat állítására.

7.5.5 Mely n-ekre oldható meg és hány megoldása van az $x^2 + 4y^2 = n$ diofantikus egyenletnek?

*7.5.6 Mely pozitív egészek írhatók fel és hányféleképpen két *relatív prím* szám négyzetének az összegeként?

*7.5.7

a) Hány olyan (páronként nem egybevágó) derékszögű háromszög létezik, amelynek az oldalai egész számok és az egyik oldal hossza k?

b) Mi a válasz akkor, ha még azt is feltesszük, hogy az oldalhosszak relatív prímek?

7.5.8 Mutassuk meg, hogy az $x^2 + y^2 = n$ diofantikus egyenlet megoldásszáma $4d'(n) - 4d''(n)$, ahol $d'(n)$, illetve $d''(n)$ az n pozitív egész $4k + 1$, illetve $4k - 1$ alakú pozitív osztóinak a számát jelöli.

*7.5.9 Átlagosan hányféleképpen írható fel egy pozitív egész két egész szám négyzetének az összegeként? Más megfogalmazásban ez az

$$\frac{r(1) + r(2) + \ldots + r(n)}{n}$$

középértékfüggvény viselkedését jelenti „nagy" n esetén, ahol $r(n)$ az $x^2 + y^2 = n$ diofantikus egyenlet megoldásszáma.

M*7.5.10 Oldjuk meg az $x^2 + 4 = y^3$ diofantikus egyenletet.

M*7.5.11 Mely Gauss-egészek írhatók fel két Gauss-egész négyzetének az összegeként?

7.5.12 A 7.5.1 Tétel bizonyítása során Gauss-egészekre is definiáltunk kanonikus alakot, és láttuk, hogy egy Gauss-egésznek több kanonikus alakja is lehet. Mutassuk meg, hogy bármely, 0-tól és egységektől különböző Gauss-egész kanonikus alakjainak a száma a 4-nek pozitív egész kitevős hatványa. (Két kanonikus alakot azonosnak tekintünk, ha csak a tényezők sorrendjében térnek el, és természetesen kizárjuk, hogy a kanonikus alakban egy Gauss-prím nulladik hatványon forduljon elő.)

7.5.13 Melyek igazak az alábbi állítások közül?

a) Ha két pozitív egész felírható két négyzetszám összegeként, akkor a szorzatuk is ilyen tulajdonságú.

b) Ha két pozitív egész szorzata felírható két négyzetszám összegeként, akkor külön-külön a két tényező is ilyen tulajdonságú.

c) Ha két pozitív egész szorzata és az egyik tényező felírható két négyzetszám összegeként, akkor a másik tényező is ilyen tulajdonságú.

d) Ha két pozitív egész felírható három négyzetszám összegeként, akkor a szorzatuk is ilyen tulajdonságú.

*7.5.14 Mi a valószínűsége annak, hogy egy pozitív egész előáll három négyzetszám összegeként?

7.5.15 Melyik az a legkisebb r, amelyre igaz, hogy minden elég nagy pozitív egész felírható legfeljebb r darab páratlan négyzetszám összegeként?

7.5.16 Vezessük le a három-négyzetszám-tételből a négy-négyzetszám-tételt.

M 7.5.17 Mely pozitív egészek állnak elő négy négyzetszám összegeként úgy, hogy az összeadandók között van (legalább) két azonos?

7.5.18 Megoldható-e az $x^2 + 9y^2 + z^2 + w^2 = 10^{11} + 23$ diofantikus egyenlet?

7.5.19 Igazoljuk a 7.5.5 Lemmát Chevalley tétele (3.6.1 Tétel), illetve a 3.6.2 feladat felhasználásával.

7.5.20 A 7.5.1 Tételből következik, hogy minden $4k + 1$ alakú pozitív prím felírható két négyzetszám összegeként. Adjunk erre a tényre új bizonyítást a 7.5.3 Tételnél látott gondolatmenet alapján.

*7.5.21 A feladat célja a négy-négyzetszám-tétel egy másik bizonyításának a bemutatása. Ennél is felhasználjuk a 7.5.4 és 7.5.5 Lemmákat,

de a végtelen leszállás helyett az alábbi a) részben szereplő állítás segítségével kapjuk meg a p prímnek egy „kicsi” szép többszörösét.

a) *Thue-lemma.* Két egész koordinátájú k-dimenziós vektort akkor nevezünk kongruensnek modulo egy p prímszám, ha a megfelelő koordinátáik kongruensek modulo p. Legyen C tetszőleges $k \times k$-as egész elemű mátrix és $u_1, \dots, u_k, v_1, \dots, v_k$ olyan pozitív egészek, amelyekre

$$u_1 \dots u_k v_1 \dots v_k > p^k .$$

Ekkor léteznek olyan $\underline{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \neq \underline{0}$ és $\underline{z} = \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix}$ egész elemű vektorok, amelyekre

$$C\underline{x} \equiv \underline{z} \pmod{p} \qquad \text{és} \qquad |x_i| < u_i, \quad |z_i| < v_i, \quad i = 1, 2, \dots, k.$$

b) Az a) rész (alkalmas $k = 2$ speciális esete) és a 7.5.5 Lemma segítségével mutassuk meg, hogy tetszőleges p prímnek létezik $4p$-nél kisebb szép pozitív többszöröse.

c) Végül igazoljuk, hogy ha egy $p > 3$ prímre $2p$ vagy $3p$ szép, akkor p is az.

7.6. A Waring-problémakör

A négyzetek után a magasabb hatványok összegeként történő előállítással foglalkozunk. Ebben a pontban k végig 1-nél nagyobb pozitív egészt jelöl, és k-adik hatványon *nemnegatív* egész számok k-adik hatványát fogjuk érteni.

Waring 1770-ben azt állította, hogy „minden szám felírható 4 négyzetszám, 9 köbszám, 19 negyedik hatvány stb. összegeként”. A nagyvonalúan odavetett „stb.” szócska két súlyos problémát is takar. Egyrészt a $4, 9, 19$ számokról nemigen látszik valami jól folytatható szabályszerűség, másrészt az sem világos, hogy ez a számsor egyáltalán folytatható a végtelenségig. Ez utóbbihoz a következőt kell megmutatni: Bármely k-hoz létezik olyan, csak a k-tól függő r, hogy *minden* pozitív egész felírható r darab k-adik hatvány összegeként. Ezt az állítást először Hilbert igazolta 1909-ben.

Ma már (később részletezendő minimális bizonytalanságtól eltekintve) tudjuk, hogyan folytatódik a Waring-féle számsor. Érdekes módon a 19 negyedik hatvány problémája állt ellen legtovább az ostromnak, ennek helyességét csak 1986-ban sikerült bizonyítani.

Mivel bármely szám k-adik hatványok összegeként történő előállítását kiegészíthetjük tetszőleges számú 0^k taggal, ezért a *legkisebb* olyan darabszámot akarjuk meghatározni, hogy annyi k-adik hatvány már minden pozitív egész előállításához elegendő legyen:

7.6.1 Definíció **D 7.6.1**

Legyen $k > 1$. Ekkor $g(k)$ a *legkisebb* olyan r, hogy minden pozitív egész felírható r darab nemnegatív egész szám k-adik hatványának összegeként. ♣

Példa: $g(2) = 4$, ugyanis egyrészt a négy-négyzetszám-tétel szerint minden pozitív egész négy négyzetszám összege, másrészt van olyan szám, például a 7, amelynek az előállításához három négyzetszám nem elegendő.

7.6.2 Tétel **T 7.6.2**

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2\,. \quad \clubsuit \tag{1}$$

Bizonyítás: A $g(k)$-ra vonatkozó alsó becsléshez elég egyetlen olyan n pozitív egészt találni, amelynek az előállításához „sok” k-adik hatványra van szükség.

Legyen n a legnagyobb olyan $t2^k - 1$ alakú szám, amely kisebb, mint 3^k. Ekkor n felírásához csak (0^k,) 1^k és 2^k tagok állnak rendelkezésre, és ezekből nyilván az

$$n = t2^k - 1 = \underbrace{2^k + \ldots + 2^k}_{t-1 \text{ darab}} + \underbrace{1^k + \ldots + 1^k}_{2^k-1 \text{ darab}}$$

előállítás használja fel a legkevesebbet. Innen azt kapjuk, hogy

$$g(k) \geq 2^k + t - 2\,.$$

Így már csak azt kell igazolni, hogy $t = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor$. Ez abból következik, hogy

$$t2^k - 1 < 3^k \iff t2^k \leq 3^k \iff t \leq \left(\frac{3}{2}\right)^k, \tag{2}$$

továbbá t a (2)-t kielégítő legnagyobb egész szám. ■

A $g(k)$-ra vonatkozó legfontosabb eredmény az, hogy (1)-ben általában egyenlőség teljesül: csak véges sok olyan k létezhet, amelyre $g(k)$ nagyobb az (1) jobb oldalán megadott értéknél. Ez csak olyan k esetén következhet

be, amikor $(3/2)^k$ (egy pontosan felírható egyenlőtlenséget kielégítve) „abnormálisan" közel esik a felső egészrészéhez. A 471600000-nél kisebb számok között egyetlenegy sem teljesíti ezt a feltételt, és csaknem biztosra vehető, hogy nincsenek is ilyen kivételek, azaz minden k-ra

$$g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2\,.$$

Ennek megfelelően (1) jobb oldala jelenti a Waring-féle számsor folytatását (speciálisan a $k = 2$, 3 és 4 esetben rendre a 4, 9, illetve 19 értékeket kapjuk).

A 7.6.2 Tétel azt mutatja, hogy egyes „kis" n-ek előállítása igen sok k-adik hatványt igényel. Ezért érdemes azt is megvizsgálni, hogy minimálisan hány k-adik hatvány szükséges minden *elég nagy* n felírásához:

7.6.3 Definíció **D 7.6.3**

Legyen $k > 1$. Ekkor $G(k)$ a *legkisebb* olyan s, hogy minden *elég nagy* pozitív egész felírható s darab nemnegatív egész szám k-adik hatványának összegeként. ♣

Példa: $G(2) = 4$, ugyanis egyrészt nyilván $G(2) \le g(2) = 4$, másrészt a három-négyzetszám-tétel szerint *végtelen sok* olyan szám létezik, amelynek az előállításához három négyzetszám nem elegendő.

Az alábbi táblázatban bemutatjuk a $g(k)$-ra és $G(k)$-ra vonatkozó eredményeket néhány kis k esetén:

k	2	3	4	5	6	7	8
$g(k)$	4	9	19	37	73	143	279
$G(k)$	4	4–7	16	6–17	9–24	8–33	32–42

A táblázat jól érzékelteti, hogy már kis k esetén is igen nagy a bizonytalanság a $G(k)$ pontos értékét illetően (például $G(3)$-nál a 4–7 jelölés azt jelenti, hogy $G(3)$-ra csak a $4 \le G(3) \le 7$ becslés ismert). A $G(k)$ pontos értékét eddig csak a $k = 2$ és 4 esetekben sikerült meghatározni.

Az viszont kiderült, hogy nagy k esetén $G(k)$ értéke jóval kisebb $g(k)$-nál: például minden $k >$ 1-re fennáll $G(k) < 6k \log k$. (A jelenlegi legjobb eredmény szerint bármely $\varepsilon > 0$-hoz létezik olyan $k_0 = k_0(\varepsilon)$, hogy minden $k > k_0$

esetén $G(k) < (1+\varepsilon)k\log k$.) Így az exponenciális nagyságrendű $g(k)$-val szemben $G(k)$ „csaknem" lineáris.

Az alábbiakban alsó becsléseket adunk $G(k)$-ra.

7.6.4 Tétel **T 7.6.4**

Minden $k > 1$ esetén $G(k) \geq k+1$. ♣

Bizonyítás: Tegyük fel indirekt, hogy valamely k-ra $G(k) \leq k$. Ekkor létezik olyan n_0, hogy minden $n \geq n_0$ egész szám felírható k darab k-adik hatvány összegeként, azaz

$$n = x_1^k + x_2^k + \ldots + x_k^k\,. \tag{3}$$

Tekintsünk egy tetszőleges M („nagy") pozitív egészt, és jelöljük $f(M)$-mel azoknak az n-eknek a számát, amelyekre

$$0 \leq n \leq M, \tag{4}$$

és n előáll k darab k-adik hatvány összegeként. Az indirekt feltevés szerint cf

$$f(M) \geq M - n_0\,. \tag{5}$$

Most felső becslést keresünk $f(M)$-re. A (4)-beli n-eket tekintve, ezek (3) típusú előállításában csak olyan x_i számok szerepelhetnek, amelyekre

$$0 \leq x_i \leq \sqrt[k]{n} \leq \sqrt[k]{M}, \qquad i = 1, 2, \ldots, k.$$

Ez azt jelenti, hogy mindegyik x_i értéke csak

$$0,\ 1,\ \ldots,\ T = \left\lfloor \sqrt[k]{M} \right\rfloor \tag{6}$$

lehet.

Mindebből következik, hogy a $0, 1, \ldots, M$ egészek közül legfeljebb annyi írható fel k darab k-adik hatvány összegeként, ahányféleképpen a (6)-beli elemek közül k darabot ki tudunk választani úgy, hogy egy elemet többször is kiválaszthatunk, és a kiválasztás sorrendjére nem vagyunk tekintettel (ugyanis (3)-ban az összeadandók között lehetnek azonosak is, továbbá a tagok permutálása esetén az összeg ugyanazt az n-et állítja elő).

Az ilyen típusú kiválasztás az ismétléses kombináció, tehát a jelzett kiválasztások száma a (6)-beli $T+1$ elem k-adosztályú ismétléses kombinációinak a száma, azaz $\binom{T+k}{k}$. A teljesség kedvéért részletezzük ennek a bizonyítását.

Egy ilyen kombinációt azzal jellemezhetünk, hányszor választjuk ki az egyes (6)-beli elemeket. Jelöljük m_j-vel, ahány j szerepel a kiválasztásban, $j = 0, 1, \ldots, T$. Rajzoljunk egymás mellé m_0 kis kört az m_0 darab 0-nak megfelelően, majd utána egy | elválasztó vonalat. Ezután m_1 kis kör következik az m_1 darab 1-est jelképezve, majd egy újabb | elválasztó vonal stb. A sort m_T kis körrel zárjuk, mert ennyi T lett kiválasztva. Tekintsük pl. a $k = 5$ és $M = 7^5$ esetet, ekkor a $0^5+1^5+1^5+3^5+7^5$ (formális) összegnek a $\circ|\circ\circ||\circ||||\circ$ jelsorozat felel meg.

Ezzel kölcsönösen egyértelmű megfeleltetést hoztunk létre a formális összegek és a k körből és $T = \left\lfloor \sqrt[k]{M} \right\rfloor$ elválasztóvonalból álló sorozatok között. Ezért a formális összegek száma megegyezik az ilyen sorozatok számával, ami $\binom{T+k}{k} = \binom{\lfloor \sqrt[k]{M} \rfloor + k}{k}$.

Mindezeket összefoglalva, azt igazoltuk, hogy

$$f(M) \le \binom{k + \lfloor \sqrt[k]{M} \rfloor}{k}. \tag{7}$$

Az (5) és (7) egyenlőtlenségekből

$$M - n_0 \le \binom{k + \lfloor \sqrt[k]{M} \rfloor}{k} \tag{8}$$

következik. Írjuk be (8) jobb oldala helyett az

$$\frac{1}{k!}\big(k + \lfloor \sqrt[k]{M} \rfloor\big)\big(k - 1 + \lfloor \sqrt[k]{M} \rfloor\big) \ldots \big(1 + \lfloor \sqrt[k]{M} \rfloor\big)$$

képletet, hagyjuk el az egészrész jeleket (ezzel (8) jobb oldalát nem csökkentettük), majd osszuk el mindkét oldalt M-mel oly módon, hogy az $i + \sqrt[k]{M}$ tényezők mindegyikét $\sqrt[k]{M}$-mel osztjuk. Ekkor az

$$1 - \frac{n_0}{M} \le \frac{1}{k!}\left(1 + \frac{k}{\sqrt[k]{M}}\right)\left(1 + \frac{k-1}{\sqrt[k]{M}}\right) \ldots \left(1 + \frac{1}{\sqrt[k]{M}}\right) \tag{9}$$

egyenlőtlenséghez jutunk. Ha $M \to \infty$, akkor (9) bal oldala 1-hez, jobb oldala pedig $1/k!$-hoz tart, ami $k > 1$ miatt ellentmondás. ■

Megjegyzés: A bizonyításból az is kiderült, hogy „nagyon sok" olyan n van, amely nem írható fel k darab k-adik hatvány összegeként (például már

$k = 5$ esetén is a számok „legalább $\dfrac{5!-1}{5!} = \dfrac{119}{120}$-ad része”, azaz „több, mint 99 százaléka” ilyen). Ugyanakkor a bizonyítás nem volt „konstruktív”: egyetlen „konkrét” n-ről sem mutatta ki, hogy n nem áll elő a kívánt alakban.

Most megmutatjuk, hogy a 7.6.4 Tétel becslése például $k = 6$ esetén javítható:

7.6.5 Tétel **T 7.6.5**

$$G(6) \geq 9. \quad \clubsuit$$

Bizonyítás: Felhasználjuk, hogy bármely a egészre

$$a^6 \equiv \begin{cases} 1 \pmod 9, & \text{ha } 3 \nmid a; \\ 0 \pmod 9, & \text{ha } 3 \mid a. \end{cases} \tag{10}$$

A $3 \nmid a$ eset az Euler–Fermat-tételből következik, a $3 \mid a$ esetben pedig a^6 nemcsak 9-cel, hanem 3^6-nal is osztható.

A 7.6.5 Tétel állításához azt kell igazolnunk, hogy végtelen sok olyan n létezik, amely nem írható fel 8 darab hatodik hatvány összegeként. Megmutatjuk, hogy például az $n = 27t + 9$ alakú számok ilyenek.

Tegyük fel indirekt, hogy

$$n = x_1^6 + \ldots + x_8^6 . \tag{11}$$

Tekintsük (11)-et modulo 9, ekkor (10) alapján azt kapjuk, hogy

$$0 \equiv u_1 + \ldots + u_8 \pmod 9, \quad \text{ahol} \quad u_i = 0 \text{ vagy } 1, \quad i = 1, 2, \ldots, 8. \tag{12}$$

A (12) kongruencia nyilván csak úgy teljesülhet, ha minden i-re $u_i = 0$. Ez azt jelenti, hogy mindegyik x_i osztható 3-mal. Ekkor azonban (11) alapján $3^6 \mid n$, ami ellentmondás. ■

A $G(k)$-ra vonatkozó további alsó becslések szerepelnek a 7.6.2 feladatban.

Feladatok

7.6.1 Mutassuk meg, hogy $G(200) \leq G(600)$.

*7.6.2

a) Igazoljuk a $G(k)$-ra vonatkozó alábbi alsó becsléseket:

(a1) $G(4) \geq 16$; (a2) $G(8) \geq 32$; (a3) $G(24) \geq 32$;

(a4) $G(100) \geq 125$; (a5) $G(250) \geq 312$.

b) Mely k értékekre általánosíthatók az a)-beli becslések?

7.6.3 Legyen $k > 1$ tetszőleges. Bizonyítsuk be, hogy van olyan n pozitív egész, amely legalább 1000 („lényegesen") különböző módon felírható $k+1$ darab k-adik hatvány összegeként.

7.6.4

a) Igazoljuk az alábbi azonosságot (a_1, a_2, a_3, a_4 tetszőleges komplex számok):

$$\sum_{1 \leq i < j \leq 4} \left((a_i + a_j)^4 + (a_i - a_j)^4\right) = 6(a_1^2 + a_2^2 + a_3^2 + a_4^2)^2 .$$

b) Bizonyítsuk be, hogy $g(4) \leq 53$.

7.6.5 Ha a számokat k-adik hatványok *előjeles* összegeként állítjuk elő, akkor általában $g(k)$-nál, illetve $G(k)$-nál kevesebb számú tag is elegendő. Mutassuk meg, hogy $k = 2$ esetén a minimális darabszám 3, ráadásul az $x^2 + y^2 - z^2 = n$ és $x^2 - y^2 - z^2 = n$ diofantikus egyenleteknek bármely n pozitív egész esetén végtelen sok megoldása van.

7.7. A Fermat-sejtés

A 7.2 pontban láttuk, hogy az $x^2 + y^2 = z^2$ pitagoraszi egyenletnek végtelen sok pozitív egész megoldása van (és az összes megoldás leírható három paraméter segítségével). Fermat-nak a közelmúltban igazolt híres sejtése szerint magasabb hatványokra alapvetően más a helyzet:

7.7.1 Tétel (Fermat-sejtés, Wiles tétele) **T 7.7.1**

Ha $k > 2$ egész szám, akkor az $x^k + y^k = z^k$ egyenlet nem oldható meg pozitív (vagy ami ezzel ekvivalens, nullától különböző) egészekben. ♣

A sejtés története 1637-ben kezdődött, amikor Diophantosz könyvének 1621-es kiadását olvasgatva, a pitagoraszi számhármasokról szóló résznél Fermat a következő bejegyzést tette: „Két köbszám összege sohasem lehet köbszám, két negyedik hatvány összege sohasem lehet negyedik hatvány stb. Erre egy csodálatos bizonyítást találtam, sajnos a margón kevés a hely ahhoz, hogy leírhassam."

Ez a néhány sor három és fél évszázadon keresztül matematikusok és laikusok egész seregét tartotta izgalomban. Mivel maga a rendkívül egyszerűen hangzó probléma minden matematikai előképzettség nélkül is megérthető, ezért igen sok műkedvelő is próbálkozott a megoldással, mindhiába. Nem ment sokkal jobban a dolog a „profi" matematikusoknak sem.

Könnyen adódik (lásd a 7.7.1 feladatot), hogy ha a sejtés igaz egy adott k kitevőre, akkor a k minden többszörösére is igaz, ennélfogva elég a $k = 4$ és $k = p =$ prím eseteket tisztázni. Fermat-nál (valóban) megtalálható a $k = 4$ eset bizonyítása, majd jó száz évvel később Euler a $k = 3$ kitevővel is boldogult. A 19. század első felében további néhány konkrét k értékre sikerült megoldani a problémát, majd a század közepén lényeges áttörést hozott az „ideális számok", mai szóhasználattal az *ideál*ok bevezetése, amelyekről a 11. fejezetben lesz részletesen szó. Ezt továbbfejlesztve számos olyan kritériumot dolgoztak ki, amelyek teljesülése esetén a Fermat-sejtés arra az adott k(=prím) kitevőre igaz. Ezek a kritériumok (elvileg) bármely konkrét k értékre numerikusan ellenőrizhetők, és ez az ellenőrzés szorgalmasan folyt is (az utóbbi évtizedekben már számítógépek segítségével).

Mindezek ellenére a 20. század hetvenes éveiben is csak véges sok prím kitevőre nyert bizonyítást a sejtés. Közben rengeteg még általánosabb sejtés született, mert várható volt, hogy a megoldás a Fermat-egyenletnél általánosabb problémára vonatkozó tételből következik majd.

Óriási szenzációt jelentett 1983-ban Gerd Faltings eredménye: a Fermat-egyenletnek bármely k kitevő esetén csak véges sok *primitív* (azaz $(x, y, z) = 1$ típusú) megoldása lehet.

Az igazi szenzációt azonban Andrew Wiles okozta 1993-ban, aki sokéves titokban végzett kutatás után a probléma végleges megoldásával rukkolt elő. Később kiderült, hogy a bizonyítás egy lényeges ponton hibás, de a hibát Wilesnak (Richard Taylor segítségével) 1994-ben sikerült kijavítania.

Így a Fermat-sejtés mára lekerült a híres megoldatlan problémák listájáról. Wiles sok száz oldalas bizonyítása a matematikusok csak egy igen szűk csoportja számára érthető, de remélhetőleg később születnek majd egyszerűbb bizonyítások is.

Ami Fermat „csodálatos bizonyítását" illeti, az minden bizonnyal csak vagy egy végig nem gondolt ötlet lehetett, vagy pedig egy hibás gondolatmenet volt, amely tulajdonképpen a számelmélet alaptételének érvényességét olyan számkörben is feltételezte, ahol ez nem teljesül (lásd bővebben a 11.2 pontban). Továbbra is gyakorlatilag kizárható, hogy a Fermat-sejtésre valaki egy „igazi elemi" bizonyítást találjon.

A Fermat-sejtés több évszázados kutatása során a matematikusok számos hatékony, új elméletet dolgoztak ki a probléma kezelésére, amelyek a

sejtés szempontjából ugyan csak részleges sikert hoztak, a matematika más területein azonban nélkülözhetetlenné váltak. Ez is jól mutatja, hogy egy adott probléma vizsgálata gyakran ilyen közvetett módon segíti elő az egész matematika fejlődését.

Az alábbiakban (a történeti sorrendet is követve) bebizonyítjuk a Fermat-sejtésnek a $k = 4$ és 3 kitevőkre vonatkozó két legegyszerűbb speciális esetét.

Mindkét esetben valamivel erősebb eredményt igazolunk, mégpedig azért, mert valójában az eredeti kérdés megoldásához is csak ilyen (vagy hasonló) erősebb tételeknek a bizonyításával tudunk eljutni.

A Fermat-sejtés $k = 4$ kitevős esete nyilván következik az alábbi tételből:

7.7.2 Tétel **T 7.7.2**

Az $x^4 + y^2 = z^4$ egyenletnek nem létezik pozitív egész megoldása. ♣

Bizonyítás: Az alábbi, önmagában is érdekes lemmát használjuk fel:

7.7.3 Lemma **L 7.7.3**

Két (nemnulla) négyzetszám összege és különbsége nem lehet egyszerre négyzetszám. ♣

A lemma bizonyítása: A végtelen leszállás módszerét használjuk (lásd a 7.5.3 Tétel utáni megjegyzést).

Tekintsük az

$$x^2 + y^2 = z^2 \tag{1a}$$

$$x^2 - y^2 = w^2 \tag{1b}$$

egyenletrendszert. A bizonyítás során megoldáson mindig pozitív egész megoldást fogunk érteni. Legyen x_0, y_0, z_0, w_0 egy olyan megoldás, ahol z_0 értéke a lehető legkisebb. Megmutatjuk, hogy ekkor létezik olyan x_1, y_1, z_1, w_1 megoldás, ahol $(0 <)z_1 < z_0$, ami nyilvánvalóan ellentmond z_0 minimalitásának.

Feltehetjük, hogy $(x_0, z_0) = 1$. Ha ugyanis egy p prím osztója x_0-nak és z_0-nak, akkor (1a)-ból a pitagoraszi számhármasoknál látott módon következik, hogy $p \mid y_0$, majd ugyanígy (1b)-ből kapjuk, hogy $p \mid w_0$, és ekkor az x_0/p, y_0/p, z_0/p, w_0/p számnégyes olyan megoldás, ahol $z_0/p < z_0$, ami ellentmond z_0 minimalitásának.

Az (1a) és (1b) egyenletekbe az x_0, y_0, z_0, w_0 megoldást behelyettesítve és a két egyenlőséget összeadva, illetve kivonva

$$2x_0^2 = z_0^2 + w_0^2 \tag{2a}$$

és

$$2y_0^2 = z_0^2 - w_0^2 \tag{2b}$$

adódik. (2a)-ból (is) látszik, hogy z_0 és w_0 azonos paritású. Ennek alapján (2a) átírható az

$$x_0^2 = \left(\frac{z_0 + w_0}{2}\right)^2 + \left(\frac{z_0 - w_0}{2}\right)^2 \tag{3}$$

alakba. Itt

$$\left(x_0\,,\,\frac{z_0 + w_0}{2}\,,\,\frac{z_0 - w_0}{2}\right) = 1\,, \tag{4}$$

mivel x_0 relatív prím a másik két szám összegéhez, z_0-hoz.

(3) és (4) alapján $\dfrac{z_0 + w_0}{2}$, $\dfrac{z_0 - w_0}{2}$ és x_0 primitív pitagoraszi számhármast alkot. A 7.2.1 Tétel szerint ekkor léteznek olyan ellentétes paritású és relatív prím $m > n > 0$ egészek, amelyekre

$$\frac{z_0 + w_0}{2} = 2mn \qquad \text{és} \qquad \frac{z_0 - w_0}{2} = m^2 - n^2\,, \tag{5}$$

vagy fordítva.

A (2b)-vel ekvivalens

$$\frac{y_0^2}{2} = \frac{z_0 + w_0}{2} \cdot \frac{z_0 - w_0}{2}$$

egyenlőség jobb oldalát írjuk át (5) felhasználásával, ekkor 2-vel történő egyszerűsítés után azt kapjuk, hogy

$$\left(\frac{y_0}{2}\right)^2 = mn(m+n)(m-n)\,. \tag{6}$$

Mivel m és n relatív prímek és különböző paritásúak, ezért a (6) jobb oldalán szereplő négy pozitív egész páronként relatív prím. Ebből következik, hogy mind a négyen négyzetszámok, azaz

$$m = x_1^2, \quad n = y_1^2, \quad m + n = z_1^2 \quad \text{és} \quad m - n = w_1^2\,. \tag{7}$$

(7) alapján x_1, y_1, z_1, w_1 megoldása az (1a)–(1b) egyenletrendszernek, továbbá

$$z_1 \le z_1^2 = m + n \le (m+n)(m-n) = \frac{z_0 \pm w_0}{2} < z_0\,,$$

ami ellentmond z_0 minimalitásának. ■

Most rátérünk a 7.7.2 Tétel bizonyítására. Tegyük fel indirekt, hogy az a, b, c pozitív egészekre teljesül

$$c^4 - a^4 = b^2 \,. \tag{8}$$

Ha $(a, b, c) = d$, akkor a/d, b/d^2, c/d is megoldása az egyenletnek, ezért feltehetjük, hogy $(a, b, c) = 1$. Ebből a már többször látott módon kapjuk, hogy a, b és c páronként is relatív prímek.

A (8) bal oldalát szorzattá bontva

$$(c^2 + a^2)(c^2 - a^2) = b^2 \tag{9}$$

adódik. Jelöljük h-val a (9) bal oldalán álló két tényező legnagyobb közös osztóját: $h = (c^2 + a^2, c^2 - a^2)$. Mivel $(a^2, c^2) = 1$, ezért h csak 1 vagy 2 lehet. A számelmélet alaptétele szerint a (9) bal oldalán álló tényezők az első esetben külön-külön is négyzetszámok, a második esetben pedig egy-egy négyzetszám kétszeresei.

A $h = 1$ esetben tehát $c^2 + a^2$ és $c^2 - a^2$ négyzetszámok, ami a 7.7.3 Lemma szerint lehetetlen.

Ha $h = 2$, akkor alkalmas $u > v > 0$ egészekkel

$$c^2 + a^2 = 2u^2 \qquad \text{és} \qquad c^2 - a^2 = 2v^2 \,. \tag{10}$$

A (10)-beli egyenlőségeket összeadva, illetve kivonva, majd a kapott eredményeket 2-vel egyszerűsítve

$$c^2 = u^2 + v^2 \qquad \text{és} \qquad a^2 = u^2 - v^2$$

adódik, és így ismét ellentmondásba kerültünk a 7.7.3 Lemmával. ■

A Fermat-sejtés $k = 3$ kitevős esetének bizonyításához egy, a Gauss-egészekhez hasonló újabb gyűrűben, az *Euler-egészek* körében építünk fel számelméletet.

7.7.4 Definíció **D 7.7.4**

*Euler-egész*eknek azokat az $a + b\omega$ komplex számokat nevezzük, ahol a, b egész számok és

$$\omega \;=\; \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} \;=\; -\frac{1}{2} + i\frac{\sqrt{3}}{2} \,. \;\clubsuit$$

Az ω és $\omega^2 = -1-\omega$ komplex számok éppen a primitív harmadik egységgyökök, és ennek megfelelően az

$$x^3 = z^3 - y^3 = (z-y)(z-y\omega)(z-y\omega^2) \tag{11}$$

szorzattá bontás mutatja az $x^3 + y^3 = z^3$ Fermat-egyenlet és az Euler-egészek kapcsolódását. A Fermat-sejtés $k = 3$ esetének igazolásához is lényegében egy (11)-hez hasonló egyenlet vizsgálata vezet majd el, és a bizonyítás során alapvetően támaszkodni fogunk az Euler-egészek számelméletére.

7.7.5 Definíció **D 7.7.5**

Az $\alpha = a + b\omega$ Euler-egész *normá*jának nevezzük és $N(\alpha)$-val jelöljük az α abszolút értékének négyzetét:

$$N(\alpha) = |\alpha|^2 = \alpha\overline{\alpha} = (a+b\omega)(a+b\omega^2) = a^2 - ab + b^2\,. \ \clubsuit$$

Nyilván $N(\alpha)$ nemnegatív egész szám, és $N(\alpha) = 0 \iff \alpha = 0$. Megjegyezzük még, hogy az $a+b\omega$ Euler-egész normájának a^2-ab+b^2 alakja mindig átírható alkalmas c, d egészekkel $c^2 + 3d^2$ alakba, lásd a 7.7.10a feladatot.

Az Euler-egészek egy paralelogrammarácsot alkotnak a komplex számsíkon: ez egységnyi oldalú rombuszokból áll, amelyek szögei 120 és 60 fokosak.

Az oszthatóság, egység, legnagyobb közös osztó, felbonthatatlan és prím fogalmát pontosan ugyanúgy definiáljuk, mint a Gauss-egészeknél (lásd a 7.4.4, 7.4.6, 7.4.9, 7.4.10 és 7.4.11 Definíciókat, a „Gauss-” jelző helyére természetesen mindenhol „Euler-” kerül).

Az Euler-egységek és az Euler-prímek leírásától eltekintve a Gauss-egészeknél szereplő tételek és az azokra adott bizonyítások ugyanúgy érvényesek az Euler-egészekre is:

— a norma tulajdonságai (7.4.3, 7.4.5 Tételek);
— maradékos osztás (7.4.8 Tétel, a bizonyítás során rácsnégyzet helyett a megfelelő rácsrombuszt kell tekinteni);
— a prím és felbonthatatlan ekvivalenciája (7.4.12 Tétel);
— a számelmélet alaptétele (7.4.13 Tétel);
— az Euler-prímek és a (**Z**-beli) prímszámok kapcsolata (7.4.14 Tétel).

Az egységeket karakterizáló 7.4.7 Tétel és annak bizonyítása is átvihető az Euler-egészekre, ha az egységeket konkrétan megadó (iv) pontot a következőképpen módosítjuk:

7.7.6 Tétel **T 7.7.6**

Az Euler-egészek körében 6 egység van:

$$\pm 1, \qquad \pm\omega, \qquad \pm\omega^2 = \mp(1+\omega),$$

ezek éppen a hatodik komplex egységgyökök. ♣

Végül, az Euler-prímeket a következő tétel írja le:

7.7.7 Tétel **T 7.7.7**

Az alábbi Euler-egészek adják az összes Euler-prímet (ε tetszőleges egységet jelöl):

(A) $\varepsilon(i\sqrt{3}) = \varepsilon(1+2\omega)$;

(B) εq, ahol q pozitív $3t-1$ alakú prímszám;

(C) π, ahol $N(\pi)$ egy pozitív $3t+1$ alakú prímszám; minden ilyen prímszámhoz egységszerestől eltekintve két Euler-prím tartozik, amelyek egymás konjugáltjai, de nem egymás egységszeresei. ♣

Bizonyítás: A 7.4.15 Tétel bizonyítását kell értelemszerűen módosítani, ezért csak röviden jelezzük az eltéréseket.

A 7.4.14 Tétel megfelelője szerint az összes Euler-prímet a pozitív prímszámoknak az Euler-prímek szorzatára történő felbontásaiból kaphatjuk meg. Más és más típusú felbontást kapunk attól függően, hogy ez a pozitív prímszám (A) a 3; (B) $3t-1$ alakú; illetve (C) $3t+1$ alakú.

(A) Mivel $3 = (-1)(i\sqrt{3})^2$, ezért a 3-nak egységszerestől eltekintve egyetlen Euler-prím osztója az $i\sqrt{3}$.

(B) A $3t-1$ alakú pozitív prímszámok Euler-prímek is: ehhez azt kell igazolni, hogy egy Euler-egész normája nem lehet $3t-1$ alakú, a gondolatmenet további része ugyanaz, mint a Gauss-egészeknél volt.

(C) Ha p egy pozitív $3t+1$ alakú prímszám, akkor $\left(\frac{-3}{p}\right) = 1$ (lásd a 4.2.2c feladatot), tehát van olyan c egész szám, amelyre $p \mid c^2+3$. Az Euler-egészek körében

$$c^2+3 = (c+i\sqrt{3})(c-i\sqrt{3}) = (c+1+2\omega)(c-1-2\omega),$$

a gondolatmenet további része megegyezik a Gauss-egészeknél látottal. ■

A Fermat-sejtés köbszámokra vonatkozó speciális esetének bizonyításánál fontos szerepet játszik az $i\sqrt{3}$ Euler-prím néhány tulajdonsága. Ezek kényelmes megfogalmazásához előbb az Euler-egészek körében is bevezetjük a kongruencia fogalmát:

7.7.8 Definíció **D 7.7.8**

Legyenek α és β Euler-egészek és $\mu \neq 0$ Euler-egész. Azt mondjuk, hogy α *kongruens* β-val modulo μ, ha $\mu \mid \alpha - \beta$. ♣

Most is az $\alpha \equiv \beta \pmod{\mu}$ vagy röviden $\alpha \equiv \beta \ (\mu)$ jelölést használjuk. A kongruenciák elemi tulajdonságai az Euler-egészek körében ugyanúgy érvényesek, mint az egész számoknál.

Az alábbi tételben az $i\sqrt{3}$ Euler-prím néhány fontos tulajdonságát foglaljuk össze:

7.7.9 Tétel **T 7.7.9**

Legyen $\lambda = i\sqrt{3} = 1 + 2\omega$.

(i) A λ összes egységszeresei a következők: $\pm(1 + 2\omega)$, $\pm(2 + \omega)$, $\pm(1 - \omega)$.

(ii) Bármely Euler-egész a 0 és ± 1 Euler-egészek közül pontosan az egyikkel kongruens modulo λ.

(iii) Bármely α Euler-egészre $\alpha^3 \equiv \alpha \pmod{\lambda}$.

(iv) $\alpha \equiv \pm 1 \pmod{\lambda} \Longrightarrow \alpha^3 \equiv \pm 1 \pmod{\lambda^4}$. ♣

Bizonyítás: (i) A 7.7.6 Tétel alapján a λ egységszeresei $\pm\lambda$, $\mp\omega\lambda$ és $\pm\omega^2\lambda$. A szorzásokat elvégezve, valamint az $\omega^2 = -1 - \omega$ és $\omega^3 = 1$ összefüggéseket felhasználva éppen a tételben megadott hat Euler-egészt kapjuk.

(ii) Az

$$a + b\omega = a + b - b(1 - \omega) = a + b - b\omega^2\lambda$$

azonosságból kapjuk, hogy

$$a + b\omega \equiv a + b \pmod{\lambda}.$$

Mivel $a + b \equiv 0,\ 1$ vagy $-1 \pmod 3$ és $\lambda \mid 3$, ezért

$$a + b \equiv 0,\ 1 \text{ vagy } -1 \pmod{\lambda}$$

is teljesül. Ezzel beláttuk, hogy bármely $a + b\omega$ Euler-egész kongruens 0-val, 1-gyel vagy -1-gyel modulo λ.

Azt kell még megmutatni, hogy a 0, 1 és -1 páronként inkongruensek modulo λ, azaz λ nem osztója semelyik két szám különbségének, ±1-nek, illetve ±2-nek. Ha $\lambda \mid \pm1$, illetve $\lambda \mid \pm2$ teljesülne, akkor $N(\lambda) \mid 1$, illetve $N(\lambda) \mid 4$ is fennállna, de ez $N(\lambda) = 3$ miatt lehetetlen.

(iii) Ez azonnal következik (ii)-ből és az

$$\alpha^3 - \alpha = \alpha(\alpha - 1)(\alpha + 1)$$

azonosságból.

(iv) Ha $\alpha \equiv 1 \pmod{\lambda}$, akkor $\alpha = 1 + \beta\lambda$ (ahol β alkalmas Euler-egész). A köbre emelést elvégezve

$$\alpha^3 = 1 + 3\beta\lambda + 3\beta^2\lambda^2 + \beta^3\lambda^3$$

adódik. Innen a $3 = -\lambda^2$ összefüggés alapján kapjuk, hogy

$$\alpha^3 = 1 - \beta\lambda^3 - \beta^2\lambda^4 + \beta^3\lambda^3 = 1 - \beta^2\lambda^4 + (\beta^3 - \beta)\lambda^3\,. \tag{12}$$

Mivel (iii) szerint $\lambda \mid \beta^3 - \beta$, ezért (12)-ből következik, hogy $\alpha^3 \equiv 1 \pmod{\lambda^4}$.

Az $\alpha \equiv -1 \pmod{\lambda}$ esetben hasonlóan járhatunk el, vagy $-\alpha \equiv 1 \pmod{\lambda}$ alapján visszavezethetjük az előző esetre. ■

Megjegyzés: A 7.7.9 Tétel több állítása a λ helyett általánosabb modulusokra is érvényes (lásd a 7.7.12 feladatot):

(ii): Bármely $\mu \neq 0$ Euler-egész esetén a „modulo μ maradékosztályok” száma $N(\mu)$. Ha ráadásul $N(\mu) = p =$prímszám, akkor egy $\mathbf{Z}$-beli modulo p teljes maradékrendszer elemei egyben teljes maradékrendszert alkotnak az Euler-egészek körében modulo μ. (A 7.7.9 Tételben a $\mu = \lambda$, $N(\lambda) = 3$ speciális eset szerepelt.)

(iii): Tetszőleges α Euler-egész és π Euler-prím esetén

$$\alpha^{N(\pi)} \equiv \alpha \pmod{\pi}\,.$$

(Ez a kis Fermat-tétel megfelelője.)

Az előkészületek után nézzük a Fermat-sejtést a $k = 3$ kitevőre:

7.7.10 Tétel **T 7.7.10**

Az $x^3 + y^3 = z^3$ egyenletnek nincs olyan megoldása, ahol x, y és z nullától különböző egész számok. ♣

Bizonyítás: Azt az általánosabb tételt igazoljuk, hogy a

$$\xi^3 + \eta^3 + \psi^3 = 0 \tag{13}$$

egyenletnek nincs olyan megoldása, ahol ξ, η és ψ nullától különböző Euler-egészek.

Indirekt feltesszük, hogy mégis létezik ilyen megoldás. A már többször látott módon szorítkozhatunk arra az esetre, amikor ξ, η és ψ relatív prímek, sőt páronként relatív prímek.

Ezután a bizonyítás gondolatmenete a következő. Először megmutatjuk, hogy ξ, η és ψ közül pontosan az egyik osztható λ-val, legyen ez mondjuk ξ. Ekkor ξ-ből a maximális λ-hatványt kiemelve és $-\eta$ helyett κ-t írva (13)-at egy

$$\varepsilon\lambda^{3n}\gamma^3 = \kappa^3 - \psi^3 \tag{14}$$

típusú egyenletre vezethetjük vissza, ahol

$$n \geq 1, \quad \varepsilon \text{ egység}, \quad \text{továbbá} \quad \lambda, \gamma, \kappa \text{ és } \psi \text{ páronként relatív prímek.} \tag{15}$$

Itt megmutatjuk, hogy egyrészt $n \neq 1$, másrészt pedig ha (14) és (15) teljesül valamely n-nel, akkor (az ε, γ, κ, ψ változók más értékei mellett) megvalósul n helyett $n-1$-gyel is. Ez a végtelen leszállás adja az ellentmondást.

A végtelen leszálláshoz a kulcslépés a (14)-nek egy (11) típusú szorzattá bontása, ahol a jobb oldali három tényező legnagyobb közös osztója λ, és a λ-val történő leosztás után már három páronként relatív prím szám marad, amelyek a számelmélet alapétele szerint Euler-egészek köbeinek az egységszeresei.

Nézzük mindezt részletesen.

I. A (13)-ban ξ, η és ψ közül a páronként relatív prímség miatt legfeljebb egy lehet osztható λ-val.

Ha egyikük sem lenne osztható λ-val, akkor a 7.7.9 Tétel (iv) állítása szerint

$$0 = \xi^3 + \eta^3 + \psi^3 \equiv \pm 1 \pm 1 \pm 1 = \pm 1 \text{ vagy } \pm 3 \pmod{\lambda^4}.$$

Innen $\lambda^4 \mid 3$, azaz $9 \mid 3$ következne, ami lehetetlen.

II. Ezzel beláttuk, hogy ξ, η és ψ közül pontosan az egyik osztható λ-val, legyen ez mondjuk ξ, azaz

$$\xi = \lambda^n\gamma, \qquad \text{ahol} \qquad \lambda \nmid \gamma. \tag{16}$$

Írjuk be (16)-ot (13)-ba, és jelöljük $-\eta$-t κ-val, ekkor átrendezés után éppen a (14) egyenletet és a (15) feltételeket kapjuk (speciálisan $\varepsilon = 1$).

Így elég azt megmutatni, hogy a (14) egyenlet és a (15) feltételek (semmilyen ε egységgel) nem teljesülhetnek.

III. Most azt igazoljuk, hogy (14)-ben $n \neq 1$.

Tekintsük (14)-et modulo λ^4, ekkor a 7.7.9 Tétel (iv) állításából kapjuk, hogy

$$\varepsilon\lambda^{3n}\gamma^3 = \kappa^3 - \psi^3 \equiv \pm 1 \pm 1 = 0 \text{ vagy } \pm 2 \pmod{\lambda^4}. \tag{17}$$

A ± 2 eset lehetetlen, mert ebből $\lambda \mid 2$ következne. Ezért (17) jobb oldalán 0 áll, azaz

$$\lambda^4 \mid \varepsilon\lambda^{3n}\gamma^3,$$

és így $(\lambda, \varepsilon\gamma) = 1$ miatt $\lambda^4 \mid \lambda^{3n}$, azaz $n \geq 2$.

IV. Most következik a kulcslépés, a végtelen leszállás: ha (14) és (15) teljesül valamely n-nel, akkor (az ε, γ, κ, ψ változók más értékei mellett) megvalósul n helyett $n-1$-gyel is.

A (14) jobb oldalát szorzattá bontva

$$\varepsilon\lambda^{3n}\gamma^3 = (\kappa - \psi)(\kappa - \psi\omega)(\kappa - \psi\omega^2) \tag{18}$$

adódik.

Mivel λ osztója (18) bal oldalának és λ Euler-prím, ezért λ a jobb oldal legalább egyik tényezőjének is osztója. Továbbá az egyes tényezők különbsége rendre $(\omega-1)\psi$, $(\omega^2-1)\psi$, illetve $(\omega^2-\omega)\psi$, amelyek valamennyien oszthatók $\omega - 1 = \varepsilon\lambda$-val. Ebből következik, hogy λ a (18) jobb oldalán szereplő mindhárom tényezőnek osztója.

Most belátjuk, hogy (18) jobb oldalán bármelyik két tényező legnagyobb közös osztója λ. Nézzük ezt például az első két tényezőre, a többi hasonlóan megy.

Legyen $\delta = (\kappa - \psi, \kappa - \psi\omega)$. Ekkor

$$\delta \mid (\kappa - \psi) - (\kappa - \psi\omega) = \psi(\omega - 1)$$

és

$$\delta \mid \omega(\kappa - \psi) - (\kappa - \psi\omega) = \kappa(\omega - 1),$$

tehát

$$\delta \mid \big(\psi(\omega - 1), \kappa(\omega - 1)\big) = (\omega - 1)(\kappa, \psi) = \omega - 1 = \varepsilon\lambda.$$

Ezt a már korábban látott $\lambda \mid \delta$ oszthatósággal összevetve valóban $\delta = \lambda$ adódik.

A fentiek alapján

$$\frac{\kappa-\psi}{\lambda}\,,\quad \frac{\kappa-\psi\omega}{\lambda}\quad\text{és}\quad \frac{\kappa-\psi\omega^2}{\lambda}$$

páronként relatív prímek, ezért a a számelmélet alaptételéből következik, hogy

$$\begin{aligned}\kappa-\psi&=\varepsilon_1\lambda\nu_1^3\,,\\ \kappa-\psi\omega&=\varepsilon_2\lambda\nu_2^3\,,\\ \kappa-\psi\omega^2&=\varepsilon_3\lambda\nu_3^3\,,\end{aligned}\tag{19}$$

ahol ε_1, ε_2, ε_3 egységek és ν_1, ν_2, ν_3 páronként relatív prím Euler-egészek.

Most a ν_i-ket a λ-val való oszthatóság szempontjából vizsgáljuk. Mivel a ν_i-k páronként relatív prímek, ezért (mondjuk) ν_2 és ν_3 nem osztható λ-val. Legyen a ν_1 „kanonikus alakjában" a λ kitevője s, megmutatjuk, hogy $s=n-1$.

Ennek igazolásához hasonlítsuk össze, hogy a (18) egyenlőség két oldala λ-nak pontosan hányadik hatványával osztható. A (18) bal oldalán ez a kitevő $3n$. A (18) jobb oldalán a tényezők (19)-beli előállításából azt kapjuk, hogy a λ mindhárom tényezőben előfordul az első hatványon, és emellett még ν_1^3-ben szerepel $3s$ kitevővel. Ennek alapján $3n=3+3s$, azaz valóban $s=n-1$, tehát

$$\nu_1=\lambda^{n-1}\gamma_1,\qquad\text{ahol}\qquad(\gamma_1,\lambda)=1.\tag{20}$$

Itt $n\ge 2$ miatt $n-1\ge 1$.

A következő lépésben megmutatjuk, hogy a (19)-beli egyenletek alkalmas lineáris kombinációját véve egy olyan (14) típusú egyenlőséghez jutunk, amelyben n helyett $n-1$ szerepel (és ezzel kész a bizonyítás).

Adjuk össze a (19)-beli első egyenletet, a második egyenlet ω-szorosát és a harmadik egyenlet ω^2-szeresét:

$$(\kappa-\psi)+\omega(\kappa-\psi\omega)+\omega^2(\kappa-\psi\omega^2)=\varepsilon_1\lambda\nu_1^3+\varepsilon_4\lambda\nu_2^3+\varepsilon_5\lambda\nu_3^3\,,\tag{21}$$

ahol $\varepsilon_4=\varepsilon_2\omega$ és $\varepsilon_5=\varepsilon_3\omega^2$ is egységek. A (21) bal oldala

$$(\kappa-\psi)+\omega(\kappa-\psi\omega)+\omega^2(\kappa-\psi\omega^2)=(1+\omega+\omega^2)(\kappa-\psi)=0.\tag{22}$$

Így (20), (21) és (22) alapján azt kapjuk, hogy

$$0=\varepsilon_1\lambda^{3(n-1)+1}\gamma_1^3+\varepsilon_4\lambda\nu_2^3+\varepsilon_5\lambda\nu_3^3\,.$$

Innen $\varepsilon_5\lambda$-val való osztás és átrendezés után

$$\varepsilon_6\lambda^{3(n-1)}\gamma_1^3 = \varepsilon_7\nu_2^3 - \nu_3^3 \tag{23}$$

adódik (ahol ε_6 és ε_7 egységek).

Belátjuk, hogy $\varepsilon_7 = \pm 1$, és így az $\varepsilon_7\nu_2^3$ tag helyére $(\pm\nu_2)^3$ írható.

Vizsgáljuk a (23) egyenletet modulo λ^3. Mivel $n-1 \geq 1$, továbbá $\lambda \nmid \nu_2$ és $\lambda \nmid \nu_3$, ezért a 7.7.9 Tétel (iv) pontja alapján azt kapjuk, hogy

$$\varepsilon_7(\pm 1) - (\pm 1) \equiv 0 \pmod{\lambda^3},$$

azaz λ^3 osztója $\varepsilon_7 - 1$-nek vagy $\varepsilon_7 + 1$-nek. Ekkor

$$N(\lambda^3) \mid N(\varepsilon_7 \mp 1), \qquad N(\lambda^3) = 27 \qquad \text{és} \qquad N(\varepsilon_7 \mp 1) < 27$$

miatt $\varepsilon_7 \mp 1 = 0$, vagyis valóban csak $\varepsilon_7 = \pm 1$ lehetséges.

Ennek alapján (23) átírható az

$$\varepsilon_6\lambda^{3(n-1)}\gamma_1^3 = (\pm\nu_2)^3 - \nu_3^3$$

alakba. Ez azt jelenti, hogy a (14) egyenlet kielégíthető n helyett $n-1$-re is, és a (15) feltételek is teljesülnek (ε, γ, κ, illetve ψ helyére rendre ε_6, γ_1, $\pm\nu_2$, illetve ν_3 került). ■

Feladatok

7.7.1

a) Mutassuk meg, hogy ha $k \mid m$, és két pozitív k-adik hatvány összege sohasem k-adik hatvány, akkor két pozitív m-edik hatvány összege sem lehet m-edik hatvány.

b) Indokoljuk meg, miért elég a Fermat-sejtést a $k = 4$ és $k = p =$ prím kitevőkre igazolni.

7.7.2 Hány megoldása van az alábbi egyenleteknek a pozitív egészek körében?

a) $x^{20} + y^{24} = z^{28}$; b) $x^3 + y^4 = z^5$.

7.7.3 Oldjuk meg a $k^x + k^y = k^z$ „exponenciális” Fermat-egyenletet (ahol k, x, y, z pozitív egészek).

7.7.4 Az alábbiakban megvizsgáljuk a „Fermat-egyenletet” néhány olyan esetben, amikor a kitevő nem pozitív egész. Határozzuk meg az összes x, y, z pozitív egész megoldást.

a) $k=-4:\quad \dfrac{1}{x^4}+\dfrac{1}{y^4}=\dfrac{1}{z^4}\,.$

b) $k=-2:\quad \dfrac{1}{x^2}+\dfrac{1}{y^2}=\dfrac{1}{z^2}\,.$

c) $k=1/2:\quad \sqrt{x}+\sqrt{y}=\sqrt{z}\,.$

d) $k=1/3:\quad \sqrt[3]{x}+\sqrt[3]{y}=\sqrt[3]{z}\,.$

7.7.5 Bizonyítsuk be az alábbi állításokat.

a) Az $x^4+y^2=z^2$ és $x^2+y^2=z^4$ egyenleteknek végtelen sok olyan pozitív egész megoldása van, ahol $(x,y,z)=1$.

M *b) Az $x^4+y^4=z^2$ egyenlet nem oldható meg a pozitív egészek körében.

Megjegyzés: A b) részből egy újabb bizonyítást nyerünk a Fermat-sejtés $k=4$ esetére.

*7.7.6 Oldjuk meg az $x^4-2y^2=-1$ diofantikus egyenletet.

M** 7.7.7 Milyen alapú számrendszerekben igaz, hogy az 1111 alakú szám négyzetszám?

7.7.8 Mely Euler-egészek oszthatók a konjugáltjukkal?

7.7.9 Igazoljuk az alábbi azonosságot (a,b,c,d tetszőleges valós számok):

$$(a^2-ab+b^2)(c^2-cd+d^2)=$$
$$=(ac-bd)^2-(ac-bd)(ad+bc-bd)+(ad+bc-bd)^2\,.$$

7.7.10

M a) Bizonyítsuk be, hogy az $x^2-xy+y^2=n$ diofantikus egyenlet akkor és csak akkor oldható meg, ha megoldható az $x^2+3y^2=n$ diofantikus egyenlet.

*b) Milyen n-ekre oldható meg az a)-beli két diofantikus egyenlet, és mennyi a megoldásszám?

M* 7.7.11 Oldjuk meg az $x^2+243=y^3$ diofantikus egyenletet.

7.7.12 Legyen $\mu\neq 0$ Euler-egész. A $\varrho_1,\dots,\varrho_r$ Euler-egészeket teljes maradékrendszernek nevezzük modulo μ, ha bármely α Euler-egészre az $\alpha\equiv\varrho_i\pmod{\mu}$ kongruencia pontosan egy ϱ_i-re teljesül. Bizonyítsuk be az alábbi állításokat.

*a) Egy modulo μ teljes maradékrendszer elemszáma $N(\mu)$.

b) Ha $N(\mu) = p =$ prímszám, akkor $0, 1, 2, \ldots, N(\mu) - 1$ teljes maradékrendszert alkotnak modulo μ.

c) Érvényes a kis Fermat-tétel megfelelője: tetszőleges α Euler-egész és π Euler-prím esetén

$$\alpha^{N(\pi)} \equiv \alpha \pmod{\pi}.$$

7.7.13 Oldjuk meg az alábbi diofantikus egyenletet:

$$\frac{u}{v} + \frac{v}{w} = \frac{w}{u}.$$

7.7.14

a) Mutassuk meg, hogy ha egy derékszögű háromszög oldalai egész számok, akkor a háromszög területe nem lehet négyzetszám.

b) Bizonyítsuk be, hogy ha egy derékszögű háromszög oldalai páronként relatív prím egész számok, akkor a háromszög területe nem lehet köbszám.

c) Van-e olyan egész oldalú derékszögű háromszög, amelynek a területe köbszám?

d) Vizsgáljuk meg a probléma általánosítását magasabb hatványokra.

7.8. Pell-egyenlet

Pell-egyenletnek egy

$$x^2 - my^2 = 1 \tag{1}$$

alakú diofantikus egyenletet nevezünk, ahol az m (rögzített) pozitív egész és nem négyzetszám. Az (1) egyenlet két triviális megoldása $x = \pm 1$, $y = 0$, az ezektől különböző (azaz $y \neq 0$ típusú) megoldások a nemtriviális megoldások.

Az (1) bal oldalát szorzattá bonthatjuk:

$$(x + y\sqrt{m})(x - y\sqrt{m}) = 1. \tag{2}$$

Ebből következik, hogy ha x, y megoldása (1)-nek, akkor az $a + b\sqrt{m}$ alakú számok körében (ahol a és b egészek) az $x + y\sqrt{m}$ és $x - y\sqrt{m}$ számok osztói az 1-nek, és így mindketten egységek. Mivel egy egység tetszőleges (egész kitevős) hatványa is egység, ezért ha létezik egy $\varepsilon \neq \pm 1$ egység, akkor az ε hatványai végtelen sok egységet adnak. Ez a Pell-egyenletre „visszafogalmazva” azt

jelenti, hogy ha (1)-nek létezik nemtriviális megoldása, akkor végtelen sok megoldás van. (Az $m = 2$, illetve $m = 3$ speciális eset lényegében szerepelt az 1.1.22 feladatban, illetve az 5.2.4 Tétel bizonyítása során.)

Az alábbiakban először megmutatjuk, hogy a Pell-egyenletnek mindig végtelen sok megoldása van (az előbbiek szerint ehhez elég azt bizonyítani, hogy legalább egy nemtriviális megoldás létezik). Ezután megadjuk, hogyan lehet az összes megoldást megkapni.

Megjegyezzük még, hogy az (1) egyenlet az $m \le 0$ és $m = k^2$ esetekben alapvetően másképpen viselkedik, lásd a 7.8.1 feladatot.

7.8.1 Tétel **T 7.8.1**

Legyen m olyan pozitív egész, amely nem négyzetszám. Ekkor az (1) diofantikus egyenletnek végtelen sok megoldása van. ♣

A bizonyítás során fel fogjuk használni a következő fejezetből a 8.1.1 Tételt.

Bizonyítás: Ha $y \neq 0$, akkor az (1)-gyel ekvivalens (2) egyenlőség az

$$\frac{x}{y} - \sqrt{m} = \frac{1}{y(x + y\sqrt{m})} \tag{3}$$

alakra hozható.

(3)-ból látszik, hogy $x > 0$, $y > 0$ esetén x, y csak akkor lehet megoldás, ha x/y „nagyon közel" van $\sqrt{m}$-hez: $\sqrt{m} > 1$ miatt (3) fennállása esetén

$$\left|\sqrt{m} - \frac{x}{y}\right| < \frac{1}{y^2}\,. \tag{4}$$

A $\sqrt{m}$ irracionalitása miatt a 8.1.1 Tételből következik, hogy (4) valóban végtelen sok x, y egész számpárra teljesül. Ezt a tényt felhasználva most azt igazoljuk, hogy (2)-nek is végtelen sok megoldása van. (A (4) és (2) feltételek nem ekvivalensek, a (4)-et kielégítő x, y értékeknek csak egy része teljesíti majd (2)-t is.)

I. Első lépésként megmutatjuk, hogy van olyan $t \neq 0$ egész, amelyre az

$$x^2 - my^2 = t \tag{5}$$

diofantikus egyenletnek végtelen sok megoldása van.

Legyenek c_j, d_j $(j = 1, 2, \ldots)$ olyan pozitív egész számpárok, amelyek eleget tesznek (4)-nek, azaz

$$\left|\sqrt{m} - \frac{c_j}{d_j}\right| < \frac{1}{d_j^2}\,, \qquad j = 1, 2, \ldots$$

Ekkor

$$|c_j^2 - md_j^2| = d_j^2\Big|\frac{c_j}{d_j} - \sqrt{m}\Big| \cdot \Big|\frac{c_j}{d_j} + \sqrt{m}\Big| < \Big|\frac{c_j}{d_j} + \sqrt{m}\Big| =$$
$$= \Big|\frac{c_j}{d_j} - \sqrt{m} + 2\sqrt{m}\Big| < \frac{1}{d_j^2} + 2\sqrt{m} \le 1 + 2\sqrt{m}\,. \tag{6}$$

A (6)-ból következik, hogy a $c_j^2 - md_j^2$ értékek csak a $(-1 - 2\sqrt{m}, 1 + 2\sqrt{m})$ intervallumba eső véges sok egész szám közül kerülhetnek ki, továbbá $\sqrt{m}$ irracionalitása miatt a 0 nem jöhet szóba. A skatulyaelv értelmében ekkor található ebben az intervallumban olyan $t \neq 0$ egész szám, hogy

$$c_j^2 - md_j^2 = t$$

végtelen sok c_j, d_j párra teljesül. Ez azt jelenti, hogy az (5) diofantikus egyenletnek végtelen sok megoldása van.

II. Most megmutatjuk, hogy az (5) egyenlet alkalmas megoldásainak „hányadosaiból" az (1) egyenlet megoldásaihoz jutunk.

Legyen $x = a_1$, $y = b_1$, illetve $x = a_2$, $y = b_2$ az (5) egyenlet két megoldása, azaz

$$a_1^2 - mb_1^2 = (a_1 + b_1\sqrt{m})(a_1 - b_1\sqrt{m}) = t, \tag{7a}$$
$$a_2^2 - mb_2^2 = (a_2 + b_2\sqrt{m})(a_2 - b_2\sqrt{m}) = t, \tag{7b}$$

és tegyük fel, hogy

$$a_1 \equiv a_2 \pmod{|t|} \qquad \text{és} \qquad b_1 \equiv b_2 \pmod{|t|}. \tag{8}$$

A (7a), (7b) és (8) feltételek teljesülése esetén az a_1, b_1 és a_2, b_2 számpárokat az (5) egyenlet modulo $|t|$ kongruens megoldásainak fogjuk nevezni.

A (7a) egyenlőséget (7b)-vel elosztva azt kapjuk, hogy

$$\frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} \cdot \frac{a_1 - b_1\sqrt{m}}{a_2 - b_2\sqrt{m}} = 1. \tag{9}$$

A (9) bal oldalán szereplő első tört

$$\frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} = u + v\sqrt{m}$$

alakba írható (ahol u és v racionális számok), és ekkor a második törtre szükségképpen fennáll

$$\frac{a_1 - b_1\sqrt{m}}{a_2 - b_2\sqrt{m}} = u - v\sqrt{m}\,.$$

Belátjuk, hogy (8) miatt u és v egész számok, tehát u és v valóban az (1) egyenlet egész megoldását adják.

A nevező szokásos „gyöktelenítésével" és (7b) felhasználásával kapjuk, hogy

$$\frac{a_1 + b_1\sqrt{m}}{a_2 + b_2\sqrt{m}} = \frac{(a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m})}{a_2^2 - mb_2^2} = \frac{(a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m})}{t}\,.$$

Így azt kell igazolnunk, hogy az

$$(a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m}) = r + s\sqrt{m}$$

felírásban r és s osztható t-vel. Ez (8)-ból és (7a)-ból következik:

$$\begin{aligned} r + s\sqrt{m} &= (a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m}) \equiv \\ &\equiv (a_1 + b_1\sqrt{m})(a_1 - b_1\sqrt{m}) = t \equiv 0 \pmod{|t|}. \end{aligned}$$

(A kongruenciát az $a + b\sqrt{m}$ számokra a már többször látott „természetes" értelemben használtuk.)

III. Mivel egy a, b számpárban az a és b is $|t|$-féle maradékot adhat modulo $|t|$, ezért az (5) egyenlet páronként inkongruens megoldásainak a száma legfeljebb t^2. Ismét a skatulyaelvet alkalmazva ebből az következik, hogy az (5) egyenlet végtelen sok megoldása között kell lennie végtelen sok olyannak, amelyek közül bármelyik kettő kongruens modulo $|t|$. Legyenek $x = f_i$, $y = g_i$, $i = 1, 2, \ldots$ ilyen megoldások.

Ekkor a II. rész szerint az f_i, g_i és f_1, g_1 „hányadosaként" keletkező r_i, s_i értékek az (1) diofantikus egyenlet végtelen sok (különböző) megoldását adják. ■

7.8.2 Tétel **T 7.8.2**

Legyen m olyan pozitív egész, amely nem négyzetszám, és x_0, y_0 az (1) diofantikus egyenletnek az a(z egyértelműen meghatározott) megoldása, amelyre $x_0 > 0$, $y_0 > 0$ és $x_0 + y_0\sqrt{m}$ minimális. Ekkor az összes megoldást az

$$x + y\sqrt{m} = \pm(x_0 + y_0\sqrt{m})^n, \qquad n = 0, \pm1, \pm2, \ldots \tag{10}$$

képlettel meghatározott x, y egész számpárok adják. ♣

A (2) egyenlőségből látszik, hogy

$$(x_0 + y_0\sqrt{m})^{-n} = (x_0 - y_0\sqrt{m})^n\,, \tag{11}$$

ezért (10) az

$$x + y\sqrt{m} = \pm(x_0 \pm y_0\sqrt{m})^n, \qquad n = 0, 1, 2, \ldots$$

formában is megadható.

Az $n = 0$ esetben a két triviális megoldást kapjuk.

Bizonyítás: Többször fel fogjuk használni, hogy két megoldásnak az alábbi értelemben vett szorzata is megoldás.

Tegyük fel, hogy x_1, y_1, illetve x_2, y_2 egy-egy megoldása (1)-nek, azaz

$$(x_1 + y_1\sqrt{m})(x_1 - y_1\sqrt{m}) = 1, \tag{12a}$$
$$(x_2 + y_2\sqrt{m})(x_2 - y_2\sqrt{m}) = 1. \tag{12b}$$

A (12a) és (12b) egyenlőségeket összeszorozva

$$(x_1x_2 + my_1y_2 + (x_1y_2 + y_1x_2)\sqrt{m})(x_1x_2 + my_1y_2 - (x_1y_2 + y_1x_2)\sqrt{m}) = 1$$

adódik, ami azt jelenti, hogy

$$x_3 = x_1x_2 + my_1y_2, \qquad y_3 = x_1y_2 + y_1x_2$$

is megoldása (1)-nek. (Mindez a bevezetőben jelzett, az egységekre vonatkozó átfogalmazásban annak felel meg, hogy két egység szorzata is egység.)

A fentiekből és (11)-ből nyilvánvalóan következik, hogy a (10) képlettel megadott x, y számpárok kielégítik (1)-et.

Most belátjuk, hogy ez az összes megoldás. Tegyük fel indirekt, hogy létezik egy x, y megoldás, amely nem ilyen alakú. Ekkor nyilván $-x$, $-y$ is megoldás és ez sem szerepel a (10)-beli megoldások között. Ezért feltehető, hogy $x + y\sqrt{m} > 0$.

Ekkor létezik olyan k egész szám, amelyre

$$(x_0 + y_0\sqrt{m})^k < x + y\sqrt{m} < (x_0 + y_0\sqrt{m})^{k+1}\,. \tag{13}$$

A (13)-at $(x_0 - y_0\sqrt{m})^k$-nal beszorozva

$$1 < (x + y\sqrt{m})(x_0 - y_0\sqrt{m})^k < x_0 + y_0\sqrt{m} \tag{14}$$

adódik. Itt

$$(x + y\sqrt{m})(x_0 - y_0\sqrt{m})^k = x' + y'\sqrt{m}$$

megoldások összeszorzásával keletkezett, tehát x', y' is megoldás, azaz

$$(x' + y'\sqrt{m})(x' - y'\sqrt{m}) = 1. \tag{15}$$

A (14)-beli első egyenlőtlenség szerint

$$x' + y'\sqrt{m} > 1, \tag{16a}$$

így (15) miatt

$$0 < x' - y'\sqrt{m} < 1\,. \tag{16b}$$

A (16b) miatt nem lehetségesek az $y' = 0$, az $x' < 0$, $y' > 0$, valamint az $x' > 0$, $y' < 0$ esetek, a (16a) miatt pedig nem fordulhat elő $x' < 0$, $y' < 0$. Ezért $x' > 0$, $y' > 0$, ez azonban (14) szerint ellentmond $x_0 + y_0\sqrt{m}$ minimalitásának. ■

Feladatok

7.8.1 Határozzuk meg az $x^2 - my^2 = 1$ diofantikus egyenlet összes megoldását, ha $m \le 0$, illetve ha m négyzetszám.

7.8.2 Hány olyan négyzetszám van, amely után (tízes számrendszerben) egy 1-est írva ismét négyzetszámot kapunk?

7.8.3 Legyen m olyan pozitív egész, amely nem négyzetszám, és $r \neq 0$ tetszőleges egész szám. Bizonyítsuk be, hogy ha az $x^2 - my^2 = r$ diofantikus egyenlet megoldható, akkor végtelen sok megoldása van.

7.8.4

a) Hány olyan négyzetszám van, amely

(a1) 1-gyel nagyobb; (a2) 1-gyel kisebb

egy négyzetszám kétszeresénél?

b) Vizsgáljuk meg a kérdést kétszeres helyett háromszorosra is.

7.8.5 Hány olyan n van, amelyre $\binom{n}{2}$ négyzetszám?

7.8.6 Hány olyan (páronként nem egybevágó) derékszögű háromszög van, amelynek a befogói szomszédos egész számok és az átfogója is egész szám?

7.8.7 Hány megoldása van az alábbi diofantikus egyenleteknek:

a) $x^2 - 3y^2 = 2$; b) $x^2 - 3y^2 = 7$; c) $x^2 - 3y^2 = 13$;

d) $x^2 - 3y^2 = 39$; e) $2x^2 - 3y^2 = 1$; f) $3x^2 - 2y^2 = 1$.

*7.8.8 Mely $p > 0$ prímszámok esetén oldható meg az $x^2 - py^2 = -1$ diofantikus egyenlet?

7.8.9 Legyenek az a, b, c nemnulla egészek páronként relatív prímek, és tegyük fel, hogy az $ax^2+by^2+cz^2 = 0$ diofantikus egyenletnek létezik nemtriviális (vagyis az $x = y = z = 0$-tól különböző) megoldása. Bizonyítsuk be, hogy ekkor a, b és c előjele nem lehet azonos, továbbá megoldhatók az

$$u^2 \equiv -bc \pmod{|a|}, \quad v^2 \equiv -ac \pmod{|b|}, \quad w^2 \equiv -ab \pmod{|c|}$$

kongruenciák.

Megjegyzés: Megmutatható, hogy ezek a feltételek nemcsak szükségesek, hanem elégségesek is ahhoz, hogy az $ax^2 + by^2 + cz^2 = 0$ diofantikus egyenletnek létezzék nemtriviális megoldása.

7.8.10 Hány olyan k egész szám létezik, amelyre $2 + 2\sqrt{28k^2 + 1}$ négyzetszám?

*7.8.11 Mutassuk meg, hogy az $x^2 - 2y^2 = 1$ Pell-egyenlet nemtriviális megoldásaiban sem x, sem y nem lehet négyzetszám.

7.9. Partíciók

7.9.1 Definíció **D 7.9.1**

Az n pozitív egész *partíció*in az n-nek pozitív egészek összegeként történő lényegesen különböző előállításait értjük (azaz azonosnak tekintjük a csupán az összeadandók sorrendjében eltérő előállításokat). Itt az egytagú összeget is megengedjük.

Az n partícióinak számát $p(n)$-nel jelöljük. ♣

Példa: A 4 összes partíciói

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1,$$

tehát $p(4) = 5$.

Bizonyítás nélkül közöljük a $p(n)$ függvényre vonatkozó aszimptotikus eredményt: ($n \to \infty$ esetén)

$$p(n) \sim \frac{ce^{d\sqrt{n}}}{n}, \quad \text{ahol} \quad c = \frac{1}{4\sqrt{3}} \quad \text{és} \quad d = \frac{\pi\sqrt{6}}{3}.$$

Gyakran vizsgálunk olyan partíciós kérdéseket, amikor az n-et előállító összeadandókra vagy azok számára teszünk bizonyos megkötéseket: például előírhatjuk, hogy csupa páratlan szám vagy csupa különböző szám szerepeljen összeadandóként stb.

A partíciós feladatok kezelésének alapvető eszköze a generátorfüggvény. Ennek illusztrálására tekintsük az ún. pénzkifizetési (vagy pénzváltási) problémát: hányféleképpen lehetett n forintot (például) 50 forintosnál kisebb pénzérmékkel kifizetni, amikor még 1- és 2-forintosok is érvényben voltak. Ekkor az n olyan partícióiról van szó, ahol összeadandóként csak az 1, 2, 5, 10 és 20 számokat engedjük meg, jelöljük az ilyen partíciók számát $f(n)$-nel.

A feladatot a következő módon érdemes átfogalmazni. Jelölje egy ilyen kifizetésnél a felhasznált 1, 2, 5, 10, illetve 20 forintosok számát rendre $u_1, \ldots, u_5$, ekkor $f(n)$ az

$$1u_1 + 2u_2 + 5u_3 + 10u_4 + 20u_5 = n \tag{1}$$

diofantikus egyenlet nemnegatív egész megoldásainak a száma.

Az $f(n)$ függvény generátorfüggvényén az

$$F(x) = 1 + \sum_{n=1}^{\infty} f(n)x^n \tag{2}$$

hatványsort értjük. Először megmutatjuk, hogy ez a sor $|x| < 1/2$ esetén abszolút konvergens.

Mivel (1)-ben bármely i-re $0 \le u_i \le n$, ezért

$$0 \le f(n) \le (n+1)^5 .$$

Könnyen látható, hogy ha n elég nagy, akkor $(n+1)^5 < 2^n$, így a (2) végtelen sor $|x| < 1/2$ esetén majorálható a

$$\sum_{n=0}^{\infty} (2|x|)^n$$

konvergens végtelen mértani sorral. Ezzel beláttuk, hogy $|x| < 1/2$ esetén $F(x)$ abszolút konvergens. (Ez igazolható $|x| < 1$-re is.)

Most $F(x)$-et előállítjuk konvergens mértani sorok szorzataként (továbbra is feltesszük, hogy $|x| < 1/2$):

$$F(x) = \big(1 + x + x^2 + \ldots\big)\big(1 + x^2 + (x^2)^2 + \ldots\big)\big(1 + x^5 + (x^5)^2 + \ldots\big)\cdot \\ \cdot \big(1 + x^{10} + (x^{10})^2 + \ldots\big)\big(1 + x^{20} + (x^{20})^2 + \ldots\big) . \tag{3}$$

Mivel egy függvény a 0 körül csak egyféleképpen fejthető hatványsorba, így azt kell megmutatnunk, hogy (3) jobb oldalán a véges sok abszolút konvergens sor szorzását elvégezve x^n együtthatója éppen $f(n)$ lesz. Az n minden (1)-beli előállításának feleltessük meg azt a szorzatot, amelyet úgy kapunk, hogy (3) jobb oldaláról rendre az

$$x^{u_1}, \qquad (x^2)^{u_2}, \qquad (x^5)^{u_3}, \qquad (x^{10})^{u_4}, \qquad (x^{20})^{u_5}$$

tagokat szorozzuk össze. Ez a szorzat éppen

$$x^{u_1}(x^2)^{u_2}(x^5)^{u_3}(x^{10})^{u_4}(x^{20})^{u_5} = x^{1u_1+2u_2+5u_3+10u_4+20u_5} = x^n\,.$$

Mivel a szóban forgó előállítások és szorzatok között kölcsönösen egyértelmű megfeleltetés áll fenn, ezért (3) jobb oldalán a szorzást elvégezve x^n együtthatója valóban $f(n)$ lesz.

A mértani sorok összegképletét felhasználva (3) átírható az

$$F(x) = \frac{1}{(1-x)(1-x^2)(1-x^5)(1-x^{10})(1-x^{20})} \qquad (|x| < 1/2)$$

alakba.

A fentiekkel teljesen azonos módon kapjuk az alábbi általánosabb eredményt is:

7.9.2 Tétel **T 7.9.2**

Legyenek $a_1, a_2, \ldots, a_r$ különböző pozitív egészek, és jelöljük $f(n)$-nel az n pozitív egésznek az $a_1, a_2, \ldots, a_r$ összeadandókból képzett partíciói számát. Ekkor $|x| < 1/2$ esetén az $1 + \sum_{n=1}^{\infty} f(n)x^n$ végtelen sor abszolút konvergens és

$$1 + \sum_{n=1}^{\infty} f(n)x^n = \prod_{i=1}^{r} \frac{1}{1-x^{a_i}}\,. \ \clubsuit$$

Hasonlóan adódik $p(n)$ generátorfüggvénye is:

7.9.3 Tétel **T 7.9.3**

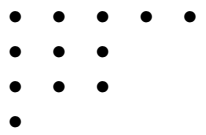
$$P(x) = 1 + \sum_{n=1}^{\infty} p(n)x^n = \prod_{i=1}^{\infty} \frac{1}{1-x^i} \qquad (|x| < 1).\ \clubsuit \tag{4}$$

A (4) jobb oldalán szereplő végtelen szorzat (az 5.6.6 és 5.6.7 feladatokban megadott módon) az alábbi határértéket jelenti:

$$\prod_{i=1}^{\infty} \frac{1}{1-x^i} = \lim_{r\to\infty} \prod_{i=1}^{r} \frac{1}{1-x^i} \,.$$

A 7.9.3 Tétel igazolásához a 7.9.2 Tételt kell az $a_i = i$ esetre alkalmazni, majd az $r \to \infty$ határátmenetet kell képezni. A bizonyítást nem részletezzük.

A partíciók kezeléséhez a generátorfüggvények mellett kombinatorikus jellegű meggondolások is jól használhatók. Az $n = a_1 + a_2 + \ldots + a_r$ partíciót, ahol $a_1 \geq a_2 \geq \ldots \geq a_r$ egy olyan pontsémával ábrázolhatjuk, amelynek első sorában a_1, a második sorában a_2 stb. pont van. Például a



(5)

séma a $12 = 5+3+3+1$ partíciónak felel meg. Az értelmezésből nyilvánvaló, hogy egy ilyen séma egyetlen sorában sem lehet több elem, mint a felette levő sorban.

A sémában az egyes sorok felelnek meg a partíció tagjainak, azonban néha hasznos a sémát „oszloponként" is leolvasni. Például az (5) sémánál ekkor a $12 = 4+3+3+1+1$ partícióhoz jutunk. A sémáknak ebből a kétféle leolvasásából kapjuk az alábbi eredményt:

7.9.4 Tétel **T 7.9.4**

Legyen $g_r(n)$, illetve $h_r(n)$ az n szám olyan partícióinak a száma, ahol az összeadandók száma, illetve maximuma r. Ekkor $g_r(n) = h_r(n)$. ♣

Bizonyítás: Tekintsük azokat az n pontból álló sémákat, amelyeknek pontosan r sora van. Egy ilyen sémát soronként nézve az n-nek egy r összeadandóból álló partícióját kapjuk, oszloponként nézve pedig az n-nek egy olyan partíciójához jutunk, amelyben a legnagyobb összeadandó r. Az összes ilyen sémát összeszámolva így éppen a kívánt $g_r(n) = h_r(n)$ egyenlőség adódik. ■

A következőkben az n számnak páros sok, illetve páratlan sok különböző összeadandóból álló partícióit vizsgáljuk. Az alábbi, Eulertől származó tételből kiderül, hogy a kétféle partíció száma között bármely n esetén legfeljebb 1 az eltérés.

7.9.5 Tétel **T 7.9.5**

Jelölje $s(n)$, illetve $t(n)$ az n pozitív egész azon partícióinak a számát, ahol minden összeadandó különböző, és a tagok száma páros, illetve páratlan. Ekkor

$$s(n)-t(n)=\begin{cases}(-1)^k, & \text{ha } n=\frac{1}{2}(3k^2\pm k);\\ 0, & \text{egyébként.}\end{cases} \qquad (6)$$

♣

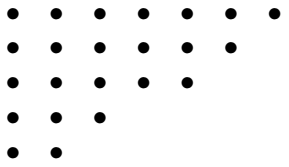
Példa: Az $n=7$ páros, illetve páratlan sok különböző összeadandóból történő előállításai

$$6+1=5+2=4+3, \quad \text{illetve} \quad 7=4+2+1,$$

tehát $s(7)=3$, $t(7)=2$. Az $s(7)-t(7)=1=(-1)^2$ egyenlőség összhangban van (6)-tal, hiszen $7=\frac{1}{2}(3\cdot 2^2+2)$.

Bizonyítás: „Majdnem” kölcsönösen egyértelmű megfeleltetést fogunk létesíteni az n páros, illetve páratlan sok különböző összeadandóból álló partíciói között.

Az n csupa különböző tagból álló partíciói olyan sémáknak felelnek meg, amelyekben az egyes sorokban fentről lefelé szigorúan csökkenő számú elem szerepel, például a $23=7+6+5+3+2$ partíciónak a



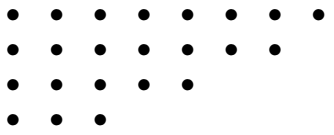
(7)

séma felel meg.

Nevezzük egy ilyen séma élének a jobb felső pontból induló, 45 fokos szögben haladó maximális hosszúságú „ÉK-DNy” irányú pontsort. A (7) séma éle 3 pontból áll. (Az elemszámot általában az határozza meg, meddig tart az összeadandók egyesével történő csökkenése, az él elemszáma lehet természetesen 1 is.)

Legyen A az a transzformáció, amely egy séma élét áthelyezi a séma utolsó sora alá (új utolsó sornak), feltéve, hogy így ismét egy csupa különböző összeadandóból álló partíció jön létre, azaz egy szigorúan csökkenő elemszámú sorokból álló sémát kapunk. Hasonlóképpen, legyen M az a transzformáció, amely egy séma utolsó sorát áthelyezi a séma éle mellé (ferdén, új élnek), amennyiben így ismét egy megfelelő séma keletkezik. A (7) séma esetén M-et

alkalmazva a

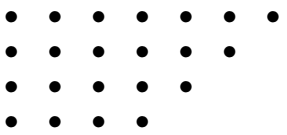


sémához jutunk, ugyanakkor A nem végezhető el.

Megmutatjuk, hogy néhány kivételtől eltekintve bármely séma esetén A és M közül pontosan az egyik hajtható végre.

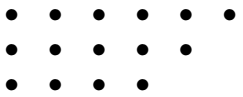
Legyen a séma utolsó sorának elemszáma a, az él elemszáma pedig m.

Ha $a \leq m$, akkor A nem hajtható végre, M viszont igen, kivéve, ha $a = m$ és az utolsó sor és az él összeér (ekkor sem A, sem M nem végezhető el):



(*)

Ha $a > m$, akkor M nem hajtható végre, A viszont igen, kivéve, ha $a = m+1$ és az utolsó sor és az él összeér (ekkor sem M, sem A nem végezhető el):



(**)

Az A, illetve M transzformáció alkalmazása a séma sorainak számát 1-gyel növeli, illetve csökkenti, tehát az eredeti és a transzformáció után keletkező partícióban az összeadandók száma ellentétes paritású. Világos továbbá, hogy A és M egymás inverzei, azaz bármilyen sorrendben történő egymás utáni alkalmazásukkal a kiindulási sémát kapjuk vissza. Ebből következik, hogy az A, M transzformációpár a (*) és (**) típusú partícióktól eltekintve kölcsönösen egyértelmű megfeleltetést létesít az n páros, illetve páratlan sok különböző összeadandóból álló partíciói között. Ebből következik, hogy $s(n) = t(n)$, kivéve ha n-nek létezik (*) vagy (**) típusú partíciója, amikor is $s(n) - t(n)$ aszerint 1, illetve -1, hogy a „rossz" partícióban az összeadandók száma páros, illetve páratlan (ehhez azt is igazolni kell még, hogy egy adott n-nek nem lehet egynél több rossz partíciója).

Ha a (*) partícióban k tag van (azaz a sémában a sorok száma k), akkor

$$n = (2k-1) + (2k-2) + \ldots + k = \frac{(3k-1)k}{2}\,. \tag{8}$$

Ugyanígy adódik, hogy ha a (**) partíció k tagból áll, akkor

$$n = 2k + (2k-1) + \ldots + (k+1) = \frac{(3k+1)k}{2}\,. \tag{9}$$

Adott n-re (8), illetve (9) nyilván legfeljebb egy k-val teljesülhet, továbbá n nem lehet egyszerre (8) és (9) alakú is, ugyanis

$$\frac{(3k-1)k}{2} = \frac{(3j+1)j}{2} \iff (3k-3j-1)(k+j) = 0,$$

ami pozitív egész k és j esetén nem állhat fenn.

Így a (8) és (9) képlettel meghatároztuk a kivételes n-eket, és beláttuk, hogy minden ilyen n-nek csak egy rossz partíciója van. Ezzel a (6) képletet teljes egészében igazoltuk. ■

Mint jeleztük, a 7.9.5 Tételnek fontos következményei vannak a $p(n)$ függvényre nézve is. Legyen $u(n) = s(n) - t(n)$, ekkor a 7.9.5 Tétel szerint $u(n)$ generátorfüggvénye

$$\begin{aligned} U(x) = 1 + \sum_{n=1}^{\infty} u(n)x^n = 1 + \sum_{k=1}^{\infty}(-1)^k \left(x^{\frac{1}{2}(3k^2+k)} + x^{\frac{1}{2}(3k^2-k)}\right) = \\ = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \ldots \end{aligned} \tag{10}$$

Ez a végtelen sor (például) $|x| < 1/2$ esetén abszolút konvergens.

Ugyanakkor $U(x)$ az alábbi ($|x| < 1/2$ esetén konvergens) végtelen szorzatként is előállítható:

$$U(x) = \prod_{i=1}^{\infty}(1-x^i) = \lim_{r\to\infty}\prod_{i=1}^{r}(1-x^i)\,. \tag{11}$$

A (11) igazolásához tekintsük a

$$\prod_{i=1}^{r}(1-x^i) \tag{12}$$

szorzatot. A szorzást elvégezve

$$(-x^{i_1})(-x^{i_2})\ldots(-x^{i_j}) = (-1)^j x^{i_1+i_2+\ldots+i_j} \tag{13}$$

típusú tagok keletkeznek, ahol $0 \le j \le r$ és $i_1, \dots, i_j$ különböző, r-nél nem nagyobb pozitív egészek. (A $j = 0$ esetben az üres szorzatnak megfelelő 1 értéket kapjuk.)

A (12) szorzás elvégzésekor (13) alapján annyiszor keletkezik x^n-es tag $+1$, illetve -1 együtthatóval, ahányféleképpen az n-et elő tudjuk állítani páros, illetve páratlan sok különböző, r-nél nem nagyobb pozitív egész összegeként. Ha $1 \le n \le r$, akkor n bármely partíciójában eleve csak r-nél nem nagyobb tagok szerepelhetnek. Ez azt jelenti, hogy $r \ge n$ esetén (12)-t polinom alakba átírva x^n együtthatója éppen $s(n) - t(n) = u(n)$ lesz.

Ezután (11)-et az $r \to \infty$ határátmenettel kaphatjuk meg, ennek bizonyítását nem részletezzük.

A 7.9.3 Tételből és (11)-ből következik, hogy $p(n)$ és $u(n)$ generátorfüggvényei egymás reciprokai, azaz

$$\Big(1 + \sum_{n=1}^{\infty} p(n)x^n\Big)\Big(1 + \sum_{n=1}^{\infty} u(n)x^n\Big) = P(x)U(x) = 1. \tag{14}$$

Így (14) bal oldalán a két hatványsort összeszorozva minden $n \ge 1$-re x^n együtthatója 0 lesz, vagyis

$$p(n) + p(n-1)u(1) + p(n-2)u(2) + \ldots + p(1)u(n-1) + u(n) = 0. \tag{15}$$

Az $u(j)$ értékeket a 7.9.5 Tételből ismerjük, ezeket (15)-be beírva $p(n)$-re az alábbi rekurziót nyerjük:

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + \ldots \tag{16}$$

A (16) rekurzió érdekessége, hogy a jobb oldalon szereplő tagok száma csak körülbelül $2\sqrt{2n/3}$, és így ez az összefüggés (viszonylag) nagy n esetén is alkalmas $p(n)$ tényleges kiszámítására. Például ily módon határozták meg $p(200)$ értékét is:

$$p(200) = 3\,972\,999\,029\,388.$$

Feladatok

7.9.1 Mutassuk meg, hogy $p(n+1) \le 2p(n)$. Mikor áll egyenlőség?

7.9.2 Számítsuk ki az alábbi határértékeket:

a) $\lim\limits_{n\to\infty} \big(p(n+1) - p(n)\big)$; b) $\lim\limits_{n\to\infty} \big(p(n+1) - 2p(n)\big)$.

7.9.3 Melyek azok a számok, amelyek páratlan sokféleképpen állnak elő különböző pozitív egészek összegeként?

7.9.4 Hányféleképpen írható fel egy n szám pozitív egészek összegeként, ha a csak a tagok sorrendjében eltérő előállításokat is külön számoljuk?

7.9.5 Mutassuk meg, hogy az n pontosan r-tagú és az $n-r$ legfeljebb r-tagú partícióinak a száma azonos.

7.9.6 Írjuk fel a 7.9.4 Tételben szereplő $h_r(n)$ függvény generátorfüggvényét.

7.9.7

a) Legyen $v(n)$ az n szám csupa különböző pozitív egészből történő előállításainak a száma, $w(n)$ pedig a csupa páratlan (de nem feltétlenül különböző) pozitív egészből történő előállítások száma. Mutassuk meg, hogy $v(n) = w(n)$.

b) (Az a) rész általánosítása.) Legyen $v_k(n)$ az n azon partícióinak a száma, ahol az összeadandók között nem szerepel egyetlen szám sem k-szor (vagy többször), $w_k(n)$ pedig azon partíciók száma, ahol egyik összeadandó sem osztható k-val. Ekkor $v_k(n) = w_k(n)$.

7.9.8 Bizonyítsuk be, hogy $|x| < 1/2$ esetén

$$\sum_{n=1}^{\infty} p(n)x^n = \sum_{r=1}^{\infty} \frac{x^r}{(1-x)(1-x^2)\dots(1-x^r)}\,.$$

**7.9.9 Bizonyítsuk be, hogy

$$\sigma(n) - \sigma(n-1) - \sigma(n-2) + \sigma(n-5) + \sigma(n-7) - \dots = \begin{cases} (-1)^{k+1}n, & \text{ha } n = \frac{1}{2}(3k^2 \pm k); \\ 0, & \text{egyébként.} \end{cases}$$

8. DIOFANTIKUS APPROXIMÁCIÓ

Ebben a fejezetben azt vizsgáljuk, mennyire jól közelíthetők az irracionális számok racionálisokkal. Itt az approximáció jóságát a közelítő tört s nevezőjéhez viszonyítjuk. Kiderül, hogy az irracionális számok „tipikusan" $1/s^2$ nagyságrendben közelíthetők. A probléma kezelésénél a geometriai számelmélet egyik alaptételét, a Minkowski-tételt, valamint a lánctörteket is felhasználjuk. Végül bizonyos számsorozatok törtrészeinek elhelyezkedésével foglalkozunk. A diofantikus approximáció már az előző fejezetben tárgyalt Pell-egyenlethez is kapcsolódott (a 7.8.1 Tétel bizonyításában felhasználtuk a 8.1.1 Tételt), és további alkalmazásokat tárgyalunk a következő fejezetben.

8.1. Irracionális szám approximációja

A racionális számok a számegyenesen mindenütt sűrűn helyezkednek el, és így bármely irracionális számnak tetszőlegesen kicsi környezetében található végtelen sok racionális szám. Ebben a fejezetben olyan „erősebb" értelemben vett közelítésekkel foglalkozunk, amikor egy adott irracionális szám és a közelítő tört eltérése a tört nevezőjének függvényében is kicsi. Erre vonatkozik az alábbi alapvető eredmény:

8.1.1 Tétel **T 8.1.1**

Tetszőleges α irracionális számhoz végtelen sok olyan r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2} \,. \quad \clubsuit \tag{1}$$

Megjegyzés: A közelítő r/s törtről mindig eleve feltesszük, hogy $s > 0$. Az is világos, hogy ha egy tört $(r, s) > 1$ esetén kielégíti (1)-et, akkor az egyszerűsítés után kapott r'/s' törtre ez ($s' < s$ miatt) „még inkább" érvényes. Másfelől az is könnyen igazolható (lásd a 8.1.2 feladatot), hogy egy r/s törtnek csak véges sok bővített alakja elégítheti ki (1)-et.

Mindezek alapján a 8.1.1 Tétel (és a későbbi hasonló tételek) állításának igazságát nem befolyásolja, akár végtelen sok különböző r/s racionális számot, akár végtelen sok különböző r/s tört*alak*ot mondunk (ez utóbbi esetben ugyanannak a racionális számnak két vagy több, az (1) feltételt kielégítő r/s alakú felírását külön számoljuk). Ugyanígy, az sem jelentene megszorítást, ha az r/s közelítő törtekre az $(r, s) = 1$ feltételt is előírnánk.

A 8.1.1 Tétel bizonyításához szükségünk lesz az alábbi tételre:

8.1.2 Tétel **T 8.1.2**

Ha α tetszőleges valós szám és n pozitív egész, akkor létezik (legalább egy) olyan r/s tört, amelyre

$$1 \le s \le n \qquad \text{és} \qquad \left|\alpha - \frac{r}{s}\right| < \frac{1}{ns}\,. \ \clubsuit \tag{2}$$

A 8.1.2 Tétel bizonyítása: Egy c valós szám *törtrész*én a $\{c\} = c - \lfloor c \rfloor$ különbséget értjük. Például $\{3\} = 0$; $\{2{,}9\} = 0{,}9$; $\{-2{,}9\} = 0{,}1$. Nyilván $0 \le \{c\} < 1$.

Tekintsük az

$$\{\alpha\},\ \{2\alpha\},\ \ldots,\ \{(n+1)\alpha\}$$

törtrészeket. Ezek valamennyien a $[0,1)$ intervallumba esnek.

Osszuk fel a $[0,1)$ intervallumot n darab $1/n$ hosszúságú balról zárt, jobbról nyílt részintervallumra. Mivel a $\{j\alpha\}$ törtrészek száma $n+1$, a részintervallumoké pedig n, ezért a skatulyaelv értelmében lesz két olyan törtrész, amelyek ugyanabba a részintervallumba esnek, és így a távolságuk kisebb, mint $1/n$. Ez azt jelenti, hogy van olyan $1 \le i < j \le n+1$, amelyre

$$\left|\{j\alpha\} - \{i\alpha\}\right| < \frac{1}{n}\,. \tag{3}$$

A (3) átírható

$$\left|(j\alpha - \lfloor j\alpha \rfloor) - (i\alpha - \lfloor i\alpha \rfloor)\right| = \left|(j-i)\alpha - (\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor)\right| < \frac{1}{n} \tag{4}$$

alakba. Legyen

$$s = j - i \qquad \text{és} \qquad r = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor,$$

ekkor (4)-et s-sel elosztva éppen a lemma állítását kapjuk. ■

A 8.1.1 Tétel bizonyítása: Vegyük észre, hogy (2)-ben $1 \le s \le n$ miatt

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{ns} \le \frac{1}{s^2}\,.$$

Ez azt jelenti, hogy a lemmát α-ra és egy tetszőleges $n = n_1$ pozitív egészre alkalmazva kapunk egy olyan r_1/s_1 törtet, amelyre

$$\left|\alpha - \frac{r_1}{s_1}\right| < \frac{1}{s_1^2}\,.$$

Most az előző lépést n_1 helyett alkalmas n_2-vel megismételjük, ekkor egy r_2/s_2 közelítő törtet állítunk elő. Azt kell csak biztosítani, hogy r_2/s_2 ne lehessen ugyanaz, mint r_1/s_1.

Mivel α irracionális, így $\alpha - r_1/s_1 \neq 0$, tehát n_2 megválasztható úgy, hogy

$$\left|\alpha - \frac{r_1}{s_1}\right| > \frac{1}{n_2}$$

teljesüljön. Ekkor a lemma alapján

$$\left|\alpha - \frac{r_2}{s_2}\right| < \frac{1}{n_2 s_2} \leq \frac{1}{n_2} < \left|\alpha - \frac{r_1}{s_1}\right|,$$

tehát

$$\frac{r_2}{s_2} \neq \frac{r_1}{s_1}\,.$$

Az eljárást hasonlóan folytatva végtelen sok (különböző) megfelelő r_i/s_i törtet kapunk. ■

Megjegyzés: Ha α racionális, akkor természetesen az α-t önmaga approximálja a legjobban. Ezzel együtt az approximációs probléma felvetése racionális α esetén sem teljesen érdektelen, például elméleti és gyakorlati szempontból egyaránt szükség lehet kis nevezőjű törtekkel történő jó közelítésre. Racionális α esetén (magát az α-t nem engedve meg közelítő törtnek) a 8.1.1 Tételben szereplő $1/s^2$-es nagyságrend helyett csak c/s érhető el, ahol c az α-tól függő konstans (lásd a 8.1.1 feladatot).

Az alábbi tétel több irracionális szám közös nevezőjű törtekkel történő approximációjára vonatkozik:

8.1.3 Tétel **T 8.1.3**

Tetszőleges $\alpha_1, \ldots, \alpha_k$ irracionális számokhoz végtelen sok olyan

$$\frac{r_{1i}}{s_i}\,, \quad \frac{r_{2i}}{s_i}\,, \quad \ldots\,, \quad \frac{r_{ki}}{s_i}\,, \qquad i = 1, 2, \ldots$$

közös nevezőjű racionális szám-k-as létezik, amelyre

$$\left|\alpha_j - \frac{r_{ji}}{s_i}\right| < \frac{1}{s_i^{1+\frac{1}{k}}}\,, \qquad j = 1, 2, \ldots, k, \qquad i = 1, 2, \ldots \ \clubsuit \tag{5}$$

A 8.1.3 Tétel a 8.1.1 Tételhez hasonló módon igazolható, ekkor a 8.1.2 Tétel k-dimenziós változatára van szükség:

8.1.4 Tétel **T 8.1.4**

Tetszőleges $\alpha_1, \ldots, \alpha_k$ valós számokhoz és n pozitív egészhez léteznek olyan $r_1, \ldots, r_k$ és s egészek, amelyekre

$$1 \le s \le n^k \qquad \text{és} \qquad \left|\alpha_j - \frac{r_j}{s}\right| < \frac{1}{ns}, \qquad j = 1, 2, \ldots, k. \ \clubsuit$$

A bizonyítások részletes végiggondolását az Olvasóra bízzuk.

A 8.1.1 Tételnek az alábbi élesítése is érvényes, amelyet bizonyítás nélkül közlünk:

8.1.5 Tétel **T 8.1.5**

Tetszőleges α irracionális számhoz végtelen sok olyan r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{\sqrt{5}s^2} \cdot \clubsuit$$

Ennél valamivel gyengébb állítást, a $\sqrt{5}$ helyett 2-vel igazolni fogunk két különböző módon is a 8.2, illetve 8.3 pontban.

A 8.1.5 Tétel tovább már nem javítható:

8.1.6 Tétel **T 8.1.6**

Legyen $\varepsilon > 0$ tetszőleges és $\alpha = (1 + \sqrt{5})/2$. Ekkor csak véges sok olyan r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{(\sqrt{5} + \varepsilon)s^2} \cdot \clubsuit \tag{6}$$

Bizonyítás: Tegyük fel indirekt, hogy (6) végtelen sok r/s-sel teljesül. Mivel adott s-re az s nevezőjű törtek távolsága (legalább) $1/s$, és $s \ge 1$ miatt

$$\frac{1}{s} > \frac{2}{(\sqrt{5} + \varepsilon)s^2},$$

ezért bármely s-hez legfeljebb egy olyan r található, amelyre (6) fennáll.

Ebből következik, hogy a (6)-ot kielégítő végtelen sok r/s tört nevezői között akármilyen nagy számok is előfordulnak.

Az α gyöke az $x^2-x-1=0$ egyenletnek, így $\alpha(\alpha-1)=1$. Ennek alapján a (6) bal oldalán álló különbséget a következő módon „gyökteleníthetjük”:

$$\left(\alpha-\frac{r}{s}\right)\left((\alpha-1)+\frac{r}{s}\right)=\alpha(\alpha-1)+\frac{r}{s}(\alpha-(\alpha-1))-\frac{r^2}{s^2}=1+\frac{r}{s}-\frac{r^2}{s^2}\,. \quad (7)$$

A (7) jobb oldalán egy s^2 nevezőjű tört áll, amely α irracionalitása miatt nem nulla, és így abszolút értéke legalább $1/s^2$. Ebből (7) alapján következik, hogy

$$\left|\alpha-\frac{r}{s}\right|\cdot\left|(\alpha-1)+\frac{r}{s}\right|\ \geq\ \frac{1}{s^2}\,. \quad (8)$$

Mivel (6) szerint r/s „közel” van α-hoz, ezért a (8) bal oldalán álló második tényező értéke „körülbelül” $2\alpha-1=\sqrt{5}$, és ezzel ellentmondásba kerülünk (6)-tal. Ennek precíz kivitelezéséhez induljunk ki az

$$\left|(\alpha-1)+\frac{r}{s}\right|\ \leq\ (2\alpha-1)+\left|\frac{r}{s}-\alpha\right|<\sqrt{5}+\frac{1}{\sqrt{5}s^2} \quad (9)$$

felső becslésből. Ha s elég nagy, akkor

$$\frac{1}{\sqrt{5}s^2}\ <\ \varepsilon\,,$$

tehát (9)-ből kapjuk, hogy

$$\left|(\alpha-1)+\frac{r}{s}\right|\ <\ \sqrt{5}+\varepsilon\,. \quad (10)$$

A (8) és (10) egyenlőtlenségekből következik, hogy elég nagy s-re

$$\left|\alpha-\frac{r}{s}\right|\ >\ \frac{1}{(\sqrt{5}+\varepsilon)s^2}\,,$$

ami ellentmond az indirekt feltevésnek. ■

A 8.1.6 Tétel mutatja, hogy a 8.1.5 és 8.1.1 Tételek az irracionális számok approximálhatóságának a helyes nagyságrendjét jelentik, hiszen van olyan α irracionális szám, amely egyáltalán nem (illetve csak „alig”) approximálható jobban, mint amit ezek a tételek biztosítanak.

A következőkben belátjuk, hogy a 8.1.5 és 8.1.1 Tételek más értelemben véve is az irracionális számok approximálhatóságának a helyes nagyságrendjét adják: olyan irracionális szám is csak „kevés” van, amelyre „lényegesen” jobb közelítés érhető el. A „kevés” pontos megfogalmazásához bevezetjük a *nullmértékű* halmaz fogalmát:

8.1.7 Definíció **D 8.1.7**

A valós számok egy H részhalmaza *nullmértékű*, ha tetszőleges $\varepsilon > 0$-hoz létezik megszámlálható sok olyan intervallum, amelyek együttesen lefedik H-t és amelyek összhossza kisebb, mint ε. ♣

Könnyen adódik, hogy minden megszámlálható H, így speciálisan a racionális számok halmaza is nullmértékű, léteznek azonban kontinuum számosságú nullmértékű halmazok is (lásd a 8.1.9 feladatot).

8.1.8 Tétel **T 8.1.8**

Legyen $\kappa > 0$ tetszőleges valós szám és H azoknak az α valós számoknak a halmaza, amelyekhez végtelen sok olyan r/s található, hogy

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2+\kappa}} \tag{11}$$

teljesül. Ekkor H nullmértékű. ♣

Bizonyítás: Legyen

$$H_i = H \cap [i, i+1), \qquad i = 0, \pm 1, \pm 2, \dots$$

A (11) szerinti approximálhatóság csak az α törtrészétől függ, ezért a H_i halmazok közül bármely kettő egybevágó. Így elég belátni, hogy H_0 nullmértékű, hiszen

$$H = \bigcup_{i=-\infty}^{\infty} H_i$$

és megszámlálható sok nullmértékű halmaz egyesítése is nullmértékű (lásd a 8.1.10c feladatot).

Adott $s > 1$ pozitív egészhez legyen A_s azoknak a $0 \le \alpha < 1$ valós számoknak a halmaza, amelyekre (11) teljesül alkalmas r-rel. Ekkor A_s nyilván a

$$\frac{0}{s}\,, \quad \frac{1}{s}\,, \quad \dots\,, \quad \frac{s}{s}$$

körüli $1/s^{2+\kappa}$ sugarú nyílt intervallumokból, illetve ezeknek a $[0,1)$-be eső részeiből tevődik össze, azaz

$$A_s = \left(\bigcup_{r=1}^{s-1}\Big(\frac{r}{s} - \frac{1}{s^{2+\kappa}}\,,\ \frac{r}{s} + \frac{1}{s^{2+\kappa}}\Big)\right) \bigcup \Big[0\,,\ \frac{1}{s^{2+\kappa}}\Big) \bigcup \Big(1 - \frac{1}{s^{2+\kappa}}\,,\ 1\Big)\,. \tag{12}$$

Az A_s-t alkotó intervallumok összhossza

$$(s-1)\frac{2}{s^{2+\kappa}} + 2\frac{1}{s^{2+\kappa}} = \frac{2s}{s^{2+\kappa}} = \frac{2}{s^{1+\kappa}}\,. \tag{13}$$

Ha $\alpha \in H_0$, akkor a feltétel szerint végtelen sok olyan s van, amelyre $\alpha \in A_s$. Ebből következik, hogy tetszőleges m esetén

$$H_0 \subseteq \bigcup_{s=m}^{\infty} A_s\,. \tag{14}$$

Ekkor (12), (13) és (14) alapján H_0 lefedhető megszámlálható sok intervallummal, amelyek összhossza

$$\sum_{s=m}^{\infty} \frac{2}{s^{1+\kappa}}\,. \tag{15}$$

Mivel a

$$\sum_{s=1}^{\infty} \frac{1}{s^{1+\kappa}}$$

végtelen sor konvergens, ezért tetszőleges $\varepsilon > 0$-hoz található olyan m, amelyre a (15)-beli összeg kisebb, mint ε. Ezzel beláttuk, hogy H_0, és így H is nullmértékű. ■

A 8.1.8 Tétel általánosításaként a következő kérdést is megvizsgálhatjuk. Legyen f a pozitív egészeken értelmezett pozitív értékű függvény, amelyre $f(s)/s$ monoton nő, és $H(f)$ azoknak az α valós számoknak a halmaza, amelyekhez végtelen sok olyan r/s található, hogy

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{sf(s)}\,.$$

A 8.1.8 Tétel bizonyításához hasonlóan igazolható, hogy ha

$$\sum_{s=1}^{\infty} \frac{1}{f(s)} < \infty\,,$$

akkor $H(f)$ nullmértékű.

Ha azonban

$$\sum_{s=1}^{\infty} \frac{1}{f(s)} = \infty\,,$$

akkor teljesen megfordul a helyzet: ekkor nullmértékű halmaztól *eltekintve* $H(f)$ minden valós számot tartalmaz. Ez utóbbi eredménynek jóval nehezebb a bizonyítása.

Feladatok

8.1.1 Legyen α rögzített racionális szám: $\alpha = a/b$, ahol $(a, b) = 1$ és $b > 0$.

a) Bizonyítsuk be, hogy

$$\frac{r}{s} \neq \frac{a}{b} \Longrightarrow \left|\alpha - \frac{r}{s}\right| \geq \frac{1}{bs}\,. \tag{16}$$

b) Mutassuk meg, hogy végtelen sok olyan r/s tört létezik, amikor (16) jobb oldalán egyenlőség teljesül.

8.1.2 A 8.1.1 Tételben az (1) egyenlőtlenséget esetleg egy adott racionális számnak több r/s alakja is kielégítheti. Mutassuk meg, hogy (1) nem teljesülhet ugyanannak a racionális számnak végtelen sok r/s alakjával.

8.1.3 Legyen α irracionális szám, és tekintsünk végtelen sok olyan r_i/s_i törtet, amelyre

$$\left|\alpha - \frac{r_i}{s_i}\right| < \frac{1}{s_i^2}\,, \qquad i = 1, 2, \ldots$$

Bizonyítsuk be, hogy

$$\text{a)}\ \lim_{i\to\infty} s_i = \infty; \qquad \text{b)}\ \lim_{i\to\infty} \frac{r_i}{s_i} = \alpha\,.$$

8.1.4 Bizonyítsuk be az alábbi állításokat:

a) Minden α valós számhoz végtelen sok olyan $r/2^k$ alakú tört létezik, amelyre

$$\left|\alpha - \frac{r}{2^k}\right| \leq \frac{1}{3\cdot 2^k}\,.$$

b) Van olyan α, hogy bármely $r/2^k$ alakú tört esetén

$$\left|\alpha - \frac{r}{2^k}\right| \geq \frac{1}{3\cdot 2^k}\,.$$

c) Minden α valós számhoz végtelen sok olyan $r/3^k$ alakú tört létezik, amelyre

$$\left|\alpha - \frac{r}{3^k}\right| \leq \frac{1}{2\cdot 3^k}\,.$$

d) Van olyan α, hogy bármely $r/3^k$ alakú tört esetén

$$\left|\alpha - \frac{r}{3^k}\right| \geq \frac{1}{2 \cdot 3^k} .$$

e) Minden $\alpha > 0$ irracionális számhoz végtelen sok r^2/s^2 alakú tört létezik, amelyre

$$\left|\alpha - \frac{r^2}{s^2}\right| < \frac{c(\alpha)}{s^2} ,$$

ahol $c(\alpha)$ egy α-tól függő konstans.

f) Van olyan $\alpha > 0$ irracionális szám és c konstans, hogy bármely r^2/s^2 alakú tört esetén

$$\left|\alpha - \frac{r^2}{s^2}\right| > \frac{c}{s^2} .$$

8.1.5 Bizonyítsuk be, hogy minden α irracionális számhoz végtelen sok olyan különböző számlálójú r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{c(\alpha)}{r^2} ,$$

ahol $c(\alpha)$ az α-tól függő konstans.

8.1.6 Bizonyítsuk be, hogy létezik olyan c konstans, hogy bármely r/s tört esetén

$$\left|\sqrt{2} - \frac{r}{s}\right| > \frac{c}{s^2} .$$

8.1.7 Legyen $t > 1$ tetszőleges valós szám. Nevezzünk egy α valós számot t-edrendben approximálhatónak, ha végtelen sok olyan r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{c(\alpha)}{s^t}$$

teljesül, ahol $c(\alpha)$ egy α-tól függő konstans. (Így a 8.1.1 Tételből következik, hogy minden irracionális szám másodrendben approximálható, a 8.1.8 Tétel szerint viszont a 2-nél nagyobb rendben approximálható valós számok halmaza nullmértékű.)

Tegyük fel, hogy az α valós szám 20-adrendben approximálható. Bizonyítsuk be, hogy ekkor

a) $a\alpha + b$ is 20-adrendben approximálható, ha a, b racionális és $a \neq 0$;

b) α^2 10-edrendben approximálható.

8.1.8 Határozzuk meg a törtrészekből képzett alábbi kifejezések összes lehetséges értékét, ha α és β egymástól függetlenül befutják a valós számokat:

a) $\{\alpha\}+\{\beta\}-\{\alpha+\beta\}$; b) $\{\alpha\}\{\beta\}-\{\alpha\beta\}$; **M***c) $\{\alpha\}^2-\{\alpha^2\}$.

8.1.9

a) Mutassuk meg, hogy a valós számok minden megszámlálható részhalmaza nullmértékű.

*b) Tekintsük azokat a 0 és 1 közé eső valós számokat, amelyek hármas alapú számrendszer szerinti „tizedes" (azaz „harmados") tört alakjában nem szerepel 1-es számjegy (ez az ún. Cantor-halmaz). Bizonyítsuk be, hogy ennek a halmaznak kontinuum sok eleme van, ugyanakkor nullmértékű.

8.1.10 Bizonyítsuk be az alábbi állításokat:

a) Egy nullmértékű halmaz bármely részhalmaza is nullmértékű.

b) Véges sok nullmértékű halmaz egyesítése is nullmértékű.

c) Megszámlálható sok nullmértékű halmaz egyesítése is nullmértékű.

d) Megszámlálhatónál több nullmértékű halmaz egyesítése lehet nullmértékű, de nem feltétlenül az.

8.2. Minkowski-tétel

Ebben a pontban egy fontos geometriai számelméleti tétellel és annak néhány alkalmazásával foglalkozunk.

8.2.1 Tétel (Minkowski-tétel) **T 8.2.1**

Legyen L a síkon egy tetszőleges paralelogrammarács, és H olyan zárt, konvex, síkbeli halmaz, amely középpontosan szimmetrikus az egyik rácspontra. Tegyük fel, hogy H területe legalább 4Δ, ahol Δ a rács alapparalelogrammájának a területe. Ekkor H a középpontján kívül is tartalmaz rácspontot.

♣

Megjegyzések: 1. Könnyen ellenőrizhető, hogy a tétel feltételei szükségesek.

2. Feltehetjük, hogy H korlátos. Ugyanis megmutatható, hogy ha egy konvex halmaz nem korlátos, akkor a területe csak nulla vagy végtelen lehet, így ez utóbbi esetben a H-nak egy a középpontja körüli elég nagy sugarú

(zárt) körrel való metszete már olyan középpontosan szimmetrikus, korlátos, zárt, konvex halmaz lesz, amelynek a területe legalább 4Δ.

3. A tétel magasabb dimenziós, illetve nagyobb területű halmazok esetén több rácspontot garantáló általánosításaira vonatkozóan lásd a 8.2.1 és 8.2.2 feladatokat.

A Minkowski-tételre két bizonyítást adunk. Jelöljük H szimmetria-középpontját O-val, területét pedig h-val.

Első bizonyítás: Tekintsük először azt az esetet, amikor $h > 4\Delta$.

Kicsinyítsük le az L rácsot az O pontból $2/k$ arányban, ahol k (nagy) egész szám, és legyen $N(k)$ az így kapott L_k rácsban azoknak a rácspontoknak a száma, amelyek benne vannak H-ban. Az L_k rács alapparalelogrammájának a területe $4\Delta/k^2$, ezért H területe

$$h = \lim_{k\to\infty} N(k)\frac{4\Delta}{k^2}\,. \tag{1}$$

Mivel $h > 4\Delta$, ezért (1)-ből következik, hogy elég nagy k esetén $N(k) > k^2$.

Vegyük azt a(z általában ferdeszögű) koordináta-rendszert, amelynek a kezdőpontja O, a tengelyek pedig párhuzamosak az alapparalelogramma oldalaival. Ekkor az L rács rácspontjainak a koordinátái (ia, jb), az L_k rács rácspontjainak koordinátái pedig

$$\Big(\frac{2i}{k}a\,,\ \frac{2j}{k}b\Big)\,,$$

ahol a, illetve b az L rács alapparalelogrammájának megfelelő oldalai, i és j pedig tetszőleges egész számok.

Mivel az (i, j) számpárok k-val való maradékos osztásakor k^2-féle „maradékpár" keletkezhet, és $N(k) > k^2$, ezért a skatulyaelv szerint létezik az L_k rácsnak két olyan (különböző) rácspontja,

$$Q_1 = \Big(\frac{2i_1}{k}a\,,\ \frac{2j_1}{k}b\Big) \qquad \text{és} \qquad Q_2 = \Big(\frac{2i_2}{k}a\,,\ \frac{2j_2}{k}b\Big)\,,$$

amelyekre

$$k \mid i_1 - i_2 \qquad \text{és} \qquad k \mid j_1 - j_2\,. \tag{2}$$

Ekkor H középpontos szimmetriája miatt a Q_2 pontnak az O-ra vonatkozó tükörképe

$$Q_2' = \Big(\frac{-2i_2}{k}a\,,\ \frac{-2j_2}{k}b\Big)$$

is H-beli, továbbá a konvexitás miatt a Q_1Q_2' szakasz felezőpontja

$$F = \Big(\frac{2i_1 - 2i_2}{2k}a\,,\ \frac{2j_1 - 2j_2}{2k}b\Big)$$

is H-beli. A (2)-beli oszthatóságok miatt $F = (ra, sb)$, ahol r és s egész számok, tehát F az eredeti L rácsnak is rácspontja. Mivel $Q_1 \neq Q_2$, ezért $F \neq O$. Ezzel igazoltuk, hogy H az O-n kívül is tartalmaz L-beli rácspontot.

Hátravan még annak az esetnek az igazolása, amikor $h = 4\Delta$. Tegyük fel indirekt, hogy H az O középpontján kívül nem tartalmaz (L-beli) rácspontot. Legyen a $P \neq O$ rácspontok H-tól való távolságának a minimuma m. Mivel H zárt, ezért $m > 0$. Ez azt jelenti, hogy H-t az O-ból ki tudjuk úgy nagyítani, hogy a kinagyított H' sem tartalmaz O-tól különböző rácspontot. Ez azonban lehetetlen, hiszen H' területe nagyobb, mint 4Δ. ■

Második bizonyítás: Először egy lemmát igazolunk, amely azt a „szemléletesen nyilvánvaló" tényt fejezi ki, hogy ha egy korlátos síkbeli halmaznak az összes rácsvektorral eltolt példányai páronként diszjunktak, akkor a halmaz területe nem lehet nagyobb a rács alapparalelogrammájának a területénél.

8.2.2 Lemma **L 8.2.2**

Legyen az L paralelogrammarács alapparalelogrammájának területe Δ, a K korlátos síkbeli halmaz területe pedig t. Legyen továbbá O rögzített rácspont, P tetszőleges rácspont, és jelöljük K_P-vel a K halmaznak az OP vektorral való eltoltját ($K_O = K$). Végül tegyük fel, hogy a K_P halmazok diszjunktak. Ekkor $t \leq \Delta$. ♣

A 8.2.2 Lemma bizonyítása: A bizonyítás lényege a következő észrevétel: Az alapparalelogrammát (minden irányban) nagyítsuk ki r-szeresére, ahol r egy „nagy" szám, és az így kapott M paralelogrammát helyezzük el úgy, hogy az O pont körülbelül M „közepére" essen. Ekkor a K-nak az M-beli rácspontok szerinti eltoltjai „nem nagyon lóghatnak ki" M-ből, és így ezen eltolt példányok együttes területe, ami (körülbelül) r^2t, nem lehet „sokkal" nagyobb az M területénél, azaz $r^2\Delta$-nál. Az állítás innen $r \to \infty$ határátmenettel adódik.

Nézzük mindezt pontosan és részletesen. Vegyük azt a (8.2.1 Tétel első bizonyításában már használt, általában ferdeszögű) koordináta-rendszert, amelynek a kezdőpontja O, a tengelyek pedig párhuzamosak az alapparalelogramma oldalaival. Ekkor az L rács rácspontjainak koordinátái (ia, jb), ahol a, illetve b az alapparalelogramma megfelelő oldalai, i és j pedig tetszőleges egész számok.

Legyen n tetszőleges pozitív egész, és tekintsük azt a $(2n+1)^2$ darab $P_{ij} = (ia, jb)$ rácspontot, amelyre $|i| \le n$ és $|j| \le n$. Az ezekhez tartozó K_P halmazok egyesítését jelöljük U_n-nel. Ekkor U_n területe $(2n+1)^2 t$.

A K korlátossága miatt van olyan $c > 0$, hogy K bármely pontjának koordinátái kisebb abszolút értékűek, mint ca, illetve cb. Ekkor U_n része annak a G_n paralelogrammának, amelynél a négy csúcs koordinátái

$$\big(\pm a(n+c)\,,\ \pm b(n+c)\big),$$

és így G_n területe $(2n+2c)^2\Delta$. A tartalmazás miatt U_n területe legfeljebb akkora, mint G_n területe, azaz

$$(2n+1)^2 t \le (2n+2c)^2 \Delta\,.$$

Ebből kapjuk, hogy

$$t \le \Big(1 + \frac{2c-1}{2n+1}\Big)^2 \Delta\,.$$

Innen a kívánt $t \le \Delta$ egyenlőtlenség az $n \to \infty$ határátmenettel következik. ■

Rátérve a 8.2.1 Tétel bizonyítására, most is elég a $h > 4\Delta$ esetet tekintenünk.

Kicsinyítsük le H-t az O középpontból a felére, az így kapott halmazt jelöljük K-val. A feltétel szerint K területe $t = h/4 > \Delta$, így a 8.2.2 Lemma alapján létezik olyan Q és R rácspont, amelyre K_Q-nak és K_R-nek van közös pontja. A QO vektorral történő eltolással azt kapjuk, hogy $K_O = K$-nak és K_P-nek is van közös pontja, ahol P alkalmas (az O-tól különböző) rácspont. Azt fogjuk igazolni, hogy a P rácspont benne van H-ban (és ezzel a tétel állítását beláttuk).

Legyen A közös pontja K-nak és K_P-nek, B az A-nak a PO vektorral való eltoltja, C a B tükörképe O-ra, és végül D az AC szakasz felezőpontja.

Mivel A eleme K_P-nek, ezért B eleme K-nak. A K középpontos szimmetriája miatt C is eleme K-nak. Végül A és C is K-beli, tehát a konvexitás miatt a D felezőpont is K-beli.

Ugyanakkor a konstrukció szerint $PAOC$ paralelogramma, hiszen az OC és AP oldalak párhuzamosak és egyenlők. Ezért D az OP átlónak is felezőpontja, és így D-t az O középpontú kétszeres nagyítás P-be viszi. Mivel ez a nagyítás a K halmazt éppen H-ba viszi, és a D pont K-ban van, ezért a P pont szükségképpen H-beli. Ezzel beláttuk, hogy H tartalmazza az O-tól különböző P rácspontot is. ■

A Minkowski-tételt először a diofantikus approximációnál alkalmazzuk a 8.1.1 Tétel javítására.

8.2.3 Tétel **T 8.2.3**

Tetszőleges α irracionális számhoz végtelen sok olyan r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2} \,. \quad \clubsuit \tag{3}$$

Bizonyítás: Az (3) egyenlőtlenség $s \neq 0$ esetén ekvivalens

$$|s(s\alpha - r)| < \frac{1}{2} \tag{4}$$

teljesülésével. Vezessük be az

$$x = s\alpha - r, \qquad y = s$$

új változókat. Ha r és s egymástól függetlenül végigfut az egész számokon, akkor az (x, y) pontok egy olyan paralelogrammarácsot alkotnak, amelynél az alapparalelogramma csúcsai

$$(0,0), \qquad (-1,0), \qquad (\alpha,1), \qquad (\alpha-1,1)\,. \tag{5}$$

Az új változók szerint (4) az $|xy| < 1/2$ feltételt jelenti, azaz azokat az (x, y) rácspontokat keressük, amelyek az $xy = 1/2$ és $xy = -1/2$ hiperbolák által határolt (az origót is tartalmazó) tartományba esnek. rácspontra az $xy = \pm 1/2$ egyenlőség az α irracionalitása miatt sohasem teljesülhet, így nem jelent változást, ha (3)-ban, illetve (4)-ben a $<$ jel helyett $\leq$ jelet írunk. Ennek alapján az iménti tartományhoz a határoló hiperbolaágakat is hozzávehetjük, és a továbbiakban az így keletkező zárt Z halmazt tekintjük.

Az $s \neq 0$ feltétel azt jelenti, hogy az x-tengelyre eső rácspontokat figyelmen kívül kell hagynunk.

A rács (5) alapparalelogrammájában a „vízszintes” oldal és az ehhez tartozó magasság is egységnyi hosszúságú, tehát az alapparalelogramma területe $\Delta = 1$.

A Z halmaz nem konvex (és nem is korlátos), ezért Minkowski tételét nem tudjuk közvetlenül magára Z-re alkalmazni. Ehelyett Z alkalmas konvex részhalmazait fogjuk tekinteni: olyan rombuszokat, amelyek csúcsai a hiperbola tengelyein vannak, és érintik a négy hiperbolaágat. Ezek a rombuszok konvex, zárt és az origóra szimmetrikus halmazok.

Megmutatjuk, hogy minden ilyen rombusz területe 4. Ha a rombusz az első síknegyedbeli hiperbolaágat az $\big(a\,,\,1/(2a)\big)$ pontban érinti, akkor az érintő egyenlete

$$y - \frac{1}{2a} = \frac{-1}{2a^2}(x - a)\,.$$

Ez az egyenes a koordinátatengelyeket az $x = 2a$, illetve $y = 1/a$ pontokban metszi. Így az origó és ezen két csúcs alkotta derékszögű háromszög területe $\frac{1}{2}(2a)(1/a) = 1$, és a rombusz területe ennek négyszerese, azaz 4.

Mivel a terület $4 = 4\Delta$, ezért Minkowski tétele szerint minden ilyen rombusz tartalmaz az origón kívül rácspontot.

Válasszuk a rombuszokat rendre úgy, hogy az y-tengely irányában egyre „keskenyebbek" legyenek. Ekkor elérhető, hogy minden újabb rombusz az előző rombuszok által tartalmazott nemtriviális rácspontok egyikét se tartalmazza, továbbá egyáltalán ne tartalmazzon az x-tengelyen az origótól különböző rácspontot. Ily módon végtelen sok megfelelő rácspontot kapunk (a középpontos szimmetria miatt a szokásos $s > 0$ feltétel is elérhető). ■

A Minkowski-tétel második alkalmazásaként új bizonyítást adunk a 7.5.1 Tétel azon részállítására, hogy minden $4k + 1$ alakú $p > 0$ prímszám előáll két négyzetszám összegeként.

8.2.4 Tétel **T 8.2.4**

Minden $4k + 1$ alakú $p > 0$ prímszám felírható két négyzetszám összegeként. ♣

Bizonyítás: A 4.1.4 Tétel alapján létezik olyan c, amelyre $c^2 \equiv -1 \pmod{p}$.

Tekintsük a síkon az

$$x = pu + cv, \qquad y = v \tag{6}$$

koordinátájú pontokat, ahol u és v egymástól függetlenül befutják az egész számokat. Ezek egy paralelogrammarácsot alkotnak, amelyben az alapparalelogramma területe $\Delta = p$.

Bármely rácspont esetén

$$x^2 + y^2 = (pu + cv)^2 + v^2 = p(pu^2 + 2cuv) + v^2(c^2 + 1) \equiv 0 \pmod{p},$$

azaz $p \mid x^2 + y^2$. Ebből következik, hogy ha egy, az origótól különböző rácspontra $x^2 + y^2 < 2p$, akkor a kívánt $x^2 + y^2 = p$ előállítás adódik.

alkalmazzuk Minkowski tételét az $x^2 + y^2 \le 4p/\pi$ egyenletű, origó körüli $4p = 4\Delta$ területű (zárt) körlapra. A tétel szerint ez a kör az origón kívül is tartalmaz legalább egy (x, y) rácspontot. Így erre a rácspontra teljesül

$$x^2 + y^2 \le \frac{4p}{\pi} < 2p. \blacksquare$$

Megjegyezzük, hogy a 3-dimenziós Minkowski-tételnek (lásd a 8.2.1a feladatot) a fentiekhez hasonló elveken alapuló, de jóval bonyolultabb alkalmazása a három-négyzetszám-tétel (7.5.2 Tétel) bizonyítás nélkül közölt „nehéz" részének igazolásához is elvezet (közben a számtani sorozatok prímszámaira vonatkozó Dirichlet-tételt is fel kell használni).

A Minkowski-tétel néhány további alkalmazására nézve lásd a 8.2.3–8.2.5 feladatokat.

Feladatok

8.2.1

a) Bizonyítsuk be a térbeli Minkowski-tételt: Legyen L a térben egy tetszőleges paralelepipedonrács, és H olyan zárt, konvex, térbeli halmaz, amely középpontosan szimmetrikus az egyik rácspontra. Tegyük fel, hogy H térfogata legalább 8Δ, ahol Δ a rács alapparalelepipedonjának a térfogata. Ekkor H a középpontján kívül is tartalmaz rácspontot.

b) Általánosítsuk a tételt tetszőleges dimenzióra.

8.2.2 Igazoljuk a Minkowski-tétel alábbi általánosítását: Ha L és H eleget tesznek a 8.2.1 Tétel feltételeinek, és H területe legalább $4r\Delta$, ahol $r > 0$ egész, akkor H a középpontján kívül legalább $2r$ darab rácspontot tartalmaz.

8.2.3 Bizonyítsuk be, hogy minden $3k+1$ alakú pozitív prímszám felírható alkalmas x, y egészekkel $x^2 + 3y^2$ alakban.

8.2.4 Legyenek a_{11}, a_{12}, a_{21}, a_{22} olyan egész számok, amelyekre

$$D = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0.$$

Bizonyítsuk be, hogy ha a b_1, b_2 pozitív számokra $b_1 b_2 \geq |D|$, akkor az

$$|a_{11}x_1 + a_{12}x_2| \leq b_1, \qquad |a_{21}x_1 + a_{22}x_2| \leq b_2$$

egyenlőtlenségrendszernek létezik nemtriviális (azaz az $(x_1, x_2) = (0,0)$-tól különböző) egész megoldása.

*8.2.5 Bizonyítsuk be, hogy tetszőleges α_1 és α_2 irracionális számokhoz végtelen sok olyan közös nevezőjű r_1/s, r_2/s racionális számpár létezik, amelyre

$$\left|\alpha_j - \frac{r_j}{s}\right| < \frac{2}{3} \cdot \frac{1}{s^{3/2}}, \qquad j = 1, 2.$$

8.3. Lánctörtek

Tetszőleges α valós szám esetén tekintsük a következő algoritmust. Legyen

$$c_0 = \lfloor \alpha \rfloor \qquad \text{és} \qquad \alpha_1 = \{\alpha\}, \qquad \text{ekkor} \qquad \alpha = c_0 + \alpha_1. \tag{1}$$

Ha $\alpha_1 \neq 0$, akkor legyen

$$c_1 = \left\lfloor \frac{1}{\alpha_1} \right\rfloor \qquad \text{és} \qquad \alpha_2 = \left\{ \frac{1}{\alpha_1} \right\}, \qquad \text{ekkor} \qquad \alpha = c_0 + \alpha_1 = c_0 + \frac{1}{c_1 + \alpha_2}\,.$$

Ha $\alpha_2 \neq 0$, akkor $1/\alpha_2$ egész- és törtrészét képezzük stb. Általában, ha a $c_0, c_1, \ldots, c_n$ és $\alpha_1, \ldots, \alpha_{n+1}$ értékeket már meghatároztuk, és $\alpha_{n+1} \neq 0$, akkor legyen

$$c_{n+1} = \left\lfloor \frac{1}{\alpha_{n+1}} \right\rfloor \qquad \text{és} \qquad \alpha_{n+2} = \left\{ \frac{1}{\alpha_{n+1}} \right\}, \tag{2}$$

ekkor

$$\alpha = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots \; c_n + \cfrac{1}{c_{n+1} + \alpha_{n+2}}}}}\,. \tag{3}$$

A (3) jobb oldalán álló sokemeletes törtet (véges) *lánctört*nek nevezzük, és az egyszerűbb írásmód kedvéért bevezetjük rá az $L(c_0, c_1, \ldots, c_n, c_{n+1} + \alpha_{n+2})$ jelölést. (A (3) képlet jobb oldalára ezt a jelölést néha olyan esetben is fogjuk alkalmazni, amikor a c_i értékek nem feltétlenül egész számok.)

Ha $\alpha_{n+1} = 0$, akkor az eljárás véget ér.

Az ily módon kapott $c_0, c_1, \ldots,$ egész számokat az α *lánctörtjegyei*nek nevezzük.

8.3.1 Definíció **D 8.3.1**

Egy α valós szám *lánctörtjegyei*n az (1) és (2) képletekkel definiált (véges vagy végtelen) $c_0, c_1, \ldots$ számsorozatot értjük. ♣

A definíció alapján világos, hogy a lánctörtjegyek egyértelműen meghatározott egész számok, és $c_i > 0$, ha $i \geq 1$.

Példák:

P1 Legyen $\alpha = 111/25$. Ekkor

$$\begin{aligned}
\frac{111}{25} &= 4 + \frac{11}{25}\,, & c_0 &= 4,\\
\frac{25}{11} &= 2 + \frac{3}{11}\,, & c_1 &= 2,\\
\frac{11}{3} &= 3 + \frac{2}{3}\,, & c_2 &= 3,\\
\frac{3}{2} &= 1 + \frac{1}{2}\,, & c_3 &= 1,\\
\frac{2}{1} &= 2 + 0\,, & c_4 &= 2.
\end{aligned}$$

A 111/25 lánctörtjegyei tehát 4, 2, 3, 1, 2. Ez egyúttal azt is jelenti, hogy

$$\frac{111}{25} = L(4,2,3,1,2) = 4 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2}}}}$$

P2 Legyen $\alpha = \sqrt{2}$. Ekkor

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1), & c_0 &= 1,\\
\frac{1}{\sqrt{2}-1} &= \sqrt{2} + 1 = 2 + (\sqrt{2} - 1), & c_1 &= 2,\\
\frac{1}{\sqrt{2}-1} &= \sqrt{2} + 1 = 2 + (\sqrt{2} - 1), & c_2 &= 2,\\
&\vdots
\end{aligned}$$

A $\sqrt{2}$ lánctörtjegyei tehát 1, 2, 2, 2, ... Erre is bevezetjük (egyelőre formálisan) a $\sqrt{2} = L(1,2,2,\ldots)$ jelölést és a „végtelen lánctört” elnevezést.

8.3.2 Tétel **T 8.3.2**

Az α valós szám lánctörtjegyeinek sorozata akkor és csak akkor véges, ha α racionális. ♣

Bizonyítás: Legyen a lánctörtjegyek sorozata véges, azaz megfelelő c_i egészekkel $\alpha = L(c_0, c_1, \ldots, c_k)$. Ekkor az emeletes törteket lebontva α végül két egész szám hányadosaként írható, tehát racionális.

Megfordítva, legyen $\alpha = a/b$, ahol $b > 0$ és a egész számok. Megmutatjuk, hogy ekkor a lánctörtjegyeket megadó algoritmus lépései tulajdonképpen az a-ra és b-re vonatkozó euklideszi algoritmus lépéseinek felelnek meg. Ebből következik, hogy a lánctörtjegyeket előállító algoritmus véges sok lépésben befejeződik.

Az euklideszi algoritmus első lépésében az a számot maradékosan elosztjuk b-vel:

$$a = bq_1 + r_1, \qquad 0 \le r_1 < b\,.$$

Ez átírható az

$$\frac{a}{b} \;=\; q_1 + \frac{r_1}{b} \;=\; \left\lfloor \frac{a}{b} \right\rfloor \;+\; \left\{ \frac{a}{b} \right\}$$

alakba, tehát (a lánctört-algoritmus jelöléseivel) $c_0 = q_1$ és $\alpha_1 = r_1/b$.

Ha $r_1 \neq 0$, akkor az euklideszi algoritmus következő lépése

$$b = r_1 q_2 + r_2, \qquad 0 \le r_2 < r_1\,,$$

azaz

$$\frac{1}{\alpha_1} \;=\; \frac{b}{r_1} \;=\; q_2 + \frac{r_2}{r_1} \;=\; \left\lfloor \frac{b}{r_1} \right\rfloor \;+\; \left\{ \frac{b}{r_1} \right\},$$

tehát $c_1 = q_2$ és $\alpha_2 = r_2/r_1$.

Ugyanígy adódik, hogy a további lánctörtjegyek is rendre az euklideszi algoritmusban szereplő hányadosok lesznek. ■

A továbbiakban feltesszük, hogy α irracionális, és megmutatjuk, hogy a lánctörtek segítségével az α-t jól közelítő racionális számokat tudunk előállítani. Ezek az α (végtelen) „lánctörtalakjának" a (véges) „szeletei" lesznek, azaz azok a (véges) lánctörtek, amelyeket tetszőleges $n \ge 0$ egészre az α első $n+1$ darab lánctörtjegyéből képezünk. Jelöljük ezeket a racionális számokat $L_n(\alpha)$-val, azaz ha $\alpha = L(c_0, c_1, \ldots)$, akkor

$$L_n(\alpha) = L(c_0, c_1, \ldots, c_n), \qquad n = 0, 1, 2, \ldots \tag{4}$$

8.3.3 Tétel **T 8.3.3**

Legyenek az α irracionális szám lánctörtjegyei $c_0, c_1, \ldots$, és

$$L_n(\alpha) = L(c_0, c_1, \ldots, c_n) = \frac{r_n}{s_n}, \qquad \text{ahol} \qquad (r_n, s_n) = 1,\ s_n > 0\,. \tag{5}$$

Ekkor bármely n esetén fennáll

$$\left|\alpha - \frac{r_n}{s_n}\right| < \frac{1}{s_n^2}\,, \tag{6}$$

sőt, ha $n > 0$, akkor az

$$\left|\alpha - \frac{r_n}{s_n}\right| < \frac{1}{2s_n^2}\,, \qquad \left|\alpha - \frac{r_{n+1}}{s_{n+1}}\right| < \frac{1}{2s_{n+1}^2} \tag{7}$$

egyenlőtlenségek közül is legalább az egyik teljesül. ♣

Megjegyzések: 1. A 8.3.3 Tétel egyrészt nyilván magában foglalja a 8.1.1 és 8.2.3 Tételek állításait, másrészt nemcsak a jó közelítő törtek létezését biztosítja, hanem egyúttal a gyakorlatban is használható algoritmust ad ezek előállítására.

2. Megmutatható, hogy az „igazán jól közelítő" törtek kivétel nélkül az (5)-ben megadott r_n/s_n törtek közül kerülnek ki: Ha

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$$

(azaz r/s a 8.2.3 Tételben előírt mértékben approximálja az α-t), akkor r/s szükségképpen valamelyik r_n/s_n-nel egyenlő.

3. A lánctörtek a (bizonyítás nélkül közölt) 8.1.5 Tétel igazolására is alkalmasak: A 8.3.3 Tétel alábbi bizonyításához hasonló elvek alapján, csak kissé bonyolultabban az is igazolható, hogy három egymást követő indexű $L_n(\alpha)$ tört közül legalább az egyik a 8.1.5 Tételben előírt közelítést is teljesíti.

4. A 8.3.3 Tételből a 8.1.3a feladat alapján következik, hogy

$$\lim_{n\to\infty} L_n(\alpha) = \alpha, \qquad \text{azaz} \qquad \lim_{n\to\infty} L(c_0, \ldots, c_n) = L(c_0, c_1, \ldots)\,.$$

Ennek alapján természetes jelentést nyert az (eddig formális) $\alpha = L(c_0, c_1, \ldots)$ végtelen lánctört.

A 8.3.3 Tétel bizonyításához szükségünk lesz a következő lemmára:

8.3.4 Lemma **L 8.3.4**

Legyenek $c_0, c_1, c_2, \ldots$ tetszőleges *valós* számok, ahol $c_i > 0$, ha $i \geq 1$, és képezzük az alábbi rekurziót:

$$r_0 = c_0, \qquad r_1 = c_1 c_0 + 1, \qquad r_n = c_n r_{n-1} + r_{n-2}, \tag{8a}$$

$$s_0 = 1, \qquad s_1 = c_1, \qquad s_n = c_n s_{n-1} + s_{n-2}. \tag{8b}$$

Ekkor

$$L(c_0, c_1, \ldots, c_n) = \frac{r_n}{s_n} \tag{9}$$

és

$$\frac{r_n}{s_n} - \frac{r_{n-1}}{s_{n-1}} = \frac{(-1)^{n-1}}{s_{n-1} s_n} \qquad (n \geq 1). \tag{10}$$

Ha a c_n számok *egészek*, akkor r_n és s_n is egész, $(r_n, s_n) = 1$, valamint $n > 0$ esetén $s_{n+1} > s_n$. ♣

Megjegyzés: A 8.3.4 Lemmából azonnal következik, hogy a 8.3.3 Tételben az (5) képlettel megadott r_n és s_n számsorozatok kielégítik a (8a)–(8b) rekurziót, tehát a 8.3.4 Lemma és a 8.3.3 Tétel c_n, r_n és s_n jelölései egymással összhangban vannak.

A 8.3.4 Lemma bizonyítása: I. A (9) egyenlőséget n szerinti teljes indukcióval igazoljuk.
Az $n = 0$, 1, illetve 2 esetekben

$$L(c_0) = c_0 = \frac{c_0}{1} = \frac{r_0}{s_0},$$

$$L(c_0, c_1) = c_0 + \frac{1}{c_1} = \frac{c_1 c_0 + 1}{c_1} = \frac{r_1}{s_1},$$

$$L(c_0, c_1, c_2) = \frac{c_2 c_1 c_0 + c_2 + c_0}{c_2 c_1 + 1} = \frac{c_2 r_1 + r_0}{c_2 s_1 + s_0} = \frac{r_2}{s_2},$$

tehát (9) valóban teljesül.

Tegyük fel, hogy (9) az $n = m \geq 2$ esetben igaz, azaz

$$L(c_0, c_1, \ldots, c_m) = \frac{r_m}{s_m} = \frac{c_m r_{m-1} + r_{m-2}}{c_m s_{m-1} + s_{m-2}},$$

ahol r_{m-1}, s_{m-1}, r_{m-2} és s_{m-2} csak a $c_0, \dots, c_{m-1}$ értékektől függ. Ekkor

$$L(c_0, \dots, c_{m-1}, c_m, c_{m+1}) = L\big(c_0, \dots, c_{m-1}, c_m + \frac{1}{c_{m+1}}\big) =$$

$$= \frac{\Big(c_m + \frac{1}{c_{m+1}}\Big) r_{m-1} + r_{m-2}}{\Big(c_m + \frac{1}{c_{m+1}}\Big) s_{m-1} + s_{m-2}} = \frac{c_{m+1}(c_m r_{m-1} + r_{m-2}) + r_{m-1}}{c_{m+1}(c_m s_{m-1} + s_{m-2}) + s_{m-1}} =$$

$$= \frac{c_{m+1} r_m + r_{m-1}}{c_{m+1} s_m + s_{m-1}} = \frac{r_{m+1}}{s_{m+1}}\,,$$

tehát (9) az $n = m + 1$ esetben is teljesül.

II. Most rátérünk (10) igazolására. A (8a)–(8b) képletek alapján

$$r_n s_{n-1} - r_{n-1} s_n = (c_n r_{n-1} + r_{n-2}) s_{n-1} - r_{n-1}(c_n s_{n-1} + s_{n-2}) =$$
$$= -(r_{n-1} s_{n-2} - r_{n-2} s_{n-1}).$$

Ugyanezt n helyett az $n-1$, $n-2$, …, 2 értékekre megismételve kapjuk, hogy

$$r_n s_{n-1} - r_{n-1} s_n = (-1)^{n-1}(r_1 s_0 - r_0 s_1) = (-1)^{n-1}\,. \tag{11}$$

Innen (10)-et $s_n s_{n-1}$-gyel való osztással nyerjük.

III. Az egész c_i-kre vonatkozó állítások a relatív prímség kivételével a feltételekből nyilvánvalók, $(r_n, s_n) = 1$ pedig (11)-ből következik. ■

A 8.3.3 Tétel bizonyítása: Mint már említettük, a 8.3.4 Lemmából következik, hogy az (5) képlettel megadott r_n és s_n számsorozatok kielégítik a (8a)–(8b) rekurziót.

A továbbiakban fel fogjuk használni, hogy maga az α is felírható véges lánctörtként: (3) alapján bármely n-re

$$\alpha = L(c_0, c_1, \dots, c_n, c_{n+1} + \alpha_{n+2})\,, \tag{12}$$

ahol (2) és α irracionalitása miatt $0 < \alpha_{n+2} < 1$.

Így az $\alpha - r_n/s_n$ különbség becsléséhez a 8.3.4 Lemmát a $c_0, c_1, \dots, c_n$ és (c_{n+1} helyett a) $c'_{n+1} = c_{n+1} + \alpha_{n+2}$ számokra fogjuk alkalmazni (és itt megállunk). Ekkor a (8a)–(8b) rekurzióval az

$$r_0,\ r_1,\ \dots,\ r_n,\ r'_{n+1}\,, \qquad \text{illetve} \qquad s_0,\ s_1,\ \dots,\ s_n,\ s'_{n+1}$$

számokhoz jutunk, ahol $n \geq 1$-re

$$r'_{n+1} = c'_{n+1} r_n + r_{n-1} = (c_{n+1} + \alpha_{n+2}) r_n + r_{n-1}\,,$$
$$s'_{n+1} = c'_{n+1} s_n + s_{n-1} = (c_{n+1} + \alpha_{n+2}) s_n + s_{n-1}\,.$$

A (12), (9) és (4) képletek szerint

$$\alpha = \frac{r'_{n+1}}{s'_{n+1}} \qquad \text{és} \qquad L_n(\alpha) = \frac{r_n}{s_n}\,,$$

amiből (10) felhasználásával azt nyerjük, hogy

$$\alpha - \frac{r_n}{s_n} = \frac{r'_{n+1}}{s'_{n+1}} - \frac{r_n}{s_n} = \frac{(-1)^n}{s_n s'_{n+1}}\,. \tag{13}$$

Mivel $s'_{n+1} > s_n$, így (13)-ból azonnal következik (6).

(7) igazolásához tegyük fel indirekt, hogy

$$\left|\alpha - \frac{r_n}{s_n}\right| \geq \frac{1}{2s_n^2} \qquad \text{és} \qquad \left|\alpha - \frac{r_{n+1}}{s_{n+1}}\right| \geq \frac{1}{2s_{n+1}^2}\,. \tag{14}$$

(13) szerint az $\alpha - r_n/s_n$ és $\alpha - r_{n+1}/s_{n+1}$ különbségek ellenkező előjelűek, tehát α az r_n/s_n és r_{n+1}/s_{n+1} törtek közé esik. Ennek megfelelően

$$\left|\alpha - \frac{r_n}{s_n}\right| + \left|\alpha - \frac{r_{n+1}}{s_{n+1}}\right| = \left|\frac{r_n}{s_n} - \frac{r_{n+1}}{s_{n+1}}\right|. \tag{15}$$

A (15) bal oldalát (14) szerint becsülve, a jobb oldal helyett pedig (10) alapján $1/(s_n s_{n+1})$-et írva

$$\frac{1}{2s_n^2} + \frac{1}{2s_{n+1}^2} \leq \frac{1}{s_n s_{n+1}}\,, \qquad \text{azaz} \qquad (s_{n+1} - s_n)^2 \leq 0 \tag{16}$$

adódik. Mivel $n > 0$-ra $s_{n+1} > s_n$, ezért (16) nem teljesülhet, vagyis ellentmondásra jutottunk. ■

Feladatok

8.3.1 Határozzuk meg az alábbi számok lánctörtjegyeit:

a) $53/11$; b) $\sqrt{3}$; c) $\sqrt{5}$; d) $(1+\sqrt{5})/2$.

8.3.2 Melyek azok a számok, amelyeknek a lánctörtkifejtése

a) 1, 2, 3, 4; b) 1, 2, 1, 2, 1, 2, ...?

8.3.3 Bizonyítsuk be, hogy bármely α irracionális számhoz végtelen sok olyan r/s tört létezik, amelyben s páratlan és

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2}\,.$$

8.3.4 Bizonyítsuk be, hogy bármely $n \geq 1$ esetén

$$\left|\frac{1+\sqrt{5}}{2} - \frac{\varphi_{n+1}}{\varphi_n}\right| < \frac{1}{\varphi_n^2}\,,$$

ahol φ_n az n-edik Fibonacci-szám (lásd az 1.2.5 feladatot).

M 8.3.5 Bizonyítsuk be, hogy a 8.3.4 Lemma feltételeinek teljesülése esetén bármely $n \geq 2$-re fennáll

$$\frac{r_n}{s_n} - \frac{r_{n-2}}{s_{n-2}} = \frac{(-1)^n c_n}{s_{n-2}s_n}\,.$$

M*8.3.6 Tegyük fel, hogy az α irracionális szám lánctörtjegyei periodikus sorozatot alkotnak (azaz létezik olyan k és M, hogy minden $n > M$ esetén $c_n = c_{n-k}$). Bizonyítsuk be, hogy ekkor van olyan másodfokú, egész együtthatós polinom, amelynek az α gyöke.
Megjegyzés: A fenti állítás megfordítása is igaz.

8.4. A törtrészek eloszlása

Ebben a pontban valós számsorozatok törtrészeinek az eloszlásával foglalkozunk.

8.4.1 Tétel **T 8.4.1**

Tetszőleges irracionális szám többszöröseinek a törtrészei mindenütt sűrűn helyezkednek el a $[0,1]$ intervallumban.

Ez részletesen kifejtve a következőt jelenti: Legyen α irracionális szám és $v \in [0,1]$. Ekkor bármely $\varepsilon > 0$-hoz létezik olyan $n > 0$ egész, amelyre $|\{n\alpha\} - v| < \varepsilon$. ♣

Bizonyítás: A 8.1.1 Tétel alapján végtelen sok olyan r/s tört létezik, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2}\,, \qquad \text{azaz} \qquad |s\alpha - r| < \frac{1}{s}\,.$$

Válasszunk olyan közelítő törtet, amelyben $s > 1/\varepsilon$, ekkor $|s\alpha - r| < \varepsilon$. Jelöljük $|s\alpha - r|$-et d-vel (tehát $d < \varepsilon$), és tekintsük az

$$\{s\alpha\},\ \{2s\alpha\},\ \{3s\alpha\},\ \ldots,\{ms\alpha\} \tag{1}$$

törtrészeket, ahol $m = \lfloor 1/d \rfloor$ (nyilván feltehető $\varepsilon < 1$, és így $m \geq 1$).
Vegyük először azt az esetet, amikor $s\alpha - r > 0$. Ekkor bármely $1 \leq i \leq m$-re

$$0 < is\alpha - ir = i(s\alpha - r) = id < 1, \qquad \text{tehát} \qquad \{is\alpha\} = id.$$

Ez azt jelenti, hogy az (1)-ben felsorolt törtrészek olyan monoton növő sorozatot alkotnak, amelyben a szomszédos elemek távolsága $d < \varepsilon$, továbbá az első elemnek a 0-tól, az utolsónak pedig az 1-től való távolsága is kisebb, mint ε. Ebből következik, hogy a sorozat elemei között van olyan, amelynek a v-től való távolsága kisebb, mint ε.

Az $s\alpha - r < 0$ eset is ugyanígy kezelhető: ekkor $1 \leq i \leq m$-re $\{is\alpha\} = 1 - id$, és így az (1)-ben megadott törtrészek olyan monoton fogyó sorozatot alkotnak, amelyben a szomszédos elemek távolsága, továbbá az első elemnek az 1-től, az utolsónak pedig a 0-tól való távolsága kisebb, mint ε. ■

Most a 8.4.1 Tételben felvetett probléma többdimenziós változatával foglalkozunk. Tekintsük először a legegyszerűbb esetet: Legyenek α_1 és α_2 irracionális számok, és vizsgáljuk meg az $P_n = (\{n\alpha_1\}, \{n\alpha_2\})$ pontok elhelyezkedését az egységnégyzetben.

A 8.4.1 Tétel bizonyításához hasonlóan a 8.1.3 Tételből kapjuk, hogy bármely $\varepsilon > 0$-hoz léteznek olyan r_1, r_2 és $s > 0$ egész számok, amelyekre

$$|s\alpha_1 - r_1| < \varepsilon \qquad \text{és} \qquad |s\alpha_2 - r_2| < \varepsilon\,.$$

Ez azt jelenti, hogy a $P_s = (\{s\alpha_1\}, \{s\alpha_2\})$ pont az egységnégyzet valamelyik csúcsának a közelében helyezkedik el. Ebből a 8.4.1 Tétel bizonyításához hasonlóan az is következik, hogy ezt a csúcsot a P_s ponttal összekötő egyenesen egymáshoz közel sorakoznak a $P_{2s}, P_{3s}, \ldots$ pontok.

Az azonban nem igaz, hogy a P_n pontok bármely α_1 és α_2 esetén mindenütt sűrűek az egységnégyzetben. Legyen például $\alpha_2 = \alpha_1 + 1$. Ekkor nyilván bármely n-re $\{n\alpha_1\} = \{n\alpha_2\}$, tehát a P_n pontok kivétel nélkül az $y = x$ egyenesre esnek.

A mindenütt sűrű elhelyezkedés feltételét a lineáris függetlenség segítségével fogalmazhatjuk meg:

8.4.2 Tétel **T 8.4.2**

Az $\alpha_1, \ldots, \alpha_k$ valós számokra a

$$P_n = (\{n\alpha_1\}, \{n\alpha_2\}, \ldots, \{n\alpha_k\}), \qquad n = 1, 2, 3, \ldots$$

pontok akkor és csak akkor helyezkednek el mindenütt sűrűn a k-dimenziós egységkockában, ha $1, \alpha_1, \ldots, \alpha_k$ lineárisan függetlenek a racionális test felett. ♣

A tételben megadott lineáris függetlenség azt jelenti, hogy racionális c_i-kkel $c_0 + c_1\alpha_1 + \ldots + c_k\alpha_k = 0$ csak a triviális $c_0 = c_1 = \ldots = c_k = 0$ esetben teljesülhet. Ebből speciálisan az is következik, hogy minden α_i szükségképpen irracionális.

Az illusztrációként vizsgált $k = 2$, $\alpha_2 = \alpha_1 + 1$ példában láttuk, hogy a P_n pontok nem lesznek mindenütt sűrűek az egységnégyzetben, és ez összhangban van azzal, hogy $1 \cdot 1 + 1\alpha_1 + (-1)\alpha_2 = 0$ szerint $1, \alpha_1, \alpha_2$ nem lineárisan függetlenek.

A 8.4.2 Tételben megadott feltétel elégségességét nem bizonyítjuk, a szükségesség igazolását a 8.4.3 feladatban tűztük ki.

Visszatérve az egydimenziós esetre, most a mindenütt sűrű elhelyezkedésnél jóval erősebb követelményt támasztó *egyenletes eloszlás* kérdését vizsgáljuk.

Az egyenletes eloszlás azt jelenti, hogy az $u_1, u_2, \ldots$ végtelen számsorozat törtrészei a $[0, 1]$ intervallum bármely I részintervallumában az I hosszával „arányosan" találhatók: nagy n esetén az első n darab $\{u_i\}$ közül „körülbelül" dn darab esik I-be, ahol d az I hossza. A pontos definíció a következő:

8.4.3 Definíció **D 8.4.3**

Az $u_1, u_2, \ldots$ végtelen valós számsorozat *modulo 1 egyenletes eloszlású* (vagy röviden *egyenletes eloszlású*), ha a $[0, 1]$ intervallum bármely I részintervallumára

$$\lim_{n\to\infty} \frac{f_n(I)}{n} = d,$$

ahol d az I intervallum hossza és $f_n(I)$ az $\{u_1\}, \ldots, \{u_n\}$ törtrészek közül az I-be esők száma. ♣

A számsorozatok egyenletes eloszlására vonatkozik Weyl alábbi tétele, amelyet bizonyítás nélkül közlünk:

8.4.4 Tétel **T 8.4.4**

Az $u_1, u_2, \ldots$ sorozat akkor és csak akkor egyenletes eloszlású, ha bármely $m \neq 0$ egészre

$$\lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} e^{2\pi i m u_t} = 0. \ \clubsuit$$

Mind az egyenletes eloszlás fogalma, mind pedig a Weyl-kritérium kiterjeszthető több dimenzióra is.

Weyl tételének felhasználásával most azt igazoljuk, hogy egy irracionális szám többszörösei egyenletes eloszlású sorozatot alkotnak.

8.4.5 Tétel **T 8.4.5**

Ha α irracionális szám, akkor az $\alpha, 2\alpha, \ldots, n\alpha, \ldots$ sorozat egyenletes eloszlású. $\clubsuit$

Bizonyítás: A 8.4.4 Tétel alapján azt kell megmutatni, hogy bármely $m \neq 0$ egészre

$$\lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} e^{2\pi i m t \alpha} = 0. \tag{2}$$

A (2) bal oldalán szereplő összeg egy n-tagú mértani sorozat, amelynek hányadosa $e^{2\pi i m\alpha} \neq 1$, mivel α irracionális. Ezért

$$\Big|\frac{1}{n} \sum_{t=1}^{n} e^{2\pi i m t \alpha}\Big| = \frac{|e^{2\pi i m\alpha}| \cdot |e^{2\pi i m n\alpha} - 1|}{n|e^{2\pi i m\alpha} - 1|} \leq \frac{1 \cdot 2}{n|e^{2\pi i m\alpha} - 1|} \to 0,$$

ha $n \to \infty$. ■

Feladatok

M 8.4.1 Vizsgáljuk meg, hogy az alábbi számsorozatok törtrészei mindenütt sűrűek-e a $[0, 1]$ intervallumban:

a) $(1 + \sqrt{2})^n$; b) $\sqrt{n}$; c) $\sqrt{n^2 + 1}$; d) $\sqrt{2n^2 + 1}$;

e) $\sin(n\pi/180)$; f) $\sin n$; g) $\lg n$.

*8.4.2 Mutassuk meg, hogy létezik olyan α valós szám, amelyre az

$$\alpha, \quad \alpha^2, \quad \alpha^3, \quad \ldots, \quad \alpha^n, \ldots$$

számsorozat törtrészei mindenütt sűrűek $[0,1]$-ben.

M 8.4.3 Bizonyítsuk be, hogy a 8.4.2 Tételben megadott lineáris függetlenségi feltétel szükséges ahhoz, hogy a P_n pontok mindenütt sűrűn helyezkedjenek el a k-dimenziós egységkockában.

8.4.4 Bizonyítsuk be a következő állításokat.

a) Ha egy sorozat törtrészei mindenütt sűrűek $[0,1]$-ben, akkor a sorozat átindexezhető egyenletes eloszlású sorozattá.

b) Bármely egyenletes eloszlású sorozat átindexezhető nem egyenletes eloszlású sorozattá.

8.4.5 Melyek igazak az alábbi állítások közül?

a) Egy egyenletes eloszlású sorozat részsorozata is egyenletes eloszlású.

b) Egy egyenletes eloszlású sorozat minden eleméhez ugyanazt a valós számot hozzáadva ismét egyenletes eloszlású sorozatot kapunk.

c) Egy egyenletes eloszlású sorozat minden elemét ugyanazzal a nemnulla valós számmal megszorozva ismét egyenletes eloszlású sorozatot kapunk.

d) Két egyenletes eloszlású sorozat összege is egyenletes eloszlású.

e) Két egyenletes eloszlású sorozat szorzata is egyenletes eloszlású.

f) Egy egyenletes eloszlású sorozat négyzete is egyenletes eloszlású.

g) Egy egyenletes eloszlású sorozat négyzete sohasem egyenletes eloszlású.

8.4.6 Mutassuk meg, hogy az alábbi számsorozatok *nem* egyenletes eloszlásúak:

a) $\lg n$; b) $\sin n$.

8.4.7 Lássuk be, hogy ha a t természetes szám nem 10^k alakú, akkor van olyan pozitív egész kitevős hatványa, amelynek első öt jegye 54321 (tízes számrendszerben).

9. ALGEBRAI ÉS TRANSZCENDENS SZÁMOK

Egy α komplex számot aszerint nevezünk algebrainak, illetve transzcendensnek, hogy létezik-e vagy sem olyan racionális (illetve egész) együtthatós, nemnulla polinom, amelynek az α gyöke. Megmutatjuk, hogy a komplex számok „túlnyomó többsége" transzcendens, ugyanakkor egy konkrét számról általában igen nehéz eldönteni, hogy algebrai-e vagy transzcendens. Ezt jól érzékelteti az e transzcendenciáját bemutató bizonyítás és a számos megoldatlan probléma felsorolása.

Az algebrai számok tárgyalását a minimálpolinom és a fokszám tulajdonságaival, valamint az algebrai számoknak a műveletekhez való viszonyával kezdjük. Ezután belátjuk, hogy az algebrai számok rosszul approximálhatók. Ennek alapján egyrészt egyszerűen lehet transzcendens számot konstruálni, másrészt fontos következményként kapjuk, hogy bizonyos típusú diofantikus egyenleteknek csak véges sok megoldása van. A fejezet végén az egész számok általánosításaként definiált algebrai egészekkel foglalkozunk.

Az algebrai számok és algebrai egészek fontos szerepet játszanak a következő két fejezetben is.

9.1. Algebrai szám, transzcendens szám

A racionális számokat az összes komplex szám között az tünteti ki, hogy elsőfokú racionális együtthatós polinomok gyökei. Ha itt a fokszámra vonatkozó korlátozást elejtjük, akkor az *algebrai szám* fogalmához jutunk:

9.1.1 Definíció **D 9.1.1**

Egy α komplex szám *algebrai szám* (vagy röviden *algebrai*), ha létezik olyan racionális együtthatós, nemnulla f polinom, amelyre $f(\alpha) = 0$. ♣

Megjegyzések: 1. Az $f = 0$ polinomot nyilván ki kell zárni, hiszen ennek a polinomnak minden komplex szám gyöke.

2. Ha α gyöke egy racionális együtthatós polinomnak, akkor a polinomot a nevezők legkisebb közös többszörösével beszorozva egy olyan *egész* együtthatós polinomot kapunk, amelynek az α továbbra is gyöke. Így ugyanahhoz a fogalomhoz jutunk, ha a 9.1.1 Definícióban „racionális együtthatós polinom" helyett „egész együtthatós polinom" létezését írjuk elő.

3. Alapvetően megváltozik a helyzet, ha a racionális vagy egész együtthatók helyett például valós vagy komplex együtthatókat írunk elő: minden komplex számhoz található olyan valós együtthatós, nemnulla polinom (és így komplex együtthatós is), amelynek az adott szám gyöke (lásd a 9.1.7 feladatot).

4. Az „algebrai szám" helyett a „racionális test felett algebrai szám" (vagy a „racionális test felett algebrai elem") kifejezést is szokás mondani, mert a fogalom általánosításaként a racionális test helyett más test feletti algebrai elemet is lehet értelmezni (lásd a 10.1.4 Definíciót).

Példák:

Mint említettük, minden racionális szám egyben algebrai szám is.

Irracionális algebrai szám például a $\sqrt{2}$ vagy az $\sqrt[5]{13}$, hiszen gyöke az $x^2 - 2$, illetve $x^5 - 13$ polinomnak.

Algebrai szám minden komplex egységgyök is, ezek az $x^n - 1$ alakú polinomok gyökei.

További példák szerepelnek a 9.1.1 és 9.1.2 feladatokban. A 9.3 pontbeli tételek segítségével igen sokféle algebrai számot tudunk majd konstruálni.

A nem algebrai számokat *transzcendens szám*oknak nevezzük:

9.1.2 Definíció **D 9.1.2**

Egy komplex szám *transzcendens szám* (vagy röviden *transzcendens*), ha a nullpolinomon kívül nem gyöke egyetlen racionális együtthatós polinomnak sem. ♣

9.1.3 Tétel **T 9.1.3**

Létezik transzcendens szám, sőt „majdnem minden" szám transzcendens: az algebrai számok számossága megszámlálható, míg a transzcendens számok számossága kontinuum. ♣

Bizonyítás: Mivel a komplex számok számossága kontinuum, ezért a tétel valamennyi állítása következni fog abból, hogy az algebrai számok számossága megszámlálható, azaz az algebrai számok sorozatba rendezhetők.

Az algebrai számok az egész együtthatós, nemnulla polinomok gyökei, ezért először ezeket a polinomokat fogjuk sorozatba rendezni. Ebből ezután úgy kapjuk meg az algebrai számok egy sorozatba rendezését, hogy rendre vesszük a polinomok összes olyan (komplex) gyökét, amely korábbi polinomok gyökeként még nem lett felsorolva.

Legyen $f = a_0 + a_1 x + \ldots + a_n x^n$ tetszőleges egész együtthatós polinom,

ahol $a_n \neq 0$, és definiáljuk $H(f)$-et a következőképpen:

$$H(f) = n + |a_0| + |a_1| + \ldots + |a_n| .$$

Például

$$\begin{aligned}
&H(f) = 1 \iff f = \pm 1;\\
&H(f) = 2 \iff f = \pm 2,\ \pm x;\\
&H(f) = 3 \iff f = \pm 3,\ \pm x \pm 1,\ \pm 2x,\ \pm x^2;\\
&H(f) = 4 \iff f = \pm 4,\ \pm x \pm 2,\ \pm 2x \pm 1,\ \pm 3x,\\
&\qquad\qquad \pm x^2 \pm 1,\ \pm x^2 \pm x,\ \pm 2x^2,\ \pm x^3.
\end{aligned} \tag{1}$$

A $H(f)$ definíciójából világos, hogy bármely k esetén csak véges sok olyan f létezik, amelyre $H(f) = k$. Ezért egy megfelelő felsorolást kapunk, ha vesszük rendre azokat a polinomokat, amelyekre $H(f) = 1, 2, 3, \ldots$

Innen a már jelzett módon nyerjük az algebrai számok egy sorozatba rendezését. Ennek első néhány tagja az f-ek (1)-beli sorrendjét figyelembe véve

$$0,\ 1,\ -1,\ 2,\ -2,\ \frac{1}{2},\ -\frac{1}{2},\ i,\ -i,\ \ldots$$

(a nemnulla konstans polinomoknak nincs gyöke, a 0 az x-ből, a ± 1 az $x \mp 1$-ből adódik stb., a konstansszorosok, illetve a korábban már számításba vett polinomok szorzatai, valamint ilyenek osztói nem adnak újabb gyököket).

A fentiekből világos, hogy elég azokra az f-ekre szorítkozni, amelyekben $n > 0$, $a_n > 0$, $(a_0, a_1, \ldots, a_n) = 1$ és f irreducibilis a racionális test felett. ■

A 9.1.3 Tételben anélkül igazoltuk „sok” transzcendens szám létezését, hogy akár egyetlen konkrét transzcendens számot előállítottunk volna. A 9.4 pontban majd konkrét konstrukciót adunk transzcendens számra, a 9.5 pontban pedig belátjuk, hogy e (a természetes logaritmus alapszáma) transzcendens.

Néhány további nevezetes transzcendens szám:

- π;
- $\sin n$, ahol az n szög (ívmértékben mérve) egész szám;
- $\lg n$, ahol n pozitív egész szám és a 10-nek nem egész kitevőjű hatványa (lásd a 9.3.7 feladatot);
- $2^{\sqrt{2}}$ (lásd a 9.3.5 Tételt);
- $\zeta(2) = \displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2}$ (lásd a 9.1.3 feladatot).

Általában egy adott számról igen nehéz eldönteni, hogy algebrai-e vagy transzcendens, az imént felsorolt példák bármelyike esetén a transzcendencia bizonyítása meghaladja a könyv kereteit (a hivatkozásként jelzett 9.3.5 Tétel bizonyítás nélkül szerepel, a másik két hivatkozás pedig erre a tételre, illetve a π transzcendenciájára vezeti vissza a kérdést).

Megoldatlan például, vajon $e+\pi$ transzcendens-e, illetve egyáltalán irracionális-e. Ugyancsak megoldatlan, hogy $\zeta(3)=\sum_{k=1}^{\infty}k^{-3}$ transzcendens-e, ennek a számnak az irracionalitását is csak 1975-ben igazolták. A $\zeta(7)$-ről az sincs tisztázva, vajon irracionális-e.

Feladatok

9.1.1 Igazoljuk, hogy az alábbi számok algebraiak:

a) $\sqrt[20]{7}$; b) $\sqrt{2}+3$; c) $\sqrt{2}+\sqrt{3}$;
d) $\sqrt{2}+\sqrt[3]{4}$; e) $\sqrt[3]{2}+\sqrt[3]{4}$; f) $\sqrt{2}+\sqrt{3}+\sqrt{5}$.

9.1.2 Bizonyítsuk be, hogy ha α algebrai szám, akkor

a) $-\alpha$; b) $\overline{\alpha}$; c) $\alpha\neq 0$ esetén $1/\alpha$;

továbbá bármely r racionális, illetve k pozitív egész szám esetén

d) $r+\alpha$; e) $r\alpha$; f) $\sqrt[k]{\alpha}$

is algebrai.

9.1.3 Felhasználva, hogy π transzcendens szám, mutassuk meg, hogy $\zeta(2)=\sum_{k=1}^{\infty}k^{-2}$ is transzcendens.

9.1.4 Tegyük fel, hogy α transzcendens és $f\neq 0$ egész együtthatós polinom. Igazoljuk, hogy ekkor $f(\alpha)$ is transzcendens.

9.1.5 Legyen g komplex együtthatós, nemnulla polinom. Bizonyítsuk be, hogy akkor és csak akkor létezik olyan h egész együtthatós, nemnulla polinom, amelyre $g\mid h$, ha g minden (komplex) gyöke algebrai szám.

9.1.6 Bizonyítsuk be, hogy az α komplex szám akkor és csak akkor algebrai, ha létezik olyan n pozitív egész, amelyre az $1,\alpha,\ldots,\alpha^n$ számok lineárisan összefüggők a racionális test felett.

9.1.7 Bizonyítsuk be, hogy bármely komplex szám gyöke egy alkalmas

a) komplex; b) valós

együtthatós polinomnak.

9.2. Minimálpolinom és fokszám

Legyen α algebrai szám. Ekkor nyilván végtelen sok olyan racionális együtthatós polinom van, amelynek az α gyöke: ha f egy ilyen polinom, akkor az f bármely (racionális együtthatós) polinomszorosa is megfelel. Így ezek közül a polinomok közül azokat érdemes kitüntetni, amelyeknek a lehető legkisebb a fokszáma:

9.2.1 Definíció **D 9.2.1**

Az α algebrai szám *minimálpolinom*ja egy olyan, minimális fokú, racionális együtthatós polinom, amelynek az α gyöke. Az α minimálpolinomját m_α-val jelöljük. ♣

A minimálpolinom nem teljesen egyértelmű: ha f az α (egyik) minimálpolinomja, akkor nyilván cf is megfelel a feltételeknek, ahol $c \neq 0$ tetszőleges racionális szám. Ettől eltekintve azonban már egyértelmű a minimálpolinom:

9.2.2 Tétel **T 9.2.2**

Ha f és g is minimálpolinomja az α algebrai számnak, akkor van olyan $c \neq 0$ racionális szám, amelyre $g = cf$. ♣

Bizonyítás: Legyen

$$f = a_0 + a_1 x + \ldots + a_n x^n, \qquad a_n \neq 0,$$
$$g = b_0 + b_1 x + \ldots + b_n x^n, \qquad b_n \neq 0.$$

Ekkor α gyöke a $h = b_n f - a_n g$ polinomnak, amely vagy a nullpolinom, vagy legfeljebb $n-1$-edfokú. Így a minimálpolinom definíciója miatt csak $h = 0$ lehetséges. Innen $g = cf$, ahol $c = b_n/a_n$. ■

Az m_α jelölés a továbbiakban is az α akármelyik minimálpolinomját jelentheti, ez a 9.2.2 Tétel alapján nem okoz majd problémát.

A minimálpolinom legfontosabb tulajdonságait a következő tételben foglaljuk össze.

9.2.3 Tétel **T 9.2.3**

(i) Legyen $g \in \mathbf{Q}[x]$. Ekkor $g(\alpha) = 0 \iff m_\alpha \mid g$.

(ii) m_α irreducibilis $\mathbf{Q}$ felett.

(iii) Ha f irreducibilis $\mathbf{Q}$ felett, és $f(\alpha) = 0$, akkor f az α (egyik) minimálpolinomja. ♣

Bizonyítás: (i) Először tegyük fel, hogy $m_\alpha \mid g$, azaz alkalmas $h \in \mathbf{Q}[x]$-re $g = hm_\alpha$. Ekkor

$$g(\alpha) = h(\alpha)m_\alpha(\alpha) = h(\alpha) \cdot 0 = 0\,.$$

Megfordítva, tegyük fel, hogy $g(\alpha) = 0$. Osszuk el a g polinomot maradékosan m_α-val:

$$g = m_\alpha h + r, \qquad \text{ahol} \qquad h, r \in \mathbf{Q}[x], \quad \text{és} \quad \deg r < \deg m_\alpha \quad \text{vagy} \quad r = 0.$$

Ekkor

$$0 = g(\alpha) = m_\alpha(\alpha)h(\alpha) + r(\alpha) = 0 + r(\alpha) = r(\alpha).$$

Ez $\deg r < \deg m_\alpha$ esetén ellentmond a minimálpolinom definíciójának. Így csak $r = 0$ lehetséges, azaz valóban $m_\alpha \mid g$.

(ii) Indirekt tegyük fel, hogy $m_\alpha = gh$, ahol g és h az m_α-nál alacsonyabb fokú racionális együtthatós polinomok. Ekkor (a komplex számtest nullosztómentessége miatt)

$$0 = m_\alpha(\alpha) = g(\alpha)h(\alpha) \implies g(\alpha) = 0 \quad \text{vagy} \quad h(\alpha) = 0,$$

ami ellentmond a minimálpolinom definíciójának.

(iii) Az (i) állítás szerint $m_\alpha \mid f$, ezért f irreducibilitása miatt $m_\alpha = c$ vagy $f = cm_\alpha$, ahol c konstans. Az első eset nem lehetséges, így f valóban (az egyik) minimálpolinom. ■

9.2.4 Definíció **D 9.2.4**

Az α algebrai szám *fok*a (vagy *fokszám*a) a minimálpolinomjának a foka: $\deg \alpha = \deg m_\alpha$. ♣

Példák:

P1 A 0 (egyik) minimálpolinomja $m_0 = x$, az 1-é $m_1 = x - 1$, és általában egy r racionális számé $m_r = x - r$. Az is világos, hogy az elsőfokú algebrai számok éppen a racionális számok, 0-adfokú algebrai szám pedig nincs.

P2 Az i minimálpolinomja $x^2 + 1$, és így $\deg i = 2$.

P3 Az $\sqrt[5]{3}$ minimálpolinomja $x^5 - 3$, mivel ez a polinom a Schönemann–Eisenstein-kritérium szerint irreducibilis $\mathbf{Q}$ felett.

P4 Bármely k pozitív egészhez végtelen sok k-adfokú algebrai szám létezik, hiszen (például ismét a Schönemann–Eisenstein-kritérium alapján) végtelen sok, $\mathbf{Q}$ felett irreducibilis, k-adfokú polinom van.

P5 Egy ϱ primitív n-edik komplex egységgyök minimálpolinomja Φ_n, az n-edik körosztási polinom (mert $\Phi_n(\varrho) = 0$ és Φ_n irreducibilis $\mathbf{Q}$ felett). Ennélfogva $\deg \varrho = \deg \Phi_n = \varphi(n)$. (A P2 példa tulajdonképpen ennek $n = 4$ speciális esete volt.)

Feladatok

9.2.1 Milyen kapcsolat van a 9.1.2 feladatban szereplő számok foka és α foka között?

9.2.2 Határozzuk meg az alábbi (algebrai) számok fokát:

a) $\sqrt[7]{12}$; b) $\cos 20°$; c) $\sqrt[3]{3} - \sqrt[3]{9}$;

d) $\sqrt{7 - 4\sqrt{3}}$; e) $\sqrt[4]{2} + \sqrt{2}$; f) $\sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$.

9.2.3 Mutassuk meg, hogy α akkor és csak akkor másodfokú algebrai szám, ha $\alpha = r + \sqrt{s}$, ahol r és s racionális számok, és s nem négyzete egy racionális számnak.

9.2.4 Mutassuk meg, hogy az n-edfokú algebrai számok

a) $n \geq 1$ esetén a valós számegyenesen;

b) $n \geq 2$ esetén a komplex számsíkon

mindenütt sűrűn helyezkednek el.

9.2.5 Legyen f egy n-edfokú racionális együtthatós polinom ($n \geq 1$), és legyenek a (multiplicitással számolt, komplex) gyökei $\alpha_1, \ldots, \alpha_n$.

a) Bizonyítsuk be, hogy $\sum_{i=1}^{n} \deg \alpha_i \leq n^2$.

b) Mikor áll a)-ban egyenlőség?

c) Mutassuk meg, hogy ha a)-ban szigorú egyenlőtlenség érvényes, akkor $\sum_{i=1}^{n} \deg \alpha_i \leq n^2 - 2n + 2$ is teljesül.

9.2.6 Tudjuk, hogy $\deg \alpha = 6$ és α gyöke az

$$f = x^7 + 8x^6 + 15x^5 + 10x^3 + 35x^2 + 5x - 30$$

polinomnak. Mi az α minimálpolinomja?

9.2.7 Tegyük fel, hogy az α és β komplex számok gyökei az f racionális együtthatós, nemnulla polinomnak és $\deg f < \deg \alpha + \deg \beta$. Bizonyítsuk be, hogy $m_\alpha = m_\beta$.

M 9.2.8 Tegyük fel, hogy az $f \neq 0$ és g racionális együtthatós polinomokra és az α és β komplex számokra $f(\alpha) = g(\alpha) = f(\beta) = 0$, $g(\beta) = 1$. Bizonyítsuk be, hogy f reducibilis $\mathbf{Q}$ felett.

9.3. Műveletek algebrai számokkal

Ebben a pontban elsősorban az algebrai számok és a négy alapművelet, illetve a hatványozás kapcsolatát tárgyaljuk.

9.3.1 Tétel **T 9.3.1**

Az algebrai számok résztestet alkotnak a komplex számtestben, azaz két algebrai szám összege, különbsége, szorzata és (ha a nevező nem nulla, akkor) hányadosa is algebrai. ♣

A tételt a *szimmetrikus polinom*ok segítségével igazoljuk. (Egy másik bizonyítás szerepel majd a 10.2 pontban.)

Egy R gyűrű feletti k-változós (vagy k-határozatlanú) $F(x_1,\dots,x_k)$ polinomot akkor nevezünk szimmetrikusnak, ha az x_i változók tetszőleges permutációja esetén ugyanazt a polinomot kapjuk. Ilyen polinom például a változók összege, a változók szorzata, vagy általában a (különböző) változókból képzett összes j-tényezős szorzatok összege:

$$\sigma_j(x_1,\dots,x_k)=\sum_{1\le i_1<\dots<i_j\le k} x_{i_1}\dots x_{i_j}=$$

$$=x_1x_2\dots x_{j-1}x_j+x_1x_2\dots x_{j-1}x_{j+1}+\dots+x_{k-j+1}x_{k-j+2}\dots x_{k-1}x_k,$$

$$j=1,\dots,k. \qquad (1)$$

A σ_j-ket az $x_1,\dots,x_k$ változók *elemi szimmetrikus polinom*jainak nevezzük.

Mivel szimmetrikus polinomok összege és szorzata is szimmetrikus polinom, így például $\sigma_1+\sigma_2^3$, és általában a σ_j-k tetszőleges (R-beli együtthatókkal képzett) polinomja is (az x_i változók szerint nézve) szimmetrikus polinom.

Az elemi szimmetrikus polinomok jelentőségét elsősorban az adja, hogy az iménti észrevételnek a megfordítása is igaz: Minden szimmetrikus polinom felírható az elemi szimmetrikus polinomok polinomjaként.

9.3.2 Tétel (A szimmetrikus polinomok alaptétele) **T 9.3.2**

Legyen $F(x_1,\dots,x_k)$ egy R gyűrű feletti tetszőleges (k-változós) szimmetrikus polinom. Ekkor létezik olyan R feletti, k-változós G polinom, amelyre

$$F(x_1,\dots,x_k)=G(\sigma_1,\dots,\sigma_k)\,,$$

ahol $\sigma_j=\sigma_j(x_1,\dots,x_k)$ az x_i változókból képzett (1)-beli elemi szimmetrikus polinomokat jelenti. ♣

Példa: Az x_i változók négyzetösszege a következőképpen állítható elő a σ_j-kkel:

$$x_1^2 + x_2^2 + \ldots + x_k^2 = (x_1 + \ldots + x_k)^2 - 2(x_1x_2 + x_1x_3 + \ldots) = \sigma_1^2 - 2\sigma_2.$$

A szimmetrikus polinomok alaptételének bizonyítása megtalálható bármely bevezető algebratankönyvben.

A tételt kiegészíthetjük azzal a megjegyzéssel, hogy a tételben szereplő G polinom egyértelmű, és G együtthatóit F együtthatóiból csak az összeadás és kivonás segítségével kapjuk.

A tételt elsősorban arra a két esetre fogjuk alkalmazni, amikor R a racionális számtest, illetve az egész számok gyűrűje. Ha tehát az F szimmetrikus polinom együtthatói racionális, illetve egész számok, akkor a megfelelő G polinom is racionális, illetve egész együtthatós lesz.

A 9.3.1 Tétel bizonyítása: A 9.1.2 feladatban láttuk, hogy egy algebrai szám ellentettje és egy nemnulla algebrai szám reciproka is algebrai, így elég azt igazolni, hogy két algebrai szám összege és szorzata is algebrai.

Legyen α és β algebrai szám, és tegyük fel, hogy α, illetve β gyöke az

$$f = \prod_{i=1}^{m}(x - \alpha_i), \qquad \text{illetve} \qquad g = \prod_{j=1}^{n}(x - \beta_j)$$

racionális együtthatós polinomnak (ahol $\alpha_1 = \alpha$, illetve $\beta_1 = \beta$). Ekkor $\alpha + \beta$ gyöke a

$$h = \prod_{i=1}^{m}\prod_{j=1}^{n}(x - \alpha_i - \beta_j)$$

polinomnak. Megmutatjuk, hogy h racionális együtthatós.

Legyen $h = c_0 + c_1x + \ldots + c_{nm-1}x^{nm-1} + x^{nm}$. Írjuk át a h polinomot

$$h = \prod_{i=1}^{m} g(x - \alpha_i)$$

alakba. Ebből látszik, hogy az α_i-k tetszőleges permutációja esetén a h polinom, és így annak minden c_r együtthatója is változatlan marad. Ez azt jelenti, hogy ha az $\alpha_1, \ldots, \alpha_m$ számokat változóknak tekintjük, akkor minden c_r együttható ezeknek az α_i változóknak szimmetrikus polinomja:

$$c_r = F_r(\alpha_1, \ldots, \alpha_m), \qquad r = 0, 1, \ldots, nm - 1,$$

ahol F_r szimmetrikus polinom és F_r együtthatói racionális számok (hiszen ezeket g együtthatóiból kapjuk). A 9.3.2 Tétel szerint így F_r felírható az α_i-kből képzett σ_j elemi szimmetrikus polinomok polinomjaként, azaz alkalmas G_r racionális együtthatós polinomra

$$c_r = F_r(\alpha_1, \dots, \alpha_m) = G_r(\sigma_1, \dots, \sigma_m)\,.$$

Az α_i-k elemi szimmetrikus polinomjai azonban a gyökök és együtthatók közötti összefüggés alapján éppen az f polinom együtthatói, illetve azok ellentettjei, tehát racionális számok, ezért $c_r = G_r(\sigma_1, \dots, \sigma_m)$ is racionális szám. Ezzel beláttuk, hogy h racionális együtthatós, tehát $\alpha + \beta$ algebrai szám.

Hasonlóan igazolható, hogy $\alpha\beta$ is algebrai szám; ekkor a

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(x - \alpha_i\beta_j) = \prod_{i=1}^{m}\alpha_i^n\, g\Big(\frac{x}{\alpha_i}\Big)$$

polinomot kell tekinteni (ha $\alpha \neq 0$, akkor feltehetjük, hogy egyik α_i sem nulla, az $\alpha = 0$ esetben pedig $\alpha\beta = 0$ nyilvánvalóan algebrai). ■

A 9.3.1 Tétel egyik fontos következménye, hogy a komplex számok algebrai, illetve transzcendens voltának eldöntése visszavezethető a valós számok hasonló vizsgálatára:

9.3.3 Tétel **T 9.3.3**

Egy komplex szám akkor és csak akkor algebrai, ha a valós része is és a képzetes része is algebrai. ♣

Bizonyítás: Legyen $\alpha = a + bi$ (ahol a és b valós számok).

Először tegyük fel, hogy a és b algebrai. Mivel i is algebrai (gyöke az $x^2 + 1$ polinomnak), és algebrai számok szorzata és összege is algebrai, ezért $\alpha = a + bi$ is algebrai.

Megfordítva, tegyük fel, hogy $\alpha = a + bi$ algebrai. Ekkor $\overline{\alpha} = a - bi$ is algebrai (lásd a 9.1.2b feladatot). Mivel algebrai számok összege, különbsége és hányadosa is algebrai, valamint 2 és $2i$ algebrai, ezért

$$a = \frac{\alpha + \overline{\alpha}}{2} \qquad \text{és} \qquad b = \frac{\alpha - \overline{\alpha}}{2i}$$

is algebrai. ■

Most rátérünk a hatványozásra. Mivel a 0-nak csak pozitív (valós) kitevős hatványai vannak értelmezve, és ezek értéke 0, ezért a továbbiakban elég a nemnulla algebrai számok hatványozásával foglalkoznunk.

9.3.4 Tétel **T 9.3.4**

Egy algebrai szám tetszőleges racionális kitevőjű hatványa is algebrai. ♣

Bizonyítás: Mivel algebrai számok szorzata és reciproka, valamint az 1 is algebrai, ezért egy algebrai szám tetszőleges egész kitevőjű hatványa is algebrai. Ennek alapján a törtkitevőre vonatkozó állítás abból következik, hogy egy algebrai számból pozitív egész kitevőjű gyököt vonva ismét algebrai számot kapunk (lásd a 9.1.2f feladatot). ■

A nem racionális kitevővel kapcsolatban talán a legegyszerűbb kérdés, vajon $2^{\sqrt{2}}$ transzcendens-e, illetve egyáltalán irracionális-e. Ez a kérdés is szerepelt a híres Hilbert-problémák között, és Hilbert ezt jóval nehezebbnek tartotta, mint a Fermat-sejtést vagy a Riemann-sejtést. Mindez nem riasztotta el a kutatókat, és 1934-ben Gelfond és Schneider egymástól függetlenül (és eltérő módszerekkel) igazolták a következő általános tételt, amelyet bizonyítás nélkül közlünk:

9.3.5 Tétel (Gelfond–Schneider-tétel) **T 9.3.5**

Ha α és β algebrai számok, $\alpha \neq 0$ vagy 1, és β nem racionális, akkor α^β transzcendens. ♣

Ebből könnyen következik például, hogy ha n egész szám és nem 10-hatvány, akkor $\lg n$ transzcendens (lásd a 9.3.7 feladatot).

A 9.3.5 Tétel (az általában végtelen sok értékű) komplex kitevőjű hatványokra is vonatkozik. Így például egyszerűen igazolható e^π transzcendenciája (lásd a 9.3.4b feladatot). Ugyanakkor megoldatlan, hogy $e+\pi$, $e-\pi$, $e\pi$, e/π és π^e egyáltalán irracionális-e, bár a legtöbbjük biztosan transzcendens (lásd a 9.3.4a feladatot).

A 9.3.4 Tételben (illetve a 9.1.2f feladatban) láttuk, hogy az algebrai számok köréből az egész kitevőjű gyökvonás nem vezet ki. Ezt a tényt a következőképpen is megfogalmazhatjuk: Ha α algebrai szám, akkor az $x^k - \alpha$ algebrai együtthatós polinom gyökei is algebraiak. Ez nemcsak ilyen speciális alakú, hanem tetszőleges algebrai együtthatós polinom esetén is igaz:

9.3.6 Tétel **T 9.3.6**

Ha az $f \neq 0$ polinom együtthatói algebrai számok, akkor f minden (komplex) gyöke algebrai szám. ♣

Bizonyítás: Ismét a szimmetrikus polinomok alaptételét (9.3.2 Tétel) fogjuk felhasználni. (Egy másik bizonyítást adunk majd a 10.2 pontban.)

Legyen $f = \alpha + \beta x + \ldots + \xi x^n$, ahol $\alpha, \beta, \ldots, \xi$ algebrai számok, és jelölje rendre $\alpha_i, \beta_j, \ldots, \xi_k$ az $\alpha, \beta, \ldots, \xi$ minimálpolinomjának többi gyökét ($\alpha_1 = \alpha$ stb.). Tekintsük a

$$h = \prod_{i,j,\ldots,k} \left(\alpha_i + \beta_j x + \ldots + \xi_k x^n\right)$$

polinomot. Mivel h tényezői között szerepel f is, ezért f minden gyöke h-nak is gyöke. Így a tétel állításához elég megmutatni, hogy h racionális együtthatós.

Legyen c_r a h polinom tetszőleges együtthatója. A 9.3.1 Tétel bizonyításának gondolatmenetéhez hasonlóan c_r az α_i-knek egy F_r szimmetrikus polinomja, ahol F_r együtthatói a $\beta_j, \ldots, \xi_k$ számokból összeadás, kivonás és szorzás segítségével adódnak. A 9.3.2 Tétel szerint F_r előáll az α_i-k elemi szimmetrikus polinomjainak a polinomjaként. Az m_α polinomra a gyökök és együtthatók közötti összefüggést alkalmazva kapjuk, hogy a szóban forgó elemi szimmetrikus polinomok racionális számok. Ennek alapján c_r-ből „kiküszöböltük" az α_i-ket. Ugyanezt a gondolatmenetet a β_j-kre stb. megismételve kapjuk, hogy c_r racionális szám. ■

A 9.3.1 és 9.3.6 Tételek együttesen azt a tényt fejezik ki, hogy az algebrai számok egy *algebrailag zárt* testet alkotnak.

Feladatok

9.3.1

a) Igazoljuk, hogy egy algebrai és egy transzcendens szám összege mindig transzcendens.

b) Mutassuk meg, hogy két transzcendens szám összege lehet transzcendens, de lehet algebrai is.

c) Vizsgáljuk meg a hasonló kérdéseket összeg helyett szorzatra is.

9.3.2 Mit állíthatunk α-ról és β-ról (algebrai, illetve transzcendens szempontból), ha

a) $\alpha + \beta$ és $\alpha - \beta$ algebrai;

b) $\alpha + \beta$ algebrai, $\alpha - \beta$ transzcendens;

c) $\alpha+\beta$ és $\alpha-\beta$ transzcendens;
d) $\alpha\beta$ és α/β algebrai;
e) $\alpha+\beta$ algebrai, $\alpha\beta$ transzcendens;
f) $\alpha+\beta$ transzcendens, $\alpha\beta$ algebrai;
g) $\alpha+\beta$ és $\alpha\beta$ transzcendens;
h) $\alpha+\beta$ és $\alpha\beta$ algebrai?

Mennyiben változik a helyzet, ha (α és β valós számok, és) az „algebrai", illetve „transzcendens" szavak helyett „racionális"-t, illetve „irracionális"-t írunk?

9.3.3 Tegyük fel, hogy $\alpha+\beta$ és $\alpha+\gamma$ algebrai, $\beta+\gamma$ transzcendens. Az alábbi számok mindegyikéről döntsük el, hogy algebrai-e vagy transzcendens:

a) α; b) $2\alpha+(1-i)\beta+(1+i)\gamma$; c) $3\alpha+(2-i)\beta+(2+i)\gamma$.

9.3.4 Mint jeleztük, megoldatlan probléma, vajon $e+\pi$, $e-\pi$, $e\pi$, e/π és π^e transzcendens-e (illetve egyáltalán irracionális-e).

a) Az $e+\pi$, $e-\pi$, $e\pi$ és e/π számok közül legfeljebb hány lehet esetleg algebrai?

b) Igazoljuk, hogy (b1) $e+i\pi$ és (b2) e^π transzcendens.

9.3.5 Az alábbi számok mindegyikéről döntsük el, hogy algebrai-e vagy transzcendens:

a) $\sin 7^\circ$; b) $i\pi+\pi/i$; c) $\pi^7+i\pi^5+\sqrt{2}\pi$.

M 9.3.6 Legyen $\alpha\neq 0$ trigonometrikus alakja $\alpha=r(\cos\varphi+i\sin\varphi)$. Bizonyítsuk be, hogy α akkor és csak akkor algebrai, ha r és $\cos\varphi$ algebrai.

9.3.7 Tegyük fel, hogy az n pozitív egész a 10-nek nem egész kitevőjű hatványa. Bizonyítsuk be, hogy $\lg n$ transzcendens.

9.3.8 Legyenek α és β komplex számok, és tekintsük a

$$H=(\alpha+\beta,\ \alpha^2+\beta^2,\ \ldots,\ \alpha^k+\beta^k,\ \ldots)$$

sorozatot. Mutassuk meg, hogy ha H-nak legalább két eleme algebrai, és ezek közül nem mindkettő 0, akkor H minden eleme algebrai.

9.3.9 Mutassuk meg, hogy bármely $\alpha>0$, $\alpha\neq 1$ (valós) algebrai számnak végtelen sok olyan valós transzcendens kitevőjű hatványa van, amely algebrai, és olyan is végtelen sok van, amely transzcendens.

9.4. Algebrai számok approximációja

Ebben a pontban algebrai számok diofantikus approximációját és ennek néhány következményét tárgyaljuk. Mivel egy nem valós komplex szám eleve nem közelíthető jól racionális számokkal, ezért csak valós algebrai számok approximációjával foglalkozunk.

A 8.1.1 feladatban láttuk, hogy a racionális számok „nagyon rosszul" approximálhatók. A 8.1.6 Tételben, illetve a 8.1.6 feladatban megmutattuk, hogy az irracionális számok közül az $(1+\sqrt{5})/2$, illetve a $\sqrt{2}$ szintén „elég rosszul" approximálható. Liouville bebizonyította, hogy az algebrai számok általában is rosszul approximálhatók, a következő értelemben:

9.4.1 Tétel **T 9.4.1**

Legyen $n \geq 2$ és α egy n-edfokú (valós) algebrai szám. Ekkor létezik olyan $c = c(\alpha) > 0$ valós konstans, hogy bármely r/s racionális számra

$$\left|\alpha - \frac{r}{s}\right| > \frac{c(\alpha)}{s^n} \,. \quad \clubsuit \tag{1}$$

Megjegyzések: 1. A 9.4.1 Tételt szokás a következő alakban is megfogalmazni: Létezik olyan $c' = c'(\alpha) > 0$ valós konstans, hogy az

$$\left|\alpha - \frac{r}{s}\right| < \frac{c'(\alpha)}{s^n}$$

egyenlőtlenség csak véges sok r/s racionális számra teljesül. Ez tulajdonképpen azt jelenti, hogy (1)-nél véges sok kivételt megengedünk az r/s értékekre. Ez a véges sok kivétel azonban könnyen megszüntethető, ha (1)-ben ettől a véges sok „rossz" r/s-től függően alkalmas kisebb c értéket választunk $c(\alpha)$-nak. Ezzel beláttuk, hogy a tétel kétféle alakja ekvivalens (azaz bármelyik változatból azonnal következik a másik).

2. A 9.4.1 Tételből az is következik, hogy bármely $t > n$ és $c^* > 0$ valós számokra az

$$\left|\alpha - \frac{r}{s}\right| < \frac{c^*}{s^t}$$

egyenlőtlenség csak véges sok r/s racionális számra teljesülhet, ugyanis ha s (a t-től és c^*-tól függően) elég nagy, akkor

$$\frac{c^*}{s^t} < \frac{c(\alpha)}{s^n} \,.$$

Ezt a tényt a 8.1.7 feladatban bevezetett szóhasználat szerint úgy is megfogalmazhatjuk, hogy egy n-edfokú algebrai szám biztosan nem approximálható n-edrendnél jobban, azaz semmilyen $t > n$ esetén nem approximálható t-edrendben. Ennél sokkal élesebb eredmény is igaz, lásd a 9.4.3 Tételt.

3. A 8.1.1 feladat szerint a 9.4.1 Tétel $n = 1$-re is érvényes, ha az $\alpha = r/s$ lehetőséget kizárjuk.

Bizonyítás: Tegyük fel indirekt, hogy bármely $c > 0$-hoz létezik olyan r/s, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{c}{s^n}\,.$$

Ez azt jelenti, hogy létezik racionális számoknak olyan r_i/s_i sorozata, hogy ($s_i > 0$ és)

$$\lim_{i\to\infty} s_i^n\Big(\alpha - \frac{r_i}{s_i}\Big) = 0. \tag{2}$$

Ebből azonnal adódik az is, hogy

$$\lim_{i\to\infty}\Big(\alpha - \frac{r_i}{s_i}\Big) = 0, \qquad \text{azaz} \qquad \lim_{i\to\infty}\frac{r_i}{s_i} = \alpha. \tag{3}$$

Tekintsük α minimálpolinomjának egy egész együtthatós alakját, és legyenek m_α komplex gyökei $\alpha_1 = \alpha$, α_2, …, α_n. Ekkor

$$m_\alpha = a_0 + a_1x + \ldots + a_nx^n = a_n\prod_{j=1}^{n}(x - \alpha_j), \tag{4}$$

ahol a_0, , a_1, , …, a_n egész és $a_n \neq 0$. Mivel m_α irreducibilis $\mathbf{Q}$ felett, ezért nem lehet többszörös (komplex) gyöke (lásd a 9.4.4 feladatot), vagyis az α_j számok mind különbözők.

Az m_α-ba r_i/s_i-t behelyettesítve (4) alapján azt kapjuk, hogy

$$a_0 + a_1\Big(\frac{r_i}{s_i}\Big) + \ldots + a_n\Big(\frac{r_i}{s_i}\Big)^n = a_n\Big(\frac{r_i}{s_i} - \alpha\Big)\prod_{j=2}^{n}\Big(\frac{r_i}{s_i} - \alpha_j\Big)\,. \tag{5}$$

Az (5) bal oldalán álló kifejezés egy s_i^n nevezőjű tört, továbbá nem lehet 0, mivel m_α-nak nincs racionális gyöke. Ezért (5) bal oldalának az abszolút értéke legalább $1/s_i^n$. Így (5)-öt s_i^n-nel beszorozva azt kapjuk, hogy

$$1 \le \left|s_i^n a_n\Big(\alpha - \frac{r_i}{s_i}\Big)\prod_{j=2}^{n}\Big(\frac{r_i}{s_i} - \alpha_j\Big)\right|. \tag{6}$$

A (2)-beli, valamint a (3)-ból adódó

$$\lim_{i\to\infty}\prod_{j=2}^{n}\Big(\frac{r_i}{s_i}-\alpha_j\Big)=\prod_{j=2}^{n}(\alpha-\alpha_j)$$

határértékek alapján (6) jobb oldala $i\to\infty$ esetén 0-hoz tart. Ez azonban nyilvánvalóan ellentmond a (6)-beli egyenlőtlenségnek. ■

A 9.4.1 Tételre támaszkodva a következőképpen lehet transzcendens számot konstruálni: ha egy α valós szám „nagyon jól" approximálható, akkor α szükségképpen transzcendens. Ilyen α számot egy olyan, racionális számokból képzett végtelen sor összegeként kaphatunk, amelynek a részletösszegei rendkívül gyorsan konvergálnak a végtelen sor összegéhez. Az alábbiakban ezt a Liouville-tól származó konstrukciót ismertetjük.

9.4.2 Tétel **T 9.4.2**

Az

$$\alpha=\sum_{k=1}^{\infty}\frac{1}{10^{k!}}=0{,}11000100000000000000000001\ldots \tag{7}$$

szám transzcendens. (A tizedes törtben a $k!$ sorszámú tizedesjegyek értéke 1, a többi jegy 0.) ♣

A (7) képlet valóban egy valós számot definiál, ez közvetlenül leolvasható a tizedestört-alakból (de azonnal adódik abból is, hogy a megadott végtelen sor konvergens, hiszen majorálható a $\sum_{k=1}^{\infty}10^{-k}$ végtelen mértani sorral).

Bizonyítás: Megmutatjuk, hogy a (7) végtelen sor részletösszegei „nagyon jól" approximálják α-t.

Írjuk fel az m-edik részletösszeget r_m/s_m alakban, ahol $(r_m,s_m)=1$ és $s_m>0$. Ezt közös nevezőre hozással kapjuk:

$$\sum_{k=1}^{m}\frac{1}{10^{k!}}=\frac{10A+1}{10^{m!}}\,,$$

tehát $s_m=10^{m!}$. Ekkor

$$0<\alpha-\frac{r_m}{s_m}=\sum_{k=m+1}^{\infty}\frac{1}{10^{k!}}<\sum_{j=(m+1)!}^{\infty}\frac{1}{10^{j}}=\frac{10}{9\cdot 10^{(m+1)!}}=\frac{10}{9s_m^{m+1}}\,.$$

Ebből következik, hogy

$$\left|\alpha - \frac{r_m}{s_m}\right| < \frac{10}{9s_m^{m+1}}\,. \tag{8}$$

Tegyük fel indirekt, hogy valamely n-re α egy n-edfokú algebrai szám. Mivel α nem szakaszos tizedes tört, ezért α irracionális, azaz $n \geq 2$. Ekkor a 9.4.1 Tétel szerint van olyan $c(\alpha) > 0$, hogy bármely r/s racionális számra (1)-nek kell teljesülnie. Így speciálisan r_m/s_m esetén is

$$\left|\alpha - \frac{r_m}{s_m}\right| > \frac{c(\alpha)}{s_m^n}\,. \tag{9}$$

Ezt (8)-cal összevetve

$$\frac{c(\alpha)}{s_m^n} < \frac{10}{9s_m^{m+1}}\,, \qquad \text{azaz} \qquad s_m^{m-n+1} < \frac{10}{9c(\alpha)}$$

adódik, ami elég nagy m-re ellentmondás. ■

Mint a 9.4.1 Tétel utáni 2. megjegyzésben jeleztük, a 9.4.1 Tétel állítása jelentősen élesíthető. Erre vonatkoznak Thue, illetve Roth alábbi eredményei, amelyeket bizonyítás nélkül közlünk:

9.4.3 Tétel **T 9.4.3**

(i) (*Thue tétele.*) Legyen $n \geq 3$ és α egy n-edfokú (valós) algebrai szám. Ekkor bármilyen (nagy) $c > 0$ valós konstans esetén az

$$\left|\alpha - \frac{r}{s}\right| < \frac{c}{s^n} \tag{10}$$

egyenlőtlenséget csak véges sok r/s racionális szám elégíti ki.

(ii) (*Roth tétele.*) Legyen α tetszőleges algebrai szám és $\kappa > 0$ tetszőleges. Ekkor az

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2+\kappa}} \tag{11}$$

egyenlőtlenséget csak véges sok r/s racionális szám elégíti ki. ♣

Megjegyzések: 1. Roth tétele nyilván jóval erősebb Thue eredményénél, azonban már Thue tételének is igen fontos következményei vannak a diofantikus egyenletek elméletében (lásd a 9.4.4 Tételt).

2. Roth tétele szerint a 8.1.8 Tételben szereplő kivételes H halmaz csupa transzcendens számból áll. Ugyanakkor a 8.1.8 Tétel azt is mutatja, hogy (az

összes algebrai számon kívül) a transzcendens számok „többsége” is „nagyon rosszul” approximálható.

A diofantikus approximáció szoros kapcsolatban áll bizonyos diofantikus egyenletek vizsgálatával. A 7.8 pontban láttuk, hogy ha az m pozitív egész nem négyzetszám, akkor az $x^2 - my^2 = 1$ Pell-egyenletnek végtelen sok megoldása van (7.8.1 Tétel); ehhez azt használtuk fel, hogy a $\sqrt{m}$ irracionális szám másodrendben approximálható. Most az algebrai számok rosszul approximálhatóságára támaszkodva azt fogjuk igazolni, hogy bizonyos magasabb fokú diofantikus egyenleteknek legfeljebb véges sok megoldása lehet.

9.4.4 Tétel **T 9.4.4**

Legyen $f = a_0 + a_1 x + \ldots + a_n x^n$ egy n-edfokú egész együtthatós polinom, ahol $n \geq 3$ és f irreducibilis $\mathbf{Q}$ felett. Ekkor bármely (rögzített) b egész szám esetén a

$$g(y,z) = y^n f\Big(\frac{z}{y}\Big) = a_0 y^n + a_1 y^{n-1} z + \ldots + a_n z^n = b \tag{12}$$

diofantikus egyenletnek csak véges sok megoldása lehet. ♣

Bizonyítás: Tegyük fel indirekt, hogy a (12) diofantikus egyenletet végtelen sok (y_i, z_i) egész számpár kielégíti. Mivel egy adott y-hoz nyilván legfeljebb n darab z tartozhat, ezért

$$\lim_{i\to\infty} |y_i| = \infty\,, \tag{13}$$

és azt is feltehetjük, hogy az y_i értékek egyike sem 0.

A (12) egyenletbe az (y_i, z_i) megoldást behelyettesítve, majd az egyenlőséget y_i^n-nel elosztva azt kapjuk, hogy

$$f\Big(\frac{z_i}{y_i}\Big) = \frac{b}{y_i^n}\,. \tag{14}$$

A (13) és (14) összefüggésekből az is következik, hogy

$$\lim_{i\to\infty} f\Big(\frac{z_i}{y_i}\Big) = 0\,. \tag{15}$$

Legyen f gyöktényezős alakja

$$f = a_n \prod_{j=1}^{n} (x - \alpha_j). \tag{16}$$

Ekkor az $f(z_i/y_i)$ helyettesítési értékre

$$f\Big(\frac{z_i}{y_i}\Big) = a_n \prod_{j=1}^{n}\Big(\frac{z_i}{y_i} - \alpha_j\Big) \tag{17}$$

adódik. Mivel (15) szerint $i \to \infty$ mellett (17) bal oldala 0-hoz tart, ezért az i indexek alkalmas részsorozatát véve a jobb oldal valamelyik tényezőjének is 0 a határértéke. Legyen ez mondjuk a jobb oldal első tényezője, és az egyszerűség kedvéért jelöljük a szóban forgó részsorozatot ugyanúgy, mint az eredeti sorozatot, ekkor tehát

$$\lim_{i\to\infty}\Big(\frac{z_i}{y_i} - \alpha_1\Big) = 0, \qquad \text{azaz} \qquad \lim_{i\to\infty}\frac{z_i}{y_i} = \alpha_1\,. \tag{18}$$

Ebből speciálisan az is következik, hogy α_1 valós szám.

(18) alapján

$$\lim_{i\to\infty} a_n \prod_{j=2}^{n}\Big(\frac{z_i}{y_i} - \alpha_j\Big) = a_n \prod_{j=2}^{n}(\alpha_1 - \alpha_j). \tag{19}$$

Jelöljük a (19)-beli határértéket d-vel. Az f irreducibilitása miatt az α_j számok különbözők, tehát $d \neq 0$. Így elég nagy i esetén

$$\Big|a_n \prod_{j=2}^{n}\Big(\frac{z_i}{y_i} - \alpha_j\Big)\Big| \;>\; \Big|\frac{d}{2}\Big|\,. \tag{20}$$

Végül (14), (17) és (20) alapján kapjuk, hogy minden elég nagy i-re

$$\begin{aligned}\Big|\frac{b}{y_i^n}\Big| \;&=\; \Big|f\Big(\frac{z_i}{y_i}\Big)\Big| \;=\; \Big|a_n \prod_{j=1}^{n}\Big(\frac{z_i}{y_i} - \alpha_j\Big)\Big| = \\ &= \Big|\alpha_1 - \frac{z_i}{y_i}\Big| \cdot \Big|a_n \prod_{j=2}^{n}\Big(\frac{z_i}{y_i} - \alpha_j\Big)\Big| \;>\; \Big|\alpha_1 - \frac{z_i}{y_i}\Big| \cdot \Big|\frac{d}{2}\Big|\,,\end{aligned}$$

azaz

$$\Big|\alpha_1 - \frac{z_i}{y_i}\Big| \;<\; \Big|\frac{2b}{d}\cdot\frac{1}{y_i^n}\Big|. \tag{21}$$

Mivel α_1 egy n-edfokú algebrai szám, ezért (21) ellentmond a 9.4.3 Tétel (i) állításának. ■

Megjegyezzük, hogy hasonló gondolatmenettel még sokkal általánosabb diofantikus egyenletekről lehet kimutatni a megoldásszám végességét, ha a 9.4.3 Tétel (ii) állítását használjuk fel (lásd a 9.4.3 feladatot).

Feladatok

9.4.1 *Liouville-szám*oknak azokat az α irracionális számokat nevezzük, amelyekhez bármely n esetén található olyan r/s tört, hogy

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^n}\,.$$

A 9.4.1 Tétel szerint minden Liouville-szám transzcendens.

M a) Tegyük fel, hogy α Liouville-szám. Mutassuk meg ekkor bármely $h \neq 0$ racionális szám, illetve k pozitív egész esetén

(a1) $h+\alpha$; (a2) $h\alpha$; (a3) α^k; (a4) $1/\alpha$

is Liouville-szám.

b) Bizonyítsuk be, hogy végtelen sok, sőt kontinuum számosságú Liouville-szám létezik.

9.4.2 Igazoljuk, hogy a 9.4.4 Tétel állítása akkor is érvényben marad, ha az f egész együtthatós, legalább harmadfokú polinomról a $\mathbf{Q}$ feletti irreducibilitás helyett csak az alábbi enyhébb feltételek valamelyikét tesszük fel:

a) Az f-nek nincs első- vagy másodfokú osztója a racionális együtthatós polinomok körében.

b) Ha $b = 0$, akkor f-nek nincs racionális gyöke, ha pedig $b \neq 0$, akkor f-nek nincs többszörös (komplex) gyöke.

9.4.3 Legyen $g(y,z)$ a 9.4.4 Tételben definiált kétváltozós polinom, és $h(y,z)$ egy tetszőleges egész együtthatós, legfeljebb $n-3$-adfokú, kétváltozós polinom. A 9.4.3 Tétel (ii) állításának felhasználásával bizonyítsuk be, hogy a $g(y,z) = h(y,z)$ diofantikus egyenletnek csak véges sok megoldása lehet.

M 9.4.4 Tegyük fel, hogy az $f \in \mathbf{Q}[x]$ polinom irreducibilis $\mathbf{Q}$ felett. Bizonyítsuk be, hogy f-nek nem lehet többszörös (komplex) gyöke.

9.5. Az e transzcendens szám

Először megmutatjuk, hogy e (a természetes logaritmus alapszáma) és π irracionális számok, majd e transzcendenciáját igazoljuk. Megjegyezzük, hogy a módszer (jelentős) továbbfejlesztésével az is belátható, hogy π transzcendens. Ez utóbbi tény fontos következménye, hogy egy adott körhöz (euklideszi szerkesztéssel) nem szerkeszthető vele azonos területű négyzet.

9.5.1 Tétel **T 9.5.1**

Az e irracionális szám. ♣

Bizonyítás: Az e szám előáll az alábbi végtelen sor összegeként:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{n!} + \ldots \tag{1}$$

Tegyük fel indirekt, hogy $e = a/b$, ahol a és b pozitív egészek. Ekkor $b!e$ egész szám, továbbá (1)-et $b!$-sal beszorozva kapjuk, hogy

$$b!e = n_b + \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \ldots,$$

ahol n_b egy b-től függő egész szám. Innen a $b!e - n_b$ egész számra az alábbi becsléseket nyerjük:

$$\begin{aligned} 0 < b!e - n_b &= \frac{1}{b+1} + \frac{1}{(b+1)(b+2)} + \ldots < \\ &< \frac{1}{b+1} + \frac{1}{(b+1)^2} + \ldots = \frac{1}{b+1} \cdot \frac{1}{1 - \frac{1}{b+1}} = \frac{1}{b}\,. \end{aligned}$$

Ez azt jelenti, hogy a $b!e - n_b$ egész szám 0 és $1/b$ közé esik, ami nyilvánvaló ellentmondás. ■

9.5.2 Tétel **T 9.5.2**

A π irracionális szám. ♣

Bizonyítás: Tegyük fel indirekt, hogy $\pi = a/b$, ahol a és b pozitív egészek.

Legyen n (nagy) pozitív egész és f a következő $2n$-edfokú polinom:

$$f(x) = \frac{x^n(1-x)^n}{n!}\,.$$

Tekintsük az

$$I = a^{2n+1} \int_0^1 \sin(\pi x) f(x) dx$$

integrált. Megmutatjuk, hogy egyrészt

(A) I egész szám,

másrészt

(B) elég nagy n esetén $0 < I < 1$,

ami nyilvánvaló ellentmondás.

(B) igazolásával kezdjük. Mivel $0 < x < 1$ esetén

$$0 < \sin(\pi x) \le 1 \qquad \text{és} \qquad 0 < f(x) < \frac{1}{n!}\,,$$

ezért

$$0 < I < \frac{a^{2n+1}}{n!}\,.$$

Ha n elég nagy, akkor $a^{2n+1}/n! < 1$, tehát ezzel a (B) állítást beláttuk.

Rátérve (A)-ra, először megmutatjuk, hogy az f függvény és valamennyi (első, második stb.) deriváltja a 0 és az 1 helyen egész értéket vesz fel, azaz

$$f^{(m)}(0) \quad \text{és} \quad f^{(m)}(1) \quad \text{egész szám}, \qquad m = 0, 1, 2, \dots \tag{2}$$

Mivel $f(x) = f(1-x)$, ezért bármely m-re $f^{(m)}(x) = (-1)^m f^{(m)}(1-x)$, és így speciálisan $f^{(m)}(0) = (-1)^m f^{(m)}(1)$. Ennek alapján elég az $x = 0$ helyet vizsgálni.

Az f polinom

$$f(x) = \frac{1}{n!}\big(c_n x^n + c_{n+1} x^{n+1} + \dots + c_{2n} x^{2n}\big)$$

alakba írható, ahol a c_i együtthatók egész számok. Innen kapjuk, hogy

$$f^{(m)}(0) = \begin{cases} 0, & \text{ha } 0 \le m < n \text{ vagy } m > 2n; \\ \dfrac{c_m m!}{n!} = c_m (n+1) \dots m, & \text{ha } n \le m \le 2n. \end{cases}$$

Ezzel (2)-t beláttuk.

Az I integrálról sorozatos parciális integrálással mutatjuk meg, hogy egész szám. Az első parciális integrálásnál, a $\pi = a/b$ indirekt feltevést is felhasználva, az adódik, hogy

$$\begin{aligned} I &= a^{2n+1} \int_0^1 \sin(\pi x) f(x) dx = \\ &= a^{2n+1} \left[\frac{-\cos(\pi x) f(x)}{\pi} \right]_0^1 - \frac{a^{2n+1}}{\pi} \int_0^1 -\cos(\pi x) f'(x) dx = \\ &= -a^{2n} b (f(1) \cos \pi - f(0) \cos 0) + I_1 \,, \end{aligned} \tag{3}$$

ahol

$$I_1 = a^{2n} b \int_0^1 \cos(\pi x) f'(x) dx.$$

Mivel a, b, $f(1)$, $f(0)$, $\cos \pi$ és $\cos 0$ egész számok, ezért (3) alapján I pontosan akkor egész szám, ha I_1 is egész szám.

Az I_1-et ismét parciálisan integráljuk, és újra felhasználjuk a $\pi = a/b$ indirekt feltevést is:

$$\begin{aligned} I_1 &= a^{2n} b \int_0^1 \cos(\pi x) f'(x) dx = \\ &= a^{2n} b \left[\frac{\sin(\pi x) f'(x)}{\pi} \right]_0^1 - \frac{a^{2n} b}{\pi} \int_0^1 \sin(\pi x) f''(x) dx = \\ &= a^{2n-1} b^2 (f'(1) \sin \pi - f'(0) \sin 0) - I_2 \,, \end{aligned}$$

ahol

$$I_2 = a^{2n-1} b^2 \int_0^1 \sin(\pi x) f''(x) dx.$$

Az előzőkhöz hasonlóan adódik, hogy I_1 pontosan akkor egész szám, ha I_2 is az.

Az eljárást ugyanígy folytatva eljutunk az

$$I_{2n+1} = b^{2n+1} \int_0^1 \cos(\pi x) f^{(2n+1)}(x) dx$$

integrálhoz, és azt kell belátni, hogy ez egész szám. Mivel az f egy $2n$-edfokú polinom volt, ezért $f^{(2n+1)}(x) = 0$, tehát $I_{2n+1} = 0$. Ennélfogva I_{2n+1}, és így I is valóban egész szám. Ezzel az (A) állítást is beláttuk. ■

9.5.3 Tétel **T 9.5.3**

Az e transzcendens szám. ♣

Bizonyítás: Tegyük fel indirekt, hogy e algebrai, azaz alkalmas $n \geq 1$ és $a_0 \neq 0$, $a_1, \ldots, a_n$ egész számokra

$$a_0 + a_1 e + \ldots + a_n e^n = 0. \tag{4}$$

A π irracionalitásának bizonyításához hasonlóan most is egy integrál segítségével jutunk majd ellentmondásra.

Legyen f később alkalmasan megválasztandó polinom, $\deg f = k$, és tetszőleges $s \geq 0$ egész számra tekintsük az alábbi integrált:

$$I(s) = \int_0^s e^{-x} f(x) dx. \tag{5}$$

Parciális integrálással kapjuk, hogy

$$I(s) = \left[-e^{-x} f(x)\right]_0^s + \int_0^s e^{-x} f'(x) dx = f(0) - f(s)e^{-s} + I_1(s)\,, \tag{6}$$

ahol

$$I_1(s) = \int_0^s e^{-x} f'(x) dx.$$

Hasonló módon, $I_1(s)$ parciális integrálásával adódik, hogy

$$I_1(s) = \left[-e^{-x} f'(x)\right]_0^s + \int_0^s e^{-x} f''(x) dx = f'(0) - f'(s)e^{-s} + I_2(s)\,, \tag{7}$$

ahol

$$I_2(s) = \int_0^s e^{-x} f''(x) dx.$$

Így (6) és (7) alapján

$$I(s) = \left[f(0) + f'(0)\right] - \left[f(s) + f'(s)\right]e^{-s} + I_2(s).$$

Az eljárást folytatva végül $f^{(k+1)} = 0$ miatt $I_{k+1} = 0$, és így

$$\begin{aligned} I(s) &= \int_0^s e^{-x} f(x) dx = \\ &= \left[f(0) + f'(0) + \ldots + f^{(k)}(0)\right] - \left[f(s) + f'(s) + \ldots + f^{(k)}(s)\right]e^{-s} \end{aligned} \tag{8}$$

adódik.

Szorozzuk be (8)-at $a_s e^s$-sel, majd adjuk össze az $s = 0, 1, \ldots, n$ értékekre ily módon kapott egyenlőségeket. Ekkor a

$$\begin{aligned}\sum_{s=0}^{n} a_s e^s I(s) &= \sum_{s=0}^{n} a_s e^s \int_0^s e^{-x} f(x)dx = \\ &= \sum_{s=0}^{n} a_s e^s \big[f(0) + f'(0) + \ldots + f^{(k)}(0)\big] - \\ &\quad - \sum_{s=0}^{n} a_s \big[f(s) + f'(s) + \ldots + f^{(k)}(s)\big]\end{aligned} \tag{9}$$

összefüggéshez jutunk. A (9) középső sorában szereplő összeg értéke a (4)-beli indirekt feltevés miatt 0, ezért (9) átírható a

$$\sum_{s=0}^{n} a_s e^s \int_0^s e^{-x} f(x)dx = -\sum_{s=0}^{n} a_s \big[f(s) + f'(s) + \ldots + f^{(k)}(s)\big] \tag{10}$$

alakba.

Az ellentmondás abból fog adódni, hogy alkalmas f-re (10) bal oldala 1-nél kisebb abszolút értékű, jobb oldala pedig egy nullától különböző egész szám.

Legyen $p > n|a_0|$ egy (nagy) prímszám és

$$f(x) = \frac{x^{p-1}(x-1)^p \ldots (x-n)^p}{(p-1)!}\,. \tag{11}$$

A 9.5.2 Tétel bizonyításában szereplő (2) állítás általánosításaként ugyanúgy igazolható az alábbi észrevétel: Ha $t \geq 0$ és j egész számok, $h(x)$ egész együtthatós polinom, akkor a

$$g(x) = \frac{(x-j)^t h(x)}{t!}$$

polinom és valamennyi deriváltja a j helyen egész értéket vesz fel: $g^{(m)}(j)$ minden m-re egész szám. Valóban: $g(x)$-et

$$g(x) = \frac{d_t(x-j)^t + d_{t+1}(x-j)^{t+1} + \ldots + d_r(x-j)^r}{t!}$$

alakba írva azt kapjuk, hogy

$$g^{(m)}(j) = \begin{cases} 0, & \text{ha } 0 \leq m < t \text{ vagy } m > r; \\ \dfrac{d_m m!}{t!} = d_m(t+1)\ldots m, & \text{ha } t \leq m \leq r. \end{cases} \tag{12}$$

Mivel

$$f(x) = p \cdot \frac{(x-1)^p h_1(x)}{p!} ,$$

ahol $h_1(x)$ egész együtthatós polinom, ezért (12)-t a $g(x) = f(x)/p$, $t = p$, $j = 1$ és $h(x) = h_1(x)$ szereposztással alkalmazva azt nyerjük, hogy minden m-re $f^{(m)}(1)$ egész szám, sőt osztható p-vel. Ugyanígy adódik, hogy

$$p \mid f^{(m)}(j), \qquad j = 1, 2, \dots, n, \qquad m = 0, 1, 2, \dots \tag{13}$$

Végül, írjuk az $f(x)$-et

$$f(x) = \frac{x^{p-1} h_0(x)}{(p-1)!}$$

alakba, ahol $h_0(x)$ egész együtthatós polinom, és alkalmazzuk (12)-t a $g(x) = f(x)$, $t = p-1$, $j = 0$ és $h(x) = h_0(x)$ szereposztással. Ekkor azt kapjuk, hogy $f^{(m)}(0)$ is minden m-re egész szám, továbbá

$$p \nmid f^{(p-1)}(0) = (-1)^{np}(n!)^p , \qquad \text{de} \qquad p \mid f^{(m)}(0), \quad \text{ha} \quad m \neq p-1 \tag{14}$$

(ez utóbbi onnan adódik, hogy (12) alapján $m < p-1$ esetén $f^{(m)}(0) = 0$, $m \geq p$ esetén pedig az $f^{(m)}(0) = d_m p \dots m$ szorzatban szerepel a p tényező).

Így (13) és (14) alapján azt kapjuk, hogy a (10) jobb oldalán álló (kettős) összeg minden tagja egész szám és az $a_0 f^{(p-1)}(0)$ tag kivételével minden tag osztható p-vel. Ebből következik, hogy (10) jobb oldala egy p-vel nem osztható egész szám, tehát speciálisan nem lehet nulla.

Most megmutatjuk, hogy elég nagy p esetén (10) bal oldalának az abszolút értéke kisebb, mint 1. Mivel $0 < x < n$ esetén

$$|e^{-x}| < 1 \qquad \text{és} \qquad |f(x)| = \left| \frac{x^{p-1}(x-1)^p \dots (x-n)^p}{(p-1)!} \right| < \frac{n^{(n+1)p-1}}{(p-1)!} ,$$

ezért

$$\left| \sum_{s=0}^{n} a_s e^s \int_0^s e^{-x} f(x) dx \right| \leq \frac{e^n \left(\sum_{s=0}^{n} |a_s| \right) \left(n^{n+1} \right)^p}{(p-1)!} . \tag{15}$$

A (15) jobb oldala $A \cdot B^p/(p-1)!$ alakú, ahol A és B konstansok. Ez a kifejezés $p \to \infty$ mellett 0-hoz tart, tehát elég nagy p-re kisebb lesz, mint 1.

Ezzel befejeztük annak igazolását, hogy a (10) egyenlőség bal oldalának abszolút értéke 1-nél kisebb, a jobb oldal pedig egy nemnulla egész szám. A (4) indirekt feltevés tehát ellentmondásra vezetett, és így az e nem lehet algebrai szám. ■

Feladatok

9.5.1 Legyen $a_1 < a_2 < \ldots < a_n < \ldots$ pozitív egészeknek olyan sorozata, ahol minden n-re $a_n \mid a_{n+1}$, továbbá bármely k pozitív egészhez létezik olyan n, amelyre $k \mid a_n$. Bizonyítsuk be, hogy a $\sum_{n=1}^{\infty} 1/a_n$ végtelen sor konvergens, és az összege irracionális szám.

9.5.2 Jelöljön r racionális számot. Igazoljuk, hogy

a) $\sin 1$ és $\cos 1$ irracionális;

*b) $0 < r \leq \pi$ esetén $\sin r$ és $\cos r$ közül legalább az egyik irracionális;

c) $0 < r < \pi/2$ esetén $\operatorname{tg} r$ irracionális.

(A szögek ívmértékben vannak megadva. Ne használjuk fel azt a korábban bizonyítás nélkül említett tényt, hogy ha n egész szám, akkor $\sin n$ transzcendens. A „fokokban mérve racionális" szögek szögfüggvényeire nézve lásd a 9.6.11 feladatot.)

*9.5.3 A 9.5.2 Tétel bizonyításának gondolatmenetét finomítva, mutassuk meg, hogy π^2 irracionális.

9.6. Algebrai egész

Az algebrai egészek olyan speciális algebrai számok, amelyek az egész számok általánosításainak tekinthetők.

A fogalom előkészítéséhez először az egészeknek a racionálisokon belül egy olyan jellemzését adjuk meg, hogy az ebben megfogalmazott tulajdonságot a racionálisok helyett az algebrai számokra is ki lehessen majd terjeszteni.

A racionális számok éppen az elsőfokú algebrai számok, az r racionális szám (egyik) minimálpolinomja $x - r$. Ez a normált (azaz 1 főegyütthatójú) minimálpolinom nyilván pontosan akkor egész együtthatós, ha az r egész szám. A racionális számok közül tehát az tünteti ki az egészeket, hogy a(z egyik) minimálpolinomjuk normált és egész együtthatós.

A minimálpolinomra előírt fenti tulajdonságot az algebrai számok körére kiterjesztve kapjuk az algebrai egész fogalmát:

9.6.1 Definíció **D 9.6.1**

Egy algebrai számot *algebrai egész*nek nevezünk, ha a(z egyik) minimálpolinomja normált és egész együtthatós. ♣

Az egyszerűbb szóhasználat érdekében ebben a pontban egy algebrai szám minimálpolinomján mindig annak normált alakját fogjuk érteni.

Példák:

P1 Egy r racionális szám akkor és csak akkor algebrai egész, ha r egész szám (az algebrai egész fogalmát éppen ennek szem előtt tartásával definiáltuk).

P2 A $\sqrt[3]{2}$ és $\sqrt[3]{1/2}$ számok közül az első algebrai egész, de a második nem az, hiszen a minimálpolinomjuk $x^3 - 2$, illetve $x^3 - (1/2)$.

P3 A 7.4 pontban szerepelt Gauss-egészek szintén algebrai egészek. Sőt, az is igaz, hogy ha tekintjük a *Gauss-racionálisok*at, vagyis az összes olyan $a + bi$ komplex számot, ahol a és b racionális, akkor ezek közül éppen a Gauss-egészek lesznek az algebrai egészek. Hasonló állítás érvényes a 7.7 pontban bevezetett Euler-egészekre (és a hozzájuk kapcsolódó Euler-racionálisokra) is. A 10. és 11. fejezetben részletesen foglalkozunk majd hasonló típusú algebrai egészek számelméleti vizsgálatával.

Az alábbi tétel lehetőséget ad arra, hogy egy algebrai számról a minimálpolinomja meghatározása nélkül is igazoljuk, hogy algebrai egész (de a tétel gyakorlatilag *nem alkalmas* annak bizonyítására, hogy a szám *nem* algebrai egész):

9.6.2 Tétel **T 9.6.2**

Egy α komplex szám akkor és csak akkor algebrai egész, ha létezik olyan f normált, egész együtthatós polinom, amelyre $f(\alpha) = 0$. ♣

Bizonyítás: Ha α algebrai egész, akkor az m_α (normált) minimálpolinom megfelel f-nek.

A megfordításhoz tegyük fel, hogy létezik olyan f normált, egész együtthatós polinom, amelyre $f(\alpha) = 0$. Ekkor a 9.2.3 Tétel szerint $m_\alpha \mid f$, azaz van olyan g racionális együtthatós polinom, amelyre $f = gm_\alpha$. Itt f és m_α főegyütthatója 1, így g főegyütthatója is 1. Továbbá f egész együtthatós, ezért a racionális együtthatós polinomokra érvényes Gauss-lemma szerint létezik olyan c racionális szám, amelyre a cg és $(1/c)m_\alpha$ polinomok mindketten egész együtthatósak. Ekkor cg, illetve $(1/c)m_\alpha$ főegyütthatója c, illetve $1/c$, amelyek egyszerre csak akkor lehetnek egészek, ha $c = \pm 1$. Ez viszont azt jelenti, hogy már maga m_α (és g) is (normált és) egész együthatós polinom, tehát α valóban algebrai egész. ■

Megjegyzések: 1. A 9.6.2 Tétel segítségével például a komplex egységgyökökről a körosztási polinomokra történő hivatkozás nélkül is megállapíthatjuk, hogy algebrai egészek, hiszen egy n-edik egységgyök gyöke az $x^n - 1$ normált, egész együtthatós polinomnak.

2. Mint említettük, a 9.6.2 Tétel alapján nem lehet kimutatni, hogy egy adott szám *nem* algebrai egész. Ugyanis abból, hogy α gyöke egy (vagy akár végtelen sok) olyan normált, racionális együtthatós polinomnak, amely nem egész együtthatós, semmilyen következtetést nem tudunk levonni arra vonatkozólag, hogy α algebrai egész-e vagy sem. Például az 1 algebrai egész, ugyanakkor gyöke az $f_n = (x-1)(x-1/2)^n$ polinomoknak ($n = 1, 2, \ldots$), és mindegyik f_n normált, racionális együtthatós, de nem egész együtthatós. Azt, hogy egy adott α nem algebrai egész, a minimálpolinomja segítségével igazolhatjuk.

Most az algebrai egészek és a műveletek kapcsolatát vizsgáljuk. A következő tételben a 9.3.1, 9.3.4 és 9.3.6 Tételek algebrai egészekre vonatkozó megfelelőit foglaljuk össze.

9.6.3 Tétel **T 9.6.3**

(i) Az algebrai egészek részgyűrűt alkotnak a komplex számtestben, azaz algebrai egészek összege, különbsége és szorzata is algebrai egész (a hányadosuk azonban általában nem az).

(ii) Egy algebrai egész tetszőleges pozitív racionális kitevőjű hatványa is algebrai egész.

(iii) Ha az f normált polinom együtthatói algebrai egészek, akkor f minden (komplex) gyöke is algebrai egész. ♣

Bizonyítás: Mindhárom állítás ugyanúgy adódik, mint ahogy az algebrai számokra vonatkozó megfelelőiket (a 9.3.1, 9.3.4, illetve 9.3.6 Tételben) igazoltuk: a gondolatmenetben az „algebrai szám" kifejezést „algebrai egész"-re, a „racionális szám"-ot „egész szám"-ra, a „racionális együtthatós"-t pedig „normált, egész együtthatós"-ra kell cserélni (és természetesen a reciprokra vonatkozó részeket figyelmen kívül kell hagyni, valamint a 9.3.6 Tétel bizonyítását nézve most a normáltság miatt $\xi = 1$, tehát a ξ_k-kra nincs szükség). A fentieknek minden lépésre kiterjedő, részletes ellenőrzését az Olvasóra bízzuk. ■

Feladatok

9.6.1 Mutassuk meg, hogy ha α algebrai egész, akkor $\overline{\alpha}$, $2\mathrm{Re}(\alpha)$, $2\mathrm{Im}(\alpha)$ és $|\alpha|$ is algebrai egész.

9.6.2 Az alábbi számok közül melyek algebrai egészek?

a) $\sqrt[5]{5} + (\sqrt[7]{7}/2)$; b) $(1+\sqrt{3})/2$; c) $(1+i\sqrt{3})/2$; d) $\cos 1^\circ$.

9.6.3 Tekintsük az $\alpha = a + bi$ komplex számot (ahol a és b valós szám). Melyek igazak az alábbi állítások közül?

a) Ha a és b algebrai egész, akkor α is algebrai egész.

b) Ha a algebrai egész, akkor α is algebrai egész.

c) Ha a és $|\alpha|$ algebrai egész, akkor α is algebrai egész.

d) Ha α algebrai egész, akkor a és b is algebrai egész.

e) Ha α és a algebrai egész, akkor b is algebrai egész.

f) Ha α algebrai egész, továbbá a és b racionális, akkor a és b egész szám.

g) Ha $\alpha + 3\beta$ és $5\alpha + 7\beta$ algebrai egész, akkor α és β is algebrai egész.

h) Ha $\alpha + \beta$ és $\alpha\beta$ algebrai egész, akkor α és β is algebrai egész.

9.6.4 Vizsgáljuk meg a Fermat-sejtés algebrai egészekre vonatkozó változatát: Rögzített $n \geq 3$ egész kitevő mellett létezik-e megoldása az $x^n + y^n = z^n$ egyenletnek a nemnulla algebrai egészek körében?

M 9.6.5 Legyen f olyan normált, racionális együtthatós polinom, amelynek nem minden együtthatója egész szám, és tekintsük f (komplex) gyökeit. Melyek igazak az alábbi állítások közül?

a) Az f-nek létezik olyan gyöke, amely nem algebrai egész.

b) Az f egyetlen gyöke sem algebrai egész.

c) Ha f irreducibilis $\mathbf{Q}$ felett, akkor f egyetlen gyöke sem algebrai egész.

d) Ha az f különböző gyökei között pontosan egy olyan van, amely nem algebrai egész, akkor f-nek létezik racionális gyöke.

9.6.6 Bizonyítsuk be, hogy minden algebrai szám felírható két algebrai egész hányadosaként, sőt az is elérhető, hogy ezek közül az egyik (akár az osztandó, akár az osztó) egész szám legyen.

9.6.7 Hogyan olvasható le az α algebrai egész minimálpolinomjáról, hogy $1/\alpha$ is algebrai egész?

9.6.8 Bizonyítsuk be az alábbi állításokat.

a) Bármely α algebrai egészhez végtelen sok olyan β algebrai egész létezik, amelyre α/β is algebrai egész.

b) Bármely olyan $\alpha \neq 0$ algebrai egészhez, amelynek a reciproka nem algebrai egész, végtelen sok olyan β algebrai egész létezik, amelynek a reciproka nem algebrai egész, és amelyre α/β algebrai egész.

c) Bármely $\alpha \neq 0$ algebrai egészhez csak véges sok olyan b egész szám létezik, amelyre α/b algebrai egész.

9.6.9 Van-e az egységnyi abszolút értékű komplex számok között az egységgyökökön kívül

a) algebrai szám;
*b) algebrai egész?

*9.6.10

a) Mutassuk meg, hogy ha $n \geq 2$, akkor az n-edfokú algebrai egészek mindenütt sűrűn helyezkednek el a valós számegyenesen.

b) Mindenütt sűrűek-e a komplex számsíkon az n-edfokú algebrai egészek, ha (b1) $n = 2$; (b2) $n = 4$?

9.6.11

a) Legyen r tetszőleges valós szám. Igazoljuk, hogy r és $\cos r^\circ$ közül legalább az egyik irracionális, kivéve ha r olyan egész szám, amely osztható 60-nal vagy 90-cel.

b) Fogalmazzuk meg és bizonyítsuk be a szinuszra és tangensre vonatkozó hasonló állítást.

10. ALGEBRAI SZÁMTESTEK

Algebrai számtesteknek a racionális test egyszerű algebrai bővítéseit nevezzük. Ebben a fejezetben az ilyen testbővítésekkel és az ezekben található algebrai egészek aritmetikai tulajdonságaival foglalkozunk. Részletesen tárgyaljuk a másodfokú bővítések algebrai egészeit. Ezek speciális eseteként a 7. fejezetben már találkoztunk a Gauss-, illetve Euler-egészekkel, amelyeket sikerrel alkalmaztunk az $x^2+y^2=n$, illetve $x^3+y^3=z^3$ diofantikus egyenletek megoldásánál. Az algebrai számtestek vizsgálatát az ideálelmélet eszközeinek bevonásával a következő fejezetben is folytatjuk.

Megjegyezzük, hogy a testbővítésekről szóló általános bevezető tetszőleges (kommutatív) test esetén érvényes, bár a továbbiakban ezt mindig csak a komplex test résztesteire fogjuk alkalmazni. Előrebocsátjuk még, hogy ebben a fejezetben számos helyen felhasználunk néhány alapvető, elsősorban a vektorterek dimenziójához kapcsolódó lineáris algebrai fogalmat és tételt.

10.1. Testbővítés

Testen mindig *kommutatív* testet fogunk érteni.

10.1.1 Definíció **D 10.1.1**

Az M testet az L test *bővítés*ének nevezzük, ha L *részteste* M-nek, azaz $L \subseteq M$ és az L testben a műveletek éppen az M-beli műveletek megszorításai. ♣

Ennek a kapcsolatnak a szokásos jelölése $M \mid L$ vagy M/L, de mivel ez könnyen félreérthető, ezért inkább az $M : L$ jelölést fogjuk alkalmazni.

Ha M bővítése L-nek, akkor M egyben vektortér is L felett a „természetesen" adódó műveletekre. Ezek a *vektortér*műveletek az M *test* műveleteiből származnak: két M-beli „*vektor*t" mint az M *test* két elemét adjuk össze, továbbá egy L-beli „*skalár*ral" úgy szorzunk meg egy M-beli „vektort", hogy az M *test*nek ezt a két elemét összeszorozzuk.

Az M-nek mint az L test feletti vektortérnek a *dimenzió*jára külön elnevezést és jelölést vezetünk be:

10.1.2 Definíció **D 10.1.2**

Ha M bővítése L-nek, akkor az M-nek mint L feletti vektortérnek a dimenzióját a testbővítés *fok*ának nevezzük és $\deg(M : L)$-lel jelöljük. Ha ez a dimenzió véges, akkor *véges* (vagy *véges fokú*) bővítésről beszélünk. ♣

Példák: $\deg(\mathbf{C} : \mathbf{R}) = 2$, $\deg(\mathbf{R} : \mathbf{Q}) = \infty$.

Alapvetően fontos tétel, hogy az egymás utáni testbővítések esetén a fokszámok összeszorzódnak:

10.1.3 Tétel (Testbővítések fokszámtétele) **T 10.1.3**

Ha az $L \subseteq M \subseteq N$ bővítéslláncban $\deg(N : M) < \infty$ és $\deg(M : L) < \infty$, akkor

$$\deg(N : L) = \deg(N : M) \cdot \deg(M : L). \ \clubsuit \tag{1}$$

Megjegyezzük, hogy a tétel végtelen dimenzióra is kiterjeszthető: Ha $\deg(N : M)$ és $\deg(M : L)$ közül legalább az egyik végtelen, akkor $\deg(N : L)$ is végtelen, sőt (1) abban a finomabb értelemben is érvényes marad, ha a fokszámot a Hamel-bázis számosságaként tekintjük.

Bizonyítás: Jelöljük L elemeit görög betűkkel, M elemeit latin kisbetűkkel, N elemeit pedig latin nagybetűkkel.

Legyen az $M : L$ vektortér egy bázisa $b_1, \dots, b_n$, az $N : M$ vektortéré pedig $C_1, \dots, C_k$. Megmutatjuk, hogy ekkor a

$$b_i C_j, \qquad i = 1, 2, \dots, n, \qquad j = 1, 2, \dots, k \tag{2}$$

elemek bázist alkotnak az $N : L$ vektortérben, amiből a tétel állítása már következik.

Először azt igazoljuk, hogy a (2)-beli elemek lineárisan függetlenek $N : L$-ben. Tegyük fel, hogy a $\lambda_{ij} \in L$ „skalárokra”

$$\sum_{i=1}^{n} \sum_{j=1}^{k} \lambda_{ij} (b_i C_j) = 0\,. \tag{3}$$

A (3) bal oldalát a(z N) testbeli azonosságok felhasználásával átalakítva azt kapjuk, hogy

$$\sum_{j=1}^{k} \Big(\sum_{i=1}^{n} \lambda_{ij} b_i \Big) C_j = 0\,. \tag{4}$$

Mivel $C_1, \ldots, C_k$ lineárisan független $N : M$-ben, ezért (4)-ből következik, hogy

$$\sum_{i=1}^{n} \lambda_{ij} b_i = 0, \qquad j = 1, \ldots, k. \tag{5}$$

Felhasználva, hogy $b_1, \ldots, b_n$ lineárisan független $M : L$-ben, (5) alapján adódik, hogy mindegyik $\lambda_{ij} = 0$. Ezzel a $b_i C_j$ elemek $N : L$-beli lineáris függetlenségét beláttuk.

Most megmutatjuk, hogy a $b_i C_j$ elemek generátorrendszert alkotnak $N : L$-ben. Mivel $C_1, \ldots, C_k$ generátorrendszer $N : M$-ben, ezért bármely $U \in N$ felírható

$$U = v_1 C_1 + \ldots + v_k C_k \tag{6}$$

alakban, ahol $v_j \in M$. Most felhasználjuk, hogy $b_1, \ldots, b_n$ generátorrendszer $M : L$-ben, és így minden v_j előáll a b_i-k lineáris kombinációjaként:

$$v_j = \alpha_{1j} b_1 + \ldots + \alpha_{nj} b_n, \qquad \alpha_{ij} \in L, \qquad 1 \le i \le n, \qquad 1 \le j \le k. \tag{7}$$

A (7)-beli előállításokat (6)-ba beírva kapjuk, hogy

$$U = \sum_{i=1}^{n} \sum_{j=1}^{k} \alpha_{ij} b_i C_j \,.$$

Ezzel beláttuk, hogy a $b_i C_j$ elemek generátorrendszert alkotnak $N : L$-ben. ■

Most az algebrai szám fogalmát általánosítjuk:

10.1.4 Definíció **D 10.1.4**

Legyen L részteste M-nek. A $\vartheta \in M$ elem *algebrai* az L test felett, ha létezik olyan nemnulla $f \in L[x]$ polinom, amelynek a ϑ gyöke, azaz $f(\vartheta) = 0$. ♣

Példák:

Az algebrai szám fogalmát az $L = \mathbf{Q}$, $M = \mathbf{C}$ speciális esetben kapjuk.

A valós, illetve a komplex test felett minden komplex szám algebrai (lásd a 9.1.7 feladatot).

Az algebrai elem minimálpolinomját és fokát értelemszerűen, a 9.2.1 és 9.2.4 Definíciók mintájára definiáljuk:

10.1.5 Definíció **D 10.1.5**

Legyen L részteste M-nek. Az L felett algebrai $\vartheta \in M$ elem *minimálpolinom*jának a(z egyik) legalacsonyabb fokú $L[x]$-beli polinomot nevezzük, amelynek a ϑ gyöke. A ϑ *fok*a (vagy *fokszám*a) a minimálpolinomjának a foka. ♣

Ne felejtsük el, hogy a ϑ minimálpolinomja és így a foka is nemcsak magától a ϑ-tól függ, hanem attól is, hogy melyik L test felett tekintettük a ϑ-t: például $\sqrt{2}$-nek a $\mathbf{Q}$ feletti minimálpolinomja $x^2 - 2$, az $\mathbf{R}$ feletti minimálpolinomja viszont $x - \sqrt{2}$. (Megmutatható, hogy M változtatása nem befolyásolja ϑ minimálpolinomját.)

Ennek megfelelően a minimálpolinom és a fokszám $m_{\vartheta,L}$, illetve $\deg_L \vartheta$ jelölésében az L testet is feltüntetjük (az algebrai számoknak megfelelő $L = \mathbf{Q}$ esetben továbbra is a sima m_ϑ, illetve $\deg \vartheta$ jelölést használjuk).

Az algebrai elem minimálpolinomjára is érvényesek a 9.2.2 és 9.2.3 Tételeknek megfelelő állítások:

10.1.6 Tétel **T 10.1.6**

Legyen L részteste M-nek, és $\vartheta \in M$ algebrai elem L felett. Ekkor

(i) az $m_{\vartheta,L}$ minimálpolinom egy L-beli konstans szorzótól eltekintve egyértelmű;

(ii) egy $f \in L[x]$ polinomra $f(\vartheta) = 0 \iff m_{\vartheta,L} \mid f$;

(iii) egy $g \in L[x]$ polinom pontosan akkor minimálpolinomja ϑ-nak, ha $g(\vartheta) = 0$ és g irreducibilis L felett. ♣

A bizonyítás pontosan a 9.2.2 és 9.2.3 Tételeknél látott módon történik.

A bővítések szerkezetére vonatkozóan fontos információt tartalmaz az alábbi egyszerű észrevétel:

10.1.7 Tétel **T 10.1.7**

Ha $\deg(M : L) < \infty$, akkor M minden eleme algebrai L felett. ♣

Bizonyítás: Legyen $\deg(M : L) = n$, és jelöljük 1-gyel a(z L és M) test (közös) egységelemét. Ekkor tetszőleges $v \in M$ esetén az $1, v, v^2, \ldots, v^n$ elemek száma nagyobb, mint az $M : L$ vektortér dimenziója, ezért ezek az elemek lineárisan összefüggők. Ez azt jelenti, hogy léteznek olyan $\alpha_0, \ldots, \alpha_n \in L$ „skalárok", amelyek közül nem mindegyik 0, és

$$\alpha_0 + \alpha_1 v + \ldots + \alpha_n v^n = 0.$$

Így v gyöke az $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \neq 0$ polinomnak, vagyis v algebrai elem L felett. ■

Megjegyzések: 1. A bizonyításból az is leolvasható, hogy $\deg_L v \leq \deg(M : L)$. A 10.2.5 Tételben a még erősebb $\deg_L v \mid \deg(M : L)$ állítást fogjuk igazolni.

2. A 10.1.7 Tétel megfordítása nem igaz. Legyen például L a racionális test, M pedig az összes ($\mathbf{Q}$ feletti) algebrai számok teste. Ekkor M minden eleme (definíció szerint) algebrai L felett, azonban $\deg(M : L) = \infty$, ugyanis $\deg(M : L) = n < \infty$ esetén az előző megjegyzés szerint minden algebrai szám foka legfeljebb n lehetne, ami ellentmond annak, hogy létezik akármilyen magas fokszámú algebrai szám (9.2 pont, P4 példa).

Feladatok

10.1.1 Legyen $\deg(M : L)$ prímszám, és tegyük fel, hogy T az M-nek olyan részteste, amely tartalmazza L-et. Mutassuk meg, hogy $T = M$ vagy $T = L$.

10.1.2 Legyen $G = \{a + bi \mid a, b \in \mathbf{Q}\}$ a Gauss-racionálisok, A pedig az algebrai számok teste. Számítsuk ki az alábbi testbővítések fokát:

a) $\deg(G : \mathbf{Q})$; b) $\deg(\mathbf{C} : A)$; c) $\deg(A : G)$.

10.1.3 Legyen $K = \{a+b\sqrt{2} \mid a, b \in \mathbf{Q}\}$. Könnyen adódik, hogy K részteste $\mathbf{R}$-nek.

a) Bizonyítsuk be, hogy egy α komplex szám akkor és csak akkor algebrai K felett, ha algebrai $\mathbf{Q}$ felett (azaz algebrai szám).

b) Határozzuk meg az alábbi komplex számoknak a K feletti fokát:

(b1) $3 + 7\sqrt{2}$; (b2) $\sqrt{2} + i$; (b3) $\sqrt[4]{2}$; (b4) $\sqrt[3]{2}$.

10.1.4 Tekintsük az $L \subseteq M \subseteq N$ bővítésláncot, és legyen $\vartheta \in N$.

a) Melyek igazak az alábbi állítások közül?

(a1) Ha ϑ algebrai L felett, akkor ϑ algebrai M felett.
(a2) Ha ϑ algebrai M felett, akkor ϑ algebrai L felett.

b) Ha ϑ algebrai M és L felett, akkor milyen kapcsolat van $m_{\vartheta,M}$ és $m_{\vartheta,L}$, illetve $\deg_M \vartheta$ és $\deg_L \vartheta$ között?

10.2. Egyszerű algebrai bővítés

A testbővítések legegyszerűbb és egyben legfontosabb típusát az egyetlen elem által generált bővítések jelentik. Ezt a fogalmat az egyszerűség kedvéért csak

a $\mathbf{Q}(\vartheta)$ speciális esetre, azaz a racionális testnek a ϑ komplex számmal történő bővítésére tárgyaljuk, azonban az elmondottak ugyanúgy érvényesek $\mathbf{Q}$ helyett bármilyen L test, illetve $\vartheta \in \mathbf{C}$ helyett $\vartheta \in M$ mellett is, ahol az M test az L-nek tetszőleges bővítése.

A $\mathbf{Q}$-nak a ϑ komplex számmal történő *egyszerű bővítés*én a $\mathbf{Q}$-ból és a ϑ-ból a komplex testbeli műveletek (és inverzeik) segítségével előálló elemek halmazát fogjuk érteni. Ehhez tekintjük az összes $a_0 + a_1\vartheta + \ldots + a_n\vartheta^n$ alakú elemet, ahol n *tetszőleges* nemnegatív egész és az a_i-k racionális számok, majd vesszük ilyenek hányadosait. Az $a_0 + a_1\vartheta + \ldots + a_n\vartheta^n$ elem nem más, mint a $g = a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Q}[x]$ polinomnak a ϑ helyen vett $g(\vartheta) \in \mathbf{C}$ helyettesítési értéke. A szóban forgó hányadosok tehát $g(\vartheta)/h(\vartheta)$ alakú komplex számok, ahol g és h tetszőleges $\mathbf{Q}[x]$-beli polinomok és természetesen $h(\vartheta) \neq 0$. Az ily módon kapott elemek a komplex számtestnek a ϑ-t és $\mathbf{Q}$-t tartalmazó *legszűkebb* résztestét alkotják. Mindezt pontosan az alábbi definícióban és tételben fogalmazzuk meg.

10.2.1 Definíció **D 10.2.1**

Tetszőleges ϑ komplex szám esetén a $\mathbf{Q}$ testnek a ϑ-val történő *egyszerű bővítés*ének nevezzük és $\mathbf{Q}(\vartheta)$-val jelöljük az alábbi alakú komplex számok halmazát:

$$\frac{g(\vartheta)}{h(\vartheta)}\,, \quad \text{ahol} \quad g,\, h \in \mathbf{Q}[x], \quad h(\vartheta) \neq 0\,, \tag{1}$$

illetve ugyanezt részletesen kiírva:

$$\frac{\sum_{i=0}^{n} a_i\vartheta^i}{\sum_{j=0}^{k} b_j\vartheta^j}\,, \quad \text{ahol} \quad a_i,\, b_j \in \mathbf{Q}, \quad \sum_{j=0}^{k} b_j\vartheta^j \neq 0, \quad n,\, k = 0,\, 1,\, 2,\, \ldots \tag{2}$$

Ha ϑ algebrai szám, akkor *egyszerű algebrai bővítés*ről beszélünk. ♣

10.2.2 Tétel **T 10.2.2**

$\mathbf{Q}(\vartheta)$ a komplex testnek az a *legszűkebb* részteste, amely a ϑ-t és a racionális testet tartalmazza, azaz

(i) $\mathbf{Q}(\vartheta)$ résztest $\mathbf{C}$-ben;

(ii) $\vartheta \in \mathbf{Q}(\vartheta)$, $\mathbf{Q} \subseteq \mathbf{Q}(\vartheta)$;

(iii) ha T részteste $\mathbf{C}$-nek és $\vartheta \in T$, $\mathbf{Q} \subseteq T$, akkor szükségképpen $\mathbf{Q}(\vartheta) \subseteq T$.

♣

Bizonyítás: (i) Azt kell megmutatni, hogy két (1)-beli elem összege, különbsége, szorzata és (ha a nevező nem nulla, akkor) hányadosa is (1)-beli. Nyilván

$$\frac{g_1(\vartheta)}{h_1(\vartheta)} + \frac{g_2(\vartheta)}{h_2(\vartheta)} = \frac{g(\vartheta)}{h(\vartheta)}\,,$$

ahol $g = g_1h_2 + g_2h_1$ és $h = h_1h_2$ is racionális együtthatós polinomok, és a komplex test nullosztómentessége miatt $h(\vartheta) = h_1(\vartheta)h_2(\vartheta) \neq 0$. A különbségre, szorzatra és hányadosra vonatkozó állítás hasonlóan igazolható.

(ii) Ha $g = x$ és $h = 1$, akkor $g(\vartheta)/h(\vartheta) = \vartheta$, tehát $\vartheta \in \mathbf{Q}(\vartheta)$.

Ha r tetszőleges racionális szám, akkor a $g = r$ és $h = 1$ (konstans) polinomokat választva $g(\vartheta)/h(\vartheta) = r$, tehát $r \in \mathbf{Q}(\vartheta)$.

(iii) Ha T a komplex számok olyan részteste, amely tartalmazza ϑ-t és $\mathbf{Q}$-t, akkor a ϑ-ból és racionális számokból képzett tetszőleges szorzatok összege és ilyenek hányadosa is szükségképpen T-beli. Ez azt jelenti, hogy minden (2)-beli komplex szám is eleme T-nek, tehát valóban $\mathbf{Q}(\vartheta) \subseteq T$. ■

Megmutatjuk, hogy ha ϑ algebrai szám, akkor $\mathbf{Q}(\vartheta)$ elemei egyszerűbb alakban is felírhatók.

Tekintsük először példaként a racionális testnek a $\sqrt{2}$-vel vett $\mathbf{Q}(\sqrt{2})$ bővítését. Ez nem más, mint az $a_0 + a_1\sqrt{2}$ alakú számok T halmaza, ahol $a_i \in \mathbf{Q}$, ugyanis T egy olyan test, amely a $\sqrt{2}$-t és a racionális számokat tartalmazza és nyilván a legszűkebb. Ez azt jelenti, hogy a 10.2.1 Definícióban felírt alakhoz képest nincs szükség osztásra és a $\sqrt{2}$-nek az egynél magasabb kitevőjű hatványaira.

Ha a $\sqrt{2}$ helyett a $\sqrt[3]{5}$-tel történő $\mathbf{Q}(\sqrt[3]{5})$ bővítést tekintjük, akkor itt $\sqrt[3]{5}$ legfeljebb második hatványaira van szükség, mert a harmadik és magasabb hatványok kifejezhetők ezekkel (és alkalmas racionális számokkal).

Az általános esetben a következő tétel érvényes:

10.2.3 Tétel **T 10.2.3**

Ha ϑ egy n-edfokú algebrai szám, akkor $\mathbf{Q}(\vartheta)$ elemei *egyértelműen* felírhatók

$$a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}$$

alakban, ahol az a_i-k racionális számok. Más szóval, minden $\alpha \in \mathbf{Q}(\vartheta)$ elemhez pontosan egy olyan $f \in \mathbf{Q}[x]$ polinom létezik, amelyre

$$\alpha = f(\vartheta) \qquad \text{és} \qquad \deg f \leq n-1 \text{ vagy } f = 0. \ \clubsuit$$

Bizonyítás: I. Először megmutatjuk, hogy (1)-ben a nevezőre „nincs szükség", azaz bármely $g, h \in \mathbf{Q}[x]$ és $h(\vartheta) \neq 0$ esetén $g(\vartheta)/h(\vartheta)$ előáll alkalmas $t \in \mathbf{Q}[x]$ polinommal $t(\vartheta)$ alakban is.

Ennek igazolásához tekintsük az alábbi ekvivalenciákat (ahol közben a $h(\vartheta) \neq 0$ feltételt és a 9.2.3(i) Tételt is felhasználjuk):

$$g(\vartheta)/h(\vartheta) = t(\vartheta) \iff g(\vartheta) = h(\vartheta)t(\vartheta) \iff (g - ht)(\vartheta) = 0 \iff$$
$$\iff m_\vartheta \mid g - ht \iff g = ht + m_\vartheta s, \quad \text{ahol} \quad s \in \mathbf{Q}[x].$$

Így azt kell belátni, hogy léteznek olyan t és s racionális együtthatós polinomok, amelyekre

$$g = ht + m_\vartheta s. \tag{3}$$

A (3) egyenlőség „olyan", mint egy lineáris diofantikus egyenlet, amelyben t és s az ismeretlenek, csak itt egész számok helyett racionális együtthatós polinomok szerepelnek. A lineáris diofantikus egyenletek megoldhatóságának szükséges és elégséges feltételét az 1.3.6 Tételben tárgyaltuk, és a bizonyításnál csak a maradékos osztásból adódó euklideszi algoritmus egyik következményét használtuk fel. Mivel a maradékos osztás a test feletti polinomok körében is elvégezhető, ezért a „polinomos" diofantikus egyenlet megoldhatóságának is ugyanaz a feltétele. Így a (3) egyenlet megoldhatóságához azt kell igazolni, hogy $(h, m_\vartheta) \mid g$.

Az m_ϑ polinom irreducibilis $\mathbf{Q}$ felett, ezért $(h, m_\vartheta) = 1$ vagy m_ϑ. Az utóbbi esetből azonban $h(\vartheta) = 0$ következne, így csak $(h, m_\vartheta) = 1$ lehetséges, tehát valóban $(h, m_\vartheta) \mid g$. Ez, mint láttuk, azt jelenti, hogy a (3) egyenlet megoldható, és az így kapott t polinomra $t(\vartheta) = g(\vartheta)/h(\vartheta)$.

II. Eddig azt igazoltuk, hogy minden $\alpha \in \mathbf{Q}(\vartheta)$ alkalmas $t \in \mathbf{Q}[x]$ polinommal $\alpha = t(\vartheta)$ alakba írható. Most megmutatjuk, hogy olyan $f \in \mathbf{Q}[x]$ polinom is létezik, amelyre $\deg f \leq n - 1$ vagy $f = 0$, és $\alpha = f(\vartheta)$.

Osszuk el a t polinomot maradékosan m_ϑ-val, ekkor a maradék megfelel f-nek. Valóban, ha

$$t = qm_\vartheta + f, \qquad \text{ahol} \qquad \deg f \leq n - 1 \qquad \text{vagy} \qquad f = 0,$$

akkor

$$\alpha = t(\vartheta) = q(\vartheta)m_\vartheta(\vartheta) + f(\vartheta) = 0 + f(\vartheta) = f(\vartheta).$$

III. Hátravan még f egyértelműségének az igazolása. Tegyük fel, hogy az f_1 és f_2 racionális együtthatós polinomkra

$$f_1(\vartheta) = f_2(\vartheta) \qquad \text{és} \qquad \deg f_i \leq n - 1 \quad \text{vagy} \quad f_i = 0, \qquad i = 1, 2.$$

Ekkor az $f_3 = f_1 - f_2$ polinom racionális együtthatós, $f_3(\vartheta) = 0$ és $\deg f_3 < n$ vagy $f_3 = 0$. Mivel $\deg \vartheta = n$, ezért csak $f_3 = 0$ lehetséges. Ez azt jelenti, hogy $f_1 = f_2$, tehát a tételben szereplő f polinom egyértelmű. ■

A 10.2.3 Tétel más megfogalmazásban azt jelenti, hogy az $1, \vartheta, \dots, \vartheta^{n-1}$ elemek bázist alkotnak $\mathbf{Q}(\vartheta)$-ban mint $\mathbf{Q}$ feletti vektortérben. Így ennek a vektortérnek a dimenziója, azaz az $\mathbf{Q}(\vartheta) : \mathbf{Q}$ testbővítés foka megegyezik a ϑ algebrai szám fokával. Ezt a fontos tényt külön tételként is kimondjuk:

10.2.4 Tétel **T 10.2.4**

Ha ϑ algebrai szám, akkor $\deg\big(\mathbf{Q}(\vartheta) : \mathbf{Q}\big) = \deg \vartheta$. ♣

A 10.2.3–10.2.4 Tételeket kiegészíthetjük azzal, hogy ha ϑ transzcendens szám, akkor $\mathbf{Q}(\vartheta)$ elemei *nem* adhatók meg a 10.2.1 Definícióban leírtnál egyszerűbb alakban, és a $\mathbf{Q}(\vartheta) : \mathbf{Q}$ bővítés foka ekkor *végtelen*. Ebben az esetben a $\mathbf{Q}(\vartheta)$ test a $\mathbf{Q}$ feletti *algebrai törtek*, azaz a racionális együtthatós polinomok formálisan képzett hányadosainak testével izomorf (lásd a 10.2.13 feladatot).

Megjegyezzük még, hogy ha ϑ algebrai szám, akkor a 10.2.3 Tétel alapján $\mathbf{Q}(\vartheta)$ elemeit az m_ϑ polinom szerinti osztási maradékokként képzelhetjük el: ilyenkor a $\mathbf{Q}(\vartheta)$ test a $\mathbf{Q}[x]/(m_\vartheta)$ *faktorgyűrű*vel izomorf (lásd a 11.1.6 Tételt és a 11.1.9a feladatot). Az egyszerű algebrai bővítéseknek ez a megközelítési módja a $\mathbf{Q}$ helyett tetszőleges L test esetén azt is lehetővé teszi, hogy „akkor is megkonstruáljuk $L(\vartheta)$-t, ha nincs eleve adva egy L-nél bővebb M test és abban egy ϑ elem”, lásd a 11.1.9b feladatot.

Végül megemlítjük, hogy a $\mathbf{Q}$ bármely véges bővítése előáll alkalmas ϑ algebrai számmal $\mathbf{Q}(\vartheta)$ alakban, azaz $\mathbf{Q}$ véges bővítései megegyeznek a $\mathbf{Q}$ egyszerű algebrai bővítéseivel. (Ugyanez fennáll $\mathbf{Q}$ helyett bármely olyan testre is, amelyben egy $a + a + \ldots + a$ összeg csak úgy lehet 0, ha $a = 0$.)

A 10.1.7 Tétel élesítéseként most megmutatjuk, hogy egy véges bővítés tetszőleges elemének a foka osztója a bővítés fokának. Az állítást most is csak a $\mathbf{Q}$ bővítéseire fogalmazzuk meg, de ugyanúgy érvényes tetszőleges (kommutatív) testekre is.

10.2.5 Tétel **T 10.2.5**

Ha M részteste $\mathbf{C}$-nek és $\deg(M : \mathbf{Q}) = k < \infty$, akkor bármely $\alpha \in M$ elemre $\deg \alpha \mid k$. ♣

Bizonyítás: A $\mathbf{Q}(\alpha)$ test a 10.2.2 Tétel szerint része M-nek, azaz

$$\mathbf{Q} \subseteq \mathbf{Q}(\alpha) \subseteq M. \tag{4}$$

A $\deg(M : \mathbf{Q}) = k < \infty$ feltételből következik, hogy a (4) bővítéslánc mindkét „láncszeme" is véges bővítés, és így alkalmazhatjuk a fokszámtételt (10.1.3 Tétel). Ebből azt kapjuk, hogy $\deg(\mathbf{Q}(\alpha) : \mathbf{Q}) \mid k$. A 10.1.7 Tétel alapján α algebrai szám, ezért a 10.2.4 Tétel miatt $\deg(\mathbf{Q}(\alpha) : \mathbf{Q}) = \deg \alpha$. Vagyis valóban $\deg \alpha \mid k$. ■

Most új bizonyítást adunk a 9.3.1 és 9.3.6 Tételekre. A könnyebb áttekinthetőség kedvéért ezeket a tételeket (új sorszámmal) újra ki is mondjuk.

10.2.6 Tétel **T 10.2.6**

Az algebrai számok résztestet alkotnak a komplex számtestben. ♣

Bizonyítás: Legyen α és β két algebrai szám. Azt kell megmutatni, hogy $\alpha+\beta$, $\alpha - \beta$, $\alpha\beta$ és (ha $\beta \neq 0$, akkor) α/β is algebrai.

Bővítsük $\mathbf{Q}$-t α-val, majd az így kapott $K = \mathbf{Q}(\alpha)$ testet β-val. Az ekkor keletkező $N = K(\beta)$ test tartalmazza α-t és β-t is, ezért a két szám összege, különbsége, szorzata és hányadosa is N-beli.

Tekintsük a $\mathbf{Q} \subseteq K \subseteq N$ bővítésláncot [ahol $K = \mathbf{Q}(\alpha)$ és $N = K(\beta)$]. Itt

$$\deg(K : \mathbf{Q}) = \deg \alpha \qquad \text{és} \qquad \deg(N : K) = \deg_K \beta \leq \deg \beta,$$

ezért a fokszámtétel szerint $\deg(N : K) < \infty$. Ebből a 10.1.7 Tétel alapján következik, hogy N minden eleme, így speciálisan $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ és α/β is algebrai szám. ■

10.2.7 Tétel **T 10.2.7**

Ha az $f \neq 0$ polinom együtthatói algebrai számok, akkor f minden (komplex) gyöke algebrai szám. ♣

Bizonyítás: Legyen $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ és γ az f tetszőleges komplex gyöke.

Definiáljuk a K_i testeket a következőképpen:

$$K_0 = \mathbf{Q}(\alpha_0), \qquad K_j = K_{j-1}(\alpha_j), \qquad j = 1, 2, \ldots, n, \qquad K_{n+1} = K_n(\gamma)\,,$$

és tekintsük a

$$\mathbf{Q} \subseteq K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq K_{n+1}$$

bővítésláncot. Itt minden lépésben az adott testet egy felette algebrai elemmel bővítjük, ezért minden „láncszem" véges bővítés. Ekkor a fokszámtétel miatt $K_{n+1} : \mathbf{Q}$ is véges bővítés, tehát K_{n+1} minden eleme, köztük γ is algebrai $\mathbf{Q}$ felett. ■

Feladatok

10.2.1 Bizonyítsuk be, hogy bármely ϑ komplex és $r \neq 0$ racionális számra az alábbi bővítések megegyeznek $\mathbf{Q}(\vartheta)$-val:

a) $\mathbf{Q}(r+\vartheta)$; b) $\mathbf{Q}(r\vartheta)$; c) $\mathbf{Q}(1/\vartheta)$ (ha $\vartheta \neq 0$).

10.2.2 Legyen $\alpha \in \mathbf{Q}(\vartheta)$. Bizonyítsuk be az alábbi állításokat.

a) $\mathbf{Q}(\alpha) \subseteq \mathbf{Q}(\vartheta)$.

b) Algebrai ϑ esetén $\mathbf{Q}(\alpha) = \mathbf{Q}(\vartheta) \iff \deg \alpha = \deg \vartheta$.

*c) Transzcendens ϑ esetén $\mathbf{Q}(\alpha) = \mathbf{Q}(\vartheta)$ akkor és csak akkor teljesül, ha

$$\alpha = \frac{a_0 + a_1\vartheta}{b_0 + b_1\vartheta}, \quad \text{ahol} \quad a_i,\, b_i \in \mathbf{Q} \quad \text{és} \quad \alpha \notin \mathbf{Q}.$$

10.2.3 Melyek igazak az alábbi állítások közül?

a) $\mathbf{Q}(\vartheta) = \mathbf{Q}(\overline{\vartheta})$.

b) Ha $|\vartheta|^2$ racionális, akkor $\mathbf{Q}(\vartheta) = \mathbf{Q}(\overline{\vartheta})$.

c) Ha $\mathbf{Q}(\vartheta) = \mathbf{Q}(\overline{\vartheta})$, akkor $|\vartheta|^2$ racionális.

d) Ha $\mathbf{Q}(\vartheta) \subseteq \mathbf{Q}(\overline{\vartheta})$, akkor $\mathbf{Q}(\vartheta) = \mathbf{Q}(\overline{\vartheta})$.

e) $\mathbf{Q}(\vartheta) = \mathbf{Q}(\vartheta + \vartheta^2)$.

10.2.4 Írjuk fel az alábbi számokat $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ alakban, ahol a_0, a_1, a_2 racionális számok:

a) $(\sqrt[3]{4} + 3\sqrt[3]{2})^2$; b) $\dfrac{1}{\sqrt[3]{2}}$; c) $\dfrac{1+\sqrt[3]{2}}{1+2\sqrt[3]{2}}$.

10.2.5 Számítsuk ki az alábbi algebrai számok fokát:

M a) $\sqrt{7} + 3i$; b) $i\sqrt[5]{3}$;

c) $\sqrt[7]{3} + \sqrt[7]{1/3}$; d) $\sqrt[4]{2} + \sqrt{2}$.

10.2.6 Adjuk meg egyszerűbb alakban az alábbi halmazokat:

a) $\mathbf{Q}(\sqrt[3]{54}) \setminus \mathbf{Q}(\sqrt[3]{16})$; b) $\mathbf{Q}(\sqrt[6]{7}) \cap \mathbf{Q}(\sqrt[9]{7})$; c) $\mathbf{Q}(\sqrt[4]{5}) \cap \mathbf{Q}(i\sqrt[4]{5})$.

M 10.2.7 Adjuk meg $\mathbf{Q}(\vartheta)$ valós elemeit, ha ϑ értéke

a) $\sqrt[5]{3}(\cos 144^\circ + i \sin 144^\circ)$;

b) $i\sqrt[6]{3}$;

c) $\sqrt{i}$ valamelyik értéke.

M*10.2.8 Bizonyítsuk be, hogy ha $|\vartheta| = 1$, akkor $\mathbf{Q}(\vartheta) \cap \mathbf{R} = \mathbf{Q}(\operatorname{Re}\vartheta)$.

10.2.9 Legyen $\alpha = 1 + 3\sqrt[7]{25} + 11\sqrt[7]{125} + 999\sqrt[7]{625}$. Bizonyítsuk be, hogy létezik olyan f racionális együtthatós polinom, amelyre $f(\alpha) = \sqrt[7]{5}$.

10.2.10 Legyen a β algebrai szám foka k. Melyek $\deg(\beta^2)$ lehetséges értékei?

M*10.2.11 Határozzuk meg az egységkörön az összes páratlan fokú algebrai számot.

10.2.12

a) Bizonyítsuk be, hogy ha α és β algebrai számok, akkor az $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$ és ($\beta \neq 0$ esetén) α/β számok foka kisebb vagy egyenlő, mint $(\deg\alpha) \cdot (\deg\beta)$.

b) Ha az $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ polinom együtthatói algebrai számok és $f(\gamma) = 0$, akkor $\deg\gamma \leq n \prod_{j=0}^{n} \deg\alpha_j$.

10.2.13 Legyenek $g_1, g_2, h_1 \neq 0, h_2 \neq 0$ racionális együtthatós polinomok és ϑ transzcendens szám. Bizonyítsuk be az alábbi állításokat.

a) $\dfrac{g_1(\vartheta)}{h_1(\vartheta)} = \dfrac{g_2(\vartheta)}{h_2(\vartheta)} \iff g_1 h_2 = g_2 h_1$.

b) A $\mathbf{Q}(\vartheta)$ test izomorf a $\mathbf{Q}$ feletti *algebrai törtek*, azaz a racionális együtthatós polinomok formálisan képzett hányadosainak testével.

10.3. Másodfokú bővítések

Ebben a pontban a $\mathbf{Q}$-nak a (komplex számtesten belüli) másodfokú bővítéseit és azok algebrai egészeit vizsgáljuk.

10.3.1 Tétel **T 10.3.1**

A $\mathbf{Q}$ összes másodfokú bővítése $\mathbf{Q}(\sqrt{t})$ alakú, ahol t (pozitív vagy negatív) négyzetmentes egész szám és $t \neq 1$. Különböző ilyen t értékekhez különböző bővítések tartoznak. ♣

Megjegyzés: A $t > 0$ esetben valós, a $t < 0$ esetben pedig képzetes (vagy imaginárius) másodfokú bővítésről beszélünk. A képzetes esetben $\sqrt{t}$ két

(komplex) értéke közül bármelyiket vehetjük, mert ezek egymás ellentettjei és $\mathbf{Q}(\vartheta) = \mathbf{Q}(-\vartheta)$ bármely ϑ-ra teljesül; a továbbiakban ilyenkor jelentse $\sqrt{t}$ mindig a négyzetgyök felső félsíkbeli értékét: $\sqrt{t} = i\sqrt{|t|}$.

Bizonyítás: Legyen M a $\mathbf{C}$ olyan részteste, amelyre $\deg(M : \mathbf{Q}) = 2$. Ekkor nyilván az M tetszőleges α nem racionális elemére $\deg \alpha = 2$ és $M = \mathbf{Q}(\alpha)$. Belátjuk, hogy $\mathbf{Q}(\alpha)$ megadható alkalmas négyzetmentes $t \neq 1$-gyel $\mathbf{Q}(\sqrt{t})$ alakban is.

Ha az α minimálpolinomja $m_\alpha = a_0 + a_1 x + a_2 x^2$, ahol a_0, a_1, a_2 egész számok, akkor a másodfokú egyenlet megoldóképletéből kapjuk, hogy $\alpha = r_0 + r_1\sqrt{s}$ alakú, ahol $r_1 \neq 0$ és r_0 racionális számok és $s \neq 0$ egész szám. Az s-ből a lehető legnagyobb négyzetszámot kiemelve $s = k^2 t$ adódik, ahol t négyzetmentes és $t \neq 1$. Így $\alpha = r_0 + r_1 k\sqrt{t}$. Innen a 10.2.1 feladat alapján következik, hogy $M = \mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{t})$.

Meg kell még mutatnunk, hogy az így kapott t egyértelmű, azaz ha $\mathbf{Q}(\sqrt{t_1}) = \mathbf{Q}(\sqrt{t_2})$, ahol t_j négyzetmentes és $t_j \neq 1$, akkor $t_1 = t_2$.

A feltételekből következik, hogy

$$\sqrt{t_2} \in \mathbf{Q}(\sqrt{t_1}), \qquad \text{azaz} \qquad \sqrt{t_2} = a + b\sqrt{t_1},$$

ahol a és b racionális. Négyzetre emeléssel

$$t_2 = a^2 + t_1 b^2 + 2ab\sqrt{t_1}$$

adódik. Ez $\sqrt{t_1}$ irracionalitása miatt csak úgy lehetséges, ha $b = 0$ vagy $a = 0$. Az első eset azt jelenti, hogy $\sqrt{t_2}$ racionális, ami ellentmondás. A második esetben azt kapjuk, hogy $\sqrt{t_2}/\sqrt{t_1}$ racionális, amiből t_j négyzetmentessége miatt $t_1 = t_2$ következik. ■

Példák:

P1 A Gauss-racionálisok a $\mathbf{Q}(i)$ bővítés elemei, ekkor $t = -1$.

P2 Az Euler-racionálisok a $\mathbf{Q}(\omega)$ bővítés elemei, ahol

$$\omega = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = \frac{-1 + i\sqrt{3}}{2}\,.$$

Ekkor $t = -3$.

Most megvizsgáljuk, hogyan adhatók meg egy másodfokú bővítés algebrai egészei.

Tekintsük először a Gauss-racionálisokat, tehát azokat az $a+bi$ komplex számokat, ahol a és b racionális. A 9.6 pontban már említettük (P3 példa, 9.6.3a és 9.6.3f feladat), hogy egy Gauss-racionális pontosan akkor algebrai egész, ha Gauss-egész, azaz ha a és b egész szám.

Nézzük meg, mi a helyzet az Euler-racionálisoknál, azaz az

$$\alpha = c + d\omega = c + d\frac{-1+i\sqrt{3}}{2} = \frac{2c-d}{2} + \frac{d}{2}\sqrt{-3} = a + b\sqrt{-3} \quad (a,b,c,d \in \mathbf{Q}) \tag{1}$$

alakú számoknál. A 9.6 pont P3 példájában jeleztük, hogy egy Euler-racionális akkor és csak akkor algebrai egész, ha Euler-egész. Ez azt jelenti, hogy az (1)-beli α Euler-racionális pontosan akkor algebrai egész, ha c és d egész szám, azaz ha a és b mindketten egész számok, vagy pedig mindketten olyan 2 nevezőjű törtek, amelyek számlálója páratlan szám.

A fentiek mutatják, hogy a $t=-1$, illetve $t=-3$ esetekben kapott eredmény kissé eltérő jellegű. Az általános esetben is kétféle lehetőség adódik, attól függően, hogy a bővítést jellemző t milyen maradékot ad 4-gyel osztva:

10.3.2 Tétel **T 10.3.2**

Legyen $t \neq 1$ négyzetmentes szám. Ekkor a $\mathbf{Q}(\sqrt{t})$ bővítés algebrai egészei éppen a $c + d\vartheta$ alakú számok, ahol c és d egész szám és

$$\vartheta = \begin{cases} \sqrt{t}, & \text{ha } t \not\equiv 1 \pmod 4; \\ (1+\sqrt{t})/2, & \text{ha } t \equiv 1 \pmod 4. \end{cases}$$

Más megfogalmazásban ez azt jelenti, hogy $\mathbf{Q}(\sqrt{t})$-ben egy $a+b\sqrt{t}$ $(a,b \in \mathbf{Q})$ elem akkor és csak akkor algebrai egész, ha

a) $t \not\equiv 1 \pmod 4$ esetén a és b egész számok;
b) $t \equiv 1 \pmod 4$ esetén $a = u/2$, $b = v/2$, ahol u és v azonos paritású egészek. ♣

A tétel kétféle megfogalmazása nyilván ekvivalens.

A Gauss-, illetve Euler-egészekre kapott eredmény ennek a tételnek a $t = -1 \not\equiv 1 \pmod 4$, illetve $t = -3 \equiv 1 \pmod 4$ speciális esete.

Bizonyítás: Mivel egy racionális szám akkor és csak akkor algebrai egész, ha egész szám, ezért a tétel állítása a $\mathbf{Q}(\sqrt{t})$ bővítés racionális elemeire azonnal adódik.

A továbbiakban így elég a bővítés nem racionális elemeivel foglalkozni. Tetszőleges ilyen $\alpha \in \mathbf{Q}(\sqrt{t})$ egyértelműen felírható $\alpha = r_0 + r_1\sqrt{t}$ alakban,

ahol $r_1 \neq 0$ és r_0 racionális számok. Közös nevezőre hozva kapjuk, hogy

$$\alpha = \frac{a + b\sqrt{t}}{c}\,, \quad \text{ahol} \quad a, b, c \text{ egészek, } (a, b, c) = 1,\ c > 0,\ b \neq 0. \tag{2}$$

Az

$$\alpha - \frac{a}{c} = \frac{b\sqrt{t}}{c}$$

egyenlőséget négyzetre emelve

$$\alpha^2 - \frac{2a}{c}\alpha + \frac{a^2 - tb^2}{c^2} = 0 \tag{3}$$

adódik. Mivel $\deg \alpha = 2$, ezért (3) alapján α minimálpolinomja

$$m_\alpha = x^2 - \frac{2a}{c}x + \frac{a^2 - tb^2}{c^2}\,. \tag{4}$$

Így α pontosan akkor algebrai egész, ha a (4)-beli minimálpolinom egész együtthatós, azaz

$$c \mid 2a \qquad \text{és} \qquad c^2 \mid a^2 - tb^2\,. \tag{5}$$

Azt kell belátnunk, hogy (5) pontosan akkor teljesül, ha

a) $t \not\equiv 1 \pmod 4$ esetén $c = 1$; (6a)

b) $t \equiv 1 \pmod 4$ esetén $c = 2$ és a, b páratlan, vagy $c = 1$. (6b)

Először tegyük fel, hogy c páratlan. Ekkor (5)-ben az első oszthatóságból $c \mid a$ következik, és így $c^2 \mid a^2 - (a^2 - tb^2) = tb^2$. Mivel t négyzetmentes, a számelmélet alaptétele szerint $c^2 \mid b^2$, tehát $c \mid b$. Ezért $c \mid (a, b, c) = 1$, azaz $c = 1$. Megfordítva, $c = 1$ esetén (5) nyilván teljesül bármely t, a és b egész számokra.

Legyen most c páros, $c = 2k$. Ekkor (5)-ben az első oszthatóságból $k \mid a$ következik, és így $k^2 \mid a^2 - (a^2 - tb^2) = tb^2$. A páratlan esethez hasonlóan kapjuk, hogy $k \mid b$, ezért $k \mid (a, b, c) = 1$, azaz $k = 1$, tehát $c = 2$. Ennek megfelelően (5)-ben a második oszthatóság átírható

$$a^2 - tb^2 \equiv 0 \pmod 4 \tag{7}$$

alakba. Itt a és b közül legalább az egyik páratlan, mivel $(a, b, c) = 1$, továbbá t négyzetmentessége miatt $t \not\equiv 0 \pmod 4$. Egy négyzetszám csak 0 vagy

1 maradékot adhat 4-gyel osztva, így a fentiek mellett (7) pontosan akkor teljesül, ha a és b mindketten páratlanok és $t \equiv 1 \pmod 4$.

Ezzel beláttuk, hogy az (5) és (6a)–(6b) feltételek ekvivalensek. ■

Jelöljük a $\mathbf{Q}(\sqrt{t})$ bővítés algebrai egészeinek halmazát $E(\sqrt{t})$-vel. A 10.3.2 Tétel szerint tehát

$$E(\sqrt{t}) = \{c + d\sqrt{t} \mid c, d \in \mathbf{Z}\}, \qquad \text{ha } t \not\equiv 1 \pmod 4; \tag{8a}$$

illetve

$$E(\sqrt{t}) = \Big\{c + d\frac{1+\sqrt{t}}{2} \mid c, d \in \mathbf{Z}\Big\}, \text{ ha } t \equiv 1 \pmod 4. \tag{8b}$$

Mivel $E(\sqrt{t})$ az algebrai egészek gyűrűjének és a $\mathbf{Q}(\sqrt{t})$ testnek a metszete, ezért $E(\sqrt{t})$ részgyűrű a komplex számtestben. Ez a gyűrű kommutatív, egységelemes és nullosztómentes, továbbá nem test, hiszen például a racionális számok közül csak az egészeket tartalmazza. Mindezek alapján — a Gauss-egészek és Euler-egészek mintájára — érdemes $E(\sqrt{t})$-ben is megvizsgálni néhány alapvető számelméleti kérdést.

Az oszthatóság, egység, legnagyobb közös osztó, felbonthatatlan és prím fogalmát $E(\sqrt{t})$-ben pontosan ugyanúgy definiáljuk, mint a Gauss-egészeknél (lásd a 7.4.4, 7.4.6, 7.4.9, 7.4.10 és 7.4.11 Definíciókat, a „Gauss-” jelzőt most természetesen elhagyjuk).

A számelméleti vizsgálatoknál $E(\sqrt{t})$-ben is kulcsszerepet játszik a norma fogalma:

10.3.3 Definíció **D 10.3.3**

Az $\alpha = a + b\sqrt{t} \in E(\sqrt{t})$ elem *normája*

$$N(\alpha) = a^2 - tb^2 = (a - b\sqrt{t})(a + b\sqrt{t})\,. \ \clubsuit$$

A 10.3.2 Tételből következik, hogy minden $\alpha \in E(\sqrt{t})$ elem normája egész szám.

Az is azonnal adódik, hogy a normára vonatkozó 7.4.3 és 7.4.5 Tételek $t < 0$ esetén bármely $E(\sqrt{t})$-ben érvényesek, és a $t > 0$ esetben is csak annyi a változás, hogy $N(\alpha)$ negatív egész is lehet (továbbá ha $t > 0$ és α nem racionális, akkor $N(\alpha)$ nem az α abszolút értékének a négyzetét jelenti).

Az egységekre vonatkozó 7.4.7, illetve 7.7.6 Tétel a következőképpen módosul:

10.3.4 Tétel **T 10.3.4**

(A) Egy $\varepsilon \in E(\sqrt{t})$ elemre az alábbi feltételek ekvivalensek:

(i) ε egység.

(ii) $\varepsilon \mid 1$.

(iii) $|N(\varepsilon)| = 1$.

(B) Ha $t > 0$, akkor $E(\sqrt{t})$-ben végtelen sok egység van.

(C) Ha $t < 0$ és $t \neq -1,\ -3$, akkor $E(\sqrt{t})$-ben az összes egység a ± 1. ♣

Bizonyítás: (A): (i) $\Longrightarrow$ (ii): Ha ε minden $E(\sqrt{t})$-beli elemnek osztója, akkor speciálisan az 1-nek is osztója.

(ii) $\Longrightarrow$ (i): Ha $\varepsilon \mid 1$, vagyis van olyan $\beta \in E(\sqrt{t})$, amelyre $\varepsilon\beta = 1$, akkor tetszőleges $\alpha \in E(\sqrt{t})$-re $\varepsilon(\beta\alpha) = \alpha$, azaz $\varepsilon \mid \alpha$, tehát ε egység.

(ii) $\Longrightarrow$ (iii): Ha $\varepsilon \mid 1$, akkor $N(\varepsilon) \mid N(1) = 1$, tehát $N(\varepsilon) = \pm 1$.

(iii) $\Longrightarrow$ (ii): Ha $\varepsilon = a + b\sqrt{t}$ és

$$N(\varepsilon) = (a + b\sqrt{t})(a - b\sqrt{t}) = \pm 1,$$

akkor $a - b\sqrt{t} \in E(\sqrt{t})$ miatt $\varepsilon \mid 1$.

(B) Ha $t > 0$, akkor az $x^2 - ty^2 = 1$ Pell-egyenletnek végtelen sok x, y egész megoldása van (7.8.1 Tétel), és az ezeknek megfelelő $\alpha = x + y\sqrt{t} \in E(\sqrt{t})$ elemekre $N(\alpha) = 1$, tehát ezek valamennyien egységek.

(C) Ha $t < 0$, $t \not\equiv 1 \pmod 4$, akkor $E(\sqrt{t})$ elemei $\alpha = a + b\sqrt{t}$ alakúak, ahol a, b egész, és így $t \neq -1$ esetén

$$N(\alpha) = a^2 + |t|b^2 = 1$$

csak úgy teljesülhet, ha $b = 0$ és $a = \pm 1$, azaz $\alpha = \pm 1$.

A $t < 0$, $t \equiv 1 \pmod 4$ esetben α még $(u/2) + (v/2)\sqrt{t}$ alakú is lehet, ahol u és v páratlan egész. Ekkor

$$N(\alpha) = \frac{u^2 + |t|v^2}{4} = 1, \qquad \text{azaz} \qquad u^2 + |t|v^2 = 4 \tag{9}$$

fennállását vizsgáljuk. Ha $|t| > 3$ és u, v páratlan, akkor

$$u^2 + |t|v^2 > 1 + 3 \cdot 1 = 4,$$

tehát (9) nem teljesülhet. ■

Megjegyzések: 1. A 10.3.4 Tétel (A)/(iii) feltétele számos t-re csak a $N(\varepsilon) = 1$ lehetőséget jelenti, mert $N(\varepsilon) = -1$ nem fordulhat elő. Ez a helyzet bármely $t < 0$ esetén, hiszen ekkor nyilván minden elem normája nemnegatív. Azonban ilyen például minden olyan pozitív t is, amelyre $t \equiv 3 \pmod 4$, hiszen ekkor $E(\sqrt{t})$ tetszőleges $\alpha = a + b\sqrt{t}$ elemére (a, b egész, és) $N(\alpha) = a^2 - tb^2 \not\equiv -1 \pmod 4$.

2. A 10.3.4 Tétel (B) részét kiegészíthetjük azzal, hogy a $t > 0$ esetben $E(\sqrt{t})$ összes egységeit az $x^2 - ty^2 = \pm 1$ egyenlet egész, illetve ha $t \equiv 1 \pmod 4$, akkor ezeken kívül az $x^2 - ty^2 = \pm 4$ egyenlet páratlan megoldásaiból adódó $x + y\sqrt{t}$ elemek szolgáltatják. Ezeknek az áttekintése a 7.8.2 Tétel felhasználásával történhet (lásd a 7.8.3 feladathoz adott útmutatást is).

Most rátérünk a számelmélet alaptételének a kérdésére. A tételnek a felbonthatóságra vonatkozó állítása bármely $E(\sqrt{t})$-ben igaz: $E(\sqrt{t})$ minden, a 0-tól és egységektől különböző eleme felbontható véges sok $E(\sqrt{t})$-beli felbonthatatlan szorzatára. Ez az állítás a norma abszolút értékét felhasználva, a Gauss-egészeknél a 7.4.13 Tétel bizonyításában látott módon igazolható.

Alapvetően más a helyzet viszont a felbontás egyértelműségével kapcsolatban, ez már általában nem teljesül. Az egyértelműség kérdését először néhány konkrét bővítésben vizsgáljuk meg, majd utána ismertetjük az általános esetre vonatkozó eredményeket és megoldatlan problémákat.

10.3.5 Tétel **T 10.3.5**

A számelmélet alaptétele érvényes $E(\sqrt{2})$-ben, viszont nem érvényes $E(\sqrt{-5})$-ben és $E(\sqrt{10})$-ben. ♣

Bizonyítás: Mint a tétel kimondása előtt jeleztük, a felbonthatóság bármely $E(\sqrt{t})$-ben igaz, így elég az egyértelműséggel foglalkoznunk.

$E(\sqrt{2})$: Megmutatjuk, hogy a Gauss-egészekhez és Euler-egészekhez hasonlóan itt is elvégezhető a maradékos osztás. Ebből a már többször látott módon következik a számelmélet alaptételének egyértelműségi része.

A Gauss-egészeknél és az Euler-egészeknél a norma szerint végezzük a maradékos osztást, ami részletesen kifejtve azt jelenti, hogy a norma nemnegatív egész szám, egyedül a nullelem normája 0, és elérhető, hogy a maradék normája kisebb legyen az osztó normájánál. (Ezek a tulajdonságok biztosítják, hogy az euklideszi algoritmus véget ér, az általánosításra vonakozóan lásd a 11.3 pontot.)

Mivel $E(\sqrt{2})$-ben egy elem normája negatív is lehet, ezért itt a norma helyett a norma abszolút értékét használjuk, azaz azt igazoljuk, hogy $E(\sqrt{2})$-ben a norma abszolút értéke szerint elvégezhető a maradékos osztás.

Nyilvánvaló, hogy $E(\sqrt{2})$-ben a norma abszolút értéke nemnegatív egész szám és egyedül a nullelem normájának abszolút értéke 0.

Azt kell tehát belátnunk, hogy $E(\sqrt{2})$ tetszőleges α és $\beta \neq 0$ elemeihez léteznek olyan γ és ϱ elemek, melyekre

$$\alpha = \beta\gamma + \varrho \qquad \text{és} \qquad |N(\varrho)| < |N(\beta)|. \tag{10}$$

A norma fogalmát $\mathbf{Q}(\sqrt{2})$ elemeire is kiterjeszthetjük: $a, b \in \mathbf{Q}$ esetén legyen

$$N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

Azonnal adódik, hogy bármely $\xi, \psi \in \mathbf{Q}(\sqrt{2})$ esetén $N(\xi)N(\psi) = N(\xi\psi)$.

Ennek megfelelően, a (10)-beli egyenlőséget β-val elosztva az alábbi, (10)-zel ekvivalens feltételt kapjuk:

$$\frac{\alpha}{\beta} = \gamma + \frac{\varrho}{\beta} \qquad \text{és} \qquad \left|N\Big(\frac{\varrho}{\beta}\Big)\right| < 1. \tag{11}$$

A (11) feltételt a következőképpen is megfogalmazhatjuk: α/β-hoz keresünk olyan $\gamma \in E(\sqrt{2})$ elemet, amelyre

$$\left|N\Big(\frac{\alpha}{\beta} - \gamma\Big)\right| < 1. \tag{12}$$

Legyen $\alpha/\beta = u + v\sqrt{2}$, ahol $u, v \in \mathbf{Q}$. Válasszuk γ-nak azt a $c + d\sqrt{2} \in E(\sqrt{2})$ számot, ahol c, illetve d az u-hoz, illetve v-hez legközelebbi (egyik) egész szám. Ekkor

$$N\Big(\frac{\alpha}{\beta} - \gamma\Big) = (u - c)^2 - 2(v - d)^2,$$

és $0 \leq |u - c| \leq 1/2,\ 0 \leq |v - d| \leq 1/2$ miatt

$$\frac{-1}{2} \leq (u - c)^2 - 2(v - d)^2 \leq \frac{1}{4}\,,$$

tehát (12) valóban teljesül.

$E(\sqrt{-5})$: Megmutatjuk, hogy (például) a 6 két lényegesen különböző módon bontható $E(\sqrt{-5})$-beli felbonthatatlanok szorzatára:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})\,.$$

Ehhez azt kell belátnunk, hogy a 2, 3, $1 + \sqrt{-5}$ és $1 - \sqrt{-5}$ felbonthatatlanok $E(\sqrt{-5})$-ben, továbbá (például) a 3 nem egységszerese $1 \pm \sqrt{-5}$-nek.

Az állítás második része nyilvánvaló, hiszen $E(\sqrt{-5})$-ben a 10.3.4 Tétel (C) része szerint nincs más egység, mint a ± 1.

A felbonthatatlanságot a 2-re igazoljuk, a másik három szám esetén ugyanígy kell eljárni.

Tegyük fel indirekt, hogy $2 = \alpha\beta$, ahol α, β egyike sem egység $E(\sqrt{-5})$-ben. Ekkor $4 = N(2) = N(\alpha)N(\beta)$, továbbá $N(\alpha) \neq 1$, $N(\beta) \neq 1$, és így (mivel $E(\sqrt{-5})$-ben a norma nemnegatív) csak $N(\alpha) = N(\beta) = 2$ lehetséges.

Legyen $\alpha = a + b\sqrt{-5}$, itt a, b egész, mivel $-5 \not\equiv 1 \pmod 4$. Ekkor $N(\alpha) = a^2 + 5b^2 = 2$ nyilván nem állhat fenn. Az ellentmondás igazolja, hogy a 2 valóban felbonthatatlan $E(\sqrt{-5})$-ben.

$E(\sqrt{10})$: Ekkor (például) a -9-nek létezik két lényegesen különböző felbontása felbonthatatlanok szorzatára:

$$-9 = 3(-3) = (1 + \sqrt{10})(1 - \sqrt{10}). \tag{13}$$

A (13)-beli felbontásokban ± 3 nem egységszerese $1 \pm \sqrt{10}$-nek, mert

$$\frac{1 \pm \sqrt{10}}{\pm 3} = \frac{\pm 1}{3} \pm \frac{\pm 1}{3}\sqrt{10} \notin E(\sqrt{10})\,.$$

Azt kell még igazolni, hogy a (13)-ban szereplő tényezők valóban felbonthatatlanok. Ha ± 3 vagy $1 \pm \sqrt{10}$ nem lenne felbonthatatlan, akkor az $E(\sqrt{-5})$-nél látott gondolatmenet szerint kapnánk, hogy létezne olyan $\alpha = a + b\sqrt{10}$, a, b egész, amelyre $N(\alpha) = a^2 - 10b^2 = \pm 3$. Ez azonban lehetetlen, mert $a^2 \not\equiv \pm 3 \pmod 5$. ■

A számelmélet alaptételének kérdése az általános másodfokú bővítések esetén igen nehéz, és jelentős részben ma is megoldatlan probléma.

Kezdjük a valós bővítésekkel:

V1 Megoldatlan, hogy végtelen sok olyan $t > 0$ létezik-e, amelyre $E(\sqrt{t})$-ben érvényes az alaptétel.

V2 Meghatározták az összes olyan $t > 0$ értéket, amikor $E(\sqrt{t})$-ben a norma abszolút értéke szerint elvégezhető a maradékos osztás (lásd az alábbi 10.3.6 Tétel (iii) részét). Ezekre a t-kre tehát $E(\sqrt{t})$-ben biztosan érvényes a számelmélet alaptétele. Léteznek azonban további olyan pozitív t-k is, amikor igaz az alaptétel, ilyen például a $t = 14$, 22, 23 vagy 31.

A képzetes bővítésekre 1968 óta ismert a teljes válasz:

K1 Pontosan kilenc olyan $t < 0$ létezik, amelyre $E(\sqrt{t})$-ben érvényes az alaptétel, ezek felsorolását lásd a 10.3.6 Tétel (i) részében. (Ezek közé tartoznak a korábban már tárgyalt Gauss-, illetve Euler-egészek is.)

K2 A kilenc eset közül pontosan öt olyan van, amikor a norma szerint elvégezhető a maradékos osztás (lásd a 10.3.6 Tétel (ii) részét). Sőt, a másik négy t-re az is igazolható, hogy nemcsak a norma szerint, de „semmilyen más értelemben sem lehet maradékos osztást végezni". Ennek a kijelentésnek a pontos értelmezésére és bizonyítására a 11.3 pontban visszatérünk.

A K1, K2 és V2 pontokban jelzett eredményeket (bizonyítás nélkül) az alábbi tételben foglaljuk össze:

10.3.6 Tétel **T 10.3.6**

(i) A $t < 0$ esetben $E(\sqrt{t})$-ben akkor és csak akkor igaz a számelmélet alaptétele, ha

$$t = -1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163.$$

(ii) Az (i)-ben felsorolt kilenc t érték közül pontosan az első öt olyan, amikor $E(\sqrt{t})$-ben a norma szerint elvégezhető a maradékos osztás.

(iii) A $t > 0$ esetben $E(\sqrt{t})$-ben akkor és csak akkor végezhető el a norma abszolút értéke szerint a maradékos osztás, ha

$$t = 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73.\ \clubsuit$$

A 10.3.6 Tétel (ii) állításának a bizonyítását a 10.3.4 feladatban tűztük ki.

Végül két tételt tárgyalunk az $E(\sqrt{t})$-beli felbonthatatlanokról, illetve prímekről. Az első tétel tetszőleges $E(\sqrt{t})$-re vonatkozik, függetlenül attól, hogy érvényes-e a számelmélet alaptétele vagy sem. Ennek megfelelően itt élesen meg kell különböztetnünk a prím és a felbonthatatlan fogalmát, hiszen ezek nem ekvivalensek. A második tétel olyan másodfokú bővítésekre vonatkozik, ahol igaz a számelmélet alaptétele, így itt a prím és a felbonthatatatlan fogalma egybeesik.

10.3.7 Tétel **T 10.3.7**

Legyen $p > 2$ prímszám és $(p, t) = 1$. Ekkor $E(\sqrt{t})$-ben p akkor és csak akkor prím, ha $\left(\frac{t}{p}\right) = -1$. $\clubsuit$

Bizonyítás: Először azt igazoljuk, hogy ha $\left(\frac{t}{p}\right) = -1$, akkor p prím $E(\sqrt{t})$-ben.

Tegyük fel, hogy $p \mid \alpha\beta$, és mutassuk meg, hogy $p \mid \alpha$ és $p \mid \beta$ közül legalább az egyik teljesül.

A $p \mid \alpha\beta$ oszthatóságból kapjuk, hogy

$$p^2 = N(p) \mid N(\alpha)N(\beta).$$

Mivel p prímszám ($\mathbf{Z}$-ben), ezért p a $N(\alpha)N(\beta)$ szorzat valamelyik tényezőjét is osztja, mondjuk $p \mid N(\alpha)$. Megmutatjuk, hogy $\left(\frac{t}{p}\right) = -1$ miatt ebből $p \mid \alpha$ is következik.

Legyen $\alpha = a + b\sqrt{t}$. Vizsgáljuk először a $t \not\equiv 1 \pmod 4$ esetet, ekkor a és b egész számok. Így a $p \mid N(\alpha) = a^2 - tb^2$ feltétel átírható az

$$a^2 \equiv tb^2 \pmod p \tag{14}$$

alakba. Ha $(a, p) = (b, p) = 1$, akkor (14)-ből

$$1 = \left(\frac{a}{p}\right)^2 = \left(\frac{t}{p}\right)\left(\frac{b}{p}\right)^2 = \left(\frac{t}{p}\right)$$

következik, ami ellentmond a $\left(\frac{t}{p}\right) = -1$ feltételnek. Ha a és b közül pontosan az egyik osztható p-vel, akkor (14) egyik oldala osztható p-vel, a másik viszont nem, ami szintén lehetetlen. Így (14) csak úgy teljesülhet, ha $a \equiv b \equiv 0 \pmod p$. Ekkor $p \mid a + b\sqrt{t}$ is igaz, tehát valóban $p \mid \alpha$.

A $t \equiv 1 \pmod 4$ esetben azt a lehetőséget is figyelembe kell venni, amikor $a = u/2$, $b = v/2$, ahol u, v páratlan. Ekkor (14) helyett az $u^2 \equiv tv^2 \pmod p$ kongruencia fentiekhez hasonló vizsgálata igazolja $p \mid \alpha$ teljesülését.

A megfordításhoz indirekt tegyük fel, hogy $\left(\frac{t}{p}\right) = 1$. Ekkor létezik olyan c egész szám, amelyre $c^2 \equiv t \pmod p$. Így

$$p \mid c^2 - t = (c + \sqrt{t})(c - \sqrt{t}), \qquad \text{de} \qquad p \nmid c \pm \sqrt{t}.$$

Ez ellentmond annak, hogy p prím $E(\sqrt{t})$-ben. ■

A következő tétel a Gauss- és Euler-egészekre bizonyított 7.4.12, 7.4.14, 7.4.15, illetve 7.7.7 Tételek általánosítása arra az esetre, amikor $E(\sqrt{t})$-ben érvényes a számelmélet alaptétele:

10.3.8 Tétel **T 10.3.8**

Tegyük fel, hogy $E(\sqrt{t})$-ben igaz a számelmélet alaptétele. Ekkor:

(i) $E(\sqrt{t})$ egy eleme akkor és csak akkor felbonthatatlan, ha prím. (Ennek alapján a továbbiakban a felbonthatatlan helyett is a prím szót fogjuk használni.)

(ii) Minden π prímhez pontosan egy olyan p pozitív prímszám létezik, amelyre $\pi \mid p$.

(iii) Minden p pozitív prímszám vagy maga is prím $E(\sqrt{t})$-ben, vagy pedig pontosan két prímnek a szorzata, amelyek normája $\pm p$, és amelyek egymás „konjugáltjai" a következő értelemben (vö. a 10.4.1 Definícióval): legyen $\pi_1 = a + b\sqrt{t}$, ekkor $\pi_2 = \pm(a - b\sqrt{t})$.

(iv) Ha $p > 2$ prímszám, $(p, t) = 1$ és $\left(\frac{t}{p}\right) = -1$, akkor p prím $E(\sqrt{t})$-ben.

(v) Ha $p > 2$ prímszám, $(p, t) = 1$ és $\left(\frac{t}{p}\right) = 1$, akkor p két $E(\sqrt{t})$-beli prím szorzata, amelyek nem egymás egységszeresei.

(vi) Páratlan t esetén a 2 a következőképpen viselkedik:

a) ha $t \equiv 3 \pmod 4$, akkor a 2 két olyan prím szorzata, amelyek egymás egységszeresei (azaz a 2 egy prím négyzetének az egységszerese);

b) ha $t \equiv 1 \pmod 8$, akkor a 2 két olyan prím szorzata, amelyek nem egymás egységszeresei;

c) ha $t \equiv 5 \pmod 8$, akkor a 2 prím.

(vii) Ha a p prímszám osztója t-nek, akkor p két olyan prím szorzata, amelyek egymás egységszeresei (azaz p egy prím négyzetének az egységszerese).

(viii) A (iv)–(vii) pontokban felsorolt prímek egységszeresei adják az összes prímet $E(\sqrt{t})$-ben. ♣

Bizonyítás: (i) Egy prím mindig szükségképpen felbonthatatlan is, lásd az 1.4.3 Tétel bizonyítását. Az, hogy minden felbonthatatlan egyben prím is, a számelmélet alaptételéből következik, lásd az 1.5.8 feladatot (vagy a 11.3.1 Tételt).

(ii) és (iii) pontosan úgy bizonyítható, mint a 7.4.14 Tétel.

(iv) következik a 10.3.7 Tételből.

Az (v)–(vii) állításokkal kapcsolatban először csak azt igazoljuk, hogy a p, illetve a 2 prím-e $E(\sqrt{t})$-ben vagy sem.

(v)-nél ez a 10.3.7 Tételből következik.

(vi) Ha $t \equiv 3 \pmod 4$, akkor

$$2 \mid t^2 - t = (t + \sqrt{t})(t - \sqrt{t}), \qquad \text{de} \qquad 2 \nmid t \pm \sqrt{t},$$

tehát a 2 nem prím.

Ha $t \equiv 1 \pmod 8$, akkor

$$2 \mid \frac{1-t}{4} = \frac{1+\sqrt{t}}{2} \cdot \frac{1-\sqrt{t}}{2}\,, \qquad \text{de} \qquad 2 \nmid \frac{1 \pm \sqrt{t}}{2}\,,$$

tehát a 2 nem prím.

Végül, ha $t \equiv 5 \pmod 8$ és a 2 nem lenne prím, akkor lenne a 2-nek olyan

$$\alpha = \frac{u + v\sqrt{t}}{2} \in E(\sqrt{m})$$

osztója (ahol u, v egész), amelyre

$$N(\alpha) = \pm 2, \qquad \text{azaz} \qquad u^2 - tv^2 = \pm 8.$$

Azonban $u^2 - tv^2$ nem lehet $16k + 8$ alakú, ami ellentmondás.

(vii) Mivel

$$p \mid t = \sqrt{t} \cdot \sqrt{t}\,, \qquad \text{de} \qquad p \nmid \sqrt{t}$$

(ez $p = 2$ esetén is igaz), ezért p nem lehet prím.

Az (v), (vi)/a, (vi)/b és (vii) esetekben az előzőkből következik, hogy a p, illetve a 2 nem prím. Ekkor (iii) alapján a p, illetve a 2 felírható két prím, π_1 és π_2 szorzataként, ahol

$$\pi_1 = a + b\sqrt{t} \qquad \text{és} \qquad \pi_2 = \pm(a - b\sqrt{t}).$$

Itt a $t \not\equiv 1 \pmod 4$ esetben a és b egész, a $t \equiv 1 \pmod 4$ esetben pedig $a = u/2$, $b = v/2$, ahol u és v azonos paritású egészek.

Mivel $|N(\pi_1)| = |N(\pi_2)| = p$ (illetve 2), ezért $|N(\pi_1/\pi_2)| = 1$. Így π_1 és π_2 pontosan akkor egységszerese egymásnak, ha

$$\frac{\pi_1}{\pi_2} = \frac{a + b\sqrt{t}}{\pm(a - b\sqrt{t})} = \frac{a^2 + tb^2}{p} + \frac{2ab}{p}\sqrt{t} \in E(\sqrt{t}). \tag{15}$$

(v)-nél (15) nem teljesül, ugyanis ($|N(\pi_1)| = p$ miatt) $2ab/p$ nem lehet egész szám vagy egy 2 nevezőjű tört.

(vi)/a esetén (15)-ben $p = 2$, továbbá $t \equiv 3 \pmod 4$ miatt a és b egészek, valamint $a^2 - tb^2 = \pm 2$ alapján a és b páratlan. Ezért

$$\frac{a^2 + tb^2}{2} \qquad \text{és} \qquad \frac{2ab}{2} = ab$$

is egész, tehát π_1 és π_2 egymás egységszeresei.

(vi)/b esetén (15)-ben $p = 2$, továbbá

$$a^2 - tb^2 = \pm 2 \qquad \text{és} \qquad t \equiv 1 \pmod 4$$

miatt a és b nem lehet egész. Ezért $a = u/2$ és $b = v/2$, ahol u, v páratlan. Ekkor (15)-ben $2ab/2 = uv/4$ nem egész és nem kettő nevezőjű tört, tehát (15) nem teljesül. Így π_1 és π_2 nem egymás egységszeresei.

(vii)-nél vizsgáljuk először azt az esetet, amikor a és b egész. Ekkor

$$a^2 - tb^2 = \pm p \qquad \text{és} \qquad p \mid t$$

miatt $p \mid a$, és így (15)-ben

$$\frac{a^2 + tb^2}{p} \qquad \text{és} \qquad \frac{2ab}{p}$$

is egész, tehát π_1 és π_2 egymás egységszeresei.

Hasonlóan kezelhető az az eset is, amikor [$t \equiv 1 \pmod 4$ és] $a = u/2$, $b = v/2$, ahol u, v páratlan.

Végül, (viii) azonnal következik (ii)-ből és (iv)–(vii)-ből. ■

Feladatok

10.3.1

a) Bizonyítsuk be, hogy $E(\sqrt{3})$-ban érvényes a számelmélet alaptétele.

b) Hogyan fér össze a számelmélet alaptétele az alábbi egyenlőségekkel:

(b1) $7 + 3\sqrt{3} = (1 + \sqrt{3})(1 + 2\sqrt{3}) = (-4 + 3\sqrt{3})(5 + 3\sqrt{3})$;

(b2) $19 + 5\sqrt{3} = (5 - \sqrt{3})(5 + 2\sqrt{3}) = (-4 + 3\sqrt{3})(11 + 7\sqrt{3})$?

c) Határozzuk meg $E(\sqrt{3})$-ban az összes prímet.

*d) Milyen n pozitív egészekre oldható meg az $x^2 - 3y^2 = n$ diofantikus egyenlet, és megoldhatóság esetén mennyi a megoldásszám?

10.3.2

a) Bizonyítsuk be, hogy $E(\sqrt{-2})$-ben érvényes a számelmélet alaptétele.

b) Határozzuk meg $E(\sqrt{-2})$-ben az összes prímet.

*c) Oldjuk meg az $x^2 + 2 = y^3$ diofantikus egyenletet.

10.3.3 Mutassuk meg, hogy az alábbi t értékekre $E(\sqrt{t})$-ben nem igaz a számelmélet alaptétele:

a) 15; b) 26; c) -6; d) -10.

*10.3.4 Igazoljuk a 10.3.6 Tétel (ii) állítását: Egy képzetes $E(\sqrt{t})$-ben a norma szerint akkor és csak akkor végezhető el a maradékos osztás, ha $t = -1, -2, -3, -7$ vagy -11.

M*10.3.5 Bizonyítsuk be, hogy ha t (négyzetmentes) negatív összetett szám, akkor $E(\sqrt{t})$-ben nem érvényes a számelmélet alaptétele.

M*10.3.6 Legyen $k > 1$ egész szám és $f = x^2 + x + k$. Bizonyítsuk be, hogy ha $E(\sqrt{-4k+1})$-ben igaz a számelmélet alaptétele, akkor az

$$f(0),\ f(1),\ \ldots,\ f(k-2)$$

számok mindegyike prímszám.

Megjegyzés: Megmutatható, hogy az állítás megfordítása is igaz. Így a 10.3.6/(i) Tétel szerint a feladatban szereplő tulajdonság csak a $k = 2, 3, 5, 11, 17$ és 41 esetben teljesül. Ha $k = 41$, akkor azt az 5.1 pontban már említett tényt kapjuk, hogy $n^2 + n + 41$ minden $0 \le n \le 39$ esetén prímszám. Az előzőek alapján ilyen típusú prímszámsorozat $k > 41$ esetén nem létezik.

10.3.7 Mutassuk meg, hogy ha egy $\alpha \in E(\sqrt{t})$ elemre $|N(\alpha)|$ prímszám, akkor α

a) felbonthatatlan; *b) prím

$E(\sqrt{t})$-ben (függetlenül attól, hogy $E(\sqrt{t})$-ben igaz-e a számelmélet alaptétele vagy sem).

10.3.8 Bizonyítsuk be, hogy ha $\alpha, \beta \in E(\sqrt{t})$ és $\alpha^2 \mid \beta^2$, akkor $\alpha \mid \beta$ is teljesül (függetlenül attól, hogy $E(\sqrt{t})$-ben igaz-e a számelmélet alaptétele vagy sem).

10.3.9 Ebben a feladatban megvizsgáljuk, mely $p > 0$ prímszámok lesznek felbonthatatlanok, illetve prímek $E(\sqrt{-5})$-ben.

a) Az 5 nem felbonthatatlan (és így nem is prím).

b) A 2 felbonthatatlan, de nem prím.

c) Ha $p \equiv 11, 13, 17$ vagy 19 (mod 20), akkor p prím (és így felbonthatatlan is).

d) Ha $p \equiv 3$ vagy 7 (mod 20), akkor p felbonthatatlan, de nem prím.

M*e) Ha $p \equiv 1$ vagy 9 (mod 20), akkor p nem felbonthatatlan (és így nem is prím).

10.4. Norma

Ebben a pontban tetszőleges $\mathbf{Q}(\vartheta)$ bővítés elemeire kiterjesztjük a norma fogalmát, ahol ϑ algebrai szám. Ehhez szükségünk lesz egy algebrai szám $\mathbf{Q}$ *feletti konjugált*jainak és az adott bővítésre vonatkozó *relatív konjugált*jainak a fogalmára.

10.4.1 Definíció **D 10.4.1**

Egy α algebrai szám minimálpolinomjának (komplex) gyökeit az α $\mathbf{Q}$ *feletti konjugált*jainak nevezzük. ♣

Mivel m_α irreducibilis $\mathbf{Q}$ felett, és egy irreducibilis polinomnak nem lehet többszörös (komplex) gyöke (lásd a 9.4.4 feladatot), ezért egy n-edfokú algebrai számnak n darab (különböző) $\mathbf{Q}$ feletti konjugáltja van, amelyek közül az egyik maga az adott szám.

Az α $\mathbf{Q}$ feletti konjugáltjai között szerepel az α komplex konjugáltja, $\overline{\alpha}$ is, hiszen α-nak és $\overline{\alpha}$-nak ugyanaz a minimálpolinomja.

A továbbiakban általában a $\mathbf{Q}$ feletti konjugált helyett röviden csak a konjugált szót fogjuk használni (viszont a komplex konjugáltnál mindig kitesszük majd a komplex jelzőt).

Példák:

P1 Egy racionális számnak egyetlen konjugáltja van, önmaga.

P2 Legyen $\alpha = a + bi$ egy nem valós Gauss-racionális, azaz $a, b \in \mathbf{Q}$, $b \neq 0$. Ekkor α egyik konjugáltja önmaga, a másik pedig az $\overline{\alpha} = a - bi$ komplex konjugált. Hasonló a helyzet a nem valós Euler-racionálisok esetén is.

P3 Legyen $\alpha = a + b\sqrt{2}$ a $\mathbf{Q}(\sqrt{2})$ bővítés egy nem racionális eleme, azaz $a, b \in \mathbf{Q}$, $b \neq 0$. Ekkor α-nak egyik konjugáltja önmaga, a másik pedig $a - b\sqrt{2}$.

P4 Az $\alpha = \sqrt[5]{2}$ konjugáltjai a $\varrho\alpha$ alakú számok, ahol ϱ tetszőleges ötödik komplex egységgyök.

10.4.2 Definíció **D 10.4.2**

Legyenek a ϑ n-edfokú algebrai szám konjugáltjai

$$\vartheta_{(1)} = \vartheta\,, \quad \vartheta_{(2)}\,, \quad \ldots, \quad \vartheta_{(n)}\,,$$

és $\alpha \in \mathbf{Q}(\vartheta)$. Tekintsük (a 10.2.3 Tétel alapján) azt az (egyértelműen meghatározott) $f \in \mathbf{Q}[x]$ polinomot, amelyre

$$\alpha = f(\vartheta) \qquad \text{és} \qquad \deg f \leq n - 1 \text{ vagy } f = 0.$$

Ekkor az

$$f(\vartheta_{(j)}), \qquad j = 1, 2, \ldots, n$$

számokat az α-nak a $\mathbf{Q}(\vartheta)$-ra vonatkozó *relatív konjugált*jainak nevezzük. ♣

Az $f(\vartheta_{(j)})$ relatív konjugált tehát a $\mathbf{Q}(\vartheta_{(j)})$ bővítés egy eleme. Ez a $\mathbf{Q}(\vartheta_{(j)})$ bővítés többnyire nem esik egybe $\mathbf{Q}(\vartheta)$-val, és így általában az α relatív konjugáltjai nem lesznek elemei $\mathbf{Q}(\vartheta)$-nak.

A 10.4.2 Definícióban az $f(\vartheta_{(j)})$ relatív konjugáltak az α-n kívül látszólag nemcsak a $\mathbf{Q}(\vartheta)$ bővítéstől, hanem annak konkrét megadási módjától, azaz a ϑ választásától is függnek. A 10.4.3 Tételből azonban azonnal következik majd, hogy valójában nem ez a helyzet: ha $\mathbf{Q}(\vartheta) = \mathbf{Q}(\psi)$, akkor az α-nak a ϑ, illetve a ψ segítségével képzett relatív konjugáltjai ugyanazok lesznek.

Példák:

P5 Egy r racionális számnak bármely $\mathbf{Q}(\vartheta)$ bővítés esetén az összes relatív konjugáltja önmaga. Ugyanis az $f(\vartheta) = r$, $\deg f < \deg \vartheta$ vagy $f = 0$ feltételt kielégítő polinom az $f = r$ konstans polinom, így bármely j-re is $f(\vartheta_{(j)}) = r$.

P6 Legyen $\vartheta = i$, akkor ϑ konjugáltjai $\vartheta_{(1)} = i$ és $\vartheta_{(2)} = -i$. A $\mathbf{Q}(i)$ bővítés egy $\alpha = a + bi$ $(a, b \in \mathbf{Q})$ elemének a relatív konjugáltjai ezért

$$a + bi = \alpha \qquad \text{és} \qquad a + b(-i) = a - bi = \overline{\alpha}.$$

Ez azt jelenti, hogy ha α nem racionális szám, akkor a relatív konjugáltjai ugyanazok, mint a $\mathbf{Q}$ feletti konjugáltjai. Hasonló a helyzet a $\mathbf{Q}(\sqrt{-3})$, a $\mathbf{Q}(\sqrt{2})$ és általában a másodfokú bővítések esetén.

P7 Legyen $\vartheta = \sqrt[4]{3}$, ekkor ϑ konjugáltjai $\pm\vartheta$ és $\pm i\vartheta$. Az $\alpha = \sqrt{3} \in \mathbf{Q}(\vartheta)$ elemet a 10.2.3 Tétel szerint előállító polinom az $f = x^2$, ugyanis $\sqrt{3} = (\vartheta)^2$. Ennek megfelelően a $\sqrt{3}$ relatív konjugáltjai a

$$(\pm\vartheta)^2 = \sqrt{3} \qquad \text{és} \qquad (\pm i\vartheta)^2 = -\sqrt{3}.$$

Ez a négy szám éppen a $\sqrt{3}$-nak a $\mathbf{Q}$ feletti két konjugáltja kétszeres multiplicitással.

A példák alapján nem meglepő, hogy egy $\alpha \in \mathbf{Q}(\vartheta)$ elem relatív konjugáltjai ugyanazok, mint az α-nak a $\mathbf{Q}$ feletti konjugáltjai, megfelelő multiplicitással számolva:

10.4.3 Tétel **T 10.4.3**

Legyen α az n-edfokú $\mathbf{Q}(\vartheta)$ bővítés egy k-adfokú eleme. Ekkor az α-nak a $\mathbf{Q}(\vartheta)$-ra vonatkozó relatív konjugáltjait úgy kapjuk meg, hogy az α-nak mindegyik $\mathbf{Q}$ feletti konjugáltját n/k-szor vesszük. ♣

A tételből következik, hogy a relatív konjugáltakat nem befolyásolja, ha $\mathbf{Q}(\vartheta)$-ban ϑ helyett egy másik generátorelemet választunk, tehát a relatív konjugáltak valóban csak α-tól és magától a bővítéstől függnek.

A 10.4.3 Tételből egyúttal új bizonyítást nyertünk arra, hogy $\deg\alpha$ osztója a $\mathbf{Q}(\vartheta)$ bővítés fokának (vö. a 10.2.5 Tétellel).

Bizonyítás: Legyen ϑ, illetve α minimálpolinomja

$$m_\vartheta = \prod_{j=1}^{n}(x-\vartheta_{(j)}) \ \text{ (ahol } \vartheta_{(1)}=\vartheta\text{)}, \qquad m_\alpha = \prod_{s=1}^{k}(x-\alpha_{(s)}) \ \text{ (ahol } \alpha_{(1)}=\alpha\text{)},$$

és f az α-t a 10.2.3 Tétel szerint előállító polinom, azaz $f(\vartheta)=\alpha$.

I. Először azt igazoljuk, hogy az α mindegyik $f(\vartheta_{(j)})$ relatív konjugáltja megegyezik az α-nak a $\mathbf{Q}$ feletti valamelyik α_s konjugáltjával (a multiplicitást egyelőre nem vizsgáljuk).

Tekintsük a $g(x)=m_\alpha(f(x))$ polinomot. Nyilván $g\in\mathbf{Q}[x]$, továbbá

$$g(\vartheta)=m_\alpha(f(\vartheta))=m_\alpha(\alpha)=0.$$

Ebből következik, hogy $m_\vartheta \mid g$, és így minden j-re

$$0=g(\vartheta_{(j)})=m_\alpha(f(\vartheta_{(j)})).$$

Ez azt jelenti, hogy $f(\vartheta_{(j)})$ gyöke m_α-nak, vagyis $f(\vartheta_{(j)})$ valóban valamelyik α_s-sel egyenlő.

II. Azt kell még megmutatnunk, hogy mindegyik α_s ugyanannyiszor szerepel az $f(\vartheta_{(j)})$ számok között ($j=1,2,\dots,n$). E célból tekintsük a

$$h=\prod_{j=1}^{n}(x-f(\vartheta_{(j)}))$$

polinomot. A szimmetrikus polinomok alaptételének (9.3.2 Tétel) felhasználásával a 9.3.1 és 9.3.6 Tételek bizonyításához hasonló módon kapjuk, hogy h racionális együtthatós: A h minden c_r együtthatója a $\vartheta_{(j)}$-knek szimmetrikus

polinomja, így c_r felírható a $\vartheta_{(j)}$-k σ_j elemi szimmetrikus polinomjainak racionális együtthatós polinomjaként. A σ_j-k a gyökök és együtthatók közötti összefüggés alapján éppen m_ϑ együtthatói, illetve azok ellentettjei, tehát racionális számok, és így c_r is racionális.

Bontsuk fel a h polinomot a $\mathbf{Q}$ felett irreducibilis polinomok szorzatára. Mivel a h gyökei, azaz az $f(\vartheta_{(j)})$ számok valamennyien gyökei az m_α irreducibilis polinomnak, ezért a h felbontásában csak m_α szerepelhet. Figyelembe véve azt is, hogy h és m_α is normált, ez azt jelenti, hogy h az m_α-nak hatványa: $h = m_\alpha^t$. A fokszámok összehasonlításából kapjuk, hogy $t = n/k$, és így az $f(\vartheta_{(j)})$-k között az m_α mindegyik α_s gyöke valóban n/k-szor fordul elő. ■

Most már minden készen áll a norma általános definíciójához:

10.4.4 Definíció **D 10.4.4**

Egy $\alpha \in \mathbf{Q}(\vartheta)$ elem *normá*ján a relatív konjugáltjainak a szorzatát értjük: ha a ϑ konjugáltjai $\vartheta_{(1)} = \vartheta, \vartheta_{(2)}, \ldots, \vartheta_{(n)}$ és $\alpha = f(\vartheta)$, akkor

$$N(\alpha) = \prod_{j=1}^{n} f(\vartheta_{(j)})\,. \ \clubsuit$$

Világos, hogy a másodfokú bővítéseknél a 10.3.3 Definícióban szereplő normafogalom a 10.4.4 Definíció speciális esete.

A norma legfontosabb tulajdonságait a következő tételben foglaljuk össze:

10.4.5 Tétel **T 10.4.5**

(i) Legyen $\alpha \in \mathbf{Q}(\vartheta)$, $\deg \vartheta = n$ és $\deg \alpha = k$. Ekkor

$$N(\alpha) = \Big(\prod_{s=1}^{k} \alpha_s\Big)^{n/k} = (-1)^n a_0^{n/k}\,,$$

ahol $\alpha_{(1)} = \alpha, \alpha_{(2)}, \ldots, \alpha_{(k)}$ az α-nak a $\mathbf{Q}$ feletti konjugáltjai, és a_0 az α normált minimálpolinomjának a konstans tagja.

(ii) $\alpha, \beta \in \mathbf{Q}(\vartheta) \Longrightarrow N(\alpha\beta) = N(\alpha)N(\beta)$.

(iii) Ha α algebrai egész, akkor $N(\alpha)$ egész szám. ♣

Bizonyítás: Az (i) állításban szereplő első egyenlőség azonnal következik a 10.4.3 Tételből, a második egyenlőség pedig az m_α polinom gyökei és együtthatói közötti összefüggésből. A $N(\alpha)$-nak ebből az (i)-beli alakjából rögtön kapjuk a (iii) állítást is.

(ii) igazolásához legyen

$$\alpha = f_1(\vartheta), \qquad \beta = f_2(\vartheta) \qquad \text{és} \qquad \alpha\beta = f_3(\vartheta).$$

Ekkor ϑ gyöke a $h = f_3 - f_1 f_2 \in \mathbf{Q}[x]$ polinomnak, tehát $m_\vartheta \mid h$. Ebből következik, hogy m_ϑ többi gyöke, azaz a ϑ mindegyik $\vartheta_{(j)}$ konjugáltja is gyöke h-nak, azaz

$$0 = h(\vartheta_{(j)}) = f_3(\vartheta_{(j)}) - f_1(\vartheta_{(j)}) f_2(\vartheta_{(j)}), \qquad j = 1, 2, \ldots, n.$$

Az így adódó $f_3(\vartheta_{(j)}) = f_1(\vartheta_{(j)}) f_2(\vartheta_{(j)})$ egyenlőségeket összeszorozva kapjuk, hogy

$$N(\alpha\beta) = \prod_{j=1}^{n} f_3(\vartheta_{(j)}) = \Big(\prod_{j=1}^{n} f_1(\vartheta_{(j)})\Big)\Big(\prod_{j=1}^{n} f_2(\vartheta_{(j)})\Big) = N(\alpha)N(\beta). \ \blacksquare$$

Feladatok

10.4.1 Adjuk meg az alábbi algebrai számok $\mathbf{Q}$ feletti konjugáltjait:

a) $\sqrt{2}+\sqrt{3}$; b) $\sqrt{2}(1+i)$; c) $\cos 20^\circ$; d) $\cos 1^\circ + i \sin 1^\circ$.

10.4.2 Jelölje $\vartheta_{(1)} = \vartheta, \vartheta_{(2)}, \ldots, \vartheta_{(n)}$ a ϑ algebrai szám $\mathbf{Q}$ feletti konjugáltjait. Igazoljuk az alábbi állításokat.

a) Ha $\deg \vartheta = 2$, akkor $\mathbf{Q}(\vartheta_{(1)}) = \mathbf{Q}(\vartheta_{(2)})$.

b) Ha ϑ nem valós és $\deg \vartheta$ páratlan, akkor van olyan j és k, amelyre $\mathbf{Q}(\vartheta_{(j)}) \neq \mathbf{Q}(\vartheta_{(k)})$.

c) Ha ϑ nem valós és $\deg \vartheta = 3$, akkor bármely $j \neq k$ esetén $\mathbf{Q}(\vartheta_{(j)}) \cap \mathbf{Q}(\vartheta_{(k)}) = \mathbf{Q}$.

10.4.3 Adjuk meg $\mathbf{Q}(\sqrt[4]{2})$ alábbi elemeinek relatív konjugáltjait és normáját:

a) $1 + \sqrt[4]{2}$; b) $1 + \sqrt{2}$; c) $1 + \sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$.

10.4.4 Bizonyítsuk be, hogy $\mathbf{Q}(\vartheta)$ összes algebrai egészeinek $E(\vartheta)$ gyűrűjében egy ε elem akkor és csak akkor egység, ha $N(\varepsilon) = \pm 1$.

Megjegyzés: Ha $\mathbf{Q}(\vartheta)$ nem képzetes másodfokú bővítés és $\mathbf{Q}(\vartheta) \neq \mathbf{Q}$, akkor $E(\vartheta)$-ban az egységek száma mindig végtelen.

10.4.5 Igazoljuk az alábbi állításokat.

a) Létezik olyan Gauss-racionális, amely nem Gauss-egész, de a normája egész szám.

b) Bármely $\mathbf{Q}(\vartheta)$ másodfokú bővítésben van olyan α elem, amely nem algebrai egész, de $N(\alpha)$ egész szám.

10.5. Egész bázis

Ebben a pontban ϑ végig egy tetszőleges n-edfokú algebrai számot jelöl.

A 10.2.3 Tételből tudjuk, hogy minden $\alpha \in \mathbf{Q}(\vartheta)$ elem egyértelműen felírható

$$\alpha = a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1}, \qquad a_j \in \mathbf{Q}, \qquad j = 0, 1, \ldots, n-1 \qquad (1)$$

alakban, azaz az $1, \vartheta, \ldots, \vartheta^{n-1}$ elemek bázist alkotnak $\mathbf{Q}(\vartheta)$-ban mint $\mathbf{Q}$ feletti vektortérben.

Az (1) előállításból általában nem olvasható le, hogy α algebrai egész-e vagy sem. A 10.3.1 és 10.3.2 Tételben azonban láttuk, hogy másodfokú bővítések esetén létezik olyan ω_1, ω_2 bázis, amely erre is alkalmas: Minden másodfokú bővítés előáll $\mathbf{Q}(\sqrt{t})$ alakban, ahol t négyzetmentes egész szám és $t \neq 1$, továbbá, ha

$$\omega_1 = 1 \qquad \text{és} \qquad \omega_2 = \begin{cases} \sqrt{t}, & \text{ha } t \not\equiv 1 \pmod 4; \\ (1+\sqrt{t})/2, & \text{ha } t \equiv 1 \pmod 4, \end{cases}$$

akkor a $\mathbf{Q}(\sqrt{t})$ minden α eleme egyértelműen felírható

$$\alpha = r_1\omega_1 + r_2\omega_2, \qquad r_1,\, r_2 \in \mathbf{Q}$$

alakban, és α akkor és csak akkor algebrai egész, ha r_1 és r_2 egész számok.

Tetszőleges $\mathbf{Q}(\vartheta)$ bővítésben egy ilyen tulajdonságú bázist *egész bázis*nak nevezünk:

10.5.1 Definíció **D 10.5.1**

Egy $\mathbf{Q}(\vartheta)$ bővítés $\omega_1, \ldots, \omega_n$ elemeit a $\mathbf{Q}(\vartheta)$ *egész bázis*ának nevezzük, ha minden $\alpha \in \mathbf{Q}(\vartheta)$ egyértelműen felírható

$$\alpha = r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n, \qquad r_j \in \mathbf{Q}, \qquad j = 1, 2, \ldots, n \qquad (2)$$

alakban, és α akkor és csak akkor algebrai egész, ha mindegyik r_j egész szám. ♣

Célunk annak igazolása, hogy minden $\mathbf{Q}(\vartheta)$ bővítésben létezik egész bázis.

Legyen ϑ tetszőleges n-edfokú algebrai szám, és tekintsük a $\mathbf{Q}(\vartheta)$ bővítést. A világosabb megkülönböztetés érdekében a $\mathbf{Q}(\vartheta)$-nak mint $\mathbf{Q}$ feletti vektortérnek a bázisait v-bázisoknak, ezek közül az egész bázisokat pedig e-bázisoknak fogjuk nevezni.

Először vizsgáljuk meg, hogyan dönthető el $\mathbf{Q}(\vartheta)$ adott n eleméről, hogy v-bázist alkotnak-e. Legyen $\alpha_1, \ldots, \alpha_n \in \mathbf{Q}(\vartheta)$,

$$\alpha_i = f_i(\vartheta), \quad \text{ahol} \quad f_i \in \mathbf{Q}[x],\ \deg f_i \leq n-1 \text{ vagy } f_i = 0, \quad i = 1, \ldots, n, \tag{3a}$$

azaz

$$\alpha_i = a_{0i} + a_{1i}\vartheta + \ldots + a_{n-1,i}\vartheta^{n-1}, \quad a_{ki} \in \mathbf{Q},\ 0 \leq k \leq n-1,\ 1 \leq i \leq n. \tag{3b}$$

Tekintsük a $\mathbf{Q}(\vartheta)$ vektortérnek azt az $\mathcal{A}$ lineáris transzformációját, amely az $1, \vartheta, \ldots, \vartheta^{n-1}$ v-bázis elemeinek rendre megfelelteti az $\alpha_1, \ldots, \alpha_n$ „vektorokat". Ekkor az $\mathcal{A}$ transzformációnak az $1, \vartheta, \ldots, \vartheta^{n-1}$ v-bázisban felírt mátrixa

$$A = \begin{pmatrix} a_{01} & a_{02} & \ldots & a_{0n} \\ a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \ldots & a_{n-1,n} \end{pmatrix}, \tag{4}$$

ahol az a_{ki} elemek a (3b)-ben szereplő racionális számok.

Az $\mathcal{A}$ transzformáció és az A mátrix segítségével könnyen meghatározhatjuk, mikor alkotnak az $\alpha_1, \ldots, \alpha_n$ vektorok v-bázist: akkor és csak akkor, ha $\mathcal{A}$ invertálható, azaz $\det A \neq 0$.

Vegyük észre, hogy az A mátrix segítségével az $\alpha_1, \ldots, \alpha_n$ számokat a következőképpen is megkaphatjuk:

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = A^T \begin{pmatrix} 1 \\ \vartheta \\ \vdots \\ \vartheta^{n-1} \end{pmatrix}, \tag{3c}$$

ahol A^T az A mátrix transzponáltját jelöli.

Az e-bázis létezésének igazolásához az A mátrix helyett egy vele szoros kapcsolatban álló mátrix determinánsának a négyzetét, az ún. *diszkriminánst* fogjuk felhasználni.

Legyen V a ϑ $\mathbf{Q}$ feletti konjugáltjai által generált Vandermonde-mátrix:

$$V = V(\vartheta_{(1)}, \vartheta_{(2)}, \ldots, \vartheta_{(n)}) = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ \vartheta_{(1)} & \vartheta_{(2)} & \vartheta_{(3)} & \ldots & \vartheta_{(n)} \\ \vartheta_{(1)}^2 & \vartheta_{(2)}^2 & \vartheta_{(3)}^2 & \ldots & \vartheta_{(n)}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vartheta_{(1)}^{n-1} & \vartheta_{(2)}^{n-1} & \vartheta_{(3)}^{n-1} & \ldots & \vartheta_{(n)}^{n-1} \end{pmatrix}, \tag{5}$$

és

$$\tilde{A} = A^T V. \tag{6}$$

Ekkor az $\tilde{A}$ mátrix i-edik sorának j-edik eleme az A i-edik és a V j-edik oszlopának a skaláris szorzata, azaz

$$a_{0i} + a_{1i}\vartheta_{(j)} + \ldots + a_{n-1,i}\vartheta_{(j)}^{n-1}\,. \tag{7}$$

Vegyük észre, hogy a (7)-beli összeg (3a)–(3b) alapján éppen az α_i szám j-edik relatív konjugáltja, $f_i(\vartheta_{(j)})$.

Az $\alpha_1, \ldots, \alpha_n$ számok $\Delta(\alpha_1, \ldots, \alpha_n)$ *diszkriminánsa*n az $\tilde{A}$ mátrix determinánsának a négyzetét értjük:

10.5.2 Definíció **D 10.5.2**

Tekintsük a $\mathbf{Q}(\vartheta)$ bővítést, ahol $\deg\vartheta = n$, és jelölje a ϑ konjugáltjait $\vartheta_{(1)} = \vartheta$, $\vartheta_{(2)}$, …, $\vartheta_{(n)}$. Az $\alpha_1, \ldots, \alpha_n \in \mathbf{Q}(\vartheta)$ számok $\Delta(\alpha_1, \ldots, \alpha_n)$ *diszkriminánsa* az $\tilde{A}$ mátrix determinánsának a négyzete, azaz a (3a)–(6) jelöléseket és (7)-et is figyelembe véve

$$\Delta(\alpha_1, \ldots, \alpha_n) = (\det(A^T V))^2 = \begin{vmatrix} f_1(\vartheta_{(1)}) & f_1(\vartheta_{(2)}) & \ldots & f_1(\vartheta_{(n)}) \\ f_2(\vartheta_{(1)}) & f_2(\vartheta_{(2)}) & \ldots & f_2(\vartheta_{(n)}) \\ \vdots & \vdots & \ddots & \vdots \\ f_n(\vartheta_{(1)}) & f_n(\vartheta_{(2)}) & \ldots & f_n(\vartheta_{(n)}) \end{vmatrix}^2 . \ \clubsuit$$

A diszkrimináns legfontosabb tulajdonságait az alábbi tételben foglaljuk össze:

10.5.3 Tétel **T 10.5.3**

(i) A $\Delta(\alpha_1, \ldots, \alpha_n)$ diszkrimináns racionális szám, és ha az α_i-k algebrai egészek, akkor egész szám.

(ii) $\alpha_1, \ldots, \alpha_n$ akkor és csak akkor v-bázis, ha $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

(iii) Ha C egy $n \times n$-es racionális elemű mátrix és

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

akkor

$$\Delta(\beta_1, \ldots, \beta_n) = (\det C)^2 \Delta(\alpha_1, \ldots, \alpha_n)\,. \ \clubsuit$$

Bizonyítás: (i) A diszkrimináns a $\vartheta_{(j)}$-knek szimmetrikus polinomja: két $\vartheta_{(j)}$ cseréje a determinánsban két oszlop cseréjét jelenti, a determináns tehát ekkor előjelet vált, és így a négyzete nem változik. Ebből a már többször (a 9.3.1, a 9.3.6 vagy a 10.4.3 Tétel bizonyításában) látott módon következik, hogy a diszkrimináns racionális szám.

Ha mindegyik α_i algebrai egész, akkor a konjugáltjaik, és így a relatív konjugáltjaik is algebrai egészek. A diszkriminánst ezekből az összeadás, kivonás és szorzás segítségével kapjuk, és mivel az algebrai egészek gyűrűt alkotnak, ezért a diszkrimináns is algebrai egész. A diszkrimináns ekkor tehát olyan racionális szám, amely algebrai egész, és így szükségképpen egész szám.

(ii) A determinánsok szorzástétele szerint

$$\Delta(\alpha_1,\dots,\alpha_n) = (\det A)^2(\det V)^2\,.$$

Mivel a V Vandermonde-mátrix $\vartheta_{(j)}$ generátorelemei között nincs két azonos, ezért $\det V \neq 0$. Így

$$\Delta(\alpha_1,\dots,\alpha_n) \neq 0 \iff \det A \neq 0\,.$$

Azt pedig már igazoltuk, hogy $\alpha_1,\dots,\alpha_n$ akkor és csak akkor v-bázis, ha $\det A \neq 0$.

(iii) A (3c) összefüggés alapján

$$\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix} = A^T\begin{pmatrix}1\\ \vartheta\\ \vdots\\ \vartheta^{n-1}\end{pmatrix} \qquad \text{és} \qquad \begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix} = B^T\begin{pmatrix}1\\ \vartheta\\ \vdots\\ \vartheta^{n-1}\end{pmatrix}\,.$$

Így

$$\begin{pmatrix}\beta_1\\ \beta_2\\ \vdots\\ \beta_n\end{pmatrix} = C\begin{pmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{pmatrix} = CA^T\begin{pmatrix}1\\ \vartheta\\ \vdots\\ \vartheta^{n-1}\end{pmatrix}\,,$$

vagyis (a β_i-khez tartozó B mátrix egyértelműsége miatt) $B^T = CA^T$. Ebből következik, hogy

$$\begin{aligned}\Delta(\beta_1,\dots,\beta_n) &= (\det(B^TV))^2 = (\det(CA^TV))^2 = \\ &= (\det C)^2(\det(A^TV))^2 = (\det C)^2\Delta(\alpha_1,\dots,\alpha_n)\,. \ \blacksquare\end{aligned}$$

Most már rátérhetünk az e-bázis létezésének a bizonyítására.

10.5.4 Tétel **T 10.5.4**

Tetszőleges ϑ algebrai szám esetén $\mathbf{Q}(\vartheta)$-ban létezik egész bázis. ♣

Bizonyítás: Először megállapítjuk az e-bázisok néhány olyan tulajdonságát, amelyek majd támpontot nyújtanak ahhoz, hogy a v-bázisok közül ki tudjunk választani e-bázist.

Ha $\omega_1, \ldots, \omega_n$ e-bázis, akkor mindegyik ω_i algebrai egész kell hogy legyen, ugyanis az

$$\omega_i = 0 \cdot \omega_1 + \ldots + 1 \cdot \omega_i + \ldots + 0 \cdot \omega_n$$

előállításban minden együttható egész szám.

Ha $\omega_1, \ldots, \omega_n$ e-bázis és $\beta_1, \ldots, \beta_n$ olyan v-bázis, amelynek az elemei algebrai egészek, akkor mindegyik β_i az ω_j bázisvektorok egész együtthatós lineáris kombinációja, azaz létezik olyan C egész elemű, invertálható mátrix, amelyre

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix} .$$

Ekkor a 10.5.3/(iii) Tételből következik, hogy

$$\Delta(\beta_1, \ldots, \beta_n) = \Delta(\omega_1, \ldots, \omega_n)(\det C)^2 .$$

Mivel $\det C$ nullától különböző egész szám, ezért $(\det C)^2 \geq 1$, és így

$$|\Delta(\beta_1, \ldots, \beta_n)| \geq |\Delta(\omega_1, \ldots, \omega_n)| .$$

Ez azt jelenti, hogy egy e-bázis diszkiminánsának abszolút értéke kisebb vagy egyenlő, mint egy algebrai egészekből álló tetszőleges v-bázis diszkriminánsának az abszolút értéke.

Ennek megfelelően e-bázis csak egy olyan v-bázis lehet, amelynek az elemei algebrai egészek, és a diszkriminánsának abszolút értéke az ilyen típusú v-bázisok közül a legkisebb.

Igazolni fogjuk, hogy ilyen tulajdonságú v-bázis létezik, és az valóban egyben e-bázis is.

Először megmutatjuk, hogy létezik olyan v-bázis, amelynek az elemei algebrai egészek. Legyen $\gamma_1, \ldots, \gamma_n$ tetszőleges v-bázis. A 9.6.6 feladat szerint

mindegyik γ_i felírható $\gamma_i = \alpha_i/c_i$ alakban, ahol α_i algebrai egész és $c_i \neq 0$ egész szám. Ekkor nyilván $\alpha_1, \ldots, \alpha_n$ is v-bázis.

Tekintsük az összes olyan v-bázist, amelynek az elemei algebrai egészek. Minden ilyen v-bázis diszkriminánsa a 10.5.3/(i)–(ii) Tétel szerint 0-tól különböző egész szám. Vegyünk ezek közül egy olyan $\omega_1, \ldots, \omega_n$ v-bázist, amelyre a diszkrimináns abszolút értéke a legkisebb. Belátjuk, hogy $\omega_1, \ldots, \omega_n$ egyben e-bázis is.

Ehhez azt kell igazolni, hogy egy $\alpha \in \mathbf{Q}(\vartheta)$ elem akkor és csak akkor algebrai egész, ha a (2) szerinti

$$\alpha = r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n, \qquad r_j \in \mathbf{Q}, \qquad j = 1, 2, \ldots, n$$

előállításban mindegyik r_j egész szám.

Mivel az ω_i-k algebrai egészek, ezért ha $r_1, \ldots, r_n$ egész számok, akkor $\alpha = \sum_{j=1}^{n} r_j\omega_j$ is algebrai egész, hiszen az algebrai egészek gyűrűt alkotnak.

Megfordítva, legyen $\alpha \in \mathbf{Q}(\vartheta)$ tetszőleges algebrai egész. Tegyük fel indirekt, hogy a (2) szerinti

$$\alpha = r_1\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n$$

előállításban van olyan r_i, például r_1, amely nem egész szám. Legyen

$$\beta_1 = \alpha - \lfloor r_1 \rfloor \omega_1 = \{r_1\}\omega_1 + r_2\omega_2 + \ldots + r_n\omega_n \qquad \text{és} \qquad \beta_j = \omega_j, \text{ ha } 2 \leq j \leq n.$$

Ez azt jelenti, hogy $\beta_1, \ldots, \beta_n$ algebrai egészek, és

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix},$$

ahol

$$C = \begin{pmatrix} \{r_1\} & r_2 & r_3 & \ldots & r_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

A 10.5.3/(iii) Tétel alapján

$$\Delta(\beta_1, \ldots, \beta_n) = \Delta(\omega_1, \ldots, \omega_n)(\det C)^2 = \Delta(\omega_1, \ldots, \omega_n)\{r_1\}^2,$$

és így $0 < \{r_1\} < 1$ miatt

$$0 < |\Delta(\beta_1, \ldots, \beta_n)| < |\Delta(\omega_1, \ldots, \omega_n)|\,,$$

ami ellentmond $|\Delta(\omega_1, \ldots, \omega_n)|$ minimalitásának. ■

Megjegyzések: 1. A fenti bizonyításból kiderült, hogy $\mathbf{Q}(\vartheta)$-ban bármely két egész bázis diszkriminánsának az abszolút értéke megegyezik. Ennél több is igaz: maguk a diszkriminánsok is egyenlők, lásd a 10.5.2b feladatot. Ezt a közös értéket a $\mathbf{Q}(\vartheta)$ bővítés diszkriminánsának nevezzük.

2. A 10.5.4 Tételre adott bizonyításunk csak egzisztenciabizonyítás, egész bázis konkrét előállítására nem alkalmas.

3. A másodfokú bővítésekben a 10.3.2 Tétel alapján kaphatunk egész bázist, magasabb fokú bővítések esetén azonban lényegesen nehezebb egész bázist konstruálni. Megmutatható például, hogy ha ϑ p-edik primitív egységgyök, ahol $p > 2$ prímszám, akkor $1, \vartheta, \ldots, \vartheta^{p-2}$ egész bázist alkotnak $\mathbf{Q}(\vartheta)$-ban.

Feladatok

10.5.1 Számítsuk ki a $\mathbf{Q}(\vartheta)$ bővítésben a $\Delta(1, \vartheta, \ldots, \vartheta^{n-1})$ diszkriminánst a következő ϑ számok esetén:

a) i; b) $\cos(2\pi/3) + i\sin(2\pi/3)$; c) $\sqrt[3]{2}$; *d) $\sqrt[n]{2}$.

10.5.2 Tekintsünk egy rögzített $\mathbf{Q}(\vartheta)$ bővítést, ahol $\deg \vartheta = n$. Bizonyítsuk be az alábbi állításokat.

a) Ha $\omega_1, \ldots, \omega_n$ egész bázis és $\beta_1, \ldots, \beta_n \in \mathbf{Q}(\vartheta)$ tetszőleges algebrai egészek, akkor $\Delta(\omega_1, \ldots, \omega_n) \mid \Delta(\beta_1, \ldots, \beta_n)$.

b) Bármely két egész bázis diszkriminánsa megegyezik.

10.5.3 Mennyi egy egész bázis diszkriminánsa az egyes másodfokú bővítésekben?

10.5.4 Legyen $\deg \vartheta = n$ és $\alpha_1, \ldots, \alpha_n$ olyan algebrai egészek $\mathbf{Q}(\vartheta)$-ban, amelyekre $\Delta(\alpha_1, \ldots, \alpha_n)$ négyzetmentes szám. Bizonyítsuk be, hogy $\alpha_1, \ldots, \alpha_n$ egész bázis $\mathbf{Q}(\vartheta)$-ban.

10.5.5

a) Mi a szükséges és elégséges feltétele annak, hogy $\mathbf{Q}(i)$-ben az $a + bi$ és $c + di$ Gauss-racionálisok egész bázist alkossanak?

b) Vizsgáljuk meg a hasonló kérdést az Euler-racionálisok körében is.

M 10.5.6 Mely másodfokú bővítésekben létezik olyan ω_1, ω_2 egész bázis, ahol ω_2 az ω_1 $\mathbf{Q}$ feletti konjugáltja?

10.5.7 Legyen $\deg \vartheta = n$, és tegyük fel, hogy az m_ϑ minimálpolinomnak csak valós gyökei vannak. Lássuk be, hogy ekkor $\mathbf{Q}(\vartheta)$ bármely $\beta_1, \ldots, \beta_n$ elemére $\Delta(\beta_1, \ldots, \beta_n) \geq 0$.

10.5.8

a) Mutassunk példát arra, hogy a $\Delta(\alpha_1, \ldots, \alpha_n)$ diszkrimináns akkor is lehet nullától különböző egész szám, ha az α_i-k között van olyan, amely nem algebrai egész.

b) Bizonyítsuk be, hogy ha $\mathbf{Q}(\vartheta) \neq \mathbf{Q}$, akkor létezik $\mathbf{Q}(\vartheta)$-ban olyan v-bázis, amelynek egyik eleme sem algebrai egész, de a diszkriminánsa egész szám.

11. IDEÁLOK

Az ideálok központi szerepet játszanak a gyűrűk vizsgálatánál, ebből mi most csak a számelméleti vonatkozásokkal foglalkozunk. Szükséges és elégséges feltételt adunk arra, hogy egy gyűrűben érvényes legyen a számelmélet alaptétele, majd megmutatjuk, hogy főideálgyűrűben és euklideszi gyűrűben mindig igaz az alaptétel. Ezután az ideálok körében építünk ki számelméletet, és belátjuk, hogy egy algebrai számtest algebrai egészeinek ideáljaira már mindig érvényes az egyértelmű prímfaktorizáció. Ennek alkalmazásaként egy konkrét példán keresztül illusztráljuk, hogy ideálok segítségével olyan diofantikus egyenleteket is kezelni tudunk, ahol a megfelelő bővítés algebrai egészeire nem igaz a számelmélet alaptétele.

11.1. Ideál

Az „ideális számokat" Kummer a Fermat-sejtés hatékonyabb kezeléséhez vezette be a 19. század közepén, erről részletesebben is szó lesz majd a 11.2 pontban. Az „ideális számok"-ból kifejlődött ideálfogalom később a számelméleti vonatkozásoktól függetlenül is a gyűrűelméleti vizsgálatok alapvető eszközévé vált.

11.1.1 Definíció **D 11.1.1**

Egy R gyűrűben egy nemüres $I \subseteq R$ részhalmazt az R *ideál*jának nevezünk, ha

(A) I zárt az (R-beli) összeadásra és ellentettképzésre, azaz

$$i,\, j \in I \implies i+j \in I,\ -i \in I;$$

(B) bármely I-beli elemet egy tetszőleges R-beli elemmel akármelyik oldalról megszorozva ismét I-beli elemet kapunk, azaz

$$i \in I,\, r \in R \implies ri \in I,\ ir \in I. \ \clubsuit$$

Az ideál fogalma könnyen láthatóan ekvivalens azzal, hogy I olyan részgyűrű, ahol egy I-beli és egy I-n kívüli elem szorzata *is* I-beli.

Példák ideálra:

P1 Az egész számok gyűrűjében (rögzített m mellett) az m-mel osztható számok.

P2 A racionális együtthatós polinomok gyűrűjében azok a polinomok, amelyeknek egy adott α komplex szám gyöke.

P3 Az egész együtthatós polinomok gyűrűjében azok a polinomok, amelyeknek a konstans tagja páros szám.

P4 Bármely gyűrűben ideál maga a gyűrű és a csak a nullából álló részhalmaz, ezeket *triviális ideál*oknak nevezzük. Testben csak a két triviális ideál létezik (lásd a 11.1.3 feladatot).

Mivel az ideálok számelméleti vonatkozásait vizsgáljuk, ezért a továbbiakban az egész fejezetben eleve csak *kommutatív, egységelemes, nullosztómentes gyűrű*kre szorítkozunk. A gyűrűt (általában továbbra is) R-rel jelöljük, és mivel általában a komplex test részgyűrűiről, illetve polinomgyűrűkről lesz szó, ezért az egységelemet 1-gyel fogjuk jelölni.

Az ideálok legegyszerűbb és egyben legfontosabb típusát az egyetlen elem által generált ideálok, más néven *főideál*ok jelentik.

11.1.2 Definíció **D 11.1.2**

Legyen a az R (kommutatív, egységelemes, nullosztómentes) gyűrű tetszőleges eleme. Ekkor az $\{ra \,|\, r \in R\}$ halmazt az a által generált *főideál*nak nevezzük és (a)-val jelöljük. ♣

Az a által generált (a) főideál tehát az a elem (R-beli elemekkel képzett) többszöröseiből áll.

A definícióban szereplő „a által generált” és „ideál” szóhasználat jogosságát az alábbi tétel mutatja:

11.1.3 Tétel **T 11.1.3**

Az (a) főideál az a elemet tartalmazó *legszűkebb* ideál, azaz

(i) (a) ideál R-ben;

(ii) $a \in (a)$;

(iii) ha I ideál R-ben és $a \in I$, akkor $(a) \subseteq I$. ♣

Bizonyítás: (i) Belátjuk, hogy az $\{ra \,|\, r \in R\}$ nemüres halmaz eleget tesz a 11.1.1 Definíciónak (a jelölések egyértelműsége érdekében a képletekben szög-

letes zárójelet használunk közönséges zárójel céljaira, és a kerek zárójelet fenntartjuk az ideál jelölésére):

$$r_1a + r_2a = [r_1 + r_2]a, \quad -[ra] = [-r]a \quad \text{és} \quad [r_1a]r_2 = r_2[r_1a] = [r_2r_1]a.$$

(ii) $a = 1a \in \{ra \,|\, r \in R\}$.

(iii) Ha az I ideál tartalmazza a-t, akkor a 11.1.1 Definíció (B) követelménye szerint minden $r \in R$-re ra-t is tartalmaznia kell, azaz valóban $(a) \subseteq I$. ■

Az R gyűrű kommutativitását, illetve az egységelem létezését (i), illetve (ii) igazolásánál használtuk fel (a nullosztómentességre nem volt szükség a bizonyításhoz).

Példák:

A (P4 példában szereplő) két triviális ideál főideál; ezeket az egységelem, illetve a nullelem generálja: $R = (1)$, illetve $\{0\} = (0)$.

Főideál P1 és P2 is: az m-mel osztható számok $\mathbf{Z}$-ben az (m) főideált, az $f(\alpha) = 0$ tulajdonságú polinomok pedig $\mathbf{Q}[x]$-ben transzcendens α esetén a (0), algebrai α esetén az (m_α) főideált alkotják (ahol m_α az α minimálpolinomja).

A P3 példa viszont nem főideál. Jelöljük I-vel azoknak az egész együtthatós polinomoknak a halmazát, amelyek konstans tagja páros, és tegyük fel indirekt, hogy alkalmas f-re $I = (f)$. Ekkor az I minden eleme, így speciálisan a 2 is, többszöröse, azaz egész együtthatós polinomszorosa f-nek. Ebből következik, hogy csak $f = \pm 1, \pm 2$ lehetséges. Azonban (± 1) az összes egész együtthatós polinomot tartalmazza, (± 2) pedig azokból a polinomokból áll, amelyek minden együtthatója páros, és így ezek a főideálok nem egyenlők I-vel. Ezzel ellentmondásra jutottunk, tehát I valóban nem főideál.

A főideál általánosításaként most bevezetjük a *végesen generált ideál* fogalmát:

11.1.4 Definíció **D 11.1.4**

Legyenek $a_1, \ldots, a_k$ az R (kommutatív, egységelemes, nullosztómentes) gyűrű tetszőleges elemei. Ekkor a $\{\sum_{j=1}^{k} r_j a_j \,|\, r_j \in R\}$ halmazt az $a_1, \ldots, a_k$ által generált ideálnak nevezzük és $(a_1, \ldots, a_k)$-val jelöljük.

Egy I ideál *végesen generált*, ha léteznek olyan $a_1, \ldots, a_k$ elemek, amelyekre $I = (a_1, \ldots, a_k)$. ♣

A 11.1.3 Tétel megfelelője a végesen generált ideálokra is igaz:

11.1.5 Tétel **T 11.1.5**

Az $(a_1, \ldots, a_k)$ ideál az a_j elemeket tartalmazó *legszűkebb* ideál, azaz

(i) $(a_1, \ldots, a_k)$ ideál R-ben;

(ii) $a_j \in (a_1, \ldots, a_k), \quad j = 1, 2, \ldots, k$;

(iii) ha I ideál R-ben és $a_j \in I$, $j = 1, 2, \ldots, k$, akkor $(a_1, \ldots, a_k) \subseteq I$. ♣

A 11.1.5 Tétel bizonyítása a 11.1.3 Tételhez hasonlóan történik, ennek végiggondolását az Olvasóra bízzuk.

Példák:

Nyilván minden főideál végesen (egyetlen elem által) generált ideál.

A P3 példa I ideálja is végesen generált: $I = (2, x)$.

Az összes algebrai egész E gyűrűjében

$$K = \{\xi \sqrt[k]{2} \mid \xi \in E,\ k = 2, 3, 4, \ldots\}$$

ideál, de nem generálható véges sok elemmel (lásd a 11.1.4 feladatot).

Ha ϑ algebrai szám, akkor $E(\vartheta)$ minden ideálja végesen generált (lásd a 11.1.10 feladatot). (A korábbiakhoz hasonlóan $E(\vartheta)$ a $\mathbf{Q}(\vartheta)$ bővítés algebrai egészeinek gyűrűjét jelöli.)

Végül röviden kitérünk az ideál szerinti maradékosztálygyűrű konstrukciójára. Ez a fogalom a modulo m maradékosztályok gyűrűjének (lásd a 2.8 pontot) az általánosítása.

A 11.1.1 Definíció utáni P1 példában láttuk, hogy az egész számok $\mathbf{Z}$ gyűrűjében az m-mel osztható számok egy I ideált alkotnak. Az I segítségével az a egész számot tartalmazó (azaz az a által „reprezentált") modulo m maradékosztályt

$$a + I = \{a + i \mid i \in I\} \tag{1}$$

alakban is megadhatjuk. A maradékosztályok összeadását és szorzását a reprezentánsok segítségével értelmeztük, ami az (1) szerinti felírásban a következőket jelenti:

$$[a + I] + [b + I] = [a + b] + I \qquad \text{és} \qquad [a + I][b + I] = ab + I. \tag{2}$$

Be kellett látni, hogy (2) az *osztályokra* valóban műveleteket definiál, azaz az eredményül kapott osztály *egyértelmű*, *nem függ* attól, hogy az egyes osztályokból melyik *reprezentáns*okat választottuk. Ha végigelemezzük ennek a

bizonyítását, akkor kiderül, hogy a szóban forgó egyértelműséget éppen I ideál volta biztosítja. Mindezek alapján a következő általánosítást kapjuk:

11.1.6 Tétel **T 11.1.6**

Legyen I ideál az R gyűrűben. Ekkor az I szerinti (1) *maradékosztály*ok az R gyűrű diszjunkt részhalmazai, melyek egyesítése R, és ezek a (2)-ben definiált összeadásra és szorzásra nézve gyűrűt alkotnak. Ezt a gyűrűt az R-nek az I szerinti *maradékosztálygyűrű*jének vagy *faktorgyűrű*jének nevezzük és R/I-vel jelöljük. ♣

Ennek megfelelően a modulo m maradékosztályok gyűrűje éppen az egész számoknak az (m) főideál szerinti faktorgyűrűje, azaz $\mathbf{Z}/(m)$.

A 11.1.6 Tétel bizonyítását nem részletezzük. Mint jeleztük, az I ideáltulajdonságaival igazolható az R/I-beli műveletek egyértelműsége (valamint az, hogy az (1) osztályok lefedik R-et, és két ilyen osztály vagy diszjunkt, vagy pedig egybeesik). Az R/I-re vonatkozó gyűrűazonosságok az R gyűrű megfelelő azonosságaiból következnek, az R/I nulleleme a $0+I$ maradékosztály, azaz maga az I ideál, az $a+I$ maradékosztály ellentettje pedig a $[-a]+I$ maradékosztály.

Példa: Tekintsük a racionális együtthatós polinomok gyűrűjének az (x^2-2) főideál szerinti faktorgyűrűjét, azaz a $\mathbf{Q}[x]/(x^2-2)$ maradékosztálygyűrűt.

Hasonló meggondolásokat alkalmazhatunk, mint az egész számoknál képzett modulo m maradékosztályok, azaz a $\mathbf{Z}/(m)$ faktorgyűrű konstrukciójánál. Most azok a polinomok kerülnek az (x^2-2) főideál szerint egy maradékosztályba, amelyek ugyanazt a maradékot adják x^2-2-vel osztva. Ily módon minden maradékosztály egyértelműen jellemezhető egy „maradékkal”, azaz egy legfeljebb elsőfokú $a+bx$ (racionális együtthatós) polinommal (idesorolva a 0 polinomot is, amely magát az ideált reprezentálja).

A maradékosztálygyűrűben tulajdonképpen ezekkel a maradékokkal számolunk, azaz pl. két maradékosztály szorzásakor ezeket a maradékokat összeszorozzuk és vesszük a szorzatnak az x^2-2-vel való osztási maradékát (pontosan ugyanúgy, ahogy pl. modulo 15 a 7-nek és a 6-nak a szorzata 12). Ennek megfelelően az összeadást az

$$[a+bx]+[c+dx]=[a+c]+[b+d]x,$$

a szorzást pedig az

$$\begin{aligned}[a+bx][c+dx] &= ac+[ad+bc]x+bdx^2 = \\ &= ac+[ad+bc]x+2bd+bd[x^2-2] = [ac+2bd]+[ad+bc]x\end{aligned}$$

szabály szerint kell végezni, azaz pontosan ugyanúgy, ahogyan $\mathbf{Q}(\sqrt{2})$-ben (képzeljünk az „x” betű helyére mindenhol „$\sqrt{2}$”-t).

Ez azt jelenti, hogy a $\mathbf{Q}[x]/(x^2-2)$ maradékosztálygyűrű izomorf (azaz szó szerinti fordításban „azonos alakú”) a $\mathbf{Q}(\sqrt{2})$ testtel.

A fentiekhez hasonlóan általában is igaz, hogy tetszőleges algebrai ϑ esetén $\mathbf{Q}(\vartheta)$ jellemezhető maradékosztálygyűrűként: a $\mathbf{Q}(\vartheta)$ test izomorf a $\mathbf{Q}[x]/(m_\vartheta)$ faktorgyűrűvel, lásd a 11.1.9 feladatot.

Feladatok

11.1.1 Legyen G a Gauss-egészek gyűrűje, és tekintsük G-ben az alábbi tulajdonságú $\alpha = a + bi$ Gauss-egészekből álló részhalmazokat:

a) a és b páros; b) $a \equiv b \pmod 2$; c) $a \equiv b \pmod 3$;
d) $2 \mid N(\alpha)$; e) $5 \mid N(\alpha)$; f) $7 \mid N(\alpha)$.

Ezek közül melyek alkotnak ideált G-ben? A főideáloknak adjuk meg egy-egy generátorelemét.

11.1.2 Tekintsük $\mathbf{Z}[x]$-ben az alábbi tulajdonságú f polinomokból álló részhalmazokat:

a) $f(1/2) = 0$; b) $f(\sqrt{2}) = f(\sqrt{3}) = 0$; c) $f(\sqrt{2}) = f(\sqrt{3})$;
d) $f(3)$ páros szám; e) f főegyütthatója páros szám vagy $f = 0$.

A megadott halmazok közül melyek alkotnak ideált $\mathbf{Z}[x]$-ben, és ezek (legkevesebb) hány elemmel generálhatók?

11.1.3 Mutassuk meg, hogy egy legalább kételemű, kommutatív, egységelemes, nullosztómentes gyűrű pontosan akkor test, ha csak triviális ideáljai vannak.

11.1.4 Legyen E az összes algebrai egész gyűrűje, és

$$K = \{\xi \sqrt[k]{2} \mid \xi \in E,\ k = 2, 3, 4, \ldots\}\,.$$

Bizonyítsuk be, hogy K ideál E-ben, de nem generálható véges sok elemmel.

11.1.5 Legyenek $\alpha_1, \ldots, \alpha_k$ és ξ az R kommutatív, egységelemes, nullosztómentes gyűrű tetszőleges elemei. Bizonyítsuk be, hogy

$$(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k) = (\alpha_1 - \xi\alpha_2,\ \alpha_2,\ \ldots,\ \alpha_k)\,.$$

11.1.6 Legyen G a Gauss-egészek gyűrűje.

a) Hány eleműek az alábbi főideálok szerinti faktorgyűrűk, és közülük melyek alkotnak testet:

a1: (2); a2: (3); a3: $(2+i)$?

*b) Vizsgáljuk meg általánosan is a fenti kérdéseket a G tetszőleges eleme által generált főideálra.

11.1.7 Tekintsük az $E(\sqrt{-5})$ gyűrűt.

a) Mutassuk meg, hogy $E(\sqrt{-5})$-ben $(2, 1+\sqrt{-5})$ nem főideál.

b) Hány eleműek az alábbi ideálok szerinti faktorgyűrűk, és közülük melyek alkotnak testet:

b1: $(2, 1+\sqrt{-5})$; b2: $(1+\sqrt{-5})$; b3: (11)?

M 11.1.8

a) Az alábbi faktorgyűrűk közül melyek alkotnak testet:

a1: $\mathbf{R}[x]/(x^2-2)$; a2: $\mathbf{R}[x]/(x^2+1)$; a3: $\mathbf{C}[x]/(x^2+1)$?

b) Legyen T tetszőleges kommutatív test és $f \in T[x]$. Mi a szükséges és elégséges feltétele annak, hogy a $T[x]/(f)$ faktorgyűrű test legyen?

c) Igazoljuk, hogy a $\mathbf{Z}[x]/(2, x^2+x+1)$ faktorgyűrű test.

*11.1.9

a) Legyen ϑ algebrai szám. Igazoljuk, hogy a $\mathbf{Q}(\vartheta)$ test a $\mathbf{Q}[x]/(m_\vartheta)$ faktorgyűrűvel izomorf.

b) Legyen L tetszőleges (kommutatív) test és f egy irreducibilis polinom L felett. Konstruáljunk egy olyan M testet, amely rendelkezik az alábbi tulajdonságokkal:

(i) M-nek van az L-lel izomorf L^* részteste;

(ii) ha $f^* \in L^*[x]$ az a polinom, amelynek az együtthatóit az f együtthatóiból az $L \to L^*$ izomorfizmus szerint kapjuk, akkor f^*-nak van egy $\vartheta \in M$ gyöke;

(iii) $M = L^*(\vartheta)$.

Megjegyzés: Ennek a konstrukciónak az alapján akkor is tudjuk az L-et egy irreducibilis polinom — még nem is létező(!) — gyökével bővíteni, ha nincs eleve adva egy, az L-et tartalmazó test.

*11.1.10

a) Legyen ϑ algebrai szám és $I \neq 0$ tetszőleges ideál $E(\vartheta)$-ban. Bizonyítsuk be, hogy az $E(\vartheta)/I$ faktorgyűrűnek véges sok eleme van.

b) Igazoljuk, hogy $E(\vartheta)$ ideáljainak szigorúan növő

$$A_1 \subset A_2 \subset \ldots \subset A_j \subset \ldots$$

lánca nem lehet végtelen.

c) Mutassuk meg, hogy $E(\vartheta)$ minden ideálja végesen generált.

Megjegyzés: A 11.5.9 Tételben bebizonyítjuk, hogy $E(\vartheta)$ minden ideálja már két elemmel is generálható.

11.2. Elemi számelméleti kapcsolatok

Ebben a pontban az ideáloknak az oszthatósággal, az egységekkel és a legnagyobb közös osztóval való kapcsolatát tárgyaljuk.

Az oszthatóság és az egység fogalma bármely R (kommutatív, egységelemes, nullosztómentes) gyűrűben a szokásos módon (az 1.1.1 és 1.1.2 Definíciók mintájára) értelmezhető, és általában is érvényesek az egészeknél megszokott (az 1.1.4 és 1.1.5 Tételnek megfelelő) elemi tulajdonságok.

Először azt mutatjuk meg, hogy az oszthatóság, illetve az egységek szerepe egyszerűen jellemezhető a főideálok segítségével.

11.2.1 Tétel **T 11.2.1**

Tetszőleges R (kommutatív, egységelemes, nullosztómentes) gyűrűben

(i) $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$;

(ii) az a akkor és csak akkor egységszerese b-nek, ha $(a) = (b)$. ♣

Bizonyítás: (i) A három (i)-beli feltétel a főideál definícióját felhasználva a következőképpen fogalmazható át:

a osztója b-nek;

b szerepel az a többszörösei között;

a b többszörösei mind megtalálhatók az a többszörösei között,

így a három feltétel ekvivalenciája nyilvánvaló.

(ii) Az (i) rész alapján $(a) = (b)$ azt jelenti, hogy $a \mid b$ és $b \mid a$ is teljesül, ami azzal ekvivalens, hogy az a a b-nek egységszerese (lásd az 1.1.5/(iii) Tételt). ■

Most rátérünk az ideálok és a legnagyobb közös osztó kapcsolatára.

A legnagyobb közös osztó (az 1.3.2, illetve 7.4.9 Definíciók mintájára) olyan közös osztót jelent, amely minden közös osztónak többszöröse.

Az egészek, Gauss-egészek vagy Euler-egészek gyűrűjében bármely két elemnek létezik legnagyobb közös osztója, ezt a maradékos osztások véges sorozatából álló euklideszi algoritmus biztosítja.

Egy gyűrűben akkor is létezhet bármely két elemnek legnagyobb közös osztója, ha a gyűrűben nem végezhető el a maradékos osztás, ilyen például az egész együtthatós polinomok gyűrűje (ennek részletesebb elemzésére később visszatérünk).

Vannak azonban olyan gyűrűk is, ahol nincs bármely két elemnek legnagyobb közös osztója, ilyen például az $E(\sqrt{-5})$ gyűrű, ahol a $2 + 2\sqrt{-5}$ és 6 elemeknek nem létezik legnagyobb közös osztója (lásd a 11.2.4 feladatot).

Végül bármely R gyűrűben igaz, hogy ha valamely két elemnek létezik legnagyobb közös osztója, akkor ez egységszerestől eltekintve egyértelmű; ez a legnagyobb közös osztó definíciójából azonnal következik.

Két elem legnagyobb közös osztója a két elem által generált ideállal áll szoros kapcsolatban. A jelölések hasonlósága miatt ebben a fejezetben a és b legnagyobb közös osztóját mindig $\operatorname{lnko}\{a, b\}$-vel jelöljük, (a, b) pedig az a és b elemek által generált ideált jelenti.

Nézzük először az egész számok gyűrűjét. Itt például a $(6, 15)$ ideál a $6u + 15v$ alakú számok halmaza, ahol u és v tetszőleges egész számok. A lineáris diofantikus egyenletek megoldhatóságáról szóló 1.3.6 Tétel alapján tudjuk, hogy ez a halmaz megegyezik $\operatorname{lnko}\{6, 15\} = 3$ többszöröseinek a halmazával, azaz a (3) főideállal. Az egészek körében ugyanígy általában is igaz, hogy ha $d = \operatorname{lnko}\{a, b\}$, akkor $(a, b) = (d)$. Tetszőleges gyűrűben ennél kicsit bonyolultabb a helyzet:

11.2.2 Tétel **T 11.2.2**

Legyen R tetszőleges (kommutatív, egységelemes, nullosztómentes) gyűrű.

(i) Ha $(a, b) = (d)$, akkor $d = \operatorname{lnko}\{a, b\}$.

(ii) A $d = \operatorname{lnko}\{a, b\}$ feltételből $(a, b) \subseteq (d)$ következik, azonban általában $(a, b) \neq (d)$.

(iii) $(a, b) = (d)$ akkor és csak akkor teljesül, ha $d = \operatorname{lnko}\{a, b\}$ és alkalmas u, $v \in R$ elemekre $d = au + bv$. ♣

Bizonyítás: (i) Az $(a, b) = (d)$ feltétel alapján $a \in (a, b) = (d)$, tehát $d \mid a$, és ugyanígy $d \mid b$, azaz d közös osztója a-nak és b-nek.

Legyen c tetszőleges közös osztó, azaz $c \mid a$ és $c \mid b$. Ekkor a 11.2.1 Tétel szerint $a \in (c)$ és $b \in (c)$. Mivel (a, b) az a és b elemet tartalmazó legszűkebb

ideál, ezért innen $(d) = (a, b) \subseteq (c)$, azaz (ismét a 11.2.1 Tételt használva) $c \mid d$ következik.

(ii) Ha $d = \text{lnko}\{a, b\}$, akkor $d \mid a$ és $d \mid b$. Ez azt jelenti, hogy a és b eleme a (d) ideálnak, és így (d) tartalmazza az a-t és b-t tartalmazó legszűkebb ideált, azaz valóban $(a, b) \subseteq (d)$.

A következő példa mutatja, hogy egyenlőség nem mindig teljesül: az egész együtthatós polinomok körében a 2 és x polinomok legnagyobb közös osztója 1, ugyanakkor $(2, x) \neq (1)$ (az előző pontban beláttuk, hogy $(2, x)$ nem is főideál).

A 11.2.4c feladatban egy más jellegű olyan példa szerepel, amikor nem teljesül egyenlőség.

(iii) Ha $(a, b) = (d)$, akkor $d = \text{lnko}\{a, b\}$ fennállását már (i)-ben igazoltuk, továbbá ekkor $d \in (a, b)$, azaz d definíció szerint felírható alkalmas R-beli elemekkel $d = au + bv$ alakban.

A megfordításhoz induljunk ki abból, hogy $d = \text{lnko}\{a, b\}$ és $d = au + bv$. Az első feltételből (ii) alapján kapjuk, hogy $(a, b) \subseteq (d)$, a második szerint pedig $d \in (a, b)$, és így $(d) \subseteq (a, b)$, azaz valóban $(a, b) = (d)$. ■

Megjegyzés: Számos gyűrű esetén a 11.2.2 Tétel a

$$d = \text{lnko}\{a, b\} \iff (a, b) = (d) \tag{1}$$

ekvivalenciára egyszerűsödik. Ilyen tulajdonságú például az egész számok gyűrűje, amint azt a tétel kimondása előtt vázoltuk. Hasonló meggondolásból adódik, hogy (1) minden olyan gyűrűben érvényes, ahol elvégezhető a maradékos osztás.

Mint már jeleztük, az ideálfogalom először a Fermat-sejtéssel kapcsolatban jelent meg Kummer vizsgálataiban. Ennek megértéséhez tekintsük az

$$x^p + y^p = z^p \tag{2}$$

Fermat-egyenletet, ahol $p > 2$ prímszám. Az

$$x^p + y^p = \prod_{j=0}^{p-1} (x + y\varrho^j), \qquad \varrho = \cos\Big(\frac{2\pi}{p}\Big) + i \sin\Big(\frac{2\pi}{p}\Big), \tag{3}$$

szorzattá bontás alapján a (2) egyenlet szoros kapcsolatban áll az $E(\varrho)$ gyűrű számelméletével.

A (2) és (3) összekapcsolásából adódó

$$\prod_{j=0}^{p-1}(x+y\varrho^j)=z^p \tag{4}$$

egyenlet bal oldalán álló szorzat p-edik hatvány. Azt gondolhatnánk, hogy itt is segítene az a korábban többször sikerrel alkalmazott taktika, hogy megpróbáljuk kimutatni, hogy minden tényező külön-külön is p-edik hatvány $E(\varrho)$-ban, majd belátni, hogy az így kapott p darab $x+y\varrho^j=\alpha_j^p$ típusú egyenlet (nemtriviális x, y, z megoldást feltételezve) együttesen ellentmondásra vezet.

Az egész számok körében tudjuk, hogy ha egy szorzat tényezői páronként relatív prímek és a szorzat p-edik hatvány, akkor a tényezők külön-külön is p-edik hatványok egységszeresei. Ugyanez igaz a Gauss-egészek vagy az Euler-egészek körében is, és általában minden olyan gyűrűben, ahol *érvényes a számelmélet alaptétele*. Az alaptétel hiánya esetén azonban ez már nem igaz: például $E(\sqrt{-5})$-ben $3^2=(2+\sqrt{-5})(2-\sqrt{-5})$, itt a jobb oldal tényezői relatív prímek, azonban nem négyzetszámok egységszeresei (hiszen felbonthatatlanok).

A Fermat-sejtés bizonyítására vázolt fenti próbálkozás tehát eleve csak akkor lehet reményteljes, ha $E(\varrho)$-ban érvényes a számelmélet alaptétele. Megmutatható, hogy $p>19$ esetén ez nem teljesül, és így más utat kell keresni.

Történeti érdekességként megjegyezzük, hogy Lamé francia akadémikus 1847-ben éppen a számelmélet alaptételét általános $E(\varrho)$-ra is feltételezve adott alapvetően rossz bizonyítást a Fermat-sejtésre a fenti gondolatmenetet követve (könnyen lehet, hogy Fermat „csodálatos bizonyítása" is — ha egyáltalán létezett ilyen — hasonló hibán alapult). A Lamé bizonyításában található „hézagra", azaz az alaptétel érvényességének a kérdésére Liouville mutatott rá (aki előtt akkor még nem volt ismert, mely esetekben igaz az alaptétel). Lamé egyébként még egy hibát elkövetett, nem vette figyelembe, hogy a (4) bal oldalán álló tényezők a páronként relatív prímség és az alaptétel fennállása esetén sem szükségképpen p-edik hatványok, hanem csak azok egységszeresei. Mivel ráadásul $E(\varrho)$-ban $p>3$ esetén végtelen sok egység van, ezért ez a „figyelmetlenség" egy újabb, nehezen javítható „hézagot" jelent Lamé gondolatmenetében.

Ugyanebben az időben a német Kummer is hasonló utat járt be, ő azonban látta, hogy szükség lenne az alaptételre $E(\varrho)$-ban, és azt is észrevette, hogy ez nem mindig teljesül. Azt is látta, hogy ha bármely két elemnek létezik legnagyobb közös osztója, akkor ebből az alaptétel könnyen levezethető. Ezért azokban az $E(\varrho)$ gyűrűkben, ahol nem volt érvényes az alaptétel, ott $E(\varrho)$-hoz hozzávett „ideális számokat": ezek voltak hivatva azon elempárok legnagyobb

közös osztóját „pótolni”, amelyeknek nem létezett $E(\varrho)$-ban legnagyobb közös osztójuk. Kummer azt remélte, hogy az így kibővített halmazban már bármely két elemnek lesz legnagyobb közös osztója, és az alaptétel is teljesül.

Az ideális számok konstrukciójához Kummer a legnagyobb közös osztó alábbi tulajdonságából indult ki. Az egész számok körében tudjuk, hogy ha $\text{lnko}\{a, b\} = d$, akkor d többszörösei éppen az $au + bv$ alakú számok, és mint jeleztük, ugyanez a helyzet minden $E(\vartheta)$-ban is. Ennek alapján rögzített α és β esetén Kummer az

$$\{\alpha\xi + \beta\psi \mid \xi,\, \psi \in E(\vartheta)\}$$

számhalmazt tekintette az α-hoz és β-hoz tartozó ideális számnak; ez mai terminológiával éppen az α és β által generált (α, β) ideál. Ha α-nak és β-nak létezik δ legnagyobb közös osztója, akkor ez a számhalmaz megegyezik a δ többszöröseivel, így „azonosítható” δ-val. Ha viszont nem létezik $\text{lnko}\{\alpha, \beta\}$, akkor ezzel az ideális számmal „pótoljuk” a legnagyobb közös osztó hiányát. Ezután Kummer az ideális számok (azaz az ideálok) körében épített ki megfelelő számelméletet (ezzel a 11.4 pontban foglalkozunk), és így jelentős előrehaladást tudott elérni a Fermat-sejtéssel kapcsolatban.

Feladatok

11.2.1 Mutassuk meg, hogy az egész számok gyűrűjében az alábbi részhalmazok főideált alkotnak, és adjuk meg ezek egy-egy generátorelemét:

a) $(30, 50, 75)$; b) $(20) \cap (30)$.

11.2.2 Tekintsük a Gauss-egészek G gyűrűjét.

a) Egy adott nemnulla főideál hányféleképpen generálható egy elemmel?

b) Hány olyan főideál van, amelynek eleme $22 + 6i$?

11.2.3 Legyen R tetszőleges kommutatív, egységelemes, nullosztómentes gyűrű, és a, $b \in R$. Mutassuk meg, hogy

$$a + b \in (a) \cap (b) \iff (a) = (b).$$

11.2.4 Tekintsük az $E(\sqrt{-5})$ gyűrűt.

a) Bizonyítsuk be, hogy a $2 + 2\sqrt{-5}$ és 6 elemeknek nem létezik legnagyobb közös osztója.

b) Adjuk meg az összes olyan főideált, amely tartalmazza a $(2+2\sqrt{-5}, 6)$ ideált.

c) Mutassunk példát olyan α, β elemre, amelyeknek létezik δ legnagyobb közös osztójuk, de $(\alpha, \beta) \neq (\delta)$.

11.3. Alaptételes gyűrű, főideálgyűrű, euklideszi gyűrű

Ebben a pontban a számelmélet alaptételének a kérdésével foglalkozunk.

A felbonthatatlan (más néven irreducibilis) elem, illetve a prím fogalmát tetszőleges R (kommutatív, egységelemes, nullosztómentes) gyűrűben ugyanúgy értelmezzük, mint a korábban vizsgált konkrét gyűrűk esetén (lásd az egész számoknál az 1.4.1, illetve 1.4.2, vagy a Gauss-egészeknél a 7.4.10, illetve 7.4.11 Definíciókat).

Az, hogy R-ben érvényes a számelmélet alaptétele (más néven az egyértelmű prímfaktorizáció), a szokásos módon azt jelenti, hogy R-ben a nullán és az egységeken kívül minden elem felírható véges sok felbonthatatlan szorzataként, és ez az előállítás a tényezők sorrendjétől és egységszeresektől eltekintve egyértelmű (lásd például az 1.5.1 Tétel megfogalmazását).

Mint a könyv különböző fejezeteiben számos alkalommal rámutattunk, a számelméleti vizsgálatoknak (az alkalmazások szempontjából is) az egyik kulcskérdése, hogy egy adott gyűrűben érvényes-e a számelmélet alaptétele. A $\mathbf{Z}$-beli alaptételre az egész számok számelméletének szinte minden fejezete támaszkodik. Az $x^2 + y^2 = n$, illetve $x^3 + y^3 = z^3$ diofantikus egyenletek vizsgálatánál azt használtuk fel, hogy a Gauss-, illetve Euler-egészeknél érvényes az alaptétel. A 11.2 pontban jeleztük, hogy a Fermat-sejtés bizonyítása lényegesen könnyebben ment volna, ha bizonyos algebrai számtestek algebrai egészeire igaz lenne az alaptétel. A racionális együtthatós polinomok számelméletének az alaptételhez kapcsolódó egyes vonatkozásai fontos szerepet játszottak az algebrai számok vizsgálatánál.

Az alábbiakban először szükséges és elégséges feltételt adunk arra, hogy egy gyűrűben érvényes legyen az alaptétel (11.3.1 Tétel). Ezután megmutatjuk, hogy a maradékos osztás elvégezhetőségéből mindig következik az alaptétel. Ennek igazolása kissé eltér az egész számoknál, Gauss-egészeknél stb. látott úttól: belátjuk, hogy a maradékos osztás elvégezhetősége esetén a gyűrű minden ideálja főideál (11.3.5 Tétel), valamint bebizonyítjuk, hogy az ilyen tulajdonságú gyűrűkben mindig igaz az alaptétel (11.3.3 Tétel).

A bizonyítások során számos olyan rész lesz, amely szó szerint megegyezik az egész számoknál látott gondolatmenettel, így ezekre csak utalni fogunk, és nem ismételjük meg őket.

Mielőtt rátérnénk a jelzett általános tételekre, a felbonthatatlan és a prím kapcsolatáról ejtünk még néhány szót. A számelmélet alaptételének *megfogalmazás*ában a két fogalom közül csak a „felbonthatatlan” szerepel, a „prím”-re nincs szükség. Az alaptétel *érvényesség*e azonban szoros összefüggésben áll a prím és a felbonthatatlan közötti viszonnyal.

Minden R (kommutatív, egységelemes, nullosztómentes) gyűrűben teljesül, hogy egy prím szükségképpen felbonthatatlan, ez az 1.4.3 Tétel bizonyításának első részében látott módon igazolható. Az állítás megfordítása nem minden gyűrűben igaz, például $E(\sqrt{-5})$-ben, ahol nem érvényes a számelmélet alaptétele, a 2 felbonthatatlan, de nem prím. Láttuk ugyanakkor, hogy az egészek, Gauss-egészek, Euler-egészek gyűrűjében minden felbonthatatlan egyben prím is, és ez volt a döntő lépés a számelmélet alaptétele egyértelműségi részének a bizonyításához. Az alábbi tételből kiderül, hogy az alaptétel fennállásának az általános esetben is az egyik lényeges feltétele éppen az, hogy minden felbonthatatlan egyben prím is legyen.

11.3.1 Tétel **T 11.3.1**

Egy R (kommutatív, egységelemes, nullosztómentes) gyűrűben akkor és csak akkor érvényes a számelmélet alaptétele, ha

(i) főideáloknak szigorúan növő

$$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

lánca nem lehet végtelen, és

(ii) minden felbonthatatlan elem prím. ♣

Bizonyítás: Először az (i) és (ii) feltételek elégségességét igazoljuk.

Az egyértelműség (ii)-ből pontosan ugyanúgy következik, mint az 1.5.1 Tételnél az egyértelműségre adott első bizonyításban.

A felbonthatósághoz (i)-et használjuk fel. Legyen a az R-nek tetszőleges, a 0-tól és az egységektől különböző eleme. Első lépésként azt mutatjuk meg, hogy a-nak létezik felbonthatatlan osztója.

Ha a felbonthatatlan, akkor készen vagyunk. Ha nem, akkor $a = a_1 b_1$, ahol a_1 és b_1 egyike sem egység. Ekkor a 11.2.1 Tétel szerint $(a) \subset (a_1)$, és itt szigorú tartalmazás áll fenn, hiszen b_1 nem egység.

Ha a_1 felbonthatatlan, akkor a_1 az a-nak egy felbonthatatlan osztója. Ha a_1 nem felbonthatatlan, akkor $a_1 = a_2 b_2$, ahol a_2 és b_2 egyike sem egység. Ekkor $(a_1) \subset (a_2)$ (szigorú tartalmazással).

Megmutatjuk, hogy a gondolatmenetet hasonlóan folytatva, valamelyik a_i már szükségképpen felbonthatatlan. Ha ugyanis ez nem teljesülne, akkor

$$(a) \subset (a_1) \subset \ldots \subset (a_j) \subset \ldots$$

főideáloknak egy végtelen, szigorúan növő láncát jelentené, ami ellentmond (i)-nek. Ezzel igazoltuk, hogy a-nak létezik felbonthatatlan osztója.

Most belátjuk, hogy a előáll felbonthatatlanok szorzataként. Ha a felbonthatatlan, akkor készen vagyunk. Egyébként az előzőek szerint $a = p_1c_1$, ahol p_1 felbonthatatlan és c_1 nem egység. Mivel p_1 sem egység, ezért $(a) \subset (c_1)$ (szigorú tartalmazással).

Ha c_1 felbonthatatlan, akkor az $a = p_1c_1$ felírásban mindkét tényező felbonthatatlan, tehát készen vagyunk. Egyébként $c_1 = p_2c_2$, ahol p_2 felbonthatatlan és c_2 nem egység. Innen $(c_1) \subset (c_2)$ (szigorú tartalmazással).

Az eljárást folytatva előbb-utóbb valamelyik c_i szükségképpen egység, ugyanis különben az

$$(a) \subset (c_1) \subset \ldots \subset (c_j) \subset \ldots$$

végtelen, szigorúan növő főideállánc ellentmondana az (i) feltételnek. Ez azt jelenti, hogy az a-t előállítottuk felbonthatatlanok szorzataként.

Rátérve a szükségességre, tegyük fel, hogy R-ben igaz az alaptétel. Ekkor (ii) pontosan ugyanúgy bizonyítható, mint az 1.5.8 feladat megoldásában.

Végül (i) igazolásához tegyük fel indirekt, hogy létezik egy

$$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

végtelen, szigorúan növő főideállánc. Itt $a_2 \neq 0$, és $a_3, a_4, \ldots$ az a_2-nek végtelen sok olyan osztója, amelyek közül semelyik kettő sem egységszerese egymásnak. Ez azonban lehetetlen, mert ha $a_2 = p_1 \ldots p_k$, ahol a p_i-k felbonthatatlanok, akkor az alaptétel miatt a_2 minden osztója (vagy egység, vagy pedig) néhány p_i szorzatának az egységszerese (illetve ha a_2 egység, akkor minden osztója is egység). ■

Megjegyzés: A korábbiakban több olyan példa is szerepelt, ahol a számelmélet alaptételének az *egyértelműségi* része nem teljesült (lásd a 10.3.5 és 10.3.6 Tételt, valamint a 11.2 pontban a Fermat-sejtéshez kapcsolódó részt). Könnyű azonban olyan gyűrűre is példát mutatni, ahol a *felbonthatóság*gal van baj: az összes algebrai egész E gyűrűjében egyáltalán nem léteznek felbonthatatlanok (lásd a 11.3.1 feladatot), és így a 0-tól és egységektől különböző elemek egyáltalán nem bonthatók fel felbonthatatlanok szorzatára.

Most megmutatjuk, hogy ha R-ben minden ideál főideál, akkor R-ben érvényes a számelmélet alaptétele.

11.3.2 Definíció **D 11.3.2**

Egy R (kommutatív, egységelemes, nullosztómentes) gyűrű *főideálgyűrű*, ha minden ideálja főideál. ♣

11.3.3 Tétel **T 11.3.3**

Főideálgyűrűben érvényes a számelmélet alaptétele. ♣

Bizonyítás: Megmutatjuk, hogy főideálgyűrűben teljesül a 11.3.1 Tétel (i) és (ii) feltétele.

(i) Tegyük fel indirekt, hogy létezik egy

$$(a_1) \subset (a_2) \subset \ldots \subset (a_j) \subset \ldots$$

végtelen, szigorúan növő főideállánc. Egyszerű számolással adódik, hogy $A = \bigcup_{j=1}^{\infty}(a_j)$ is ideál (lásd a 11.3.4 feladatot). Mivel R főideálgyűrű, ezért A is főideál, $A = (b)$. Ekkor

$$b \in A = \bigcup_{j=1}^{\infty}(a_j)$$

miatt van olyan k, amelyre $b \in (a_k)$, azaz $(b) \subseteq (a_k)$. Így

$$A = (b) \subseteq (a_k) \subset (a_{k+1}) \subset \bigcup_{j=1}^{\infty}(a_j) = A,$$

ami ellentmondás.

(ii) Először azt igazoljuk, hogy bármely a és b elemnek létezik legnagyobb közös osztója. Mivel az (a, b) ideál is főideál, azaz $(a, b) = (d)$, így a 11.2.2 Tételből következik, hogy $d = \text{lnko}\{a, b\}$.

A legnagyobb közös osztó létezéséből már következik (ii): lásd az 1.3.4 Tételre az 1.3.11 feladat megoldásában adott bizonyítást, az 1.3.9 Tétel bizonyítását és végül az 1.4.3 Tétel bizonyításának II. részét. ■

Megjegyzések: 1. Létezik olyan gyűrű, amely nem főideálgyűrű, és mégis érvényes benne a számelmélet alaptétele, a legegyszerűbb ilyen példa $\mathbf{Z}[x]$. A 11.1 pontban láttuk, hogy $\mathbf{Z}[x]$-ben a $(2, x)$ nem főideál, ugyanakkor $\mathbf{Z}[x]$-ben igaz az alaptétel (ez visszavezethető a $\mathbf{Z}$-beli és a $\mathbf{Q}[x]$-beli alaptételre, ugyanis a racionális együtthatós polinomokra vonatkozó Gauss-lemmából következik, hogy egy f polinom akkor és csak akkor irreducibilis $\mathbf{Z}$ felett, ha f vagy egy olyan konstans, amely prímszám, vagy pedig az f együtthatói relatív prímek és f irreducibilis $\mathbf{Q}$ felett).

2. Az algebrai számtestekben az alaptételes gyűrűk és a főideálgyűrűk egybeesnek: egy algebrai számtestben az algebrai egészek $E(\vartheta)$ gyűrűje akkor

és csak akkor főideálgyűrű, ha érvényes a számelmélet alaptétele (lásd a 11.3.9b feladatot).

Végül rátérünk a maradékos osztás általános megfogalmazására, és annak igazolására, hogy ha R-ben elvégezhető a maradékos osztás, akkor R főideálgyűrű, tehát (a 11.3.3 Tétel alapján) R-ben érvényes a számelmélet alaptétele.

11.3.4 Definíció **D 11.3.4**

Egy R (kommutatív, egységelemes, nullosztómentes) gyűrű *euklideszi gyűrű*, ha minden $c \in R$ elemhez hozzá tudunk rendelni egy $f(c)$ nemnegatív egész számot úgy, hogy $f(c) = 0 \iff c = 0$, továbbá minden $a, b \in R$, $b \neq 0$ esetén létezik olyan $q, r \in R$, hogy

$$a = bq + r \qquad \text{és} \qquad f(r) < f(b). \ \clubsuit \tag{1}$$

Megjegyzések: 1. Az euklideszi gyűrű definícióját szokás abban a formában is megadni, hogy R-ben csak a 0-tól különböző elemekhez rendelünk hozzá egy $f(c)$ nemnegatív egész számot, és ekkor (1)-ben $f(r) < f(b)$ mellett az $r = 0$ lehetőséget is megengedjük. Ez nyilván ekvivalens a 11.3.4 Definícióval.

2. A 11.3.4 Definícióban nem szükséges kikötni, hogy az R egységelemes legyen: a maradékos osztás elvégezhetőségéből következik, hogy a gyűrűnek létezik egységeleme (lásd a 11.3.6 feladatot).

3. Az alábbiakban felsorolunk néhány olyan korábban már vizsgált gyűrűt, amelyekben elvégezhető a maradékos osztás. Ezeknél a megfelelő f függvény általában további hasznos tulajdonságokkal is rendelkezett, például $f(ab) = f(a)f(b)$ vagy legalábbis $f(a) \leq f(ab)$ teljesült. Ilyen tulajdonságokat azonban az euklideszi gyűrű definíciójában nem kell kikötni.

Példák:

P1 Az egész számoknál az $f(c) = |c|$ választás megfelel, azaz $|r| < |b|$ elérhető. Megjegyezzük, hogy ebben az esetben a hányados és a maradék általában nem egyértelmű, például $a = 33$ és $b = 5$ esetén

$$33 = 6 \cdot 5 + 3 = 7 \cdot 5 + (-2).$$

Az 1.2.1, illetve 1.2.1A Tételekben azért szerepeltettük az $|r| < |b|$-nél szigorúbb $0 \leq r < |b|$, illetve $-|b|/2 < r \leq |b|/2$ előírást, hogy a hányados és a maradék *egyértelmű* legyen. Az egyértelműségnek azonban az alaptétel bizonyítása szempontjából nincs jelentősége.

P2 A Gauss- vagy Euler-egészeknél megfelel $f(c) = N(c)$. (A 7.4.8 Tétel bizonyítása során láttuk, hogy a hányados és a maradék általában nem egyértelmű.)

P3 $E(\sqrt{2})$-ben megfelel $f(c) = |N(c)|$.

P4 Test feletti polinomgyűrűben a fokszám szerint elvégezhető a maradékos osztás. Ahhoz, hogy formailag pontosan eleget tegyünk a 11.3.4 Definíciónak, legyen $f(0) = 0$ és $f(c) = 1 + \deg c$, ha $c \neq 0$.

P5 A véges tizedes törtek is euklideszi gyűrűt alkotnak, lásd az 1.5.5c feladatot.

11.3.5 Tétel **T 11.3.5**

Ha R euklideszi gyűrű, akkor R főideálgyűrű. ♣

Bizonyítás: Azt kell igazolni, hogy az R tetszőleges I ideálja főideál.

Ha I csak a 0-ból áll, akkor $I = (0)$. Egyébként tekintsük I-ben a 0-tól különböző c elemekhez rendelt $f(c)$ értékeket. Mivel ezek pozitív egész számok, így van közöttük legkisebb, legyen ez $f(b)$ (itt a $b(\neq 0)$ elem nem egyértelmű). Megmutatjuk, hogy $I = (b)$.

Mivel $b \in I$, ezért $(b) \subseteq I$. Megfordítva, legyen a az I ideál tetszőleges eleme. Azt kell megmutatnunk, hogy $a \in (b)$, vagyis $b \mid a$.

Osszuk el a-t maradékosan b-vel: létezik olyan q, $r \in R$, amelyre (1) teljesül. Mivel a, $b \in I$ és I ideál, ezért $r = a - bq \in I$. Továbbá $f(b)$ minimális volt és $f(r) < f(b)$, így csak $r = 0$ lehetséges, azaz valóban $b \mid a$. ■

Megjegyzés: A 11.3.5 Tétel megfordítása nem igaz, léteznek olyan főideálgyűrűk, amelyek nem euklideszi gyűrűk: az algebrai számtestek algebrai egészeiből álló gyűrűk közül bizonyítottan ilyenek az

$$E(\sqrt{-19}), \quad E(\sqrt{-43}), \quad E(\sqrt{-67}) \quad \text{és} \quad E(\sqrt{-163}) \tag{2}$$

(lásd a 11.3.10 feladatot).

Általában igen nehéz annak az eldöntése, hogy egy R gyűrű euklideszi-e vagy sem. Természetesen, ha találunk egy megfelelő f-et, akkor R euklideszi gyűrű, ha pedig R-ben nem érvényes a számelmélet alaptétele vagy R nem főideálgyűrű, akkor a 11.3.3 és 11.3.5 Tételekből következik, hogy R nem lehet euklideszi gyűrű sem. Nemigen van támpontunk azonban, ha egy főideálgyűrűről akarjuk kimutatni, hogy nem euklideszi. Ekkor ugyanis nemcsak azt kell igazolni, hogy egy adott, esetleg „természetes módon” szóba jövő f függvény nem teljesíti a 11.3.4 Definícióban előírt kikötéseket, hanem ezt *minden lehetséges* f-re be kell látni.

Vizsgáljuk meg mindezt kicsit behatóbban az algebrai számtestek egészeiből álló gyűrűk esetén. A 11.3.3 Tétel utáni 2. megjegyzésben jeleztük, hogy ha $E(\vartheta)$-ban érvényes a számelmélet alaptétele, akkor $E(\vartheta)$ főideálgyűrű (lásd a 11.3.9b feladatot). Ami a maradékos osztást illeti, az eddigi konkrét esetekben (Gauss-egészek, Euler-egészek, $E(\sqrt{2})$ stb.) ezt a norma abszolút értéke szerint próbáltuk elvégezni. Voltak olyan alaptételes $E(\vartheta)$ gyűrűk is, amikor ez nem sikerült (lásd a 10.3.6 Tételt). Ilyenkor azonban még mindig nyitva áll annak a lehetősége, hogy valamilyen más f függvény szerint mégis van maradékos osztás. Ezzel kapcsolatos jelenlegi ismereteinket a következő paradox helyzet jellemzi:

(A) Bizonyos mély sejtések azt valószínűsítik, hogy a másodfokú képzetes számtestektől eltekintve, *minden* alaptételes $E(\vartheta)$ euklideszi gyűrű, azaz létezik egy alkalmas f függvény, amely kielégíti a 11.3.4 Definíciót (akkor is, amikor $|N(\alpha)|$ nem felel meg erre a célra).

(B) Azonban hosszú ideig egyetlen konkrét $E(\vartheta)$ sem volt ismert, amelyben igaz a számelmélet alaptétele, nem euklideszi a $|N(\alpha)|$ szerint, és mégis elvégezhető valamilyen másféle maradékos osztás. Az első ilyen bizonyított példa az $E(\sqrt{69})$ volt 1994-ben, amit aztán nagyon sok másik követett. Ma már például tudjuk, hogy legfeljebb 2(!) kivételtől eltekintve minden olyan másodfokú valós számtest euklideszi, amelyben igaz a számelmélet alaptétele.

A kivételként említett másodfokú képzetes számtestekre megmutatható, hogy ha $E(\vartheta)$ euklideszi, akkor $|N(\alpha)|$ szerint is elvégezhető a maradékos osztás (lásd a 11.3.10 feladatot). Így a 10.3.6 Tételből következik, hogy a (2)-ben felsorolt négy példa főideálgyűrű, de nem euklideszi gyűrű.

Feladatok

11.3.1 Legyen E az összes algebrai egész gyűrűje.

a) Jellemezzük az E-beli egységeket a minimálpolinomjuk segítségével.

b) Mutassuk meg, hogy E-ben nem léteznek felbonthatatlanok, és így nem igaz a számelmélet alaptétele.

11.3.2 Számelméleti kérdéseket egy T (kommutatív) testben is vizsgálhatunk (csak ennek nincs sok értelme, amint ez az alábbiakból is kiderül).

a) Milyen $a, b \in T$ esetén teljesül $a \mid b$?

b) Mik lesznek T-ben az egységek, a felbonthatatlanok, illetve a prímek?

c) Mutassuk meg, hogy T-ben érvényes a számelmélet alaptétele, ráadásul T főideálgyűrű, sőt euklideszi gyűrű.

11.3.3 Legyen W a racionális számoknak a páratlan nevezőjű törtekből álló részhalmaza.

a) Bizonyítsuk be, hogy W-ben egységszerestől eltekintve egyetlen felbonthatatlan elem létezik.

b) Hol bukik meg W-ben az a gondolatmenet, amellyel az egész számok körében végtelen sok prímszám létezését igazoltuk (lásd az 5.1.1 Tételt).

c) Mutassuk meg, hogy W euklideszi gyűrű.

d) Határozzuk meg W összes ideálját.

11.3.4 Legyenek $I_1 \subseteq I_2 \subseteq \dots$ tetszőleges ideálok egy R gyűrűben. Mutassuk meg, hogy ekkor $\bigcup_{j=1}^{\infty} I_j$ is ideál R-ben.

M 11.3.5 Legyen R kommutatív, egységelemes, nullosztómentes gyűrű. Bizonyítsuk be, hogy az $R[x]$ polinomgyűrű akkor és csak akkor főideálgyűrű, ha R test.

11.3.6 Mutassuk meg, hogy az euklideszi gyűrű 11.3.4 Definíciójában nem szükséges kikötni, hogy R egységelemes, ez a többi feltételből következik.

11.3.7 Legyen R euklideszi gyűrű, f egy olyan függvény, amely teljesíti a 11.3.4 Definíció előírásait és k az f függvény legkisebb pozitív értéke. Melyek igazak az alábbi állítások közül?

a) Ha $f(c) = k$, akkor c egység.

b) Ha c egység, akkor $f(c) = k$.

11.3.8 Mutassuk meg, hogy az egész számok körében (nemcsak az abszolút érték, hanem) az alábbi f függvény szerint is elvégezhető a maradékos osztás:

$$f(c) = \begin{cases} 1 + \lfloor \log_2 |c| \rfloor, & \text{ha } c \neq 0; \\ 0, & \text{ha } c = 0, \end{cases}$$

azaz

$$f(0) = 0, \qquad f(\pm 1) = 1, \qquad f(\pm 2) = f(\pm 3) = 2,$$
$$f(\pm 4) = f(\pm 5) = f(\pm 6) = f(\pm 7) = 3, \qquad \dots$$

11.3.9

M *a) Tegyük fel, hogy az R (kommutatív, egységelemes, nullosztómentes) gyűrűben érvényes a számelmélet alaptétele, továbbá minden $I \neq 0$ ideálra az R/I faktorgyűrűnek véges sok eleme van. Bizonyítsuk be, hogy R főideálgyűrű.

b) Bizonyítsuk be, hogy ha ϑ algebrai és $E(\vartheta)$-ban érvényes a számelmélet alaptétele, akkor $E(\vartheta)$ főideálgyűrű.

M*11.3.10 Legyen t negatív négyzetmentes egész szám. Bizonyítsuk be, hogy a $\mathbf{Q}(\sqrt{t})$ másodfokú képzetes bővítés algebrai egészei akkor és csak akkor alkotnak euklideszi gyűrűt, ha $t = -1, -2, -3, -7$ vagy -11.

11.4. Ideálok oszthatósága

Ebben a pontban egy R (kommutatív, egységelemes, nullosztómentes) gyűrű ideáljai között értelmezünk szorzást, majd ennek segítségével oszthatóságot, ezután pedig áttekintjük az ideálokra ebből adódó számelméleti fogalmak (legnagyobb közös osztó, felbonthatatlan ideál, prímideál) jelentését és fontosabb tulajdonságait.

Mivel az ideálok közötti számelmélet kiépítésével a fő célunk az $E(\vartheta)$ gyűrűk további vizsgálata, ezért a fogalmak bevezetése során olyan megszorító feltevésekkel is fogunk élni, amelyek $E(\vartheta)$ ideáljaira teljesülnek, azonban nem minden R-ben igazak.

11.4.1 Definíció **D 11.4.1**

Legyen A és B az R (kommutatív, egységelemes, nullosztómentes) gyűrű két tetszőleges ideálja. Ekkor A és B *szorzat*át a következőképpen értelmezzük:

$$AB = \Big\{ \sum_{i=1}^{n} a_i b_i \;\mid\; n = 1, 2, \ldots,\ a_i \in A,\ b_i \in B,\ i = 1, \ldots, n \Big\}. \quad \clubsuit \qquad (1)$$

A két ideál szorzata tehát az A-beli és B-beli elemek szorzataiból képzett összes lehetséges (akárhány tagú) összegek halmaza.

Az ideálok szorzásának néhány fontos tulajdonságát az alábbi tételben foglaljuk össze.

11.4.2 Tétel **T 11.4.2**

(i) Az A és B ideálok AB szorzata a legszűkebb ideál, amely az összes ab alakú elemet tartalmazza, ahol $a \in A$ és $b \in B$.

(ii) Végesen generált ideálok szorzata is végesen generált.

(iii) Főideálok szorzata főideál.

(iv) $AB \subseteq A \cap B$.

(v) Az R gyűrű ideáljainak szorzása kommutatív és asszociatív művelet, egységelem az $(1) = R$ triviális ideál:

$$AB = BA, \qquad (AB)C = A(BC), \qquad (1)A = A(1) = A. \tag{2}$$

Inverze csak az egységelemnek létezik, továbbá

$$AB = (0) \iff A = (0) \quad \text{vagy } B = (0). \ \clubsuit$$

Bizonyítás: (i) A következőket kell igazolni:
(a) AB ideál;
(b) $a \in A$, $b \in B \Longrightarrow ab \in AB$;
(c) ha egy I ideál tartalmazza az összes ab alakú elemet, ahol $a \in A$, $b \in B$, akkor $AB \subseteq I$.

(a) Megmutatjuk, hogy AB eleget tesz a 11.1.1 Definíció előírásainak. Két $\sum_{i=1}^{n} a_i b_i$ alakú elem összege nyilván ismét ilyen alakú. Egy ilyen elem ellentettje, illetve egy $r \in R$ elemmel való szorzata átírható a

$$-\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (-a_i) b_i, \qquad \text{illetve} \qquad r \sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} (r a_i) b_i$$

alakba, és A ideáltulajdonsága miatt $-a_i$, illetve $ra_i \in A$.

(b) Az (1) képletben $n = 1$ esetén éppen az ab alakú elemeket kapjuk.

(c) Ha egy I ideál tartalmazza az $a_i b_i$ elemeket, akkor az ideáltulajdonság miatt ezek összegét, azaz minden $\sum_{i=1}^{n} a_i b_i$ alakú elemet is tartalmaznia kell, tehát valóban $AB \subseteq I$.

(ii) Megmutatjuk, hogy ha

$$A = (\alpha_1, \ldots, \alpha_k) \qquad \text{és} \qquad B = (\beta_1, \ldots, \beta_m),$$

akkor

$$AB = (\alpha_1\beta_1,\ \alpha_1\beta_2,\ \ldots,\ \alpha_i\beta_j,\ \ldots,\ \alpha_k\beta_m),$$

vagyis az A és B generátorelemeinek szorzatai az AB ideál (egyik lehetséges) generátorrendszerét alkotják.

Az $\alpha_i\beta_j$ elemek definíció szerint elemei AB-nek, így az általuk generált ideál része AB-nek.

A fordított irányú tartalmazáshoz (i) alapján elég azt belátni, hogy minden ab alakú elem, ahol $a \in A$, $b \in B$, benne van az $\alpha_i\beta_j$-k által generált

ideálban, vagyis ab felírható az $\alpha_i\beta_j$ elemek R-beli együtthatós kombinációjaként. Ez valóban teljesül, ugyanis (alkalmas r_i, $s_j \in R$ elemekkel)

$$ab = \Big(\sum_{i=1}^{k} r_i\alpha_i\Big)\Big(\sum_{j=1}^{m} s_j\beta_j\Big) = \sum_{i=1}^{k}\sum_{j=1}^{m}(r_is_j)(\alpha_i\beta_j).$$

(iii) A (ii)-re adott bizonyításból a $k = m = 1$ speciális esetben kapjuk, hogy $(\alpha)(\beta) = (\alpha\beta)$.

(iv) Az A ideáltulajdonsága miatt bármely $a_i \in A$ és $b_i \in B$ esetén $a_ib_i \in A$, és így $\sum_{i=1}^{n} a_ib_i \in A$, tehát $AB \subseteq A$. Ugyanígy kapjuk, hogy $AB \subseteq B$.

(v) A (2)-ben felsorolt azonosságok azonnal következnek az ideálok szorzásának definíciójából (és az R gyűrű tulajdonságaiból).

Az $R = (1)$ egységelem inverze önmaga. Megfordítva, ha az I ideálnak létezik inverze, azaz alkalmas J ideálra $JI = R$, akkor (iv) alapján $R \subseteq I$, tehát $I = R$.

Ha $A = (0)$ vagy $B = (0)$, akkor az AB definíciójában szereplő összes összeg 0, tehát $AB = (0)$. Ha viszont A-nak, illetve B-nek létezik egy $a \neq 0$, illetve $b \neq 0$ eleme, akkor R nullosztómentessége miatt $ab \neq 0$ és $ab \in AB$, tehát $AB \neq (0)$. ■

Megjegyzések: 1. Az A és B ideál elemeiből képzett ab szorzatok általában nem alkotnak ideált (lásd a 11.4.1a feladatot), ezért kellett AB definíciójában az ilyen szorzatokból képzett összegeket venni.

2. Az ideálok között (egyelőre) csak szorzást értelmeztünk. Az összeadás is definiálható, ezzel kapcsolatban lásd a 11.4.5 Tétel utáni 4. megjegyzést. Előrebocsátjuk azonban, hogy ez az összeadás nem rendelkezik a szokásos „jó" tulajdonságokkal (csak a nullelemnek lesz ellentettje), és így az R ideáljai az ideálok összeadására és szorzására nézve *nem* alkotnak gyűrűt.

Példák:

P1 Legyen $R = \mathbf{Z}[x]$, és A, illetve B álljon azokból a polinomokból, amelyek konstans tagja páros, illetve osztható 3-mal. Ekkor AB azoknak a polinomoknak a halmaza, amelyek konstans tagja osztható 6-tal:

$$\begin{aligned} AB = (2,x)(3,x) &= (6,\, 2x,\, 3x,\, x^2) = \\ &= (6,\, 2x,\, 3x-2x,\, x^2) = (6,\, 2x,\, x,\, x^2) = (6,x). \end{aligned}$$

P2 Legyen $R = E(\sqrt{-5})$, $A = (3,\ 1+\sqrt{-5})$ és $B = (3,\ 1-\sqrt{-5})$. Ekkor AB a (3) főideál:

$$AB = (3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5}) = (9,\ 3+3\sqrt{-5},\ 3-3\sqrt{-5},\ 6) =$$
$$= (9-6,\ 3+3\sqrt{-5},\ 3-3\sqrt{-5},\ 6) = (3).$$

Az ideálok szorzása lehetővé teszi, hogy az R gyűrű ideáljai között oszthatóságot értelmezzünk:

11.4.3 Definíció **D 11.4.3**

A B ideál *osztó*ja az A ideálnak, ha létezik olyan C ideál, amellyel $BC = A$. Ezt a szokásos módon $B \mid A$ jelöli. ♣

Megjegyzések: 1. Könnyen adódik, hogy főideálok oszthatósága ekvivalens a generátorelemek (R-beli) oszthatóságával:

$$(\beta) \mid (\alpha) \iff \beta \mid \alpha.$$

Sőt, ha $\beta \neq 0$ és $(\alpha) = (\beta)C$, akkor C is szükségképpen főideál, $C = (\gamma)$, ahol γ úgy is választható, hogy $\alpha = \beta\gamma$ teljesüljön (lásd a 11.4.3 feladatot). Ez azt jelenti, hogy az ideálok oszthatósága az R-beli oszthatóság általánosításának is tekinthető.

2. Az oszthatóság néhány elemi tulajdonságát a 11.4.2 feladatban tárgyaljuk. Ezek közül külön is kiemeljük, hogy

$$B \mid A \Longrightarrow A \subseteq B. \tag{3}$$

Az előző megjegyzés és a 11.2.1 Tétel alapján főideálokra (3) megfordítása is érvényes, tetszőleges ideálokra azonban (3) megfordítása általában nem igaz, lásd a 11.4.6 feladatot.

A továbbiakban csak olyan R gyűrűkkel foglalkozunk, amelyekben az ideálok szorzásánál érvényes az egyszerűsítési szabály:

$$AB = AC,\ \ A \neq (0) \Longrightarrow B = C, \tag{4}$$

valamint igaz (3) megfordítása is:

$$B \mid A \iff A \subseteq B. \tag{5}$$

A 11.5 pontban megmutatjuk, hogy a fő vizsgálati irányunkat képező $E(\vartheta)$ típusú gyűrűk eleget tesznek a (4) és (5) követelménynek.

Most két ideál legnagyobb közös osztóját definiáljuk, ez a szokásos módon olyan közös osztót jelent, amely minden közös osztónak többszöröse:

11.4.4 Definíció **D 11.4.4**

Az A és B ideálok legnagyobb közös osztója a D ideál, ha

(i) $D \mid A$, $D \mid B$; és

(ii) ha egy C ideálra $C \mid A$, $C \mid B$ teljesül, akkor $C \mid D$. ♣

11.4.5 Tétel **T 11.4.5**

Bármely A és B ideálnak létezik és egyértelmű a D legnagyobb közös osztója, és

$$D = \{a + b \mid a \in A,\ b \in B\}. \ \clubsuit \tag{6}$$

Bizonyítás: A legnagyobb közös osztó definícióját (5) alapján a tartalmazás segítségével is megfogalmazhatjuk: a legnagyobb közös osztó a legszűkebb olyan ideál, amely A-t és B-t is tartalmazza. Könnyen adódik (lásd a 11.4.4a feladatot), hogy a (6) képletben szereplő D az egyetlen olyan ideál, amely rendelkezik ezzel a tulajdonsággal. ■

Megjegyzés: 1. A bizonyításban megfogalmazott tulajdonsága alapján D-t tekinthetjük az A és B ideálok által generált ideálnak. Ennek megfelelően a $D = (A, B)$ jelölés összhangban van mind a legnagyobb közös osztóra, mind pedig a generált ideálra alkalmazott szokásos jelölésmóddal.

2. Ha A és B főideál, $A = (\alpha)$, $B = (\beta)$, akkor a (6) képlet szerint a legnagyobb közös osztójuk $D = \{r\alpha + s\beta \mid r, s \in R\}$, ami éppen az (α, β) ideál. Ez ismét rámutat arra, hogy a két elem által generált ideál a legnagyobb közös osztó fogalom általánosításának tekinthető.

3. Ha A és B végesen generált ideál,

$$A = (\alpha_1, \ldots, \alpha_k) \qquad \text{és} \qquad B = (\beta_1, \ldots, \beta_m),$$

akkor a (6) képlet szerint a legnagyobb közös osztójuk

$$D = (\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k,\ \beta_1,\ \beta_2,\ \ldots,\ \beta_m),$$

vagyis az A és B generátorelemei együttesen a D ideál (egyik lehetséges) generátorrendszerét alkotják.

4. A (6) képlet alapján D az A és B ideálok *összeg*eként is felfogható. Még egyszer hangsúlyozzuk, hogy az R ideáljai erre az összeadásra és a 11.4.1 Definícióban értelmezett szorzásra *nem* alkotnak gyűrűt (lásd a 11.4.4b feladatot).

Most rátérünk a felbonthatatlan ideál és a prímideál fogalmára, ezek tulajdonságaira és kapcsolatára.

Mindkét értelmezés a korábbi felbonthatatlan, illetve prím fogalomnak megfelelően történik. Mivel egyedül az $(1) = R$ ideálra igaz, hogy minden ideálnak osztója (lásd a 11.4.2e feladatot), ezért R ideáljai körében az (1) az egyetlen egység.

11.4.6 Definíció **D 11.4.6**

Az R gyűrű egy nemtriviális (azaz (0)-tól és (1)-től különböző) F ideálja *felbonthatatlan* ideál, ha **csak** úgy bontható fel két ideál szorzatára, hogy valamelyik tényező (1), azaz

$$F = AB \Longrightarrow A = (1) \text{ vagy } B = (1). \ \clubsuit \tag{7}$$

A (4) és (5) tulajdonság alapján azonnal adódik, hogy egy F nemtriviális ideál felbonthatatlansága az alábbi két feltétel bármelyikével is ekvivalens (itt A tetszőleges ideált jelöl):

F-nek csak triviális osztói léteznek, azaz

$$A \mid F \Longrightarrow A = (1) \text{ vagy } A = F, \tag{8}$$

illetve

nem létezik az F-et valódi módon tartalmazó nemtriviális ideál, azaz

$$F \subseteq A \subseteq R \Longrightarrow A = R \text{ vagy } A = F. \tag{9}$$

A (9) tulajdonsággal rendelkező ideálokat *maximális* ideáloknak szokás nevezni (olyan gyűrű esetén is, amikor az (5) feltétel nem teljesül).

11.4.7 Definíció **D 11.4.7**

Az R gyűrű egy P nemtriviális ideálja *prímideál*, ha csak úgy lehet osztója két ideál szorzatának, ha legalább az egyik tényezőnek osztója, azaz

$$P \mid AB \Longrightarrow P \mid A \text{ vagy } P \mid B. \ \clubsuit \tag{10}$$

A prímideál definícióját is átfogalmazhatjuk tartalmazásra (5) alapján: a (0)-tól és (1)-től különböző P ideál akkor és csak akkor prímideál, ha

$$AB \subseteq P \Longrightarrow A \subseteq P \text{ vagy } B \subseteq P. \tag{11}$$

További ekvivalens megfogalmazást jelent az

$$ab \in P \Longrightarrow a \in P \text{ vagy } b \in P \tag{12}$$

feltétel. A (11) és (12) tulajdonságok ekvivalenciája akkor is igaz, ha R-ben nem teljesül (5) (lásd a 11.4.7 feladatot), és ebben az esetben ezek valamelyikével szokás a prímideált értelmezni.

A (4) és (5) feltételek fennállása esetén a prímideálok megegyeznek a felbonthatatlan ideálokkal:

11.4.8 Tétel **T 11.4.8**

Egy P ideál akkor és csak akkor prímideál, ha felbonthatatlan ideál. ♣

Bizonyítás: Az 1.4.3 Tétel bizonyításának a gondolatmenetét követjük. Nyilván feltehetjük, hogy P nemtriviális ideál.

Először tegyük fel, hogy P prímideál, és lássuk be, hogy felbonthatatlan ideál is. Induljunk ki egy $P = AB$ szorzat-előállításból; azt kell igazolnunk, hogy $A = (1)$ vagy $B = (1)$.

Mivel $P = AB$, ezért $P \mid AB$ is igaz. Mivel P prímideál, ezért ebből $P \mid A$ vagy $P \mid B$ következik.

Ha $P \mid A$, akkor alkalmas C-vel $A = PC = ABC$. Ezt a nyilvánvaló $A = A(1)$ egyenlőséggel összehasonlítva kapjuk, hogy $ABC = A(1)$, ahonnan az $A \neq 0$ ideállal történő egyszerűsítés után $BC = (1)$ adódik. Ebből következik, hogy $B = (1)$ [és $C = (1)$].

A $P \mid B$ esetben ugyanígy nyerjük, hogy $A = (1)$.

Most tegyük fel, hogy P felbonthatatlan ideál, és lássuk be, hogy prímideál is. Induljunk ki egy $P \mid AB$ oszthatóságból; azt kell igazolnunk, hogy $P \mid A$ és $P \mid B$ közül legalább az egyik teljesül.

Ha $P \mid A$, akkor készen vagyunk. Ha $P \nmid A$, akkor P felbonthatatlansága miatt $(P, A) = (1)$.

Mivel $P \mid PB$ és $P \mid AB$, ezért $P \mid (PB, AB)$. A 11.4.4c feladat felhasználásával kapjuk, hogy

$$(PB, AB) = (P, A)B = (1)B = B, \qquad \text{és így} \qquad P \mid B. \ \blacksquare$$

Feladatok

Valamennyi feladatban A, B, illetve C egy R egységelemes, kommutatív, nullosztómentes gyűrű ideáljait jelöli. A legnagyobb közös osztóval, felbonthatatlan ideálokkal és prímideálokkal kapcsolatos feladatoknál — ha mást nem mondunk — eleve feltesszük, hogy R-ben érvényes a (4) és (5) tulajdonság is, azaz az ideálokra vonatkozó egyszerűsítési szabály, valamint az oszthatóság és a („fordított irányú") tartalmazás ekvivalenciája (mint jeleztük, ezek az $E(\vartheta)$ gyűrűkben teljesülnek).

11.4.1 Legyen H az A és B ideálok elemeiből képzett ab szorzatok halmaza: $H = \{ab \mid a \in A,\ b \in B\}$.

a) Mutassunk példát arra, hogy H nem feltétlenül ideál.

b) Bizonyítsuk be, hogy ha A és B közül legalább az egyik főideál, akkor H ideál (és így $H = AB$).

11.4.2 Igazoljuk az ideálok oszthatóságának alábbi elemi tulajdonságait:

a) Minden A-ra $A \mid A$.

b) $C \mid B,\ B \mid A \Longrightarrow C \mid A$.

c) $B \mid A \Longrightarrow A \subseteq B$.

d) $A \mid B,\ B \mid A \Longrightarrow A = B$.

e) Minden A-ra $B \mid A \iff B = (1)$.

11.4.3 Igazoljuk a főideálok oszthatóságára vonatkozó alábbi állításokat:

a) $(\beta) \mid (\alpha) \iff \beta \mid \alpha$.

b) Ha $\beta \neq 0$ és $(\alpha) = (\beta)C$, akkor C is szükségképpen főideál, $C = (\gamma)$, ahol γ úgy is választható, hogy $\alpha = \beta\gamma$ teljesüljön.

11.4.4 Legyen $D = \{a + b \mid a \in A,\ b \in B\}$.

a) Bizonyítsuk be, hogy D a legszűkebb olyan ideál, amely A-t és B-t is tartalmazza.

b) A D ideált az A és B ideálok összegének tekintve, mutassuk meg, hogy az ideálok összeadása kommutatív és asszociatív, nullelem a (0), de ellentettje csak a nullelemnek létezik.

Megjegyzés: Az a) rész alapján D felfogható az A és B által generált ideálnak, és így a tartalmazás és az oszthatóság kapcsolata szerint D az A és B legnagyobb közös osztója (lásd a 11.4.5 Tételt). Ebben a két szerepkörben D-re az (A, B) jelölést használjuk. A b) rész szempontjából a $D = A + B$ jelölés alkalmazása célszerű.

c) Igazoljuk az $A(B, C) = (AB, AC)$ (vagy a másik jelölésmód szerint az $A(B + C) = AB + AC$) disztributivitási azonosságot.

11.4.5 Definiáljuk ideálokra a legkisebb közös többszörös fogalmát, és igazoljuk, hogy a (4) és (5) tulajdonságok fennállása esetén bármely A és B ideálnak egyértelműen létezik az M legkisebb közös többszöröse, éspedig $M = A \cap B$.

11.4.6 Mutassunk példát olyan A és B ideálra, ahol $A \subseteq B$, de $B \not| A$.

11.4.7 Mutassuk meg, hogy a 11.4.7 Definíció után szereplő, a prímideálokra vonatkozó (11) és (12) tulajdonságok bármely R (kommutatív, egységelemes, nullosztómentes) gyűrűben ekvivalensek (akkor is, ha R-ben nem érvényes a (4) és/vagy (5) feltétel).

11.4.8 Tekintsük az $E(\sqrt{-5})$ gyűrűt.

M a) Határozzuk meg az alábbi ideálok összes osztóját:

a1: $(2, 1+\sqrt{-5})$; a2: (2); a3: $(1+\sqrt{-5})$.

b) Számítsuk ki az alábbi ideálok legnagyobb közös osztóját:

b1: (2) és $(1+\sqrt{-5})$; b2: $(2, 1+\sqrt{-5})$ és $(3, 1-\sqrt{-5})$.

c) Döntsük el, hogy az alábbi ideálok közül melyek lesznek felbonthatatlan ideálok:

c1: $(2, 1+\sqrt{-5})$; c2: (2); c3: (11).

M 11.4.9 Melyek igazak az alábbi állítások közül?

a) Ha α felbonthatatlan elem R-ben, akkor (α) felbonthatatlan ideál.

b) Ha (α) felbonthatatlan ideál, akkor α felbonthatatlan elem R-ben.

c) Ha α prímelem R-ben, akkor (α) prímideál.

d) Ha (α) prímideál, akkor α prímelem R-ben.

11.4.10

a) Mutassunk példát arra, hogy $\mathbf{Z}[x]$ ideáljai között nem érvényes a (4) egyszerűsítési szabály: $AB = AC$, $A \neq (0) \not\Rightarrow B = C$.

b) Bizonyítsuk be, hogy nemnulla főideállal bármely R (kommutatív, egységelemes, nullosztómentes) gyűrű esetén lehet egyszerűsíteni: Ha $A = (\alpha) \neq (0)$, akkor $AB = AC \Rightarrow B = C$.

11.4.11 Tekintsük a nemnegatív racionális kitevőjű, valós együtthatós „polinomok” R gyűrűjét (ilyen „polinom” például $3 + 7x^{4/7} + 11x^{5/3}$).

a) Mutassuk meg, hogy R-ben azok az elemek, amelyekben nem szerepel x^0 tag (azaz a konstans tagjuk 0), egy I ideált alkotnak.

b) Bizonyítsuk be, hogy I csak a következőképpen bontható fel két ideál szorzatára: $I = (1)I = I(1) = I \cdot I$.

Megjegyzés: A fenti I ideál eleget tesz a felbonthatatlan ideáloknál látott (8) és (9) kikötéseknek, ezzel együtt az $I = I \cdot I$ „nemtriviális" felbontással is rendelkezik (ebből is következik, hogy R-ben nem érvényes a (4) egyszerűsítési szabály). Ilyen és hasonló „furcsaságok" miatt a felbonthatatlanságot (és egyéb számelméleti tartalmú fogalmakat) általában csak olyan gyűrűk ideáljaira szokták vizsgálni, amelyekben érvényes a (4) és (5) tulajdonság.

11.4.12 Legyen R tetszőleges (kommutatív, egységelemes, nullosztómentes) gyűrű (de a (4) és (5) feltételek érvényességét ebben a feladatban nem követeljük meg). A nemtriviális ideálok körében értelmezzük a maximális ideál, illetve a prímideál fogalmát a (9), illetve a (12) tulajdonságokkal, kvázi-felbonthatatlan ideálnak pedig egy olyan (nemtriviális) ideált nevezzünk, amely csak úgy bontható két ideál szorzatára, hogy valamelyik tényező önmaga (vö. az előző feladattal).

a) Bizonyítsuk be, hogy minden prímideál egyben kvázi-felbonthatatlan ideál is.

b) Mutassunk példát olyan kvázi-felbonthatatlan ideálra, amely nem prímideál.

c) Bizonyítsuk be, hogy minden maximális ideál egyben prímideál (és így kvázi-felbonthatatlan ideál is).

d) Mutassunk példát olyan prímideálra, amely nem maximális ideál.

e) Bizonyítsuk be, hogy I akkor és csak akkor maximális ideál, ha az R/I faktorgyűrű test, illetve I akkor és csak akkor prímideál, ha R/I nullosztómentes.

Megjegyzés: A kvázi-felbonthatatlan ideál fogalmát csak a feladat kedvéért vezettük be, viszont a maximális ideálnak és a prímideálnak az ebben a feladatban adott értelmezés szerinti fogalma tetszőleges gyűrűben fontos szerepet játszik (jelentőségüket a feladat e) részéből is érzékelhetjük).

11.5. Dedekind-gyűrű

Ebben a pontban ϑ végig algebrai számot jelöl.

Megmutatjuk, hogy $E(\vartheta)$ ideáljaira teljesül „a számelmélet alaptétele", azaz bármely, a (0)-tól és (1)-től különböző ideál prímideálok szorzatára bontható, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű. Az ilyen tulajdonságú gyűrűket *Dedekind-gyűrű*knek nevezzük.

Első lépésként egy algebrai egész együtthatós polinomok szorzatára vonatkozó, önmagában is érdekes eredményt igazolunk (11.5.1 Tétel), amely a racionális együtthatós polinomokra vonatkozó Gauss-lemma általánosításának is tekinthető (lásd a 11.5.9 feladatot). Ennek felhasználásával bebizonyítjuk, hogy $E(\vartheta)$ bármely $A \neq (0)$ ideáljához található olyan $B \neq (0)$ ideál, amelyre AB főideál (11.5.5 Tétel). Ebből egyszerűen következik majd az ideálokra vonatkozó egyszerűsítési szabály (11.5.6 Tétel), valamint az ideálok oszthatóságának és a („fordított irányú") tartalmazásnak az ekvivalenciája (11.5.7 Tétel); ezeket a tulajdonságokat kötöttük ki az előző pontban az ideálokkal kapcsolatos általánosabb számelméleti fogalmak vizsgálatánál. Ezután bebizonyítjuk az ideálok egyértelmű prímfaktorizációját (11.5.8 Tétel). Végül érdekességként megmutatjuk, hogy $E(\vartheta)$ bármely ideálja generálható legfeljebb két elemmel (11.5.9 Tétel).

11.5.1 Tétel **T 11.5.1**

Legyen az

$$f(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_m x^m \qquad \text{és} \qquad g(x) = \beta_0 + \beta_1 x + \ldots + \beta_n x^n$$

algebrai egész együtthatós polinomok szorzata

$$f(x)g(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_{m+n} x^{m+n}\,.$$

Tegyük fel, hogy egy δ algebrai egészre

$$\delta \mid \gamma_k, \qquad k = 0, 1, \ldots, m+n. \tag{1}$$

Ekkor

$$\delta \mid \alpha_i \beta_j, \qquad i = 0, 1, \ldots, m, \qquad j = 0, 1, \ldots, n. \ \clubsuit$$

Bizonyítás: A bizonyításhoz szükségünk lesz három, egymásra épülő segédtételre.

11.5.2 Lemma **L 11.5.2**

Egy algebrai egész együtthatós polinom főegyütthatójának és a polinom tetszőleges gyökének szorzata algebrai egész szám. $\clubsuit$

A 11.5.2 Lemma bizonyítása: Legyen

$$h(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_r x^r = \lambda_r \prod_{i=1}^{r} (x - \xi_i), \tag{2}$$

és belátjuk, hogy például $\lambda_r\xi_1$ algebrai egész. A

$$0 = f(\xi_1) = \lambda_0 + \lambda_1\xi_1 + \ldots + \lambda_r\xi_1^r$$

egyenlőséget λ_r^{r-1}-nel megszorozva kapjuk, hogy

$$0 = \lambda_0\lambda_r^{r-1} + \lambda_1\lambda_r^{r-2}(\lambda_r\xi_1) + \ldots + \lambda_{r-1}(\lambda_r\xi_1)^{r-1} + (\lambda_r\xi_1)^r.$$

Ez azt jelenti, hogy $\lambda_r\xi_1$ gyöke a

$$\lambda_0\lambda_r^{r-1} + \lambda_1\lambda_r^{r-2}x + \ldots + \lambda_{r-1}x^{r-1} + x^r$$

normált, algebrai egész együtthatós polinomnak, és így a 9.6.3/(iii) Tétel szerint $\lambda_r\xi_1$ algebrai egész. ■

11.5.3 Lemma **L 11.5.3**

Egy algebrai egész együtthatós polinomot bármely gyöktényezőjével leosztva ismét algebrai egész együtthatós polinomot kapunk. ♣

A 11.5.3 Lemma bizonyítása: Legyen h a (2)-ben megadott polinom, és megmutatjuk, hogy a

$$h_1(x) = \frac{h(x)}{x - \xi_1}$$

polinom együtthatói algebrai egészek.

A bizonyítást a h fokszáma, azaz r szerinti teljes indukcióval végezzük.

Az állítás $r = 1$ esetén igaz: ekkor $h_1(x)$ a λ_1 konstans polinom.

Tegyük fel, hogy az állítás minden legfeljebb $r-1$-edfokú polinomra igaz. Tekintsük az

$$s(x) = h(x) - \lambda_r(x - \xi_1)x^{r-1}$$

polinomot. Nyilván $s(x)$ legfeljebb $r-1$-edfokú, továbbá $s(\xi_1) = 0$, és végül a 11.5.2 Lemma alapján $\lambda_r\xi_1$ algebrai egész, tehát $s(x)$ algebrai egész együtthatós.

Az indukciós feltétel szerint így az

$$s_1(x) = \frac{s(x)}{x - \xi_1} = \frac{h(x)}{x - \xi_1} - \lambda_r x^{r-1} = h_1(x) - \lambda_r x^{r-1}$$

polinom is algebrai egész együtthatós. Mivel λ_r algebrai egész, ebből következik, hogy $h_1(x)$ együtthatói is algebrai egészek. ■

11.5.4 Lemma **L 11.5.4**

Egy algebrai egész együtthatós polinom főegyütthatójának és a polinom tetszőleges számú gyökének szorzata algebrai egész szám. ♣

A 11.5.4 Lemma bizonyítása: Legyen h a (2)-ben megadott polinom, és megmutatjuk, hogy (például) $\lambda_r\xi_1\dots\xi_k$ algebrai egész.

Osszuk le $h(x)$-et a „kimaradó" (azaz a k-nál nagyobb indexű) gyöktényezőkkel, ekkor a

$$t(x)=\lambda_r\prod_{j=1}^{k}(x-\xi_j)$$

polinomhoz jutunk, amely a 11.5.3 Lemma (többszöri alkalmazása) alapján algebrai egész együtthatós. Így a $t(x)$ polinom konstans tagja, azaz

$$(-1)^k\lambda_r\xi_1\dots\xi_k$$

is algebrai egész. ■

Most rátérünk a 11.5.1 Tétel bizonyítására.

Legyenek az f, illetve g polinom gyökei $\xi_1,\dots,\xi_m$, illetve $\eta_1,\dots,\eta_n$. Ekkor

$$f(x)g(x)=\sum_{k=0}^{m+n}\gamma_kx^k=\alpha_m\beta_n\prod_{i=1}^{m}(x-\xi_i)\prod_{j=1}^{n}(x-\eta_j). \tag{3}$$

A (3) egyenlőséget (a 11.5.1 Tétel állításában szereplő) δ-val elosztva kapjuk, hogy

$$\sum_{k=0}^{m+n}\frac{\gamma_k}{\delta}x^k=\frac{\alpha_m\beta_n}{\delta}\prod_{i=1}^{m}(x-\xi_i)\prod_{j=1}^{n}(x-\eta_j)\,. \tag{4}$$

Az (1) feltétel miatt a (4) bal oldalán álló polinom algebrai egész együtthatós. Így a 11.5.4 Lemma szerint tetszőleges

$$\frac{\alpha_m\beta_n}{\delta}\xi_{i_1}\dots\xi_{i_r}\eta_{j_1}\dots\eta_{j_s} \tag{5}$$

szorzat algebrai egész.

Az f polinom tetszőleges α_i együtthatója a gyöktényezős előállítás alapján úgy keletkezik, hogy bizonyos $\pm\alpha_m\xi_{i_1}\dots\xi_{i_r}$ típusú tagokat összegezünk, és hasonló a helyzet g-nél is. Így minden $\alpha_i\beta_j$ előáll

$$\alpha_i\beta_j=\Big(\sum\pm\alpha_m\xi_{i_1}\dots\xi_{i_r}\Big)\Big(\sum\pm\beta_n\eta_{j_1}\dots\eta_{j_s}\Big)$$

alakban, azaz

$$\frac{\alpha_i\beta_j}{\delta} = \frac{\alpha_m\beta_n}{\delta}\Big(\sum \pm\xi_{i_1}\dots\xi_{i_r}\Big)\Big(\sum \pm\eta_{j_1}\dots\eta_{j_s}\Big)\,. \tag{6}$$

A (6) jobb oldala (5) típusú algebrai egészek előjeles összege, tehát algebrai egész. Ezzel beláttuk, hogy a bal oldalon álló $\alpha_i\beta_j/\delta$ is algebrai egész. ■

Az alábbi, Kroneckertől származó tétel kulcsszerepet játszik $E(\vartheta)$ ideáljainak vizsgálatánál: a tétel alapján az ideálokkal kapcsolatos számos kérdésre (legalábbis részben) a jóval áttekinthetőbb szerkezetű főideálok segítségével adhatunk választ.

11.5.5 Tétel **T 11.5.5**

$E(\vartheta)$ bármely $A \neq (0)$ ideáljához található olyan $B \neq (0)$ ideál, amelyre AB főideál. ♣

Megjegyzés: A bizonyításból kiderül, hogy olyan $B \neq (0)$ is választható, amelyre $AB = (c)$, ahol c egész szám. Ez a „többlet" azonban a tétel állításából is könnyen levezethető (lásd a 11.5.1 és 11.5.2 feladatot).

Bizonyítás: A 11.1.10c feladat szerint az A ideál végesen generált:

$$A = (\alpha_0,\ \alpha_1,\ \dots,\ ,\alpha_k).$$

Legyenek $\vartheta_{(1)} = \vartheta, \vartheta_{(2)}, \dots, \vartheta_{(n)}$ a ϑ $\mathbf{Q}$ feletti konjugáltjai (azaz a minimálpolinomjának a gyökei), és jelölje $f_\nu(\vartheta_{(j)})$ az α_ν generátorelem j-edik relatív konjugáltját (lásd a 10.4 pontot); speciálisan $f_\nu(\vartheta_{(1)}) = \alpha_\nu$.

Tekintsük az

$$F_j(x) = f_0(\vartheta_{(j)}) + f_1(\vartheta_{(j)})x + \ldots + f_k(\vartheta_{(j)})x^k, \qquad j = 1, 2, \dots, n$$

polinomokat. (Az $F_j(x)$ polinomban x^i együtthatója tehát az α_i generátorelem j-edik relatív konjugáltja.) Speciálisan

$$F_1(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k.$$

Legyen $G(x) = \prod_{j=1}^{n} F_j(x)$.

A $G(x)$, és így minden együtthatója is szimmetrikus polinomja a ϑ_j változóknak. Ezért a szimmetrikus polinomok alaptételét és ϑ minimálpolinomjára a gyökök és együtthatók közötti összefüggéseket felhasználva (a már többször látott módon) nyerjük, hogy $G(x)$ racionális együtthatós.

Mivel $G(x)$ együtthatóit az α_ν algebrai egészekből és szintén algebrai egész relatív konjugáltjaikból összeadás és szorzás segítségével kapjuk, ezért $G(x)$ együtthatói algebrai egészek. Az előzőkkel együtt ez azt jelenti, hogy $G(x)$ egész együtthatós,

$$G(x) = a_0 + a_1 x + \ldots + a_{kn} x^{kn}, \qquad a_s \in \mathbf{Z}, \qquad s = 0, 1, \ldots, kn.$$

Legyen

$$H(x) = \frac{G(x)}{F_1(x)} = \prod_{j=2}^{n} F_j(x).$$

Mivel minden $F_j(x)$ algebrai egész együtthatós, ezért $H(x)$ együtthatói is algebrai egészek. Továbbá $G(x)$ és $F_1(x)$ együtthatói $\mathbf{Q}(\vartheta)$-beliek, és a (maradékos) osztási eljárás nem vezet ki az együtthatókat tartalmazó testből, így $H(x)$ együtthatói $\mathbf{Q}(\vartheta)$-beliek. A két megállapítás alapján $H(x)$ együtthatói $E(\vartheta)$-ból valók,

$$H(x) = \beta_0 + \beta_1 x + \ldots + \beta_{kn-k} x^{kn-k}.$$

Megmutatjuk, hogy a

$$B = (\beta_0, \beta_1, \ldots, \beta_{kn-k}) \qquad \text{és} \qquad c = \text{lnko}\,\{a_0, a_1, \ldots, a_{kn}\}$$

választással $AB = (c)$.

Mivel c a $G \neq 0$ polinom együtthatóinak legnagyobb közös osztója, ezért $c \neq 0$ (és így nyilván $B \neq (0)$).

Először az $AB \subseteq (c)$ tartalmazást igazoljuk. A c definíciója szerint c osztója a $G(x) = F_1(x)H(x)$ polinom minden a_i együtthatójának. Ezért a 11.5.1 Tétel szerint c mindegyik $\alpha_i\beta_j$ szorzatnak osztója, azaz $\alpha_i\beta_j \in (c)$. Ebből azonnal következik, hogy $AB \subseteq (c)$.

A másik irányú, $(c) \subseteq AB$ tartalmazás igazolásához vegyük észre, hogy a $G(x) = F_1(x)H(x)$, azaz

$$a_0 + a_1 x + \ldots + a_{kn} x^{kn} = (\alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k)(\beta_0 + \beta_1 x + \ldots + \beta_{kn-k} x^{kn-k})$$

egyenlőség alapján

$$a_s = \sum_{i+j=s} \alpha_i \beta_j \in AB, \qquad s = 0, 1, \ldots, kn.$$

Az egész számok körében a legnagyobb közös osztóra vonatkozó 1.3.5 Tétel szerint c felírható alkalmas u_s egészekkel

$$c = \sum_{s=0}^{kn} a_s u_s$$

alakban, ezért

$$c \in (a_0, a_1, \ldots, a_{kn}) \subseteq AB, \qquad \text{tehát} \qquad (c) \subseteq AB.$$

A kölcsönös tartalmazással beláttuk, hogy valóban $AB = (c)$. ■

11.5.6 Tétel **T 11.5.6**

$E(\vartheta)$ ideáljaira érvényes az egyszerűsítési szabály:

$$AB = AC,\ A \neq (0) \implies B = C. \clubsuit$$

Bizonyítás: A 11.5.5 Tétel szerint az $A \neq (0)$ ideálhoz létezik olyan $D \neq (0)$ ideál, amelyre AD főideál, azaz alkalmas $(0 \neq)\psi \in E(\vartheta)$-val $AD = (\psi)$ (sőt, ψ egész számnak is választható).

Az $AB = AC$ egyenlőséget D-vel megszorozva $(\psi)B = (\psi)C$ adódik. Innen a 11.4.10b feladat alapján következik, hogy $B = C$. ■

11.5.7 Tétel **T 11.5.7**

$E(\vartheta)$ ideáljaira $B \mid A \iff A \subseteq B$. ♣

Bizonyítás: A 11.4.2c feladatban láttuk, hogy az $\Rightarrow$ irány tetszőleges (kommutatív, egységelemes, nullosztómentes) gyűrűben érvényes.

A megfordításhoz tegyük fel, hogy $A \subseteq B$. Nyilván elég a $B \neq (0)$ esetre szorítkozni. A 11.5.5 Tétel alapján ekkor létezik olyan $D \neq (0)$ ideál, amelyre $BD = (\psi)$ főideál. Ekkor $AD \subseteq BD = (\psi)$.

Az $E(\vartheta)$ gyűrű minden ideálja, így AD is végesen generált. Az $AD \subseteq (\psi)$ feltétel miatt minden generátorelem osztható ψ-vel:

$$AD = (\eta_1\psi, \ldots, \eta_s\psi) = (\psi)(\eta_1, \ldots, \eta_s).$$

Az $(\eta_1, \ldots, \eta_s)$ ideált K-val jelölve, így

$$AD = (\psi)K = BDK$$

adódik, ahonnan a $D \neq (0)$ ideállal egyszerűsítve kapjuk, hogy

$$A = BK, \qquad \text{azaz} \qquad B \mid K. \ \blacksquare$$

A 11.5.6, illetve 11.5.7 Tétel szerint $E(\vartheta)$ ideáljaira érvényes az egyszerűsítési szabály, illetve az oszthatóság ekvivalens a (fordított irányú) tartalmazással. Ennek megfelelően $E(\vartheta)$ ideáljaira érvényesek a 11.4 pontban az ehhez a két tulajdonsághoz kötött eredmények. Ezek közül kiemeljük a felbonthatatlan ideál és a prímideál ekvivalenciáját (11.4.8 Tétel). Ez a tény fontos szerepet játszik a következő tétel bizonyításában is: megmutatjuk, hogy $E(\vartheta)$ ideáljaira érvényes a számelmélet alaptétele.

11.5.8 Tétel **T 11.5.8**

$E(\vartheta)$ bármely, a (0)-tól és az (1)-től különböző ideálja felbontható véges sok felbonthatatlan ideál szorzatára, és ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű. ♣

Bizonyítás: A bizonyítás szorosan követi a 11.3.1 Tétel elégségességi részénél látott gondolatmenetet.

Felbonthatóság. Legyen A tetszőleges nemtriviális ideál. Első lépésként azt mutatjuk meg, hogy A-nak létezik olyan osztója, amely felbonthatatlan ideál.

Ha maga az A felbonthatatlan ideál, akkor készen vagyunk.

Ha A nem felbonthatatlan, akkor $A = A_1B_1$, ahol $A_1 \neq (1)$, $B_1 \neq (1)$. Ekkor $A \subset A_1$, és itt szigorú tartalmazás áll fenn, hiszen $A = A_1$ esetén az $A(1) = A = AB_1$ egyenlőségből az egyszerűsítési szabály miatt $(1) = B_1$ következne.

Ha A_1 felbonthatatlan, akkor A_1 az A-nak egy felbonthatatlan osztója. Egyébként $A_1 = A_2B_2$, ahol $A_2 \neq (1)$, $B_2 \neq (1)$. Ekkor $A_1 \subset A_2$ (szigorú tartalmazással).

A gondolatmenetet hasonlóan folytatva valamelyik A_i már szükségképpen felbonthatatlan ideál, ugyanis ellenkező esetben az

$$A \subset A_1 \subset A_2 \subset \ldots \subset A_j \subset \ldots$$

szigorúan növő végtelen ideálláncot kapnánk, ami ellentmond a 11.1.10b feladat állításának.

Most belátjuk, hogy A előáll felbonthatatlan ideálok szorzataként. Ha A felbonthatatlan, akkor készen vagyunk. Egyébként az előzőek szerint

$A = P_1C_1$, ahol P_1 felbonthatatlan ideál és $C_1 \neq (1)$. Mivel $P_1 \neq (1)$, ezért $A \subset C_1$ (szigorú tartalmazással).

Ha C_1 felbonthatatlan, akkor az $A = P_1C_1$ felírásban mindkét tényező felbonthatatlan, tehát készen vagyunk. Egyébként $C_1 = P_2C_2$, ahol P_2 felbonthatatlan ideál és C_2 nem egység. Innen $C_1 \subset C_2$ (szigorú tartalmazással).

Az eljárást folytatva előbb-utóbb valamelyik $C_i = (1)$, ugyanis különben az

$$A \subset C_1 \subset \ldots \subset C_j \subset \ldots$$

végtelen, szigorúan növő ideállánc ellentmondana a 11.1.10b feladat állításának. Ez azt jelenti, hogy A-t előállítottuk felbonthatatlan ideálok szorzataként.

Egyértelműség: Tegyük fel indirekt, hogy valamely A-nak létezik (legalább) két lényegesen különböző felbontása felbonthatatlan ideálok szorzatára:

$$A = P_1P_2 \ldots P_r = Q_1Q_2 \ldots Q_s. \tag{7}$$

Ha itt valamelyik P_i megegyezik valamelyik Q_j-vel, akkor az egyszerűsítési szabály miatt ezzel a közös tényezővel egyszerűsíthetünk. Így feltehetjük, hogy a (7)-beli előállításban $P_i \neq Q_j$.

(7)-ből kapjuk, hogy $P_1 \mid Q_1Q_2 \ldots Q_s$. Mivel P_1 felbonthatatlan ideál, így a 11.4.8 Tétel alapján prímideál is, ezért P_1 szükségképpen osztója legalább az egyik Q_j tényezőnek.

Azonban ha $P_1 \mid Q_j$, akkor Q_j felbonthatatlansága miatt $P_1 = (1)$ vagy $P_1 = Q_j$, és mindkettő lehetetlen. ■

Példa: Bontsuk fel $E(\sqrt{-5})$-ben a (6) főideált felbonthatatlan ideálok szorzatára.

Korábban láttuk, hogy $E(\sqrt{-5})$-ben a 6 két lényegesen különböző módon is előáll felbonthatatlan elemek szorzataként:

$$6 = 2 \cdot 3 = [1 + \sqrt{-5}][1 - \sqrt{-5}].$$

Ennek megfelelően a (6) főideál is kétféleképpen bomlik főideálok szorzatára:

$$(6) = (2)(3) = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Itt mindegyik tényező tovább bontható két felbonthatatlan ideál szorzatára:

$$\begin{aligned}
(2) &= (2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (2, 1 + \sqrt{-5})^2\,; \\
(3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}); \\
(1 + \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}); \\
(1 - \sqrt{-5}) &= (2, 1 - \sqrt{-5})(3, 1 - \sqrt{-5}).
\end{aligned}$$

Így a (6) főideál a következőképpen áll elő felbonthatatlan ideálok szorzataként:

$$(6) = (2, 1 + \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}).$$

Vegyük észre, hogy a fellépő felbonthatatlan ideálok tulajdonképpen a 6 elemnek a felbonthatatlan tényezőkre való kétféle felbontásából származnak: például a $(3, 1 + \sqrt{-5})$ ideált úgy is felfoghatjuk mint a bal oldali 3 és a jobb oldali $1 + \sqrt{-5}$ tényezőben „ideális számként megbújó közös osztót", és tulajdonképpen az ilyen „rejtett tényezők" segítségével finomítottuk a fenti két különböző felbontást a (6) főideálnak egy közös felbontásává.

A továbbiakban a felbonthatatlan ideál és a prímideál ekvivalenciája alapján mindkét fogalomra a prímideál elnevezést fogjuk használni.

A 11.5.8 Tétel alapján bevezethetjük az ideálok kanonikus alakját: Ha $A \neq (0)$ és $A \neq (1)$, akkor

$$A = P_1^{\alpha_1} \dots P_r^{\alpha_r} = \prod_{i=1}^{r} P_i^{\alpha_i} ,$$

ahol $P_1, \dots, P_r$ különböző prímideálok és $\alpha_1, \dots, \alpha_r$ pozitív egészek.

Az ideálok legnagyobb közös osztójának (lásd a 11.4.4 Definíciót és a 11.4.5 Tételt), illetve legkisebb közös többszörösének (lásd a 11.4.5 feladatot) kanonikus alakjára is az egész számoknál megszokott képlet érvényes: az ideálokban szereplő mindegyik prímideált az előforduló minimális, illetve maximális hatványon kell venni, és értelemszerűen $P^0 = (1)$. A bizonyítás is ugyanúgy történik, mint az egész számoknál.

Végül a 11.5.5 és 11.5.8 Tételek alkalmazásaként bebizonyítjuk, hogy $E(\vartheta)$ minden ideálja „majdnem főideál":

11.5.9 Tétel **T 11.5.9**

$E(\vartheta)$ minden ideálja generálható legfeljebb két elemmel. ♣

Bizonyítás: Nyilván feltehetjük, hogy $A \neq (0)$ és $A \neq (1)$.

A 11.5.5 Tétel szerint létezik olyan $B \neq (0)$ ideál, amelyre $AB = (\psi)$. Olyan (γ) főideált keresünk, amelynek az $AB = (\psi)$ ideállal vett legnagyobb közös osztója A, ekkor ugyanis a 11.4.5 Tétel (illetve az azt követő 2. megjegyzés) alapján

$$A = (\psi, \gamma). \tag{8}$$

Legyen $P_1, \dots, P_r$ az összes olyan prímideál, amely A és B közül legalább az egyiket osztja, és legyen az A kanonikus alakja

$$A = P_1^{\alpha_1} \dots P_r^{\alpha_r} = \prod_{i=1}^{r} P_i^{\alpha_i} ,$$

ahol az előbbieknek megfelelően előfordulhat $\alpha_i = 0$, azaz $P_i^0 = (1)$ is, ha P_i csak a B-nek osztója.

Tekintsük a következő ideálokat:

$$C = \prod_{i=1}^{r} P_i^{1+\alpha_i} , \quad \text{és} \quad C_j = P_j^{\alpha_j} \prod_{i \neq j} P_i^{1+\alpha_i} , \quad j = 1, 2, \dots, r.$$

Ekkor

$$C_j \mid C , \qquad \text{azaz} \qquad C \subset C_j , \qquad \text{de} \qquad C \neq C_j .$$

Válasszunk olyan $\gamma_1, \dots, \gamma_r$ elemeket, amelyekre

$$\gamma_j \in C_j , \qquad \text{de} \qquad \gamma_j \notin C , \qquad j = 1, 2, \dots, r.$$

Megmutatjuk, hogy

$$\gamma_j \in P_i^{1+\alpha_i} , \qquad \text{ha} \qquad j \neq i , \tag{9a}$$

$$\gamma_i \in P_i^{\alpha_i} , \tag{9b}$$

$$\gamma_i \notin P_i^{1+\alpha_i} . \tag{9c}$$

Ha $j \neq i$, akkor $P_i^{1+\alpha_i} \mid C_j$ miatt $C_j \subseteq P_i^{1+\alpha_i}$, és így $\gamma_j \in C_j$ alapján $\gamma_j \in P_i^{1+\alpha_i}$, amivel (9a)-t beláttuk. Hasonlóan igazolható (9b) is.

A (9c) képletet indirekt bizonyítjuk. Ha $\gamma_i \in P_i^{1+\alpha_i}$, akkor ezt (9a)-val összevetve az adódik, hogy

$$\gamma_i \in \bigcap_{t=1}^{r} P_t^{1+\alpha_t} . \tag{10}$$

A 11.4.5 feladat szerint ideálok metszete éppen a legkisebb közös többszörösük, azaz

$$\bigcap_{t=1}^{r} P_t^{1+\alpha_t} = \operatorname{lkkt}(P_1^{1+\alpha_1}, \dots, P_r^{1+\alpha_r}) = \prod_{t=1}^{r} P_t^{1+\alpha_t} = C. \tag{11}$$

A (10) és (11) összefüggésekből kapjuk, hogy $\gamma_i \in C$, ami ellentmond a γ_i választásának.

Megmutatjuk, hogy a

$$\gamma = \gamma_1 + \ldots + \gamma_r$$

elem esetén az AB és (γ) ideálok legnagyobb közös osztója A, és így (8) valóban teljesül.

Azt kell igazolni, hogy AB és (γ) legnagyobb közös osztójának a kanonikus alakjában

(i) a P_i-ken kívül más prímideál nem fordulhat elő, és

(ii) a P_i kitevője éppen α_i $(i = 1, 2, \ldots, r)$.

Az (i) feltétel teljesül, hiszen AB kanonikus alakjában csak a P_i prímideálok szerepelnek.

Mivel $A \mid AB$, ezért AB kanonikus alakjában a P_i kitevője legalább α_i. Ennek alapján (ii)-höz elég azt belátni, hogy (γ) kanonikus alakjában a P_i kitevője pontosan α_i, azaz

(iii) $P_i^{\alpha_i} \mid (\gamma)$, de

(iv) $P_i^{1+\alpha_i} \nmid (\gamma)$.

(iii): A (9a) és (9b) feltétel szerint

$$\gamma_t \in P_i^{\alpha_i}, \qquad t = 1, 2, \ldots, r,$$

azaz a γ-t előállító összeg minden tagja eleme $P_i^{\alpha_i}$-nek. Mivel $P_i^{\alpha_i}$ ideál, ezért $\gamma \in P_i^{\alpha_i}$ is teljesül, és így

$$(\gamma) \subseteq P_i^{\alpha_i}, \qquad \text{azaz} \qquad P_i^{\alpha_i} \mid (\gamma).$$

(iv): A (9a) és (9c) feltétel szerint

$$\gamma_j \in P_i^{1+\alpha_i}, \quad \text{ha} \quad j \neq i, \quad \text{de} \quad \gamma_i \notin P_i^{1+\alpha_i},$$

azaz a γ-t előállító összeg tagjai pontosan egy tag kivételével elemei $P_i^{1+\alpha_i}$-nek. Mivel $P_i^{1+\alpha_i}$ ideál, ezért $\gamma \notin P_i^{1+\alpha_i}$, és így

$$(\gamma) \not\subseteq P_i^{1+\alpha_i}, \qquad \text{azaz} \qquad P_i^{1+\alpha_i} \nmid (\gamma). \ \blacksquare$$

Feladatok

Valamennyi feladat $E(\vartheta)$ ideáljaira vonatkozik.

11.5.1 Bizonyítsuk be, hogy egy $\alpha \in E(\vartheta)$ elemhez és egy A ideálhoz akkor és csak akkor létezik olyan B ideál, amelyre $AB = (\alpha)$, ha $\alpha \in A$.

11.5.2

a) Mutassuk meg, hogy bármely $\alpha \in E(\vartheta)$ esetén $\alpha \mid N(\alpha)$.

b) Bizonyítsuk be, hogy $E(\vartheta)$-ban bármely $A \neq (0)$ ideál végtelen sok egész számot tartalmaz, amelyek egy (fő)ideált alkotnak $\mathbf{Z}$-ben.

11.5.3 Igazoljuk, hogy bármely $A \neq (0)$ ideálnak csak véges sok osztója van.

11.5.4 Tekintsük egy adott $E(\vartheta)$ prímideáljait.

a) Bizonyítsuk be, hogy minden prímideál pontosan egy pozitív prímszámot tartalmaz.

b) Mutassuk meg, hogy a prímideálok száma végtelen.

c) Lehet-e egy prímszám két különböző prímideálnak is eleme?

d) Lehet-e egy prímszám végtelen sok különböző prímideálnak is eleme?

11.5.5 Bizonyítsuk be, hogy $E(\vartheta)$-ban bármely két ideál szorzata megegyezik az összegük és a metszetük szorzatával.

11.5.6 Mutassuk meg, hogy bármely α, $\beta \in E(\vartheta)$ esetén $\alpha\beta \in (\alpha^2, \beta^2)$.

11.5.7 Tekintsük az $E(\sqrt{-5})$ gyűrűt.

a) Bontsuk fel a (21) főideált prímideálok szorzatára.

b) Melyek azok a $p > 0$ prímszámok, amelyek esetén $(p, 1+\sqrt{-5})$ prímideál?

M *c) Melyek azok a $p > 0$ prímszámok, amelyekre alkalmas a egész számmal $(p, a+\sqrt{-5})$ prímideál?

11.5.8 Bizonyítsuk be, hogy $E(\vartheta)$ elemeire akkor és csak akkor érvényes a számelmélet alaptétele, ha minden prímideál főideál.

M 11.5.9 Egy egész együtthatós, nemkonstans polinomot *primitív*nek nevezünk, ha az együtthatói relatív prímek. Vezessük le a 11.5.1 Tételből az alábbi két állítást:

a) (*A Gauss-lemma első alakja.*) Két primitív polinom szorzata is primitív.

b) (*A Gauss-lemma második alakja.*) Ha egy H *egész* együtthatós polinom felírható az F és G *racionális* együtthatós polinomok szorzataként, $H = FG$, akkor H előáll $H = F_1G_1$ alakban is, ahol F_1 és

G_1 olyan *egész* együtthatós polinomok, amelyek az F-nek, illetve a G-nek (racionális) konstansszorosai.

Megjegyzés: Az a) és b) állítás könnyen levezethető egymásból, ezért szokás mindkettőt Gauss-lemmának nevezni. Az irodalom egy részében azonban csak az a) állítást illetik ezzel az elnevezéssel.

11.6. Osztályszám

Ebben a pontban is feltesszük, hogy ϑ algebrai szám, és $E(\vartheta)$ nemnulla ideáljai között egy ekvivalenciarelációt vezetünk be. Az így keletkező ekvivalenciaosztályok száma fontos szerepet játszik $E(\vartheta)$ számelméleti vizsgálatánál. Befejezésül, az ideálokról tanultak alkalmazásaként megmutatjuk, hogy az $x^2 + 17 = y^3$ diofantikus egyenletnek nincs megoldása.

11.6.1 Definíció **D 11.6.1**

Az $A \neq (0)$ és $B \neq (0)$ ideálok *ekvivalens*ek, ha léteznek olyan $(\alpha) \neq (0)$ és $(\beta) \neq (0)$ főideálok, amelyekre

$$(\alpha)A = (\beta)B. \ \clubsuit$$

Jelölés: $A \sim B$.

A továbbiakban mindig eleve feltesszük, hogy a szereplő ideálok egyike sem nulla (beleértve a főideálokat is).

Az ekvivalencia néhány egyszerű, de fontos tulajdonságát az alábbi tételben foglaljuk össze.

11.6.2 Tétel **T 11.6.2**

(i) A 11.6.1 Definícióban definiált $\sim$ valóban ekvivalenciareláció, azaz reflexív, szimmetrikus és tranzitív.

(ii) $A \sim B, \quad C \sim D \implies AC \sim BD.$

(iii) $A \sim B \iff AC \sim BC.$

(iv) $A \sim (1) \iff A$ főideál. $\clubsuit$

Bizonyítás: (i) Mivel $(1)A = A$, ezért $A \sim A$. A szimmetria nyilvánvaló a definícióból. Végül, ha $A \sim B$ és $B \sim C$, azaz alkalmas nemnulla főideálokkal

$$(\alpha)A = (\beta)B \qquad \text{és} \qquad (\gamma)B = (\delta)C,$$

akkor

$$(\alpha\gamma)A = (\beta\gamma)B = (\beta\delta)C.$$

(ii) Ha $A \sim B$ és $C \sim D$, azaz alkalmas nemnulla főideálokkal

$$(\alpha)A = (\beta)B \qquad \text{és} \qquad (\varrho)C = (\xi)D,$$

akkor

$$(\alpha\varrho)AC = (\beta\xi)BD.$$

(iii) Mivel $C \neq (0)$, ezért $(\alpha)A = (\beta)B \iff (\alpha)AC = (\beta)BC$.

(iv) Ha $A = (\varrho)$, akkor $(1)A = (1)(\varrho) = (\varrho)(1)$ miatt $A \sim (1)$. Megfordítva, ha $A \sim (1)$, azaz $A(\alpha) = (1)(\beta) = (\beta)$, akkor a 11.4.3b feladat szerint A főideál. ■

A $\sim$ ekvivalenciareláció alapján $E(\vartheta)$ nemnulla ideáljai diszjunkt osztályokba sorolhatók. Bizonyítás nélkül közöljük az alábbi alapvető tételt:

11.6.3 Tétel **T 11.6.3**

$E(\vartheta)$ ideálosztályainak a száma véges. ♣

Az $E(\vartheta)$ ideálosztályainak a számát $h(\vartheta)$-val jelöljük.

Az alábbi táblázatban néhány negatív t-hez tartozó $E(\sqrt{t})$ esetén megadjuk az osztályszámot:

t	-1	-3	-5	-17	-31	-35	-74
$h(\sqrt{t})$	1	1	2	4	3	2	10

Könnyen adódik, hogy $E(\vartheta)$ elemeire akkor és csak akkor érvényes a számelmélet alaptétele, ha $h(\vartheta) = 1$ (lásd a 11.6.2 feladatot).

Most megmutatjuk, hogy tetszőleges $E(\vartheta)$-ban egy (nemnulla) ideál $h(\vartheta)$-adik hatványa mindig főideál:

11.6.4 Tétel **T 11.6.4**

Legyen $E(\vartheta)$ ideálosztályainak száma $h(\vartheta)$ és $A \neq (0)$ tetszőleges ideál. Ekkor $A^{h(\vartheta)}$ főideál. ♣

Bizonyítás: Az Euler–Fermat-tétel (2.4.1 Tétel) bizonyításánál látott gondolatmenetet követjük. Legyen $h(\vartheta) = h$ és

$$A_1\,,\ A_2\ \ldots\,,\ A_h \tag{1}$$

a különböző ideálosztályok egy-egy reprezentánsa.

Megmutatjuk, hogy ekkor

$$AA_1\,,\ AA_2\ \ldots\,,\ AA_h \tag{2}$$

is mind különböző ideálosztályokba esnek. Ha ugyanis $AA_i \sim AA_j$, azaz alkalmas $(\varrho) \neq (0)$ és $(\tau) \neq (0)$ főideálokkal

$$(\varrho)AA_i = (\tau)AA_j\ ,$$

akkor az $A \neq (0)$ ideállal történő egyszerűsítés után $A_i \sim A_j$, azaz (a feltétel miatt) $i = j$ adódik.

Mindezek alapján a (2)-ben felsorolt ideálok rendre ekvivalensek valamilyen sorrendben az (1)-beli ideálokkal. Ez azt jelenti, hogy minden $1 \leq i \leq h$-hoz létezik egy és csak egy olyan $1 \leq j \leq h$, amelyre $AA_i \sim A_j$. Jelöljük ezt az A_j-t B_i-vel:

$$\begin{array}{rcl} AA_1 & \sim & B_1\,, \\ AA_2 & \sim & B_2\,, \\ \vdots & & \\ AA_h & \sim & B_h\,. \end{array} \tag{3}$$

Itt a $B_1, \ldots, B_h$ ideálok az $A_1, \ldots, A_h$ ideálok egy permutációját alkotják.

A (3)-beli ekvivalenciákat összeszorozva, a 11.6.3/(ii) Tétel alapján azt kapjuk, hogy

$$A^h A_1 A_2 \ldots A_h \sim B_1 B_2 \ldots B_h = A_1 A_2 \ldots A_h\ . \tag{4}$$

Használjuk fel most a 11.6.3 Tétel (iii) és (iv) állítását: (iii) szerint a (4) ekvivalenciát az összes $A_i \neq (0)$ ideállal egyszerűsíthetjük, és az így keletkező $A^h \sim (1)$ ekvivalenciából (iv) szerint következik, hogy A^h főideál. ■

A fejezetet annak illusztrálásával zárjuk, hogy az ideálok segítségével gyakran olyan diofantikus egyenleteket is kezelni tudunk, ahol a megfelelő bővítés algebrai egészeire nem érvényes a számelmélet alaptétele.

11.6.5 Tétel **T 11.6.5**

Az $x^2 + 17 = y^3$ diofantikus egyenletnek nincs megoldása. ♣

Bizonyítás: Hasonló alakú diofantikus egyenletek már korábban is szerepeltek: ilyen volt az $x^2 + 4 = y^3$ (7.5.10 feladat), illetve az $x^2 + 243 = y^3$ (7.7.11 feladat). Ezeknél a bal oldalt a Gauss-, illetve Euler-egészek körében szorzattá bontottuk, majd a számelmélet alaptételének felhasználásával kimutattuk, hogy mindkét tényező egy köbszám egységszerese, végül ennek alapján meghatároztuk a megoldásokat.

A mostani egyenlet esetén azt a nehézséget kell áthidalni, hogy az

$$[x + \sqrt{-17}][x - \sqrt{-17}] = y^3 \tag{5}$$

szorzattá bontás után nem járhatunk el a korábbi példák mintájára, mert $E(\sqrt{-17})$-ben nem érvényes a számelmélet alaptétele. Ezért az elemekre vonatkozó (5) egyenletről át kell térni a megfelelő főideálok közötti egyenletre:

$$(x + \sqrt{-17})(x - \sqrt{-17}) = (y)^3\,. \tag{6}$$

Megmutatjuk, hogy az $(x + \sqrt{-17})$ és $(x - \sqrt{-17})$ ideálok relatív prímek. Tegyük fel indirekt, hogy van egy P prímideál közös osztójuk. Ekkor P osztója $(y)^3$-nak is, és mivel P prímideál, ezért (y)-nak is. Az oszthatóságoknak megfelelő tartalmazások alapján

$$x + \sqrt{-17} \in P, \qquad x - \sqrt{-17} \in P \qquad \text{és} \qquad y \in P.$$

Ekkor

$$\sqrt{-17}\big[[x - \sqrt{-17}] - [x + \sqrt{-17}]\big] = 2 \cdot 17 = 34 \in P$$

is igaz.

Megmutatjuk, hogy y és 34 relatív prímek (az egész számok körében).

Ha $17 \mid y$, akkor az eredeti egyenletből kapjuk, hogy x is osztható 17-tel, ekkor azonban a 17-nek $x^2 + 17$ pontosan az első, y^3 viszont legalább a harmadik hatványával osztható, ami lehetetlen.

Ha $2 \mid y$, akkor x páratlan, és az egyenlet bal oldala 2, a jobb oldala viszont 0 maradékot ad 8-cal osztva, ami szintén lehetetlen.

Ezzel beláttuk, hogy y és 34 relatív prímek. Ekkor alkalmas u és v egész számokra $1 = yu + 34v$. Mivel 34 és y is eleme P-nek, ezért az 1 is eleme P-nek, azaz $P = (1)$, ami ellentmond annak, hogy P prímideál.

Így a (6) egyenlőség bal oldalán szereplő két (fő)ideál valóban relatív prím. Az ideálokra vonatkozó egyértelmű prímfaktorizációból (11.5.8 Tétel) következik, hogy mindkét ideál egy alkalmas ideál köbe, azaz (például)

$$(x+\sqrt{-17}) = A^3\,. \tag{7}$$

Mivel $E(\sqrt{-17})$-ben az ideálosztályok száma $h(\sqrt{-17}) = 4$, ezért a 11.6.4 Tétel szerint A^4 főideál, $A^4 = (\gamma)$. Így (7)-et A-val beszorozva

$$A(x+\sqrt{-17}) = (\gamma)$$

adódik, amiből a 11.4.3b feladat alapján kapjuk, hogy A főideál, azaz $A = (\alpha)$. Ekkor (7) átírható az

$$(x+\sqrt{-17}) = (\alpha^3), \qquad \text{azaz} \qquad x+\sqrt{-17} = \varepsilon\alpha^3 \tag{8}$$

alakba, ahol ε egység $E(\sqrt{-17})$-ben. Az $E(\sqrt{-17})$ egységei csak a ±1, és ezek maguk is köbszámok, továbbá $-17 \equiv -1 \pmod 4$ miatt $E(\sqrt{-17})$ elemei $a+b\sqrt{-17}$ alakúak, ahol a és b egész számok. Ezért (8) tovább ekvivalens azzal, hogy

$$x+\sqrt{-17} = \beta^3 = [a+b\sqrt{-17}]^3\,.$$

A köbre emelést elvégezve és a képzetes részeket összehasonlítva

$$1 = 3a^2b - 17b^3 = b[3a^2 - 17b^2]$$

adódik. Innen $b = \pm1$, azonban a-ra nem kapunk egész értéket, tehát az $x^2+17 = y^3$ diofantikus egyenletnek nincs megoldása. ■

Feladatok

11.6.1 Igazoljuk, hogy $E(\sqrt{-6})$-ban a $(2,\sqrt{-6})$ és $(3,\sqrt{-6})$ ideálok ekvivalensek.

11.6.2 Bizonyítsuk be, hogy $E(\vartheta)$ elemeire akkor és csak akkor érvényes a számelmélet alaptétele, ha $h(\vartheta) = 1$.

M 11.6.3 Tegyük fel, hogy a $k > 0$ egész és $h = h(\vartheta)$ relatív prímek. Bizonyítsuk be az alábbi állításokat:

a) $A^k \sim B^k \implies A \sim B$.

b) Ha A^k főideál, akkor A is főideál.

11.6.4 Oldjuk meg az alábbi diofantikus egyenleteket:

a) $x^2+5 = y^3$;

b) $17x^2+1 = y^3$;

c) $x^2+74 = y^3$;

M d) $x^2+35 = y^3$.

12. KOMBINATORIKUS SZÁMELMÉLET

A számelmélet és a kombinatorika határterülete viszonylag rövid múltra tekinthet vissza (legalábbis más számelméleti ágak „életkorához" képest), hiszen „klasszikus" eredményei (Schur és Van der Waerden tételei) is száz évnél fiatalabbak. Ez a terület tematikájában és módszereiben is rendkívül sokszínű: szerteágazó kérdéseinek vizsgálata során szellemes elemi meggondolások mellett gyakran az analízis, az algebra és a valószínűségszámítás kifinomult eszközeit kell felhasználni. Jelenleg is rendkívül dinamikus fejlődésének egyik fő mozgatórugója Erdős Pál munkássága volt, így az ebben a fejezetben tárgyalt problémák szinte mindegyike kapcsolódik az ő nevéhez.

12.1. Csupa különböző összeg

1993-ban az Eötvös Loránd Tudományegyetem felkérte frissen avatott díszdoktorát, a 80 éves Erdős Pált, hogy „A matematika aktuális problémái" címmel tartson az Eötvös-napon előadást. A zsúfolásig megtelt Gólyavárban elhangzott előadás elejének (hangfelvétel alapján történő) felidézésével Erdős lebilincselő egyéniségéről is képet kaphatunk.

„Jól hallanak, ugye? Hátul is? Ha nem hallanak, tessék tiltakozni.

Nahát, az előadás címe egy kicsit szemtelen, de ezt nem én fogalmaztam így; nem lehet azt mondani, hogy ezek, amiről beszélni fogok, lennének a matematika aktuális problémái. Az utolsó ilyen előadást Hilbert tartotta 1900-ban, a párizsi matematikai kongresszuson, és nem is teljesen biztos, hogy most volna egy földi halandó, aki tudna egy ilyen előadást tartani. De az biztos, hogy évekig kellene rá készülni, és egy matematikai kongresszuson kellene megtartani. Én erre nem vállalkozom, talán már a magas korom miatt sem, de egy csomó dologról nem is tudok semmit, például algebrai topológiához, algebrai geometriához, logikához kevéssé értek. Így az előadás címe inkább „Kedvenc problémáim", és minthogy a hallgatóság egy része nem matematikus itten, elemi geometriáról és elemi számelméletről fogok beszélni.

Hát kezdjük először az elemi számelmélettel. Most mondok két problémát. Az elsőt 1931-ben vetettem fel, olyan régen, hogy nem is vagyok biztos benne, hogy ez Krisztus előtt volt vagy Krisztus után. Egy régi viccem különben, hogy két és fél milliárd éves vagyok. Erre az a bizonyíték, hogy amikor kicsi voltam, a Föld kora kétmilliárd év volt, és most közismert, hogy 4,6 milliárd év. Nyilván a különbség az én korom, és egyszer Los Angelesben tar-

tottam egy előadást, amelynek ez volt a címe: „Az első kétmilliárd évem a matematikában”, és a diákok készítettek egy ábrát, amelyre felrajzoltak egy diagramot: „a Föld születése, Erdős születése, a dinoszauruszok születése”, és volt egy kép, amelyen egy dinoszaurusz hátán ülök.

De hagyjuk most a viccet, a probléma így hangzik, különben 500 dollárt adok a bizonyításáért vagy cáfolásáért, azt hiszem, talán még kréta is van, hopp, kaphatok egy kis krétát, mert a [*mikrofon*]dróttal be vagyok fogva egy kicsit, köszönöm szépen, nahát a következő a probléma:

Legyen egész számoknak egy sorozata megadva: $a_1 < a_2 < \ldots < a_k \le n$, és tegyük fel, hogy az összes

$$\sum_{j=1}^{k} \varepsilon_j a_j, \qquad \varepsilon_j = 0 \text{ vagy } 1,$$

alakú részösszegek mind különbözők. Ilyen számok például a kettő hatványai: 1, 2, 4, 8, 16, ..., mert minden csecsemő tudja, hogy minden szám egyértelműen írható fel kettő hatványainak összegeként. Na most az 500 dolláros probléma az, hogy mennyi $\max k$, azaz maximálisan hány számot lehet n-ig megadni, hogy ezek az összegek mind különbözők legyenek.”

A kettőhatványok esetén ($2^0 = 1$-et is beleértve) $k = 1 + \lfloor \log_2 n \rfloor$, és első ránézésre azt gondolhatnánk, hogy így kapjuk a maximumot. Ez azonban nem így van: Conway és Guy $n = 2^{21}$-re talált ennél egyetlen elemmel sűrűbb sorozatot is, amelyre tehát $k = 2 + \lfloor \log_2 n \rfloor$. Ebből következik, hogy minden $n \ge 2^{21}$-re is létezik ilyen sorozat, lásd a 12.1.12 feladatot. Nem ismeretes, hogy ez tovább javítható-e.

Másfelől Erdős megmutatta, hogy $\log_2 n$-nél „sokkal” több elem már biztosan nem adható meg:

12.1.1 Tétel **T 12.1.1**

Tegyük fel, hogy az $1 \le a_1 < a_2 < \ldots < a_k \le n$ egész számok közül akárhány (különbözőnek az) összege mind különböző értéket ad. Ekkor

$$k \le \log_2 n + \log_2 \log_2 n + 1, \tag{1}$$

sőt ($n > 8$-ra)

$$k \le \log_2 n + \frac{\log_2 \log_2 n}{2} + 2. \quad \clubsuit \tag{2}$$

Az élesebb (2) eredmény Erdős és Leo Moser közös munkája, ennél jobb felső becslés ma sem ismeretes (eltekintve attól, hogy a képlet végén szereplő 2 helyére kicsit kisebb konstans írható, lásd a 12.1.13 feladatot).

A fentiek alapján az Erdős által keresett maximum az alábbi határok közé esik:

$$\lfloor \log_2 n \rfloor + 2 \le \max k \le \log_2 n + \frac{\log_2 \log_2 n}{2} + 2. \tag{3}$$

Erdős az 500 dollárt annak tisztázásáért ajánlotta fel, vajon a $\max k - \log_2 n$ eltérés n növekedésével korlátos marad-e. Ez a probléma tehát ma is megoldatlan.

Bizonyítás: Az a_i számokból 2^k darab u_j összeg képezhető (az u_j-k között szerepel a 0 mint „üres" összeg és $Z = \sum_{i=1}^{k} a_i$ is). Mindegyik u_j a $[0, nk-1]$ intervallumba esik (ha $k > 1$). Mivel a feltétel szerint mindegyik u_j különböző, ezért a darabszámuk legfeljebb annyi lehet, ahány egész szám a fenti intervallumban található, azaz

$$2^k \le nk. \tag{4}$$

Innen logaritmálással kapjuk, hogy

$$k \le \log_2 n + \log_2 k. \tag{5}$$

Most (5) jobb oldalán a második tagot fogjuk n függvényében felülről becsülni. Mivel nyilván $k \le n$, ezért $\log_2 k \le \log_2 n$, tehát (5)-ből következik

$$k \le 2 \log_2 n. \tag{6}$$

Ezt logaritmálva nyerjük, hogy

$$\log_2 k \le 1 + \log_2 \log_2 n, \tag{7}$$

amit (5)-be beírva éppen a kívánt (1) becslés adódik.

Az élesebb eredmény igazolásához azt fogjuk felhasználni, hogy az u_j-k nem egyenletesen helyezkednek el a $[0, nk-1]$ intervallumban, hanem a „zömük az átlag közelében csoportosul." Ezt az elemi valószínűségszámítás segítségével fogjuk pontosítani (bár minden elmondható és bizonyítható lenne anélkül is, a lényeget azonban éppen a valószínűségi szemlélet mutatja majd).

Tekintsük azt az η valószínűségi változót, amely a 2^k darab u_j mindegyikét 2^{-k} valószínűséggel veszi fel. A várható értéket E-vel, a szórást D-vel, a valószínűséget pedig P-vel jelölve, a

$$P\big(|\eta - E(\eta)| > cD(\eta)\big) < c^{-2} \tag{8}$$

Csebisev-egyenlőtlenség ekkor azt fejezi ki, hogy az u_j értékeknek csak kevesebb, mint c^{-2}-szerese esik az $E(\eta)$ középpontú $2cD(\eta)$ hosszúságú intervallumon kívülre, vagyis legalább $1-c^{-2}$-szeresük az adott intervallumban helyezkedik el. Ezután (alkalmas c-vel) erre az intervallumra és a biztosan itt levő u_j értékek számára fogjuk megismételni az (1) igazolásánál látott gondolatmenetet.

Nézzük a részleteket. A várható érték $E(\eta) = Z/2$, ugyanis az u_j-k összepárosíthatók úgy, hogy az egy párban levő u_j-k összege Z legyen. A szórás kiszámításához vezessük be a ξ_i, $i = 1, 2, \ldots, k$ valószínűségi változókat: ξ_i az a_i, illetve 0 értéket 1/2–1/2 valószínűséggel veszi fel. Ekkor a ξ_i változók függetlenek és összegük éppen η, tehát a szórásnégyzetre

$$D^2(\eta) = \sum_{i=1}^{k} D^2(\xi_i) = \frac{1}{4}\sum_{i=1}^{k} a_i^2 < \frac{kn^2}{4}$$

adódik.

alkalmazzuk most a (8) Csebisev-egyenlőtlenséget az $E(\eta) = Z/2$ és $D(\eta) < n\sqrt{k}/2$ értékekre és $c = 2$-re. Ekkor azt kapjuk, hogy a 2^k darab (csupa különböző) u_j legalább háromnegyed része a $Z/2$ középpontú $2n\sqrt{k}$ hosszúságú intervallumba esik. Ezért szükségképpen

$$\frac{3\cdot 2^k}{4} \le 2n\sqrt{k}, \qquad \text{azaz} \qquad 2^k \le \frac{8n\sqrt{k}}{3} \tag{9}$$

(tehát a (4)-beli hasonló becsléshez képest lényegében a jobb oldal változott k helyett $\sqrt{k}$-ra).

A (9) egyenlőtlenséget logaritmálva

$$k < \log_2 n + \frac{\log_2 k}{2} + \log_2\left(\frac{8}{3}\right) \tag{10}$$

adódik. (10)-ből ($n > 8$-ra) nyilvánvalóan következik (6), és így (7) is, amit (10)-be beírva kapjuk a kívánt (2) becslést. ■

A csupa különböző összeget szolgáltató pozitív egész számhalmazokhoz még egy érdekes Erdős-probléma kapcsolódik:

12.1.2 Tétel **T 12.1.2**

Ha az $a_1 < a_2 < \ldots < a_k$ pozitív egész számok közül akárhány (különbözőnek az) összege mind különböző értéket ad, akkor

$$\sum_{i=1}^{k} \frac{1}{a_i} < 2. \quad \clubsuit \tag{11}$$

A kettőhatványok példája mutatja, hogy (11)-ben a 2 helyére kisebb érték már nem írható (ha k értékét nem korlátozzuk). Rögzített k esetén a legnagyobb reciprokösszeget éppen az első k kettőhatvány (azaz $1, 2, 4, \dots 2^{k-1}$) esetén kapjuk, ez a második és a harmadik bizonyításból is leolvasható majd. Ha végtelen számhalmazokat is megengedünk, akkor a tétel olyan formában igaz, hogy a reciprokösszeg kisebb vagy egyenlő, mint 2, és az egyenlőség csak az összes kettőhatvány esetén teljesül. Ez az eredmény az alábbi bizonyítások bármelyikének értelemszerű módosításával igazolható.

A 12.1.2 Tétel állítása Erdős egy sejtése volt, és először Ryavec igazolta egy nagyon szellemes trükksorozattal (lásd az első bizonyítást). Ez a bizonyítás azonban egyrészt jelentősen támaszkodik az analízisre, másrészt egyáltalán nem könnyű belelátni, mitől „működik". Sok évvel később született két újabb bizonyítás, amelyek csak középiskolai ismereteket használnak és (egymástól is különböző) gondolatmenetük nagyon természetes (lásd a második és harmadik bizonyítást, ezek Bruentől és Borweintől, illetve Frenkel Pétertől származnak; a harmadik bizonyítást Frenkel Péter középiskolás korában találta). Ez is jól mutatja, hogy a kombinatorikus számelméletben időnként teljesen elemi módon is lehet új eredményeket elérni.

A bizonyítások közül tehát az első a legnehezebb, de a történeti szempontok mellett talán azért is érdemes végigrágnunk magunkat rajta, hogy utána még inkább élvezhessük a második és harmadik bizonyítás természetes szépségét és egyszerűségét.

Első bizonyítás: Tekintsük az

$$(1 + x^{a_1})(1 + x^{a_2}) \dots (1 + x^{a_k}) \tag{12}$$

szorzatot. A szorzást elvégezve olyan x^m tagokat kapunk, ahol m előáll valahány különböző a_i összegeként (az $1 = x^0$ az üres összegnek felel meg). A feltétel szerint csupa különböző x^m tag adódik, tehát a (12) szorzat $0 < x < 1$ esetén kisebb, mint az

$$1 + x + x^2 + \dots + x^n + \dots = \frac{1}{1 - x}$$

végtelen mértani sor összege, azaz

$$(1 + x^{a_1})(1 + x^{a_2}) \dots (1 + x^{a_k}) < \frac{1}{1 - x}, \quad \text{ha} \quad 0 < x < 1. \tag{13}$$

Most jön a „trükk": vegyük mindkét oldal (természetes alapú) logaritmusát, osszunk x-szel, majd integráljunk 0-tól 1-ig:

$$\sum_{i=1}^{k} \int_0^1 \frac{\log(1 + x^{a_i})}{x} dx < -\int_0^1 \frac{\log(1 - x)}{x} dx. \tag{14}$$

A bal oldali integráloknál helyettesítést alkalmazunk:

$$x^{a_i} = y, \quad \text{ekkor} \quad dy = a_i x^{a_i-1} dx, \quad \text{azaz} \quad dx = \frac{dy}{a_i x^{a_i-1}},$$

és így

$$\int_0^1 \frac{\log(1+x^{a_i})}{x} dx = \int_0^1 \frac{\log(1+y)}{x a_i x^{a_i-1}} dy = \frac{1}{a_i} \int_0^1 \frac{\log(1+y)}{y} dy. \tag{15}$$

(15) alapján (14) átírható a következő alakba:

$$\left(\sum_{i=1}^{k} \frac{1}{a_i}\right) \int_0^1 \frac{\log(1+y)}{y} dy < -\int_0^1 \frac{\log(1-x)}{x} dx. \tag{16}$$

Azt kell megmutatnunk, hogy (16)-ban a bal oldali $A = \int_0^1 \frac{\log(1+x)}{x} dx$ integrál a fele a jobb oldalon álló $B = -\int_0^1 \frac{\log(1-x)}{x} dx$ integrálnak. Tekintsük az $A-B$ különbséget:

$$A - B = \int_0^1 \left(\frac{\log(1+x)}{x} + \frac{\log(1-x)}{x}\right) dx = \int_0^1 \frac{\log(1-x^2)}{x} dx.$$

Innen $t = x^2, dt = 2x dx$ helyettesítéssel kapjuk, hogy

$$A - B = \int_0^1 \frac{\log(1-t)}{x \cdot 2x} dt = \frac{1}{2} \int_0^1 \frac{\log(1-t)}{t} dt = -\frac{1}{2} B, \text{ azaz } A = \frac{B}{2}. \blacksquare$$

Megjegyzés: A bizonyítást a (16)-beli integrálok kiszámításával is befejezhetjük. Ezt az integrandusok hatványsorba fejtésével és (a jelen feltételek mellett megengedett) tagonkénti integrálással végezhetjük el:

$$\frac{-\log(1-x)}{x} = 1 + \frac{x}{2} + \frac{x^2}{3} + \ldots + \frac{x^{j-1}}{j} + \ldots,$$

tehát

$$-\int_0^1 \frac{\log(1-x)}{x} dx = \left[x + \frac{x^2}{4} + \frac{x^3}{9} + \ldots + \frac{x^j}{j^2} + \ldots\right]_0^1 = \sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}. \tag{17}$$

Hasonló módon nyerjük, hogy

$$\begin{aligned}\int_0^1 \frac{\log(1+y)}{y}dy &= \Big[y-\frac{y^2}{4}+\frac{y^3}{9}-\ldots+(-1)^{j+1}\frac{y^j}{j^2}+\ldots\Big]_0^1 = \\ &= \sum_{j=1}^{\infty}(-1)^{j+1}\frac{1}{j^2} = \sum_{j=1}^{\infty}\frac{1}{j^2}-2\sum_{t=1}^{\infty}\frac{1}{(2t)^2} = \big(1-\frac{2}{4}\big)\sum_{j=1}^{\infty}\frac{1}{j^2} = \frac{\pi^2}{12}\,.\end{aligned} \tag{18}$$

(18)-at és (17)-et (16)-ba beírva kapjuk, hogy

$$\left(\sum_{i=1}^{k}\frac{1}{a_i}\right)\frac{\pi^2}{12} < \frac{\pi^2}{6}\,, \quad \text{azaz} \quad \sum_{i=1}^{k}\frac{1}{a_i} < 2.$$

Második bizonyítás: A feltétel szerint bármely $1 \le i \le k$ esetén az $a_1, a_2, \ldots, a_i$ számokból képezett 2^i-1 darab nemüres összeg csupa különböző pozitív egészt ad, ezért a legnagyobb ilyen összeg értéke legalább 2^i-1, azaz

$$a_1 + a_2 + \ldots + a_i \ge 2^i - 1, \qquad i = 1, 2, \ldots, k. \tag{19}$$

Bevezetve a

$$b_i = 2^{i-1}, \qquad i = 1, 2, \ldots, k$$

jelölést, (19) átírható az

$$a_1 + a_2 + \ldots + a_i \ge b_1 + b_2 + \ldots + b_i, \qquad i = 1, 2, \ldots, k \tag{20}$$

alakba. A tétel igazolásához elég belátnunk, hogy ekkor

$$\frac{1}{a_1} + \ldots + \frac{1}{a_k} \le \frac{1}{b_1} + \ldots + \frac{1}{b_k}\,, \tag{21}$$

hiszen (21) jobb oldala

$$1 + \frac{1}{2} + \frac{1}{4} + \ldots + \frac{1}{2^{k-1}} = 2 - \frac{1}{2^{k-1}} < 2.$$

Azt (a tétel állításánál erősebb eredményt) is be fogjuk bizonyítani, hogy (21)-ben csak az $a_i = b_i$, $i = 1, 2, \ldots k$ esetben áll egyenlőség, tehát a maximális reciprokösszeget akkor kapjuk, amikor $a_i = 2^{i-1}$.

Megmutatjuk, hogy (20)-ból mindig következik (21), ha

$$0 < a_1 < a_2 < \ldots < a_k, \qquad 0 < b_1 < b_2 < \ldots < b_k \tag{22}$$

tetszőleges *valós* számok.

(21)-et, illetve (20)-at átrendezve, az

$$\frac{1}{b_1}-\frac{1}{a_1}+\frac{1}{b_2}-\frac{1}{a_2}+\ldots+\frac{1}{b_k}-\frac{1}{a_k}\geq 0 \tag{21a}$$

egyenlőtlenséget kell igazolnunk, feltéve hogy (22) teljesül és

$$c_i=a_1-b_1+a_2-b_2+\ldots+a_i-b_i\geq 0,\quad i=1,2,\ldots,k. \tag{20a}$$

(21a) bal oldalát a következőképpen alakíthatjuk át (a második és harmadik lépésben az ún. Abel-féle átrendezést alkalmazzuk):

$$\begin{aligned}\frac{1}{b_1}-\frac{1}{a_1}+\frac{1}{b_2}-\frac{1}{a_2}+\ldots+\frac{1}{b_k}-\frac{1}{a_k}&=\frac{a_1-b_1}{a_1b_1}+\frac{a_2-b_2}{a_2b_2}+\ldots+\frac{a_k-b_k}{a_kb_k}=\\ &=\frac{c_1}{a_1b_1}+\frac{c_2-c_1}{a_2b_2}+\ldots+\frac{c_k-c_{k-1}}{a_kb_k}=c_1\left(\frac{1}{a_1b_1}-\frac{1}{a_2b_2}\right)+\\ &+c_2\left(\frac{1}{a_2b_2}-\frac{1}{a_3b_3}\right)+\ldots+c_{k-1}\left(\frac{1}{a_{k-1}b_{k-1}}-\frac{1}{a_kb_k}\right)+\frac{c_k}{a_kb_k}\,.\end{aligned} \tag{23}$$

A (23) képlet végén kapott előállításban (20a) és (22) alapján a $c_i\geq 0$ számok pozitív számokkal vannak szorozva, és így az összeg is nemnegatív, amint állítottuk.

A bizonyításból az is kiderült, hogy (21)-ben akkor és csak akkor áll egyenlőség, ha minden $c_i=0$, ami (20a) alapján azzal ekvivalens, hogy minden i-re $a_i=b_i$. Ebből következik, hogy a csupa különböző összeg probléma esetén a maximális reciprokösszeget akkor kapjuk, amikor $a_i=2^{i-1}$, amint jeleztük. ■

Harmadik bizonyítás: Csak a második bizonyítás elején látott (19) összefüggést fogjuk felhasználni, és megmutatjuk, hogy ha az $a_1<a_2<\ldots<a_k$ pozitív egészekre ez teljesül, akkor a reciprokösszeg kisebb, mint 2.

Ha (19)-ben minden i-re egyenlőség érvényes, akkor $a_i=2^{i-1}$ és a reciprokösszeg $2-1/2^{k-1}<2$.

Ha (19)-ben nem minden i-re áll egyenlőség, akkor egy vagy két alkalmas a_j megváltoztatásával növelni fogjuk a reciprokösszeget, miközben (19) továbbra is érvényben marad. Az eljárásból világos lesz, hogy véges sok ilyen lépésben eljutunk ahhoz az állapothoz, amikor (19)-ben végig egyenlőség van. Ezzel (azt a tétel állításánál élesebb eredményt) igazoltuk, hogy a reciprokösszeg az $a_i=2^{i-1}$ esetben a legnagyobb.

Legyen r a legkisebb olyan szám, amelyre (19)-ben nem áll egyenlőség ($r = 1$ is lehet), azaz

$$\begin{aligned} &a_1 + a_2 + \ldots + a_i = 2^i - 1, \qquad i = 1, 2, \ldots, r-1, \quad \text{és} \\ &a_1 + a_2 + \ldots + a_r > 2^r - 1. \end{aligned} \tag{24}$$

Két esetet különböztetünk meg: (A) Egyetlen $i > r$-re sem áll (19)-ben egyenlőség; (B) Van olyan $i > r$, melyre (19)-ben egyenlőség teljesül.

(A) Legyen $a_r' = a_r - 1$, a többi a_i pedig maradjon változatlan. Ezzel a reciprokösszeg nyilván növekedett (hiszen $1/a_r' > 1/a_r$), de (19) továbbra is érvényben maradt, hiszen bármely $i \geq r$-re (19) bal oldala pontosan 1-gyel csökkent, tehát az egyenlőtlenség továbbra is fennáll, legfeljebb $>$ helyett $\geq$ formában.

Meg kell még mutatni, hogy az új számaink is szigorúan növekedő pozitív sorozatot alkotnak. Ha $r = 1$, akkor (24)-ből kapjuk, hogy $a_1 > 1$, tehát $a_1' > 0$. Ha $r > 1$, akkor azt kell belátni, hogy $a_r' = a_r - 1 > a_{r-1}$, azaz $a_r \geq a_{r-1} + 2$. Ismét (24) alapján

$$a_r = (a_1 + \ldots + a_r) - (a_1 + \ldots + a_{r-1}) \geq 2^r - (2^{r-1} - 1) = (2^{r-1} - 1) + 2 \geq a_{r-1} + 2.$$

(B) Legyen s a legkisebb olyan r-nél nagyobb szám, amelyre (19)-ben ismét egyenlőség teljesül ($s = r + 1$ is lehet), azaz

$$\begin{aligned} &a_1 + a_2 + \ldots + a_i > 2^i - 1, \qquad i = r, r+1, \ldots, s-1, \quad \text{és} \\ &a_1 + a_2 + \ldots + a_s = 2^s - 1. \end{aligned} \tag{25}$$

Legyen $a_r' = a_r - 1$, $a_s' = a_s + 1$, a többi a_i pedig maradjon változatlan. Ekkor (19) továbbra is érvényben maradt, hiszen ha $r \leq i \leq s - 1$, akkor (19) bal oldala pontosan 1-gyel csökkent, tehát az egyenlőtlenség továbbra is fennáll (legfeljebb $>$ helyett $\geq$ formában), az $i \geq s$ (valamint az $i < r$) esetben pedig (19) bal oldala változatlan maradt.

A reciprokösszeg növekedéséhez azt kell megmutatni, hogy

$$\frac{1}{a_r} + \frac{1}{a_s} < \frac{1}{a_r'} + \frac{1}{a_s'},$$

azaz

$$\frac{a_r + a_s}{a_r a_s} < \frac{(a_r - 1) + (a_s + 1)}{(a_r - 1)(a_s + 1)}.$$

A számlálók egyenlősége miatt ez ekvivalens a nevezők közötti fordított irányú egyenlőtlenséggel (mindenhol pozitív számok szerepelnek), amit tovább alakítva a nyilvánvalóan igaz $a_r - 1 < a_s$ egyenlőtlenség adódik.

Végül, az (A) esethez hasonlóan igazolható, hogy az új számaink is szigorúan növekedő pozitív sorozatot alkotnak.

Az eljárásból világos, hogy a fenti lépéseket véges sokszor alkalmazva elérjük, hogy (19)-ben már $i = r$ mellett is egyenlőség teljesüljön. Ezután megismételjük az egészet az első olyan (r-nél már nagyobb) i értékre, amelyre (19)-ben szigorú egyenlőtlenség van, mindaddig, amíg már ott is egyenlőséget kapunk stb. Ezzel igazoltuk, hogy véges sok lépésben eljutunk ahhoz az állapothoz, amikor (19)-ben mindenütt egyenlőség szerepel, amint állítottuk.

■

Feladatok

A feladatokban $1 \le a_1 < a_2 < \ldots < a_k \le n$ egész számok, amelyekre különféle feltételeket írunk elő.

12.1.1

a) Mennyi k maximuma (n függvényében), ha egyik a_i sem áll elő csupa különböző (és egynél több) a_j összegeként.

*b) Legyen $a_1 < a_2 < \ldots$ pozitív egészeknek olyan *végtelen* sorozata, amelyben egyik a_i sem áll elő csupa különböző (és egynél több) a_j összegeként. Jelölje $A(n)$ a sorozat n-nél nem nagyobb elemeinek a számát. Lássuk be, hogy $\lim_{n\to\infty} A(n)/n = 0$.

12.1.2 Tegyük fel, hogy egyik a_i sem írható fel $a_j + a_{j+1}$ alakban. Jelöljük ezen feltétel mellett k maximumát $f(n)$-nel. Mutassuk meg, hogy $\lim_{n\to\infty} f(n)/n = 2/3$.

M 12.1.3 Azt vizsgáljuk, hogy egy t szám hányféleképpen állhat elő egymás után következő a_i-k összegeként, azaz $t = a_i + a_{i+1} + \ldots + a_j$ alakban (a tagszámot nem korlátozzuk és $i = j$ is megengedett). Legyen $L(k)$ a $t = a_i + a_{i+1} + \ldots + a_j$ egyenlet megoldásszámának maximuma, ahol a maximumot az összes lehetséges a_i rendszerre és t-re vesszük (n is tetszőleges lehet). Igazoljuk, hogy $L(k) = \lceil k/2 \rceil$.

12.1.4 Tegyük fel, hogy bármely $i \ne j$-re $[a_i, a_j] > n$. Bizonyítsuk be, hogy az a_i számok reciprokösszege kisebb, mint (a) 2; (b) 3/2.

Megjegyzés: Schinzel és Szekeres megmutatták, hogy a reciprokösszeg maximuma 31/30, és ez csak a 2, 3, 5 számok és $n = 5$ esetén lép fel.

12.1.5 Lássuk be, hogy (tetszőleges a_i-kre) $\displaystyle\sum_{i=1}^{k-1} \frac{1}{[a_i, a_{i+1}]} < 1$.

12.1.6 Tegyük fel, hogy $a_i + a_j$ sohasem négyzetszám. Jelöljük ezen feltétel mellett k maximumát $g(n)$-nel.

a) Igazoljuk, hogy

$$\frac{1}{3} \le \liminf_{n\to\infty} \frac{g(n)}{n} \quad \text{és} \quad \limsup_{n\to\infty} \frac{g(n)}{n} \le \frac{1}{2}\,.$$

*b) Javítsuk az előző egyenlőtlenségben az alsó becslést $11/32$-re.

Megjegyzés: 2002-ben Szemerédi Endre bebizonyította, hogy $\lim_{n\to\infty} g(n)/n = 11/32$.

*12.1.7 Tegyük fel, hogy $a_i - a_j$ ($i \ne j$-re) sohasem négyzetszám. Jelöljük ezen feltétel mellett k maximumát $h(n)$-nel. Igazoljuk, hogy elég nagy n-re $h(n) \ge n^{0.7}$.

Megjegyzés: A fenti eredmény Ruzsától származik. Sárközy és Fürstenberg megmutatták, hogy (az összegre vonatkozó kérdéssel ellentétben) $\lim_{n\to\infty} h(n)/n = 0$, azonban $h(n)$ pontos nagyságrendje nem ismert.

*12.1.8 Tegyük fel, hogy az a_i számok közül akárhány különbözőnek a *szorzata* mind különböző értéket ad. Jelöljük ezen feltétel mellett k maximumát $s(n)$-nel. Mutassuk meg, hogy

$$|s(n) - \pi(n)| < 2n^{2/3}$$

(ahol $\pi(n)$ az n-nél nem nagyobb prímek száma).

Megjegyzés: Erdős bebizonyította, hogy alkalmas c_1 és c_2 pozitív konstansokkal minden elég nagy n-re

$$\pi(n) + c_1 \frac{\sqrt{n}}{\log n} < s(n) < \pi(n) + c_2 \frac{\sqrt{n}}{\log n}\,.$$

Egy rokon kérdés a (következő pontban vizsgált additív) Sidon-probléma egy multiplikatív változata, amikor csak azt követeljük meg, hogy a kéttényezős $a_i a_j$ szorzatok ($i < j$) legyenek mind különbözők. Erdős belátta, hogy ekkor (alkalmas c_3 és c_4 pozitív konstansokkal, minden elég nagy n-re)

$$\pi(n) + c_3 \frac{n^{3/4}}{(\log n)^{3/2}} < \max k < \pi(n) + c_4 \frac{n^{3/4}}{(\log n)^{3/2}}\,.$$

12.1.9 Mennyi k maximuma (n függvényében), ha egyik a_i sem osztója tőle különböző a_j-k szorzatának?

12.1.10 Tegyük fel, hogy $6 \mid n$. Mennyi k maximuma (n függvényében), ha bármely három a_i között található kettő olyan, amelyek nem relatív prímek?

12.1.11 Lássuk be, hogy ha k prím, akkor van olyan i, j, melyre $\dfrac{a_i}{(a_i, a_j)} \geq k$.

Megjegyzés: Az állítás tetszőleges k esetén is igaz. R. L. Grahamnek ezt a sokáig megoldatlan sejtését (elég nagy k-ra) Szegedy Márió bizonyította be 1985-ben, még egyetemi hallgatóként.

12.1.12 Tegyük fel, hogy $n = 2^j$-re 1 és n között megadható $k = 2 + \lfloor \log_2 n \rfloor$ olyan a_i, amelyek közül akárhány (különbözőnek az) összege különböző értéket ad. Lássuk be, hogy akkor ugyanez igaz minden $n \geq 2^j$ esetén is.

12.1.13 A 12.1.1 Tétel bizonyításában a Csebisev-egyenlőtlenséget optimális c-vel alkalmazva mennyire javítható a tételben a (2) felső becslés?

12.2. Sidon-sorozatok

Erdős egy másik „kedvenc" területe a Sidon-problémakör volt. Sidon-sorozatoknak a természetes számok olyan $a_1 < a_2 < \ldots$ véges vagy végtelen részsorozatait nevezzük, amelyeknél az $a_i + a_j$, $i \leq j$ összegek (vagy ami ugyanaz: az $a_i - a_j$, $i \neq j$ különbségek) mind különbözők. Ezek először Sidon Simonnak a Fourier-sorokra vonatkozó vizsgálatai közben merültek fel az 1930-as években.

Az alábbiakban először véges Sidon-sorozatokkal foglalkozunk.

Maximálisan hány eleme lehet egy Sidon-sorozatnak az $[1, n]$ intervallumban? Bebizonyítjuk, hogy ez a maximum „körülbelül" $\sqrt{n}$. Ez két állítást jelent: egyrészt azt, hogy 1 és n között valóban található körülbelül $\sqrt{n}$ elemszámú Sidon-sorozat (alsó becslés a maximális elemszámra), másrészt azt, hogy az adott határok között ennél lényegesen hosszabb Sidon-sorozat már nem létezik (felső becslés a maximális elemszámra).

Erdős és Turán Pál 1941-ben megmutatták, hogy a keresett maximum legfeljebb $n^{1/2} + 2n^{1/4}$. Ezt később B. Lindström más módon $n^{1/2} + n^{1/4} + 1$-re javította, de ugyanez az eredmény az Erdős–Turán-bizonyítás pontosabb végigszámolásával is kiadódik (12.2.4 Tétel). J. Singer egy eredményének felhasználásával Erdős és tőle függetlenül S. Chowla 1944-ben azt is igazolták, hogy elég nagy n-re $n^{1/2} - n^{\varrho}$ elemszámú Sidon-sorozat valóban meg is adható n-ig, ahol ϱ egy alkalmas, 1/2-nél kisebb pozitív állandó (12.2.3 Tétel).

Ez a két eredmény együtt azt jelenti, hogy az $[1, n]$ intervallumban a Sidon-sorozatok maximális elemszáma nagyon pontos aszimptotikával $\sqrt{n}$. Máig is megoldatlan azonban a még jobb hibatagok kérdése. Az sejthető, hogy a maximális elemszámnak $\sqrt{n}$-től való eltérése egy n-től független korlát alatt marad. Ennek igazolásáért vagy cáfolásáért korábban Erdős összesen 1000 dollárt ajánlott fel.

Jelöljük $s = s(n)$-nel az n-ig megadható leghosszabb Sidon-sorozat elemszámát. Próbáljunk először egyszerű felső becslést keresni s-re. Mivel egy 1 és n közötti Sidon-sorozatban az $a_i + a_j$ összegek mind különbözők, 2 és $2n$ közé esnek és számuk $\binom{s+1}{2}$, így $\binom{s+1}{2} < 2n$, azaz $s < 2\sqrt{n}$. Jobb becslést kapunk, ha az $a_i - a_j > 0$ különbségeket vizsgáljuk; ezek is mind különbözők, n -nél kisebbek és számuk $\binom{s}{2}$, így $\binom{s}{2} < n$, azaz $s < \sqrt{2n} + 1$. A felső becslésnél tehát azonnal adódott a $\sqrt{n}$-es nagyságrend, „csak" a $\sqrt{n}$ együtthatóját kell 1-re leszorítani.

„Alulról nézve" sokkal kevésbé világos, hogyan érhető el a $\sqrt{n}$-es nagyságrend. A kettőhatványok példája csak $\log_2 n$-et ad, és a mohó algoritmussal is csak $\sqrt[3]{n}$ biztosítható (lásd a 12.2.1 feladatot). Egy szintén Erdőstől származó nagyon szép elemi konstrukcióval már $\sqrt{n/2}$ hosszú Sidon-sorozatot kapunk (lásd a 12.2.2 feladatot), és mint említettük, a $\sqrt{n}$ együtthatója „feltornázható" 1-re.

Lássunk akkor hozzá nagy elemszámú Sidon-sorozatok konstrukciójához. Ezt először bizonyos típusú n-ekre végezzük el, és ezek segítségével térünk majd át tetszőleges n-re.

12.2.1 Tétel **T 12.2.1**

Legyen p tetszőleges prímszám. Ekkor $n = p^2 + p + 1$-re létezik olyan Sidon-sorozat az $[1, n]$ intervallumban, amelynek $\lceil \sqrt{n} \rceil = p + 1$ eleme van. ♣

A 12.2.1 Tétel helyett egy jóval élesebb és önmagában is nagyon érdekes és meglepő állítást igazolunk.

12.2.2 Tétel **T 12.2.2**

Legyen p tetszőleges prímszám. Ekkor létezik $p + 1$ darab olyan a_i, amelyekre az $a_i - a_j,\ i \neq j$ különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo $p^2 + p + 1$. ♣

Megjegyzés: A 12.2.2 Tételben szereplő különbségek száma $p^2 + p$, és modulo $p^2 + p + 1$ éppen ennyi nemnulla maradék van. Vagyis az $a_i - a_j$ különbségek minden maradékot előállítanak, éspedig mindegyiket pontosan egyszer.

Nyilvánvaló, hogy a 12.2.2 Tételben az a_i-k maguk is páronként inkongruensek kell hogy legyenek, tehát választhatók 1 és $n = p^2 + p + 1$ közöttieknek, és így valóban azonnal adódik a 12.2.1 Tétel.

A 12.2.2 Tétel bizonyítása: A bizonyítás a véges testek segítségével történik, az ezek szerkezetére vonatkozó alapvető tételek és egy kevés lineáris algebra felhasználásával.

Tekintsük a p^3 elemű T_3 véges testet és ebben a p elemű T_1 résztestet. Legyen Δ a T_3 test multiplikatív csoportjának (egyik) generáló eleme, azaz

$$T_3 = \{0, \Delta, \Delta^2, \ldots, \Delta^{p^3-1} = 1\}\,. \tag{1}$$

A T_1-beli nemnulla elemek T_3 multiplikatív csoportjának részcsoportját alkotják, amelynek generátoreleme nyilván Δ^n, ahol $n = (p^3-1)/(p-1) = p^2+p+1$.

Vagyis

$$T_1 = \{0, \Delta^n, \Delta^{2n}, \ldots, \Delta^{(p-1)n} = \Delta^{p^3-1} = 1\}\,.$$

Tekintsük most T_3-at mint T_1 feletti vektorteret. Az előzőek alapján kapjuk, hogy T_3 két eleme, Δ^i és Δ^j pontosan akkor lineárisan összefüggő T_1 felett, ha

$$i \equiv j \pmod{n}\,. \tag{2}$$

A keresett a_i egészeket ezután a következőképpen adjuk meg. Vegyünk egy tetszőleges $\Theta \in T_3 \setminus T_1$ elemet, és legyenek T_1 elemei $\gamma_1, \ldots, \gamma_p$. Írjuk fel a $\Theta + \gamma_i$ elemeket

$$\Theta + \gamma_i = \Delta^{a_i} \tag{3}$$

alakban. Ez (1) alapján megtehető, és így kijelöltünk p darab a_i egész számot, a $p+1$-ik pedig legyen $a_{p+1} = 0$.

Megmutatjuk, hogy ezek eleget tesznek a feltételnek, azaz az $a_i - a_j$ különbségek, vagy ami ugyanaz, az $a_i + a_j$ összegek páronként különböző maradékot adnak modulo $p^2 + p + 1$.

Tegyük fel, hogy $a_i + a_j \equiv a_k + a_l \pmod{p^2 + p + 1}$. Ekkor (2) és (3) alapján

$$(\Theta + \gamma_i)(\Theta + \gamma_j) - \gamma(\Theta + \gamma_k)(\Theta + \gamma_l) = 0$$

adódik valamely $\gamma \in T_1$ elemmel. Mivel Θ harmadfokú a T_1 test felett, ezért nem lehet gyöke egy legfeljebb másodfokú polinomnak. Vagyis csak $\gamma = 1$ és $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$ lehetséges, így a megfelelő a_i-k is egyenlők, ami éppen a bizonyítandó állítás volt.

A bizonyítás ugyanígy megy akkor is, ha $a_{p+1} = 0$ is szerepel a négy a_i között. ■

Megjegyzés: A 12.2.2 Tétel és a bizonyítás ugyanúgy érvényes akkor is, ha p egy prímszám hatványa. Mindez szoros kapcsolatban áll a véges projektív síkokkal.

12.2.3 Tétel **T 12.2.3**

Minden elég nagy n-re megadható olyan Sidon-sorozat az $[1, n]$ intervallumban, amelynek legalább $n^{1/2} - n^{0,27}$ eleme van. ♣

Bizonyítás: Vegyük azt a legnagyobb p prímszámot, amelyre $p^2 + p + 1 \leq n$, és $p^2 + p + 1$-re készítsük el az előző $(p + 1$ elemű) konstrukciót. Mivel az 5.5.4/(A) Tétel alapján $n^{1/2} - n^{0,27}$ és $n^{1/2}$ között elég nagy n-re mindig van prímszám, ezért $p > n^{1/2} - n^{0,27}$, amivel a tételt tetszőleges n-re igazoltuk. ■

Megjegyzés: A tetszőleges n-re történő áttérésnél azt használtuk fel, hogy a prímek elég „sűrűn" helyezkednek el. Ha tudjuk, hogy m és $m + m^c$ között elég nagy m-re mindig van prímszám, akkor a tételünkben a hibatag $n^{c/2}$ nagyságrendűnek vehető. Mint az 5.5 pontban láttuk, a szomszédos prímek közötti hézag vizsgálata igen nehéz kerdés.

A 12.2.3 Tétel más bizonyításaira nézve lásd a 12.2.3 és 12.2.4 feladatot.

Most rátérünk a Sidon-sorozatok elemszámának a(z éles) felső becslésére.

12.2.4 Tétel **T 12.2.4**

Az $[1, n]$ intervallumba eső bármely Sidon-sorozatnak legfeljebb $n^{1/2} + n^{1/4} + 1$ eleme van. ♣

Első bizonyítás: Legyen t később alkalmasan megválasztandó egész szám, és toljunk végig egy $t - 1$ hosszúságú szakaszt a $[0, n]$ intervallumon, azaz tekintsük a $[-t + 1, 0], [-t + 2, 1], \ldots, [n, n + t - 1]$ intervallumokat. Legyen az s elemű Sidon-sorozat elemszáma az egyes intervallumokban $A_1, A_2, \ldots, A_{n+t}$. Ekkor nyilván

$$\sum_{i=1}^{n+t} A_i = ts\,. \tag{4}$$

Számoljuk össze *multiplicitással* azokat az $\{a_i, a_j\}$, $i > j$ elempárokat, amelyek egy-egy ilyen intervallumba esnek, azaz mindegyik elempárt annyiszor vegyük, ahány intervallum azt tartalmazza. Legyen D ezek együttes száma.

Ekkor nyilván

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \sum_{i=1}^{n+t} \frac{A_i^2}{2} - \sum_{i=1}^{n+t} \frac{A_i}{2}\,. \tag{5}$$

Másrészt, ha egy ilyen elempárban az $a_i - a_j$ különbség d, akkor ez az elempár pontosan $t-d$ intervallumba esik bele. A Sidon-tulajdonság miatt minden d legfeljebb egyszer fordulhat elő, így

$$D \le \sum_{d=1}^{t-1} (t-d) = \frac{t(t-1)}{2}\,. \tag{6}$$

(5) és (6) alapján

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \le t(t-1) \tag{7}$$

adódik. A számtani és négyzetes közép közötti egyenlőtlenség, valamint (4) felhasználásával (7) bal oldalát a következőképpen becsülhetjük alulról:

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \ge \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{n+t} - ts = \frac{t^2 s^2}{n+t} - ts\,. \tag{8}$$

Így (7) és (8) összekapcsolásával azt nyerjük, hogy

$$s^2 - s\left(\frac{n}{t}+1\right) - \left(\frac{n}{t}+1\right)(t-1) \le 0\,.$$

Ezt a másodfokú egyenlőtlenséget megoldva

$$s \le \frac{n}{2t} + \frac{1}{2} + \sqrt{n+t+\frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}}$$

adódik. Ha most t-nek a $t = \lfloor n^{3/4} \rfloor + 1$ értéket választjuk, akkor a tétel állítását kapjuk. ■

Második bizonyítás: Most bizonyos $a_i - a_j$ különbségek összegét fogjuk két oldalról megbecsülni. Legyen

$$K = \sum_{0<i-j\le r} (a_i - a_j)\,, \tag{9}$$

ahol r-et később alkalmasan megválasztjuk. A Sidon-tulajdonság miatt a (9)-beli összeg tagjai között nincs két azonos különbség, számuk

$$(s-1)+(s-2)+\cdots+(s-r)=rs-\frac{r(r+1)}{2}=rw\,,$$

ahol

$$w=s-\frac{r+1}{2}\,, \tag{10}$$

így K legalább akkora, mint az első rw darab pozitív egész összege, azaz

$$K\ge\frac{rw(rw+1)}{2}>\frac{r^2w^2}{2}\,. \tag{11}$$

Másrészt a (9)-beli összegnek része pl.

$$(a_s-a_{s-1})+(a_{s-1}-a_{s-2})+\cdots+(a_2-a_1)<a_s\le n$$

és számos más teleszkopikus összeg, amelyek hasonlóképpen becsülhetők felülről. Ezek általános alakja

$$(a_{s-\nu}-a_{s-\nu-\mu})+(a_{s-\nu-\mu}-a_{s-\nu-2\mu})+\cdots<a_{s-\nu}\le n\,,\quad 0\le\nu<\mu\le r\,.$$

Sőt az egész K ilyen teleszkopikus részösszegekre bontható, amelyeket úgy kapunk, hogy az indexek befutják az összes olyan 1 és s közötti (tovább már nem bővíthető) számtani sorozatot, amelynek differenciája legfeljebb r. Mivel μ differenciájú számtani sorozat éppen μ darab van, így a teleszkopikus részösszegek száma $1+2+\cdots+r=r(r+1)/2$, és mindegyik részösszeg értéke legfeljebb n, tehát

$$K\le\frac{nr(r+1)}{2}\,. \tag{12}$$

Egybevetve (11)-et és (12)-t, $2/r^2$-tel történő szorzás után a $w^2<n+n/r$ egyenlőtlenséget nyerjük. Innen gyökvonással és (10) felhasználásával kapjuk, hogy

$$s<\frac{r+1}{2}+\sqrt{n+\frac{n}{r}}\,.$$

Ha most r-nek az $r=\lfloor n^{1/4}\rfloor+1$ értéket választjuk, akkor a tétel állítását kapjuk. ■

Most rátérünk a végtelen Sidon-sorozatok vizsgálatára. Erdős 1955-ben megmutatta, hogy egy végtelen Sidon-sorozat már szükségképpen „ritkább”:

nem fordulhat elő, hogy a sorozatnak az $[1, n]$ intervallumba eső része minden n-re a véges maximum, vagyis $\sqrt{n}$ körüli elemszámot adjon:

12.2.5 Tétel **T 12.2.5**

Ha $A(n)$ jelöli egy végtelen A sorozat elemszámát n-ig, akkor bármely A végtelen Sidon-sorozatra szükségképpen

$$\liminf_{n\to\infty} \frac{A(n)}{\sqrt{n}} = 0, \quad \text{sőt} \quad \liminf_{n\to\infty} \frac{A(n)}{\sqrt{n/\log n}} < \infty. \ \clubsuit$$

Bizonyítás: Tekintsünk egy tetszőleges A végtelen Sidon–sorozatot, és legyen N egy nagy természetes szám. Jelöljük A_i-vel, hány eleme esik a sorozatnak az $[(i-1)N+1, iN]$ intervallumba, azaz

$$A_i = A(iN) - A((i-1)N), \quad i = 1, 2, \ldots, N.$$

Mivel egy–egy ilyen intervallumon belül a pontpárok különbsége $< N$, így a Sidon–tulajdonság miatt

$$\sum_{i=1}^{N} \binom{A_i}{2} < N\,.$$

Innen

$$2N > \sum_{i=1}^{N} A_i(A_i - 1) \geq \frac{1}{2} \sum_{i=1}^{N} (A_i^2 - 1)\,,$$

vagyis

$$\sum_{i=1}^{N} A_i^2 < 5N\,. \tag{13}$$

Most két oldalról meg fogjuk becsülni az

$$S = \sum_{i=1}^{N} \frac{A_i}{\sqrt{i}}$$

összeget. Egyrészt a Cauchy–Bunyakovszkij-egyenlőtlenség és (13) felhasználásával azt kapjuk, hogy

$$S \leq \sqrt{\left(\sum_{i=1}^{N} A_i^2\right)\left(\sum_{i=1}^{N} \frac{1}{i}\right)} <\approx \sqrt{5N \log N}\,. \tag{14}$$

Másrészt alakítsuk át S-et (az ún. Abel-féle átrendezés szerint) a következőképpen:

$$\begin{aligned} S &= \sum_{i=1}^{N} \frac{A(iN) - A((i-1)N)}{\sqrt{i}} > \\ &> \sum_{i=1}^{N-1} A(iN) \left(\frac{1}{\sqrt{i}} - \frac{1}{\sqrt{i+1}} \right) > \sum_{i=1}^{N-1} \frac{A(iN)}{2(i+1)\sqrt{i}} \,. \end{aligned} \tag{15}$$

Ha most feltesszük, hogy

$$A(iN) > c\sqrt{\frac{iN}{\log(iN)}}\,, \quad i = 1, 2, \ldots, N, \tag{16}$$

akkor (15) alapján

$$S > c \sum_{i=1}^{N-1} \frac{\sqrt{iN}}{2(i+1)\sqrt{i \log N^2}} = \frac{c\sqrt{N}}{\sqrt{8 \log N}} \sum_{i=1}^{N-1} \frac{1}{i+1} \approx \frac{c}{\sqrt{8}} \sqrt{N \log N} \tag{17}$$

következik.

Mivel $c > \sqrt{40}$ esetén (17) ellentmond (14)-nek, így $c > \sqrt{40}$ mellett (16) nem teljesülhet, ami igazolja a tétel állítását. ■

A 12.2.5 Tétel nem jelenti azt, hogy egy végtelen Sidon-sorozat ne lehetne „időnként" olyan sűrű, mint egy véges: Erdős, majd F. Krückeberg konstruált olyan végtelen Sidon-sorozatot, amelynek végtelen sok n-re az $[1, n]$ intervallumba eső szelete „közel" $\sqrt{n}$ elemet tartalmaz (lásd a 12.2.5 feladatot).

Ha most egy minden véges szeletében „elég" sűrű Sidon-sorozatot szeretnénk megadni, akkor az ún. mohó algoritmussal készíthetünk egy olyant, amelynek n-ig mindig legalább $\sqrt[3]{n}$ eleme van (lásd a 12.2.1 feladatot). Meglepő, hogy ezt a nagyságrendet nagyon hosszú ideig egyáltalán nem sikerült megjavítani. Csak 1981-ben igazolták Ajtai Miklós, Komlós János és Szemerédi Endre, hogy létezik olyan végtelen Sidon-sorozat, amelynek minden (elég nagy) n-re n-ig legalább $c\sqrt[3]{n \log n}$ eleme van, ahol c alkalmas pozitív konstans. Amint látjuk, ez is csak „alig" volt jobb, mint a mohó algoritmussal adódó $\sqrt[3]{n}$. 1997-ben Ruzsa Imre ezt jelentősen megjavította $cn^{\sqrt{2}-1-\varepsilon}$-ra, azonban még ez az eredmény is igen messze van az Erdős által sejtett $n^{1/2-\varepsilon}$-os nagyságrendtől (ahol ε tetszőlegesen kicsi pozitív valós szám).

Végül tekintsünk olyan végtelen sorozatokat, amelyekre a Sidon-tulajdonság helyett csak azt a gyengébb kikötést tesszük, hogy a pozitív egészeknek

az $a_i + a_j$ alakban történő előállításszáma maradjon korlátos (a Sidon-sorozatoknál ez a korlát 1). Megmutatjuk, hogy az ilyen sorozatokra az $n^{1/2-\varepsilon}$-os nagyságrend valóban elérhető:

12.2.6 Tétel **T 12.2.6**

Minden $\epsilon > 0$-hoz létezik olyan m egész és olyan $A = \{1 \le a_1 < a_2 < \ldots\}$ végtelen sorozat, amelyre

$$\liminf_{n\to\infty} \frac{A(n)}{n^{1/2-\epsilon}} > 0,$$

és bármely természetes szám legfeljebb m-féleképpen áll elő $a_i + a_j$ alakban. ♣

A 12.2.6 Tétel Erdős és Rényi eredménye, bizonyításuk az ún. véletlen módszerek egyik első számelméleti megjelenése volt: a természetes számok sorozatainak halmazán alkalmas valószínűségi mezőt bevezetve azt mutatták meg, hogy (ezen valószínűség szerint) „majdnem minden" számsorozat megfelel a követelményeknek. Ezt a módszert használjuk majd a 12.6.3 Tétel bizonyításánál.

A 12.2.6 Tételre adott alábbi elemi bizonyítás Ruzsa Imrétől származik.

Bizonyítás: Változó alapú számrendszert fogunk használni, azaz a számokat

$$c_0 + c_1k_1 + c_2k_1k_2 + \cdots + c_ik_1 \ldots k_i + \cdots$$

alakban írjuk fel, ahol $k_1, k_2, \ldots$ rögzített 1-nél nagyobb egészek (a „változó alap") és $0 \le c_i < k_{i+1}$ a számjegyek. Az alapokat most lassan növő sorozatként úgy választjuk meg, hogy valamilyen kis rögzített pozitív δ-val

$$k_{i+1} \approx k_i^{1+\delta} \tag{18}$$

teljesüljön. Lerögzítünk továbbá minden i-re 0 és $k_i/2$ között egy-egy maximális elemszámú (véges) S_i Sidon-sorozatot.

A tétel előírásainak megfelelő sorozatot ezután a következőképpen konstruálunk. Azokat a számokat vesszük, amelyek minden számjegye a megfelelő Sidon-sorozatból való, azaz $c_i \in S_{i+1}$, és ráadásul legfeljebb t kivétellel valamennyi számjegy 0.

Az ilyen számok összeadásakor nem keletkezik átvitel, és így a Sidon-tulajdonság miatt bármely természetes szám legfeljebb 2^t-féleképpen áll elő két ilyen szám összegeként (a jegyek az egyes helyiértékeken felcserélődhetnek),

tehát $m = 2^t$. A megfelelő sűrűséget δ és t alkalmas megválasztásával fogjuk biztosítani.

Legyen n tetszőleges, ekkor alkalmas j-re

$$k_1 k_2 \dots k_j \le n < k_1 k_2 \dots k_j k_{j+1} \,. \tag{19}$$

A sorozatban biztosan szerepelnek azok az egészek, amelyek számjegyeire

$$c_0 = c_1 = \dots = c_{j-t-1} = 0 \quad \text{és} \quad c_i \in S_{i+1},\ i = j-t, \dots, j-1 \tag{20}$$

teljesül. Megmutatjuk, hogy már ezek száma is $> n^{1/2-\varepsilon}$, ha a δ-t elég kicsinek, t értékét pedig elég nagynak választjuk.

Nézzük a részleteket. Legyen $k_1 = r$ és (18)-nak megfelelően

$$k_i = \left\lfloor\, r^{(1+\delta)^{i-1}} \right\rfloor , \tag{21}$$

és így

$$|S_i| > \sqrt{\frac{k_i}{3}} > r^{h_i}, \quad \text{ahol} \quad h_i = \frac{(1+\delta)^{i-1} - \log_r 4}{2} \,. \tag{22}$$

A (20)-nak eleget tevő számok számát K-val jelölve, elég belátnunk, hogy minden elég nagy n-re

$$K > n^{1/2-\varepsilon} \,, \quad \text{azaz} \quad \log_r K > \Big(\frac{1}{2} - \varepsilon\Big) \log_r n \,. \tag{23}$$

Először felülről becsüljük $\log_r n$-et (19) és (21) alapján:

$$\log_r n < \log_r (k_1 k_2 \dots k_{j+1}) \le 1 + (1+\delta) + \dots + (1+\delta)^j < \frac{(1+\delta)^{j+1}}{\delta} \,. \tag{24}$$

Most alulról becsüljük $\log_r K$-t. Mivel $K = |S_{j-t+1}| \cdot \ldots \cdot |S_j|$, így (22) alapján

$$\begin{aligned} \log_r K &> \frac{(1+\delta)^{j-t} + \dots + (1+\delta)^{j-1} - t \log_r 4}{2} = \\ &= \frac{(1+\delta)^{j-t}\big((1+\delta)^t - 1\big)}{2\delta} - \frac{t \log_r 4}{2} = \\ &= \frac{(1+\delta)^j}{2\delta}\big(1 - (1+\delta)^{-t}\big) - \frac{t \log_r 4}{2} \,. \end{aligned} \tag{25}$$

Végül (24) és (25) alapján

$$\frac{2\log_r K}{\log_r n} > \frac{(1+\delta)^j\bigl(1-(1+\delta)^{-t}\bigr)-t\delta\log_r 4}{(1+\delta)^{j+1}} = \\ = \frac{1-(1+\delta)^{-t}}{1+\delta} - \frac{t\delta\log_r 4}{(1+\delta)^{j+1}}. \tag{26}$$

Válasszuk először δ-t elég kicsire, majd utána t értékét elég nagyra ahhoz, hogy (26) utolsó sorában az első tag nagyobb legyen, mint $1-\varepsilon$. Mivel a második tag számlálója ezután már konstans, a nevező pedig végtelenhez tart, ha $j\to\infty$, így elég nagy j-re (azaz elég nagy n-re) a második tag kisebb, mint ε, és így az egész kifejezés nagyobb, mint $1-2\varepsilon$, amivel (23)-at beláttuk. ■

Feladatok

12.2.1 Mutassuk meg, hogy a mohó algoritmussal 1 és n között egy legalább $\sqrt[3]{n}$ elemű Sidon-sorozatot kapunk.

12.2.2 Legyen p prímszám és $a_i = 1+2ip+\langle i^2 \bmod p\rangle \quad i=0,1,\dots,p-1$, ahol $\langle i^2 \bmod p\rangle$ az i^2 legkisebb nemnegatív maradékát jelöli modulo p. Lássuk be, hogy így $n=2p^2$-re egy $\sqrt{n/2}$ elemszámú Sidon-sorozatot kapunk az $[1,n]$ intervallumban.

M*12.2.3 Legyen p tetszőleges prímszám. Ekkor létezik p darab olyan a_i, amelyekre az a_i+a_j összegek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo p^2-1.

Megjegyzés: Az előzővel nyilván ekvivalens, hogy $i\neq j$-re az a_i-a_j különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo p^2-1. A szereplő különbségek száma p^2-p, és modulo p^2-1 összesen csak p^2-2 darab nemnulla maradék van. Vagyis az a_i-a_j különbségek majdnem minden maradékot előállítanak. A bizonyításból leolvasható, hogy éppen a $p+1$-gyel osztható maradékok maradnak ki. — A feladatból a 12.2.3 Tétel hasonló módon vezethető le, mint ahogyan a 12.2.2 Tételből következett (ugyanez érvényes a következő feladatra is).

M*12.2.4 Legyen p tetszőleges prímszám. Ekkor létezik $p-1$ darab olyan a_i, amelyekre az a_i-a_j, $i\neq j$ különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo p^2-p.

12.2.5 Konstruáljunk olyan A végtelen Sidon-sorozatot, amelyre bármely $\varepsilon>0$ esetén *végtelen sok* n-re $A(n)>(1/\sqrt{2}-\varepsilon)\sqrt{n}$ (azaz $\limsup_{n\to\infty} A(n)/\sqrt{n}\geq 1/\sqrt{2}$).

Megjegyzés: Megoldatlan, hogy ugyanez $1/\sqrt{2}$ helyett 1-gyel is igaz-e.

12.2.6 *Többtagú összegek*. Legyen $h \geq 2$ rögzített természetes szám, és az $[1, n]$ intervallumban tekintsünk most olyan sorozatokat, ahol az elemekből képezett h-tagú összegek mind különbözők. (A $h = 2$ eset éppen a Sidon-sorozatokat jelenti.)

*a) Mutassuk meg, hogy van olyan sorozat, amelynek „körülbelül" $n^{1/h}$ eleme van.

b) Lássuk be, hogy van olyan csak a h-tól függő $c = c(h)$ konstans, hogy minden ilyen sorozatnak legfeljebb $c(h)n^{1/h}$ eleme van.

Megjegyzés: Megoldatlan probléma, hogy $c(h)$ vajon $1 + \varepsilon$-ra csökkenthető-e, azaz bármely h-ra igaz-e, hogy a $h = 2$ esethez hasonlóan a maximális elemszám aszimptotikusan $n^{1/h}$. A 12.2.4 Tétel bizonyítása azért nem vihető át, mert $h \neq 2$-re a feltételt nem lehet összegekről különbségekre átjátszani.

12.2.7 Mutassuk meg, hogy létezik egészeknek olyan $a_1 < a_2 < \ldots$ végtelen sorozata, hogy a 0-n kívül minden egész szám egyértelműen írható fel $a_i - a_j$ alakban.

12.2.8 A természetes számok két (végtelen) részsorozatát, A-t és B-t nevezzük jó sorozatpárnak, ha az $a+b$ ($a \in A$, $b \in B$) összegek mind különbözők. Jó sorozatpárt kapunk például, ha egy Sidon-sorozatot két részre vágunk. Lássuk be, hogy léteznek ennél „sűrűbb" jó sorozatpárok is: adjunk meg olyat, amelynél minden n-re $A(n) > c\sqrt{n}$, $B(n) > c\sqrt{n}$ alkalmas $c > 0$ konstanssal.

12.3. Összeghalmazok

Ebben a pontban $A + A = \{a_i + a_j \mid a_i, a_j \in A\}$ típusú halmazokkal foglalkozunk, ahol A elemei a $[0, n-1]$ intervallumba eső egészek vagy pedig modulo p maradékosztályok, ahol p prím. Jelölje A elemszámát $|A| = k$.

$A + A$ elemszáma akkor a lehető legnagyobb, ha A Sidon-sorozat, ekkor $|A+A| = \binom{k+1}{2}$. Most először az ellenkező végletet vizsgáljuk meg: mekkora lehet $|A + A|$ lehető legkisebb értéke. Ha A elemei egész számok, akkor ez a várakozásnak megfelelően akkor lép fel, ha A elemei egy számtani sorozat egymást követő tagjai, és így $\min |A + A| = 2k - 1$ (lásd a 12.3.1 feladatot). Hasonló eredmény adódik $|A + A|$ minimumára akkor is, ha $A \subseteq \mathbf{Z}_p$ (azaz A elemei modulo p maradékosztályok), ezt a (már egyáltalán nem nyilvánvaló) tényt a 12.3.1 Tételben igazoljuk. Ezt a tételt már Cauchy is bebizonyí-

totta, majd 120 évvel később két kiváló matematikus, Davenport és Chowla, egymástól függetlenül újra felfedezte. A tételre két bizonyítást adunk, és a feladatok között a tételnek, illetve a bizonyítási módszereknek több érdekes alkalmazását mutatjuk be (lásd a 12.3.3–12.3.8 feladatokat).

Az összeghalmazokkal kapcsolatos másik vizsgálatunk is valamilyen értelemben a Sidon-tulajdonság duálisának tekinthető. A véges Sidon-sorozatok esetén olyan, minél *nagyobb* elemszámú A halmazok előállítása volt a(z egyik) cél, hogy minden egész szám *legfeljebb* egyféleképpen legyen felírható $a_i + a_j$ alakban. Most olyan, minél *kisebb* elemszámú A halmazokat keresünk, hogy minden, a $[0, n-1]$ intervallumba eső egész szám *legalább* egyféleképpen legyen felírható $a_i + a_j$ alakban. Az ilyen tulajdonságú A halmazokat (másodrendű additív) *bázis*oknak nevezzük. A bázisok elemszámának minimumára a 12.3.3 Tételben adunk alsó és felső becslést.

Térjünk rá $|A + A|$ minimumának a meghatározására, ha $A \subseteq \mathbf{Z}_p$. Kicsit általánosabban, az $A + B = \{a + b \mid a \in A, b \in B\}$ halmaz elemszámának minimumát fogjuk meghatározni $|A|$ és $|B|$ függvényében. Ezt nemcsak azért tesszük, hogy minél általánosabb eredményt nyerjünk, hanem — mint a matematikában oly sokszor — az általánosítás adja a kulcsot magának az eredeti állításnak az igazolásához is.

12.3.1 Tétel (Cauchy–Davenport–Chowla-tétel) **T 12.3.1**

Legyen p prím, $A, B \subseteq \mathbf{Z}_p$, $|A| = k(> 0)$, $|B| = r(> 0)$. Ekkor

$$|A + B| \geq \min(p, k + r - 1). \ \clubsuit \tag{1}$$

A p-re mint korlátra (1)-ben azért van szükség, mert $A + B \subseteq \mathbf{Z}_p$, és így nyilván $|A + B| \leq p$.

Az egyenlőtlenség éles: ha $A = \{0, 1, \ldots, k-1\}$, $B = \{0, 1, \ldots, r-1\}$, akkor ($k+r \leq p+1$ esetén) $A+B = \{0, 1, \ldots, k+r-2\}$, tehát $|A+B| = k+r-1$, azaz (1)-ben egyenlőség teljesül.

Az $A = B$ speciális esetben kapjuk, hogy $|A + A| \geq \min(p, 2k - 1)$, és egyenlőség teljesül, ha (például) $A = \{0, 1, \ldots, k-1\}$.

Első bizonyítás: Tegyük fel indirekt, hogy (valamilyen rögzített p mellett) van olyan A és B, amelyre (1) nem igaz, és nevezzük (házi használatra) csúnyának az ilyen halmazpárokat.

Tekintsünk egy olyan A, B csúnya halmazpárt, $|A| = k$, $|B| = r$, amelyre r a lehető legkisebb. Konstruálni fogunk olyan A', B' csúnya halmazpárt, $|A'| = k'$, $|B'| = r'$, ahol $r' < r$, ami ellentmond r minimalitásának. Ez azt

jelenti, hogy az indirekt feltevésünk (ti. hogy léteznek csúnya halmazpárok) ellentmondásra vezetett, amivel a tétel állítását bebizonyítottuk.

Ha $k+r-1>p$, akkor B-ből hagyjunk el $k+r-1-p(<r)$ elemet, a maradék halmazt jelölje B', és legyen $A'=A$. Nyilván

$$|A'+B'|\le|A+B|<\min(p,k+r-1)=p=\min(p,k'+r'-1),$$

tehát A', B' is csúnya és $(0<)r'<r$, ami lehetetlen. Ezért $k+r-1\le p$.

Nyilván $k\ge r\ge 2$, hiszen $k<r$ esetén A és B szerepcseréjével ellentmondásra jutunk r minimalitásával, $r=1$ esetén pedig (1)-ben egyenlőség áll, azaz A, B nem lenne csúnya. Mivel $r\ge 2$ és $k+r-1\le p$, ezért $k<p$ is teljesül.

Azt is feltehetjük, hogy $0\in B$, mivel B minden eleméhez ugyanazt az értéket hozzáadva, $|A|$, $|B|$ és $|A+B|$ egyike sem változik.

Megmutatjuk, hogy ha $b\ne 0$ tetszőleges rögzített eleme B-nek, akkor $A+b=\{a+b\mid a\in A\}\not\subseteq A$. Ellenkező esetben ugyanis $A+b=A$ teljesülne, és így a két oldalon álló halmazok elemeinek összege megegyezne:

$$\sum_{a\in A}a=\sum_{a\in A}(a+b)=kb+\sum_{a\in A}a,\quad\text{vagyis}\quad kb=0,$$

ami $k<p$ és $b\ne 0$ miatt lehetetlen.

Az előzők alapján van olyan $a_1\in A$ és $b_1\in B$, amelyre $a_1+b_1\notin A$. Legyen

$$A'=A\cup\{a_1+b\mid b\in B,a_1+b\notin A\}\quad\text{és}\quad B'=\{b\mid a_1+b\in A\}.$$

Ekkor nyilván $k'+r'=k+r$ és $0<r'<r$ (hiszen $0\in B'$, de $b_1\notin B'$). Megmutatjuk, hogy $A'+B'\subseteq A+B$. Legyen $a'+b'\in A'+B'$. Ha $a'\in A$, akkor nyilván $a'+b'\in A+B$. Ha $a'=a_1+b$, akkor

$$a'+b'=(a_1+b)+b'=(a_1+b')+b\in A+B,$$

hiszen B' definíciója miatt $a_1+b'\in A$. Mindezek alapján

$$|A'+B'|\le|A+B|<\min(p,k+r-1)=k+r-1=k'+r'-1=\min(p,k'+r'-1),$$

tehát A', B' is csúnya, továbbá $r'<r$, amivel a kívánt ellentmondásra jutottunk. ■

A 12.3.1 Tétel második bizonyításához szükségünk lesz az alábbi egyszerű segédtételre:

12.3.2 Lemma **L 12.3.2**

Legyen T tetszőleges kommutatív test, $A, B \subseteq T$, $|A| = k$, $|B| = r$, és $f(x, y)$ olyan T feletti kétváltozós polinom, amelynek x, illetve y szerinti foka k-nál, illetve r-nél kisebb (azaz $f(x, y) = \sum_{i<k,\, j<r} \alpha_{ij} x^i y^j$). Tegyük fel, hogy minden $a \in A$ és $b \in B$ esetén $f(a, b) = 0$. Ekkor f a nullpolinom (azaz minden együtthatója 0). ♣

A 12.3.2 Lemma bizonyítása: Írjuk fel $f(x, y)$-t y polinomjaként, ekkor az együtthatók x polinomjai lesznek:

$$f(x, y) = h_0(x) + h_1(x)y + \ldots + h_{r-1}(x)y^{r-1}, \quad \deg h_i \leq k - 1. \qquad (2)$$

Legyen $a \in A$-ra

$$g_a(y) = f(a, y) = h_0(a) + h_1(a)y + \ldots + h_{r-1}(a)y^{r-1}.$$

Ekkor egyrészt $\deg g_a \leq r - 1$, másrészt minden $b \in B$-re $g_a(b) = f(a, b) = 0$, azaz g_a-nak legalább r gyöke van. Ez csak úgy lehetséges, ha g_a minden együtthatója 0. Ez azt jelenti, hogy a legfeljebb $k-1$-edfokú h_i polinomoknak minden $a \in A$ gyöke, azaz legalább k gyökük van, és így szükségképpen $h_i = 0$ (azaz minden együtthatójuk 0). Ebből (2) alapján kapjuk, hogy $f = 0$. ■

A 12.3.1 Tétel második bizonyítása: Indirekt tegyük fel, hogy van olyan A és B, amelyre (1) nem igaz. Az első bizonyításban látottak szerint feltehető, hogy $k + r - 1 \leq p$ (ahol $|A| = k$, $|B| = r$). Legyen $C = A + B$, ekkor $|C| \leq k + r - 2 < p$. Legyen

$$f_1(x, y) = (x + y)^m \prod_{c \in C} (x + y - c), \quad \text{ahol } m = k + r - 2 - |C|. \qquad (3)$$

Ekkor $f_1(a, b) = 0$ minden $a \in A$, $b \in B$ esetén.

Az $f_1(x, y)$ polinomra közvetlenül nem alkalmazhatjuk a 12.3.2 Lemmát, mert előfordulnak benne olyan $x^i y^j$ tagok, amelyekben $i \geq k$ vagy $j \geq r$. Tekintsünk egy tetszőleges x^i-t, ahol $i \geq k$, és cseréljük ezt ki egy olyan legfeljebb $k-1$-edfokú $u_i(x)$ polinomra, amely minden $a \in A$ helyen ugyanazt az értéket veszi fel, mint x^i, azaz minden $a \in A$-ra $u_i(a) = a^i$. Ilyen $u_i(x)$ ún. interpolációs polinom (egyértelműen) létezik (lásd például Freud: Lineáris algebra, 3.2.4 Tétel). Hasonlóan járjunk el, ha $j \geq r$, ekkor y^j helyére kerül olyan legjeljebb $r - 1$-edfokú $v_j(y)$, amelynél minden $b \in B$-re $v_j(b) = b^j$.

Az így kapott $f(x, y)$ polinomra $f(a, b) = f_1(a, b) = 0$ minden $a \in A$, $b \in B$ esetén, továbbá csak olyan $x^i y^j$ tagok szerepelnek f-ben, ahol $i \leq k-1$, $j \leq r - 1$. A 12.3.2 Lemma szerint így f minden együtthatója 0.

Vizsgáljuk most meg f-ben $x^{k-1}y^{r-1}$ együtthatóját közvetlenül is.

Mivel az f_1 polinomban (3) alapján csak $(x+y)^{k+r-2}$-ből keletkeznek olyan x^iy^j tagok, ahol $i+j=k+r-2$, minden más tagra $i+j<k+r-2$, továbbá az f-et előállító redukciós eljárás során az $i\geq k$, illetve $j\geq r$ típusú x^i, illetve y^j tényezők kisebb fokszámúakra cserélődnek, így f-ben egyetlen $x^{k-1}y^{r-1}$ tag képződik, az, amely az $(x+y)^{k+r-2}$ hatványozás elvégzéséből közvetlenül adódik; ennek együtthatója $\binom{k+r-2}{k-1}$. Mivel $k+r-2<p$, ezért ez az együttható ($\mathbf{Z}_p$-ben) nem 0. Ez ellentmond annak, hogy f minden együtthatója 0. ■

Most rátérünk a bázisok elemszámának vizsgálatára. A definíciót megismételve, a $[0,n-1]$ intervallum egy (másodrendű additív) bázisán nemnegatív egészek olyan A halmazát értjük, hogy minden $0\leq r\leq n-1$ egész felírható két A-beli elem összegeként, azaz $r=a_i+a_j$ alakban $(a_i,a_j\in A)$.

Ha $|A|=k$, akkor az a_i+a_j összegek száma $\binom{k+1}{2}$, és ha A bázis, akkor ezek az összegek legalább n különböző értéket adnak, tehát

$$\binom{k+1}{2}\geq n,\qquad \text{azaz}\qquad k>\sqrt{2n}-\frac{1}{2}\,.$$

Másrészt, ha n négyzetszám, $n=s^2$, akkor az n-nél kisebb egészek az s alapú számrendszerben (legfeljebb) kétjegyűek, vagyis felírhatók $i+sj$ alakban, ahol $0\leq i,j\leq s-1$. Ezt azt jelenti, hogy

$$A=\{0,1,\dots,s-1,s,2s,\dots,(s-1)s\}$$

másodrendű bázis, amelynek elemszáma $2s=2\sqrt{n}$. Ha n nem négyzetszám, akkor a fentieket n helyett az n-et követő legkisebb négyzetszámra lehet elmondani, ekkor tehát $s=\lceil\sqrt{n}\rceil$.

Az előző meggondolásokból a bázisok elemszámának minimumára az alábbi becsléseket kapjuk:

$$\sqrt{2n}-\frac{1}{2}<\min k<2\sqrt{n}+2\,. \tag{4}$$

A következő tételben megmutatjuk, hogy $\sqrt{n}$ együtthatója mindkét becslésben (valamelyest) javítható:

12.3.3 Tétel **T 12.3.3**

Jelölje $f(n)$ a $[0, n-1]$ intervallumra vonatkozó másodrendű additív bázisok elemszámának minimumát. Ekkor bármely $\varepsilon > 0$ mellett elég nagy n-re

$$\sqrt{\frac{289}{144}}\sqrt{n} - 2 < f(n) < (\sqrt{3{,}5} + \varepsilon)\sqrt{n}. \ \clubsuit \tag{5}$$

A Fried Katalintól származó felső becslés a jelenleg ismert legjobb eredmény, az alsó becslés esetén a (Leo Mosertől származó) módszer további finomításával valamivel jobb konstans is elérhető.

Bizonyítás: A felső becsléshez vegyük észre, hogy a tétel kimondása előtt megadott számrendszeres konstrukció tulajdonképpen két számtani sorozat egyesítéseként állítja elő a bázist. Ennek a gondolatnak a variálásával most öt számtani sorozat uniójaként készítjük el a megfelelő bázist.

Legyen t tetszőleges pozitív egész, és tekintsük az alábbi öt (diszjunkt) számtani sorozatot:

$$\begin{aligned}
B &= \{b_0, \ldots, b_t\} &&= \{j \mid 0 \le j \le t\};\\
C &= \{c_0, \ldots, c_{3t-1}\} &&= \{2t+1+j(t+1) \mid 0 \le j \le 3t-1\};\\
D &= \{d_0, \ldots, d_t\} &&= \{3t^2+5t+1+j \mid 0 \le j \le t\};\\
E &= \{e_0, \ldots, e_t\} &&= \{6t^2+12t+3+jt \mid 0 \le j \le t\};\\
F &= \{f_0, \ldots, f_t\} &&= \{10t^2+18t+5+jt \mid 0 \le j \le t\}.
\end{aligned}$$

A számtani sorozatok különbsége tehát rendre $1, t+1, 1, t, t$, az elemszámuk pedig $t+1, 3t, t+1, t+1, t+1$.

Jelölje A_t az öt sorozat egyesítését, ekkor $|A_t| = 7t+4$. Belátjuk, hogy A_t másodrendű bázis $n = 14t^2+24t+7$-re, azaz $14t^2+24t+6$-ig minden egész előáll két A_t-beli elem összegeként. Innen a felső becslés már következik: tetszőleges n esetén vegyük azt a legkisebb t értéket, amelyre $n \le 14t^2+24t+7$, ekkor A_t megfelelő bázis n-hez és $|A_t| = 7t+4 \sim \sqrt{3{,}5n}$, ha $n \to \infty$ (hiszen $t \sim \sqrt{n/14}$).

Most tehát azt igazoljuk, hogy minden $0 \le r \le 14t^2+24t+6$ egész felírható két A_t-beli elem összegeként. Jelöljük $[[x, y]]$-nal az $[x, y]$ intervallumba eső egészek halmazát. Nyilván

$$B + B = [[0\,,\, 2t]] \qquad \text{és} \qquad B + C = [[2t+1\,,\, 3t^2+5t]].$$

Hasonlóan adódik, hogy

$$\begin{aligned}
B + D &= [[3t^2 + \ \ 5t + 1\,,\, 3t^2 + \ \ 7t + 1]],\\
C + D &= [[3t^2 + \ \ 7t + 2\,,\, 6t^2 + 10t + 1]],\\
D + D &= [[6t^2 + 10t + 2\,,\, 6t^2 + 12t + 2]],\\
B + E &= [[6t^2 + 12t + 3\,,\, 7t^2 + 13t + 3]].
\end{aligned}$$

Az eddigiek alapján $A_t + A_t \supseteq [[0\,,\, 7t^2 + 13t + 3]]$.
Most megmutatjuk, hogy $C + E \supseteq [[7t^2 + 13t + 4\,,\, 9t^2 + 17t + 3]]$. Először is

$$c_0 + e_{t-1} = (2t + 1) + (7t^2 + 11t + 3) = 7t^2 + 13t + 4.$$

Mivel a C sorozat differenciája $t + 1$, az E-é pedig t, ezért érdemes C egymás után következő elemeihez rendre E-nek mindig a megfelelő korábbi elemeit hozzáadni:

$$\begin{aligned}
c_1 + e_{t-2} &= c_0 + e_{t-1} + 1,\\
c_2 + e_{t-3} &= c_0 + e_{t-1} + 2,\\
&\dots\\
c_{t-1} + e_0 &= c_0 + e_{t-1} + (t - 1).
\end{aligned}$$

A következő egészt a $c_0 + e_t = c_0 + e_{t-1} + t$ összegként kapjuk meg, majd ismét C elemein előre, E elemein pedig visszafelé haladva a $c_i + e_{t-i}$ összegek minden egészt előállítanak $c_t + e_0 = c_0 + e_t + t$-ig. Ezután $c_1 + e_t = c_0 + e_t + (t + 1)$-re ugorva, majd a $c_{1+i} + e_{t-i}$ összegeket véve megkapjuk a következő $t + 1$ egészt. Az eljárást hasonlóan folytatva egészen a $c_{3t-1} + e_1 = 9t^2 + 17t + 3$ összegig juthatunk el, azaz valóban $C + E \supseteq [[7t^2 + 13t + 4\,,\, 9t^2 + 17t + 3]]$.

Továbbhaladva, nyilván $D + E = [[9t^2 + 17t + 4\,,\, 10t^2 + 18t + 4]]$.

Végül, az előzőekhez hasonlóan megmutatható, hogy

$$\begin{aligned}
B + F &= [[10t^2 + 18t + 5\,,\, 11t^2 + 19t + 5]],\\
C + F &= [[11t^2 + 19t + 6\,,\, 13t^2 + 23t + 5]],\\
D + F &= [[13t^2 + 23t + 6\,,\, 11t^2 + 24t + 6]].
\end{aligned}$$

Ezzel igazoltuk, hogy valóban minden $0 \le r \le 14t^2 + 24t + 6$ egész számra $r \in A_t + A_t$, és ezzel a felső becslés bizonyítását befejeztük.

Az alsó becsléshez tekintsünk egy $A = \{0 \le a_1 < \dots < a_k \le n - 1\}$ tetszőleges másodrendű bázist a $[0, n - 1]$ intervallumon. Legyen

$$h(x) = \sum_{i=1}^{k} x^{a_i} \tag{6}$$

az A bázishoz tartozó „generátorfüggvény”, ekkor

$$h^2(x) = \Big(\sum_{i=1}^{k} x^{a_i}\Big)\Big(\sum_{j=1}^{k} x^{a_j}\Big) = \sum_{i,j=1}^{k} x^{a_i+a_j} = 2\sum_{1\le i<j\le k} x^{a_i+a_j} + \sum_{i=1}^{k} x^{2a_i} =$$

$$= 2\sum_{1\le i\le j\le k} x^{a_i+a_j} - \sum_{i=1}^{k} x^{2a_i} = 2\sum_{1\le i\le j\le k} x^{a_i+a_j} - h(x^2).$$

Innen

$$g(x) = \sum_{1\le i\le j\le k} x^{a_i+a_j} = \frac{h^2(x)+h(x^2)}{2}. \tag{7}$$

A $g(x)$ polinomban x^r együtthatója éppen azt mutatja, hogy az r hányféleképpen áll elő $a_i + a_j$ alakban, ahol $i \le j$. Mivel az $a_i + a_j$ összegek minden $0 \le r \le n-1$ számot előállítanak, ezért ezekre az r-ekre x^r együtthatója legalább 1, azaz

$$g(x) = 1 + x + \ldots + x^{n-1} + \sum_{m=0}^{2n-2} u_m x^m, \quad \text{ahol } \ u_m \ge 0. \tag{8}$$

(7) és (8) alapján

$$g(1) = \frac{h^2(1)+h(1)}{2} = \frac{k^2+k}{2} = n + \sum_{m=0}^{2n-2} u_m. \tag{9}$$

Mivel $u_m \ge 0$, ezért (9)-ből azonnal kapjuk, hogy $(k^2+k)/2 \ge n$, ami a tételünk kimondása előtti $k \ge \sqrt{2n} - (1/2)$ becslést adja. Ezt akkor tudjuk javítani, ha $\sum_{m=0}^{2n-2} u_m$-re a 0-nál (lényegesen) jobb alsó becslést találunk.

Megmutatjuk, hogy

$$S = \sum_{m=0}^{2n-2} u_m > \nu k^2, \tag{10}$$

ahol a $\nu > 0$ konstans értékét a bizonyításból explicite meg fogjuk határozni, és azt (9)-be visszahelyettesítve adódik majd a tétel állításában szereplő alsó becslés.

Jelölje $N = \tau k$, illetve $P = (1-\tau)k$ azoknak az a_i-knek a számát, amelyekre $a_i > (n-1)/2$, illetve $a_i \le (n-1)/2$ (itt tehát $N + P = k$ és τ a „nagy” a_i elemek *arányát* jelöli ebben a konkrét A bázisban).

Vegyük észre, hogy $S' = \sum_{m=n}^{2n-2} u_m$ éppen az $n-1$-nél nagyobb $a_i + a_j$, $i \le j$ összegeknek a száma. Ha a_i és a_j is nagyobb, mint $(n-1)/2$, akkor $a_i + a_j > n-1$, tehát

$$S \ge S' \ge \frac{(N+1)N}{2} = \frac{(\tau k+1)(\tau k)}{2} \ge \frac{\tau^2}{2} \cdot k^2. \tag{11}$$

(Ez szemléletesen azt jelenti, hogy ha „sok" $(n-1)/2$-nél nagyobb a_i van, akkor sok összeg „vész kárba", és így nagyobb elemszámú bázis szükséges az $n-1$-ig terjedő számok előállításához. Ehhez a meggondoláshoz nem is lett volna szükség a generátorfüggvényre. Azonban, ha A-ban a „pici" a_i elemek dominálnak, akkor már csak így boldogulunk, lásd az alábbiakban.)

Helyettesítsünk most be (8)-ba az x helyére egy $\varrho \ne 1$ komplex n-edik egységgyököt. Ekkor a jobb oldal elején szereplő $1 + \varrho + \ldots + \varrho^{n-1}$ összeg 0, tehát

$$g(\varrho) = \sum_{m=0}^{2n-2} u_m \varrho^m.$$

Mindkét oldal abszolút értékét véve

$$|g(\varrho)| = \Big|\sum_{m=0}^{2n-2} u_m \varrho^m\Big| \le \sum_{m=0}^{2n-2} |u_m| \cdot |\varrho|^m = \sum_{m=0}^{2n-2} u_m = S,$$

hiszen $u_m \ge 0$ és $|\varrho| = 1$. Innen (7) alapján

$$S \ge |g(\varrho)| = \frac{|h^2(\varrho) + h(\varrho^2)|}{2} \ge \frac{|h^2(\varrho)|}{2} - \frac{|h(\varrho^2)|}{2}. \tag{12}$$

Ezt folytatva a (12) jobb szélén álló különbségre kell alsó becslést adnunk, azaz a kivonandót felülről, a kisebbítendőt pedig alulról kell becsülnünk.

A $h(x)$ generátorfüggvény (6) definíciója alapján

$$|h(\varrho^2)| = \Big|\sum_{i=1}^{k} \varrho^{2a_i}\Big| \le \sum_{i=1}^{k} |\varrho|^{2a_i} = k,$$

hiszen $|\varrho| = 1$, tehát

$$\frac{|h(\varrho^2)|}{2} \le \frac{k}{2} \tag{13}$$

(ami elhanyagolható lesz a másik kérdéses tag, a $|h^2(\varrho)|/2$ kisebbítendő k^2-es nagyságrendjéhez képest).

Alsó becslést keresünk tehát a

$$|h(\varrho)| = \Big|\sum_{i=1}^{k} \varrho^{a_i}\Big| \tag{14}$$

kifejezésre. Emlékezzünk vissza, hogy lényegében azzal az esettel kell megbirkóznunk, amikor az $(n-1)/2$-nél nem nagyobb a_i-k dominálnak, vagyis $P = (1-\tau)k$ nagy. Ennek megfelelően (14)-ben különválasztjuk a pici és a nagy a_i-knek megfelelő részt:

$$\begin{aligned} |h(\varrho)| &= \Big|\sum_{i=1}^{P} \varrho^{a_i} + \sum_{i=P+1}^{k} \varrho^{a_i}\Big| \ge \Big|\sum_{i=1}^{P} \varrho^{a_i}\Big| - \Big|\sum_{i=P+1}^{k} \varrho^{a_i}\Big| \ge \\ &\ge \Big|\sum_{i=1}^{P} \varrho^{a_i}\Big| - \sum_{i=P+1}^{k} |\varrho^{a_i}| = \Big|\sum_{i=1}^{P} \varrho^{a_i}\Big| - N. \end{aligned} \tag{15}$$

Így elég a

$$T(\varrho) = \Big|\sum_{i=1}^{P} \varrho^{a_i}\Big| \tag{16}$$

kifejezésre jó alsó becslést találnunk.

Legyen $\omega = \cos(2\pi/n) + i\sin(2\pi/n)$ és $z_j = \omega^{a_j}$, $j = 1, \dots, P$. Mivel $0 \le a_j \le (n-1)/2$, ezért valamennyi z_j komplex szám képzetes része nemnegatív, azaz a felső félsíkba esnek.

Legyen α egy később alkalmasan megválasztandó hegyesszög, és legyen F azoknak a z_j-knek a száma, amelyek β_j szögére $\alpha \le \beta_j \le \pi - \alpha$, nevezzük ezeket „felső" z_j-knek. (A többi $P - F$ darab „alsó" z_j esetén tehát $0 \le \beta_j < \alpha$ vagy $\pi - \alpha < \beta_j < \pi$.)

A felső z_j-k képzetes része $\operatorname{Im}(z_j) \ge \sin\alpha$, az alsóké $\operatorname{Im}(z_j) \ge 0$, ezért

$$\Big|\sum_{j=1}^{P} z_j\Big| \ge \operatorname{Im}\Big(\sum_{j=1}^{P} z_j\Big) \ge F \cdot \sin\alpha. \tag{17}$$

Ha most ϱ-t éppen ω-nak választjuk, akkor $\varrho^{a_j} = z_j$, és így (16) és (17) alapján

$$T(\omega) \ge F \cdot \sin\alpha. \tag{18}$$

Legyen most $\varrho = \omega^2$, ekkor $\varrho^{a_j} = z_j^2$. Az alsó z_j-kre z^2 szöge -2α és 2α közé esik, tehát a valós részük $\operatorname{Re}(z_j^2) > \cos(2\alpha)$, a felsők esetén pedig

$\mathrm{Re}(z_j^2) \geq -1$ triviálisan. Ennek alapján

$$T(\omega^2) = \Big|\sum_{j=1}^{P} z_j^2\Big| \geq \mathrm{Re}\Big(\sum_{j=1}^{P} z_j^2\Big) \geq (P-F)\cos(2\alpha) - F. \tag{19}$$

Az $\alpha = \pi/6$ választással (18)-ból, illetve (19)-ből

$$T(\omega) \geq F/2 \qquad \text{és} \qquad T(\omega^2) \geq (P-3F)/2. \tag{20}$$

Legyen

$$M = \max\big(T(\omega), T(\omega^2)\big),$$

ekkor (20) alapján

$$M \geq \frac{3T(\omega) + T(\omega^2)}{4} \geq \frac{P}{8},$$

és így azt kaptuk, hogy alkalmas ϱ-val ($\varrho = \omega$ vagy $\varrho = \omega^2$) a (16)-beli $T(\varrho)$-ra $T(\varrho) \geq P/8$ teljesül. Ezt (15)-be beírva

$$|h(\varrho| \geq \frac{P}{8} - N = \frac{1-9\tau}{8}k \tag{21}$$

adódik. Így (12), (13) és (21) alapján

$$S \geq \frac{(1-9\tau)^2}{128}k^2 - \frac{k}{2}. \tag{22}$$

Figyelembe véve (11)-et is kapjuk, hogy

$$S \geq \max\Big(\frac{\tau^2}{2}k^2, \frac{(1-9\tau)^2}{128}k^2 - \frac{k}{2}\Big). \tag{23}$$

A „legrosszabb” eset, ha a két értékben a k^2 együtthatója megegyezik, azaz $\tau = 1/17$, és ekkor

$$S \geq \frac{k^2}{578} - \frac{k}{2}, \tag{24}$$

azaz (10) (a $k/2$ hibatagtól eltekintve) a $\nu = 1/578$ konstanssal teljesül.

(24)-et (9)-be behelyettesítve kapjuk, hogy

$$\frac{k^2+k}{2} \geq n + \frac{k^2}{578} - \frac{k}{2},$$

ahonnan

$$\frac{144}{289}k^2 + k \geq n, \quad \text{és így} \quad (k+2)^2 > \frac{289}{144}n,$$

ami éppen a tételben állított alsó becslést jelenti. ■

Feladatok

12.3.1 Igazoljuk a valós számok részhalmazaira vonatkozó alábbi állításokat.

a) Ha $|A| = k$, akkor $|A+A| \geq 2k-1$, és egyenlőség akkor és csak akkor teljesül, ha A elemei számtani sorozatot alkotnak.

b) Ha $|A| = k$, $|B| = r$, akkor $|A+B| \geq k+r-1$, és egyenlőség akkor és csak akkor teljesül, ha $k = 1$ vagy $r = 1$, vagy pedig A és B elemei azonos differenciájú számtani sorozatot alkotnak.

c) Ha $|A_i| = k_i$, $i = 1, 2, \ldots, t$, akkor $|A_1 + \ldots + A_t| \geq k_1 + \ldots + k_t + 1 - t$, és ha $k_i > 1$, $i = 1, 2, \ldots, t$, akkor egyenlőség pontosan abban az esetben teljesül, ha minden A_i-ben az elemek azonos differenciájú számtani sorozatot alkotnak.

12.3.2 Igazoljuk a 12.3.1 Tétel tetszőleges m modulusra vonatkozó alábbi általánosítását: Legyen $A, B \subseteq \mathbf{Z}_m$, $0 \in B$. Ekkor $|A+B| \geq$ $\geq \min(m, |A|+s)$, ahol s a B elemei között az m-hez relatív prímek száma. Mutassunk példát olyan összetett m-re és $s < |B| - 1$-re, amikor egyenlőség teljesül.

12.3.3 Bizonyítsuk be az alábbi állításokat.

a) Legyen $A, B \subseteq \mathbf{Z}_m$, $0 \in A \cap B$, és tegyük fel, hogy $a \in A$, $b \in B$ mellett $a + b = 0$ csak $a = b = 0$ esetén teljesül. Ekkor $|A+B| \geq$ $\geq |A|+|B|-1$. (A feltételből most következik, hogy $|A|+|B|-1 \leq m$, ezért az állításban az egyenlőtlenségnél nincs szükség a 12.3.1 Tételhez hasonló minimumos megfogalmazásra.)

b) Az (a)-beli egyenlőtlenség éles.

c) Az (a)-beli állítás $\mathbf{Z}_m$ helyett tetszőleges Abel-csoport (véges) részhalmazaira is teljesül.

*12.3.4 Legyen p prím, $A \subseteq \mathbf{Z}_p$, $|A| = k$ és $A \hat{+} A = \{a+a' \mid a, a' \in A, a \neq a'\}$, azaz most csak a *különböző* elemekből képezett kéttagú összegek halmazát vizsgáljuk. Igazoljuk, hogy $|A \hat{+} A| \geq \min(p, 2k-3)$.

Megjegyzések: 1. Erdősnek és Heilbronn-nak ezt a sokáig megoldatlan sejtését Hamidoune és Da Silva igazolta először, majd Alon, Ruzsa és Nathanson adott rá egyszerűbb bizonyítást.

2. Az $A = \{0, 1, \ldots, k-1\}$ példa mutatja, hogy ez a becslés nem javítható.

12.3.5

a) Legyen T tetszőleges kommutatív test, $A, B \subseteq T$, $|A| = k$, $|B| = r$, továbbá $F(x, y)$ olyan T feletti kétváltozós polinom, amelynek a foka $k + r - 2$, és amelyben az $x^{k-1}y^{r-1}$ tag együtthatója nem nulla. Lássuk be, hogy van olyan $a \in A$, $b \in B$, amelyre $F(a, b) \neq 0$.

b) Általánosítsuk az (a) részt 2 helyett n részhalmazra és n-változós F polinomra.

M*12.3.6 Legyen $p > 2$ prím, és C, ill. D a $\mathbf{Z}_p$-nek két tetszőleges, azonos elemszámú részhalmaza. Mutassuk meg, hogy C és D elemei párba állíthatók úgy, hogy az egyes párok elemeiből képezett kéttagú összegek mind különbözők legyenek.

12.3.7 Fogalmazzuk meg és bizonyítsuk be a 12.3.1 Tétel megfelelőjét kettőnél több halmaz esetére.

12.3.8 A 3.6.6 feladatot és annak síkbeli, valamint magasabb dimenziós általánosításait vizsgáljuk.

*a) Adjunk új bizonyítást a 3.6.6 feladatra a 12.3.7 feladat felhasználásával.

b) Igazoljuk, hogy a szokásos síkbeli négyzetrácson 5 tetszőleges rácspont között biztosan van két olyan, amelyeknek a szakaszfelező pontja is rácspont.

c) Legyen $f(n)$ a legkisebb olyan szám, hogy $f(n)$ darab tetszőleges síkbeli rácspont közül mindig kiválasztható n darab olyan, amelyek súlypontja is rácspont. Mutassuk meg, hogy $f(n) \geq 4n - 3$.
Megjegyzés: 2004-ben igazolták azt a régi sejtést, hogy $f(n) = 4n-3$.

d) Legyen $f(n, d)$ a legkisebb olyan szám, hogy a d-dimenziós szokásos rácson $f(n, d)$ darab rácspont közül mindig kiválasztható n darab olyan, amelyeknek a súlypontja is rácspont. Bizonyítsuk be, hogy

(i) $2^d(n - 1) + 1 \leq f(n, d)) \leq n^d(n - 1) + 1$;

(ii) $f(nm, d) \leq f(n, d) + n(f(m, d) - 1)$.

Megjegyzés: (i)-ben a felső becslés nagymértékben, $c_d n$-re javítható, ahol c_d csak a d-től függő konstans. Az alsó becslés $d = 1$ és 2 esetén pontos (lásd az (a) részt, illetve a (c) rész utáni megjegyzést). Kiderült azonban, hogy minden $d > 2$-re és *páratlan* $n \geq 3$-ra az alsó becslés javítható ($n = 2^k$ esetén az alsó becslés adja a helyes értéket minden d-re, lásd alább). Az $f(n, d)$ pontos értéke $n > 2$ és $d > 2$ mellett csak az alábbi néhány esetben ismert:

$$f(3, 3) = 19,\ f(3, 4) = 41,\ f(3, 5) = 91 \ \text{ és } \ f(2^k, d) = (2^k - 1)2^d + 1.$$

12.3.9 Legyen p prím, $A \subseteq \mathbf{Z}_p$, és tegyük fel, hogy két különböző A-beli elem különbsége sohasem négyzetelem $\mathbf{Z}_p$-ben (azaz $a_i - a_j$ semmilyen $i \neq j$-re sem kvadratikus maradék mod p). Lássuk be, hogy $|A| < \sqrt{p}$.

12.3.10 A $[0, n-1]$ intervallum egy h-adrendű bázisán nemnegatív egészek olyan A halmazát értjük, hogy minden $0 \leq r \leq n-1$ egész felírható h darab A-beli elem összegeként. Jelölje $g(h,n)$ az ilyen bázisok elemszámának minimumát. Bizonyítsuk be, hogy

$$\sqrt[h]{h!n} - h + 1 < g(h,n) < \sqrt[h]{h^h n} + h.$$

12.4. Schur tétele

A kombinatorikus számelméletnek ez a klasszikus eredménye érdekes módon az ettől igen távolinak tűnő Fermat-sejtéssel kapcsolatban született, a bizonyításhoz pedig gráfelméleti módszerekre van szükség. A ma is intenzíven vizsgált témakör számos megoldatlan problémával is „büszkélkedhet".

Először a gráfelméleti háttérrel foglalkozunk. Kiindulásul tekintsük az alábbi közismert feladványt: 6 ember között biztosan van vagy 3 olyan, akik közül bármelyik kettő ismeri egymást, vagy 3 olyan, akik közül semelyik kettő sem ismeri egymást (az ismeretséget kölcsönösnek tételezzük fel).

Fogalmazzuk ezt át a gráfelmélet nyelvezetére. Tekintsük azt a 6 szögpontú teljes gráfot, amelynek a csúcsai az embereink, és két csúcsot összekötő él legyen piros, ha a két ember ismeri egymást, és kék, ha nem ismerik egymást. Az állítás ekkor úgy szól, hogy akárhogyan is színezzük ki egy 6 szögpontú teljes gráf éleit pirossal és kékkel, biztosan keletkezik egyszínű háromszög.

Ennek igazolásához vegyük a gráf egy tetszőleges A csúcsát. Az ebből kiinduló 5 él között van (legalább) 3 azonos színű, mondjuk piros. Ha ezen 3 él másik végpontja, B, C és D között vezet piros él, pl. a BC él piros, akkor ABC piros háromszög, ellenkező esetben pedig BCD kék háromszög.

A feladványt a következőképpen általánosíthatjuk: az n szögpontú teljes gráf éleit t színnel színezzük, és egyszínű háromszög helyett olyan k szögpontú teljes részgráfot akarunk találni, amelynek minden éle azonos színű (az eredeti probléma a $t = 2$, $k = 3$ speciális esetet jelenti). Ramsey alapvető tétele azt mondja ki, hogy (k-tól és t-től függően) elég nagy n esetén mindig van ilyen részgráf:

12.4.1 Tétel (Ramsey tétele) **T 12.4.1**

Bármely t és k esetén létezik olyan $n = R(k,t)$, hogy ha egy n szögpontú teljes gráf éleit akárhogyan színezzük ki t színnel, lesz olyan k szögpontú teljes részgráf, amelynek minden éle azonos színű. ♣

A továbbiakban $R(k,t)$-vel a legkisebb ilyen tulajdonságú n-et fogjuk jelölni.

Az előzőkben beláttuk, hogy $R(3,2) \leq 6$, és könnyen adódik, hogy itt valójában egyenlőség áll (lásd a 12.4.1 feladatot). A tétel bizonyításából leolvasható, hogy $R(3,t) \leq 3t!$, sőt az is kihozható, hogy $R(3,t) \leq \lceil et! \rceil$, ahol $e = 2{,}71\ldots$ a természetes logaritmus alapszáma (lásd a 12.4.2 feladatot). Finomabb módszerekkel a konstans szorzó $e - 1/24$-re javítható, ennél jobb felső becslés nem ismeretes, bár ez minden bizonnyal igen messze van a tényleges $R(3,t)$ értéktől. Az $R(k,t)$ Ramsey-számok pontos értéke csak nagyon kevés esetben ismert, pl. $R(3,3) = 17$, és az alsó és felső becslések is igen messze esnek egymástól.

Bizonyítás: A jobb áttekinthetőség kedvéért először a $k = 3$ esetet igazoljuk t szerinti teljes indukcióval, és utána térünk át általános k-ra. (Megjegyezzük, hogy a Schur-tétel bizonyításánál majd csak a $k = 3$ esetre lesz szükség.)

I. Az indukció kezdő esete lehet akár $t = 1$ (nyilván $R(3,1) = 3$), akár $t = 2$, a már igazolt $R(3,2) \leq 6$ összefüggés alapján. Az utóbbi bizonyításához használt gondolatmenetből leolvashatjuk az általános indukciós lépést is.

Tegyük fel, hogy $n = R(3,t-1)$ létezik, és színezzük ki egy N szögpontú teljes gráf éleit most t színnel. Ha $N \geq 1+t(n-1)+1$, akkor egy tetszőleges A csúcsból induló éleket nézve, ezen $t(n-1)+1$ él között a skatulyaelv alapján lesz (legalább) n egyszínű, pl. piros. Ha ezen élek másik végpontjai, pl. B és C között vezet piros él, akkor ABC piros háromszög. Ellenkező esetben pedig ezek a végpontok egy olyan n szögpontú teljes gráf csúcsai, amelynek élei csak $t-1$ színnel vannak színezve, és így az indukciós feltétel szerint van benne egyszínű háromszög.

II. Az általános eset bizonyításához az alábbi módon érdemes finomítani a feladatot. Az egyszerűbb megfogalmazás kedvéért a gráf mérete jelentse a csúcsok számát, a színek legyenek az $1,2,\ldots,t$ számok, és j színű gráfon értsünk olyan (teljes) gráfot, amelyben minden él színe j. Ekkor a módosított állítás a következő.

Bármely t és $k_1,\ldots,k_t$ esetén létezik olyan $n = R^*(k_1,k_2,\ldots,k_t)$, hogy ha egy n szögpontú teljes gráf éleit akárhogyan színezzük ki az $1,2,\ldots,t$ színekkel, lesz olyan j, hogy a gráf tartalmaz egy k_j méretű j színű teljes részgráfot.

($R^*(k_1, k_2, \ldots, k_t)$ most is jelentse a legkisebb ilyen tulajdonságú n-et.)

A két probléma könnyen átjátszható egymásra: egyrészt nyilván $R(k,t) = R^*(k,\ldots,k)$, másrészt $R^*(k_1,\ldots,k_t) \le R(k,t)$, ahol $k = \max(k_1,\ldots,k_t)$.

A módosított állításnál a minden $k_i = 1$ vagy 2 kiindulási eset triviális, az indukció pedig az alábbi formában működik:

$$R^*(k_1,\ldots,k_t) \le 1 + \sum_{j=1}^{t} [R^*(k_1,\ldots,k_j-1,\ldots,k_t) - 1] + 1. \qquad (1)$$

Valóban, színezzük ki egy N szögpontú teljes gráf éleit t színnel, ahol N az (1) jobb oldalán álló érték. Ekkor egy tetszőleges A csúcsot véve, az innen induló élek között a skatulyaelv miatt valamelyik j-re lesz (legalább) $R^*(k_1,\ldots,k_j-1,\ldots,k_t)$ darab j színű. Az ezen élek másik végpontjai alkotta teljes gráfban van egy, az indukciós feltétel által biztosított méretű egyszínű részgráf. Ha ennek színe $i \ne j$, akkor egy k_i méretű i színű részgráfot kaptunk, tehát készen vagyunk. A j szín esetén pedig $k_j - 1$ csúcsú részgráf adódott, ami az A csúccsal együtt már egy k_j méretű j színű részgráfot jelent. ■

Schur tétele számok színezésére vonatkozik:

12.4.2 Tétel (Schur tétele) **T 12.4.2**

Bármely t esetén létezik olyan $n = S(t)$, hogy ha az $1, 2, \ldots, n+1$ számokat akárhogyan színezzük ki t színnel, lesz olyan azonos színű a és b, amelyek $a+b$ összege is ugyanilyen színű ($a = b$ is megengedett). ♣

A továbbiakban $S(t)$-vel a legkisebb ilyen tulajdonságú n-et fogjuk jelölni, vagyis $S(t)$ a legnagyobb „rossz” szám: $1, 2, \ldots, S(t)$ még kiszínezhető t színnel úgy, hogy az $x+y=z$ egyenletnek ne legyen egyszínű megoldása. (A Ramsey-tételnél $R(k,t)$ a legkisebb „jó” számot jelentette; a két kissé eltérő szellemű jelölés hagyományosan így alakult ki, ezért mi is ezekhez tartjuk magunkat.)

Nyilván $S(1) = 1$ és könnyen adódik, hogy $S(2) = 4$. Ezeken kívül pontos értékként csak $S(3) = 13$ és $S(4) = 44$ ismert. Az $S(t)$ Schur-számok alsó és felső becsléseire vonatkozóan lásd a 12.4.3 feladatot.

Bizonyítás: Megmutatjuk, hogy $S(t) < R(3,t)$, azaz az $1, 2, \ldots, R(3,t)$ számokat akárhogyan színezzük ki t színnel, teljesül az előírt tulajdonság. Tekintsük azt a teljes gráfot, amelynek csúcsai a fenti számok, és az (i,j) él (gráf)színe legyen az $|i-j|$ (szám)színe. Ekkor a Ramsey-tétel alapján keletkezik a gráfban egyszínű háromszög, azaz van olyan $i < j < m$, amelyre az (i,j), (j,m) és

(i, m) gráfélek azonos színűek, vagyis $a = j - i$, $b = m - j$ és $a + b = m - i$ (szám)színe azonos. ■

Most rátérünk a Schur-tételnek a Fermat-sejtéssel való kapcsolatára.

Tekintsük az $x^t + y^t \equiv z^t \pmod{p}$ kongruenciát. Ha végtelen sok p prímre csak triviális, azaz $xyz \equiv 0 \pmod{p}$ megoldás létezik, akkor abból következik a Fermat-sejtés a t kitevőre: ha ugyanis indirekt az a, b, c nemnulla számokra $a^t + b^t = c^t$, akkor ezek a kongruenciának is nemtriviális megoldását adják minden $p > \max(|a|, |b|, |c|)$ prímre, és ez ellentmond annak, hogy végtelen sok prímre csak triviális megoldás létezik. Megmutatjuk azonban, hogy ez az ötlet sajnos nem vezethet el a Fermat-sejtés bizonyításához:

12.4.3 Tétel **T 12.4.3**

Az $x^t + y^t \equiv z^t \pmod{p}$ kongruenciának minden (t-től függően) elég nagy p prímre van nemtriviális, azaz $xyz \not\equiv 0 \pmod{p}$ megoldása. ♣

Bizonyítás: Legyen $p - 1 > S(t)$, g primitív gyök mod p, és színezzük ki az $1, 2, \ldots, p-1$ számokat a $0, 1, \ldots, t-1$ színekkel a következőképpen: r színűek legyenek azok a számok, amelyek g^r, g^{r+t}, g^{r+2t}, ... -vel kongruensek mod p.

Ekkor a Schur-tétel szerint keletkezik azonos színű $a, b, a + b$, azaz valamilyen r-rel

$$a \equiv g^{st+r}, \quad b \equiv g^{ut+r}, \quad a + b \equiv g^{vt+r} \pmod{p},$$

és így

$$g^{st+r} + g^{ut+r} \equiv g^{vt+r} \pmod{p}.$$

Ezt a p-hez relatív prím g^r-rel egyszerűsítve

$$(g^s)^t + (g^u)^t \equiv (g^v)^t \pmod{p}$$

adódik, vagyis $x = g^s, y = g^u, z = g^v$ egy nemtriviális megoldását adja a kongruenciának. ■

A természetes számok színezésével kapcsolatban Schur egy másik problémát is felvetett, amelyet először Van der Waerden oldott meg, ezt bizonyítás nélkül közöljük:

12.4.4 Tétel (Van der Waerden tétele) **T 12.4.4**

A természetes számokat tetszőlegesen színezve két színnel, biztosan keletkezik akármilyen hosszú (véges) egyszínű számtani sorozat. ♣

Van der Waerden valójában a tételnek az alábbi végesített és több színt szerepeltető változatát igazolta egy ravasz teljes indukcióval:

12.4.4A Tétel (Van der Waerden tétele) **T 12.4.4A**

Bármely t és k esetén létezik olyan $n = w(k,t)$, hogy az $1, 2, \dots, n$ számokat t színnel tetszőlegesen kiszínezve biztosan keletkezik k-tagú egyszínű számtani sorozat. ♣

Az $R(k,t)$ Ramsey- és $S(t)$ Schur-számokhoz hasonlóan a (minimális) $w(k,t)$ Van der Waerden-számok alsó és felső becslései is nagyon messze esnek egymástól, és csak nagyon kevés pontos érték ismert:

$$w(3,2) = 9, \quad w(4,2) = 35, \quad w(5,2) = 178, \quad w(6,2) = 1132,$$
$$w(3,3) = 27, \quad w(4,3) = 293, \quad w(3,4) = 76,$$

valamint triviálisan $w(k,1) = k$ és $w(2,t) = t+1$. A két szín esetére a $w(k) = w(k,2)$-re vonatkozó alsó becslésekről lásd a 12.4.11 feladatot.

Könnyen adódik, hogy a természetes számokat két színnel színezve nem feltétlenül kapunk végtelen hosszú egyszínű számtani sorozatot, sőt még az is elérhető, hogy pirosból végtelen hosszú, kékből pedig még háromtagú számtani sorozat se keletkezzék (lásd a 12.4.7 feladatot).

Befejezésül a Van der Waerden-tétel egy nagyfokú általánosítását említjük meg. Erdősnek és Turánnak ezt a nevezetes, sok évtizeden át megoldatlan sejtését végül Szemerédi Endre igazolta, és ezzel elnyerte a legnagyobb díjat (1000 dollárt), amelyet Erdős matematikai problémák megoldásáért kitűzött, és amelyet tényleg ki is kellett fizetnie, mert a problémát valóban megoldották. (Jóval Erdős halála után, 2014-ben egy 10000 dolláros problémáját is megoldották. Ez a prímszámok közötti hézagra vonatkozó 5.5.4 Tétel (B) része, ami Erdős és Rankin 78(!) évvel korábbi eredményének minimális(!) javítása: az Erdős–Rankin becslésben a nevező négyzete szerepelt.) Szemerédi 2012-ben az egyik legrangosabb matematikai kitüntetésben, Abel-díjban részesült a számelméletben, kombinatorikában és számítógéptudományban elért alapvető eredményeiért.

Nézzük tehát Erdős és Turán kérdését. Van der Waerden tétele „csak” azt állítja, hogy a természetes számsort, illetve annak elég nagy kezdőszeletét kiszínezve biztosan keletkezik előírt hosszúságú egyszínű számtani sorozat, de nem mondja meg, melyik színből. Természetesen azt érezzük, hogy bizonyára a leggyakrabban előfordulóból. Ennek kapcsán vetette fel Erdős és Turán, hogy ha a természetes számoknak egy tetszőleges, elég sűrű részsorozatát vesszük, akkor ennek is kell tartalmaznia előírt hosszúságú számtani sorozatot. Sejtésük pontos megfogalmazása a következő.

12.4.5 Tétel (Szemerédi tétele) **T 12.4.5**

Tekintsük az $\{1, 2, \ldots, n\}$ legnagyobb elemszámú olyan részhalmazát, amely még *nem* tartalmaz k hosszúságú számtani sorozatot, ennek elemszámát jelölje $r_k(n)$. Ekkor bármely rögzített k-ra $\lim_{n\to\infty} r_k(n)/n = 0$. ♣

Ebből van der Waerden tétele valóban következik, ugyanis ha az $1, 2, \ldots, n$ számokat t színnel színezzük, akkor van olyan szín, ami legalább n/t-szer fordul elő, és elég nagy n-re $n/t > r_k(n)$ (hiszen $1/t$ nagyobb lesz, mint a 0-hoz tartó $r_k(n)/n$), vagyis ebből a színből biztosan kapunk k hosszúságú számtani sorozatot.

A Szemerédi-tétel más megfogalmazásban azt mondja ki, hogy a természetes számoknak bármely pozitív felső sűrűségű részsorozata tartalmaz akármilyen hosszú (véges) számtani sorozatot. Erdős ezután azt sejtette, hogy ez a tulajdonság ennél ritkább sorozatokra is igaz: elég az, hogy az elemek reciprokösszege divergens legyen. Nagy meglepetést keltett, amikor ezt a sejtést a prímszámok sorozatára 2004-ben igazolták (vagyis a prímszámok között előfordul tetszőlegesen hosszú számtani sorozat, lásd az 5.1. pontot is), az általános sejtés azonban továbbra is megoldatlan.

Feladatok

12.4.1 Lássuk be, hogy $R(3, 2) = 6$, $R(k, 1) = k$, $R(1, t) = 1$ és $R(2, t) = 2$.

12.4.2 Mutassuk meg, hogy (a) $R(3, t) \le 3t!$; (b) $R(3, t) \le \lceil et! \rceil$.

12.4.3 Igazoljuk a Schur-számokra vonatkozó alábbi egyenlőtlenségeket:

(a) $S(t) < et!$; (b) $S(t + 1) \ge 3S(t) + 1$;

(c) $S(t) \ge (3^t - 1)/2$; *(d) $S(t + v) \ge 2S(t)S(v) + S(t) + S(v)$.

Megjegyzések: A (b) rész a (d)-nek $v = 1$ speciális esete. A (d) rész és $S(5) \ge 160$ felhasználásával a (c)-beli alsó becslés kicsit javítható.

12.4.4 Adott n-hez adjuk meg azt a legnagyobb $r = f(n)$-et, amelyre az $n, n+1, \ldots, r$ számok kiszínezhetők két színnel úgy, hogy az $x+y = z$ egyenletnek ne legyen egyszínű megoldása.

12.4.5 Bizonyítsuk be, hogy bármely t esetén létezik olyan n, hogy ha az $1, 2, \ldots, n+1$ számokat akárhogyan színezzük ki t színnel, lesz 3 olyan azonos színű, de nem feltétlenül különböző szám, amelyek összege is ugyanilyen színű.

12.4.6 Legyen t rögzített. Mutassuk meg, hogy minden elég nagy p prímre létezik két szomszédos t-edik hatványmaradék mod p, azaz olyan

$a \not\equiv 0, 1 \pmod{p}$, hogy az $x^t \equiv a - 1$ és a $z^t \equiv a \pmod{p}$ kongruencia is megoldható.

12.4.7 Bizonyítsuk be, hogy a természetes számokat ki lehet úgy színezni pirossal és kékkel, hogy ne jöjjön létre

a) végtelen hosszú egyszínű számtani sorozat;

*b) se végtelen hosszú piros, se pedig 3-tagú kék számtani sorozat.

12.4.8 Lássuk be, hogy a természetes számokat akárhogyan színezzük ki véges sok színnel, bármely k-ra *végtelen sok* olyan k-tagú számtani sorozat keletkezik, amelyek mind azonos színűek.

12.4.9 Igazoljuk, hogy a természetes számokat tetszőlegesen kiszínezve véges sok színnel, biztosan keletkezik akármilyen hosszú (véges) egyszínű *mértani* sorozat.

12.4.10 Lássuk be, hogy $w(3, 2) = 9$.

**12.4.11 Igazoljuk a $w(k) = w(k, 2)$-re vonatkozó alábbi alsó becsléseket:

(a) $w(k) \geq 2^{k/2}\sqrt{k-1}$; **M**(b) $w(p+1) > p(2^p - 1)$, ha p prím.

M**12.4.12 Lássuk be az $r_3(n)$-re vonatkozó alábbi alsó becslést: minden elég nagy n-re megadható 1 és n között $n/e^{c\sqrt{\log n}}$ olyan egész szám (ahol $c > 0$ alkalmas konstans), amelyek között nem fordul elő háromtagú számtani sorozat.

12.5. Fedőrendszerek

Ismét Erdős egyik „kedvenc” problémája következik: a nemnegatív egész számokat véges sok, különböző differenciájú számtani sorozat egyesítéseként állítjuk elő:

$$\{0, 1, \ldots, n, \ldots\} = \\ = \{a_1, a_1 + m_1, a_1 + 2m_1, \ldots\} \cup \ldots \cup \{a_k, a_k + m_k, a_k + 2m_k, \ldots\}, \\ \text{ahol } 1 < m_1 < \ldots < m_k. \tag{1}$$

Ennek (ekvivalens) átfogalmazása, hogy az egész számokat különböző modulusok szerinti maradékosztályokkal fedjük le: minden t egész szám eleme az

$$a_1 \pmod{m_1}, \ldots, a_k \pmod{m_k}, \quad 1 < m_1 < \ldots < m_k \tag{2}$$

maradékosztályok közül legalább az egyiknek, azaz van olyan i, amelyre $t \equiv a_i \pmod{m_i}$.

A számtani sorozatok, illetve maradékosztályok ilyen rendszerét (kongruencia) *fedőrendszernek* nevezzük.

Példa fedőrendszerre:

$$0 \pmod 2, \quad 0 \pmod 3, \quad 1 \pmod 4, \quad 1 \pmod 6, \quad 11 \pmod{12}. \tag{3}$$

Ennél kevesebb modulusú fedőrendszer nem létezik, és 5 kongruencia esetén is csak ez az 5 modulus lehet (lásd a 12.5.4 feladatot).

Erdős a fedőrendszereket egy látszólag távoli probléma megoldásához találta ki, lásd a 12.5.2 Tételt. Számos nyitott kérdés kapcsolódik a fedőrendszerekhez, ezek közül a két legrégibb és egyben legérdekesebb a következő:

- Van-e fedőrendszer csupa páratlan modulusból? Ez továbbra is megoldatlan.
- Van-e minden L-hez olyan fedőrendszer, amelynek minden modulusa nagyobb L-nél?

Itt L értékét sikerült fokozatosan növelni egészen $L = 40$-ig. Nielsennek ebben a 2008-as rendkívül terjedelmes és ravasz konstrukciójában csak a megfelelő jelölésrendszer elmagyarázása több oldalon át zajlik.

Ezek után nagy meglepetést okozott, hogy erre a kérdésre a válasz negatív, azaz létezik egy felső korlát a fedőrendszerek legkisebb modulusára. Hough ezt az eredményt éppen az Erdős születésének 100-adik évfordulójára rendezett konferencián jelentette be 2013-ban.

Természetesen merül fel az *egzakt* vagy *diszjunkt* fedés, vagyis amikor az (1)-beli számtani sorozatok, illetve a (2)-beli maradékosztályok diszjunktak, azaz minden egész szám *pontosan* egy (2)-beli kongruenciát elégít ki.

Az alábbi tétel mutatja, hogy ez nem lehetséges:

12.5.1 Tétel **T 12.5.1**

A nemnegatív egészek nem állíthatók elő véges sok, különböző differenciájú számtani sorozat diszjunkt egyesítéseként. ♣

A tételre két bizonyítást adunk, az első a komplex számokra vonatkozó elemi analízisre támaszkodik, a második az állítást egy önmagában is érdekes geometriai problémára átfogalmazva igazolja.

Első bizonyítás: Generátorfüggvényt használunk, z komplex számot jelöl, ahol $|z| < 1$.

Tegyük fel indirekt, hogy (1)-ben diszjunkt egyesítés szerepel. Ekkor minden $n \geq 0$ egyértelműen áll elő $n = a_i + rm_i$ alakban, ahol $1 \leq i \leq k$ és $r \geq 0$. Ezért a $|z| < 1$-re érvényes abszolút konvergencia és az ebből adódó átrendezhetőség miatt

$$(z^{a_1} + z^{a_1+m_1} + z^{a_1+2m_1} + \ldots) + \ldots + (z^{a_k} + z^{a_k+m_k} + z^{a_k+2m_k} + \ldots) = \\ = 1 + z + z^2 + \ldots + z^n + \ldots .$$

A mértani sorokat összegezve kapjuk, hogy

$$\sum_{i=1}^{k} z^{a_i} \frac{1}{1 - z^{m_i}} = \frac{1}{1 - z} . \tag{4}$$

Ha a z komplex változó (egy $|z| < 1$ tartománybeli úton) tart egy m_i-edik egységgyökhöz, akkor (4) bal oldalán az ennek megfelelő $z^{a_i}/(1 - z^{m_i})$ tag nem lesz korlátos. Ha tehát $z \to w = \cos(2\pi/m_k) + i \sin(2\pi/m_k)$, akkor a bal oldal utolsó tagja nem korlátos, a többi tag és a jobb oldal viszont igen, hiszen m_k maximalitása miatt w nem lesz m_i-edik egységgyök $i < k$-ra. Így ellentmondásra jutottunk. ■

Második bizonyítás: Tegyük fel most is indirekt, hogy (1)-ben diszjunkt egyesítés szerepel. Mivel a számtani sorozatok periodikusak a differenciák legkisebb közös többszöröse $M = [m_1, \ldots, m_k]$ szerint, ezért az indirekt feltevés ekvivalens azzal, hogy az $1, 2, \ldots, M$ számok mindegyike pontosan egy lefedő számtani sorozatnak eleme.

Rajzoljunk egy szabályos M-szöget, a csúcsait számozzuk meg sorban $1, 2, \ldots, M$-mel. Minden lefedő számtani sorozathoz válasszunk egy-egy (különböző) színt, és az adott számtani sorozat által lefedett csúcsokat fessük az ehhez tartozó színűre. Pl. ha $M = 12$, és az 1 (mod 4) számtani sorozathoz a piros tartozik, akkor az 1, 5 és 9 csúcsok lesznek piros színűek.

Nyilván az $a_i \pmod{m_i}$ számtani sorozat által lefedett csúcsok egy $n_i = M/m_i$ oldalú szabályos sokszöget alkotnak (megengedve a szakasszá, illetve ponttá elfajuló $n_i = 2$, illetve 1 eseteket is), és így $n_1 > n_2 > \ldots > n_k$.

Az indirekt feltevés ebben a geometriai átfogalmazásban azt jelenti, hogy van olyan szabályos M-szög, amelynek a csúcsai kiszínezhetők néhány ($k > 1$) színnel úgy, hogy az egyszínű csúcsok különböző oldalszámú (esetleg elfajuló) szabályos sokszögeket alkossanak.

Azt az egyszerű geometriai tényt fogjuk felhasználni, hogy egy szabályos n-szög középpontjából a csúcsokba mutató vektorok összege nulla, ha $n > 1$ (beleértve az $n = 2$ elfajuló esetet is). Ez azért igaz, mert az összegvektor

a középpont körüli $2\pi/n$ szögű elforgatáskor egyrészt nem változik, hiszen a sokszög önmagába megy át, másrészt viszont maga is elfordul az adott szöggel, és így csak a nullvektor lehet.

A gondolatmenet jobb megvilágítása céljából tegyük fel először, hogy $n_k = 1$. Legyen $\mathbf{s}$, illetve $\mathbf{s}_i$, $i = 1, \ldots, k$, a szabályos M-szög középpontjából az M-szög, illetve az i-edik színű csúcsok alkotta n_i-szögbe mutató vektorok összege. Ekkor nyilván $\mathbf{s} = \sum_{i=1}^{k} \mathbf{s}_i$, másrészt az előbbi megjegyzés alapján $\mathbf{s} = \mathbf{s_1} = \ldots = \mathbf{s}_{k-1} = \mathbf{0}$, de $\mathbf{s}_k \neq \mathbf{0}$, ami ellentmondás.

Az általános esetet erre a következőképpen tudjuk visszavezetni. Legyen t rögzített, és tekintsük a szabályos M-szög csúcsainak azt a transzformációját, amely a j csúcsot a $tj \pmod M$ csúcsba viszi át ($j = 1, \ldots, M$). Megmutatjuk, hogy ekkor az eredetileg egyszínű csúcsok képei továbbra is egy szabályos sokszög csúcsait fedik le azonos multiplicitással. Például, ha $M = 12$, $t = 2$, akkor az $1 \pmod 4$ számtani sorozatnak megfelelő 1, 5, 9 csúcsok képe rendre 2, 10, 6, vagyis a 2, 6, 10 szabályos háromszöget kapjuk; a $2 \pmod 3$ kongruencia esetén a 2, 5, 8, 11 csúcsok képe rendre 4, 10, 4, 10, tehát a 4, 10 szabályos kétszög csúcsait nyerjük, mindegyiket kétszer; és végül a $4 \pmod 6$-ból adódó 4, 10 csúcsok képe 8, 8, tehát ez az „egyszög” jött létre kétszeres multiplicitással.

Általában is, az $a_i \pmod{m_i}$-nek megfelelő $a_i + jm_i$, $j = 0, 1, \ldots, n_i - 1$ csúcsok képe $ta_i + jtm_i \pmod M$. Ezt a tm_i differenciájú számtani sorozatot $\bmod M$ nézve kapjuk, hogy a képek (alkalmas sorrendben) ta_i-ból indulva az egymástól $(tm_i, M) = (t, n_i)m_i$ távolságra levő csúcsokat adják, mindegyiket ugyanannyiszor, éspedig (t, n_i)-szer. Vagyis a képek valóban egy szabályos sokszög csúcsait fedik le azonos multiplicitással, és pontosan akkor kapunk „egyszöget”, ha $n_i \mid t$.

Ennek alapján válasszuk t értékét n_k-nak. Ekkor a képekre megismételve a kőzéppontból a csúcsokba mutató vektorok összegét vizsgáló gondolatmenetünket, minden $i < k$-ra az n_i-szögek, valamint az eredeti M-szög képénél ez az összegvektor nulla, az n_k-szög képénél viszont nem, és ezzel ugyanúgy ellentmondásra jutottunk, mint az $n_k = 1$ speciális esetben. ■

Most rátérünk Romanov problémájára, amelynek megoldásához Erdős a fedőrendszereket felhasználta.

12.5.2 Tétel **T 12.5.2**

Végtelen sok olyan páratlan szám van, amely nem írható fel egy kettőhatvány és egy prímszám összegeként. ♣

Bizonyítás: Azt a jóval erősebb állítást igazoljuk, hogy létezik olyan, páratlan

számokból álló végtelen számtani sorozat, amelynek egyik eleme sem írható fel a fenti alakban.

Induljunk ki az alábbi $a_i \pmod{m_i}$, $i = 1, 2, \ldots, 6$ fedőrendszerből:

$$0 \pmod 2,\ 0 \pmod 3,\ 1 \pmod 4,\ 3 \pmod 8,\ 7 \pmod{12},\ 23 \pmod{24}. \tag{5}$$

Felhasználjuk, hogy minden m_i-hez létezik olyan p_i prím, amelyre a 2 rendje mod p_i éppen m_i, azaz $o_{p_i}(2) = m_i$: ilyen p_i prímek rendre a 3, 7, 5, 17, 13, illetve 241:

$$o_3(2) = 2,\ o_7(2) = 3,\ o_5(2) = 4,\ o_{17}(2) = 8,\ o_{13}(2) = 12,\ o_{241}(2) = 24. \tag{6}$$

(Megjegyezzük, hogy minden $m \neq 6$ esetén létezik olyan p prím, amelyre a 2 rendje mod p éppen m, ezért a céljainkra a (3) fedőrendszer nem lett volna alkalmas, de minden olyan fedőrendszer megfelelt volna, amelyben a modulusok között a 6 nem szerepel. Az nyilvánvaló, hogy különböző m-ekhez mindig különböző p prímek tartoznak.)

Tekintsük a fenti a_i, m_i, p_i értékeket és válasszuk s-et úgy, hogy $2^{s-1} > \max_i p_i$ teljesüljön, tehát az (5)–(6) fedőrendszer esetén pl. $s = 9$ megfelel.

Megmutatjuk, hogy az

$$x \equiv 2^{a_i} \pmod{p_i},\ \ i = 1, \ldots, k, \quad x \equiv 1 \pmod{2^s} \tag{7}$$

szimultán kongruenciarendszer tetszőleges $x = c$ megoldását véve c nem írható fel egy kettőhatvány és egy prímszám összegeként. Mivel (7)-ben a modulusok páronként relatív prímek, ezért a kongruenciarendszer megoldható, és a megoldások egy páratlan számokból álló végtelen számtani sorozatot alkotnak, tehát ezzel a tétel állítása igazolva lesz.

Indirekt tegyük fel, hogy egy c megoldásra $c = 2^n + p$, ahol p prím. Mivel $a_i \pmod{m_i}$ fedőrendszer, ezért van olyan i, amelyre $n \equiv a_i \pmod{m_i}$. Tudjuk, hogy a 2 rendje mod p_i éppen m_i, továbbá c kielégíti (7)-et, tehát

$$2^n \equiv 2^{a_i} \equiv c \pmod{p_i}.$$

Ebből következik, hogy $p = c - 2^n \equiv 0 \pmod{p_i}$, vagyis csak $p = p_i$ lehetséges.

Így az ellentmondáshoz elég azt igazolnunk, hogy $c = 2^n + p_i$ nem teljesíti a (7)-beli utolsó kongruenciát, azaz $2^n + p_i \not\equiv 1 \pmod{2^s}$. Ha $n \leq s-1$, akkor ezt $1 < 2^n + p_i < 2^{s-1} + 2^{s-1} = 2^s$ biztosítja. Ha pedig $n \geq s$, akkor azonnal adódik, hogy $2^n + p_i \equiv p_i \not\equiv 1 \pmod{2^s}$. ■

Feladatok (Az (1), illetve (2)-beli jelöléseket használjuk.)

12.5.1 Lássuk be, hogy bármely fedőrendszerre $\sum_{i=1}^{k} 1/m_i \geq 1$.

12.5.2 Mutassuk meg, hogy ha egy fedőrendszerben egy m_i modulust egy (a többi modulustól különböző) osztójára cserélünk ki, akkor továbbra is fedőrendszert kapunk.

12.5.3 Tekintsünk egy minimális fedőrendszert, azaz olyat, amelyből akármelyik maradékosztályát hagyjuk is el, már nem marad fedőrendszer. Igazoljuk, hogy ekkor bármelyik m_i osztója a többi m_j legkisebb közös többszörösének.

12.5.4 Bizonyítsuk be, hogy nincs 2, 3 vagy 4 maradékosztályból álló fedőrendszer, és 5 maradékosztály esetén is csak a (3)-beli modulusok lehetségesek.

12.5.5 Konstruáljunk olyan fedőrendszert, amelyben 3 a legkisebb modulus.

12.5.6 Ahhoz, hogy a diszjunkt fedőrendszer (DFR) fogalma ne legyen üres, engedjük meg, hogy a modulusok között azonosak is előfordulhassanak: $a_i \pmod{m_i}$, $i = 1, \ldots, k$, ahol $1 < m_1 \leq \ldots \leq m_k$, és minden egész szám pontosan egy maradékosztálynak az eleme. Igazoljuk az ilyen DFR-ekre az alábbiakat:
a) $\sum_{i=1}^{k} 1/m_i = 1$;
b) $m_k = m_{k-1}$;
c) minden k-hoz van olyan DFR, ahol $m_1 < m_2 < \ldots < m_{k-1}$.

12.5.7 Bizonyítsuk be, hogy végtelen sok páros szám nem írható fel egy háromhatvány és egy prímszám összegeként. Sőt, általánosan, bármely rögzített $a > 1$ páratlan számhoz, illetve $b > 2$ páros számhoz van végtelen sok olyan páros, illetve páratlan szám, amely nem írható fel $a^n + p$, illetve $b^n + p$ alakban, ahol p prím.

12.6. Additív komplementumok

A nemnegatív egészek A és B végtelen részhalmazai egymás *additív komplementum*ai, ha minden elég nagy természetes szám előáll $a + b$ alakban, ahol $a \in A$, $b \in B$.

Például, legyenek A, illetve B elemei a 0, valamint azok a pozitív egészek, amelyek tízes számrendszerbeli alakjában az egyesektől számítva minden páratlan, illetve páros helyiértéken csakis 0 számjegy szerepel (tehát pl. $3010 \in A$,

$70005 \in B$). Ekkor nyilván minden nemnegatív egész (egyértelműen) felírható $a+b$ alakban, tehát A és B egymás additív komplementumai (a továbbiakban a rövidség kedvéért az additív jelzőt általában elhagyjuk).

Először egy egyszerű szükséges feltételt adunk A és B sűrűségére ahhoz, hogy A és B egymás komplementumai lehessenek, majd megnézzük, mennyire éles ez a sűrűségi feltétel. Ezután konkrét halmazok, nevezetesen a kettőhatványok és a prímek esetén megvizsgáljuk, mennyire ritka komplementum található hozzájuk.

Jelölje $A(n)$, illetve $B(n)$ az A, illetve B halmaz n-nél nem nagyobb elemeinek a számát. Legyen $f(n)$ azoknak a $0 \le t \le n$ egészeknek a száma, amelyek előállnak $t = a + b$ alakban. Ekkor $f(n) \le A(n)B(n)$, hiszen az ilyen t-k felírásában $a \le t \le n$, $b \le t \le n$. (Ez két szempontból is durva becslés, ugyanis egyes t-k többféleképpen is előállhatnak $a+b$ alakban, továbbá az ilyen a, b számokból képezett $a + b$ összegek egy része n-nél nagyobb lesz.) Ha A és B egymás komplementumai, akkor minden $t > t_0$ felírható $t = a + b$ alakban, vagyis $f(n) \ge n - t_0$. Az $f(n)$-re adott alsó és felső becslést összevetve kapjuk, hogy bármely n-re $A(n)B(n) \ge n - t_0$. Ezt n-nel osztva, majd $n \to \infty$ mellett adódik, hogy additív komplementumok esetén

$$\liminf_{n\to\infty} \frac{A(n)B(n)}{n} \ge 1. \tag{1}$$

A gondolatmenetben alkalmazott durva becslések miatt azt gondolhatnánk, hogy (1)-ben nem állhat egyenlőség, az pedig végképp kizártnak tűnhet, hogy a lim inf helyett a lim sup értéke is lehet 1 (azaz ekkor az (1)-beli hányados határértéke 1). Meglepő módon ez mégis megvalósulhat, sőt igen sok ilyen konstrukció is született, ezekből a legelsőt, Danzer példáját mutatjuk be.

12.6.1 Tétel **T 12.6.1**

Léteznek olyan A és B additiv komplementumok, amelyekre

$$\lim_{n\to\infty} A(n)B(n)/n = 1. \clubsuit \tag{2}$$

Bizonyítás: Az A egy igen gyorsan növő, és bizonyos oszthatósági tulajdonságokkal is rendelkező sorozat lesz:

$$a_k = (k^2)! + k. \tag{3}$$

Nyilván $a_k \equiv k \pmod{d}$, ha $d \le k^2$. Ebből következik, hogy

$$a_k,\ a_{k-1},\ \ldots,\ a_{k-d_k+1} \text{ teljes maradékrendszer mod } d_k, \tag{4}$$

ha $d_k \le (k - d_k + 1)^2$. Minden k-hoz válasszunk egy ilyen tulajdonságú, viszonylag nagy d_k-t, amelyre

$$d_k \le d_{k+1} \tag{5}$$

és

$$\lim_{k\to\infty} d_k/k = 1, \tag{6}$$

pl. $d_k = \lfloor k - \sqrt{k} \rfloor$ megfelel.

Legyen most n tetszőleges, és k olyan, amelyre

$$ka_k \le n < (k+1)a_{k+1}. \tag{7}$$

Ekkor (4) alapján van olyan $0 \le s < d_k$, amelyre $n \equiv a_{k-s} \pmod{d_k}$, vagyis n felírható

$$n = a_{k-s} + rd_k \tag{8}$$

alakban. Becsüljük meg itt r lehetséges értékeit (7) és $0 < a_{k-s} \le a_k$ felhasználásával:

$$\frac{(k-1)a_k}{d_k} \le r = \frac{n - a_{k-s}}{d_k} < \frac{(k+1)a_{k+1}}{d_k}\,. \tag{9}$$

Álljon most B_k azokból az rd_k alakú számokból, ahol r kielégíti (9)-et, és legyen

$$B = \bigcup_{k=1}^{\infty} B_k = \bigcup_{k=1}^{\infty} \Big\{ rd_k \mid \frac{(k-1)a_k}{d_k} \le r < \frac{(k+1)a_{k+1}}{d_k} \Big\}\,. \tag{10}$$

Ekkor (8) alapján A és B egymás komplementumai.

Most rátérünk (2) igazolására, ehhez $A(n)$-et, illetve $B(n)$-et felülről becsüljük.

Mivel (7), illetve (3) szerint $n < (k+1)a_{k+1} < a_{k+2}$, ezért

$$A(n) \le k + 1 \tag{11}$$

(valójában $A(n) = k$ vagy $k+1$).

Mivel (10) miatt B_{k+2} legkisebb eleme is legalább $(k+1)a_{k+2}$, ami (7) miatt nagyobb, mint n, ezért $B(n)$-nél B_{k+2}-t már nem kell számításba venni, és így

$$B(n) \le B_{k+1}(n) + B_k(n) + |B_{k-1}| + \Big|\bigcup_{i=1}^{k-2} B_i\Big|. \tag{12}$$

Vizsgáljuk most egyenként a (12) jobb oldalán szereplő tagokat.

(10) szerint B_{k+1} legkisebb eleme legalább ka_{k+1}, tehát B_{k+1} eleve csak akkor játszik szerepet $B(n)$-ben, ha

$$ka_{k+1} \le n, \quad \text{azaz} \quad a_{k+1} \le \frac{n}{k}\,. \tag{13}$$

Ebben az esetben is (7) alapján $n < (k+1)a_{k+1}$, ezért $B_{k+1}(n)$-hez mindenképpen a d_{k+1}-nek legfeljebb a ka_{k+1} és $(k+1)a_{k+1}$ közé eső többszöröseit kell figyelembe venni, tehát

$$B_{k+1}(n) \le \frac{(k+1)a_{k+1} - ka_{k+1}}{d_{k+1}} + 1 = \frac{a_{k+1}}{d_{k+1}} + 1 \le \frac{n}{kd_{k-1}} + 1 \tag{14}$$

(az utolsó egyenlőtlenségnél (5)-öt és (13)-at használtuk fel).

$B_k(n)$, hasonló módon, a d_k-nak a $(k-1)a_k$ és n közé eső többszöröseit számolja össze, vagyis

$$B_k(n) \le \frac{n-(k-1)a_k}{d_k} + 1 \le \frac{n-(k-1)a_k}{d_{k-1}} + 1. \tag{15}$$

Ugyanígy

$$|B_{k-1}| \le \frac{ka_k - (k-2)a_{k-1}}{d_{k-1}} + 1 \le \frac{ka_k}{d_{k-1}} + 1. \tag{16}$$

Végül, $i \le k-2$ esetén B_i minden eleme kisebb $(k-1)a_{k-1}$-nél, tehát

$$\Big|\bigcup_{i=1}^{k-2} B_i\Big| \le (k-1)a_{k-1} - 1. \tag{17}$$

A (12), (14), (15), (16) és (17) egyenlőtlenségek alapján

$$B(n) \le \frac{\frac{n}{k} + n + a_k}{d_{k-1}} + (k-1)a_{k-1} + 2. \tag{18}$$

Mivel (7) alapján $a_k \le n/k$, így (18)-ból

$$B(n) \le n\Big(\frac{1+\frac{2}{k}}{d_{k-1}} + \frac{(k-1)a_{k-1}+2}{n}\Big) \tag{19}$$

következik.

Így (11) és (19) szerint

$$\frac{A(n)B(n)}{n} \le \frac{(k+1)(1+\frac{2}{k})}{d_{k-1}} + \frac{(k+1)((k-1)a_{k-1}+2)}{n}\,. \tag{20}$$

Ha n, és így k is tart a végtelenhez, akkor (20) jobb oldalán az első tört (6) szerint 1-hez, a második tört pedig (7) és (3) alapján 0-hoz tart, azaz

$$\limsup_{n\to\infty} \frac{A(n)B(n)}{n} \le 1. \tag{21}$$

Mivel A és B komplementumok, ezért (1) is teljesül, ami (21)-gyel együtt éppen a kívánt (2) képletet adja. ■

Nevezzük a B-t az A halmaz *teljesen gazdaságos komplementum*ának (TGK), ha (komplementuma az A-nak és) (2) érvényes. A 12.6.1 Tétel szerint az $A = \{(k^2)! + k \mid k = 1, 2, \ldots\}$ halmazhoz létezik TGK. Ruzsa Imre megmutatta, hogy minden olyan $A = \{a_1 < a_2 < \ldots\}$ halmazhoz létezik TGK, amelyre $\lim_{k\to\infty} a_{k+1}/(ka_k) = \infty$ (azaz a 12.6.1 Tételben szereplő A-nál kevésbé ritka halmazok is megfelelnek, ráadásul semmiféle oszthatósági tulajdonságra sincs szükség).

A következőkben áttekintjük, hogy a kettőhatványok, illetve a prímszámok halmazához mennyire ritka komplementum található. Kezdjük a kettőhatványokkal. Ruzsa belátta, hogy ezekhez is létezik TGK. Az alábbiakban csak ennél egy kicsit gyengébb eredményt igazolunk.

12.6.2 Tétel **T 12.6.2**

A kettőhatványok $H = \{2, 4, 8, \ldots\}$ halmazához létezik olyan M komplementum, amelyre

$$M(n) < cn/\log_2 n \tag{22}$$

(ahol c explicite kiszámolható konstans). ♣

Mivel $H(n) = \lfloor \log_2 n \rfloor$, ezért $H(n)M(n)/n < c$, ami valóban nem sokkal rosszabb (2)-nél. Megjegyezzük, hogy tetszőleges $s > 1$ egészre is az s hatványaiból álló $H_s = \{s, s^2, s^3, \ldots\}$ halmazhoz létezik TGK.

Bizonyítás: Mivel a 2 primitív gyök mod 9, ezért primitív gyök mod 3^r is minden r-re (lásd a 3.3.5 Tétel bizonyításában az L2 részt). Ez azt jelenti, hogy ha $(3, n) = 1$, akkor van olyan $0 < k \le \varphi(3^r) < 3^r$, amelyre $n \equiv 2^k \pmod{3^r}$.

Ha $3 \mid n$, akkor ugyanígy $n-1 \equiv 2^k \pmod{3^r}$. Így minden n-hez és r-hez van olyan v és $0 < k < 3^r$, hogy

$$n = 2^k + 3^r v \quad \text{vagy} \quad n = 2^k + 3^r v + 1. \tag{23}$$

Ennek megfelelően az M komplementum elemei majd alkalmas $3^r v$ és $3^r v + 1$ alakú számok lesznek.

Adott n-hez először r-et fogjuk megválasztani, majd megnézzük, milyen v-kre van szükség.

Mivel $k < 3^r$ miatt $2^k < 2^{3^r}$, ezért (23)-ban v mindenképpen pozitív, ha $2^{3^r} \le n$. Ennek alapján válasszuk n-hez r-et a következőképpen:

$$2^{3^r} \le n < 2^{3^{r+1}}. \tag{24}$$

Ekkor (23) és (24) szerint

$$v \le 3^r v < n < 2^{3^{r+1}},$$

és így legyen

$$M = \bigcup_{r=1}^{\infty} M_r, \quad \text{ahol} \quad M_r = \{3^r v,\, 3^r v + 1 \mid 0 < v < 2^{3^{r+1}}\}. \tag{25}$$

Az eddigi meggondolások alapján M komplementuma H-nak.

Most belátjuk, hogy (22) is teljesül.

Legyen

$$K = \{3^r v \mid 0 < r,\, 0 < v < 2^{3^{r+1}}\}, \tag{26}$$

ekkor

$$M(n) \le 2|K|. \tag{27}$$

A K halmazt is kétfelé bontjuk, K_1-re és K_2-re aszerint, hogy $v \le T$, illetve $v > T$, ahol a T-t (az n-től függően) később alkalmasan megválasztjuk.

K_1-ben v értéke T-féle, r értéke pedig legfeljebb $\log_3 n$-féle lehet, vagyis

$$|K_1| \le T \log_3 n. \tag{28}$$

K_2-ben (26) szerint $T < v < 2^{3^{r+1}}$, azaz

$$3^{r+1} > \log_2 T. \tag{29}$$

A 3^r-hez tartozó v-k száma legfeljebb $\lfloor n/3^r \rfloor$, tehát

$$|K_2| < \sum_{r \geq r_0} \frac{n}{3^r} = \frac{3}{2} \cdot \frac{n}{3^{r_0}} ,$$

ahol r_0 a (29)-nek eleget tevő legkisebb r érték. Ebből kapjuk, hogy

$$|K_2| < \frac{9}{2} \cdot \frac{n}{\log_2 T} . \tag{30}$$

(27), (28) és (30) alapján $M(n) < 2T \log_3 n + 9n/\log_2 T$. Innen (22) például a $T = \lfloor n/(\log_2 n)^2 \rfloor$ választással adódik. ■

Most a prímszámok halmazához keresünk minél ritkább komplementumot. Az ezzel kapcsolatos legjobb eredmény Erdőstől származik:

12.6.3 Tétel **T 12.6.3**

A prímszámok P halmazához létezik olyan R komplementum, amelyre

$$R(n) < c \log^2 n \tag{31}$$

(ahol c explicite kiszámolható konstans és log a természetes alapú logaritmust jelöli). ♣

Mivel $P(n) = \pi(n) \sim n/\log n$, ezért $P(n)R(n)/n < c \log n$, ami már lényegesen rosszabb (2)-nél. A másik irányból Ruzsa Imre igazolta, hogy itt (2) biztosan nem érhető el, azaz P-hez nem létezik TGK.

A bizonyítás fő gondolatmenete: Egy olyan valószínűségi mezőt konstruálunk, amelynek elemei a pozitív egészek bizonyos R részsorozatai, és meg fogjuk mutatni, hogy egy ilyen R sorozat 1 valószínűséggel komplementuma a P-nek, és $R(n) \sim c \log^2 n$ ugyancsak 1 valószínűséggel teljesül. Ebből következik, hogy van a tétel állításának eleget tevő R. (Figyeljük meg, hogy ez a gondolatmenet konkrét konstrukció megadása nélkül igazolja a kívánt tulajdonságú sorozat létezését, sőt azt is, hogy „majdnem minden” R sorozat ilyen, ez utóbbit persze a megadott valószínűség mértéke szerint kell érteni.)

Legyenek $0 \leq \alpha_i \leq 1$, $i = 1, 2, \ldots$ tetszőleges valós számok. Ekkor létezik olyan valószínűségi mező, amely a pozitív egészek bizonyos részsorozataiból áll, és bármely n pozitív egészre α_n annak a valószínűsége, hogy $n \in R$, továbbá az $n \in R$ és $m \in R$ események bármely $n \neq m$ esetén függetlenek.

Szemléletesen ezt úgy lehet elképzelni, hogy a sorozatok képzésénél az $1, 2, \ldots$ számokat egymástól függetlenül és rendre $\alpha_1, \alpha_2, \ldots$ valószínűséggel választjuk be a sorozatba.

Legyen most

$$\alpha_i = \min(1,\, d(\log i)/i), \tag{32}$$

ahol $d > 0$ később alkalmasan megválasztandó konstans.

Először azt vázoljuk, hogy egy R sorozat ekkor 1 valószínűséggel komplementuma P-nek.

Legyen Q_n az az esemény, hogy az n *nem* írható fel $n = p + r$ alakban, ahol p prím, $r \in R$, és jelöljük Q_n valószínűségét q_n-nel. Az R akkor lesz komplementuma P-nek, ha a Q_n események közül csak véges sok következik be. A Borel–Cantelli-lemma szerint ennek 1 a valószínűsége, ha a q_n-ek összege konvergens, azaz

$$S = \sum_{n=1}^{\infty} q_n < \infty\,. \tag{33}$$

Számoljuk ki q_n-et. Egy p prímre $n \neq r + p$ azt jelenti, hogy $n - p \notin R$, és ennek $1 - \alpha_{n-p}$ a valószínűsége. A Q_n esemény az, hogy n semmilyen p prímmel sem írható fel $n = r + p$ alakban, és így

$$q_n = \prod_{p<n} (1 - \alpha_{n-p})\,. \tag{34}$$

(34)-et és $1 - x \leq e^{-x}$-et felhasználva, a (33)-beli S-re

$$S = \sum_{n=1}^{\infty} q_n = \sum_{n=1}^{\infty} \prod_{p<n} (1 - \alpha_{n-p}) \leq \sum_{n=1}^{\infty} e^{-\sum_{p<n} \alpha_{n-p}} \tag{35}$$

adódik. Itt a jobb oldalon az e kitevője (32) alapján „lényegében”

$$-d \sum_{p<n} \frac{\log(n-p)}{n-p}\,. \tag{36}$$

Belátható, hogy alkalmas h konstanssal

$$\sum_{p<n} \frac{\log(n-p)}{n-p} > h \log n\,, \tag{37}$$

ha n elég nagy, tehát a (36)-beli kifejezés kisebb, mint $-dh\log n$, és így (35) alapján

$$S < \sum_{n=1}^{\infty} e^{-dh\log n} = \sum_{n=1}^{\infty} n^{-dh},$$

ami valóban konvergens, ha d-t úgy választjuk, hogy $dh > 1$ teljesüljön.

A (37) állítás kicsit hasonlít az 5.6.3 Tételbeli $\sum_{p<n}(\log p)/p \sim \log n$ összefüggéshez, mindkettőben $(\log k)/k$ típusú tagok szerepelnek, azonban a prímek fokozatos ritkulása miatt ez utóbbi összegben a kis k értékekhez tartozó, és így nagyobb $(\log k)/k$ tagok dominálnak, míg (37)-ben fordított a helyzet. (37) igazolásához éppen azt kell felhasználni, hogy a prímek későbbi „viszonylag rövid" intervallumokban is „elég sűrűn" helyezkednek el.

Most rátérünk annak vázolására, hogy 1 valószínűséggel $R(n) \sim c\log^2 n$. $R(n) = \sum_{i=1}^{n} \xi_i$, ahol a ξ_i valószínűségi változó értéke 1, ha $i \in R$, és 0, ha $i \notin R$. Ekkor

$$\sum_{i=1}^{n} E(\xi_i) = \sum_{i=1}^{n} \alpha_i \sim \sum_{i=1}^{n} d\frac{\log i}{i} \sim d\int_1^n \frac{\log x}{x}dx = \frac{d\log^2 n}{2}.$$

Így elég azt igazolni, hogy 1 valószínűséggel $\sum_{i=1}^{n} \xi_i \sim \sum_{i=1}^{n} E(\xi_i)$. Ez általánosan igaz, ha $E(\xi_i)$-re és $D(\xi_i)$-re megfelelő feltételek teljesülnek, amelyek a jelen esetben könnyen ellenőrizhetően valóban fennállnak. ■

Végül bizonyítás nélkül megemlítjük Lorentznek általános halmazok komplementumára vonatkozó alábbi eredményét:

12.6.4 Tétel **T 12.6.4**

Tetszőleges A-hoz létezik olyan B komplementum, amelyre

$$B(n) < 10\sum_{i=a_1}^{n} \frac{\log A(i)}{A(i)}. \ \clubsuit$$

Feladatok

12.6.1 Általánosítsuk a pont legelején szereplő példát 10 helyett tetszőleges $c > 1$ alapú számrendszerre és a helyiértékeknek a páros-páratlan helyett tetszőleges más csoportosítására. Mutassuk meg, hogy az így kapott A és B halmazok egymás komplementumai, és határozzuk meg $\liminf_{n\to\infty} A(n)B(n)/n$ értékét.

12.6.2 Legyen H a kettőhatványok halmaza és $P_1 = \{p, p+1 \mid p \text{ prím}\}$, azaz a prímek mellé vegyük be a $p+1$ alakú számokat is. Igaz-e, hogy H és P_1 egymás komplementumai?

12.6.3 Az alábbi feltételek mindegyikéről döntsük el, hogy szükséges-e, illetve elégséges-e ahhoz, hogy az $A = \{a_1 < a_2 < \ldots\}$ halmaznak létezzen *véges* komplementuma, azaz alkalmas véges B halmazt véve minden elég nagy pozitív egész előálljon egy A-beli és egy B-beli elem összegeként.

a) $a_{i+1} - a_i$ korlátos.
b) A tartalmaz végtelen számtani sorozatot.
c) $\liminf_{n\to\infty} A(n)/n > 0$.
d) $\lim_{n\to\infty} A(n)/n = 1$.

*12.6.4 Legyenek A elemei $a_k = 6^k + k$, B elemei pedig a $6^k(1 - 1/k)$ és 6^{k+1} között a d_k-val oszthatók, ahol d_k egy olyan $2^i 3^j$ alakú szám, amelyre $d_k < k - 5\log_6 k$, de $d_k \sim k$ és $d_{k+1} \geq d_k$. Igazoljuk, hogy A és B egymás teljesen gazdaságos komplementumai.

12.6.5 Mutassuk meg, hogy a prímekhez a 12.6.4 Tétel egy olyan S komplementumot biztosít, amelyre $S(n) < c\log^3 n$ (vagyis így a 12.6.3 Tételnél gyengébb eredményt kapunk).

12.6.6 Lássuk be, hogy tetszőleges A (végtelen) halmaznak van olyan B komplementuma, amelyre $B(n)/n \to 0$, ha $n \to \infty$ (azaz B nulla sűrűségű).

EREDMÉNYEK ÉS ÚTMUTATÁSOK

1. Számelméleti alapfogalmak

1.1.

1.1.1 A hatjegyű szám a háromjegyű szám 1001-szerese, és 1001 osztható 91-gyel.

1.1.2 Mutassuk meg, hogy az $a^2-b^2=(a-b)(a+b)$ szorzatban mindkét tényező páros és (pontosan) az egyik osztható 4-gyel.
Másik lehetőség: $(2k+1)^2-(2m+1)^2=4k(k+1)-4m(m+1)$ jobb oldalán mindkét tag osztható 8-cal.

1.1.3 $\overline{bca}=100b+10c+a=10\cdot\overline{abc}-999a$.

1.1.4 Szorozzuk be $5a+9b$-t alkalmas egész számmal úgy, hogy ehhez a 23 megfelelő többszörösét hozzáadva éppen $3a+10b$-t kapjunk.

1.1.5 Igaz: b), d), f).

1.1.6

(i) Használjuk az $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\ldots+b^{n-1})$ azonosságot.
(ii)–(iii) alkalmazzuk (i)-et b helyett $-b$-vel.

1.1.7 $c=\pm 3$.

1.1.8 $11^{n+2}+12^{2n+1}=12(144^n-11^n)+133\cdot 11^n$.
Bizonyíthatunk teljes indukcióval is.

1.1.9 $n=4k+2$. (Belátható, hogy ez az összes megfelelő n.)

1.1.10 A $(b-1)^2 \mid b^k-1$ oszthatóság ekvivalens $b-1 \mid b^{k-1}+b^{k-2}+\ldots+1$ teljesülésével. Itt a jobb oldalt írjuk át

$$(b^{k-1}-1)+(b^{k-2}-1)+\ldots+(1-1)+k$$

alakba, ekkor az első k tag mindig osztható $b-1$-gyel.

1.1.11 Ha $a\geq b$, akkor $2^a+1=2^{a-b}(2^b-1)+2^{a-b}+1$. Az eljárást folytatva kapjuk, hogy van olyan $d<a$, amelyre $2^b-1 \mid 2^d+1$. Innen $2^b-1\leq$ $\leq 2^d+1\leq 2^{b-1}+1$, amiből a kívánt $b\leq 2$ adódik. — Egy másik út: Ha b-nek van egy $c>1$ páratlan osztója, akkor $2^c-1 \mid 2^{ac}-1$, továbbá $2^c-1 \mid 2^b-1 \mid 2^a+1 \mid 2^{ac}+1$, ahonnan $2^c-1 \mid 2$, ami ellentmondás. Ha b osztható 4-gyel, akkor $15=2^4-1 \mid 2^b-1 \mid 2^a+1$, ez azonban lehetetlen, ugyanis $3 \mid 2^a+1 \iff a$ páratlan és $5 \mid 2^a+1 \iff a=4k+2$.

1.1.12
a) $a = bq$ alapján $|a| = |b| \cdot |q| \geq |b| \cdot 1$, ha $q \neq 0$.
b) Az a) rész alapján a osztóinak a száma legfeljebb $2 \cdot |a|$.

1.1.13 Használjuk fel, hogy egy pozitív egész számnak önmagán kívül a legnagyobb pozitív osztója legfeljebb a szám fele, a következő pedig legfeljebb a szám harmada lehet. — Válasz:
a) a pozitív páros számok;
b) a 3-mal, illetve a 4-gyel osztható pozitív számok (csak $3k = k + k + k$, $4k = 2k + k + k$ és $6k = 3k + 2k + k$ lehetséges).

1.1.14 Jelölje a szám számjegyeit az egyes helyi értéktől (azaz „hátulról") kezdve $a_0, \ldots, a_s$, ekkor a szám

$$\overline{a_s a_{s-1} \ldots a_1 a_0} = a_s 10^s + a_{s-1} 10^{s-1} + \ldots + a_1 10 + a_0.$$

Használjuk fel a következőket:
a) $10^k - 1$ mindig osztható 9-cel.
b) $k \geq 2$ esetén 10^k osztható 4-gyel, illetve 25-tel.
c) $k \geq 3$ esetén 10^k osztható 8-cal, illetve 125-tel.
d) Ha k páratlan, akkor $10^k + 1$, ha pedig k páros, akkor $10^k - 1$ osztható 11-gyel.

1.1.15 Nem létezik, vizsgáljuk a 3-mal való oszthatóságot.

1.1.16 Létezik: bizonyítsuk be teljes indukcióval, hogy bármely k-ra létezik (pontosan egy) olyan k-jegyű szám, amelyben csak az 1 és 2 számjegyek fordulnak elő, és amely osztható 2^k-val.

1.1.17 b) $\binom{n}{k}$ egész szám.

1.1.18 Minden $n > 1$-re az első játékosnak van nyerő stratégiája.

1.1.19 Írjuk fel a számokat egy kettőhatvány és egy páratlan szám szorzataként, és használjuk a skatulyaelvet. — Okoskodhatunk teljes indukcióval is.

1.1.20 A $0 = 0 \cdot q$ felírásban q nem egyértelmű.

1.1.21 a) $n = 4k + 2$. b) $n = \pm 4$.

1.1.22
a) Osztható; a hányadosuk (a nevező gyöktelenítése után) ilyen alakra hozható.
b) $1 + \sqrt{2} \mid 1$.
c) $1 + \sqrt{2}$ hatványai megfelelnek.
d) Végtelen sok.

e) Ha $\pm 1 = c^2 - 2d^2 = (c + d\sqrt{2})(c - d\sqrt{2})$, akkor $c + d\sqrt{2} \mid 1$.
A megfordításhoz mutassuk meg, hogy ha $c + d\sqrt{2} \mid r + s\sqrt{2}$, akkor $c^2 - 2d^2 \mid r^2 - 2s^2$.

f) Ha lenne ezeken kívül is egység, akkor azt alkalmas $\pm(1 + \sqrt{2})^k$-val beszorozva egy olyan $u + v\sqrt{2}$ egységet is kapnánk, amelyre

$$1 < u + v\sqrt{2} < 1 + \sqrt{2}.$$

Itt e) felhasználásával u és v előjelének mind a négy lehetséges értékrendszeréből ellentmondáshoz jutunk.

g) Mindkét lehetőség végtelen sokszor előfordul: ez lényegében e)-ből következik.

1.1.23 d) (ii) és (iv) bármely integritási tartományban igaz, (i) és (iii) pedig pontosan akkor, ha létezik egységelem. (Ha nincs egységelem, akkor $a \mid b$, $b \mid a \iff a = b = 0$.)

1.2.

1.2.1 Válasz: 97.
Útmutatás: A háromjegyű szám osztója a két szám különbségének.

1.2.2 Mivel csak m-féle osztási maradék lehet, ezért lesz végtelen sok olyan kettőhatvány, amelyek azonos maradékot adnak m-mel osztva.

1.2.3 Tekintsük a $c_1, c_1 + c_2, \ldots, c_1 + c_2 + \ldots + c_n$ számok n-nel való osztási maradékait.

1.2.4 Ha m az adott szám, akkor vegyük azokat a legfeljebb $m + 1$-jegyű számokat, amelyeknek minden számjegye 1-es: 1, 11, 111, ... Ezek között biztosan lesz két olyan, amelyek azonos maradékot adnak m-mel osztva, így a különbségük osztható m-mel és a kívánt alakú.

1.2.5 Jelöljük φ_k-nak m-mel való osztási maradékát r_k-val. Az (r_k, r_{k+1}) párok csak m^2 különböző értéket vehetnek fel, ezért lesz olyan $t > s$, amelyre $(r_t, r_{t+1}) = (r_s, r_{s+1})$. Lássuk be, hogy ekkor bármely k-ra $(r_k, r_{k+1}) = (r_{k+t-s}, r_{k+t-s+1})$, azaz az r_n maradékok periodikusan ismétlődnek ($t - s$ periódus szerint). Mivel $r_0 = 0$, ezért bármely j-re $r_{j(t-s)} = 0$, azaz $m \mid \varphi_{j(t-s)}$.

1.2.6

a) Minden szám $3k$ vagy $3k \pm 1$ alakú, ezek négyzete $3s$, illetve $3s + 1$ alakú, azaz egy négyzetszám 3-mal osztva 0 vagy 1 maradékot adhat.

b) 0, 1. c) 0, ± 1. d) 0, 1, 4.

1.2.7 Vizsgáljuk az összeg maradékát 3-mal vagy 4-gyel osztva.

1.2.8

a) Nincs. Vizsgáljuk a 4-gyel és az 5-tel való osztási maradékot.

b) Az a) részhez hasonlóan megmutatható, hogy a nyolc- vagy többjegyű számok között nincs ilyen négyzetszám, továbbá a négy- vagy hatjegyű ilyen számok utolsó jegye csak 4 lehet. Ez utóbbiaknál vizsgáljuk a 11-gyel, illetve a $111/3 = 37$-tel való oszthatóságot. — Válasz: az egyetlen ilyen négyzetszám a 7744.

1.2.9 Mutassuk meg, hogy egy számnak és bármely páratlan kitevőjű hatványának ugyanaz a maradéka 3-mal osztva.

1.2.10 Válasz: 16 (azaz a szorzat minden esetben osztható 2^{16}-nal, és vannak olyan számok, amikor 2^{17}-nel már nem).

1.2.11 A $\lfloor\sqrt{n}\rfloor = k$ egyenlőség pontosan a $k^2 \le n < (k+1)^2$ számokra teljesül. Ezek közül éppen a k^2, $k^2 + k$ és $k^2 + 2k$ osztható k-val. — Válasz: $3(10^5 - 1) = 299\,997$.

1.2.12 $\lfloor a + b\rfloor - (\lfloor a\rfloor + \lfloor b\rfloor) = 0$ vagy 1.

1.2.13 Nem. Például $12 = 4q + r$ esetén $|r| \ge 4$.

1.2.14 Legyen a számrendszer alapszáma t. Ha $d \mid t - 1$, akkor egy szám d-vel való osztási maradéka megegyezik a számjegyei összegének az osztási maradékával. Ha $d \mid t^k$, akkor az osztási maradék megegyezik az utolsó k számjegyből álló szám osztási maradékával. Ha $d \mid t + 1$, akkor az osztási maradék megegyezik a számjegyek váltakozó előjelű összegének az osztási maradékával (az egyesek helyén álló számjegyet pozitív előjellel kell venni).

1.2.15 Ez tulajdonképpen az előző feladatnak a $t = 100, d = 99$ speciális esete.

1.2.16 Vizsgáljuk a 9-cel való osztási maradékot. — Válasz: 8.

1.2.17 A 9-es számrendszerbeli jegyeket egyenként átírjuk 3-as számrendszerbeli (esetleg 0-val kezdődő) kétjegyű számokká. — Hasonló meggondolás alkalmazható minden olyan esetben, amikor az egyik alap a másiknak (pozitív egész kitevős) hatványa.

1.2.18 Válasz: $n = 8$.
Útmutatás: A $t^3 \le n \le (t+1)^2 - 1$ feltételből $t = 2$ adódik.

1.2.19 A feltételekből rögtön adódik, hogy a jobb oldali szorzótényező 1102. A részletszorzatok összeadásából látszik, hogy a számrendszer alapszáma $t \le 4$, a szorzat utolsó jegye miatt viszont t páratlan, így $t = 3$. Hasonló meggondolásokból kapjuk, hogy az első szorzótényező 2102.

1.2.20 A $t \mid 735$, $t \ge 6$ és $t < 10$ feltételekből $t = 7$.

1.2.21

a) Az $1, 2, 4, \ldots, 2^9$ súlyokkal $2^{10}-1 = 1023$ grammig bezárólag minden egész gramm lemérhető. Ez a lehető legtöbb: egy mérés során minden egyes súlynál két lehetőség között választhatunk: betesszük a serpenyőbe vagy nem tesszük be. Így tíz súllyal legfeljebb $2^{10}-1$-féle értéket lehet lemérni (az 1-et azon eset miatt kell levonni, amikor egyik súlyt sem tesszük be a serpenyőbe).

b) Az $1, 3, 9, \ldots, 3^9$ súlyokkal $(3^{10}-1)/2$ grammig minden egész gramm lemérhető: a hármas számrendszerbeli felírásnál a 2-es számjegyeket „-1-esekre" kell átváltani. Ennél jobb súlykészlet nincs: a méréseknél minden súlyra 3 lehetőség van (egyik serpenyő — másik serpenyő — egyik sem), azonban a két serpenyő szimmetriája miatt az így kapott számot 2-vel el kell osztani.

1.2.22 A keresett határérték $\log_2 10 = 3.3219\ldots$

1.2.23 Az 1.2.2 Tétel bizonyítását kell értelemszerűen módosítani.

1.3.

1.3.1 $14 = 3794 \cdot (-44) + 2226 \cdot 75$.

1.3.2

a) A $(3n+5, 7n+12) = d$ jelöléssel $d \mid -7(3n+5) + 3(7n+12) = 1$, és így $d = 1$.

b) A $(3n^2+1, 4n^2+3) = d$ jelöléssel $d \mid -4(3n^2+1)+3(4n^2+3) = 5$, továbbá $5 \nmid 3n^2+1$, és így $d = 1$.

c) Az $(n!-1, (n+1)!-1) = d$ jelöléssel $d \mid (n+1)!-1-(n+1)(n!-1) = n$, és így $d \mid n! - (n!-1) = 1$.

d) A $(7^n-2, 7^{n+1}-5) = d$ jelöléssel $d \mid (7^{n+1}-5) - 7(7^n-2) = 9$, továbbá $7^n - 2 = (2\cdot 3+1)^n - 2 = 3k+1-2 = 3k-1$, tehát d nem lehet osztható 3-mal.

1.3.3 1, ha n páratlan, és 2, ha n páros.

1.3.4 a) 5 vagy 10. b) 5, 15 vagy 45.

1.3.5 6, 10, 15 vagy 21, 66, 77 stb.

1.3.6 Igaz: a), c).

1.3.7 Válasz: (a, b). — Útmutatás: $b \mid ka \iff \frac{b}{(a,b)} \mid k$.

1.3.8

a) Igaz: mivel $(a+n, b+n) \mid (a+n) - (b+n) = a - b$, biztosan megfelelnek azok az n-ek, amelyekre $a + n = k(a-b) + 1$ alakú.

b) Igaz. c) Hamis, ellenpélda $a = 1, b = 4$.

1.3.9

a) Végtelen sok; ha u, v ilyen számpár, akkor bármely t egésszel az $u + tb, v - ta$ számpár is megfelel.

b) 1.

c) (a, b).

1.3.10 b) Használjuk fel, hogy δ és δ_1 kölcsönösen osztják egymást.

1.3.11 Először lássuk be, hogy $c(a, b) \mid (ca, cb)$. Ezután a $c(a, b)q = (ca, cb)$ egyenlőségben mutassuk meg, hogy q egység.

1.3.12

a) Pontosan azoknak, amelyek a 10-hez relatív prímek (azaz nem oszthatók sem 2-vel, sem 5-tel). — Útmutatás: Használjuk az 1.2.4 feladat gondolatmenetét, majd az 1.3.9 Tételt.

b) A legkisebb ilyen a 3^{1000} darab 1-esből álló csupaegy. — Útmutatás: Igazoljuk k szerinti teljes indukcióval, hogy a 3^k-nal osztható legkisebb csupaegy éppen 3^k darab 1-esből áll.

1.3.13 Használjuk fel többször az $r \mid s \Rightarrow c^r - 1 \mid c^s - 1$ összefüggést, valamint az $(n, k) = nu + kv$ előállítást.

1.3.14

a) Mutassuk meg, hogy ha (n, k kettőhatványok és például) $k < n$, akkor $a^k + 1 \mid a^n - 1$.

b) $a^{(n,k)} + 1$, ha $n/(n, k)$ és $k/(n, k)$ páratlan, egyébként pedig 1, illetve 2, aszerint, hogy a páros, illetve páratlan.

1.3.15 A másodszomszédok is relatív prímek. A harmadszomszédok közül a 3-mal osztható indexűek legnagyobb közös osztója 2, a többiek relatív prímek.

1.3.16 Használjuk fel a $\varphi_{m+n} = \varphi_{m-1}\varphi_n + \varphi_m\varphi_{n+1}$ azonosságot. Ebből a $k \mid n \Longrightarrow \varphi_k \mid \varphi_n$ állítást az n/k szerinti teljes indukcióval igazolhatjuk. A megfordításhoz és a legnagyobb közös osztóra vonatkozó állításhoz lássuk be, hogy ha $a = bq + r$, akkor $(\varphi_a, \varphi_b) = (\varphi_b, \varphi_r)$. — Egy másik lehetőség: Mutassuk meg, hogy bármely m-re az m-mel osztható Fibonacci-számok indexei éppen a legkisebb ilyen tulajdonságú nemnulla Fibonacci-szám indexének a többszörösei.

1.3.17 A két szakasz hosszát a-val és b-vel jelöljük, k és n pedig alkalmas pozitív egészeket jelentenek.

a) Ha $a/b = k/n$, akkor $a/k = b/n$ közös mérték. Megfordítva, ha c közös mérték, azaz $a = kc$, $b = nc$, akkor $a/b = k/n$.

b) Végtelen sok; bármely n-re egy közös mérték n-edrésze is közös mérték.

c) A maradékos osztás megfelelője: annyiszor felmérjük a kisebbik szakaszt a nagyobbikra, ahányszor csak lehet, azaz $a = bq + r$, ahol q pozitív egész, r valós, és $0 \leq r < b$. Ha a két szakasz összemérhető, $a = kc$, $b = nc$ (ahol c közös mérték), akkor az a-val és b-vel végzett euklideszi algoritmus tulajdonképpen ugyanaz, mint a k és n egész számokkal végzett euklideszi algoritmus, tehát véget ér. Megfordítva, ha a szakaszokkal végzett euklideszi algoritmus véget ér, akkor az utolsó nemnulla maradék közös mérték lesz.

d) Ilyen „kitüntetett" közös mérték létezése az euklideszi algoritmusból következik.

e) Az $ABCD$ négyzet b hosszúságú oldalát mérjük fel A-ból az a hosszúságú AC átlóra. Az így kapott E pontra $AE = b$ és $EC = r$. Állítsunk E-ből merőlegest az átlóra, ez messe a BC oldalt F-ben. Ekkor $r = EC = EF = FB$. Ha most az algoritmus következő lépésében b-t osztjuk maradékosan r-rel, akkor először BF-et felmérve BC-re, ezután az EFC egyenlőszárú derékszögű háromszög CF átfogóját és CE oldalát kell maradékosan elosztanunk. Ezzel azonban a kiindulási helyzet ismétlődött meg kisebb méretekben: egy (kisebb) négyzet átlóját és oldalát kell összehasonlítanunk. Ez azt mutatja, hogy az euklideszi algoritmus a végtelenségig folytatódik.

1.4.

1.4.1 Eredmény: a) és b) 3. c) 5. d) 7.
Útmutatás: Vizsgáljuk a 3-mal, 5-tel, illetve 7-tel való osztási maradékokat.

1.4.2 Nem létezik; ha a d differencia pozitív, és $c > 1$ a számtani sorozat tetszőleges eleme, akkor például a $c + cd$ elem biztosan összetett.

1.4.3 Válasz: 3 éves. — Útmutatás: Vizsgáljuk a 3-mal való osztási maradékokat. — *Megjegyzés*: A két nagyobb unoka életkorára nem tudunk következtetni, például a $3, 5, 7$, illetve $3, 7, 11$, illetve $3, 13, 17$ számhármasok mindegyike megfelel a feltételeknek. Megoldatlan probléma, hogy létezik-e végtelen sok ilyen tulajdonságú számhármas. A feladat állítása éppen az volt, hogy akármelyik ilyen számhármas legkisebb eleme szükségképpen a 3.

1.4.4

a) alkalmazzuk az $a - 1 \mid a^k - 1$, illetve $k = rs$ esetén az $a^r - 1 \mid a^k - 1$ oszthatóságokat.

b) Ha $k = rs$, ahol s páratlan, akkor $a^r + 1 \mid a^k + 1$.

1.4.5 Eredmény: $t = 2, k = 1$.
Útmutatás: Vizsgáljuk a $t + 1$-gyel vagy t-vel való oszthatóságot.

1.4.6 Eredmény: a), d) és e) $n = 1$. b) $n = 2, 4$. c) Nincs ilyen n.
Útmutatás: a)-nál vizsgáljuk a 3-mal való oszthatóságot, a másik négy kifejezést pedig bontsuk szorzattá.

1.4.7
a) Ha $n = ab$, ahol $0 < a \leq b$, akkor $a \leq \sqrt{n}$, így csak $a = 1$ lehet.
b) Ha ennek a legkisebb d osztónak lenne egy nemtriviális pozitív s osztója, akkor $s \mid n$ is igaz és $1 < s < d$, ami ellentmondás.
c) Ha $n = dk$, ahol d az 1-nél nagyobb osztók közül a legkisebb, akkor a b) rész szerint d prím, és az a) rész felhasználásával kapjuk, hogy k is prím.

1.4.8 Használjuk ki a 17 *prím* tulajdonságát.

1.4.9 A felbonthatatlanok a $4k + 2$ alakú számok, prímek pedig nincsenek.

1.4.10
a) Vizsgáljuk a $p \mid p^2$ oszthatóságot (és használjuk fel az 1.1.23a feladat megoldásánál látott gondolatmenetet is).
b) Ugyanúgy okoskodhatunk, mint az 1.4.3 Tétel bizonyításának I. részében.

1.5.

1.5.1 Ha $a = p_1 \dots p_r$, akkor $|p_i| \geq 2$ miatt $|a| \geq 2^r$.

1.5.2
a) A $2t$, $\pm 2^k$ és $2^k p$ alakú elemek, ahol t tetszőleges páratlan szám és p tetszőleges páratlan, az egészek körében felbonthatatlan szám.
b) Például $2^2 \cdot 3^{1998}$.

1.5.3 Első bizonyítás: nem igaz a páros számok körében, hogy egy felbonthatatlan szükségképpen prím (sőt, egyáltalán nincsenek prímek).
Második bizonyítás: a legutolsó lépésben szereplő $p_1 \mid q_1 - p_1 \Rightarrow p_1 \mid q_1$ következtetés a páros számok körében nem érvényes, hiszen itt $p_1 \nmid p_1$.

1.5.4 $1000 = 20 \cdot 50 = 10 \cdot 10 \cdot 10$.

1.5.5 Felhasználjuk, hogy V nemnulla elemei egyértelműen felírhatók $2^k 5^m t$ alakban, ahol a k és m kitevők tetszőleges egészek és t a 10-hez relatív prím egész.
a) Egységek: $\pm 2^k 5^m$. — Felbonthatatlanok: $2^k 5^m p$, ahol $p \neq \pm 2, \pm 5$ az egészek körében felbonthatatlan szám.
b) A $2^k 5^m t$ felbontása V-ben tulajdonképpen t felbontását jelenti az egész számok körében.

c) Legyen $f(2^k 5^m t) = |t|$ és $f(0) = 0$.

1.5.6 Az utolsó lépésben $p_1 \mid q_1 q_3 \dots q_s$ adódik, és ennek lehetetlenségéhez még egyszer fel kell használni az indukciós feltevést $a = q_1 q_3 \dots q_s$-re.

1.5.7 Legyen $a = \pm p_1^{k_1} \dots p_r^{k_r}$, ahol a p_i számok páronként különböző pozitív felbonthatatlanok és $k_i > 0$, továbbá $k = k_1 + \dots + k_r$. Ekkor a felbontások száma $2^{k-1} k!/(k_1! \dots k_r!)$.

1.5.8 Az ab felbonthatatlan tényezőkre bontását állítsuk elő a és b felbontásából, és használjuk fel, hogy az ab felbontásában szerepelnie kell a p egységszeresének is.

1.5.9 A megfelelő p_1, p_2, p_3 értékhármasok: $5, 2, 2$; $-5, -2, -2$; $5, 2, -3$; $5, -3, 2$; $-5, -2, 3$; $-5, 3, -2$. — Útmutatás: Az átalakítás után kapott $p_2 p_3 = (p_1 - p_2 - p_3)(p_2 + p_3)$ egyenlőség a számelmélet alaptétele szerint csak úgy teljesülhet, ha $p_2 + p_3 = \pm p_2, \pm p_3, \pm 1$ vagy $\pm p_2 p_3$.

1.5.10 Válasz: 2 és 3. — Útmutatás: Legyen $x^3 + y^3 = p^\alpha$. Itt feltehető, hogy x és y relatív prímek. Bontsuk a bal oldalt szorzattá, ekkor mindkét tényező szükségképpen a p-nek hatványa. Fejezzük ki innen xy-t.

1.6.

1.6.1 Akkor és csak akkor k-adik hatvány, ha a kanonikus alakjában minden prím kitevője osztható k-val.

1.6.2

a) Legyen p az ab szorzat a tényezőjének egy tetszőleges prímosztója. Mivel $(a, b) = 1$, ezért $p \nmid b$, vagyis a p ugyanakkora kitevővel szerepel az a és az ab kanonikus alakjában. Ezután használjuk fel az 1.6.1 feladatot.

b) Ha a szorzat nem nulla, akkor a két tényező egy-egy k-adik hatvány egységszerese lesz.

c) A tényezőkről azt kell feltenni, hogy páronként relatív prímek.

1.6.3 Az 1.6.2a feladatra támaszkodjunk.

1.6.4 Válasz: 3 és 7. — Útmutatás: A számlálót bontsuk szorzattá, majd alkalmazzunk az 1.6.2a feladathoz hasonló gondolatmenetet.

1.6.5

a) Ha $a_1 \mid a$ és $b_1 \mid b$, akkor az oszthatóság elemi tulajdonságai alapján $a_1 b_1 \mid ab$. A megfordításhoz az 1.6.2 Tételt használjuk fel. Tekintsük az ab egy tetszőleges p prímosztóját, és legyen a p kitevője a, b, illetve c kanonikus alakjában rendre α, β, illetve γ (ezek között a 0 is előfordulhat). A $c \mid ab$ feltétel szerint $\gamma \le \alpha + \beta$, és azt kell megmutatni, hogy γ előáll $\gamma = \alpha' + \beta'$ alakban, ahol $0 \le \alpha' \le \alpha$ és $0 \le \beta' \le \beta$.

b) alkalmazzuk az a)-ban látott gondolatmenetet, és használjuk fel, hogy α és β közül az egyik 0. — Egy másik lehetőség: Legyen $a_1b_1 = a_2b_2$, ahol $a_i \mid a$ és $b_i \mid b$. Ekkor $a_1 \mid a_2b_2$, továbbá $(a_1, b_2) = 1$, tehát $a_1 \mid a_2$. Ugyanígy a fordított oszthatóság is teljesül, ezért (a pozitivitás miatt) $a_1 = a_2$.

c) Például a és b tetszőleges $c > 1$ közös osztója előáll $c = 1 \cdot c = c \cdot 1$ alakban.

d) Használjuk az a), illetve b) részben látott gondolatmenetet.

e) $(a, b) \mid c \mid [a, b]$.

1.6.6 Használjuk az 1.6.2 Tételt.

1.6.7 a) 2^{30}. b) $2^{10} \cdot 3^2$. c) $2^3 \cdot 3 \cdot 5 \cdot 7 = 840$.

1.6.8 A keresett n-ek a négyzetszámok. — Útmutatás: Használjuk fel a $d(n)$ képletét és az 1.6.1 feladatot. — Egy másik lehetőség: Képezzünk *osztópár*okat; minden $d \mid n$ osztóhoz párosítsuk az n/d *komplementer osztó*t, és vizsgáljuk meg, mely esetben fordul elő, hogy egy osztó és a komplementer osztója megegyeznek.

1.6.9 Válasz: 20. — Útmutatás: Vizsgáljuk meg, hogy egy adott sorszámú zárhoz mely őrök nyúltak hozzá, és alkalmazzuk az előző feladatot.

1.6.10 b) Egyenlőség akkor és csak akkor teljesül, ha n kanonikus alakjában minden prím kitevője páratlan.

1.6.11

a)–b) Vizsgáljuk meg, hány olyan osztója lehet n-nek, amely nagyobb, mint $n/2$, illetve $n/3$.

c) Képezzünk osztópárokat, amelyek szorzata n, ezekben a kisebbik (pontosabban a nem-nagyobbik) elem legfeljebb $\sqrt{n}$. — Egy másik lehetőség: alkalmazzuk az a) és b) részben látott gondolatmenetet általában n/k-ra, és válasszuk meg k értékét optimálisan.

1.6.12 Válasz: $n^{d(n)/2}$. — Útmutatás: Képezzünk osztópárokat.

1.6.13 Válasz: $n + 1$. — Útmutatás: (i) $n + 1$ darab osztó valóban megadható, mert $2^i 5^{n-i}$, $i = 0, 1, \ldots, n$ (az egyetlen) megfelelő választás. (ii) Több osztó már nem lehet jó, ugyanis bármely $n + 2$ osztó között a skatulyaelv alapján található (legalább) kettő olyan, amelyekben az 5 kitevője azonos, és így ezek valamelyike osztója lesz a másiknak.

1.6.14

a) $a \mid b$.

b) 8.

c) 2^r, ahol r a b/a különböző prímosztóinak a száma.
(A b) és c) résznél az x, y és y, x számpárokat $x \neq y$ esetén különbözőknek tekintettük.)

1.6.15 Az $(a,b)[a,b]=ab$ azonosság (1.6.6/III. Tétel) bizonyításához hasonló gondolatmenetet lehet alkalmazni.

1.6.16 Igaz: b), d).

1.6.17

a) $a \mid [a,b] \mid a+b \Longrightarrow a \mid b$, ugyanígy $b \mid a$.

b), d) Osszunk le (a,b)-vel, és használjuk fel az 1.6.16b feladatot.

c) Például $a=10k$, $b=15k$, vagy $a=u(u+v)$, $b=v(u+v)$.

1.6.18 Mind a feltétel, mind pedig az állítás azzal ekvivalens, hogy a és b bármely *közös* prímosztója ugyanakkora kitevővel szerepel a és b kanonikus alakjában.

1.6.19 Legyen egy tetszőleges p prím kitevője a, b, illetve c kanonikus alakjában rendre α, β, illetve γ (ezek között a 0 is előfordulhat). Ekkor az a)-beli azonossághoz azt kell igazolni, hogy $\max\bigl(\alpha,\min(\beta,\gamma)\bigr) = \min\bigl(\max(\alpha,\beta),\max(\alpha,\gamma)\bigr)$. Ennek helyességét külön-külön ellenőrizzük le abban a három esetben, amikor α a három kitevő közül a legkisebb, a középső, illetve a legnagyobb. Hasonlóan bizonyíthatunk a b) résznél is.

1.6.20

a) Az előző feladat jelöléseivel élve, mindkét feltétel azzal ekvivalens, hogy α, β és γ közül kettő egyenlő, és a harmadik ezeknél nem kisebb.

b) Végtelen sok.

c) Az a)-beli állítás megfelelője igaz marad, ha a legnagyobb közös osztót mindenhol legkisebb közös többszörösre cseréljük. A kitevőkre ez azt jelenti, hogy α, β és γ közül kettő egyenlő, és a harmadik ezeknél nem nagyobb. — A megoldásszám az abc különböző prímosztóihoz tartozó δ értékek szorzata, ahol $\delta=3\alpha+1$, ha $\alpha=\beta=\gamma$, és $\delta=2\min(\alpha,\beta,\gamma)+1$ egyébként. (A megoldás akkor és csak akkor egyértelmű, ha $(a,b,c)=1$.)

1.6.21 Bontsuk minél jobban szorzattá p^4-1-et, és külön-külön igazoljuk a 16-tal, a 3-mal és az 5-tel való oszthatóságot.

1.6.22 Bontsuk szorzattá a^6-b^6-t, és külön-külön igazoljuk a 8-cal, a 7-tel és a 9-cel való oszthatóságot.

1.6.23 A kifejezést bontsuk szorzattá, és a 360 prímhatvány tényezőire külön-külön mutassuk meg az oszthatóságot.

1.6.24 Az osztó kanonikus alakjában a megfelelő tényezőkre külön-külön igazoljuk az oszthatóságot. Használjuk fel az $a-b \mid a^m-b^m$ típusú oszthatóságokat, valamint a 101-gyel való oszthatósághoz a binomiális tételt.

1.6.25 a) 275. b) Nem végződik nullára.

1.6.26 a) Az $n!$ kanonikus alakjában bármely p prím kitevője kisebb, mint n: ha $p^s \le n < p^{s+1}$, akkor

$$\alpha_p = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{s} \left\lfloor \frac{n}{p^k} \right\rfloor \le \sum_{k=1}^{s} \frac{n}{p^k} = \frac{n(p^s-1)}{p^s(p-1)} < \frac{n}{p-1} \le n\,.$$

b) $c = 2$, $n = 2^j$.

1.6.27

a) $\binom{n}{k} = (n/k)\binom{n-1}{k-1}$. Innen $k \mid n\binom{n-1}{k-1}$, és mivel $(k,n) = 1$, ezért $k \mid \binom{n-1}{k-1}$. Ez azt jelenti, hogy $\binom{n}{k}/n = \binom{n-1}{k-1}/k$ egész szám.

b) Nem igaz, ellenpélda $\binom{10}{4}$.

c) (c1) $n =$ prím. (c2) $n = 2^j$. (c3) $n = 2^j - 1$.

d) Nincs: $k\binom{n}{k} = n\binom{n-1}{k-1}$. Innen $n \mid k\binom{n}{k}$. Ha $(n, \binom{n}{k}) = 1$ lenne, akkor ebből $n \mid k$ következne, ami lehetetlen.

1.6.28 A megfelelő rozmárlétszámok éppen a kettőhatványok.

1.6.29 Első megoldás: Megfelel egy olyan prím, amely az adott $n! + k$ szám kanonikus alakjában magasabb hatványon szerepel, mint a k-ban.
Második megoldás: Mindegyik számnak van $n/2$-nél nagyobb prímosztója, és ez semelyik másik számnak sem osztója.

1.6.30 9.

1.6.31 A négyzetmentes számok (azaz amelyek nem oszthatók semmilyen egynél nagyobb egész szám négyzetével).

1.6.32 Bizonyítsunk indirekt. Vezessük vissza a feladatot arra az esetre, amikor a két k-adik hatvány relatív prím, majd mutassuk meg, hogy a különbségük osztója mindkét k-adik hatvány 2-szeresének, és így a 2-nek is, ami lehetetlen.

1.6.33

a) Indirekt: $(a/b)^5 = 100 \Rightarrow a^5 = 100b^5$, majd vizsgáljuk a két oldal kanonikus alakjában az 5 (vagy a 2) kitevőjét.

b) Indirekt: $6^{a/b} = 18 \Rightarrow 6^a = 18^b$, itt feltehető a, $b > 0$. Vizsgáljuk a két oldal kanonikus alakjában a 2 és a 3 kitevőjét.

1.6.35 a) Nem létezik. b) Létezik.

2. Kongruenciák

2.1.

2.1.1 alkalmazzuk a P1 példánál látott módszert.

2.1.2 Válasz: 999. — Útmutatás: $999 \equiv -1 \pmod{1000}$.

2.1.3 A 11-gyel való oszthatósági szabály bizonyítása:

$$10 \equiv -1 \pmod{11} \implies 10^k \equiv (-1)^k \pmod{11},$$

és így

$$\overline{a_s a_{s-1} \dots a_1 a_0} = a_s 10^s + a_{s-1} 10^{s-1} + \dots + a_1 10 + a_0 \equiv$$
$$\equiv a_0 - a_1 + a_2 \pm \dots + (-1)^s a_s \pmod{11}.$$

2.1.4 Igaz: a), d), e), h).

2.1.5 Válasz: 50. — Útmutatás: A négyzetszámok lehetséges utolsó számjegyeit a 101-féle számjegy, azaz a 101 szerinti összes maradék négyzetre emeléséből kapjuk meg. Határozzuk meg, hogy így hány páronként inkongruens érték keletkezik, ehhez vizsgáljuk meg, hogy a négyzetre emeléskor milyen egybeesések történnek. Használjuk fel a 2.1.4h feladatot.

2.1.6 A „tétel" hamis, például $\binom{7}{4} \not\equiv \binom{8}{4}$. A bizonyításban ott a hiba, hogy egy (egész értékű) tört számlálójába nem szabad azzal kongruens értéket helyettesíteni, még akkor sem, ha az új tört is egész szám lesz.

2.1.7 Az $a \equiv b \pmod{m}$ kongruencia felhasználásával lássuk be, hogy az $(a^m - b^m)/(a - b) = a^{m-1} + a^{m-2}b + \dots + b^{m-1}$ kifejezés is osztható m-mel.

2.1.8 Mutassuk meg, hogy $a \equiv b \pmod{3}$, majd ennek felhasználásával lássuk be, hogy $(a^n - b^n)/(a - b)$ relatív prím a 3-hoz.

2.1.9

b) A legegyszerűbb, ha k szerinti indukcióval bizonyítunk, felhasználva a)-t és az $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ azonosságot. — Egy másik lehetőség: a törtekkel kapcsolatos problémák elkerülése érdekében érdemes átszorozni a $k!$ nevezővel; mivel $(k!, p) = 1$, ezért így a bizonyítandóval *ekvivalens* kongruenciához jutunk, változatlan modulus mellett. A „törtmentes" alak a $p - j \equiv -j \pmod{p}$ kongruenciák összeszorzásával igazolható.

c) A b) résznél jelzett bármelyik módszer értelemszerű módosítása célhoz vezet.

2.1.10 Válasz: $p = 5$. — Útmutatás: Lássuk be, hogy $\binom{3p}{p} \equiv 3 \pmod{p}$.

2.1.11

a) A p-vel történő egyszerűsítés után a nevezőben $(p-1)!$ marad, ami relatív prím a p-hez, tehát a vele történő beszorzás ekvivalens kongruenciához vezet. Ez utóbbi helyességét az előző két feladat mintájára igazolhatjuk.

b)–c) Hasonló módszerrel bizonyíthatunk, mint az a) résznél.

2.2.

2.2.1 a) 3. b) 5. c) 2.
Útmutatás: A modulus relatív prím a megadott elemekhez, és osztója azok különbségének.

2.2.2 a) $6^2 \cdot 5^{m-2} \cdot m!$ b) $6 \cdot 5^{\varphi(m)-1} \cdot \varphi(m)!$
(Két maradékrendszert akkor is különbözőnek tekintettünk, ha csak az elemek sorrendjében különböznek.)

2.2.3 Mindkét tulajdonság csak a számtani sorozat differenciájától függ, jelöljük ezt d-vel.
a) $d \mid m$. b) $(d, m) = 1$.

2.2.4

a) m páratlan.
b) Minden m jó.
c) $m = 2$.
d) $(m, 10) = 1$.
e) $m = 2$.
f) $m = 3^k$.
g) m négyzetmentes.
(Az a) és d) kérdés a 2.2.3b feladat speciális esetének is tekinthető.)

2.2.5

a) $(m, 15) = 1$.
b) Minden m jó.
c) $m = 2$.
d) $(m, 20) \leq 2$.
e) Minden m jó. — Ez a 2.2.4g bizonyításában szereplő gondolatmenethez hasonlóan, de annál jóval egyszerűbben igazolható.

2.2.6 Igaz: b).

2.2.7

a) A maradék 0, ha m páratlan, és $m/2$, ha m páros. — Útmutatás: Lássuk be, hogy a maradék nem függ attól, hogy melyik teljes maradékrendszert választottuk, ezután vizsgáljuk meg például a legkisebb nemnegatív vagy a legkisebb abszolút értékű maradékok rendszerét. — Egy másik lehetőség: állítsuk ügyesen párba a teljes maradékrendszer elemeit.

b) Használjuk fel az a) részt. — Páratlan m esetén mindig tudunk példát mutatni arra is, hogy az $a_i + b_i$ elemek teljes maradékrendszert alkotnak, és arra is, hogy nem alkotnak teljes maradékrendszert.

c) Egy redukált maradékrendszer elemeinek az összege 0 maradékot ad, ha $m > 2$. — Az $a_i + b_i$ összegekre ugyanaz a válasz, mint teljes maradékrendszer esetén.

2.2.8 a) m páratlan vagy osztható 4-gyel. b) m páratlan.

2.2.9

a) $m = 2^k$. — Útmutatás: Pontosan akkor kapunk teljes maradékrendszert, ha a megadott számok páronként inkongruensek, azaz $(i+1)+(i+2)+\ldots+j = (i+j+1)(j-i)/2$ semmilyen $0 \le i < j \le m-1$ esetén sem lehet osztható m-mel. Ha $m = 2^k$, akkor a két tényező ellentétes paritását kihasználva lássuk be, hogy ilyen oszthatóság sohasem áll fenn. Ha viszont az m nem kettőhatvány, azaz $m = 2^k(2s+1)$, ahol $s > 0$ (a k kitevő lehet 0 is), akkor $(2^k - s) + (2^k - s + 1) + \ldots + (2^k + s)$ osztható (sőt egyenlő) m-mel. Itt a legnagyobb tagra biztosan teljesül az előírt $2^k + s < m$ feltétel, azonban a legkisebb tagnál $2^k - s \le 0$ előfordulhat. Ebben az esetben az előző összeg tagjai közül hagyjuk el az összes negatívat, a (-1)-szereseiket és a 0-t; ekkor már egy, a megfelelő határok közé eső, és továbbra is m-mel osztható „tiltott” összeget kapunk.

b) m páros.

2.2.10 Igaz: a), c), e).

Útmutatás c)-hez és e)-hez: Mutassuk meg, hogy mindkét állítás következik az alábbiból:

Ha $(r,k) = 1$, akkor létezik olyan s, hogy $s \equiv r \pmod{k}$ és $(s,m) = 1$.

Ennek igazolása: Ha az m minden prímosztója osztója a k-nak is, akkor $(r,k) = 1 \Rightarrow (r,m) = 1$, és ekkor $s = r$ megfelel. Egyébként legyenek $q_1, \ldots, q_t$ az m olyan prímosztói, amelyek nem osztói a k-nak, és tegyük fel, hogy ezek közül éppen $q_1, \ldots, q_j$ osztója az r-nek ($j = 0$ és $j = t$ is lehetséges). Ekkor $s = r + q_{j+1} \ldots q_t k$ megfelel.

2.2.11 b) Válasz: $m/(a,m)$.
Útmutatás: $ar_i + b \equiv ar_j + b \pmod m \iff r_i \equiv r_j \pmod{m/(a,m)}$.

2.2.12
a) $(a,m) = 1$ vagy 2, ha $m = 4k+2$ alakú, és $(a,m) = 1$, egyébként.
b) $p_1 \cdot \ldots \cdot p_s \mid b$, ahol $p_1, \ldots, p_s$ az m összes különböző prímosztója.

2.2.13 $(k,m) = 1$.

2.2.14 c) Használjuk fel a b) részt.

2.3.

2.3.1 Állítsuk párba egy (ügyesen választott) redukált maradékrendszer elemeit, vagy használjuk $\varphi(n)$ képletét.

2.3.2
a) 3, 4, 6.
b) 5, 8, 10, 12.
c) Nincs ilyen n.
d) 61, 77, 93, 99, 122, 124, 154, 186, 198.

2.3.3
a) $1285 = 5 \cdot 257$. — Útmutatás: $\varphi(2^{11}) = 2^{10}$, ezért a keresett szám legfeljebb 2^{11}. Ennél kisebb megfelelő tulajdonságú számot csak $2^k + 1$ alakú prímek szorzata adhat.
b) 3^{11}. — Útmutatás: Használjuk fel, hogy (i) $2 \cdot 3^{10} + 1$ nem prím (osztható 17-tel), továbbá (ii) ha egy $p(>2)$ prímre $3^j \mid p-1$, akkor $p \geq 2 \cdot 3^j + 1$.

2.3.4 100, 80, 50, 40.

2.3.5
a) Használjuk fel k és n kanonikus alakját és a φ-függvény képletét. Vigyázzunk arra, hogy mindkét szám kanonikus alakjában csak pozitív kitevők szerepeljenek.
b) Következik az a) részből.
c) A legkevesebb számolással úgy érünk célhoz, ha a

$$\varphi\big((a,b)\big)\varphi\big([a,b]\big) = \big(\varphi(a),\varphi(b)\big)\big[\varphi(a),\varphi(b)\big]$$

azonosságot igazoljuk.

2.3.6 A $\varphi(a)/\varphi(b) = a/b$ egyenlőség átírható a következő alakba:

$$\prod_{\substack{p\mid a\\ p \text{ prím}}} \left(1 - \frac{1}{p}\right) = \prod_{\substack{q\mid b\\ q \text{ prím}}} \left(1 - \frac{1}{q}\right). \tag{1}$$

Ha a és b prímosztói megegyeznek, akkor (1) nyilván teljesül. A megfordítás igazolásához indirekt tegyük fel, hogy (1) valamely más esetben is teljesülne. Hagyjuk el a közös $1-1/p = 1-1/q$ tényezőket, majd szorozzuk be mindkét oldalt a közös nevezővel (azaz a megmaradt p-k és q-k szorzatával). Ekkor a p-k és q-k közül a legnagyobb csak az egyik oldalnak lesz osztója, ami ellentmondás.

2.3.7 Igaz: a).

2.3.8 Legyen a k kanonikus alakja $k = \prod_{i=1}^{r} p_i^{\beta_i}$, $\beta_i > 0$. Ekkor megfelel

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \text{ ahol } \alpha_i = \begin{cases} \beta_i, & \text{ha } p_i \mid \prod_{j=1}^{r}(p_j - 1); \\ \beta_i + 1, & \text{egyébként.} \end{cases}$$

2.3.9 Használjuk fel, hogy ha $r > 1$, akkor az $r \mid n$ és $(r, n) = 1$ feltételek kizárják egymást. — Egyenlőség akkor és csak akkor teljesül, ha $n = 1$, 4 vagy prím. — Útmutatás: Minden más esetben található olyan $1 < r < n$, amelyre $(r, n) > 1$, de $r \nmid n$; például $n - p$ megfelel, ahol p az n legkisebb prímosztója.

2.3.10

a), c) Használjuk $\varphi(n)$ képletét.

b) Ekkor az (1) táblázat oszlopai nem alkotnak teljes maradékrendszert modulo b.

2.3.11

a) Az n legkisebb prímosztójának a többszörösei biztosan nem relatív prímek az n-hez. — Egyenlőség akkor és csak akkor teljesül, ha n egy prímszám négyzete.

b) (b1) n prím. (b2) 10. (b3) 15, 49. (b4) Nincs ilyen n.

2.3.12 1, 2 és 3. — Útmutatás: Mutassuk meg, hogy $\varphi(n) \mid n \iff n = 2^\alpha 3^\beta$, ahol $\alpha \geq 0$ és $\beta = 0$, vagy $\alpha > 0$ és $\beta > 0$.

2.3.13 Bizonyítsunk indirekt; használjuk a φ-függvény képletét, ekkor az egyszerűsítések után megmaradó legnagyobb prímosztó csak az egyik oldalnak lesz osztója.

2.3.14 Egyszerűsítsük az $1/n, 2/n, \ldots, n/n$ törteket, és számoljuk össze, hogy egy adott nevező hányszor fordul elő.

2.3.15 A $\varphi(n)$ képletének felhasználásával lássuk be, hogy $\varphi(n) \geq \sqrt{n}/2$.
Egy másik lehetőség: az n prímosztóin kívül minden prímszám relatív prím az n-hez, és n-ig „sok” prímszám van (lásd az 5.4 pontot).

2.3.16 Jelölje $2 = p_1 < p_2 < \ldots$ a (pozitív) prímszámok sorozatát, és legyen p_j a legkisebb olyan prím, amely *nem* osztója a k-nak. Ekkor $n = (p_j - 1)k$ megfelel.

2.3.17 Legyen $2 = p_1 < p_2 < \ldots < p_{1000}$ az első 1000 prímszám, és jelölje P ezek szorzatát. Ekkor az $n_i = P(p_i - 1)/p_i$ számok megfelelnek.

2.3.18 Válasz: $n \leq 3$. — Útmutatás: Hasonlítsuk össze a 2 kitevőjét $\varphi(n!)$ és $k!$ kanonikus alakjában.

2.3.19 $m = 2^k$ vagy p vagy $2p$, ahol $p > 2$ prím.

2.4.

2.4.1 Használjuk fel, hogy $\varphi(n) \leq n$ miatt $\varphi(n) \mid n!$. — A feladatot megoldhatjuk az Euler–Fermat-tétel nélkül is. Az $1, 2, 2^2, \ldots, 2^n$ számok között a skatulyaelv alapján található két olyan, amelyek kongruensek modulo n: $2^i \equiv 2^j \pmod{n}$, ahol $0 \leq i < j \leq n$. Mivel $(2, n) = 1$, ezért 2^i-vel egyszerűsíthetünk, és így $2^{j-i} \equiv 1 \pmod{n}$, ahol $1 \leq j - i \leq n$. Innen $j - i \mid n!$ alapján következik a feladat állítása.

2.4.2 Válasz: 49.
Útmutatás: $(1793, 10^2) = 1$ miatt $1793^{k\varphi(100)} \equiv 1 \pmod{100}$. Számítsuk ki $\varphi(100)$-at és használjuk fel, hogy $1793 \equiv -7 \pmod{100}$.

2.4.3 alkalmazzuk (többször) a kis Fermat-tételt $p = 13$-ra.

2.4.4 Lássuk be, hogy a két szám közül az egyik osztható 7-tel.

2.4.5 Határozzuk meg az osztó kanonikus alakját, és minden prímhatványtényezőre külön igazoljuk az oszthatóságot az Euler–Fermat-tétel felhasználásával. Ne felejtsük el azokat az eseteket is megvizsgálni, amikor ez a prímhatvány az a-hoz nem relatív prím.

2.4.6 Lássuk be, hogy egy 30-adik hatvány csak 0 vagy 1 maradékot adhat 11-gyel, illetve 9-cel osztva.

2.4.7 Mutassuk meg, hogy egy 88-adik hatvány csak 0 vagy 1 maradékot adhat 23-mal osztva.

2.4.8 Ha r_i és r_j egyike sem kongruens 0-val mod p, akkor az $r_i^{2p-3} \equiv r_j^{2p-3} \pmod{p}$ kongruenciát $r_i r_j$-vel beszorozva, a kis Fermat-tétel felhasználásával $r_i \equiv r_j \pmod{p}$, azaz $i = j$ következik.

2.4.9

a) A 2.4.1B Tétel bizonyításának a mintájára válasszuk külön a $p \nmid a$ és $p \mid a$ eseteket.

b) Jelölje k az m kanonikus alakjában előforduló *kitevők* maximumát. Ekkor $i, j \geq k$, $i \equiv j \pmod{\varphi(m)} \Longrightarrow a^i \equiv a^j \pmod{m}$. — Útmutatás: Lássuk be, hogy az m kanonikus alakjában szereplő minden egyes p^α prímhatványtényezőre $a^i \equiv a^j \pmod{p^\alpha}$. Ehhez használjuk fel, hogy $\varphi(p^\alpha) \mid \varphi(m)$ (lásd a 2.3.5a feladatot).

2.4.10 Igaz: a), c).

a) Használjuk az Euler–Fermat-tételt ($a = 133$, $m = 1000$), vagy alkalmazzuk a 2.4.1 feladatnál vázolt módszer megfelelő módosítását.

b) Vizsgáljuk a 4-gyel való oszthatóságot.

c) Induljunk ki a $136^k \equiv 136 \pmod{1000} \iff 136^{k-1} \equiv 1 \pmod{125}$ összefüggésből.

2.4.11 Útmutatás: $a^k \equiv a \pmod{d} \iff a^{k-1} \equiv 1 \pmod{d/(a,d)}$.

2.4.12 A csupaegyek a $(10^k - 1)/9$ alakú számok, tehát azokat az m-eket kell meghatározni, amelyekre $10^k \equiv 1 \pmod{9m}$ teljesül alkalmas (pozitív) k-val.

2.4.13 Elég azt megmutatni, hogy $n^2 + 1$-nek bármely p páratlan, pozitív *prím*osztója $4k+1$ alakú. Ennek belátásához az $n^2 \equiv -1 \pmod{p}$ kongruenciát emeljük $(p-1)/2$-edik hatványra, és használjuk a kis Fermat-tételt.

A feladatot megoldhatjuk a kis Fermat-tétel nélkül is. Tegyük fel indirekt, hogy létezne egy $4k-1$ alakú a pozitív egész és egy olyan n, amelyre $a \mid n^2 + 1$. Vegyük a legkisebb ilyen a-t. Az ellentmondást úgy fogjuk kihozni, hogy találunk egy a-nál kisebb b pozitív egészt, amely szintén $4k-1$ alakú és osztója egy $s^2 + 1$ alakú számnak.

Mivel az $a \mid n^2 + 1$ oszthatóság csak az n-nek az a-val vett osztási maradékától függ, ezért feltehető, hogy $0 \leq n \leq a - 1$ (sőt azt is előírhatnánk, hogy $|n| \leq a/2$ teljesüljön).

Legyen $n^2 + 1 = aq$. Ekkor $aq = n^2 + 1 \leq (a-1)^2 + 1 < a^2$, tehát $(0 <)q < a$.

Ha n páros, akkor az $n^2 + 1$ szám $4k + 1$ alakú, és így a q szám $4k - 1$ alakú.

Ha n páratlan, akkor az $n^2 + 1$ szám $8k + 2 = 2(4k + 1)$ alakú, és így a $q/2$ szám $4k - 1$ alakú.

Azt kaptuk, hogy az a-nál kisebb q, illetve $q/2$ pozitív szám is osztója $n^2 + 1$-nek, ami ellentmondás.

2.4.14 A kis Fermat-tétel alapján $n^{40} \equiv n^4 \pmod{19}$, így a feltétel $a^4 \equiv -b^4 \pmod{19}$ alakba írható. Ezt a kongruenciát emeljük 9-edik hatványra.

2.4.15 Az a) és b) állításból az $m = p$ speciális esetben éppen a kis Fermat-tétel második alakját kapjuk. A c) állítás azt mutatja, hogy van olyan *összetett*

m is, amelynél $a^m \equiv a \pmod{m}$ teljesül minden a-ra. (Az ilyen összetett számokat *univerzális álprím*eknek vagy *Carmichael-szám*oknak hívjuk, és ezekkel részletesebben az 5.7 pontban foglalkozunk.) — Útmutatások:

a) Négyzetmentes m esetén az m minden p prímosztójára lássuk be, hogy $a^{\varphi(m)+1} \equiv a \pmod{p}$. Ha az m nem négyzetmentes, azaz osztható egy p prímszám négyzetével, akkor például $a = p$-re nem teljesül a szóban forgó kongruencia.

b) Használjuk fel a 2.4.9b feladat eredményét.

c) Vizsgáljuk az $a^{1729} \equiv a \pmod{k}$ kongruenciákat, ahol k az 1729 egy tetszőleges prím(hatvány)osztója.

2.4.16 2.4.1B: Nyilván elegendő $a^p \equiv a \pmod{p}$ teljesülését egy teljes maradékrendszer elemeire, azaz például $a = 1, 2, \ldots, p$-re belátni. Tegyük fel, hogy a kongruencia valamely $a = k$-ra teljesül, ekkor $(k+1)^p$-t a binomiális tétel szerint kifejtve kapjuk, hogy a kongruencia $a = k+1$-re is érvényes. 2.4.1A: Legyen $(a, p) = 1$. Ekkor az (imént igazolt) $a^p \equiv a \pmod{p}$ kongruenciát szabad a-val egyszerűsíteni, azaz $a^{p-1} \equiv 1 \pmod{p}$ is fennáll.

2.5.

2.5.2

a) $x \equiv 11, 28, 45 \pmod{51}$.

b) $x \equiv 9, 38, 67, 96 \pmod{116}$.

c) $x \equiv 1011 + 11111k \pmod{55555}$, $0 \le k \le 4$.

d) $x \equiv (2^{k+3} + 4)/3 \pmod{2^{k+2} + 1}$, ha k páros, és nincs megoldás, ha k páratlan.

e) $x \equiv 0, 11 \pmod{19}$.
Útmutatás: A kis Fermat-tétel alapján az $x(8x + 7) \equiv 0 \pmod{19}$ kongruenciához jutunk. Ezután ismét használjuk fel, hogy a 19 prím.

f) $x \equiv 79 \pmod{100}$. — Útmutatás: Mivel $(27, 1000) = 1$, ezért csak olyan megoldás jöhet szóba, amely relatív prím a 100-hoz. Így használhatjuk az Euler–Fermat-tételt.

2.5.3 A $13x \equiv 31 \pmod{49}$ kongruenciából 25 és 74 adódik.

2.5.4 Válasz: 67.
Útmutatás: Az Euler–Fermat-tételből $3^{280} \equiv 1 \pmod{100}$, így a $3x \equiv 1 \pmod{100}$ kongruenciát kell megoldani.

2.5.5 Elégséges: a), c), f).

2.5.6 Igaz: a), b).

2.5.7 m.

2.6.

2.6.1
a) 93.
b) Az $x \equiv 4 \pmod{12}$, $x \equiv 8 \pmod{15}$ kongruenciarendszer nem oldható meg.

2.6.2 a) Akármi lehet. b) 3 vagy 7.

2.6.3 alkalmazzuk a P1 példánál bemutatott eljárást: Alakítsuk át mindegyik kongruenciát olyan szimultán kongruenciarendszerré, amelyben a modulusok az eredeti modulus kanonikus alakjában szereplő prímhatványok. Ne felejtsük el, hogy az egyes prímhatvány modulusú kongruenciák vizsgálata során általában két esetet érdemes megkülönböztetni aszerint, hogy a keresett x megoldás relatív prím-e a modulushoz, vagy sem. — Eredmények:
a) $x \equiv 20 \pmod{176}$.
b) $x \equiv 60 \pmod{333}$ és $x \equiv 208 \pmod{333}$.
c) $x \equiv 91 \pmod{105}$.

2.6.4 a) 1. b) 2.

2.6.5 A kérdéses modulo 1000 kongruencia helyett vizsgáljuk a modulo 125 és modulo 8 adódó szimultán kongruenciarendszert. — Válasz: 016.

2.6.6 1166.

2.6.7 a) 25, 76. b) 376, 625.

2.6.8
a) Válasz: 36. — Útmutatás: Az $x^2 \equiv x \pmod{10^{20}}$ kongruencia helyett vizsgáljuk a megfelelő prímhatvány modulusok szerinti szimultán kongruenciarendszert. Mutassuk meg, hogy egy prímhatvány modulusra nézve az $x(x-1) \equiv 0$ kongruencia megoldásszáma 2.
b) Válasz: 135. — Útmutatás: Határozzuk meg az $x^3 \equiv x \pmod{10^{20}}$ kongruencia megoldásszámát az a)-beli eljáráshoz hasonló módon.

2.6.9 Mivel egy napban $24 \cdot 60 = 1440$ perc van, tehát az $x \equiv 39^{38^{37}} \pmod{1440}$ kongruenciát kell vizsgálnunk. $1440 = 2^5 \cdot 3^2 \cdot 5$ alapján ehelyett a 2^5, 3^2 és 5 modulusokra nézzük a kongruenciát. — Válasz: 13 óra 21 perc.

2.6.10 A 2.2.14b-c feladat megoldásához hasonlóan járhatunk el.

2.6.11 Legyenek $p_1, \ldots, p_K$ különböző prímszámok, és tekintsük az $x + i \equiv 0 \pmod{p_i^2}$, $i = 1, 2, \ldots, K$ szimultán kongruenciarendszert.

2.6.12

a) Egy-egy megoldás $x = a + b + c$, illetve $x = ab + bc + ca$.

b) *Szükségesség*: alkalmazzuk a 2.6.1 Tételt a két kongruenciából álló részrendszerekre. — *Elégségesség*: Legyen $a = da_1$, $b = db_1$, $c = dc_1$, ahol a_1, b_1 és c_1 páronként relatív prímek, és $x = dx_1$. Osszuk el valamennyi kongruenciát d-vel (a modulusokat is beleértve). Az így kapott szimultán kongruenciarendszerben x_1 az ismeretlen és a_1, b_1 és c_1 a modulusok. Mivel a modulusok páronként relatív prímek, ezért ez a kongruenciarendszer megoldható, és így megoldható az eredeti rendszer is.

2.6.13 *Szükségesség*: alkalmazzuk a 2.6.1 Tételt a két kongruenciából álló részrendszerekre. — *Elégségesség*: Bizonyítsunk k szerinti teljes indukcióval. A $k-1$-re vonatkozó indukciós feltevés szerint az első $k-1$ kongruenciából álló részrendszer megoldható, legyen c egy megoldás. Ekkor elég az

$$x \equiv c \pmod{[m_1, \ldots, m_{k-1}]}, \qquad x \equiv c_k \pmod{m_k}$$

kongruenciarendszer megoldhatóságát igazolni. A 2.6.1 Tétel kritériumának az ellenőrzéséhez használjuk fel az 1.6.19b feladat több tagra vonatkozó általánosítását, valamint $1 \le i \le k-1$-re az $(m_k, m_i) \mid c_k - c_i$ és $m_i \mid c_i - c$ feltételek teljesülését.

2.6.14 Nincs. — Útmutatás: A kongruencia megoldásszáma megegyezik a prím-(hatvány)tényezők szerinti szimultán kongruenciarendszerben szereplő kongruenciák megoldásszámainak a szorzatával.

2.6.15

a) *Szükségesség*: A rendszer elemszáma $\varphi(k) = n$. A $0 \pmod n$ előállításához használt c számra $n \mid c$, továbbá $(c, k) = 1$, ezért $(k, n) = 1$.
Elégségesség: Legyen $r_1, \ldots, r_n$ tetszőleges teljes maradékrendszer modulo n, $s_1, \ldots, s_n$ tetszőleges redukált maradékrendszer modulo k (a feltétel szerint $\varphi(k) = n$). Ekkor $(k, n) = 1$ miatt az

$$x \equiv r_i \pmod{n}, \quad x \equiv s_i \pmod{k}, \quad i = 1, 2, \ldots, n$$

szimultán kongruenciarendszerek megoldhatók, és ezek egy-egy megoldása a kívánt tulajdonságú számhalmazt szolgáltat.

b) A szükségesség nyilvánvaló. Az elégségesség bizonyítása $(k, n) = 1$ esetén az a) rész mintájára történhet, az általános esetben azonban úgy kell a két redukált maradékrendszer elemeit összepárosítani, hogy az így

létrejövő szimultán kongruenciarendszerek megoldhatók legyenek. Annak igazolásához, hogy az ilyen párosítás tényleg megvalósítható, a következő állítást kell belátni: ha $d \mid n$, akkor egy modulo n redukált maradékrendszer elemeiből *minden* modulo d redukált maradékosztályba ugyanannyi elem esik.

2.6.16

a) Először mutassuk meg, hogy bármely n-re és $i \neq j$-re $(a_i + n, a_j + n)$ csak az $S = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3)$ osztói közül kerülhet ki. Legyen ezután p az S tetszőleges prímosztója, és válasszuk meg n-et modulo p úgy, hogy az $a_i + n$ számok közül legfeljebb egy legyen osztható p-vel ($p > 3$-ra akár az is elérhető, hogy $a_1 + n$, $a_2 + n$ és $a_3 + n$ egyike se legyen osztható p-vel). Az S különböző prímosztóira így adódó kongruenciák egy szimultán kongruenciarendszert alkotnak, amely a modulusok páronként relatív prím volta miatt biztosan megoldható.

b) Például $1, 2, 3, 4$ megfelel.

c) Finomítsuk az a)-beli eljárást úgy, hogy az $S = \prod_{1 \leq i < j \leq 4}(a_i - a_j)$ szorzat páratlan prímosztóit és a 4-et tekintjük modulusoknak.

d) Most olyan n-et kell választani, hogy az S bármely p prímosztójával az $a_i + n$ számok közül legfeljebb kettő legyen osztható.

e) Öt szám esetén mindkét állítás igaz, hat számra viszont már mindkettő hamis.

2.7.

2.7.1

a) Válasz: 2, ha $m = 4$, és 0, ha $m > 4$. — Útmutatás: Ha m felírható két különböző, 1-nél nagyobb egész szám szorzataként, akkor ezek mindketten szerepelnek tényezőként $(m-1)!$-ban, tehát $m \mid (m-1)!$. Hátravan még az $m = p^2$ eset, ahol p prím. Ha $p > 2$, akkor p és $2p$ is szerepel tényezőként $(m-1)!$-ban.

b) Válasz: 2, ha $m = 4$; $p - 1$, ha $m = 2p$, ahol $p > 2$ prím, és 0 egyébként. — Útmutatás: Először lássuk be, hogy ha $m = p^\alpha t$, ahol $p \nmid t$ és $t > 2$, akkor $\varphi(m) \geq p^\alpha$. Ebből következik, hogy az $m = 2^\alpha$, p^α és $2p^\alpha$ (ahol $p > 2$ prím) esetek kivételével a keresett maradék 0. Ha $m = p^\alpha$ vagy $2p^\alpha$, ahol $\alpha \geq 2$, akkor a $\big(\varphi(m)\big)!$ szorzatban $p^{\alpha-1}$ és $2p^{\alpha-1}$ is szerepel, ezért $m \mid \big(\varphi(m)\big)!$. Hasonlóan, ha $m = 2^\alpha$, ahol $\alpha \geq 3$, akkor $2^{\alpha-1}$ és 2 is szerepel tényezőként $\big(\varphi(m)\big)!$-ben. Végül az $m = 2p$ esetben a $\big(\varphi(m)\big)! = (p-1)!$ szorzat maradékát vizsgáljuk külön modulo p és modulo 2.

c) Válasz: -1, ha $m = 4$, p^α vagy $2p^\alpha$, ahol $p > 2$ prím, és 1 egyébként. — Útmutatás: A Wilson-tételre adott párba állításos bizonyítás módosításánál a fő nehézséget az jelenti, hogy (a legtöbb) összetett m esetén $c^2 \equiv 1 \pmod m$ nem csak $c \equiv \pm 1 \pmod m$ esetén teljesül. A párba állításnál a redukált maradékrendszer azon c elemei okoznak problémát, amelyeknek „önmaga a párja", azaz $c^2 \equiv 1 \pmod m$. Jelöljük ezek halmazát H-val. Ekkor a keresett r maradék megegyezik a H-beli elemek szorzatának a maradékával. Ha $m = 4$, p^α vagy $2p^\alpha$, akkor H-ban csak $c \equiv \pm 1 \pmod m$ szerepel, és így $r \equiv -1 \pmod m$. A többi esetben a kínai maradéktétel segítségével lássuk be, hogy H-nak több, mint két eleme van. Legyen $d \not\equiv 1 \pmod m$ a H tetszőleges eleme, és állítsuk párba (csak) H elemeit a $c \mapsto cd \pmod m$ megfeleltetéssel. Innen $r \equiv d$ vagy $1 \pmod m$ adódik. A H-beli párba állítást most egy másik $d' \not\equiv 1 \pmod m$ elem szerint elvégezve kapjuk, hogy csak $r \equiv 1 \pmod m$ lehetséges.

2.7.2 Válasz: 7 és 17. — Útmutatás: Ha m prím, akkor használjuk fel a Wilson-tételt. Ha m összetett és $m - 6 \geq m/2$, akkor $(m-6)!$ nem lehet relatív prím az m-hez.

2.7.3 Azt kell igazolni, hogy az $a_1b_1, \ldots, a_mb_m$ szorzatok nem alkotnak teljes maradékrendszert modulo m.

a) Legyen m prím, $m = p$. Ha a $p = a_i = b_j$ előállításnál $i \neq j$, akkor $a_ib_i \equiv a_jb_j \equiv 0 \pmod p$. Ha $p = a_i = b_i$, akkor a többi a_j elem, illetve a többi b_j elem redukált maradékrendszert alkot modulo p, és megmutatjuk, hogy az a_jb_j szorzatok viszont nem alkotnak azt. A Wilson-tétel alapján

$$\prod_{j\neq i} a_jb_j \equiv \prod_{j\neq i} a_j \prod_{j\neq i} b_j \equiv (-1)(-1) = 1 \not\equiv -1 \pmod p\,,$$

tehát az a_jb_j $(j \neq i)$ szorzatok nem alkothatnak redukált maradékrendszert modulo p.

b) Először mutassuk meg, hogy ha $k \mid m$, akkor a k-val osztható a-kat és b-ket eleve „egymással kell összeszorozni". Ha m nem négyzetmentes, azaz van olyan p prím, amelyre $p^2 \mid m$, akkor az előző észrevétel alapján bármely a_ib_i szorzat vagy relatív prím a p-hez, vagy pedig osztható p^2-tel, tehát például a $(p)_m$ maradékosztály nem lesz reprezentálva. Ha m négyzetmentes, és p az m egy páratlan prímosztója, akkor lássuk be, hogy az m/p-vel osztható a és b elemek egy-egy teljes maradékrendszert alkotnak modulo p, és vezessük vissza a feladatot az a) részre.

2.7.4 A $(p-1)! \equiv -1 \pmod p$ kongruenciában a $p - c > (p-1)/2$ tényezők helyére írjunk $-c$-t, majd a „négyzetgyökvonásnál" használjuk ki p prím tulajdonságát.

2.7.5 A $(p^2-1)!$-ból p^{p-1}-et kiemelve $p+1$ darab modulo p redukált maradékrendszer szorzata marad (a $p+1$-edik a p-vel osztható számok együtthatóiból keletkezik).

2.7.6 $(p-3)/2$.

2.7.7 Válasz: 10000. — Útmutatás: Vizsgáljuk külön a maradékot modulo 101 és modulo 100, majd oldjuk meg a kapott szimultán kongruenciarendszert.

2.7.8 Válasz: 3, 4, 5, 9. — Útmutatás: Először „ejtsük ki a faktoriálist": az első szám alkalmas többszörösét a másodikból levonva kapjuk, hogy a keresett d legnagyobb közös osztó osztója $3n(n+3)$-nak. Ennek alapján mutassuk meg, hogy ha $n \geq 4$, akkor $d = 3$. Használjuk fel, hogy $(n+2)!$ maradéka 0 vagy -1 modulo $n+3$.

2.7.9 Mindkét kérdésre $m \leq 3$ a válasz. — Útmutatás: Nyilván elég megmutatni, hogy $m > 3$-ra nem létezik ilyen alakú *redukált* maradékrendszer. Ha $m = p > 3$ prím, akkor csak $1!, 2!, \ldots, (p-1)!$ jöhetne szóba, de a Wilson-tétel alapján $(p-2)! \equiv 1!$. Ha m összetett és p a legkisebb prímosztója, akkor egyrészt $p \leq k$ esetén $(k!, m) \neq 1$, másrészt egyszerűen igazolható, hogy $p \leq \varphi(m)$, tehát a faktoriálisok között csak $\varphi(m)$-nél kevesebb olyan van, amely relatív prím az m-hez.

2.7.10 A 31-gyel való oszthatóságot nem befolyásolja, ha az összeget a 31-hez relatív prím $(a_1a_2a_3)^{27}$ számmal beszorozzuk. Ezután használjuk fel a Wilson- és a kis Fermat-tételt.

2.7.11 Válasz: $0, \pm 1$. — Útmutatás: Lássuk be, hogy ha a számtani sorozat egyik eleme sem osztható p-vel, akkor az elemek vagy redukált maradékrendszert alkotnak modulo p, vagy pedig mind azonos maradékot adnak p-vel osztva. Ennek megfelelően használjuk fel a Wilson-, illetve a kis Fermat-tételt.

2.7.12 Válasz: $x = 1$, $z = 2$. — Útmutatás: Az $x!$-ban minden $1 \leq i \leq x-1$ tényező helyére írjuk a vele kongruens $-(z-i)$ számot, ekkor

$$x!(z-x)! \equiv (-1)^{x-1}x(z-1)! \pmod{z}$$

adódik. Ezután használjuk fel a Wilson-tételt, illetve a 2.7.1a feladatot.

2.7.13 Válasz: $p \leq 5$. — Útmutatás: Tegyük fel indirekt, hogy egy $p > 5$ prímre $(p-1)! + 1 = p^k$ teljesül. Ezt átalakítva a

$$(p-2)! = \frac{p^k - 1}{p-1} = p^{k-1} + p^{k-2} + \ldots + 1 \tag{1}$$

egyenlőséget nyerjük. Vizsgáljuk (1)-et modulo $(p-1)$: a 2.7.1a feladat, illetve $p \equiv 1 \pmod{p-1}$ alapján $0 \equiv k \pmod{p-1}$ adódik. Innen azt

kapjuk, hogy $k \geq p-1$, azonban ekkor $p^k \geq p^{p-1} > (p-1)! + 1$, ami ellentmondás.

2.8.

2.8.1 Páros m-ek esetén.

2.8.2

a) A $13x \equiv 1 \pmod{100}$ kongruenciát kell megoldani. — Válasz: (77).

b) $100 - \varphi(100) - 1 = 59$.

c) 19.

d) Van.

2.8.3 Válaszok:

a) 2. b) 4. c) 8.

d) Legyen $m = 2^\alpha t$, ahol t páratlan, és jelölje t különböző prímosztóinak a számát k. Ekkor a keresett érték 2^k, ha $\alpha \leq 1$; 2^{k+1}, ha $\alpha = 2$; és 2^{k+2}, ha $\alpha \geq 3$.

Útmutatás: Az $x^2 \equiv 1 \pmod{m}$ kongruencia megoldásszámát kell meghatározni. Vizsgáljuk először azt a speciális esetet, amikor m egy páratlan prím hatványa, illetve kettőhatvány, majd általános m esetén térjünk át az m kanonikus alakjában szereplő prímhatvány tényezők szerinti szimultán kongruenciarendszerre.

2.8.4

a)–b) Használjuk a nullosztó definícióját vagy a 2.8.5 Tételt.

c) Ezek az m-ek a prímhatványok.

d) Az összeg (0), ha m páratlan, és $(m/2)$, ha m páros. A szorzat (2), ha $m = 4$, és (0), ha $m > 4$.

e) Pontosan a *nem* négyzetmentes számok ilyenek, azaz amelyek legalább egy prímszám négyzetével oszthatók.

2.8.5

a) Először be kell látni, hogy a műveletek „jól vannak definiálva”, azaz két ilyen maradékosztály összege és szorzata megint ilyen típusú maradékosztály. A műveleti azonosságok az összes modulo 20 maradékosztály körében érvényesek, tehát a H részhalmazon is „automatikusan” teljesülnek. Nullelem a $(0)_{20}$, a $(4s)_{20}$ ellentettje a $(-4s)_{20} = (20 - 4s)_{20}$. Egységelem a $(16)_{20}$, a $(16)_{20}$ és a $(4)_{20}$ inverze önmaga, a $(8)_{20}$ és a $(12)_{20}$ pedig egymás inverzei.

b) Bármely $(a) \in K$-ra $(a)_{40}(20)_{40} = (0)_{40}$, tehát valóban minden elem nullosztó. Ebből következik, hogy nem létezhet egységelem, és K nem lehet test. (Az, hogy K kommutatív gyűrű, az a) részhez hasonlóan igazolható.)

c) Legyen $1 < k < m$ és $k \mid m$.
   (i) Ekkor a modulo m maradékosztályok közül a „k-val oszthatók” a maradékosztályok közötti összeadásra és szorzásra egy R kommutatív gyűrűt alkotnak.
   (ii) Ha $(k, m/k) = 1$, akkor ez az R gyűrű egységelemes.
   (iii) Ha $(k, m/k) = 1$ és m/k prím, akkor R test.
   (iv) Ha $(k, m/k) \neq 1$, akkor R minden nemnulla eleme nullosztó, és így már egységelem sem létezik.

2.8.6 Csak a köbre emeléssel nincs semmi probléma. Részletesen az alábbiakat mondhatjuk:
a) Lnko: a jobb oldalon álló maradékosztály általában függ attól, hogy az $(a)_m$ és $(b)_m$ maradékosztályból melyik reprezentánst választottuk.
b) Köbre emelés: értelmes a definíció.
c) Köbgyökvonás: a jobb oldalon álló maradékosztály általában függ attól, hogy az $(a)_m$ maradékosztályból melyik reprezentánst választottuk, sőt további problémát jelent, hogy egy adott maradékosztálynál már az is függhet a reprezentáns választásától, hogy $\sqrt[3]{a}$ egyáltalán egész szám-e.
d) Számtani közép: hasonló a helyzet, mint c)-nél. — Ha finomabb vizsgálatot akarunk végezni, akkor érdemes a páros és páratlan m esetét megkülönböztetni. Ha m páratlan és a két maradékosztályból olyan reprezentánsokat veszünk, amelyekre $(a+b)/2$ egész szám (ilyen reprezentánsok mindig vannak), akkor ez egyértelműen meghatározza az $\big((a+b)/2\big)_m$ maradékosztályt, tehát ily módon (kissé erőltetetten) értelmezhetjük bármely két maradékosztály számtani közepét. Ha m páros, akkor a két maradékosztály bármely két reprezentánsára egyformán igaz, hogy $(a+b)/2$ egész szám-e vagy sem, azonban $\big((a+b)/2\big)_m$ az első esetben sem lesz egyértelmű. Ez azt jelenti, hogy páros m esetén sehogyan sem tudjuk két maradékosztály számtani közepét a fenti módon értelmezni.
e) Hatványozás: a jobb oldalon álló maradékosztály általában függ attól, hogy a $(b)_m$ maradékosztályból melyik reprezentánst választottuk.

2.8.7 Kövessük — értelemszerű módosításokkal — a 2.4.1 Tételre adott bizonyítás gondolatmenetét. Legyen G összes eleme $g_1, \dots, g_k$. Először mutassuk meg, hogy ekkor $ag_1, \dots, ag_k$ is kiadja a csoport összes elemét. Ebből következik, hogy $(ag_1)(ag_2)\dots(ag_k) = g_1 g_2 \dots g_k$. Ezt az egyenlőséget $g_1 g_2 \dots g_k$ inverzével beszorozva a feladat állítását kapjuk.

2.8.8 A Wilson-tétel bizonyításának a mintájára párosítsunk minden elemet az inverzével. Ebből azonnal következik az állítás, ha (e-vel együtt) legfeljebb két olyan elem van, amelynek a négyzete az egységelem. Ha kettőnél több ilyen elem van, akkor ezek körében csináljunk egy másféle párosítást.

3. Magasabb fokú kongruenciák

3.1.

3.1.1 a) 2. b) 4. c) 0. d) 60.

3.1.2 alkalmazzuk a $\mathbf{Z}_m$ gyűrűre azt a tételt, hogy egy (kommutatív) gyűrű feletti polinom akkor és csak akkor osztható $x-\alpha$-val, ha a megfelelő polinomfüggvénynek az α gyöke.

3.1.3 Csak c) igaz.

3.1.4 a) Pl. $f=x^2(x-1)\dots(x-11)$. b) $37\cdot 36\cdot\binom{36}{11}$.

3.1.5 Ha i megoldás, akkor $f(i)^{p-1}\equiv 0 \pmod p$, ha pedig nem megoldás, akkor a kis Fermat-tétel miatt $f(i)^{p-1}\equiv 1 \pmod p$.

3.1.6 Használjuk fel a Wilson-tételre ebben a pontban adott bizonyítást: a keresett szorzat $(-1)^{j+1}a_{p-1-j}$, ahol a_{p-1-j} a bizonyításban szereplő f polinom megfelelő együtthatója.

3.1.7 Írjunk f-ben x^{p-1} helyére mindaddig 1-et, amíg ez csak lehetséges.

3.1.8 Kezeljük a kérdést a $\mathbf{Z}_p$ test feletti polinomok körében. Itt az f polinomhoz tartozó polinomfüggvénynek p helyettesítési értéke van. A Lagrange- vagy Newton-féle interpoláció egy olyan g polinom létezését garantálja, amelynek a foka legfeljebb $p-1$ vagy g a nullpolinom, és a g-hez tartozó polinomfüggvény az adott helyeken az előre megadott értékeket veszi fel, vagyis jelen esetben minden helyettesítési értéke ugyanaz, mint az f-hez tartozó megfelelő helyettesítési érték. — Az interpolációs polinom előállítására többféle eljárás ismert, azonban mindenképpen szükség van hozzá az f összes helyettesítési értékére, tehát eleve ismernünk kell magukat a gyököket és így a megoldásszámot is. Ennek megfelelően az interpolációs polinom nem használható a megoldásszám megkereséséhez.

3.1.9 Tegyük fel, hogy a g_1 és g_2 polinom is megfelel, és tekintsük a $h=g_1-g_2$ polinomot. A feltételek alapján a h modulo p vett foka legfeljebb $p-1$ lehet, ugyanakkor a $h(x)\equiv 0 \pmod p$ kongruenciának minden c megoldása, azaz a megoldásszám p. Az ellentmondás csak úgy oldható fel, hogy h-nak modulo p nincs foka, azaz h minden együtthatója osztható p-vel.

3.1.10 A 3.1.3 Tételre adott első bizonyítást módosítsuk a 2.4.15b feladat felhasználásával.

3.2.

3.2.1 a) 1. b) 2. c) 12.
d) 46. (Azt, hogy nem 23 a rend, minden számolás nélkül is megmutathatjuk $43 \equiv -2^2 \pmod{47}$ és a kis Fermat-tétel felhasználásával.)

3.2.2 Csak a c) esetben van ilyen a szám.

3.2.3 9, 21 és 63.

3.2.4 Használjuk az $(a^i)^t = a^{it}$ összefüggést és a 3.2.2 Tétel (i) állítását. Ennek alapján a legnehezebb c) rész (amelynek a) és b) speciális esete) a következőképpen igazolható:

$$1 \equiv (a^i)^t = a^{it} \pmod{m} \iff k \mid it \iff \frac{k}{(i,k)} \,\Big|\, t\frac{i}{(i,k)} \iff \frac{k}{(i,k)} \,\Big|\, t\,.$$

3.2.5
a) 10 és 30 (mutassunk példát is arra, hogy mindkettő valóban előfordul).
b) 36.

3.2.7 16.

3.2.8
a) $p \mid a^3 - 1 = (a-1)(a^2+a+1)$, de $p \nmid a - 1$.
b) Válasz: 6. — Útmutatás: Az a) rész alapján $(1+a)^2 \equiv a \pmod{p}$.

3.2.9 16.

3.2.10
a) (A kongruenciák az m modulusra vonatkoznak):

$$\left.\begin{array}{rcl} a^n \equiv 1 & \iff & o_m(a) \mid n \\ a^k \equiv 1 & \iff & o_m(a) \mid k \end{array}\right\} \iff o_m(a) \mid (n,k) \iff a^{(n,k)} \equiv 1\,.$$

b) Az a) rész alapján $a^n - 1$ és $a^k - 1$ közös osztói ugyanazok, mint $a^{(n,k)} - 1$ osztói.

3.2.11 Indirekt tegyük fel, hogy $m > 2$-re $a^n \equiv 1$ és $a^k \equiv -1 \pmod{m}$ teljesül. Ekkor $o_m(a) \mid n$ miatt $o_m(a)$ páratlan, továbbá $a^{2k} \equiv 1 \pmod{m}$ alapján $o_m(a) \mid 2k$. Innen $o_m(a) \mid k$, azaz $a^k \equiv 1 \pmod{m}$ következik, ami ellentmondás.

3.2.12 Ha $a^s \equiv -1 \pmod{p}$, akkor az előző feladat útmutatásához hasonló módon kapjuk, hogy $o_p(a)$ páros. Ez az állítás p helyett tetszőleges $m > 2$ modulusra is igaz. A megfordításnál legyen $o_p(a) = 2k$, ekkor $a^k \equiv -1$

(mod p). Ez a rész összetett modulusra általában nem igaz, legyen például $m = 15$ és $a = 4$.

3.2.13 b) Használjuk fel, hogy $a^k \equiv 1 \pmod{[m,n]}$ akkor és csak akkor igaz, ha az $a^k \equiv 1 \pmod{m}$ és $a^k \equiv 1 \pmod{n}$ kongruenciák egyszerre teljesülnek.

3.2.14 Válasz: 7. — Útmutatás: Az $x^2 \equiv 1 \pmod{1000}$ kongruencia $x \not\equiv 1 \pmod{1000}$ megoldásainak a számát keressük. A mod 1000 kongruencia helyett vizsgáljuk az $x^2 \equiv 1 \pmod{125}$, $x^2 \equiv 1 \pmod{8}$ szimultán kongruenciarendszert.

3.2.15

a) Mivel $(ab)^{[u,v]} = a^{[u,v]}b^{[u,v]} \equiv 1 \cdot 1 = 1 \pmod{m}$, ezért $o(ab) \mid [u,v]$. Ebből következik, hogy ha $o(ab) = uv$, akkor $(u,v) = 1$. A megfordításhoz tegyük fel, hogy $(ab)^t \equiv 1 \pmod{m}$; azt kell belátni, hogy ekkor $uv \mid t$. A kongruenciát u-adik hatványra emelve kapjuk, hogy $1 \equiv a^{tu}b^{tu} \equiv b^{tu} \pmod{m}$. Innen $o(b) = v \mid tu$, és $(u,v) = 1$ miatt így $v \mid t$. Hasonlóan adódik, hogy $u \mid t$, tehát $uv = [u,v] \mid t$.

b) Az a) részben már megmutattuk, hogy $o(ab) \mid [u,v]$. A másik oszthatóságot az a) rész második felében látott gondolatmenet mintájára igazolhatjuk.

3.2.16 Legyen $d = \big(o(a), o(b)\big)$, és emeljük a kongruenciát $o(a)/d$-edik, illetve $o(b)/d$-edik hatványra.

3.2.17 Vegyük észre, hogy modulo $a^n - 1$ az a rendje éppen n.

3.2.18 Mutassuk meg, hogy ha $ab \equiv 1 \pmod{m}$, akkor $o_m(a) = o_m(b)$, és így $o_m(a) + o_m(b)$ páros szám. Külön kell kezelni, ha itt $a \equiv b \pmod{m}$, vagyis $a^2 \equiv 1 \pmod{m}$; ez azt jelenti, hogy $o_m(a) = 2$ (ami páros szám) vagy $a \equiv 1 \pmod{m}$ (amelynek a rendje 1).

3.2.19

a) A maradék 1, ha $a \equiv 1 \pmod{p}$, és 0 egyébként.

b) A maradék 1, ha $o(a)$ páratlan, és -1, ha $o(a)$ páros.

3.2.20

a) Legyen az a/b racionális szám tizedestört-alakja $a/b = 0, c_1c_2c_3\ldots$, ekkor a c_i tizedesjegyeket a következő maradékos osztásokból kapjuk:

$$\begin{aligned} 10a &= c_1b + r_1, \qquad \text{ahol} \quad 0 \le r_1 < b, \\ 10r_1 &= c_2b + r_2, \qquad \text{ahol} \quad 0 \le r_2 < b, \\ 10r_2 &= c_3b + r_3, \qquad \text{ahol} \quad 0 \le r_3 < b, \\ &\vdots \end{aligned} \tag{1}$$

Ha itt valamelyik $r_i = 0$, akkor az eljárás véget ér, és véges tizedes törtet kapunk. A többi esetben, mivel mindegyik r_i csak az $1, 2, \ldots, b-1$ értékeket veszi fel, ezért lesz olyan $h < j$, amelyre $r_h = r_j$. Ekkor (1) alapján $c_{h+1} = c_{j+1}$, $r_{h+1} = r_{j+1}$, és így $c_{h+2} = c_{j+2}$, $r_{h+2} = r_{j+2}$ stb., vagyis ekkor végtelen szakaszos tizedes törtet kapunk.

A megfordításhoz tegyük fel, hogy a $0 < \alpha < 1$ valós szám tizedestörtalakja véges:

$$\alpha = 0, u_1 u_2 \ldots u_k, \qquad u_k \neq 0\,, \tag{2a}$$

illetve végtelen szakaszos:

$$\alpha = 0, u_1 u_2 \ldots u_k v_1 \ldots v_n v_1 \ldots v_n \ldots\,, \tag{2b}$$

ahol $u_1 u_2 \ldots u_k$ a nem ismétlődő rész (a tiszta szakaszos esetben ez hiányzik, azaz $k = 0$), $v_1 \ldots v_n$ pedig a (legkisebb ismétlődő) szakasz.
A (2a) esetben $\alpha = \overline{u_1 \ldots u_k}/10^k$, a (2b) esetben pedig $\alpha(10^{n+k} - 10^k)$ lesz egész szám.

b) Ezt lényegében már az a) részben beláttuk.

c) Egy tiszta szakaszos tizedes tört az a)-ban látott eljárással egy $10^n - 1$ nevezőjű (közönséges) törtté alakítható, a b az ennek (esetleges) egyszerűsítésével kapott tört nevezője, tehát $(b, 10) = 1$.

A megfordításhoz tekintsük az (1)-beli eljárást, legyen $r_0 = a$, ekkor

$$\begin{aligned} r_0 &\equiv \quad a \qquad\quad (\mathrm{mod}\ b)\,, \\ r_1 &\equiv 10a \qquad (\mathrm{mod}\ b)\,, \\ r_2 &\equiv 10r_1 \equiv 10^2 a\ (\mathrm{mod}\ b)\,, \end{aligned}$$

és ugyanígy általában $r_i \equiv 10^i a \pmod{b}$.

Az $r_h = r_j$ $(h < j)$ egyenlőség a $10^h a \equiv 10^j a \pmod{b}$ kongruenciát jelenti, ami $(10a, b) = 1$ miatt ekvivalens $10^{j-h} \equiv 1 \pmod{b}$ teljesülésével. Ez azt jelenti, hogy lesz olyan $i > 0$, amelyre $r_i = r_0 = a$, vagyis a szakasz rögtön a tizedesvessző után kezdődik, a szakasz hossza pedig annyi, ahány modulo b páronként inkongruens hatványa van a 10-nek, azaz $o_b(10)$.

d) Az ekvivalencia az előző két részből a „maradékelv" szerint következik, hiszen a kimaradt racionális számok adják a kimaradt vegyes szakaszos esetet. Itt a nem ismétlődő rész, illetve a szakasz hosszára vonatkozó állítást a c) résznél látottak mintájára igazolhatjuk.

3.3.

3.3.1 Azoknak a redukált maradékosztályoknak az elemei, amelyek egy-egy reprezentánsa: a) 3, 5; b) 3, 7; c) 5, 11.

3.3.2 Megfelel például az $x \equiv 2 \pmod{11}$, $x \equiv 3 \pmod{14}$ szimultán kongruenciarendszer megoldása: $x \equiv 101 \pmod{154}$.

3.3.3

a) Kövessük a 3.3.5 Tétel bizonyításában az (L1) és (L2) rész gondolatmenetét. Először keressünk egy primitív gyököt modulo 5, ilyen például a 2. Ezután nézzük meg, hogy a 2 primitív gyök-e modulo 25; ehhez elég $2^{5-1} \not\equiv 1 \pmod{25}$ teljesülését ellenőrizni, ami valóban fennáll. Mivel a 2 primitív gyök modulo 5^2, ezért primitív gyök minden 5-hatványra is.

b) Keressük a számot $a = 2 + 5t$ alakban. Az a akkor nem lesz primitív gyök mod 25, ha $1 \equiv (2+5t)^{5-1} \equiv 2^4 + 4 \cdot 8 \cdot (5t) \pmod{25}$, azaz $t \equiv 1 \pmod{5}$. Innen $a \equiv 7 \pmod{25}$. Lássuk még be, hogy ha a nem primitív gyök modulo 25, akkor nem lehet az modulo 625 sem; ehhez a 3.3.2 Tételt érdemes használni.

3.3.4 Igaz: b), d), e), f).

3.3.5

a) Ha g primitív gyök, akkor $g^{(p-1)/2} \equiv -1 \pmod{p}$, és így

$$(g_1 g_2)^{(p-1)/2} \equiv (-1)(-1) = 1 \pmod{p}.$$

b) Mutassuk meg, hogy ha g primitív gyök és $gh \equiv 1 \pmod{p}$, akkor h is primitív gyök. Ennek alapján megfelel egy ilyen g és h pár, valamint egy t tetszőleges primitív gyök, hiszen $ght \equiv t \pmod{p}$.

c) Ezek a $2^k + 1$ alakú prímek, az ún. Fermat-prímek (ekkor a k kitevő szükségképpen 2-hatvány, lásd az 1.4.4 feladatot).

3.3.6 Legyen $p > 2$ prím, g primitív gyök mod p. Ekkor az $1, g \ldots, g^{p-2}$ elemek redukált maradékrendszert alkotnak mod p, és így

$$(p-1)! \equiv 1 \cdot g \cdot \ldots \cdot g^{p-2} = \left(g^{(p-1)/2}\right)^{p-2} \equiv (-1)^{p-2} = -1 \pmod{p}.$$

3.3.7 Az összeg maradéka 0, ha $p-1 \nmid k$, és $p-1$, ha $p-1 \mid k$. — Útmutatás: A keresett maradék nem változik, ha az $1, 2, \ldots, p-1$ számok helyett egy másik redukált maradékrendszert vizsgálunk. Ennek megfelelően érdemesebb az $1^k + g^k + \ldots + g^{(p-2)k}$ összeget tekinteni, ahol g primitív gyök mod p. Ha $g^k \equiv 1 \pmod{p}$, akkor az összeg maradéka nyilván $p-1$, egyébként pedig használjuk fel a (véges) mértani sorozat összegképletét.

3.3.8 Válasz: 1, ha $p > 3$, és 2, ha $p = 3$. — Útmutatás: Állítsuk párba a primitív gyököket úgy, hogy az egy párba tartozó elemek szorzata 1 maradékot adjon.

3.3.9

a) Használjuk fel a 3.2.4c feladatot.

b) Tekintsük az a) részben szereplő $j = t(p-1)/d$ értékeket a $0 \le j < p-1$ feltétel mellett: ekkor $0 \le t < d$ és $(t, d) = 1$ miatt ezek száma $\varphi(d)$.

3.3.10 Az egyik irány könnyen következik a 3.2.4a feladatból. A megfordításhoz induljunk ki abból, hogy a és b egy g primitív gyök alkalmas hatványaival kongruensek modulo p, és használjuk fel a 3.2.4c feladatot. — Másik lehetőség: $(c, p) = 1$ esetén az összes $o_p(c)$-edrendű elem száma megegyezik a c hatványai között előforduló $o_p(c)$-edrendű elemek számával.

3.3.11 Minden állítás érvényben marad, ha $p-1$ helyére $\varphi(m)$-et írunk.

3.3.12

a) Vegyük észre, hogy elég a következő összefüggést igazolni:

$$5^{2^{\alpha-3}} = 1 + t2^{\alpha-1}, \qquad \text{ahol } t \text{ páratlan (és } \alpha \ge 3),$$

és ezt bizonyítsuk be α szerinti teljes indukcióval.

b) A kongruencia már mod 4 sem teljesül.

c) A megadott számok relatív prímek m-hez, számuk $\varphi(m)$, továbbá a feladat a) és b) részéből könnyen adódik, hogy páronként inkongruensek modulo m.

3.3.13 Legyen g_i primitív gyök mod $p_i^{\alpha_i}$, $i = 1, 2, \ldots, r$. Ekkor megfelel, ha u_i az $x \equiv g_i \pmod{p_i^{\alpha_i}}$, $x \equiv 1 \pmod{m/p_i^{\alpha_i}}$ szimultán kongruenciarendszer megoldása. — Páros m esetén használjuk fel a 3.3.12c feladatot is. Legyen az m kanonikus alakjában a 2 kitevője α. Ha $\alpha = 1$, akkor a képleten semmit sem kell változtatni. Ha $\alpha = 2$, akkor a képletben a hatványok szorzatát egy u^j tényezővel kell kiegészíteni, ahol $0 \le j < 2 = \varphi(4)$. Ha $\alpha \ge 3$, akkor egy $u^j v^k$ kiegészítő tényező kell, ahol $0 \le j < 2$ és $0 \le k < 2^{\alpha-2}$. Itt az u, illetve v értékeket az $x \equiv -1 \pmod{2^\alpha}$, $x \equiv 1 \pmod{m/2^\alpha}$, illetve az $x \equiv 5 \pmod{2^\alpha}$, $x \equiv 1 \pmod{m/2^\alpha}$ szimultán kongruenciarendszerek megoldásaként kaphatjuk meg.

3.3.14

a) Egy tetszőleges F egész együtthatós polinom esetén jelölje $\deg F$ az F fokszámát, $N(F)$ pedig az $F(x) \equiv 0 \pmod{p}$ kongruencia megoldásszámát. A 3.1.2 Tétel alapján $N(F) \le \deg F$. Ha $x^{p-1} - 1 = fh$, akkor a kis Fermat-tétel és p prím volta miatt egy redukált maradékrendszer minden

eleme kielégíti az $f(x) \equiv 0 \pmod{p}$ és $h(x) \equiv 0 \pmod{p}$ kongruenciák közül (legalább) az egyiket, ezért

$$p - 1 \leq N(f) + N(h) \leq \deg f + \deg h = p - 1\,,$$

így mindenhol egyenlőség teljesül. Tehát valóban $N(f) = \deg f$.

b) alkalmazzuk az f_i polinomokra az a) részt.

c) Egy c elemre akkor és csak akkor teljesül $o_p(c) = q^\beta$, ha $f_1(c) \equiv 0 \pmod{p}$, de $f_2(c) \not\equiv 0 \pmod{p}$. Ilyen c létezése a b) rész alapján következik.

d) Legyen a d kanonikus alakja $d = q_1^{\beta_1} \dots q_r^{\beta_r}$. A c) rész alapján létezik olyan c_i, amelyre $o_p(c_i) = q_i^{\beta_i}$ $(i = 1, 2, \dots, r)$. Ekkor a 3.2.15a feladat szerint $o_p(c_1 \dots c_r) = d$.

3.4.

3.4.1 A feltétel szerint $p \mid 7^3 - 2 = 11 \cdot 31$, azaz csak $p = 11$ és $p = 31$ jöhet szóba. A 7 primitív gyök mod 11, de nem primitív gyök mod 31, és így egyedül $p = 11$ felel meg a feltételeknek.

3.4.2 a) 0. b) $(p-1)/2$. c) $(p+1)/2$.

3.4.3

a) Kétféleképpen is előállítunk olyan g-hatványokat, amelyek az ab szorzattal kongruensek mod p:

$$g^{\operatorname{ind}(ab)} \equiv ab \equiv g^{\operatorname{ind} a} \cdot g^{\operatorname{ind} b} = g^{\operatorname{ind} a + \operatorname{ind} b} \pmod{p}\,,$$

és így az első és utolsó tagban a g kitevői kongruensek mod $p - 1$.

b) Az a) részhez hasonló gondolatmenetet alkalmazunk:

$$g^{\operatorname{ind}(a^k)} \equiv a^k \equiv \left(g^{\operatorname{ind} a}\right)^k = g^{k \cdot \operatorname{ind} a} \pmod{p}\,.$$

3.4.4 Az előző feladatnál látott módon bizonyíthatunk.

3.4.5 $o_p(a)$.

3.4.6 Ez a 3.3.4 Tétel (i) állításának az átfogalmazása.

3.4.7

a) Az előző feladat alapján mindkét feltétel azzal ekvivalens, hogy a primitív gyök mod p.

b) A 3.2.4c feladat alapján $o_p(a) = (p-1)/(\operatorname{ind} a, p-1)$, bármelyik primitív gyök szerint képeztük is az indexet.

3.4.8 Használjuk fel a 3.4.6 feladatot.

3.4.9 Induljunk ki a 3.4.7b feladathoz adott útmutatásból.

3.4.10 Egy-egy táblázat felső sorában a mod p redukált maradékosztályok legkisebb pozitív reprezentánsait soroljuk fel növekvő sorrendben, az alsó sorban pedig rendre ezeknek az elemeknek a g alapú indexei szerepelnek.

a) $p = 7$, $g = 3$:

1	2	3	4	5	6
0	2	1	4	5	3

b) $p = 11$, $g = 2$:

1	2	3	4	5	6	7	8	9	10
0	1	8	2	4	9	7	3	6	5

c) $p = 17$, $g = 3$:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

3.4.11 Ha $p \mid a$, akkor a megfelelő k számok a p többszörösei. Legyen most $(a, p) = 1$ és g egy primitív gyök mod p. Ekkor az $x \equiv g \pmod{p}$ és $x \equiv \operatorname{ind}_g a \pmod{p-1}$ szimultán kongruenciarendszer megoldásait vehetjük k-nak. — A feladat megoldható primitív gyök nélkül is, csak a kis Fermat-tételre támaszkodva: az $x \equiv a \pmod{p}$, $x \equiv 1 \pmod{p-1}$ szimultán kongruenciarendszer megoldásai megfelelnek k-nak.

3.5.

3.5.1

a) Nincs megoldása.

b) $x \equiv 51 \pmod{101}$. — Útmutatás: Használjuk fel a kis Fermat-tételt.

c) $x \equiv \pm 2 \pmod{23}$. — Útmutatás: A szokásos redukció után az $x^2 \equiv 4 \pmod{23}$ kongruencia adódik.

d) $x \equiv 0, \pm 6, \pm 7 \pmod{17}$.

e) $x \equiv 0, 2, 5, 6 \pmod{13}$.

f) $x \equiv \pm 5 \pmod{11}$. — Útmutatás: Mivel $x \equiv 0 \pmod{11}$ nem megoldás, ezért a redukciónál x^{20} helyére 1 írható.

3.5.2

a) Válasz: 12. — Útmutatás: Az $x^{30} \equiv 1 \pmod{73}$ és $x^{45} \equiv 1 \pmod{73}$ kongruenciák megoldásszámának összegéből le kell vonni a közös megoldások számát, azaz az $x^{(30,45)} \equiv 1 \pmod{73}$ kongruencia megoldásszámát.

b) Válasz: $(k+1, 30)$, ha $31 \mid k+1$, és $(k+1, 30) - 1$, egyébként.

Útmutatás: A bal oldal $(x^{k+1}-1)/(x-1)$ alakba írható. Így a kérdéses kongruencia megoldásai $x \equiv 1$-től esetleg eltekintve azonosak az $x^{k+1} \equiv 1 \pmod{31}$ kongruencia megoldásaival. Külön meg kell vizsgálni, hogy az $x \equiv 1 \pmod{31}$ milyen k esetén lesz megoldása az eredeti kongruenciának.

3.5.3 $a \equiv 0, \pm 1 \pmod{p}$.

3.5.4 A megoldhatóság feltétele: $(k, p-1) \mid \operatorname{ind}_g g = 1$. Ekkor a megoldásszám $(k, p-1) = 1$.

3.5.5 $x \equiv cb_i \pmod{p}$, $i = 1, \ldots, r$.

3.5.6 a) 1. b) ± 1.

3.5.7 A keresett feltétel: $(k, p-1) = 1$.

3.5.8 A 3-ra és a $3t-1$ alakú prímekre.

3.5.9 Használjuk a 3.5.3 Tételben szereplő két kritérium bármelyikét vagy a 3.5.2 Definíciót (az utóbbi esetben a b) résznél a kis Fermat-tételre is szükség van).

3.5.10 $(k, p-1) = 2$.

3.5.11

a) Válasz: 1, ha $p-1 \mid k$, és 0 egyébként. — Útmutatás: Ha $d = (k, p-1)$, akkor a k-adik hatványmaradékok g^{rd} alakban írhatók, ahol $0 \leq r < (p-1)/d$. Használjuk ezután a véges mértani sorozat összegképletét. — Egy másik lehetőség: A 3.3.7 feladatban szereplő összegben minden k-adik hatványmaradék $(k, p-1)$-szer fordul elő. — Egy harmadik út: Vegyük észre, hogy a k-adik hatványmaradékok éppen a $\mathbf{Z}_p$ feletti $x^{\frac{p-1}{(k,p-1)}} - 1$ polinom (egyszeres) gyökei, és használjuk fel a gyökök és együtthatók közötti összefüggést.

b) Válasz: -1, illetve 1, aszerint, hogy $\dfrac{p-1}{(k, p-1)}$ páros, illetve páratlan.

Útmutatás: Állítsuk párba a k-adik hatványmaradékokat úgy, hogy az egy párba tartozó elemek szorzata 1 maradékot adjon. — További lehetőségek: Írjuk fel a k-adik hatványmaradékokat az a) részhez adott első útmutatás szerint, illetve alkalmazzuk az a) részhez adott harmadik útmutatást.

3.5.12 Lásd a 3.5.9 feladathoz adott útmutatást. — Általánosítás: a akkor és csak akkor lesz egyszerre k-adik és n-edik hatványmaradék, ha $[k, n]$-edik hatványmaradék.

3.6.

3.6.1 Egy olyan homogén lineáris egyenletrendszernek, amelyben az ismeretlenek száma nagyobb az egyenletek számánál, mindig van nemtriviális megoldása. (Ez nemcsak modulo p, hanem bármely más test felett is érvényes.)

3.6.2 alkalmazzuk a Chevalley-tételt.

3.6.3

a) A kínai maradéktétel szerint elegendő a problémát egy p^α prímhatvány modulusra megoldani. Ha $\alpha > 1$, akkor az $x_1 = p^{\lceil \alpha/2 \rceil}$, $x_2 = x_3 = 0$ választás megfelelő. Ha $\alpha = 1$, akkor (pl. a Chevalley-tétel alapján) az $x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{p}$ kongruenciának van nemtriviális megoldása. Itt feltehető $|x_i| \le p/2$, ezért $0 < x_1^2+x_2^2+x_3^2 < p^2$, tehát az $x_1^2+x_2^2+x_3^2$ összeg (amely a feltétel szerint p-vel osztható) p^2-tel már nem lehet osztható.

b) Az a)-beli eljárást kell egyetlen esetben finomítani: ha $\alpha > 1$ és páratlan, akkor legyen $x_i = p^{(\alpha-1)/2} y_i$, és az y_i-kre alkalmazzuk az előbb $\alpha = 1$-re látott gondolatmenetet.

3.6.4 A $p = 2$ eset nyilvánvaló. Ha $p > 2$, akkor a Chevalley-tétel szerint léteznek olyan u_i egészek, $1 \le i \le 5$, amelyek a $\sum_{i=1}^5 x_i^4 \equiv 0 \pmod{p}$ kongruencia egy nemtriviális megoldását adják. Ha itt pl. $u_1 \not\equiv 0 \pmod{p}$, akkor $v_i = u_1^{p-2} u_i$ is megoldás és $v_1 \equiv 1 \pmod{p}$. A többi v_i-ről is feltehető $|v_i| \le (p-1)/2$. Ennek megfelelően $\sum_{i=1}^5 v_i^4$ osztható p-vel és

$$0 < \sum_{i=1}^{5} v_i^4 \le 1 + 4\Big(\frac{p-1}{2}\Big)^4 < \frac{p^4}{4}\,.$$

3.6.5

a) A c_j számban a q_i prím kitevője legyen γ_{ij} $(1 \le i \le k, 1 \le j \le t)$. Az $f_i(x_1, \dots, x_t) = \sum_{j=1}^t \gamma_{ij} x_j^2$ polinomokra és $p = 3$-ra alkalmazzuk a Chevalley-tételt.

b) Itt $t \ge (m-1)k + 1$ a megfelelő feltétel.

3.6.6 Először azt igazoljuk, hogy ha az állítás igaz $n = r$-re és $n = s$-re, akkor teljesül $n = rs$-re is. A $2rs-1$ számból vegyünk tetszőleges $2r-1$-et, ekkor az r-re vonatkozó állítás szerint kiválaszthatunk r olyat, amelyek összege osztható r-rel. A maradék $2rs - 1 - r$ számból ismét vegyünk tetszőleges $2r-1$-et, ezek között is van r darab olyan, amelyek összege osztható r-rel. Lássuk be, hogy ily módon $2s-1$ darab olyan r-es csoport keletkezik, ahol minden csoport elemeinek az összege osztható r-rel. alkalmazzuk ezután az s-re vonatkozó állítást ezen összegek r-edrészére.

Ennek alapján elég az $n = p =$ prím esettel foglalkozni. Legyen $f_1 = \sum_{j=1}^{2p-1} c_j x_j^{p-1}$, $f_2 = \sum_{j=1}^{2p-1} x_j^{p-1}$, és alkalmazzuk a Chevalley-tételt.

3.6.7

a) Indirekt tegyük fel, hogy az egyetlen megoldás $x_j = a_j$, $j = 1, 2, \ldots, t$. Ekkor a Chevalley-tételre adott bizonyításban csak a G polinom definícióját kell módosítani: legyen most

$$G(x_1, \ldots, x_t) = \prod_{j=1}^{t} \left(1 - (x_j - a_j)^{p-1}\right).$$

b) Legyen a megoldásszám s, a megoldások $\mathbf{a}_1, \ldots, \mathbf{a}_s$. Mindegyik $\mathbf{a}_v$ megoldáshoz készítsük el az a) résznek megfelelően megadott G_v polinomot ($v = 1, \ldots, s$). Legyen $G = \sum_{v=1}^{s} G_v$. Ekkor a Chevalley-tétel bizonyítását követve $F^* = G$ adódik. A fokszámokat összehasonlítva ebből azt kapjuk, hogy G-ben az $(x_1 \ldots x_t)^{p-1}$ tag együtthatója csak 0 lehet modulo p, azaz $s(-1)^t \equiv 0 \pmod{p}$.

3.6.8

a) Az A mátrix determinánsa

$$\begin{vmatrix} -b & a & 0 & \ldots & 0 \\ 0 & -b & a & \ldots & 0 \\ 0 & 0 & -b & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a & 0 & 0 & \ldots & -b \end{vmatrix} = (-b)^{p-1} + (-1)^{p-2} a^{p-1} \equiv 0 \pmod{p},$$

tehát $r(A) \leq p - 2$. Másrészt a bal felső elemhez tartozó aldeterminánsz $(-b)^{p-2} \not\equiv 0 \pmod{p}$, tehát $r(A) \geq p - 2$. Vagyis $r(A) = p - 2$, és a megoldásszám $p - 1 - (p - 2) = 1$. (Az eredményt természetesen jól ismerjük a 2.5.5 Tételből.)

b) A kérdéses mátrix minden eleme 1, tehát a rangja 1, és így a megoldásszám $p - 2$ (vö. a 3.5.3 feladattal).

c) Az a) részhez hasonlóan igazolható, hogy a rang $p - 2$, és így a megoldásszám 1. A megoldás könnyen láthatóan $x \equiv a^{p-2} \pmod{p}$. A megoldásszám a 3.5.7 feladatból is következik.

3.6.9 Azt kell belátnunk, hogy a mátrix determinánsa 0 (mod p).

a) A sorok összege 0.

b) Az i-edik sort s_i-vel jelölve $s_1 + s_2 - s_3 - s_4 + s_5 + \ldots = 0$.

3.6.10 Jelölje a Kőnig–Rados-tételben a három polinomhoz tartozó mátrixokat A_f, A_g, illetve A_h. Az A_f mátrixból a sorok permutálásával úgy kapjuk

meg A_g-t, hogy az utolsó sorból lesz az első, miközben a többi sor egymáshoz viszonyított helyzete nem változik. Az A_f-ből úgy jutunk el A_h-hoz, hogy tükrözünk a főátlóra, majd az utolsó sorból első sort csinálunk. Mivel ezek az átalakítások a mátrix rangját nem változtatják meg, a három kongruencia megoldásszáma azonos. — Könnyen megoldhatjuk a feladatot a Kőnig–Rados-tétel nélkül is. Ha $(j,p)=1$, akkor $f(j)\equiv jg(j) \pmod p$, és így az első két kongruenciának ugyanazok a megoldásai. Hasonlóan igazolható, hogy

$$f(a)\equiv 0 \pmod p \iff h(a^{-1})\equiv 0 \pmod p,$$

ahol a^{-1} az a multiplikatív inverzét jelenti: $aa^{-1}\equiv 1 \pmod p$.

3.6.11 A 3.1.3 Tételben leírt redukciós eljárással kiküszöbölhetjük a $p-1$-nél magasabb fokú tagokat. Mivel könnyen eldönthető, hogy $x\equiv 0 \pmod p$ mikor megoldás, ezért elég a p-hez relatív prím megoldások keresésére szorítkozni. Ebben az esetben a kis Fermat-tétel alapján x^{p-1} helyére 1-et írhatunk. Ha a kapott $h=d_0+d_1x+\ldots+d_{p-2}x^{p-2}$ polinomban minden d_j osztható p-vel, akkor $h(x)\equiv 0 \pmod p$ nyilván minden x-re teljesül. Végül, ha $d_0\equiv\ldots\equiv d_{i-1}\equiv 0 \pmod p$, de $d_i\not\equiv 0 \pmod p$, akkor a $h_1=h/x^i$ polinomra már alkalmazhatjuk a Kőnig–Rados-tételt, és a $h(x)\equiv 0 \pmod p$, ill. $h_1(x)\equiv 0 \pmod p$ kongruenciáknak ugyanazok a redukált maradékosztályok lesznek a megoldásai.

3.7.

3.7.1 a) 1. b) 0. c) 12. d) 73. e) 15.

3.7.2 Használjuk a 3.7.1 Tételt.

3.7.3

a) A megoldhatóság feltétele $a\equiv 1 \pmod{11}$, a megoldásszám 10. Útmutatás: Használjuk a kis Fermat-tételt és a 3.7.1 Tételt.

b) A megoldhatóság feltétele $a\equiv 1 \pmod 8$, a megoldásszám 4.

3.7.4 Az állítás leolvasható a 3.7.1 Tételre adott bizonyításból.

3.7.5

a) $x\equiv 32 \pmod{7^3}$.

b) Nem oldható meg.

c) $x\equiv 2+49j \pmod{7^3}$.

4. Legendre- és Jacobi-szimbólum

4.1.

4.1.1 *Első bizonyítás*: Az $x^2 \equiv c^2 \pmod p$ kongruencia megoldható; az egyik megoldás $x \equiv c \pmod p$.

Második bizonyítás: $(c^2)^{(p-1)/2} = c^{p-1} \equiv 1 \pmod p$.

Harmadik bizonyítás: $\left(\frac{c^2}{p}\right) = \left(\frac{c}{p}\right)^2 = 1$.

4.1.2 a) 1. b) -1. c) -1.

4.1.3 Az összeg 0, a szorzat 1, ha $p \equiv 1 \pmod 4$, és -1, ha $p \equiv -1 \pmod 4$.

4.1.4 Az $x^2 \equiv a \pmod p$ kongruencia megoldása szükségképpen kongruens a $\pm1, \pm2, \dots, \pm\left(\frac{p-1}{2}\right)$ redukált maradékrendszer valamelyik j elemével, és így valóban $a \equiv |j|^2 \pmod p$. Továbbá mind a megadott elemek, mind pedig a kvadratikus maradékok száma $(p-1)/2$, ezért a megadott elemek között már nem lehetnek kongruensek. Ez utóbbi közvetlenül is bizonyítható: Indirekt, ha valamely $1 \le u < v \le (p-1)/2$ esetén $u^2 \equiv v^2 \pmod p$, akkor $p \mid (v-u)(v+u)$, de itt $1 \le v-u < v+u \le$ $\le (p-1)$, tehát egyik tényező sem osztható p-vel, ami ellentmond p prím voltának.

4.1.5 Megmutatjuk, hogy $a \equiv b \equiv 0 \pmod{77}$, és így $5929 = 77^2 \mid a^2 + b^2$. Indirekt okoskodva, ha például a nem osztható (mondjuk) 7-tel, akkor 7 prím volta és $7 \mid a^2 + b^2$ miatt b sem osztható 7-tel. Ekkor $a^2 \equiv -b^2 \pmod 7$ és $\left(\frac{-1}{7}\right) = -1$ felhasználásával az alábbi módon jutunk ellentmondásra:

$$1 = \left(\frac{a}{7}\right)^2 = \left(\frac{a^2}{7}\right) = \left(\frac{-b^2}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{b}{7}\right)^2 = -1.$$

4.1.6 Használjuk fel a Wilson-tételt.

4.1.7 $(\pm a^{(p+1)/4})^2 = a^{(p+1)/2} = a \cdot a^{(p-1)/2} \equiv a \cdot 1 = a \pmod p$.

4.1.8 a) Ha $o_p(a) = 2t-1$, akkor $(a^t)^2 \equiv a \pmod p$. b) $p = 4k+3$.

4.1.9

a) Ha $o_p(g) = p-1$, akkor $g^{(p-1)/2} \not\equiv 1 \pmod p$.

b) $p = 2^k + 1$ (ezek az ún. Fermat-prímek, lásd az 1.4.4 feladatot és az 5.2 pontot).

4.1.10 32.

4.1.11
a) Mivel $p+1=4k$, így $1=\left(\frac{1}{p}\right)=\left(\frac{p+1}{p}\right)=\left(\frac{4k}{p}\right)=\left(\frac{2}{p}\right)^2\left(\frac{k}{p}\right)=\left(\frac{k}{p}\right)$.
b) Bizonyítsunk az a) részhez hasonlóan.

4.1.12 Ha $p\le 11$, akkor legalább az egyik kongruencia $x^2\equiv 0 \pmod p$ típusú. Egyébként használjuk ki, hogy a jobb oldalak szorzata négyzetszám, és így a megfelelő öt Legendre-szimbólum szorzata szükségképpen 1.

4.1.13
a) $x\equiv 1$ és $6 \pmod{13}$. — Útmutatás: alkalmazzuk a teljes négyzetté kiegészítést.
b) $x\equiv -3 \pmod{17}$.
c) $x\equiv 0, \pm 8 \pmod{23}$. — Útmutatás: Az x^{25} helyére a kis Fermat-tétel alapján x^3 írható. Az x kiemelése után egy másodfokúra visszavezethető negyedfokú kongruencia adódik.
d) Nincs megoldás. — Útmutatás: $x\equiv 0 \pmod{19}$ nem megoldás, így ekvivalens lépést végzünk, ha x-szel szorzunk és x^{18} helyére 1-et írunk.

4.1.14
a) alkalmazzuk a Legendre-szimbólum multiplikativitását.
b) Legyen $n(p)=n$ és r a legkisebb olyan egész, amelyre $rn>p$. Ekkor $0<rn-p<n$, ezért $1=\left(\frac{rn-p}{p}\right)=\left(\frac{rn}{p}\right)=-\left(\frac{r}{p}\right)$, és így $r\ge n$. Ezt felhasználva $(r-1)n<p$-ből adódik az állítás.

4.1.15
a) $\left(\frac{i^2}{p}\right)=1$, ha $(i,p)=1$, és 0, ha $p\,|\,i$.
b) Mutassuk meg, hogy ha $S(a,p)$-ben i helyére mindenütt ai-t írunk, akkor egyrészt az összeg nem változik, másrészt $\left(\frac{a^2}{p}\right)=1$ kiemelése után az új összeg éppen $S(1,p)$-vel egyenlő.
c) Rögzített i-re az $i+a$ értékek teljes maradékrendszert alkotnak mod p, és így az ezekhez tartozó Legendre-szimbólumok összege a 4.1.3 feladat alapján 0.
d) Az előző három részből következik.

4.1.16
a) Vegyük észre, hogy $\left(\frac{c}{p}\right)+1$ értéke aszerint 2, 0, illetve 1, hogy c kvadratikus maradék, kvadratikus nemmaradék, illetve osztható p-vel.
b) Az a) részből következik a 4.1.3 és 4.1.15d feladatok, valamint a $\left(\frac{-1}{p}\right)$-re tanultak felhasználásával.

4.2.

4.2.1 Megoldható: c), e), f). — A c)-nél használjuk fel a Wilson-tételt, az összetett modulusok esetén pedig akkor és csak akkor oldható meg a kongruencia, ha a modulusok minden prímhatvány osztójára nézve létezik megoldás.

4.2.2

a) $p = 8k + 1$ vagy $8k + 3$. — Útmutatás: $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$.

b) $p = 12k \pm 1$ vagy $p = 3$. — Útmutatás: A reciprocitási tétel alkalmazásánál az számít, hogy $p > 3$ mivel kongruens mod 4, utána pedig az, hogy p mivel kongruens mod 3. Ezért aszerint érdemes az eseteket megkülönböztetni, hogy p mivel kongruens mod 12.

c) $p = 6k + 1$ vagy $p = 3$.

d) $p = 5k \pm 1$ vagy $p = 5$.

e) $p = 8k \pm 1$ vagy $8k + 3$. — Útmutatás: Bontsuk szorzattá $x^4 - 4$-et.

f) $p = 4k + 1$. — Útmutatás: alkalmazzuk a 3.5.1 Tételt, vizsgáljuk az eseteket a p-nek a 8-cal való osztási maradéka szerint, és használjuk fel a $\left(\frac{-1}{p}\right)$ és $\left(\frac{2}{p}\right)$ képletét.

g) Minden p-re. — Útmutatás: Használjuk fel az e) és f) részt, vagy alkalmazzuk a 3.5.1 Tételt.

h) A $24k + 17$ alakú prímek kivételével minden prímre.

4.2.3 Kövessük a 4.1.5 feladatra adott útmutatást, felhasználva, hogy az 1999 prím és $\left(\frac{-2}{1999}\right) = -1$.

4.2.4 A feltétel ekvivalens azzal, hogy $(2c)^8 \equiv -2^7 \pmod{43^{100}}$. Az $x^8 \equiv -2^7 \pmod{43}$ kongruencia megoldhatóságához használjuk fel a 3.5.1 Tételt, valamint, hogy $\left(\frac{-2}{43}\right) = 1$. A 43^{100} modulusra a 3.7.2 feladat (vagy a 3.7.1 Tétel) alapján térhetünk át. Végül a kapott maradékosztályoknak a modulus páratlansága miatt biztosan van páros eleme is.

4.2.5

a) Ha $8c^2 \equiv 1 \pmod{p}$, akkor

$$1 = \left(\frac{1}{p}\right) = \left(\frac{8c^2}{p}\right) = \left(\frac{2}{p}\right)^3 \left(\frac{c}{p}\right)^2 = \left(\frac{2}{p}\right).$$

A második állítást indirekt bizonyítjuk: Ha $8c^2 - 1$ minden prímtényezője $8k + 1$ alakú volna, akkor ezek (megfelelő multiplicitással vett) szorzata, azaz maga a $8c^2 - 1$ is $8k + 1$ alakú lenne, ami ellentmondás.

b) Az a) részhez hasonlóan okoskodhatunk (most $\left(\frac{3}{p}\right) = 1$ adódik).

c) A $\left(\frac{-1}{p}\right)$ felhasználásával kapjuk, hogy $c^2 + 4$ minden (páratlan) p prímosztójára $p \equiv 1 \pmod{4}$. Ez azt jelenti, hogy $p \equiv 1$ vagy 5

(mod 8) és (mod 12) is. Mivel $c^2+4 \equiv 5 \pmod 8$ és (mod 12), ezért nem teljesülhet minden prímosztóra $p \equiv 1 \pmod 8$, illetve (mod 12).

4.2.6

a) A reciprocitási tétel alapján

$$\prod_{i=1}^{5} \left(\frac{a_i}{p_i}\right) = (-1)^{\binom{r}{2}},$$

ahol r a $4k-1$ alakú p_i-k száma, továbbá $\binom{r}{2}$ pontosan akkor páratlan, ha $r = 2$ vagy 3.

b) A feltétel szerint minden $i \neq j$-re $\left(\frac{p_i}{p_j}\right) = 1$. Így a reciprocitási tétel miatt a p_i prímek között legfeljebb egy lehet $4k-1$ alakú.

4.2.7

a) A középső számot c-vel jelölve, az összeg

$$S = (c-9)^2 + (c-8)^2 + \ldots + (c+9)^2 = 19(c^2+30)$$

alakba írható. Mivel $\left(\frac{-30}{19}\right) = -1$, ezért S a 19-nek pontosan az első hatványával osztható, és így nem lehet teljes hatvány.

b) Az a) részhez hasonlóan elég belátnunk, hogy $a = (1-p^2)/12$ kvadratikus nemmaradék mod p. Vegyük észre, hogy $\left(\frac{a}{p}\right) = \left(\frac{36a}{p}\right) = \left(\frac{3}{p}\right)$.

4.2.8 Például $f = (x^2+1)(x^2-17)(x^2+17)$ megfelel.

4.3.

4.3.1 a) 1. b) -1. c) -1. d) 1.

4.3.2

a) Legyen $m = p_1 \ldots p_r$. Ha az $x^2 \equiv a \pmod m$ kongruencia megoldható, akkor minden i-re az $x^2 \equiv a \pmod{p_i}$ kongruencia is megoldható, tehát minden i-re $\left(\frac{a}{p_i}\right) = 1$, és így $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \ldots \left(\frac{a}{p_r}\right) = 1$.

b) Például $m = 9, a = 2$, vagy $m = 15, a = 8$ stb.

c) $m = p^{2k+1}$ (ahol p prím, $k \geq 0$).

4.3.3 A $p = 2$ eset nyilvánvaló. Egyébként $p \equiv 1 \pmod 4$, ekkor $\left(\frac{-1}{p}\right) = 1$, tehát elég az $a, b > 0$ esetet nézni. Legyen (mondjuk) az a páratlan, ekkor ($a > 1$ esetén) $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1$.

4.3.4 Mindkét összeg -1.
Útmutatás b)-hez: Lássuk be, hogy $\left(\frac{k}{2k+1}\right) = \left(\frac{-2}{2k+1}\right)$.

4.3.5

a) Ha $a \equiv 1 \pmod 4$, akkor $\left(\frac{a}{m}\right) = \left(\frac{m}{a}\right) = \left(\frac{n}{a}\right) = \left(\frac{a}{n}\right)$. Ha $a = 2^k t$, ahol $k \geq 2$ és t páratlan, akkor $m \equiv n \pmod 4$ miatt a reciprocitás egyformán működik a t, m és t, n párra, továbbá $k \geq 3$ esetén $m \equiv n \pmod 8$ miatt $\left(\frac{2}{m}\right) = \left(\frac{2}{n}\right)$, ha pedig $k = 2$ (vagy tetszőleges páros szám), akkor nincs szükség $\left(\frac{2}{m}\right)$-re, illetve $\left(\frac{2}{n}\right)$-re.

b) Mindkét esetben megfelel tetszőleges (az a-hoz relatív prím, 1-nél nagyobb, páratlan) m és $n = m + 2a$.

4.3.6

a) 0 vagy $\varphi(m)$. — Útmutatás: Ha minden $\left(\frac{r}{m}\right) = 1$, akkor az S összeg nyilván $\varphi(m)$. Egyébként legyen c tetszőleges szám, amelyre $\left(\frac{c}{m}\right) = -1$, és írjunk r helyére mindenhová cr-et. Az így keletkező S' összegről lássuk be, hogy egyrészt $S' = S$, másrészt $S' = -S$.

b) -1, ha m egy $4k + 3$ alakú prím páratlan hatványa, és 1 minden más esetben.

4.3.7

a) m négyzetszám. — Útmutatás: A négyzetszámok nyilván megfelelnek. Ha m nem négyzetszám, akkor van olyan p prímosztója, amely páratlan hatványon szerepel az m kanonikus alakjában, azaz $m = p^k t$, ahol $(t, p) = 1$ és k páratlan. Legyen c egy kvadratikus nemmaradék mod p. Ekkor az $x \equiv c \pmod p$, $x \equiv 1 \pmod t$ szimultán kongruenciarendszer egy a megoldására $\left(\frac{a}{m}\right) = -1$.

b) a négyzetszám. — Útmutatás: Az a) részhez hasonlóan bizonyíthatunk, használjuk fel a reciprocitást is. Ne felejtsük el, hogy a lehet páros és/vagy negatív szám is.

5. Prímszámok

5.1.

5.1.1 Ha valamilyen $m > 1$ modulusra (például) $r_1, \ldots, r_j$ teljes maradékrendszer modulo m, akkor bármely n-re az $n + r_1, \ldots, n + r_j$ számok is teljes maradékrendszert alkotnak modulo m, és így biztosan van közöttük m-mel osztható. Ha $m \mid n + r_i$ és $n + r_i > m$, akkor $n + r_i$ nem lehet prím.

5.1.2

a) Legyen $n \geq 7$ páratlan. Ekkor $n - 3 \geq 4$ páros, és így $n - 3 = p_1 + p_2$, tehát $n = 3 + p_1 + p_2$.

b) Ha egy páros szám három prím összege, akkor az egyik prím szükségképpen a 2, továbbá $n-2=p_1+p_2 \iff n=2+p_1+p_2$.

5.1.3 Minden $n \geq 8$. — Minden $n \geq 40$, valamint $n = 18, 24, 30, 34$ és 36.

5.1.4 Csak az 5 és 2 pár ilyen.

5.1.5 c) Használjuk fel, hogy ha $(p,d)=1$, akkor a számtani sorozat első p tagja teljes maradékrendszer modulo p.

5.1.6 *Mersenne és Fermat*: Az 1.4.4 feladatban láttuk, hogy ha k összetett, akkor 2^k-1, ha pedig k nem kettőhatvány, akkor 2^k+1 biztosan összetett. n^2+1: Ha $n>1$ páratlan, akkor $n^2+1>2$ páros, és általában, ha $k<n\equiv k \pmod{k^2+1}$, akkor $n^2+1\equiv k^2+1\equiv 0 \pmod{k^2+1}$, tehát ekkor n^2+1 összetett.
Csupaegy: A k darab 1-esből álló szám is biztosan összetett, ha k összetett.
$333\ldots31$: Ezek a számok $(10^k-7)/3$ alakúak, és $2\leq k\leq 8$ esetén prímek. Azonban ha $k=2+30r$, akkor a kis Fermat-tétel alapján $10^k-7\equiv 10^2-7 \pmod{31}$, és így $(3,31)=1$ miatt

$$\frac{10^k-7}{3}\equiv\frac{10^2-7}{3}=31\equiv 0 \pmod{31},$$

tehát ilyenkor mindig 31-gyel osztható számot kapunk. Ugyanígy adódik, hogy például végtelen sok 17-tel osztható van közöttük: a 10 primitív gyök modulo 17, tehát létezik olyan s, amelyre $10^s\equiv 7 \pmod{17}$, és ekkor $k=s+16r$ esetén $17\mid(10^k-7)/3$.
Fibonacci: Minden harmadik elem páros, sőt tetszőleges m-re végtelen sok m-mel osztható van közöttük (lásd az 1.2.5 feladatot).

5.1.7 Használjuk fel az ún. interpolációs polinomokra vonatkozó tételt: Bármely k helyen tetszőlegesen előírva a helyettesítési értékeket, pontosan egy legfeljebb $k-1$-edfokú megfelelő polinom létezik (amelynek együtthatói az adott testből valók).

5.1.8

a) Ha $a\equiv b \pmod{f(b)}$, akkor $f(a)\equiv 0 \pmod{f(b)}$.

(b1) Az állítás átfogalmazható arra, hogy ha g egész együtthatós polinom, akkor $g(n)$ nem lehet minden n-re egy prímszám rögzített konstansszorosa. Ennek bizonyítása az a)-hoz hasonlóan történhet.

(b2) Ha egy komplex együtthatós polinom a fokszámánál több racionális helyen racionális értéket vesz fel, akkor szükségképpen racionális együtthatós. Ez például az interpolációs polinomok segítségével igazolható.

(b3) Egy kivételével minden változónak adjunk rögzített egész értéket, ezzel a feladatot visszavezettük az egyváltozós esetre.

5.1.9

a) Az 5.1.1 Tétel bizonyításának gondolatmenetéből n szerinti teljes indukcióval következik.

b) A $\lfloor 10^{2^{2^j}} c \rfloor$ egész szám „végén" éppen p_j áll.

c) A c számot (valószínűleg) csak úgy tudjuk megadni, ha már előre ismerjük (az éppen a c segítségével meghatározni remélt) prímszámokat.

5.1.10 Pl. $K = (10^4)!$ megfelel.

5.2.

5.2.1

a) A könnyen adódó $F_{n+1} = F_n(F_n - 2) + 2$ összefüggést felhasználva bizonyítsunk teljes indukcióval.

b) Támaszkodjunk az a) részre.

c) Mindegyik Fermat-számnak van olyan prímtényezője, amely semelyik másik Fermat-számnak sem lehet osztója.

d) Az n-edik prímszám nem lehet nagyobb F_{n-1}-nél.

5.2.2 Ha F_n prím, akkor mutassuk meg, hogy $\left(\frac{5}{F_n}\right)$, illetve $\left(\frac{10}{F_n}\right)$ értéke -1. A megfordítás pontosan ugyanúgy igazolható, mint az 5.2.2 Tételben.

5.2.3 A feltétel szükségességét ugyanúgy igazolhatjuk, mint az 5.2.2 Tételben. A megfordításnál okoskodjunk indirekt; ekkor feltehető, hogy K_n-nek létezik egy $q \leq \sqrt{K_n}$ prímosztója. Mutassuk meg, hogy $o_q(3) = 2^n$ vagy $5 \cdot 2^n$. Innen kapjuk, hogy $2^n \mid q - 1$. Ezt a $q \leq \sqrt{K_n}$ feltétellel összevetve ellentmondásra jutunk.

5.2.4 Használjuk fel a $\varphi(N)$ képletét.

5.2.5 Válasz: 5. — Útmutatás: Először mutassuk meg, hogy k szükségképpen kettőhatvány. Ezután használjuk fel az 5.2.1a feladatot és azt a tényt, hogy F_5 osztható 641-gyel.

5.2.6 Az 5.2.3 Tétel alapján a legkisebb szóba jövő prímek a 47, a 233, a 223, illetve a 431, és az ismételt négyzetre emelések módszerével ellenőrizhetjük, hogy ezek valóban osztói a megadott Mersenne-számoknak.

5.2.8 Ha $2^{2^n} \equiv -1 \pmod{q^2}$, akkor az 5.2.1 Tétel bizonyításához hasonló módon $o_{q^2}(2) = 2^{n+1} \mid \varphi(q^2) = q(q-1)$ adódik. Ebből kapjuk, hogy $o_{q^2}(2) \mid q - 1$, és így valóban $2^{q-1} \equiv 1 \pmod{q^2}$. A Mersenne-számokra vonatkozó állítás hasonlóan igazolható.

5.2.9 A $(8, 9)$ páron kívül csak azok a párok lesznek megfelelők, amelyek egyik tagja egy Fermat- vagy Mersenne-prím, a másik tag pedig a megfelelő kettőhatvány.

5.2.10 Ha $k \mid n$ teljesül H-ban, akkor egyrészt alkalmas a és b egészekkel $n/k = a + b\sqrt{3}$, másrészt n/k racionális. Innen $\sqrt{3}$ irracionalitása miatt következik, hogy $b = 0$ és a egész szám. Az állítás másik iránya nyilvánvaló.

5.2.11 Elég belátni, hogy ha F_n prím, akkor alkalmas k-ra $F_n \mid H_k$. Ennek igazolásához használjuk fel, hogy $o_{F_n}(6) \mid F_n - 1$, tehát $o_{F_n}(6) = 2^j$ alakú. Ekkor $F_n \mid H_{j-1}$.

5.3.

5.3.1 Válasz: 6003. (A redukált maradékosztályokban végtelen sok, a 9999 prímosztói által reprezentált maradékosztályokban pedig egy-egy (pozitív) prím található.)

5.3.2 A problémát az jelenti, hogy az $A = 4p_1 \dots p_r + 1$ számnak nem feltétlenül van $4k + 1$ alakú prímosztója, mert lehet, hogy páros sok $4k + 3$ alakú prím szorzata.

5.3.3

a) Kövessük az 5.3.2 Tétel bizonyításának a gondolatmenetét.

b)–h) Járjunk el az 5.3.3 Tétel bizonyításának a mintájára. Az egyes esetekben mindig vizsgáljuk meg, milyen alakú prímosztói lehetnek a következő alakú számoknak [a c), d), f) és h) résznél használjuk fel a 4.2.5 feladatot]:
b) $n^2 + 2$; c) $n^2 + 4$; d) $n^2 - 2$ vagy $8n^2 - 1$;
e) $5n^2 - 1$; f) $n^2 + 4$; g) $(2n)^2 + 3$; h) $12n^2 - 1$.

5.3.4 Végtelen sok; a $10\,000k + 4321$ számtani sorozatról van szó.

5.3.5 Indirekt tegyük fel, hogy a szóban forgó tizedes tört szakaszos lenne, k hosszúságú szakasszal. Azonban végtelen sok prím van, amelynek az utolsó $2k$ jegye 1-es, és olyan prím is végtelen sok van, amelynek az utolsó $2k$ jegye 3-as, ezért a szakasznak egyrészt csupa 1-esből, másrészt csupa 3-asból kellene állnia, ami lehetetlen.

5.3.6 A feltétel: $(a, b, c) = 1$. A szükségesség nyilvánvaló. Útmutatás az elégségességhez: Legyen $(a, b) = s$, ekkor $(s, c) = 1$. A Dirichlet-tétel alapján van olyan k, amelyre $a + bk = sp$, ahol p egy c-nél nagyobb prím. Ezután alkalmazzuk ismét a Dirichlet-tételt az $sp + cn$, $n = 0, 1, \dots$ számtani sorozatra.

5.3.7

a) Például a $p = 8 \cdot |c| \cdot k + 1$ alakú prímekre $\left(\frac{c}{p}\right) = 1$. Ennek igazolásához felhasználhatjuk $|c|$ kanonikus alakját és a Legendre-szimbólum (vagy a Jacobi-szimbólum) tulajdonságait. (Gondoljunk arra az esetre is, amikor c páros és/vagy negatív szám.)

b) Válasz: c nem négyzetszám. — Útmutatás: használjuk fel a 4.3.7b feladatot (vagy az ott látott megoldás gondolatmenetét).

5.3.8 Legyenek $p_1, \dots, p_{n-1}$ különböző prímek. Ekkor alkalmas k egész számra az $f = x\big(1 + k(x - p_1)\dots(x - p_{n-1})\big)$ polinom megfelel: $v_1 = p_1$, …, $v_{n-1} = p_{n-1}$, $v_n = 1$.

5.3.9 Legyenek a és d rögzített relatív prím pozitív egészek. Válasszunk olyan r nemnegatív egészt, amelyre $a_1 = a + rd$ összetett szám. Ekkor bármely s pozitív egészre $(a_1, d^s) = 1$, és így a feltétel szerint létezik olyan k_s, amelyre $p_s = a_1 + k_s d^s$ prím. Ezek a p_s prímek valamennyien egyben $a + kd$ alakúak is, és ($k_s \neq 0$ miatt) szükségképpen végtelen sok különböző van közöttük.

5.4.

5.4.1 Írjuk fel az a és b számot $a = \lfloor a \rfloor + \{a\}$, illetve $b = \lfloor b \rfloor + \{b\}$ alakban, ahol $0 \leq \{a\}, \{b\} < 1$. Ekkor $a + b = \lfloor a \rfloor + \lfloor b \rfloor + \{a\} + \{b\}$. Ha itt az utolsó két tag összege 1-nél kisebb, akkor $\lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor$, ha pedig 1 és 2 közé esik, akkor $\lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor + 1$.

5.4.2 Lássuk be, hogy elég x egész értékeire szorítkoznunk, majd használjuk fel, hogy csak véges sok olyan pozitív egész van, amely kisebb, mint (az 5.4.3 Tétel által garantált) x_0.

5.4.3 alkalmazzunk az 5.4.2 Tétel bizonyításához hasonló gondolatmenetet. A $\pi(p_n) = n$ összefüggésből és a $\pi(x)$-re adott felső becslésből azonnal adódik, hogy $p_n > (1/c_2) \cdot n \cdot \log n$, ha n elég nagy. A másik irányú becslés kicsit bonyolultabb, itt szükségünk van a $\log p_n < (1 + \varepsilon) \log n$ egyenlőtlenség igazolására is. Eredmény: bármely $\varepsilon > 0$ esetén minden (ε-tól is függően) elég nagy n-re $p_n < (1/c_1 + \varepsilon) \cdot n \cdot \log n$.

5.4.4 A feladat két része könnyen következik egymásból: az a) rész a b) rész logaritmizált változata. Az a) rész igazolásához támaszkodhatunk a

$$\log n \cdot \pi(n) \geq \sum_{p \leq n} \log p \geq \log f(n) \cdot \big(\pi(n) - \pi(f(n))\big)$$

egyenlőtlenségekre, ahol például az $f(n) = n/(\log n)^2$ választás célhoz vezet.

5.4.5 A (iii) a (iv)-nek logaritmizált alakja. Az (i)⇒(ii), illetve (i)⇒(iii) következtetés ugyanúgy igazolható, mint az 5.4.2 Tétel, illetve az 5.4.4 feladat. A megfordításoknál is hasonló gondolatmenetet érdemes követni.

5.4.6

a) A felső becslés azonnal adódik az $S(n) \le n \cdot \pi(n)$ összefüggésből és $\pi(x)$ felső becsléséből. Az alsó becslés igazolásához induljunk ki az $S(n) \ge \big(\pi(n) - \pi(cn)\big) \cdot (cn)$ egyenlőtlenségből, ahol $0 < c < 1$, és a prímszámtétel segítségével mutassuk meg, hogy található olyan $c' > 0$, amelyre $\pi(n) - \pi(cn) > c' \cdot n/\log n$. (A prímszámtétel helyett használhatjuk az 5.4.3 Tételt is, ekkor a c értékét elegendően kicsinek kell választanunk ahhoz, hogy megfelelő c' létezését biztosítani tudjuk.)

b) A $p_k \sim k \log k$ összefüggés alapján mutassuk meg, hogy

$$S(n) \sim \sum_{k=2}^{\pi(n)} k \log k \sim \int_2^{\pi(n)} t \log t \, dt \,.$$

Használjuk fel, hogy

$$\int t \log t \, dt = \frac{2t^2 \log t - t^2}{4} \qquad \text{és} \qquad \pi(n) \sim \frac{n}{\log n} \,.$$

5.4.7 Használjuk fel, hogy egy adott N-ig „sok” prímszám van, és így ezekből sok kéttagú összeg, illetve különbség képezhető, ugyanakkor az így keletkező páros számok „kevesen” vannak, ezért a skatulyaelv alapján legalább az egyik páros szám sokféleképpen áll elő ilyen összegként, illetve különbségként.

Nézzük mindezt részletesebben az összegekre, a különbségek is hasonlóan tárgyalhatók. Bármely két, N-nél nem nagyobb páratlan prímszám összege egy $2N$-nél nem nagyobb páros szám. Az ilyen összegek száma

$$\binom{\pi(N) - 1 + 1}{2} \sim \frac{N^2}{2(\log N)^2} \,,$$

a $2N$-nél nem nagyobb páros számok száma pedig N. Ezért (elég nagy N esetén) van olyan páros szám, amely legalább

$$\frac{N}{3(\log N)^2} > K$$

-féleképpen áll elő két prímszám összegeként.

5.4.8 A képlet alapja a Wilson-tétel és a megfordítása: $j > 1$ esetén $j \mid (j-1)! + 1 \iff j$ prím. — A $\pi(n)$ gyakorlati kiszámítására ez a formula nem használható, mert már a faktoriálisok, illetve ezek osztási maradékainak meghatározására sem ismerünk gyors algoritmust.

5.5.

5.5.1 Használjuk fel a Csebisev-tételt.

5.5.2 Írjuk fel a nagyobbik számot $n = p + (n-p)$ alakban, ahol p a legnagyobb prím n-ig, majd ismételjük meg ugyanezt n helyett $n-p$-vel stb. Az eljárás addig folytatható, amíg a „maradék" 0 vagy 1 lesz. Az n-et vagy $n-1$-et ily módon előállító prímek a Csebisev-tétel alapján mind különbözők.

5.5.3

a) Az 1-es számjeggyel kezdődő $k+1$-jegyű számok $10^k \le n < 2 \cdot 10^k$ alakúak, és ezek között a Csebisev-tétel szerint minden k-ra található prímszám.

b) A Csebisev-tétel helyett támaszkodjunk az 5.5.5 Tétel (A) részére.

5.5.4

a) Legyen p olyan prím, amelyre $n/2 < p \le n$. A törteket közös nevezőre hozva a közös nevező is, és pontosan egy tag kivételével az összes számláló is osztható p-vel. Ezért az összeg nem lehet egész (csak olyan törtként írható fel, amelynek a nevezője osztható p-vel). — Az állítás bizonyítható a Csebisev-tétel felhasználása nélkül is, ha az $\mathrm{lkkt}(1, 2, \ldots, n)$ közös nevezőben és az így adódó számlálókban a 2 kitevőjét vizsgáljuk.

b) Ha $n \ge 2k-1$, akkor az a) részre adott (bármelyik) bizonyítás átvihető. Ha $n < 2k-1$, akkor az összeg kisebb, mint 1.

5.5.5 Mivel $\binom{2n}{k} = \binom{2n}{2n-k}$, ezért feltehető, hogy $k < n$. Ekkor

$$\binom{2n}{n} = \binom{2n}{k} \cdot \frac{(2n-k)\ldots(n+1)}{(k+1)\ldots n}\,.$$

A jobb oldali törtnél a számláló és a nevező is $n-k$ darab tényező szorzata, és a számláló bármely tényezője nagyobb, mint a nevező bármely tényezője. Ennélfogva a tört nagyobb, mint 1.

5.5.6 A modulusok páronként relatív prímek, ezért a kongruenciarendszer megoldható. A megoldások egy redukált maradékosztályt alkotnak modulo $m = p_1 \ldots p_K q_1 \ldots q_K$, amelyben a Dirichlet-tétel szerint található (végtelen sok) $p > m$ prímszám. A kongruenciarendszer konstrukciójának megfelelően $p-j$ osztható p_j-vel, $p+j$ pedig q_j-vel, továbbá $p-j > p_j$, $p+j > q_j$, tehát valamennyi $p \pm j$ összetett szám.

5.5.7

a) A $\binom{2n}{n}$ számlálójának a p az egyik tényezője, viszont a nevező és a számláló többi tényezője nem osztható p-vel.

b) Mind a számláló, mind a nevező a p-nek pontosan a második hatványával osztható (a számlálóban a $3p$ és $4p$, a nevezőben a p és $2p$ tényezőkben szerepel a p). — Általánosítás: Ha $2n/(2k+1) < p \le n/k$ és $p > 2k$, akkor $\binom{2n}{n}$ nem osztható p-vel.

5.5.8 Jelöljük L-lel az n és $2n$ közötti prímek számát. Az 5.5.3 Tétel bizonyításában szereplő C az 5.5.7a feladat szerint éppen az n és $2n$ közötti prímek szorzata, ennélfogva $C < (2n)^L$. Másrészt a bizonyításban szereplő (6) egyenlőtlenségből elég nagy n-re $C > 4^{n/4}$ következik, hiszen az ottani (7) jobb oldalán szereplő különbségben a kivonandó elhanyagolható a kisebbítendőhöz képest. A C-re most felírt két egyenlőtlenségből kapjuk, hogy $4^{n/4} < (2n)^L$, ahonnan logaritmálással adódik a feladat állítása elég nagy n-re, majd az 5.4.2 feladat mintájára minden $n \ge 2$-re.

5.5.9

a) Használjuk fel, hogy elég nagy n esetén az $(n, n+n^{2/3})$ intervallum tartalmaz prímszámot.

b) A $q_n = \lfloor \alpha^{3^n} \rfloor$ feltétel ekvivalens

$$\sqrt[3^n]{q_n} \le \alpha < \sqrt[3^n]{q_n+1} \tag{1}$$

teljesülésével. Válasszuk meg a q_n prímeket rendre úgy, hogy (1) azt jelentse, hogy α egy egymásba skatulyázott intervallumsorozat minden intervallumának eleme. Ez megtehető, mert az egymásba skatulyázottság ekvivalens a $q_n^3 \le q_{n+1} < (q_n+1)^3 - 1$ egyenlőtlenséggel.

c) A b)-beli képletben α pontos értéke nem ismert, csak α létezését tudtuk igazolni.

5.5.10

a) Az 5.5.5 Tétel (B) részének bizonyítását követve azt kapjuk, hogy alkalmas $c > 0$ mellett az $(n, n + c\log n)$ intervallum végtelen sok n-re nem tartalmaz prímszámot.

b) Az 5.5.1 Tétel bizonyítása szerint $n = (K+1)! + 1$ esetén az $(n, n+K)$ intervallum prímmentes. Fejezzük ki a K-t az n segítségével. Ehhez használjuk fel az $m!$-ra vonatkozó alábbi becsléseket:

$$\left(\frac{m}{e}\right)^m < m! \le m^m .$$

(A felső becslés nyilvánvaló, az alsó becslés pedig könnyen igazolható teljes indukcióval.) Ezeket az egyenlőtlenségeket (vagy a Stirling-formulát) logaritmálva $\log m! \sim m\log m$ adódik. A jelen esetben ez azt jelenti, hogy $\log n \sim K \log K$, ahonnan azt nyerjük, hogy $K \sim \log n / \log\log n$.

Ezzel azt igazoltuk, hogy bármely $\varepsilon > 0$ esetén végtelen sok olyan n pozitív egész létezik, amelyre az $\big(n, n+(1-\varepsilon)\log n/\log\log n\big)$ intervallum nem tartalmaz prímszámot.

c) A jelzett megjegyzés szerint, ha $n-1$ a $K+1$-nél nem nagyobb prímek szorzata, akkor az $(n, n+K)$ intervallum prímmentes. Az 5.4.5 Lemma szerint $n \le 4^{K+1}$, az 5.4.4b feladat szerint pedig $n < e^{(1+\varepsilon)(K+1)}$ is igaz (ez utóbbihoz felhasználtuk a prímszámtételt). Innen $K > c\log n$ adódik, vagyis az a)-beli eredményt kapjuk, illetve az élesebb becslést felhasználva az 5.5.5 Tétel (B) részének állítása adódik.

5.5.11 Alkalmazzunk az 5.5.5 Tétel (B) részének bizonyításához hasonló gondolatmenetet (természetesen most fordított irányú egyenlőtlenségekről van szó). Az egyetlen lényeges eltérést az jelenti, hogy $p_j < N$ miatt $\log p_j > \log N$ nem teljesül (erre a (15) megfelelőjénél lenne szükség). Ezen például az alábbi módon segíthetünk: Ha $N > p_j > N/(\log N)^2$, akkor elég nagy N-re $\log p_j > (1-\varepsilon')\log N$. Ezért a (13)-nak megfelelő egyenlőtlenségeket ezekre a prímekre érdemes felírni és összegezni.

5.6.

5.6.1 Divergens: a), c), e).
Az egyes sorozatokat jelölje rendre $A, B, \dots, F$, az n-nél nem nagyobb elemek számát pedig rendre $A(n), B(n), \dots, F(n)$. Ekkor

$$A(n) \sim c_1 n; \qquad B(n) \sim \sqrt{n}; \qquad E(n) \sim c_2 n; \qquad F(n) \sim c_3\sqrt{n}\,,$$

ahol a c_i-k alkalmas pozitív konstansok (amelyek a c_3 kivételével függnek L-től). A D sorozatra

$$D(n) \sim c_4(\log n)^k$$

teljesül, ahol k az L-nél kisebb prímek száma; itt lényegesen egyszerűbb annak a gyengébb eredménynek az igazolása, hogy

$$c_5(\log n)^k < D(n) < c_6(\log n)^k\,.$$

5.6.2 Csak c) divergens. — A megfelelő integrálok:

$$\text{a)}\ \int \frac{dx}{x^{1,01}} = \frac{-100}{x^{0,01}}\,; \qquad \text{b)}\ \int \frac{dx}{x(\log x)^2} = \frac{-1}{\log x}\,;$$

$$\text{c)}\ \int \frac{dx}{x\cdot\log x\cdot\log\log x} = \log\log\log x\,.$$

5.6.3 Divergens: b). — Az 5.6.1 Tétel első bizonyításához hasonló gondolatmenetet érdemes alkalmazni.

5.6.4

a) Konvergens: rendezzük át a számokat a legkisebb prímosztóik szerint (ezek a feltétel szerint mind különbözők), ekkor $a_n \geq p_n^2$, tehát

$$\sum_{n=1}^{\infty} \frac{1}{a_n} \leq \sum_{n=1}^{\infty} \frac{1}{p_n^2} < \infty\,.$$

b) Konvergens: A feltétel alapján $a_n \geq 2^{2\log n} = n^{2\log 2}$. Mivel $\alpha = 2\log 2 > 1$, ezért

$$\sum_{n=1}^{\infty} \frac{1}{a_n} \leq \sum_{n=1}^{\infty} \frac{1}{n^{\alpha}} < \infty\,.$$

c) Divergens: elég nagy n-re $a_n < cn$, ahol $c = 10^{1001}$.

d) Lehet konvergens, és lehet divergens.

e) Konvergens: Rendezzük át a számokat az osztóik száma szerint, ekkor a feltétel szerint $d(a_n) \geq n$. Az 1.6.11c feladat alapján ebből $n \leq 2\sqrt{a_n}$, azaz $a_n \geq n^2/4$ következik. Ezután használjuk fel, hogy a négyzetszámok reciprokösszege konvergens.

5.6.5 Nem érdemes; az összeg nagyságát aránytalanul befolyásolhatja az első néhány tag. Például, ha a köbszámokhoz hozzávesszük a 2-t és a 3-at, akkor a reciprokösszeg már nagyobb lesz a négyzetszámok reciprokösszegénél, ugyanakkor a köbszámok lényegesen gyorsabban nőnek, mint a négyzetszámok, tehát a köbszámok(nak a 2-vel és a 3-mal kibővített) sorozata ritkább a négyzetszámokénál.

5.6.6 Az 5.6.1 Tétel harmadik bizonyításához hasonló gondolatmenetet érdemes alkalmazni.

5.6.7 Ha az a_j sorozat nem tart 0-hoz, akkor könnyen adódik, hogy a végtelen sor divergens, a végtelen szorzat pedig 0. Ezért a továbbiakban feltehetjük, hogy az a_j sorozat 0-hoz tart. A végtelen szorzat logaritmusát véve kapjuk, hogy

$$\prod_{j=1}^{\infty}(1-a_j) = 0 \iff \sum_{j=1}^{\infty} -\log(1-a_j) = \infty\,.$$

Használjuk fel, hogy $0 < a_j < 1/2$ esetén $a_j < -\log(1-a_j) < 2a_j$.

5.6.8 A bizonyítandó egyenlőtlenséggel ekvivalens, ha a két oldal logaritmusára igazoljuk a megfelelő egyenlőtlenséget. Ehhez használjuk fel az 5.6.2 Tételt és azt, hogy $0 < a \leq 1/2$ esetén $-\log(1-a)$ jól közelíthető a-val.

5.6.9

a) Divergens: az $n = 2p$ alakú számokra $np(n) = 4p$, és már a $\sum_p 1/(4p)$ sor is divergens.

b) Konvergens. — Legyen q rögzített prímszám és S_q azon n egészek reciprokösszege, amelyekre $P(n) = q$. Mutassuk meg, hogy

$$S_q = \frac{1}{q} \prod_{p \leq q} \frac{1}{1 - \frac{1}{p}} \,.$$

Az 5.6.8 feladat alapján ekkor $S_q < c(\log q)/q$. Innen kapjuk, hogy

$$\sum_{n=2}^{\infty} \frac{1}{nP(n)} = \sum_q \frac{S_q}{q} < c \sum_q \frac{\log q}{q^2} < \infty \,.$$

5.7.

5.7.1

a) Az algoritmusban szerepel az $r_k = r_{k+1}q_{k+2} + r_{k+2}$ lépés. Itt a jobb oldal első tagjában szereplő szorzatot $r_{k+1} > r_{k+2}$ és $q_{k+2} \geq 1$ felhasználásával csökkentve a kívánt $r_k > 2r_{k+2}$ egyenlőtlenség adódik.

b) $2 \log_2 b$.

c) A legkisebb b-hez akkor jutunk, ha $(a, b) = r_{s-1} = 1$ és a q_i hányadosok a lehető legkisebbek, azaz $q_s = 2$, a többi q_i pedig 1. Ekkor az algoritmus egyenlőségei a végéről kezdve a következő alakot öltik:

$$r_{s-1} = 1,\ r_{s-2} = 2,\ r_{s-3} = r_{s-2} + r_{s-1},\ \ldots,\ b = r_1 + r_2,$$

ahonnan a Fibonacci-számok képzési szabálya szerint $r_{s-j} = \varphi_{j+1}$, és $b = \varphi_{s+1}$.

5.7.2 Az eljárás során a „számláló” és a „nevező” legnagyobb közös osztója nem változik (még a „számláló” felezésekor sem, hiszen a „nevező” és így a legnagyobb közös osztó is páratlan). Az eljárás euklideszi algoritmus jellege miatt végül el kell jutnunk $(a, b) = d$-hez. Ez a d érték a „számlálóba” kerül, hiszen az egyes lépések végén ott jelennek meg az új számok. Ekkor a v „nevezőre” $(d, v) = (a, b) = d$ teljesül, tehát $d \mid v$.

5.7.3 $341 = 11 \cdot 31$. Ekkor

$$\varphi(11) \mid 340 \Rightarrow 2^{340} \equiv 1 \pmod{11}, \quad \text{és}$$
$$2^5 \equiv 1 \pmod{31} \Rightarrow 2^{340} \equiv 1 \pmod{31}.$$

Ebből következik, hogy $2^{340} \equiv 1 \pmod{11 \cdot 31}$, vagyis a 341 kettes alapú álprím. Ugyanakkor

$$3^{340} \equiv 3^{10} \not\equiv 1 \pmod{31} \Rightarrow 3^{340} \not\equiv 1 \pmod{341},$$

tehát a 341 nem hármas alapú álprím.

5.7.5 Mivel p páratlan, ezért

$$n = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1} =$$
$$= (a^{p-1} + a^{p-2} + \ldots + 1)(a^{p-1} - a^{p-2} + \ldots + 1),$$

ahonnan kapjuk, hogy n páratlan és összetett. Az $a^{n-1} \equiv 1 \pmod{n}$ kongruencia abból következik, hogy $a^{2p} \equiv 1 \pmod{n}$ és $n \equiv 1 \pmod{2p}$; ez utóbbi az $n(a^2 - 1) = a^{2p} - 1$ egyenlőség modulo p vizsgálatából és n páratlanságából adódik.

5.7.6 $561 = 3 \cdot 11 \cdot 17$. Így $(a, 561) = 1 \Longrightarrow a^{560} \equiv 1 \pmod{561}$ igazolásához elég belátni a kongruencia fennállását a 3, a 11 és a 17 modulusokra, ez pedig a kis Fermat-tétel felhasználásával könnyen adódik.

5.7.7 (a)⇒(b): Ha n nem négyzetmentes, akkor az 5.7.4 Tétel bizonyításának idevágó részét követve (de az ottani (2) képletet értelemszerűen kihagyva) ellentmondásra jutunk. Ha $p \mid n$, akkor vegyünk egy olyan g primitív gyököt mod p, amely relatív prím n-hez (ez utóbbi feltétel teljesülését az 5.7.4 Tétel bizonyításában többször alkalmazott szimultán kongruenciarendszeres eljárással biztosíthatjuk). Ekkor

$$(g, n) = 1 \Longrightarrow g^{n-1} \equiv 1 \pmod{n} \Longrightarrow$$
$$\Longrightarrow g^{n-1} \equiv 1 \pmod{p} \Longrightarrow o_p(g) = p - 1 \mid n - 1.$$

(b)⇒(c): Mivel n négyzetmentes, ezért elég az n minden p prímosztójára igazolni az $a^n \equiv a \pmod{p}$ kongruenciát. Ha $p \mid a$, akkor ez nyilvánvalóan teljesül, ha pedig $(p, a) = 1$, akkor a kis Fermat-tétel és $p - 1 \mid n - 1$ alapján $a^{n-1} \equiv 1 \pmod{p}$, amiből a bizonyítandó kongruencia a-val való szorzással adódik.

(c)⇒(a): Ha $(a,n)=1$, akkor az $a^n \equiv a \pmod{n}$ kongruenciát a-val egyszerűsítve kapjuk, hogy $a^{n-1} \equiv 1 \pmod{n}$.

5.7.8 Használjuk fel az 5.7.7 feladat b) feltételét.

5.7.9

a) Ha véletlenül $1 < (a,n) < n$ adódik, akkor ezzel nemcsak n összetettségét igazoltuk, hanem sikerült az n egy nemtriviális osztóját is előállítanunk. (Ennek azonban igen kicsi az esélye, lásd a b) részt.)

b) Nagyjából 10^{-100}.

5.7.10 Ekkor $(a-1,n)$ [illetve $(a+1,n)$] egy nemtriviális osztó.

5.7.11 Először egy prímteszttel megállapítjuk, hogy az n prím-e. Nyilván elég azzal az esettel foglalkoznunk, amikor n páratlan összetett szám.

Először egy gyors algoritmussal meg tudjuk állapítani, hogy n teljes hatvány-e: megvizsgáljuk, hogy $\sqrt[k]{n}$ egész szám-e, ahol $2 \le k \le \log_2 n$. Ha $n = m^k$, akkor elég m-et faktorizálnunk. A feladat feltétele m-re is teljesül, hiszen $\varphi(m) \mid \varphi(n)$ miatt a $\varphi(n)$ általunk ismert többszöröse a $\varphi(m)$-nek is többszöröse. Így a továbbiakban feltehetjük, hogy az n nem teljes hatvány.

Válasszunk (mondjuk) 1000 véletlen $n \nmid a$ értéket, és számítsuk ki (a,n)-et. Ha $(a,n) > 1$, akkor az 5.7.9 feladat alapján az n-et két nemtriviális osztója szorzatára tudjuk bontani.

Ha $(a,n) = 1$, akkor tekintsük az 5.7.5 Tétel alapötletéhez hasonlóan az

$$a^e,\ a^{\frac{e}{2}},\ a^{\frac{e}{4}},\ \ldots$$

sorozatot, ahol e-ről tudjuk, hogy osztható $\varphi(n)$-nel. Az első elem modulo n maradéka az Euler–Fermat-tétel szerint 1. Az 5.7.5 Tétel bizonyításának „négyzetmentes” részében tulajdonképpen csak azt használtuk ki, hogy az n nem prímhatvány, ennek mintájára most is megmutatható, hogy egy modulo n redukált maradékrendszer elemeinek legalább a felére a maradékok sorozata olyan, hogy valahány 1 után egy ± 1-től különböző maradék következik. Ekkor az 5.7.10 feladat alapján az n-et fel tudjuk bontani.

Ha $n = n_1 n_2$, ahol $n_i > 1$, akkor ismételjük meg az egész eljárást n_1-re és n_2-re ($\varphi(n_i) \mid \varphi(n)$ miatt ugyanaz az e továbbra is használható), majd hasonlóan folytassuk mindaddig, amíg megkapjuk az n prímtényezős felbontását. Mivel a prímtényezők száma legfeljebb $\log_2 n$, és minden egyes szorzatra bontás lépésszámigénye legfeljebb $c \log_2 n$, ezért a kanonikus alakot legfeljebb $c(\log_2 n)^2$ lépésben megkapjuk, ahol c alkalmas konstans.

5.7.12 Nem alkalmas, ugyanis nem ismerünk gyors algoritmust a faktoriálisok, illetve ezek osztási maradékainak meghatározására.

5.7.13

a) Kövessük az 5.7.4 Tétel bizonyításának azt a részét, amikor azt igazoltuk, hogy ha van tanú, akkor legalább annyi tanú van, mint cinkos.

b) Legyen $n > 1$ páratlan szám. Válasszunk (mondjuk) 1000 véletlen $a \not\equiv 0 \pmod{n}$ értéket, és mindegyikre vizsgáljuk meg, hogy $a^{n-1} \equiv 1 \pmod{n}$ teljesül-e. Ha legalább egy esetben nem teljesül, akkor az n biztosan összetett. Ha mind az 1000 esetben teljesül, akkor 2^{-1000}-nél kisebb annak a valószínűsége, hogy az n nem prím és nem univerzális álprím.

5.7.14 Jelölje R a kipróbált a-k számát. Ha n prím, akkor mindig ± 1 maradékot kapunk, és 2^{-R} a valószínűsége annak, hogy minden maradék 1. (Ennél a tesztnél tehát a „másik irányban" is tévedhetünk, azaz egy prímet is tévesen összetett számnak vélhetünk.) Ha n összetett, akkor az 5.7.4 és 5.7.5 Tételek bizonyításához hasonlóan járhatunk el.

5.7.15 Módosítsuk értelemszerűen az 5.2.3 feladat útmutatásánál szereplő gondolatmenetet.

5.7.16

a) Lássuk be, hogy $o_n(a) = n - 1$.

b) Legyen $n - 1$ kanonikus alakja

$$n - 1 = p_1^{\beta_1} \dots p_r^{\beta_r} .$$

A feltétel alapján $p_i^{\beta_i} \mid o_n(a_i)$. Ekkor (pl. a 3.2.4c feladat szerint) léteznek olyan b_i számok, amelyekre $o_n(b_i) = p_i^{\beta_i}$, ahonnan a 3.2.15a feladat alapján kapjuk, hogy $o_n(b_1 \dots b_r) = n - 1$.

c) Tegyük fel indirekt, hogy n összetett, ekkor létezik egy $q \le \sqrt{n}$ prímosztója. Ezután ismételjük meg a b) rész gondolatmenetét az n helyett a q modulusra. Azt kapjuk, hogy van olyan b, amelyre $o_q(b) = c > \sqrt{n} \ge q$, ami ellentmondás.

5.7.17 Azt kell igazolni, hogy ha egy a-ra jó sorozatot kapunk, akkor

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n} \qquad (*)$$

is teljesül.

Ha $a^r \equiv 1 \pmod{n}$, akkor könnyen adódik, hogy (*) mindkét oldalán 1 áll.

Rátérve az $a^{2^j r} \equiv -1 \pmod{n}$ esetre, az $a^{(n-1)/2}$ maradékának a meghatározása most sem jelent nehézséget. Ezután mutassuk meg, hogy ha q az n prímosztója, akkor $o_q(a)$ a 2^{j+1}-nek páratlan többszöröse, és így $2^{j+1} \mid q-1$ is teljesül. Ezek alapján bizonyítsuk be, hogy $\left(\frac{a}{q}\right)$ értéke $(q-1)/2^{j+1}$ paritásától függ, majd az n kanonikus alakjának segítségével írjuk fel $\left(\frac{a}{n}\right)$ értékét. Végül, ha az n kanonikus alakjában a q prímek helyére beírjuk a $2^{j+1} \mid q-1$ feltételből adódó alakot, akkor a beszorzást elvégezve és egy alkalmas kettőhatvány szerinti oszthatóságot vizsgálva megkapjuk, hogy $\left(\frac{a}{n}\right)$ valóban a (*)-nak megfelelő értéket veszi fel.

5.8.

5.8.1 Ekkor ez egy aláírás nélküli, névtelen levél, amelyet akár egy harmadik fél is hamisíthatott A nevében.

5.8.2 T invertálhatósága azt jelenti, hogy az $r^t \equiv s \pmod{N}$ kongruenciának bármely s esetén (r-ben) pontosan egy megoldása van. Ez a kongruencia ekvivalens az

$$r^t \equiv s \pmod{p}, \qquad r^t \equiv s \pmod{q} \tag{1}$$

szimultán kongruenciarendszerrel. Az (1)-beli két kongruenciának a 3.5.7 feladat szerint akkor és csak akkor van minden s-re pontosan egy megoldása, ha $(t, p-1) = (t, q-1) = 1$, azaz ha $(t\,,\, \varphi(N)) = 1$.

5.8.3

a) Elég megmutatni, hogy a szóban forgó kongruencia mod p és mod q is fennáll. Nézzük például mod p. Ha $p \mid r$, akkor mindkét oldal 0-val kongruens, ha pedig $(p, r) = 1$, akkor

$$r^{1+k\varphi(N)} \equiv r\big(r^{p-1}\big)^{k(q-1)} \equiv r \cdot 1 = r \pmod{p}\,.$$

b) $v \equiv 1 \pmod{[p-1, q-1]}$.

5.8.4 Nem okoz gondot, hiszen csak azt használjuk fel, hogy az $r^p \equiv r \pmod{p}$ kongruencia minden r-re teljesül (lásd az 5.8.3a feladatot). Természetesen ekkor a $\varphi(N)$-nek vélt $(p-1)(q-1)$ szorzat valójában nem $\varphi(N)$.

5.8.5 Legyen $s \equiv r^t \pmod{N}$, ahol s és t ismert, és r értékét szeretnénk meghatározni. Emeljük s-et a t-edik hatványra, majd az eredményt megint a t-edik hatványra stb., amíg ismét s-sel kongruens számot nem kapunk:

$$s^{t^k} \equiv s \pmod{N}\,. \tag{2}$$

Mivel $(t, \varphi(N)) = 1$, ezért az 5.8.2 feladat szerint a (2) kongruenciából lehet t-edik gyököt vonni, azaz

$$s^{t^{k-1}} \equiv r \pmod{N}.$$

Ez azt jelenti, hogy ha (2) elég kis k-ra bekövetkezik, akkor r-et meg tudjuk határozni. Ha $t^k \equiv 1 \pmod{\varphi(N)}$, akkor az 5.8.3a feladat szerint (2) biztosan teljesül, ezért nem szabad, hogy a t modulo $\varphi(N)$ vett rendje kicsi legyen.

5.8.6 Az A, illetve B a

$$g^{k_A k_B} = (g^{k_B})^{k_A} = (g^{k_A})^{k_B}$$

egyenlőségek alapján tudja a megadott értéket kiszámítani. Más ezt (remélhetőleg) nem tudja megcsinálni, hiszen nem ismeri k_A és k_B egyikét sem.

5.8.7

a) Tegyük fel indirekt, hogy két részösszeg egyenlő. A közös tagokat kiejtve elérhetjük, hogy a két összegben együttvéve is csupa különböző tag szerepeljen. Ekkor az előforduló legnagyobb tag a (6) feltétel szerint egymagában is nagyobb már, mint a teljes másik összeg, ami ellentmondás.

b) Tegyük fel indirekt, hogy bizonyos d_i-kre és d_j-kre $\sum d_i = \sum d_j$. Ekkor (7) alapján $\sum rc_i \equiv \sum rc_j \pmod{m}$. Az $(r, m) = 1$ feltétel miatt r-rel egyszerűsíthetünk, azaz $\sum c_i \equiv \sum c_j \pmod{m}$. Végül, mivel $m > \sum_{i=0}^{k-1} c_i$, ezért a kongruencia helyett egyenlőség is írható, ami ellentmond C összeginjektivitásának.

c) Közvetlenül következik az összeginjektivitás definíciójából.

d) Az u előállításához a δ_i értékekre van szükség, vagyis arra, hogy a megadott v az összeginjektív sorozat mely tagjainak az összege. A (6) sorozatnál ehhez alkalmazzuk a mohó algoritmust, azaz vegyük mindig a lehető legnagyobb c_i-t. A (7) sorozatnál az $rx \equiv d_i$, illetve $rx \equiv v \pmod{m}$ kongruenciák legkisebb pozitív megoldásai megadják a c_i-ket és a megfelelő v'-t, amelyekre már alkalmazhatjuk az előző eljárást.

6. Számelméleti függvények

6.1.

6.1.1 A multiplikativitás igazolásához alkalmazzuk a $d(n)$ függvény képletét (1.6.3 Tétel), vagy használjuk fel az 1.6.5a-b feladatot. A teljes multiplikativitás cáfolásához elég egyetlen olyan a, b számpár, amelyre $d(ab) \neq \neq d(a)d(b)$ és $(a, b) \neq 1$.

6.1.2

a), c) $f(n)$ és $h(n)$ se nem additív, se nem multiplikatív.
b) $g(n)$ teljesen multiplikatív.
d) $k(n)$ additív, de nem teljesen additív.

6.1.3 Multiplikatív h nem létezik. A feltételek alapján

$$0 = h(6) = h(2)h(3) \Rightarrow h(10)h(15) = h(2)h(5)h(3)h(5) = 0 \neq 3\,.$$

Additív, sőt teljesen additív h viszont végtelen sok létezik. A feltételekből adódó

$$0 = h(2) + h(3), \qquad 1 = h(2) + h(5), \qquad 3 = h(3) + h(5)$$

egyenletrendszert megoldva $h(2) = -1$, $h(3) = 1$ és $h(5) = 2$. Válasszuk $h(7)$ értékét egy c paraméternek, a többi p prímre pedig legyen $h(p) = 0$, ekkor egyértelműen meghatározható a h teljesen additív függvény, amely ezeket a feltételeket kielégíti: Ha

$$n = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}7^{\alpha_4}t, \quad \text{ahol} \quad (t, 210) = 1 \quad \text{és} \quad \alpha_i \geq 0, \;\; i = 1, 2, 3, 4,$$

akkor

$$h(n) = -\alpha_1 + \alpha_2 + 2\alpha_3 + c\alpha_4\,.$$

6.1.4 Ha van ilyen $f \neq 0$ multiplikatív függvény, akkor a 6.1.6 Tétel szerint $f(1) = 1$, továbbá ha az n kanonikus alakjában szereplő prímhatványok $q_j, \ldots, q_w$, akkor a 6.1.7 Tétel alapján csak $f(n) = c_j \ldots c_w$ lehetséges. Az ily módon a c_i-k segítségével definiált függvényről mutassuk meg, hogy valóban multiplikatív. Az additív esetben és a b) résznél is hasonlóan kell eljárni.

6.1.5 Igaz: a), d).

6.1.6

a) A szükséges és elégséges feltétel $f(k) = 0$.

b) Most is $f(k) = 0$ a szükséges és elégséges feltétel. Az elégségesség bizonyításához vegyük a, b és k kanonikus alakját, és a 6.1.7 Tétel alapján írjuk fel $g(a) = f(ka)$, $g(b) = f(kb)$ és $g(ab) = f(kab)$ értékét. Használjuk fel, hogy $(a, b) = 1$ miatt a k bármely prímosztója az a és b közül legfeljebb az egyiket osztja.

c) A teljesen multiplikatív esetben $f(k) = 1$ vagy 0 a szükséges és elégséges feltétel. A multiplikatív esetben ez csak szükséges, de nem elégséges: legyen például

$$f(n) = \begin{cases} 0, & \text{ha } n \equiv 4 \pmod 8; \\ 1, & \text{egyébként,} \end{cases} \qquad \text{és} \qquad k = 4,$$

ekkor $f(k) = 0$, de g nem multiplikatív, pl. $g(3)g(2) = 0 \neq 1 = g(6)$. Szükséges és elégséges feltétel: $f(k) = 1$ vagy $f(kn) = 0$ minden n-re (ez utóbbi a $g = 0$ függvényt jelenti).

6.1.7

a) Használjuk fel az $ab = (a, b)[a, b]$ összefüggést.

b) Használjuk fel a számok kanonikus alakját.

c) Azok az f-ek, amelyek előállnak egy additív és egy konstans függvény összegeként.

d) A szóban forgó egyenlőséget a multiplikatív függvények konstansszorosai mindig kielégítik. Ha feltesszük, hogy $f(1) \neq 0$, akkor ezek adják az összes megoldást. Az általános esetben az összes megoldást az alábbi függvények szolgáltatják:

$$f(n) = \begin{cases} 0, & \text{ha } K \nmid n; \\ cg\left(\frac{n}{K}\right), & \text{ha } K \mid n, \end{cases}$$

ahol $g(n)$ multiplikatív, c konstans és K rögzített pozitív egész.

6.1.8 Az állítás a multiplikativitás és additivitás definíciójának közvetlen következménye.

6.1.9

a), e) Azonnal következik a definíciókból.

b)–d) Először mutassuk meg, hogy az fg szorzat akkor és csak akkor teljesen additív, illetve additív, ha $f(a)g(b) + f(b)g(a) = 0$ minden a, b, illetve minden relatív prím a, b esetén teljesül. — Válasz d)-re: Ha $f \neq 0$ és $g \neq 0$, akkor f és g egy vagy két prím hatványaitól eltekintve minden prímhatvány helyen 0, és a második esetben az adott két prím hatványain felvett függvényértékekre is szoros szabályszerűség érvényes.

f) Következik a 6.1.6 Tételből.

6.1.10
a) Közvetlenül következik a definíciókból.
b) A feltétel átalakítható az $\big(f(a)-g(a)\big)\big(f(b)-g(b)\big)=0$ egyenlőséggé. A multiplikatív esetben a két függvény egy p prím hatványain esetleg eltérő értékű lehet, minden más prímhatvány helyen viszont azonos értéket kell felvenniük.

6.1.11 Ha $f=0$, akkor a feltétel alapján $g=0$ is igaz, és az állítás triviálisan teljesül. Egyébként az 1 helyen felvett függvényértékek alapján a két függvény összege csak az 1 konstans lehet. Az $f=1-g$ függvényre a multiplikativitást felírva a g additivitása alapján az adódik, hogy $(a,b)=1$ esetén $g(a)g(b)=0$. Ebből következik, hogy esetleg egy p prím hatványaitól eltekintve minden prímhatvány helyen a g értéke 0, az f értéke pedig 1, és így $p\nmid n$ esetén $g(n)=0$ és $f(n)=1$. Innen azonnal adódik, hogy $p\nmid n$ esetén $(f^{1000}+g^{1000})(n)=1$ és $(f^{1000}g^{1000})(n)=0$, amiből a kívánt multiplikativitás, illetve additivitás könnyen leolvasható.

6.1.12 A 6.1.9d feladat megoldásához hasonló gondolatmenetet érdemes alkalmazni. Most a következő egyenlőségekből lehet kiindulni:
a) Ha $h=f-g$, ahol f és g multiplikatív, akkor bármely $(a,b)=1$ esetén

$$\big(f(a)-1\big)\big(f(b)-1\big)=\big(g(a)-1\big)\big(g(b)-1\big)\,.$$

b) Ha $h=fg$, ahol f multiplikatív és g additív, akkor bármely $(a,b)=1$ esetén

$$f(a)g(a)\big(f(b)-1\big)+f(b)g(b)\big(f(a)-1\big)=0\,.$$

6.1.13
a) Mutassuk meg, hogy végtelen sok páronként relatív prím helyen a függvény értéke 0.
b) Legyen $f(1)=f(2)=1$ és $f(n)=0$, ha $n>2$.
c) Ha létezik végtelen sok különböző p prím és $\nu_p>0$, amelyre $f(p^{\nu_p})\neq 0$, akkor ezek segítségével az a) részhez hasonlóan megmutatható, hogy a függvény minden függvényértéket végtelen sok helyen vesz fel. Ezért csak véges sok ilyen p létezhet, és ekkor ezek maximuma megfelel K-nak.

6.1.14
a) Hamis. Ellenpélda: $f(n)=3$, ha $2\mid n$, de $4\nmid n$, és $f(n)=0$ egyébként. Ez az f additív, továbbá $f(4)+f(8)=f(32)$ is teljesül, de nem teljesen additív, mert pl. $f(2)+f(6)\neq f(12)$.
b) Igaz. Ha $(c,ab)=1$, akkor $(ca,b)\geq(a,b)>1$ és

$$f((ca)b)=f(c(ab))=f(c)+f(ab)=f(c)+f(a)+f(b)=f(ca)+f(b)\,.$$

c) Hamis. Ez más megfogalmazásban ugyanaz, mint az a) állítás.
d) Igaz. A bizonyítás a b)-nél látott módon történhet.
e) Hamis. Ellenpélda: $f(1) = f(2) = 1$ és $f(n) = 0$, ha $n > 2$.
Érdemes végiggondolni, miért változott meg a válasz a d)-hez képest: ott az $f(ab) \neq f(a) + f(b)$ egyenlőtlenséghez $f(c)$-t hozzáadva az egyenlőtlenség továbbra is érvényes marad, ezzel szemben ha e)-nél az $f(ab) \neq \neq f(a)f(b)$ egyenlőtlenséget $f(c) = 0$-val szorozzuk meg, akkor már egyenlőséget kapunk.

6.1.15 Eredmény: $\varphi_2(n) = n\prod_{p|n}(1 - 2/p)$ (ahol p prímet jelöl).
Útmutatás: Bizonyítsuk be, hogy $\varphi_2(n)$ multiplikatív, ehhez szimultán kongruenciarendszereket érdemes felhasználni. Ezután elég a függvény értékét a prímhatvány helyeken meghatározni.

6.1.16 Lássuk be, hogy a bal és a jobb oldalon álló függvény egyaránt multiplikatív (a bal oldali összegnél az előző feladathoz hasonló gondolatmenetet érdemes alkalmazni). Ennek alapján elég az egyenlőséget a prímhatvány helyeken igazolni.

6.2.

6.2.1 Legyen a, illetve b összes pozitív osztója $a_1, \ldots, a_r$, illetve $b_1, \ldots, b_s$. Az 1.6.5a-b feladat szerint $(a, b) = 1$ esetén az a_ib_j számok kiadják ab összes pozitív osztóját, és mindegyiket csak egyszer. Így

$$\sigma(ab) = \sum_{i=1}^{r}\sum_{j=1}^{s} a_ib_j = \Big(\sum_{i=1}^{r} a_i\Big)\Big(\sum_{j=1}^{s} b_j\Big) = \sigma(a)\sigma(b)\,.$$

Ezután a multiplikativitás alapján elég a σ-függvény értékét a prímhatvány helyeken meghatározni.

6.2.2 Használjuk fel a függvények képletét, vagy támaszkodjunk az 1.6.5a-c feladatra.

6.2.3 Mivel $3 \nmid n\varphi(n)$, ezért az n minden p prímosztója $3k - 1$ alakú. Legyen egy ilyen p kitevője az n kanonikus alakjában α. Ha α páratlan, akkor $\sigma(p^\alpha)$-ból kiemelhető $1 + p$, és így $\sigma(n)$ osztható 3-mal, ami ellentmond a feltételnek. Ezért minden p kitevője páros, tehát az n négyzetszám.

6.2.4 Legyen az n kanonikus alakja $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. Ekkor minden olyan k megfelel, amelyre

$$p_i^{\alpha_i+1} - 1 \mid p_i^{k\alpha_i+1} - 1, \quad i = 1, \ldots, r.$$

Ez teljesül, ha minden i-re

$$\alpha_i + 1 \mid k\alpha_i + 1, \quad \text{azaz} \quad \alpha_i + 1 \mid (k-1)\alpha_i\,.$$

Így biztosan megfelel, ha a $k-1$ tetszőleges közös többszöröse az $\alpha_i + 1$ számoknak.

6.2.5 Válasz: n. — Útmutatás: Az osztók reciprokösszegénél hozzunk közös nevezőre, és használjuk fel, hogy ha d végigfut az n osztóin, akkor n/d is végigfut az n osztóin.

6.2.6

a) Válasz: A négyzetszámok és a négyzetszámok kétszeresei. — Útmutatás: Használjuk fel a $\sigma(n)$ képletének törtmentes alakját. — Másik lehetőség: Legyen $n = 2^k t$, ahol t páratlan. A feladat szempontjából csak n páratlan osztói, azaz t osztói számítanak; azt kell megvizsgálni, mikor lesz $d(t)$ páratlan. Az 1.6.8 feladat szerint ez pontosan akkor teljesül, ha t négyzetszám.

b) Válasz: Különböző Mersenne-prímek szorzatai. — Útmutatás a szükségességhez: Legyen az n kanonikus alakja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Ekkor

$$2^k = \sigma(n) = \prod_{i=1}^{r} (1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i})\,.$$

Itt minden tényező maga is kettőhatvány, és így páros is, tehát minden $p_i > 2$ és mindegyik α_i páratlan. Ekkor $1 + p_i$ kiemelhető:

$$2^k = \prod_{i=1}^{r} (1 + p_i)(1 + p_i^2 + p_i^4 + \ldots + p_i^{\alpha_i - 1})\,.$$

A jobb oldalon minden tényező kettőhatvány, ezért p_i Mersenne-prím. Azt kell még igazolni, hogy $\alpha_i = 1$. Tegyük fel indirekt, hogy valamelyik $\alpha_i > 1$. Ekkor az $1 + p_i^2 + p_i^4 + \ldots + p_i^{\alpha_i - 1}$ tényezőből (annak párossága miatt) $1 + p_i^2$ kiemelhető, és $1 + p_i^2$ is kettőhatvány. Ez azonban nem lehetséges, mert $1 + p_i^2$ már 4-gyel sem osztható.

6.2.7 *Első megoldás*: $\sigma(n) \neq 2p$, ahol p egy $3k-1$ alakú páratlan prím.

Második megoldás: $\sigma(n) \neq 3^s$, ha $s > 1$.

Harmadik megoldás: Használjuk fel, hogy a σ-függvény „ritkán” vesz fel páratlan értéket.

Negyedik megoldás: Az $1, 2, \ldots, N$ értékeket a σ-függvény csak az $1, 2, \ldots, N$ helyek valamelyikén veheti fel. Mutassuk meg, hogy ezen $x \leq N$ helyek

közül is „sokszor”, mondjuk r esetben $\sigma(x) > N$. Ekkor a $\sigma(1), \dots, \sigma(N)$ függvényértékek közül legfeljebb $N - r$ darab lehet kisebb vagy egyenlő, mint N, vagyis az $1, 2, \dots, N$ számok közül legalább r darab nem szerepel a σ-függvény értékkészletében.

Ötödik megoldás: Mutassuk meg, hogy „sok” olyan $x_i \neq x_j$ pár van, amelyre $\sigma(x_i) = \sigma(x_j)$, majd alkalmazzunk a negyedik megoldáshoz hasonló gondolatmenetet.

6.2.8 Csak $n = 1$ felel meg.
Útmutatás: Lássuk be, hogy ha $n \geq 2$, akkor $n! < \sigma(n!) < (n+1)!$.

6.2.9 Használjuk fel, hogy $n = ab$ esetén a és b közül az egyik nagyobb vagy egyenlő, mint $\sqrt{n}$. — Egyenlőség pontosan akkor teljesül, ha az n egy prímszám négyzete.

6.2.10

a) (a1) n prím. (a2) Nincs megoldás. (a3) $n = 10,\ 49$.
(a4) $n = 21$.
b) Csak $c = 1$ esetén.
c) Ha $c = 2k + 1 > 7$ és $2k = p + q$, ahol p és q különböző prímek, akkor $n = pq$ megfelel.

6.2.11

a) (a1) n prím. (a2) Nincs megoldás. (a3) $n = 4$.
(a4) $n = 6$.
b) Csak $c = 2$ esetén.
c) $c = 4k$, ahol $k > 3$.

6.2.12

a) Végtelen sok. — Ha találunk egy megfelelő a_0, b_0 párt, és p az a_0 és b_0 közös prímosztója, akkor $a_k = a_0 p^k$, $b_k = b_0 p^k$ is megfelel. Kiindulásnak vehető például $a_0 = 6$, $b_0 = 8$ vagy $a_0 = 12$, $b_0 = 14$ stb.
b) Végtelen sok. — Ha n felírható $n = p_1 + p_2 = p_3 + p_4$ alakban, ahol a p_i számok különböző prímek, akkor $a = p_1 p_2$, $b = p_3 p_4$ megfelel. Az 5.4.7 feladathoz hasonlóan igazolható, hogy végtelen sok ilyen n létezik (azaz amelyik legalább kétféleképpen írható fel két különböző prímszám összegeként). — Megjegyezzük, hogy ugyanez a gondolatmenet az a) résznél is alkalmazható, ott azonban egyszerűbben is célhoz értünk.

6.2.13 Használjuk fel, hogy az 1-en és n-en kívül az n minden minden osztója legfeljebb $n/2$, illetve legalább 2.
Egyenlőség: a) $n = 1$ vagy prím; b) és c) $n = 4$ vagy prím.

6.2.14 Válasz: $n = 6$. — Útmutatás: Az előző feladat gondolatmenetét kell finomítani.

6.2.15

a) Használjuk fel az (a1) egyenlőtlenséghez a függvények képletét, az (a2)-höz pedig azt, hogy a $\varphi(n)$ az n bizonyos osztóinak előjeles összege. Mindkét esetben az egyenlőség pontosan akkor teljesül, ha n prím.

b) Mutassuk meg, hogy ha n kanonikus alakja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, akkor

$$\frac{\sigma(n)\varphi(n)}{n^2} = \prod_{i=1}^{r}\Big(1 - \frac{1}{p_i^{\alpha_i+1}}\Big) \geq \prod_{i=1}^{r}\Big(1 - \frac{1}{p_i^2}\Big)\,.$$

A (b1) állítás ebből $p_i \geq i+1$ alapján következik.
A (b2) állításhoz igazoljuk, hogy

$$\inf \frac{\sigma(n)\varphi(n)}{n^2} = \lim_{N\to\infty} \prod_{p\leq N}\Big(1 - \frac{1}{p^2}\Big)\,,$$

majd használjuk fel az 5.6.6 feladatot.

6.2.16 Legyen az n kanonikus alakja $n = 2^{\alpha} p_1^{\alpha_1} \dots p_r^{\alpha_r}$, ahol $p_i > 2$ (itt $\alpha = 0$, illetve $r = 0$ is lehet). Mutassuk meg, hogy minden $\alpha_i = 1$, $\alpha \leq 2$ és $r \leq 1$. Ebből következik, hogy $n = 1, 2, 4, p, 2p$ vagy $4p$, ahol p páratlan prím. Ezeket behelyettesítve könnyen igazolható, hogy csak a megadott n értékek teljesítik a feltételt.

6.2.17 Mindkét függvény csak a 0 és ± 1 értékeket veszi fel.

6.2.18

a) 3. — Útmutatás: Négy egymást követő egész szám közül valamelyik osztható 4-gyel.

b) Akármilyen sok. — Útmutatás: Lásd a 2.6.11 feladatot.

6.2.19 Legyen az n-edik primitív egységgyökök összege $S(n)$. Elég belátni, hogy $S(n)$ multiplikatív, továbbá $S(p^{\alpha}) = \mu(p^{\alpha})$ bármely p^{α} prímhatványra. Az $S(n)$ multiplikativitásához mutassuk meg, hogy $(a, b) = 1$ esetén egy a-adik és egy b-edik primitív egységgyök szorzata ab-edik primitív egységgyök, és minden ab-edik primitív egységgyök egyértelműen felírható ilyen szorzat alakban. — A feladat az összegzési és megfordítási függvények segítségével is megoldható, lásd a 6.5.9a feladatot.

6.2.20 0.

6.2.21

a) Használjuk fel a függvények képletét, vagy pedig azt, hogy az n osztói a multiplicitással számolt prímosztók bizonyos részhalmazainak felelnek

meg. — Ha n négyzetmentes, akkor mindkét helyen egyenlőség teljesül, egyébként pedig mindkét helyen szigorú egyenlőtlenség áll.

b) $k^{\omega(n)} \le d_k(n) \le k^{\Omega(n)}$.

6.2.22 Igaz: a).

6.2.23 Hasonlóan járhatunk el, mint a σ-függvény esetében, lásd a 6.2.2 Tételnek és a 6.2.8 Tétel σ-ra vonatkozó részének a bizonyítását, vagy pedig a 6.2.1 feladatot. Eredmény: Ha az n kanonikus alakja $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ és $\nu \neq 0$, akkor

$$\sigma_\nu(n) = \prod_{i=1}^{r}(1 + p_i^\nu + p_i^{2\nu} + \ldots + p_i^{\nu\alpha_i}) = \prod_{i=1}^{r} \frac{p_i^{\nu(\alpha_i+1)} - 1}{p_i^\nu - 1}\,.$$

6.3.

6.3.1 Használjuk fel a 6.3.2 Tételt.

6.3.2

a) Ha az n kanonikus alakja $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, akkor a $2n = \sigma(n)$ feltétel a

$$2\prod_{i=1}^{r} p_i^{\alpha_i} = \prod_{i=1}^{r}\left(1 + p_i + \ldots + p_i^{\alpha_i}\right) \tag{1}$$

egyenlőséget jelenti. Az (1) bal oldala a 2-nek pontosan az első hatványával osztható, ezért a jobb oldal tényezői közül az egyik 2-vel osztható, de 4-gyel már nem, a többi tényező pedig páratlan. Ez azt jelenti, hogy egyetlen α_i kitevő lesz páratlan és az ehhez tartozó p_i prím biztosan $4k+1$ alakú, a többi α_j kitevő pedig páros.

b) Az a) rész szerint $n = s^2p$, ahol p egy $4k+1$ alakú prím. Ebből azonnal következik, hogy $n \equiv 1 \pmod 4$. Ha $3 \mid s$, akkor $9 \mid n$, tehát $n \equiv 9 \pmod{36}$. Ha $3 \nmid s$, akkor $p \neq 3$ miatt $3 \nmid n$. Mivel p kitevője az n kanonikus alakjában páratlan, ezért $1+p \mid \sigma(n)$, és így $3 \nmid p+1$. Ez azt jelenti, hogy csak $p \equiv 1 \pmod 3$ lehetséges, tehát $n = s^2p \equiv 1 \pmod 3$. Az $n \equiv 1 \pmod 4$ kongruenciával együtt ebből azt kapjuk, hogy $n \equiv 1 \pmod{12}$.

6.3.3

a) A bizonyítandó $2p^\alpha > \sigma(p^\alpha)$ egyenlőtlenség ekvivalens átalakításokkal a $p^\alpha(p-2) > -1$ alakra hozható.

b)
$$\frac{\sigma(p^\alpha q^\beta)}{p^\alpha q^\beta} = \Big(1+\frac{1}{p}+\ldots+\frac{1}{p^\alpha}\Big)\Big(1+\frac{1}{q}+\ldots+\frac{1}{q^\beta}\Big) < \\ < \frac{p}{p-1}\cdot\frac{q}{q-1} \le \frac{3}{2}\cdot\frac{5}{4} < 2\,.$$

c) Példák bővelkedőre: legyen n kanonikus alakja $\prod_{i=1}^{k} p_i^{\alpha_i}$, ahol p_i az i-edik *páratlan* prímszám (tehát $p_1 = 3, p_2 = 5$ stb.) és $\alpha_1 \ge 3$, a többi α_i pedig tetszőleges pozitív egész.
Példák hiányosra: k darab olyan különböző q_i prím szorzata, amelyekre
$$1+\frac{1}{q_i} < \sqrt[k]{2}\,.$$

d) Mutassuk meg, hogy ha $a > 1$, akkor
$$\frac{\sigma(an)}{an} > \frac{\sigma(n)}{n}\,. \tag{2}$$
A (2)-t legegyszerűbben annak alapján igazolhatjuk, hogy ha n összes osztója $d_1, \ldots, d_t$, akkor az ad_i számok az an különböző osztói, és így $\sigma(an) > a\sigma(n)$. Másik két lehetőség, ha a σ képletét használjuk, illetve azt a tényt, hogy $\sigma(m)/m$ az m szám osztóinak a reciprokösszege.

e) Egy hiányos számot tetszőleges bővelkedő számmal megszorozva bővelkedő számot, egy elég nagy prímszámmal szorozva pedig hiányos számot kapunk.

6.3.4 A 6.2.6a feladat alapján egy ilyen szám csak $n = 2^\alpha t^2$ alakú lehet. Azt kell még igazolni, hogy $\alpha = 0$. A $\sigma(n) = 2n+1$ feltételt átalakítva
$$(2^{\alpha+1}-1)(\sigma(t^2)-t^2) = t^2+1 \tag{3}$$
adódik. Ha $\alpha \ge 1$, akkor (3) bal oldalának első tényezője $4k-1$ alakú, és így létezik $4k-1$ alakú prímosztója. Ez azonban ellentmond annak, hogy egy t^2+1 alakú számnak nem lehet $4k-1$ alakú prímosztója.

6.3.5

a) A 6.3.2 Tétel bizonyításához hasonló gondolatmenetet lehet alkalmazni.

b) Azt kell belátni, hogy ekkor $\sigma(n)$ is páratlan. Írjuk fel $\sigma(n)$-et $\sigma(n) = 2^v w$ alakban, ahol w páratlan, és mutassuk meg, hogy $v \ge 1$ esetén ellentmondásra jutunk.

c) Tegyük fel, hogy p^α szupertökéletes, és írjuk fel $\sigma(p^\alpha)$ kanonikus alakjának felhasználásával $\sigma(\sigma(p^\alpha))$ értékét.

6.3.6

a) Az n osztóinak harmonikus közepe

$$\frac{d(n)}{\sum_{d|n}\frac{1}{d}} = \frac{nd(n)}{\sigma(n)}\,.$$

b) Az a) rész alapján elég azt igazolni, hogy ha n tökéletes szám, akkor $d(n)$ páros, azaz n nem lehet négyzetszám. Ez valóban igaz, hiszen ha n négyzetszám, akkor $\sigma(n)$ páratlan, és így $\sigma(n) \neq 2n$.

c) Tegyük fel indirekt, hogy $1 + p + \ldots + p^\alpha \mid p^\alpha(\alpha + 1)$. Mivel $(1 + p + \ldots + p^\alpha, p^\alpha) = 1$, ezért $1 + p + \ldots + p^\alpha \mid \alpha + 1$. Ez azonban lehetetlen, hiszen $1 + p + \ldots + p^\alpha > \alpha + 1$.

d) Legyen $n = p_1 p_2 \ldots p_r$, ahol p_i prím és $p_1 < p_2 < \ldots < p_r$. Ha mindegyik p_i páratlan, akkor a

$$\frac{p_1 + 1}{2} \cdots \frac{p_r + 1}{2} \mid p_1 \ldots p_r$$

oszthatóság azért nem teljesülhet, mert $(p_1 + 1)/2$ a jobb oldal minden tényezőjéhez relatív prím.

Ha $p_1 = 2$, akkor szükségképpen $p_2 = 3$. Az $n = 6$ harmonikus szám, ha pedig az n-nek további prímtényezői is vannak, akkor az előző esethez hasonlóan juthatunk ellentmondásra.

6.3.7

a) Ha $a < b$ és $\sigma(a) = \sigma(b) = a + b$, akkor $\sigma(b) = a + b < 2b$ és $\sigma(a) = a + b > 2a$.

b) Tegyük fel indirekt, hogy $a = 2^k$ és b barátságos számpár. Ekkor

$$\sigma(2^k) = 2^{k+1} - 1 = \sigma(b) = 2^k + b,$$

ahonnan $b = 2^k - 1$, továbbá b és $\sigma(b)$ páratlansága miatt $b = u^2$. Az így adódó $2^k - 1 = u^2$ egyenlőség azonban már modulo 4 sem teljesülhet, ha $k \geq 2$.

6.4.

6.4.1 Az $\Omega(n)$-re vonatkozó völgytétel szó szerint a 6.4.1 Tétel mintájára bizonyítható, a $d_k(n)$ esetén annyit kell változtatni, hogy a szimultán kongruenciarendszer modulusai 2^{K+k} és 3^{K+k}, az $\omega(n)$-hez pedig két olyan relatív prím modulust érdemes választani, amelyek mindegyike $K + 2$ darab különböző prímszám szorzata.

A $\sigma(n)$ völgytételénél bármely elég nagy prím megfelel n-nek, hiszen ekkor $\sigma(n) = n + 1$, ugyanakkor $n + 1$ és $n - 1$ párossága miatt

$$\sigma(n-1) > (n-1) + \frac{n-1}{2} \quad \text{és} \quad \sigma(n+1) > (n+1) + \frac{n+1}{2}\,.$$

Ugyanígy bizonyítható a $\varphi(n)$-re vonatkozó hegytétel is.

A többi függvény hegytételénél és $\varphi(n)$ völgytételénél a 6.4.2 Tétel bizonyításához hasonlóan n-et az első r prímszám szorzatának érdemes választani.

A $d_k(n)$ és $\sigma(n)$ hegytétele, illetve a $\varphi(n)$ völgytétele a 6.4.2 Tétel bizonyításának értelemszerű módosításával igazolható.

Végül, az $\Omega(n)$ és $\omega(n)$ függvények esetén, a 6.4.2 Tétel bizonyításának a jelöléseivel élve, azt kell megmutatni, hogy $r-s > K$. Ez abból következik, hogy

$$n \le p_1 \dots p_{K+1} p_r^{r-K-1} < p_r^{r-K}\,,$$

ha r elég nagy, ugyanakkor

$$n + 1 = q_1 \dots q_s > p_r^s\,.$$

6.4.2 Kövessük a 6.4.5 Tétel bizonyításának gondolatmenetét.

6.4.3

a) Megfelel például, ha n az első 101 prím szorzatának elég nagy hatványa.

b) Legyen n az első r prímszám szorzata. Ekkor az 5.4 pont eredményei alapján

$$\log n \sim p_r \sim r \log r, \qquad \text{és így} \qquad r \sim \frac{\log n}{\log\log n}$$

adódik. Ebből $d(n) = 2^r$ miatt a feladatban megadott becslést kapjuk.

6.4.4 Legyen $\Omega(n) = s$, azaz $n = q_1 \dots q_s$, ahol $q_i = q_j$ is előfordulhat. Ekkor $q_i \ge 2$ miatt $n \ge 2^s$. — Egyenlőség pontosan akkor teljesül, ha n kettőhatvány.

6.4.5 Lássuk be, hogy adott r esetén az első r prímszám szorzata a legkisebb olyan n, amelyre $\omega(n) = r$. Ez azt jelenti, hogy $\omega(n)$ az n függvényében mért maximális nagyságrendjét az ilyen alakú számokon éri el. Ha n az első r prím szorzata, akkor 6.4.3b-hez hasonlóan kapjuk a feladat állításait.

6.4.6

a) Alkalmazzuk a 6.4.6 Tételt az $n^{0,99}/\varphi(n)$ függvényre, vagy használjuk fel a $d(n)\varphi(n) \ge n$ összefüggést és a 6.4.5 Tételt.

b) $\varphi(n) \geq \pi(n) - \omega(n)$.

c) Legyen n tetszőleges olyan egész, amelyre $\omega(n) = r$, és legyen n_r az első r prímszám szorzata. Mutassuk meg, hogy

$$\frac{\varphi(n)}{n} \geq \frac{\varphi(n_r)}{n_r} \qquad \text{és} \qquad \log\log n \geq \log\log n_r\,.$$

Ennek alapján az állítást elég az n_r számokra igazolni.

A prímszámok eloszlásáról tanult eredményeket felhasználva kapjuk, hogy

$$\log\left(\frac{\varphi(n_r)}{n_r}\right) = \log\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right) = \sum_{i=1}^{r}\log\left(1-\frac{1}{p_i}\right) \geq$$
$$\geq -\sum_{i=1}^{r}\frac{1}{p_i} - \sum_{i=1}^{r}\frac{1}{p_i^2} > -\sum_{p\leq p_r}\frac{1}{p} - 2 > -\log\log p_r - c - 2\,,$$

azaz

$$\frac{\varphi(n_r)}{n_r} > \frac{1}{c'\log p_r}\,.$$

Ezután vegyük figyelembe a $\log\log n_r \sim \log p_r$ összefüggést (ami $\log n_r \sim p_r$-ből a mindkét oldal végtelenhez tartása miatt jogos „logaritmálással" adódik).

d) Alkalmazzuk a 6.4.6 Tételt a $\sigma(n)/n^{1,01}$ függvényre, vagy használjuk fel a $\sigma(n) \leq nd(n)$ összefüggést és a 6.4.5 Tételt.

e) $\sigma(n)/n$ az n osztóinak a reciprokösszege, és így

$$\frac{\sigma(n)}{n} \leq \sum_{j=1}^{n}\frac{1}{j} \leq 1 + \log n\,.$$

f) A c) részhez hasonlóan kell bizonyítani.

Megjegyezzük, hogy a 6.2.15a feladat alapján a $\sigma(n)$-re vonatkozó állítások közvetlenül is következnek a $\varphi(n)$-re vonatkozó megfelelő állításokból (és a 6.2.15b feladat szerint ez fordítva is „majdnem" igaz).

6.4.7 Használjuk fel, hogy

a) $\lim\limits_{n\to\infty}\prod\limits_{p\leq n}\left(1-\frac{1}{p}\right) = 0$; b) $\lim\limits_{n\to\infty}\prod\limits_{p\leq n}\left(1+\frac{1}{p}\right) = \infty$.

6.4.8

a) Legyenek $v_1, v_2, \dots$ azok a prímek, amelyekre $k \mid v_i - 1$, és $B_r = v_1 \dots v_r$.
Ha $(n, B_r) > 1$, akkor az n osztható valamelyik v_i-vel, és így

$$k \mid v_i - 1 \mid \varphi(n)\,.$$

Ezek szerint $k \nmid \varphi(n)$ legfeljebb azokra az n-ekre fordulhat elő, amelyek a B_r-hez relatív prímek. Az ilyen n-ek száma N-ig nagy N esetén körülbelül

$$\frac{\varphi(B_r)}{B_r} N\,.$$

Így elég megmutatni, hogy bármely $\varepsilon > 0$-hoz található olyan r, hogy

$$\frac{\varphi(B_r)}{B_r} = \prod_{i=1}^{r} \left(1 - \frac{1}{v_i}\right) < \varepsilon\,.$$

Ez az 5.6.7 feladat alapján következik abból, hogy $\sum_{i=1}^{\infty} 1/v_i$ divergens.

b) Ha $\omega(n)$ nagy, akkor $\varphi(n)$ osztható a 2-nek egy nagy hatványával, tehát eleve kevés ilyen $\varphi(n)$ érték keletkezik. Ha $\omega(n)$ kicsi, akkor $\varphi(n) > cn$, ahol c (kis pozitív) konstans, és így ha $\varphi(n) \le N$, akkor $n < N/c$. De ezekre az n-ekre (is) az a) rész szerint $\varphi(n)$ majdnem mindig osztható egy előre megadott nagy k-val (ez a k lehet a már szerepelt kettőhatvány is), azaz ismét csak kevés $\varphi(n)$ érték keletkezhet.

6.4.9

a) A 6.4.8a feladathoz hasonlóan bizonyíthatunk. Legyenek $w_1, w_2, \dots$ azok a prímek, amelyekre $k \mid w_i + 1$, és legyen $C_r = w_1 \dots w_r$.
Ha az n valamelyik w_i-nek pontosan az első hatványával osztható, akkor

$$k \mid w_i + 1 \mid \sigma(n)\,.$$

Ezek szerint $k \nmid \sigma(n)$ legfeljebb azokra az n-ekre fordulhat elő, amelyek vagy relatív prímek C_r-hez, vagy pedig C_r valamelyik prímtényezőjének a négyzetével is oszthatók. Ezek az n-ek bizonyos maradékosztályokba esnek mod C_r^2. Az ilyen mod C_r^2 maradékosztályok számának és C_r^2-nek az aránya

$$\prod_{i=1}^{r} \left(1 - \frac{w_i - 1}{w_i^2}\right).$$

Mutassuk meg a 6.4.8a feladatban látott módon, hogy ez az arány tetszőlegesen kicsi lehet, ha r elég nagy.

b) Itt egyszerűbb a dolgunk, mint a $\varphi(n)$-nél volt, ugyanis $\sigma(n) \leq N$-ből következik, hogy $n \leq N$. Ennek megfelelően a $\varphi(n)$-nél látott bizonyításnak csak az utolsó lépésére van szükség: mivel $\sigma(n)$ majdnem mindig osztható egy előre megadott nagy k-val, ezért csak kevés $\sigma(n)$ érték keletkezhet.

6.5.

6.5.1 A $d_j(n)$ függvények definíciójából következik.

6.5.2

a) Tegyük fel, hogy f multiplikatív, és legyen $(a,b) = 1$. Az f^+ multiplikativitásának igazolásához felhasználjuk, hogy az 1.6.5a-b feladat szerint ab osztóit egyértelműen előállíthatjuk az a és a b egy-egy osztójának szorzataként (amelyek nyilván szintén relatív prímek). Ennek alapján

$$f^+(ab) = \sum_{d|ab} f(d) = \sum_{a_1|a, b_1|b} f(a_1 b_1) =$$
$$= \sum_{a_1|a, b_1|b} f(a_1) f(b_1) = \big(\sum_{a_1|a} f(a_1)\big)\big(\sum_{b_1|b} f(b_1)\big) = f^+(a) f^+(b)\,.$$

A megfordítást hasonló módon igazolhatjuk $n = ab$ szerinti teljes indukcióval vagy a Möbius-féle megfordítási formula felhasználásával.

b) Ha f helyére f^+-t írunk, akkor éppen az a)-beli állításhoz jutunk.

6.5.3

a) $f = 0$ és a 6.5.1 Definíció utáni példáknál definiált $e(n)$. — Útmutatás: Mutassuk meg, hogy egy p prímre $f^+(p^2) = \big(f^+(p)\big)^2$ csak $f(p) = 0$ esetén teljesülhet.

b) $f = 0$. — Útmutatás: Vizsgáljuk az f^+ függvény értékét rendre az alábbi helyeken: p_1p_2, p_1p_3, p_2p_3, $p_1^2p_2$, $p_1^3p_2$ stb., ahol p_1, p_2, p_3 különböző prímek, és olvassuk le ebből, hogy f értéke minden prímhatvány helyen nulla.

6.5.4

a) Használjuk fel a 6.5.2 feladatot.

b) Következik az a) részből és f teljes multiplikativitásából. Az $f(n) = n$ esetben $\sigma(n)$, illetve $\varphi(n)$ képletét nyerjük.

6.5.5

a) $\tilde{f}(n) = \begin{cases} c, & \text{ha } n = 1; \\ 0, & \text{ha } n > 1. \end{cases}$ b) $\tilde{g}(n) = \begin{cases} 1, & \text{ha } n = 2; \\ 0, & \text{ha } n \neq 2. \end{cases}$

c) $\tilde{\Omega}(n) = \begin{cases} 1, & \text{ha } n \text{ prímhatvány;} \\ 0, & \text{egyébként.} \end{cases}$ d) $\tilde{\omega}(n) = \begin{cases} 1, & \text{ha } n \text{ prím;} \\ 0, & \text{egyébként.} \end{cases}$

6.5.6 Legyen n kanonikus alakja $n = \prod_{i=1}^{r} p_i^{\alpha_i}$. Ekkor

$$f(n) = \sum_{i=1}^{r} f(p_i^{\alpha_i}) = \sum_{i=1}^{r} \sum_{\beta_i=0}^{\alpha_i} \tilde{f}(p_i^{\beta_i}) = \sum_{p^\beta \mid n} \tilde{f}(p^\beta)\,.$$

Innen $\tilde{f}$ egyértelműségéből következik, hogy ha k nem prímhatvány, akkor $\tilde{f}(k) = 0$.

6.5.7 A Möbius-féle megfordítási formula szerint ez az $f(n) = n$ függvény.

6.5.8 A Möbius-féle megfordítási formula szerint

$$\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}\,.$$

6.5.9

a) Jelöljük az összes n-edik egységgyök összegét $T(n)$-nel, az n-edik primitív egységgyökök összegét pedig $S(n)$-nel. Ekkor $S^+(n) = T(n) = e(n)$ miatt $S(n) = \mu(n)$. (Egy másik bizonyítást a 6.2.19 feladatban vázoltunk.)

b) Jelöljük az összes n-edik egységgyök, illetve az n-edik primitív egységgyökök k-adik hatványainak összegét $T_k(n)$-nel, illetve $S_k(n)$-nel. Ekkor $S_k(n) = \tilde{T}_k(n)$ és

$$T_k(n) = \begin{cases} n, & \text{ha } n \mid k; \\ 0, & \text{ha } n \nmid k. \end{cases}$$

Írjuk fel $S_k(n)$-et a Möbius-féle megfordítási formula segítségével, és használjuk fel a 6.5.8 feladatot is. — Másik lehetőség: Mivel $S_k(n)$ és a feladatban megadott függvény is multiplikatív, ezért elég az egyenlőségüket a prímhatvány helyeken igazolni.

c) Térjünk át a modulo p testre. Jelöljük az $x^k \equiv 1 \pmod{p}$ kongruencia megoldásainak összegét $V(k)$-val, a k-adrendű elemek összegét pedig $U(k)$-val. Mutassuk meg, hogy $U^+(n) = V(n)$, továbbá $d \mid p-1$ esetén

$V(d) = e(d)$. Ebből vezessük le, hogy $d \mid p-1$ esetén $U(d) = \mu(d)$, és így speciálisan $U(p-1) = \mu(p-1)$.

6.5.10 a) $\varphi(1)\varphi(2)\dots\varphi(n)$. b) $n!$. c) 1. d) 0.

6.5.11 A 6.5.4 Tétel bizonyítása átvihető erre az általános esetre is.

6.6.

6.6.1 $d_k(n)$.

6.6.2 Az összeadással közismerten minden rendben van, a szorzás szerepét betöltő konvolúcióra az asszociativitás, a kommutativitás és az egységelem létezése a 6.6.2 Tételből következik, és az

$$(f+g)*h = (f*h)+(g*h)$$

disztributivitás is könnyen ellenőrizhető (a „szorzás" kommutativitása miatt elég az egyik oldali disztributivitást igazolni). Nullosztómentesség: Lássuk be, hogy ha k, illetve m a legkisebb olyan pozitív egész, amelyre $f(k) \neq 0$, illetve $g(m) \neq 0$, akkor $(f*g)(km) \neq 0$.

6.6.3 Válasz: k. — Útmutatás: Írjuk fel minden n-re a $(g*g*\dots*g)(n) = f(n)$ egyenlőséget, ebből $n = 1$-re

$$g(1) = \sqrt[k]{f(1)}$$

adódik, majd $n = 2, 3, \dots$ esetén rendre egyértelműen meghatározhatók a $g(2), g(3), \dots$ függvényértékek.

6.6.4

a) A 6.5.2 feladat útmutatásához hasonló gondolatmenetet lehet alkalmazni.

b) Ha $f = 0$ vagy $g = 0$, akkor az állítás igaz, ezért a továbbiakban feltehetjük, hogy $f(1) = g(1) = 1$. Ha $f*g$ teljesen multiplikatív, akkor az

$$(f*g)(p^2) = \big((f*g)(p)\big)^2$$

egyenlőségből bármely p prímre $f(p)g(p) = 0$, és így f és g teljes multiplikativitása miatt minden $n > 1$-re is $f(n)g(n) = 0$ adódik. A megfordításhoz mutassuk meg, hogy az $f(p)g(p) = 0$ feltételből

$$(f*g)(p^k) = f(p^k) + g(p^k) = \big((f*g)(p)\big)^k$$

következik.

6.6.5 Az egyik lehetőség, ha kihasználjuk, hogy az egyenlőség mindkét oldalán multiplikatív függvény áll, így elég az egyenlőséget a prímhatvány helyeken igazolni. Elegánsabb azonban a konvolúció tulajdonságaira támaszkodni: Legyen $g(n) = n$, ekkor $\sigma * \varphi = (g * 1) * (\mu * g) = g * g$, tehát

$$\sum_{d|n} \sigma(d)\varphi(\frac{n}{d}) = (\sigma * \varphi)(n) = (g * g)(n) = \sum_{k|n} k \cdot \frac{n}{k} = nd(n)\,.$$

6.6.6

$$\sum_{n=1}^{\infty} \Big| \frac{f(n)}{n^s} \Big| = \sum_{n=1}^{\infty} \Big| \frac{f(n)}{n^{s_0}} \Big| \cdot \frac{1}{n^{s-s_0}} < c \sum_{n=1}^{\infty} \frac{1}{n^{s-s_0}} < \infty\,.$$

6.6.7 Alkalmazzuk a 6.6.4 Tételt.

6.6.8 Használjuk fel a 6.6.1 feladatot és a 6.6.4 Tételt.

6.6.9 Írjuk fel a σ, illetve μ függvényt összegzési, illetve megfordítási függvényként, és alkalmazzuk a 6.6.7 feladatot.

6.6.10

a) A jobb oldal definíció szerint a

$$\prod_{p \le N} (\sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}) \tag{1}$$

szorzat határértéke, ha $N \to \infty$. Az (1)-ben szereplő véges sok abszolút konvergens sor szorzását elvégezve a számelmélet alaptétele és f multiplikativitása miatt azokból az $f(n)/n^s$ értékekből álló $F_N(s)$ végtelen sort kapjuk, ahol az n minden prímosztója kisebb vagy egyenlő, mint N. Mivel az

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

sor abszolút konvergens, ezért

$$\lim_{N \to \infty} F_N(s) = F(s)\,.$$

b) Az f teljes multiplikativitása miatt

$$\frac{f(p^k)}{p^{ks}} = \Big(\frac{f(p)}{p^s}\Big)^k\,,$$

és így az a)-beli képlet jobb oldalán most végtelen mértani sorok állnak.

6.6.11 Az egyenlőség következik a ζ-függvény szorzat-előállításából és abból, hogy a μ-függvény $M(s)$ Dirichlet-sora a ζ-függvény reciproka. — Másik lehetőség: Alkalmazzuk a 6.6.10a feladatot az $f = \mu$ függvényre.

6.6.12

a) Válasz: $\pi^4/36$. — Útmutatás: Használjuk fel a 6.6.8a feladatot.

b) Válasz: $5\pi^4/72$. — Útmutatás: A $d^2(n)$ függvény $T(s)$ Dirichlet-sorát a 6.6.10a feladat alapján végtelen szorzattá alakítva, majd a szorzat tényezőiként fellépő végtelen sorokat kiszámítva lássuk be, hogy

$$T(s) = \frac{\zeta^4(s)}{\zeta(2s)}\,.$$

6.6.13 Válasz: $15/\pi^2$. — Útmutatás: Alkalmazzuk a 6.6.10a feladatot az $f = |\mu|$ függvényre, majd lássuk be, hogy az így kapott végtelen szorzat értéke $\zeta(s)/\zeta(2s)$.

6.6.14

a) $$\sum_{n=1}^{\infty} \frac{f(n)x^n}{1-x^n} = \sum_{n=1}^{\infty} f(n)\Big(\sum_{j=1}^{\infty} x^{jn}\Big) = \sum_{k=1}^{\infty} x^k \Big(\sum_{d|k} f(d)\Big) = \sum_{k=1}^{\infty} f^+(k)x^k\,.$$

b) Alkalmazzuk a feladat a) részét a μ, illetve φ függvényre és $x = 1/2$-re. Eredmény: (b1) $1/2$; (b2) 2.

6.7.

6.7.1 Válasz: 1. — Útmutatás: A 6.7.5 Tétel második bizonyításához hasonló meggondolásokkal kapjuk, hogy ez az összeg az $1, 2, \ldots, n$ egészek közül azoknak a számát határozza meg a logikai szitaformula segítségével, amelyek egyetlen prímmel sem oszthatók. Nyilván csak egyetlen ilyen pozitív egész van: az 1, tehát az összeg értéke 1. (A „tanulság”: időnként a dolgok elbonyolítása is hasznos lehet; most is az történt, hogy egy nyilvánvaló darabszámot bonyolult képlettel is meghatároztunk, és éppen ez tette lehetővé a bonyolult képlet egyszerű alakjának a megtalálását.) — Másik lehetőség: miután a választ (néhány n kipróbálása után) megsejtettük, az eredmény helyességét teljes indukcióval is igazolhatjuk.

6.7.2 Válasz: $6/\pi^2$. — Útmutatás: Jelölje $K(n)$ az $1, 2, \ldots, n$ egészek között a négyzetmentesek számát. A feladat ekkor a

$$\lim_{n\to\infty} \frac{K(n)}{n}$$

határérték vizsgálata. A 6.7.5 Tétel második bizonyításához hasonlóan a logikai szitaformula segítségével lássuk be, hogy

$$K(n) = \sum_{j \le \sqrt{n}} \mu(j) \left\lfloor \frac{n}{j^2} \right\rfloor .$$

Vegyük észre, hogy az egészrész elhagyásakor legfeljebb $\sqrt{n}$ nagyságú „hibatag" keletkezik, ami az

$$n \sum_{j \le \sqrt{n}} \frac{\mu(j)}{j^2}$$

„főtaghoz" képest elhanyagolható.

6.7.3

a) A 6.7.2 Tételt a $d_3 = d_2 * 1$ konvolúcióra alkalmazva

$$D_3(n) = \sum_{j=1}^{n} d(j) \left\lfloor \frac{n}{j} \right\rfloor$$

adódik. Az n-nel való osztás és az egészrész elhagyása után (a keletkező hibatagtól eltekintve) a

$$\sum_{j=1}^{n} \frac{d(j)}{j} \tag{1}$$

összeget kell megbecsülni. Ehhez felhasználjuk a $d(n)$ középértékére vonatkozó 6.4.3 Tételt. Az ottani jelölésekkel $d(j) = D(j) - D(j-1)$. Rendezzük át az (1) összeget ennek megfelelően, majd alkalmazzuk $D(j)$-re a 6.4.3 Tételt, ekkor hibatagoktól eltekintve a

$$\sum_{k=2}^{n} \frac{\log j}{j} \sim \int_2^n \frac{\log t}{t} dt \sim \frac{\log^2 n}{2}$$

eredményhez jutunk. Ne felejtsük el azt is megmutatni, hogy a hibatagok elhanyagolhatók ehhez a főtaghoz képest.

b) Kövessük a 6.7.3 Tétel bizonyításának gondolatmenetét. Legyen $f_\nu(n) = n^\nu$, és alkalmazzuk a 6.7.2 Tételt a $\sigma_\nu = 1 * f_\nu$ konvolúcióra, ekkor

$$\Sigma_\nu(n) = \sum_{j=1}^{n} \sum_{k=1}^{\lfloor \frac{n}{j} \rfloor} k^\nu$$

adódik. Ezután a jobb oldal k szerinti belső összegét becsüljük a szokásos módon az integrálkritériummal (lásd az 5.6.1 Tétel első bizonyítását, illetve az 5.6.2 feladatot).

6.7.4 Mivel a σ középértékfüggvénye „viszonylag kicsi", ezért az $1, 2, \dots, n$ számok között „sok" olyan i van, amelyre (például) $\sigma(i) \le 2n$. A 6.4.9 feladat alapján „kevés" ilyen $\sigma(i)$ érték van, ezért valamelyiket a függvénynek sok helyen fel kell vennie.

6.7.5

a) Az alsó becslés $\Omega(i) \ge \omega(i)$ miatt nyilvánvaló. A felső becsléshez írjuk be $\Omega(i)$ és $\omega(i)$ előállítását a megfordítási függvényeik segítségével (lásd a 6.5.5c-d feladatot), ekkor a szokásos összegátrendezéssel, majd az egészrészt elhagyva azt kapjuk, hogy

$$\sum_{i=1}^{n} \big(\Omega(i) - \omega(i)\big) < n \sum_{r \le n}{}' \frac{1}{r} \ ,$$

ahol $\sum'$-vel azt jelöljük, hogy csak azokra az r értékekre kell az összegzést végezni, amelyek a prímek egynél nagyobb kitevőjű hatványai. Az 5.6.1b feladat megoldásánál beláttuk, hogy ez az összeg kisebb 1-nél.

b) Ez az a) részből és az említett tételekből következik.

6.7.6 Használjuk fel a 6.2.21a feladatot, és alkalmazzuk a Hardy–Ramanujan-tételt ω-ra és (a 6.7.5b feladat alapján) Ω-ra.

6.7.7 A (meglepő) válasz: 0. — Útmutatás: Használjuk fel, hogy a Hardy–Ramanujan-tétel megfelelője érvényes Ω-ra is (lásd a 6.7.5b feladatot). Tegyük fel, hogy $i = ab$, ahol a és b kisebb, mint $\sqrt{n}$. Ekkor a „legtöbb esetben" $\Omega(a)$ és $\Omega(b)$ is „körülbelül"

$$\log\log\sqrt{n} \sim \log\log n \,,$$

és így $\Omega(i) \sim 2\log\log n$. Ilyen i azonban (ismét a 6.7.5b feladat szerint) csak kevés van.

6.7.8 A pontos tételt úgy kapjuk, ha a 6.7.7 Tételben az ω helyére az (előírt tulajdonságokkal rendelkező) f-et, a $\log\log i$ helyére pedig a

$$\sum_{p \le i} \frac{f(p)}{p}$$

értéket írjuk. A bizonyítás ugyanúgy történik, mint a 6.7.7 (és 6.7.7A) Tétel esetén.

6.8.

6.8.1 Rögzített m és $k = 1, 2, \ldots$ mellett az $f(m^k) = kf(m)$ számsorozat csak úgy lehet korlátos, ha $f(m) = 0$.

6.8.2 Legyen m rögzített, és tekinsük azokat a k pozitív egészeket, amelyekre $(k, m) = 1$. Ekkor $f(m) = f(km) - f(k)$. A Cauchy-féle konvergenciakritérium szerint bármilyen $\varepsilon > 0$ esetén elég nagy k mellett $|f(km) - f(k)| < \varepsilon$ teljesül, és így csak $f(m) = 0$ lehetséges.

6.8.3 Az alábbi függvények felelnek meg:

$$f = 0; \qquad g_c(n) = n^c; \qquad h_r(n) = \begin{cases} 1, & \text{ha } n = 1; \\ r, & \text{ha } n = 2; \\ 0, & \text{ha } n > 2, \end{cases}$$

ahol c tetszőleges valós szám és $0 \le r \le 1$.
Útmutatás: Ha a függvény mindenhol pozitív értéket vesz fel, akkor a logaritmusára alkalmazhatjuk a 6.8.1 Tételt, és így a fenti g_c függvényeket nyerjük. Ha a függvény valahol a 0 értéket veszi fel, akkor minden nagyobb helyen is 0-t kell felvennie; ennek alapján mutassuk meg, hogy a legkisebb olyan hely, ahol a 0-t veszi fel, nem lehet nagyobb, mint 3. Ebből az $f = 0$ mellett a fenti h_r függvényeket kapjuk. Végül könnyen adódik, hogy a függvény sehol sem vehet fel negatív értéket.

6.8.4 Ekkor a $-f$ függvény kielégíti a 6.8.1 Tétel bizonyításában szereplő (1) feltételt.

6.8.5 Az f valós és képzetes részére külön-külön alkalmazható a 6.8.1 Tétel.

6.8.6

a) Megfelel például a

$$k_1,\ 2k_1,\ 2k_2,\ 3k_2,\ 3k_3,\ 4k_3,\ \ldots,\ jk_j,\ (j+1)k_j,\ \ldots$$

sorozat, ahol $\big(k_j, j(j+1)\big) = 1$ és a k_j számok (az előírt b_n elemekhez képest) elegendően nagyok. Ha a sorozat elemein az f például monoton növő, akkor az additivitás miatt

$$f(j) + f(k_j) = f(jk_j) \le f((j+1)k_j) = f(j+1) + f(k_j)\,,$$

ahonnan $f(k_j)$ kivonása után $f(j) \le f(j{+}1)$, azaz f monotonitása adódik. Ezután a 6.8.1 Tételből következik, hogy $f(n) = c \log n$.

b) Megfelel például a

$$c_1,\ c_1d_1,\ c_2,\ c_2d_2,\ c_3,\ c_3d_3,\ \ldots,\ c_j,\ c_jd_j,\ \ldots$$

sorozat, ahol a $d_1, d_2, \ldots$ számsorozatban minden 1-nél nagyobb egész végtelen sokszor fordul elő, továbbá $(c_j, d_j) = 1$ és a c_j számok (az előírt b_n elemekhez képest) elegendően nagyok. Legyen $m > 1$ rögzített és $\varepsilon > 0$ tetszőleges. Ekkor a sorozat konstrukciója, f additivitása és a feladat feltétele miatt van olyan (nagy) j, amelyre $m = d_j$ és

$$|f(m)| = |f(c_j d_j) - f(c_j)| < \varepsilon\,,$$

tehát csak $f(m) = 0$ lehetséges.

7. Diofantikus egyenletek

7.1.

7.1.1 Háromféleképpen. ($10\,000 = 201 \cdot 47 + 7 \cdot 79 = 122 \cdot 47 + 54 \cdot 79 = 43 \cdot 47 + 101 \cdot 79$.)

7.1.2 14.

7.1.3 Hétféleképpen. — Útmutatás: A $7x + 13y + 15z = 500$, $x + y + z = 50$ egyenletrendszerből például x-et kiküszöbölve a $6y + 8z = 150$, majd ezt 2-vel osztva a $3y + 4z = 75$ diofantikus egyenlethez jutunk. Ennek olyan megoldásait keressük, ahol $y \geq 0$, $z \geq 0$, továbbá $x \geq 0$ miatt $y + z \leq 50$.

7.1.4 9.

7.1.5 Az $ax + by = c$ diofantikus egyenletet $b \neq 0$ esetén egy x, y egész számpár pontosan akkor elégíti ki, ha x megoldása az $ax \equiv c \pmod{b}$ lineáris kongruenciának (és y értéke ekkor egyértelműen adódik az egyenletből). Vegyük észre, hogy a 2.5.4 Tétel bizonyításában szereplő (5) képlet (a jelölések „konverziója" után) éppen a 7.1.1 Tétel (1) képletének az x'-re vonatkozó részével azonos. (Nem feltétlenül szükséges a bizonyításra támaszkodni, elég csak a 2.5.4 Tétel állítását felhasználni, ekkor azonban kicsit nehézkesebb a gondolatmenet.)

7.1.6 a) 0 vagy ∞. b) 0 vagy 1.

7.1.7 $x = -3 - 5u - 10v$, $y = 3u + 3v + 1$, $z = 2v + 1$. — Útmutatás: A kétismeretlenes esethez hasonlóan az egyik ismeretlent kifejezve, majd a törtből a biztosan egész értékű részt leválasztva és alkalmas új ismeretlent bevezetve csökkentsük az együtthatók abszolút értékét mindaddig, amíg a tört nevezője 1 lesz. Ezután az így adódó *két* egész paraméterrel írjuk fel az eredeti ismeretlenek értékeit.

7.1.8 Egy lehetséges út, ha a 7.1.1 Tétel után vázolt megoldási algoritmust általánosítjuk (ezt alkalmaztuk az előző feladatnál is), ebből a megoldhatóságra vonatkozó állítás is kihozható. — Egy másik lehetőség a k szerinti teljes indukció. A k ismeretlenes $a_1x_1 + \ldots + a_kx_k = c$ egyenletet a következőképpen vezethetjük vissza $k-1$ ismeretlenesre: Legyen $d = (a_{k-1}, a_k)$, ekkor $a_{k-1}x_{k-1} + a_kx_k$ alakban éppen d többszörösei, azaz a dy számok állnak elő. Így az eredeti egyenlet helyett vizsgálhatjuk a $k-1$ ismeretlenes $a_1x_1 + \ldots + a_{k-2}x_{k-2} + dy = c$ egyenletet, amelyre már alkalmazhatjuk az indukciós feltételt.

7.1.9 Ha az egyenlet megoldható, akkor az egyenlet bármely megoldása nyilván megoldása a kongruenciának is tetszőleges m modulus esetén. Ha az egyenlet nem oldható meg, akkor $(a_1, \ldots, a_k) \nmid c$, és ekkor az $m = (a_1, \ldots, a_k)$ modulusra nyilván a kongruencia sem oldható meg.

7.1.10 Ez pontosan akkor igaz, ha az a_i számok relatív prímek és található közöttük pozitív. – Útmutatás: A feltétel szükségessége nyilvánvaló. Az elégségességhez tegyük fel, hogy például $a_1 > 0$. Ha valamely c_0-ra sikerül pozitív egészekből álló megoldást találni, akkor x_1 értékét növelve és a többi x_i értékét változatlanul tartva, a c_0-lal reprezentált modulo a_1 maradékosztály minden c_0-nál nagyobb elemére is kapunk megfelelő megoldást. Így elég azt megmutatni, hogy minden modulo a_1 maradékosztálynak van olyan c eleme, amelyre létezik pozitív egész megoldás. Ehhez használjuk fel, hogy az

$$a_1x_1 + \ldots + a_kx_k = c \tag{1}$$

diofantikus egyenlet (a 2.5 pontban pontosan megfogalmazott értelemben) „ekvivalens” az

$$a_2x_2 + \ldots + a_kx_k \equiv c \pmod{a_1} \tag{2}$$

kongruenciával. Oldjuk meg a (2) kongruenciát $c = 1, 2, \ldots, a_1$-re. (Biztosan létezik megoldás, mert $(a_1, \ldots, a_k) = 1$ miatt (1) bármely c-re megoldható az egész számok körében.) Mivel kongruenciáról van szó, nyilván az is feltehető, hogy mind az a_1 darab kongruencia esetében a kapott $x_2, \ldots, x_k$ értékek mindegyike pozitív.

7.1.11

a) Legyen $a > b$, és alkalmazzuk az előző feladat alapötletét. Eszerint ha egy c összerakható, akkor nyilván bármely pozitív t-vel $c + tb$ is összerakható. Így a feladat megoldásához mindegyik modulo b maradékosztályban meg kell keresni a legkisebb összerakható elemet. Mivel $(a, b) = 1$, ezért a $0a, 1a, 2a, \ldots, (b-1)a$ elemek teljes maradékrendszert alkotnak modulo b, vagyis az egyes maradékosztályok legkisebb összerakható elemei

$b, a, 2a, \ldots, (b-1)a$. Ez azt jelenti, hogy a legnagyobb nem összerakható szám az „utolsóként belépő” $(b-1)a$-val reprezentált maradékosztály $(b-1)a - b = ab - a - b$ eleme.

b) Válasz: $(a-1)(b-1)/2$. (Ez biztosan egész szám, hiszen $(a,b) = 1$ miatt a és b közül legalább az egyik páratlan.) — Útmutatás: Mutassuk meg, hogy ha két pozitív egész összege $ab - a - b$, akkor közülük az egyik összerakható, a másik pedig nem.

7.1.12 A megoldáshoz kényelmesebb a feladatot „fordított” szemlélettel, „összeállítás” helyett „szétvágásra” átfogalmazni: egy adott kocka a) minden elég nagy n, illetve b) $n \geq 48$ esetén szétvágható pontosan n darab kockára.

a) Mivel egy kockából könnyen csinálhatunk 8, illetve 27 kis kockát, ezek egymás utáni alkalmazásával egy kocka $1 + 7x + 26y$ részre is bontható, ahol x és y tetszőleges nemnegatív egészek. A 7 és a 26 relatív prímek, és így valóban minden elég nagy n előállítható ilyen alakban.

b) Mivel egy kockát 8 részre vágva, a kis kockák számát mindig tudjuk 7-tel növelni, ezért elég az állítást a 48 és 54 közötti n-ekre igazolni.

48: $48 = 27 + 3 \cdot 7$, azaz a kockát vágjuk 27 részre, majd 3 kis kockát 8-8 részre.

49: egy 6 oldalú kocka alsó felét bontsuk 4 darab 3 oldalú kockára, a felső sorát 36 darab egységkockára, a fennmaradó két sort pedig 9 darab 2 oldalú kockára.

50: $50 = 7 \cdot 7 + 1$.

51: egy 6 oldalú kocka alsó felét és még egy nyolcadát bontsuk 5 darab 3 oldalú kockára, a megmaradt részből kiválaszthatunk 5 darab 2 oldalú kockát és marad még 41 darab egységkocka.

52: egy 4 oldalú kockából vegyünk ki egy 3 oldalú részt, ekkor marad 37 egységkocka, ezekből kettőt 8-8 részre osztva összesen 52 kockára bontottuk az eredeti kockát.

53: $53 = 1 + 2 \cdot 19 + 2 \cdot 7$ alapján elég olyan eljárást mutatni, amely 19-cel növeli a kockák darabszámát; egy 3 oldalú kockát bontsunk egy 2 oldalúra és a megmaradó 19 egységkockára.

54: egy 8 oldalú kocka háromnegyedét bontsuk 6 darab 4 oldalú kockára, a maradékból leválasztható 2 darab 3 oldalú és 4 darab 2 oldalú kocka, valamint marad 42 darab egységkocka.

7.2.

7.2.1 Mutassuk meg, hogy ha $x^2 + y^2 = z^2$, akkor x, y és z között található 3-

mal, 4-gyel, illetve 5-tel osztható. Nézzük például az 5-tel való oszthatóságot. Egy négyzetszám 5-tel osztva 0, 1 vagy -1 maradékot ad. Tegyük fel indirekt, hogy x, y és z egyike sem osztható 5-tel, ekkor $x^2+y^2=z^2$ bal oldala 0-val vagy ± 2-vel kongruens modulo 5, a jobb oldal viszont ± 1-gyel, ami ellentmondás. A 4-gyel, illetve 3-mal való oszthatóság is hasonlóan igazolható. (Mindhárom oszthatóságnál az egyenlet helyett a 7.2.1 Tétel szerinti karakterizációt használva is hasonlóan bizonyíthatunk.)

7.2.2 Válasz: $8, 15, 17$. — Útmutatás: Az $xy/2$ területképlet alapján $xy=120$. A 120 összes lehetséges felbontását megvizsgálva csak a $8\cdot 15$ esetben lesz x^2+y^2 négyzetszám. — Másik lehetőség: A 7.2.1 Tétel alapján a $60=d^2mn(m-n)(m+n)$ egyenletet kell megoldani az ott megadott (4) feltételrendszert is figyelembe véve. Így egyedül a $d=1$, $m=4, n=1$ eset lehetséges.

7.2.3 Válasz: $6, 8, 10$ és $5, 12, 13$. — Útmutatás: A 7.2.1 Tétel alapján a terület $d^2mn(m-n)(m+n)$, a kerület pedig

$$d\big(2mn+(m^2-n^2)+(m^2+n^2)\big)=2md(m+n)\,.$$

Ezek egyenlősége az egyszerűsítések után a $dn(m-n)=2$ egyenletet jelenti. Ennek a 7.2.1 Tétel (4) feltételét is kielégítő megoldásai $d=m=2, n=1$, illetve $d=1, n=2, m=3$. — Másik lehetőség: Az

$$\frac{xy}{2}=x+y+z, \qquad x^2+y^2=z^2$$

diofantikus egyenletrendszert kell megoldani. Az első egyenletből átrendezéssel kapott $(xy/2)-z=x+y$ egyenlőséget emeljük négyzetre, ekkor a második egyenlet felhasználásával és xy-nal történő egyszerűsítés után $z=(xy/4)-2$ adódik. Ezt az első egyenletbe visszahelyettesítve, átrendezés és szorzattá alakítás után az $(x-4)(y-4)=8$ egyenlethez jutunk. Mivel x és y pozitív, ezért (a tényezők sorrendjétől eltekintve) csak az $1\cdot 8$ és $2\cdot 4$ előállítás ad megoldást.

7.2.4 Válasz: minden $k\geq 3$-ra. — Útmutatás: Használjuk a 7.2.1 Tételt. Lássuk be, hogy az 1 és a 2 nem állítható elő az ott megadott x, y, illetve z alakok egyikeként sem. A 2-nél nagyobb számok esetén pedig a képletben szereplő d szorzó miatt elég azt igazolni, hogy a 4 és a páratlan számok előállnak ilyen alakban: $4=2\cdot 2\cdot 1$, illetve $2r+1=(r+1)^2-r^2$.

7.2.5 Ha x, y, z primitív pitagoraszi számhármas, akkor $(y-x)^2$, z^2 és $(x+y)^2$ relatív prímek, és számtani sorozatot alkotnak.
Megjegyzés: Az $u^2+v^2=2w^2$ diofantikus egyenlet $0<u<w<v$ és az $x^2+y^2=z^2$ pitagoraszi egyenlet $0<x<y<z$ megoldásai kölcsönösen

visszavezethetők egymásra, az $u = y - x$, $v = x + y$, $w = z$, illetve a fordított irányú $x = (v - u)/2$, $y = (u + v)/2$, $z = w$ helyettesítéssel (x-re és y-ra egész számokat kapunk, mivel u és v szükségképpen azonos paritású). Ennek alapján az $u^2 + v^2 = 2w^2$ egyenlet összes megoldását is felírhatjuk három egész paraméter segítségével.

7.3.

7.3.1 Mivel az x és y előjele most nem számít, ezért az összes egészek körében kapott megoldásokat négyesével csoportosítva kapunk egy-egy „lényegesen különböző megoldást", kivéve az $y = 0$ esetet (amely csak akkor fordul elő, ha n négyzetszám). Ennek megfelelően a „lényegesen különböző megoldások" száma $\left\lceil \frac{f(n)}{4} \right\rceil$, ahol $f(n)$ a 7.3.1 Tételben megadott megoldásszám.

7.3.2 Két megoldás van: a süteményt a tepsi oldalaival párhuzamosan 6, illetve 8, vagy pedig 5, illetve 12 részre kell vágni (az első esetben 48, a második esetben 60 szelet keletkezik). — Útmutatás: Ha a tepsi oldalaival párhuzamosan x, illetve y részre vágunk, akkor $xy/2$ égett és $(x-2)(y-2)$ nem égett szelet keletkezik. Az így kapott egyenlet az $(x - 4)(y - 4) = = 8$ alakra hozható. — Másik lehetőség: A tepsi fala mentén körbehaladó „sorban" összesen 8-cal több szelet van, mint a következő (szintén „körbefutó") sorban. Ez azt jelenti, hogy ennél a két sornál beljebb is összesen 8 szelet van, amelyek egy 2×4-es vagy egy 1×8-as téglalapot alkotnak.

7.3.3 A $2/p = 1/x + 1/y$ egyenlet a $(2x - p)(2y - p) = p^2$ alakra hozható. — Ottlik Géza megoldása: Az egyenletet xy-nal beszorozva kapjuk, hogy valamelyik ismeretlen osztható p-vel, mondjuk $x = kp$. Ezt visszahelyettesítve fejezzük ki y-t, és lássuk be, hogy $p = 2k - 1$. Innen x és y is egyértelmű.

7.3.4 Pontosan azok, ahol a nevezőnek van nem $4k + 1$ alakú pozitív osztója.

7.3.5 Az

$$\frac{1}{u} = \frac{1}{2u} + \frac{1}{2u}$$

egyenlőség alapján elég megmutatni, hogy a megadott n-ekre $4/n$ felírható két vagy három természetes szám reciprokának az összegeként.

$n = 2s$: $\quad \dfrac{4}{n} = \dfrac{1}{s} + \dfrac{1}{s}$

$n = 4s - 1$: $\quad \dfrac{4}{n} = \dfrac{1}{s} + \dfrac{1}{s(4s - 1)}$

$n = 8s - 3$: $\quad \dfrac{4}{n} = \dfrac{1}{2s} + \dfrac{1}{s(8s-3)} + \dfrac{1}{2s(8s-3)}$

$n = 24s - 15$: $\quad \dfrac{4}{n} = \dfrac{1}{8s-5} + \dfrac{1}{24s-15}$

$n = 24s - 7$: $\quad \dfrac{4}{n} = \dfrac{1}{6s} + \dfrac{1}{s(24s-7)} + \dfrac{1}{6s(24s-7)}$

7.3.6 Induljunk ki az $a/b = 1/b + 1/b + \ldots + 1/b$ („rossz") előállításból, majd alkalmazzuk elég sokszor például az

$$\frac{1}{n} = \frac{1}{n+1} + \frac{1}{n(n+1)}$$

azonosságot.

7.3.7 Nincs. — Útmutatás: Az $x^4 - 4 = y^5$ diofantikus egyenlet bal oldalát szorzattá bontva, a két tényező páratlan x esetén relatív prím, és így külön-külön is ötödik hatványok, a különbségük 4, ami lehetetlen. Páros x-re pedig az egyenlet bal oldala nem osztható 8-cal, a jobb oldal viszont igen.

7.3.8 Az egyetlen megoldás $x = y = s = t = 0$. — Útmutatás: A feladat egyszerűen visszavezethető az egész megoldások keresésére, sőt (az indirekt feltételezett nemtriviális megoldásról) az is feltehető, hogy $(x, y, s, t) = 1$. Ekkor a paritást vizsgálva ellentmondásra jutunk. — Másik lehetőség: Egy nemtriviális egész megoldás olyan szabályos háromszöghöz vezet, amelynek mindhárom csúcsa rácspont. Területi megfontolásokkal mutassuk meg, hogy nincs ilyen háromszög.

7.3.9 Az összeg 3-mal osztható, de 9-cel nem.

7.3.10 ± 4, ± 6.

7.3.11 A feladat „csúnya" megoldása: Legyen a hat szám $n, n+1, \ldots, n+5$, és osszuk ezeket minden lehetséges módon két csoportba. Azt kell igazolni, hogy az így adódó egyenletek egyikének sincs egész megoldása. Mivel egy egész együtthatós polinom egész (sőt racionális) gyökei könnyen megkereshetők, ezért a feladat megoldása csak némi türelmes számolást igényel. Természetesen nem kell minden lehetőséget számításba venni, például a tényezőnkénti összehasonlításból látszik, hogy $n(n+1)(n+4)$ minden $n \geq 0$ esetén kisebb, mint $(n+2)(n+3)(n+5)$, és más hasonló megfontolások is alkalmazhatók.

Lényegesen „elegánsabb" a következő gondolatmenet: Mivel a hat szám közül három osztható 2-vel, további egy 3-mal, és legfeljebb további egy

5-tel, ezért $n > 1$ esetén a számok valamelyikének van 5-nél nagyobb prímosztója. Ezzel a prímmel a többi szám egyike sem lehet osztható, így ez a prím csak az egyik szorzatnak lehet osztója.

Harmadik lehetőség: Ha a számok valamelyike osztható 7-tel, akkor az előzőleg látott módon készen vagyunk. Egyébként a hat szám redukált maradékrendszert alkot modulo 7. Ha létezne két egyenlő szorzat, akkor a hat szám szorzata négyzetszám lenne. A hat szám szorzata -1 maradékot ad 7-tel osztva, viszont egy négyzetszámnak nem lehet ez a maradéka.

A harmadik megoldás a Wilson-tétel és a $\left(\frac{-1}{p}\right)$ Legendre-szimbólum felhasználásával átvihető a 6 helyett 106-ra (mivel a 107 egy $4k-1$ alakú prímszám). Az első megoldás (elvileg vagy jól programozott számítógép segítségével) átvihető a 106-ra vagy bármely konkrét darabszámra. Lényegében a második megoldás is általánosítható: Sylvester és Schur egy klasszikus tétele szerint k darab k-nál nagyobb egymást követő egész szám valamelyikének mindig van k-nál nagyobb prímosztója, így ez a prím a két részszorzat közül csak az egyiknek lehet osztója. A fennmaradó esetekben a Csebisev-tétel biztosít olyan prímszámot, amely csak az egyik részszorzatnak osztója.

Végül megjegyezzük, hogy maga az állítás hat helyett tetszőleges k egymást követő egész esetén is igaz. Ez következik abból a nehéz tételből, hogy egymást követő pozitív egészek szorzata sohasem lehet teljes hatvány (lásd az 1.6.3 feladathoz fűzött megjegyzést).

7.3.12 Csak páros m-re van megoldás: $n = m+1$ és $x = y = 2^{m/2}$.
Útmutatás: Az egyenletet (x, y) segítségével átírva mutassuk meg, hogy csak $x = y$ lehetséges. Ebben az esetben az egyenlet a

$$2^m = x^{2n-2m} \tag{3}$$

alakra hozható. Ekkor nyilván $x = 2^s$. Ezt (3)-ba visszaírva lássuk be, hogy $m = 2s$ és $n = m+1$.

7.3.13

a) Az $(x+5)(y+3) = 22$ alakból könnyen leolvasható a $2d(22) = 8$ darab megoldás.

b) Nincs megoldás. Az egyenletet modulo 11 érdemes vizsgálni.

c)–e) Csak a triviális $x = y = z = 0$ megoldás létezik. A „jó” modulusok: c)-nél 3 vagy 8; d)-nél 5, 7, 8 vagy 23; e)-nél 11.

f) $x = \pm 1$, $z = -2$. — Útmutatás: a bal oldal két tényezője bármely x egész szám esetén relatív prím, ezért külön-külön is köbszámok.

g) $x = \pm 1$, $y = 0$. — Útmutatás: Egyszerű átalakítások után azt kapjuk, hogy két szomszédos szám szorzata „majdnem” negyedik hatvány. Ezen

az úton továbbhaladva, alkalmas kongruenciavizsgálatok után még egy szorzattá bontásra van szükség.

h) $y = x$, valamint $x = 2$, $y = 4$ és $x = 4$, $y = 2$. — Útmutatás: Írjuk át az egyenletet (x, y) segítségével, vagy pedig logaritmálás után használjuk fel az $f(z) = z/\log z$ (valós) függvény viselkedését.

i) $x = 5$, $y = 1$. — Útmutatás: Vizsgáljuk az egyenletet modulo 31, és használjuk fel a hatványmaradékokról tanultakat.

7.3.14

a) Nincs ilyen számrendszer. — Útmutatás: $x > 0$ esetén $1 + x + x^2$ mindig két szomszédos négyzetszám közé esik.

b) A 3-as számrendszer az egyetlen megoldás. — Útmutatás: $x > 3$ esetén $4(1 + x + x^2 + x^3 + x^4)$ két szomszédos négyzetszám közé esik.

c) Nincs ilyen számrendszer. — Útmutatás: A megfelelő kifejezés két relatív prím tényező szorzatára bontható, és közülük az egyik nem lehet négyzetszám.

7.4.

7.4.1 $1 + i \mid a + bi \iff a \equiv b \pmod 2$.

7.4.2

a) $\alpha = \gamma\varrho \iff \overline{\alpha} = \overline{\gamma}\,\overline{\varrho}$,

b) Az a) részből következik.

c) Következik akár a Gauss-felbonthatatlan, akár a Gauss-prím definíciójából, vagy pedig a 7.4.15 Tételből.

7.4.3 A 7.4.2a feladat szerint $\alpha \mid \overline{\alpha} \iff \overline{\alpha} \mid \alpha$, vagyis ekkor $\alpha = \varepsilon\overline{\alpha}$, ahol ε egység. Mutassuk meg, hogy itt a két oldal abszolút értéke mindig egyenlő, a szögek összehasonlításából pedig $\arg(\alpha) = k \cdot 45^\circ$ adódik. Ez pontosan azt jelenti, hogy α a koordinátatengelyek vagy pedig az $y = \pm x$ egyenesek valamelyikén helyezkedik el. (Az $\alpha = \varepsilon\overline{\alpha}$ egyenlőségből az $\varepsilon = \pm 1, \pm i$ esetek végigpróbálásával is ugyanerre az eredményre jutunk.)

7.4.4

a) Használjuk fel, hogy az a/b racionális szám akkor és csak akkor Gauss-egész, ha egész szám.

b) Ha $(a, b) = d$ az egész számok körében, akkor azt kell igazolni, hogy az $a_1 = a/d$ és $b_1 = b/d$ számok a Gauss-egészek körében is relatív prímek. Ha egy γ Gauss-egész közös osztója a_1-nek és b_1-nek, akkor $N(\gamma)$ az egész számok körében közös osztója $N(a_1) = a_1^2$-nek és $N(b_1) = b_1^2$-nek, amiből következik, hogy $N(\gamma) = 1$, tehát γ egység. (Egy másik lehetőség, hogy

alkalmas u és v egész számokkal $1 = a_1u + b_1v$, és így $\gamma \mid a_1$ és $\gamma \mid b_1$ esetén szükségképpen $\gamma \mid 1$.)

7.4.5 Igaz: a), c).

7.4.6 (Természetesen a megadott eredmények helyett azok bármelyik egységszerese is helyes.)

a) $2 - i$. — Útmutatás: alkalmazzuk az euklideszi algoritmust.

b) 2. — Útmutatás: használjuk fel, hogy $1-i$ és $2+i$ Gauss-prímek, továbbá $2 = \varepsilon(1 - i)^2$ és $2 + i \nmid 39$.

c) $1 + i$. — Útmutatás: A keresett δ legnagyobb közös osztó osztója a két szám összegének és különbségének is, ahonnan $(4+i, 2+i) = 1$ miatt $\delta \mid 2$ adódik. Innen $\delta = 1$ vagy 2 vagy $1+i$. Végül mutassuk meg, hogy az első két eset nem lehetséges.

7.4.7

a) Igaz: (a1).

b) $(\alpha, \overline{\alpha}) = (a, b)$ vagy $(\alpha, \overline{\alpha}) = (1 + i)(a, b)$.

7.4.8 Mutassuk meg, hogy β akkor és csak akkor barátja α-nak, ha $\beta = \varepsilon\overline{\alpha}$ és $(\alpha, \overline{\alpha}) = 1$. Így α-nak (0 vagy) 4 barátja van, és könnyen adódik az a)-beli feltétel is.

7.4.9 $3^2(2 + i)^3(2 - i)(1 + i)^3(-1 - 4i)$. — Útmutatás: Érdemes először a 90-et kiemelni és a 7.4.15 Tétel szerint Gauss-prímek szorzatára bontani. A fennmaradó rész $3 + 29i = \pi_1 \dots \pi_r$ felbontásának a meghatározásához térjünk át a normákra: $850 = N(\pi_1) \dots N(\pi_r)$. A 850 kanonikus alakjából kapjuk, hogy $r = 4$, és a π_i Gauss-prímek normái 2, 5, 5 és 17. Innen $\pi_1 = 1 + i$, $\pi_2 = \pi_3 = 2 + i$ vagy $2 - i$, aszerint hogy $(3 + 29i)/(2 + i)$ Gauss-egész-e vagy sem ($\pi_3 = \overline{\pi_2}$ nem lehet, miért?) stb.

7.4.10 Igaz: b), c), e).

7.4.11 Bizonyítsunk $N(\alpha)$ szerinti teljes indukcióval. A kulcslépés: Ha az α két különböző felbontása Gauss-prímek szorzatára

$$\alpha = \pi_1 \dots \pi_r = \varrho_1 \dots \varrho_s, \qquad \text{ahol} \qquad \pi_i \neq \varepsilon\varrho_j,$$

akkor létezik olyan ε egység, hogy $N(\pi_1) \leq N(\varrho_1)$ esetén az

$$\alpha_1 = \varepsilon\alpha - \pi_1\varrho_2 \dots \varrho_s$$

Gauss-egészre $N(\alpha_1) < N(\alpha)$, és α_1-nek is két különböző felbontása van Gauss-prímek szorzatára.

7.5.

7.5.1 $\left\lceil \frac{r(n)}{8} \right\rceil$, ahol $r(n)$ a 7.5.1 Tételben megadott megoldásszám (ha az egyenlet nem oldható meg, akkor $r(n) = 0$). — Útmutatás: Az x és y felcseréléséből, illetve az előjelek változtatásával kapott megoldások nem adnak „lényegesen különböző" megoldást. Ez általában 8 lehetőség, kivéve azokat a megoldásokat, amikor x és y valamelyike 0, vagy $x = y$ (ezek csak az $n = k^2$, illetve $n = 2k^2$ esetekben fordulhatnak elő).

7.5.2 16.

7.5.3 Válasz: 7. — Útmutatás: A $8k + 6$ alakú számok nem írhatók fel két négyzetszám összegeként vagy különbségeként, tehát $r \leq 7$. Azt kell még igazolni, hogy végtelen sok esetben teljesül, hogy két egymást követő $8k+6$ alakú szám között mind a hét szám előáll a kívánt módon.

7.5.4 A 7.5.1 Tétel szerint az a^2+b^2 kanonikus alakjában szereplő 7 és 11 prímek kitevője páros, azaz legalább 2 kell hogy legyen. — Másik lehetőség: a 7 és a 11 Gauss-prímek, tehát

$$7 \mid a^2 + b^2 = (a + bi)(a - bi) \Longrightarrow 7 \mid a + bi \text{ vagy } 7 \mid a - bi \Longrightarrow$$
$$\Longrightarrow \frac{a + bi}{7} \text{ vagy } \frac{a - bi}{7} \text{ Gauss-egész } \Longrightarrow 7 \mid a \text{ és } 7 \mid b,$$

és ugyanez érvényes a 11-re is.

7.5.5 Akkor és csak akkor van megoldás, ha az n kanonikus alakjában minden $4k - 1$ alakú prím kitevője páros és a 2 kitevője nem 1. Ekkor a megoldásszám ugyanaz, mint a 7.5.1 Tételben, ha n osztható 4-gyel, és az ottani értéke fele, ha n páratlan.

7.5.6 Akkor és csak akkor van megoldás, ha n nem osztható 4-gyel és nincs $4k - 1$ alakú prímosztója. Ebben az esetben a megoldásszám 2^{r+2}, ahol r az n páratlan ($4k + 1$ alakú) prímosztóinak a száma.

7.5.7

a) Annak megfelelően, hogy k az átfogó, illetve az egyik befogó hossza, az $x^2 + y^2 = k^2$, illetve $x^2 - y^2 = k^2$ diofantikus egyenletek „lényegesen különböző", pozitív egész x, y megoldásainak a számát kell meghatározni. A 7.5.1 Tétel (és a 7.5.1 feladat) alapján az első egyenletnél ez a megoldásszám

$$\frac{(2\beta_1 + 1) \dots (2\beta_r + 1) - 1}{2},$$

ahol $\beta_1, \dots, \beta_r$ a k kanonikus alakjában szereplő $4t + 1$ alakú prímek kitevői. A második egyenletnél pedig a 7.3.1 Tétel (és a 7.3.1 feladat)

felhasználásával kapjuk, hogy a keresett megoldásszám

$$\begin{array}{ll} \frac{1}{2}(d(k^2)-1) & \text{ha } k \text{ páratlan;} \\ \frac{1}{2}(d(\frac{k^2}{4})-1) & \text{ha } k \text{ páros.} \end{array}$$

b) A 7.5.6 feladat alapján az átfogó akkor és csak akkor lehet k hosszúságú, ha a $k>1$ szám minden prímosztója $4t+1$ alakú, és ekkor a háromszögek száma $2^{\omega(k)-1}$. Hasonló gondolatmenettel adódik, hogy k akkor és csak akkor lehet egy befogó hossza, ha $k>1$ páratlan vagy pedig $4 \mid k$, és mindkét esetben $2^{\omega(k)-1}$ ilyen háromszög létezik.

A fenti meggondolások helyett a primitív pitagoraszi számhármasokat karakterizáló 7.2.1 Tétel alkalmazása is célhoz vezet.

7.5.8 Először tegyük fel, hogy egy $4k-1$ alakú q prím az n kanonikus alakjában a $2w-1$ páratlan kitevővel szerepel. Ekkor az egyenletnek nincs megoldása, tehát azt kell igazolni, hogy n (pozitív) páratlan osztóinak a fele $4k+1$, a másik fele pedig $4k-1$ alakú. Az n tetszőleges páratlan osztója felírható tq^u alakban, ahol $(t,2q)=1$ és $0 \le u \le 2w-1$. Ekkor (bármely $0 \le j \le$ $\le w-1$ esetén) a tq^{2j} és tq^{2j+1} osztók közül az egyik $4k+1$, a másik pedig $4k-1$ alakú.

Most vizsgáljuk azt az esetet, amikor az n kanonikus alakjában minden $4k-1$ alakú q_ν prím kitevője páros, jelöljük q_ν kitevőjét $2w_\nu$-vel. Ekkor a 7.5.1 Tétel alapján azt kell megmutatni, hogy

$$d'(n)-d''(n)=\prod_{\mu=1}^{r}(\beta_\mu+1)\,, \tag{1}$$

ahol a β_μ értékek az n kanonikus alakjában szereplő $4k+1$ alakú prímek kitevői. Végezzük el az előző párosítást a q_1 szerint, ekkor csak azok a (pozitív páratlan) osztók maradnak ki, amelyekben a q_1 kitevője $2w_1$. Ezekre az osztókra ismételjük meg az eljárást, most a q_2 szerint stb. Így végül azok a (pozitív) páratlan osztók maradnak meg, amelyekben mindegyik q_ν kitevője $2w_\nu$. Ezeknek az osztóknak a száma egyrészt nyilván az (1) jobb oldalán szereplő érték, másrészt ezek az osztók valamennyien $4k+1$ alakúak, tehát a számuk éppen $d'(n)-d''(n)$. — A feladat állítását egy lépésben is bebizonyíthatjuk, ha a $D=d'(n)-d''(n)$ különbséget az alábbi módon írjuk fel:

$$D=\sum_{\substack{0\le\beta'_\mu\le\beta_\mu\\ 0\le\gamma'_\nu\le\gamma_\nu}}(-1)^{\gamma'_1+\ldots+\gamma'_s}=\prod_{\mu=1}^{r}(\beta_\mu+1)\prod_{\nu=1}^{s}\bigl(1-1+\ldots+(-1)^{\gamma_\nu}\bigr)\,.$$

7.5.9 Válasz: π. — Útmutatás: Vegyük észre, hogy $1 + \sum_{i=1}^{n} r(i)$ éppen az origó körüli $\sqrt{n}$ sugarú kör belsejébe vagy határára eső rácspontok száma. Mutassuk meg, hogy ezeknek a rácspontoknak a száma aszimptotikusan egyenlő a kör területével (ha $n \to \infty$).

7.5.10 Az összes megoldás: $x = \pm 2, y = 2$ és $x = \pm 11, y = 5$. — Útmutatás: Az egyenlet bal oldalát a Gauss-egészek körében bontsuk szorzattá, és vizsgáljuk meg a két tényező legnagyobb közös osztójának lehetséges értékeit. Ebből kiderül, hogy mindkét tényező egy-egy Gauss-egész köbe. Végül végezzük el a köbre emelést, és hasonlítsuk össze a képzetes részeket.

7.5.11 $\alpha = a + bi$ akkor és csak akkor *nem* írható fel ilyen alakban, ha b páratlan, vagy $a \equiv b \equiv 2 \pmod 4$. — Útmutatás: Alkalmazzuk a 7.3.1 Tétel bizonyításának gondolatmenetét.

7.5.12 A kanonikus alakban szereplő Gauss-prímek helyettesíthetők bármelyik egységszeresükkel (és ezt a „külön egység” módosításával kompenzálhatjuk).

7.5.13 Igaz: a), c).

7.5.14 Válasz: 5/6. — Útmutatás: Jelölje $F(N)$ az $1, 2, \ldots, N$ egészek között azoknak a számát, amelyek nem írhatók fel három négyzetszám összegeként. Mutassuk meg, hogy

$$F(N) = \left\lfloor \frac{N+1}{8} \right\rfloor + \left\lfloor \frac{N+4}{8 \cdot 4} \right\rfloor + \left\lfloor \frac{N+4^2}{8 \cdot 4^2} \right\rfloor + \ldots ,$$

és innen

$$\lim_{N \to \infty} \frac{F(N)}{N} = \frac{1}{8} \sum_{k=0}^{\infty} \frac{1}{4^k} .$$

7.5.15 Válasz: 10. — Útmutatás: A három-négyzetszám-tétel segítségével igazoljuk, hogy 10 páratlan négyzetszám minden esetben elég, és a két-négyzetszám-tétel alapján mutassuk meg, hogy végtelen sok $8k + 2$ alakú számhoz 10-nél kevesebb páratlan négyzetszám nem elég.

7.5.16 Ha $n = 4^k(8m+7)$, akkor $n-(2^k)^2$ előáll három négyzetszám összegeként.

7.5.17 Egy n pozitív egész akkor és csak akkor *nem* áll elő így, ha $n = 4^k(16m + 14)$ alakú. — Útmutatás: Mutassuk meg, hogy n akkor és csak akkor áll elő a kívánt alakban, ha $2n$ felírható három négyzetszám összegeként.

7.5.18 Megoldható. — Útmutatás: Azt kell megmutatni, hogy a megadott szám felírható négy olyan négyzetszám összegeként, amelyek közül legalább az egyik osztható 3-mal.

7.5.19 Chevalley tételéből (illetve a 3.6.2 feladatból) következik, hogy az $X^2+Y^2+Z^2 \equiv 0 \pmod p$ kongruenciának létezik nemtriviális X, Y, Z megoldása. Ha például $Z \not\equiv 0 \pmod p$, akkor a kongruenciát $p>2$ esetén Z^{p-3}-mal megszorozva kapjuk, hogy

$$1+c^2+d^2 \equiv 0 \pmod p, \quad \text{ahol} \quad c = XZ^{(p-3)/2} \text{ és } d = YZ^{(p-3)/2}.$$

7.5.20 A 7.5.5 Lemma helyett az $x^2+1 \equiv 0 \pmod p$ kongruencia megoldhatóságára, a 7.5.4 Lemma helyett pedig az

$$(a_1^2+a_2^2)(b_1^2+b_2^2) = (a_1b_1+a_2b_2)^2 + (a_1b_2-a_2b_1)^2 \tag{2}$$

azonosságra támaszkodhatunk. Megjegyezzük, hogy m páratlanságát itt fölösleges igazolni (bár a bizonyítás ugyanúgy megy), továbbá (2) a Gauss-egészek normáira vonatkozó $N(\alpha)N(\beta) = N(\beta\overline{\alpha})$ azonosság kifejtett alakja.

7.5.21

a) Képezzük azokat a $\underline{d} = C\underline{s} - \underline{t}$ vektorokat, ahol $\underline{s}$ és $\underline{t}$ megfelelő komponenseire

$$0 \le s_i < u_i, \quad 0 \le t_i < v_i, \quad i = 1, 2, \ldots, k$$

teljesül. A skatulyaelv alapján ezen $\underline{d}$ vektorok között lesz kettő, amelyik kongruens modulo p, és ekkor az ezekhez tartozó $\underline{s}$, illetve $\underline{t}$ vektorok különbsége megfelel $\underline{x}$-nek, illetve $\underline{z}$-nek.

b) Az a) részt alkalmazzuk a

$$k=2, \qquad u_1 = u_2 = v_1 = v_2 = \lceil \sqrt{p} \rceil, \qquad C = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$$

esetre, ahol $1+c^2+d^2 \equiv 0 \pmod p$. Innen azt kapjuk, hogy

$$0 < x_1^2+x_2^2+z_1^2+z_2^2 < 4p \qquad \text{és} \qquad p \mid x_1^2+x_2^2+z_1^2+z_2^2.$$

c) A $2p$ esetben ugyanúgy járhatunk el, mint amikor a 7.5.3 Tétel bizonyítása során m páratlanságát igazoltuk.

Ha $3p = a_1^2+a_2^2+a_3^2+a_4^2$, akkor legyen b_i az a_i legkisebb abszolút értékű maradéka modulo 3, és alkalmazzuk a 7.5.4 Lemma (10) azonosságát. A $9p$-nek az így adódó felírásában mind a négy négyzetszám osztható 3-mal, tehát 9-cel való osztás után azt kapjuk, hogy a p is „szép”. (Ebben a lépésben tulajdonképpen a 7.5.3 Tétel bizonyítását ismételtük meg az $m=3$ speciális esetre.)

7.6.

7.6.1 Ha n előáll s darab 600-adik hatvány összegeként, akkor n ugyanennyi 200-adik hatvány összege is, hiszen

$$n = x_1^{600} + \ldots + x_s^{600} = (x_1^3)^{200} + \ldots + (x_s^3)^{200}\,.$$

7.6.2 A 7.6.5 Tétel bizonyításához hasonlóan alkalmas modulusok szerinti kongruenciák adják a megoldás kulcsát.

(a1) Bizonyítsuk be j szerinti teljes indukcióval, hogy a $31 \cdot 16^j$ alakú számok nem állíthatók elő 16-nál kevesebb negyedik hatvány összegéből.

(a2) A $64t + 32$ alakú számok nem írhatók fel 31 nyolcadik hatványból.

(a3) A 7.6.1 feladathoz hasonlóan következik, hogy $G(24) \geq G(8)$.

(a4) A $625t + 125$ alakú számokhoz nem elég 124 századik hatvány.

(a5) Vizsgáljuk a $625t + 312$ alakú számokat.

b) Az (a1)–(a3) részt a $k = 2^r$ és $k = 3 \cdot 2^r$ esetekre általánosíthatjuk, ahol $r \geq 2$. Mutassuk meg, hogy a^k csak 0 vagy 1 maradékot adhat modulo 2^{r+2}, ennek igazolásához használjuk fel, hogy erre a modulusra nem létezik primitív gyök.

Az (a4) rész a $k = \varphi(p^\alpha)$ esetre általánosítható, ahol $p > 2$ prím és $\alpha \geq 2$. A bizonyításhoz (a 7.6.5 Tételnél látott módon) az Euler–Fermat-tételt érdemes alkalmazni.

Az (a5) a $k = \frac{1}{2}\varphi(p^\alpha)$ esetre általánosítható, ahol $p > 2$ prím és $\alpha \geq 2$. Lássuk be és használjuk fel, hogy bármely a-ra

$$a^{\varphi(p^\alpha)/2} \equiv 0 \text{ vagy } \pm 1 \pmod{p^\alpha}\,.$$

Ily módon a fenti esetekben a következő alsó becsléseket nyerhetjük $G(k)$-ra ($p > 2$ prím, $\alpha \geq 2$ és $r \geq 2$):

$$G(3 \cdot 2^r) \geq G(2^r) \geq 2^{r+2}; \qquad G(p^\alpha - p^{\alpha-1}) \geq p^\alpha;$$
$$G\Big(\frac{p^\alpha - p^{\alpha-1}}{2}\Big) \geq \frac{p^\alpha - 1}{2}\,.$$

Megjegyezzük, hogy a 7.6.4 Tétel mellett mindössze ezek az alsó becslések ismertek $G(k)$-ra.

7.6.3 Legyen R elég nagy szám, és képezzük az

$$x_1^k + \ldots + x_{k+1}^k, \quad x_i \text{ egész}, \quad 0 \leq x_i \leq R, \quad i = 1, 2, \ldots, k+1$$

összegeket. Mutassuk meg, hogy sokkal több összeg van, mint ahány különböző értéket felvehetnek. Ebből következik, hogy kell lennie olyan n-nek, amely sokféleképpen előáll ilyen összeg alakban.

7.6.4

a) A bal oldalon a műveletek elvégzése és összevonások után csak a_i^4 és $a_i^2 a_j^2$ $(i < j)$ típusú tagok maradnak, és ezek mindegyike 6, illetve 12 együtthatóval szerepel. Ugyanezt kapjuk, ha a jobb oldalon elvégezzük a négyzetre emelést.

b) Legyen $n = 6q + r$, ahol $0 \leq r \leq 5$. A 7.5.3 Tétel alapján $q = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Írjuk fel mind a négy x_i-t ismét négy négyzetszám összegeként. Ezután az a)-beli azonosságot alkalmazva azt kapjuk, hogy $6q$ előáll 48 negyedik hatványból, a maradék r pedig legfeljebb 5 darab 1^4 tag összege.

7.6.5 A $8t + 6$ alakú számok nem állnak elő $x^2 \pm y^2$ alakban, tehát két négyzetszám nem elegendő. Az állítás másik részének igazolásához rendezzük át az $x^2 + y^2 - z^2 = n$ diofantikus egyenletet $z^2 - y^2 = x^2 - n$ alakba, ezután válasszuk meg x értékét tetszőlegesen, csak arra ügyelve, hogy $x^2 - n$ ne legyen $4t + 2$ alakú (bármely n esetén vagy az összes páros vagy az összes páratlan szám biztosan megfelel x-nek, esetleg mind a párosak, mind a páratlanok jók). Végül használjuk fel a 7.3.1 Tételt (és azt, hogy ha egy szám előáll két négyzetszám különbségeként, akkor a negatívja is). A másik diofantikus egyenlet esetén hasonlóan járhatunk el.

7.7.

7.7.1

a) Ha $m = qk$, akkor

$$x^m + y^m = z^m \Longrightarrow (x^q)^k + (y^q)^k = (z^q)^k \,.$$

b) Az a) részből következik, mivel bármely $k > 2$ esetén k-nak létezik páratlan prímosztója vagy $4 \mid k$.

7.7.2

a) Nincs megoldás, ez a Fermat-sejtés $k = 4$ esetéből következik.

b) Végtelen sok megoldás van. Keressünk $x = 2^\alpha$, $y = 2^\beta$, $z = 2^\gamma$ alakú megoldásokat, ekkor a

$$2^{3\alpha} + 2^{4\beta} = 2^{5\gamma}$$

egyenlethez jutunk. Az $\alpha = 4\nu$, $\beta = 3\nu$ választás mellett a $12\nu + 1 = 5\gamma$ feltételnek kell teljesülnie.

Megjegyzés: A fenti gondolatmenetek az alábbi $x^k + y^m = z^n$ típusú diofantikus egyenletekre általánosíthatók:

(i) Ha $(k, m, n) \geq 3$, akkor nincs pozitív egész megoldás.

(ii) Ha $(km, n) = 1$, akkor végtelen sok pozitív egész megoldás van.

7.7.3 Az összes megoldás: $k = 2$, $x = y = z - 1$.

7.7.4

a) Nincs megoldás: visszavezethető a Fermat-sejtés $k = 4$ esetére.

b) Az összes megoldás: $x = vwd$, $y = uwd$, $z = uvd$, ahol u, v, w (primitív) pitagoraszi számhármas (w az „átfogó") és d tetszőleges pozitív egész. — Útmutatás: Azt, hogy ezek valóban megoldások, behelyettesítéssel ellenőrizhetjük. Megfordítva, tegyük fel, hogy x, y, z megoldás. Most is elég az $(x, y, z) = 1$ esettel foglalkozni. Legyen $(x, y) = w$, $(x, z) = v$ és $(y, z) = u$. Lássuk be, hogy u, v és w páronként relatív prímek, és így $x = vwx_1$, $y = uwy_1$ és $z = uvz_1$, ahol x_1, y_1 és z_1 páronként relatív prímek. Ezeket az egyenletbe beírva, mutassuk meg, hogy $x_1 = y_1 = z_1 = 1$, továbbá $u^2 + v^2 = w^2$.

c) Az összes megoldás: $x = a^2 d$, $y = b^2 d$, $z = (a + b)^2 d$, ahol a, b, d pozitív egészek és $(a, b) = 1$ is feltehető (ez utóbbi a megadott paraméteres előállítás egyértelműségéhez kell). — Útmutatás: Ez a feladat is visszavezethető az $(x, y, z) = 1$ eset vizsgálatára, ekkor a kétszeri négyzetre emelés után kapott

$$xy = \left(\frac{z - x - y}{2}\right)^2$$

egyenletben $(x, y) = 1$, és így x és y (relatív prím) négyzetszámok.

d) Az összes megoldás: $x = a^3d,\ y = b^3d,\ z = (a+b)^3d$, ahol $a,\ b,\ d$ pozitív egészek és $(a, b) = 1$. — Útmutatás: Az első köbre emelésnél

$$x + y + 3\sqrt[3]{x}\sqrt[3]{y}\big(\sqrt[3]{x} + \sqrt[3]{y}\big) = z$$

adódik, itt $\sqrt[3]{x} + \sqrt[3]{y}$ helyére írjuk be $\sqrt[3]{z}$-t, majd átrendezés után ismét emeljünk köbre. A kapott

$$xyz = \left(\frac{z - x - y}{3}\right)^3$$

egyenlet bal oldalán a három tényező páronként relatív prím, tehát különkülön köbszámok.

7.7.5 Használjuk fel a primitív pitagoraszi számhármasok karakterizációját.

a) Az $x^4 + y^2 = z^2$ egyenlet vizsgálatánál az $x^2 = 2mn$ vagy $x^2 = m^2 - n^2$ feltételnek, az $x^2+y^2 = z^4$ esetben pedig $z^2 = m^2+n^2$-nek kell teljesülnie. Az m és n értékeket végtelen sokféleképpen meg lehet választani úgy, hogy $2mn$, $m^2 - n^2$, illetve $m^2 + n^2$ négyzetszámok legyenek (és emellett $m > n > 0$, $(m, n) = 1$ és $m \not\equiv n \pmod 2$ is fennálljon).

b) Alkalmazzunk végtelen leszállást.

7.7.6 Az összes megoldás: $x = \pm1$, $y = \pm1$. — Útmutatás: Az egyenlet átírható $x^4 + (y^2 - 1)^2 = y^4$ alakba.

7.7.7 Csak a hetes számrendszer ilyen. — Útmutatás: Sorozatos szorzattá bontások és a primitív pitagoraszi számhármasok karakterizációjának felhasználásával az egyenletet visszavezehetjük a 7.3.13g és 7.7.6 feladatokra.

7.7.8 Hasonlóan járhatunk el, mint a 7.4.3 feladatnál. — Válasz: A 0, valamint azok az Euler-egészek, amelyeknek mint komplex számoknak a szöge $\pi/6$-nak egész számú többszöröse. Ugyanez más alakban megadva: a

$$c, \quad c\omega, \quad c(1 + 2\omega), \quad c(1 + \omega), \quad c(1 - \omega), \quad c(2 + \omega)$$

Euler-egészek, ahol c tetszőleges egész szám.

7.7.9 Legyen $\alpha = a + b\omega$, $\beta = c + d\omega$, ekkor a feladatban szereplő azonosság éppen az

$$|\alpha|^2 \cdot |\beta|^2 = |\alpha\beta|^2$$

egyenlőség kifejtett alakja. (Az azonosságot természetesen beszorzással és a két oldalon keletkező tagok összehasonlításával is ellenőrizhetjük, azonban ez a megoldás egyrészt „csúnya”, másrészt nem derül ki belőle a feladat háttere.)

7.7.10

a) A két egyenlet kapcsolatát az Euler-egészek normájának felhasználásával lehet a legegyszerűbben megmutatni.

b) Az egyenletek akkor és csak akkor oldhatók meg, ha az n **Z**-beli kanonikus alakjában minden $3t-1$ alakú prímszám páros hatványon fordul elő.

A megoldásszámnál a csak a sorrendben vagy előjelben különböző megoldásokat is különbözőknek tekintjük. Tegyük fel, hogy az egyenletek megoldhatók, és legyen

$$L = \prod_{\mu=1}^{r} (\beta_\mu + 1)\,,$$

ahol $\beta_1, \ldots, \beta_r$ az n **Z**-beli kanonikus alakjában a $3t+1$ alakú prímszámok kitevői (ha n-nek nincs ilyen alakú prímosztója, akkor $L = 1$).

Ekkor az $x^2 - xy + y^2 = n$ egyenlet megoldásszáma $6L$, az $x^2 + 3y^2 = n$ egyenleté pedig $6L$, ha $4 \mid n$, és $2L$, ha n páratlan. [Az n nem lehet $4s+2$ alakú, mert a 2 (mint $3t-1$ alakú prímszám) az n kanonikus alakjában szükségképpen páros kitevővel szerepel.]

Az $x^2 - xy + y^2 = n$-re vonatkozó állítást a két-négyzetszám-tétel (7.5.1 Tétel) bizonyításához hasonlóan igazolhatjuk.

A másik egyenlet megoldásszámát visszavezethetjük az előző eredményre. Ehhez létesítsünk kölcsönösen egyértelmű megfeleltetést (például az a) rész bizonyításának a mintájára) az $x^2 + 3y^2 = n$ diofantikus egyenlet megoldásai és az $x^2 - xy + y^2 = n$ egyenlet olyan megoldásai között, ahol x páros. Ennek alapján a $4 \mid n$ esetben azt kell belátni, hogy az $x^2 - xy + y^2 = n$ egyenletnek csak olyan megoldásai vannak, ahol x páros. Végül, páratlan n esetén az állítás abból következik, hogy egy n normájú Euler-egész hat egységszerese közül pontosan két esetben lesz a szóban forgó x érték páros.

7.7.11 Az összes megoldás: $x = \pm 10$, $y = 7$. — Útmutatás: Kövessük a 7.5.11 feladat megoldásának gondolatmenetét. Első lépésként az egyenlet bal oldalát bontsuk szorzattá az Euler-egészek körében, ekkor a két tényező a legnagyobb közös osztójukban szereplő Euler-prímektől és esetleges egységtényezőktől eltekintve külön-külön is köbszám.

7.7.12

a) Jelölje k_μ egy modulo μ teljes maradékrendszer elemszámát. Legyen R az Euler-egészek rombuszrácsa. A μ-vel osztható Euler-egészek egy olyan R_μ rombuszrácsot alkotnak, amely R-ből μ-vel való szorzással keletkezik. Így R_μ-ben az alaprombusz oldalait alkotó „vektorok” μ és $\omega\mu$. Az R_μ rács bármely ilyen alaprombuszába eső Euler-egészek egy teljes maradékrendszert alkotnak modulo μ. Ebből következik, hogy k_μ „körülbelül” az R_μ,

illetve R rácsokat generáló alaprombuszok területeinek az aránya, azaz $|\mu|^2 = N(\mu)$. A „körülbelül”-től úgy lehet megszabadulni, hogy tekintjük a két rácsnak egy H nagy sugarú körbe vagy nagy oldalú négyzetbe stb. eső rácspontjainak a számát. Legyen H területe T, az R, illetve R_μ rács H-beli rácspontjainak a száma n, illetve n_μ, az alaprombuszok területe pedig t, illetve t_μ. Mivel R_μ bármely alaprombuszába k_μ Euler-egész esik, ezért $T \to \infty$ mellett

$$k_\mu \sim \frac{n}{n_\mu}. \tag{3}$$

Másrészt

$$n \sim \frac{T}{t}, \qquad n_\mu \sim \frac{T}{t_\mu} = \frac{T}{tN(\mu)},$$

tehát

$$\frac{n}{n_\mu} \sim \frac{\frac{T}{t}}{\frac{T}{t_\mu}} = \frac{t_\mu}{t} = N(\mu). \tag{4}$$

A (3) és (4) alapján a k_μ és $N(\mu)$ konstansok aszimptotikusan egyenlők, és így szükségképpen egyenlők is.

b) Az a) rész szerint az elemek darabszáma megfelelő, így csak azt kell igazolni, hogy az elemek páronként inkongruensek modulo μ. Ehhez használjuk fel, hogy

$$\mu \mid j \implies p = N(\mu) \mid j^2 \implies p \mid j.$$

c) Alkalmazzuk az Euler–Fermat-tétel (2.4.1 Tétel) bizonyításánál látott gondolatmenetet.

7.7.13 Nincs megoldás. — Útmutatás: Az egyenletet uvw-vel beszorozva $u^2w + v^2u = w^2v$ adódik. Az $u^2w = c$ és $v^2u = d$ jelölést bevezetve azt kapjuk, hogy $cd(c+d) = (uvw)^3$. A szokásos módon elérhető, hogy a bal oldal tényezői páronként relatív prímek legyenek, és így c, d és $c+d$ (nemnulla) köbszámok, ami ellentmond a Fermat-sejtés $k = 3$ esetének.

7.7.14 A pitagoraszi számhármasok képlete szerint a háromszög területe

$$d^2mn(m+n)(m-n),$$

ahol $m > n > 0$, $(m, n) = 1$ és $m \not\equiv n \pmod 2$.

a) A terület pontosan akkor négyzetszám, ha $mn(m+n)(m-n)$ négyzetszám. A feltételekből következik, hogy a négy tényező (pozitív és) páronként relatív prím, és így külön-külön is négyzetszámok. Ez ellentmond a 7.7.3 Lemmának.

b) A feltétel szerint $d = 1$, és így az előző gondolatmenethez hasonlóan kapjuk, hogy m, n és $m+n$ köbszámok, ami ellentmond a 7.7.10 Tételnek.

c) Végtelen sok ilyen háromszög létezik, sőt minden pitagoraszi háromszöghöz található hozzá hasonló ilyen háromszög: adott m, n esetén d értékét válasszuk $mn(m+n)(m-n)$-nek. — Ugyanez a paraméteres jellemzés nélkül is elmondható: Ha egy háromszög területe T, akkor az oldalakat T-szeresre nagyítva az új háromszög területe T^3 lesz.

d) Ha k páros, akkor a)-ból következik, hogy a terület nem lehet k-adik hatvány. Ha k páratlan, akkor b)-hez, illetve c)-hez hasonlóan kapjuk, hogy relatív prím oldalak esetén a terület nem lehet k-adik hatvány, azonban minden pitagoraszi háromszöghöz található olyan hozzá hasonló háromszög, amelynek a területe k-adik hatvány.

7.8.

7.8.1 Ha $m = 0$, akkor $x = \pm 1$ és y tetszőleges, ha $m = -1$, akkor $x = \pm 1$, $y = 0$, illetve $x = 0$, $y = \pm 1$, ha pedig $m \leq -2$ vagy $m = k^2 > 0$, akkor $x = \pm 1$, $y = 0$. — Útmutatás: Az $m = k^2$ esetben az $(x - ky)(x + ky) = = 1$ szorzattá bontásból kapjuk, hogy mindkét tényező 1, illetve -1.

7.8.2 A $10y^2 + 1 = x^2$ Pell-egyenletről van szó, tehát végtelen sok ilyen négyzetszám létezik.

7.8.3 Ha az $x^2 - my^2 = r$ egyenlet egy megoldását az $x^2 - my^2 = 1$ Pell-egyenlet egy megoldásával (a 7.8.2 Tétel bizonyításában látott módon) összeszorozzuk, akkor ismét az $x^2 - my^2 = r$ egyenlet egy megoldásához jutunk.

7.8.4 Végtelen sok megoldás: (a1), (a2), (b1). Nincs megoldás: (b2) (ez utóbbi az $x^2 - 3y^2 = -1$ egyenlet modulo 3 vagy modulo 4 vizsgálatából következik).

7.8.5 Végtelen sok. — Útmutatás: Az $n(n-1) = 2y^2$ egyenletet 4-gyel szorozva a $z^2 - 8y^2 = 1$ Pell-egyenlethez jutunk (a $z = 2n - 1$ feltétel nem jelent megszorítást, mert a $z^2 - 8y^2 = 1$ egyenletnek eleve csak olyan megoldásai lehetnek, ahol z páratlan). Másik lehetőség: n és $n - 1$ közül az egyik négyzetszám, a másik egy négyzetszám kétszerese, és az így adódó $u^2 - 2v^2 = \pm 1$ egyenletek mindegyikének végtelen sok megoldása van.

7.8.6 Végtelen sok. — Útmutatás: Az $x^2 + (x+1)^2 = z^2$ egyenletet 2-vel szorozva a $(2x+1)^2 - 2z^2 = -1$ egyenlethez jutunk. Másik lehetőség: a primitív pitagoraszi számhármasok paraméteres előállításának felhasználása is az $u^2 - 2v^2 = \pm 1$ egyenletekhez vezet.

7.8.7 Nincs megoldás: a), b), d), e). Végtelen sok megoldás van: c), f). — Útmutatás: A megoldhatatlanságot egy alkalmas modulus szerinti kongruenciával lehet kimutatni. A 8 mind a négy esetben megfelel ilyen modulusnak, emellett még (a felsorolás sorrendjében) a 3, 7, 9, illetve 3 választás is célhoz vezet. A c) esetben $x = 4$, $y = 1$ megoldás, így a 7.8.3 feladat szerint végtelen sok megoldás létezik. Az f) eset 3-mal való szorzás után ekvivalens a $z^2 - 6y^2 = 3$ diofantikus egyenlettel. Ennek $z = 3$, $y = 1$ megoldása, tehát végtelen sok megoldás van. Világos, hogy minden megoldásban $3 \mid z$, tehát $x = z/3$ is egész szám lesz.

7.8.8 Az egyenlet akkor és csak akkor oldható meg, ha $p \equiv 1 \pmod 4$ vagy $p = 2$. — Útmutatás: A szükségesség az egyenlet modulo 4 vizsgálatból azonnal adódik. Az elégségességhez tekintsük az $x^2 - py^2 = 1$ egyenletnek azt az $x > 0$, $y > 0$ megoldását, ahol x minimális. Mutassuk meg, hogy x csak páratlan lehet, és írjuk át az egyenletet

$$\frac{x+1}{2} \cdot \frac{x-1}{2} = p\Big(\frac{y}{2}\Big)^2 \tag{5}$$

alakba. Az (5) bal oldalán a tényezők egyike négyzetszám, a másik pedig egy négyzetszám p-szerese. Innen $u^2 - pv^2 = \pm 1$ adódik, az x minimalitása miatt azonban a + előjel nem lehetséges.

7.8.9 Az előjelekre vonatkozó állítás nyilvánvaló. A kongruenciákra vonatkozó rész igazolásához vegyünk egy olyan nemtriviális megoldást, amelyben $(x, y, z) = 1$. Mutassuk meg, hogy $(z, a) = (y, a) = 1$. Az egyenletet $bz^{2(\varphi(|a|)-1)}$-gyel beszorozva és modulo $|a|$ tekintve ekkor a

$$(byz^{\varphi(|a|)-1})^2 \equiv -bc \pmod{|a|}$$

kongruenciát kapjuk. A másik két kongruencia ugyanígy adódik.

7.8.10 Végtelen sok. — Útmutatás: Nyilván szükséges, hogy $28k^2 + 1$ négyzetszám legyen, ez végtelen sokszor teljesül. Mutassuk meg, hogy minden ilyen esetben $2 + 2\sqrt{28k^2 + 1}$ is négyzetszám lesz. Ehhez az $r^2 - 1 = 28k^2$ egyenlőséget osszuk el 4-gyel és a bal oldalt bontsuk szorzattá, ekkor a keletkező tényezők olyan szomszédos egészek, amelyek egyike négyzetszám, a másik pedig egy négyzetszám 7-szerese. Végül lássuk be,

hogy szükségképpen az $(r+1)/2$ tényező négyzetszám, és így a feladatban megadott $2r+2$ is négyzetszám.

7.8.11 Ha $x = u^2$, akkor az egyenlet átírható $(u^2-1)(u^2+1) = 2y^2$ alakba. Lássuk be, hogy ekkor u^2-1 négyzetszám, ami $u \neq \pm 1$ esetén lehetetlen. (Ez az egyenlet szerepelt a 7.7.7 feladat megoldásában is.) — Az $y = v^2$ eset megegyezik a 7.3.13g feladattal.

7.9.

7.9.1 Ha az $n+1$ partíciójában szerepel 1-es, akkor egy 1-est hagyjunk el, egyébként pedig a legkisebb tagot csökkentsük 1-gyel. Így nyilván n minden partícióját legfeljebb kétszer kapjuk meg. A második módon csak olyan partíciókat kaphatunk, amelyekben legfeljebb egy darab 1-es fordul elő, tehát $n >$ 1-re nem kapjuk meg n minden partícióját. Ezért egyenlőség csak $n =$ 1-re teljesül.

7.9.2 a) ∞. b) $-\infty$.

7.9.3 A 7.9.5 Tétel alapján ezek a $(3k^2 \pm k)/2$ alakú számok.

7.9.4 2^{n-1}. — Útmutatás: Tekintsük az n egy $n = x_1+x_2+\ldots+x_r$ előállítását (ahol r és $x_1, \ldots, x_r$ pozitív egészek), és mérjük fel a $[0, n]$ intervallumban az origóból kiindulva egymás után rendre az $x_1, \ldots, x_r$ hosszúságú szakaszokat. Ez azt jelenti, hogy az intervallumon az $1, 2, \ldots, n-1$ pontok közül néhányat kijelöltünk osztópontnak (esetleg az összeset, esetleg egyet sem). Az n előállításai és az osztópont-halmazok között kölcsönösen egyértelmű megfeleltetés áll fenn. Ezért a keresett előállításszám megegyezik egy $n-1$ elemű halmaz összes részhalmazainak a számával.

7.9.5 Az n egy r-tagú előállításában minden összeadandóból vonjunk ki 1-et, ekkor az $n-r$ egy legfeljebb r tagból álló előállítását kapjuk (a tagok száma akkor lesz r-nél kevesebb, ha az eredeti előállításban szerepelt 1-es). Mutassuk meg, hogy így kölcsönösen egyértelmű megfeleltetés jött létre a kétféle partíciók között.

7.9.6 $$\frac{x^r}{\prod_{i=1}^{r}(1-x^i)}\,.$$

7.9.7 A feladat állításait mind alkalmas bijekció megadásával, mind pedig a generátorfüggvények segítségével igazolhatjuk.

a) *Bijekció*: Tekintsük n-nek egy $n = x_1 + \ldots + x_r$ előállítását, ahol az x_i számok mind különbözők. Mindegyik x_i egyértelműen felírható $2^\alpha t$ alakban, ahol $\alpha \geq 0$ és t páratlan. Az azonos t értékeket kiemelve egy $n = 1u_1+3u_2+5u_3+\ldots$ egyenlőséghez jutunk, ahol minden u_j nemnegatív

egész. Ezt tekinthetjük az n olyan partíciójának, amelyben u_1 darab 1-es, u_2 darab 3-as stb szerepel.

Illusztrációs példa: Induljunk ki a $23 = 10+6+4+3$ partícióból. Ekkor

$$23 = 2^1\cdot 5+2^1\cdot 3+2^2\cdot 1+2^0\cdot 3 = 2^1\cdot 5+(2^1+2^0)\cdot 3+2^2\cdot 1 = 1\cdot 4+3\cdot 3+2\cdot 5$$

szerint a $23 = 5+5+3+3+3+1+1+1+1$ partícióhoz jutunk.

Mutassuk meg, hogy ily módon egy bijekciót adtunk meg az n kétféle partíciói között.

Generátorfüggvény: A megfelelő generátorfüggvények

$$V(x) = \prod_{i=1}^{\infty}(1+x^i) \qquad \text{és} \qquad W(x) = \prod_{j=1}^{\infty}\frac{1}{(1-x^{2j-1})}\,.$$

Ha $V(x)$-et átírjuk az

$$(1+x^i) = \frac{1-x^{2i}}{1-x^i}$$

azonosság felhasználásával, akkor az egyszerűsítések után éppen $W(x)$-et kapjuk. A precíz igazoláshoz vagy formális hatványsorokkal és formális végtelen szorzatokkal kell dolgozni, vagy pedig gondosan meg kell vizsgálni a végtelen szorzatokban a határátmenetnél fellépő problémákat.

b) A bijekcióhoz a tagokat most $k^\alpha t$ alakban kell felírni, ahol $k \nmid t$.
A generátorfüggvények:

$$V_k(x) = \prod_{i=1}^{\infty}(1+x^i+\ldots+(x^i)^{k-1}) \qquad \text{és} \qquad W_k(x) = \prod_{\substack{t=1\\ k\nmid t}}^{\infty}\frac{1}{(1-x^t)}\,.$$

7.9.8 *Első megoldás*: A 7.9.6 feladat szerint

$$\frac{x^r}{(1-x)(1-x^2)\ldots(1-x^r)}$$

sorfejtésében x^n együtthatója az n olyan partícióinak a száma, ahol a legnagyobb tag r, így ezeket az együtthatókat r szerint összegezve valóban $p(n)$ adódik.

Második megoldás: x^n együtthatóját csak a jobb oldali összeg első n tagja befolyásolja, ami közös nevezőre hozva

$$-1+\frac{1}{(1-x)(1-x^2)\ldots(1-x^n)}\,.$$

A 7.9.2 Tétel alapján itt x^n együtthatója megegyezik az n-nek az $1, 2, \ldots,$ n összeadandókból képzett partíciói számával, ami éppen $p(n)$.

7.9.9 Az $U(x) = \prod_{i=1}^{\infty}(1 - x^i)$ egyenlőség logaritmusának vegyük a deriváltját:

$$\frac{U'(x)}{U(x)} = \sum_{i=1}^{\infty} \frac{-ix^{i-1}}{1 - x^i} \,. \tag{6}$$

(A tényezőnkénti logaritmálás és a tagonkénti deriválás $|x| < 1/2$-re jogos.) Szorozzuk be (6)-ot $-xU(x)$-szel, és használjuk fel, hogy

$$\sum_{i=1}^{\infty} \frac{ix^i}{1 - x^i} = \sum_{i=1}^{\infty} i(x^i + x^{2i} + \ldots) = \sum_{j=1}^{\infty} \sigma(j)x^j \,.$$

Ekkor

$$-xU'(x) = U(x) \sum_{j=1}^{\infty} \sigma(j)x^j \tag{7}$$

adódik. Végül írjuk be (7)-be az

$$\begin{aligned} U(x) &= 1 - x - \ x^2 + \ x^5 + \ x^7 - \ \ x^{12} - \ \ x^{15} + \ldots \\ xU'(x) &= \ \ - x - 2x^2 + 5x^5 + 7x^7 - 12x^{12} - 15x^{15} + \ldots \end{aligned}$$

képleteket, és szorozzuk össze a (7) jobb oldalán álló két hatványsort.

8. Diofantikus approximáció

8.1.

8.1.1

a) Közös nevezőre hozva a számláló $as - br \neq 0$, ezért $|as - br| \geq 1$.

b) Az $|as - br| = 1$ egyenlőség végtelen sokszor teljesül, mert az $as - br = = \pm 1$ diofantikus egyenleteknek végtelen sok megoldása van.

8.1.2 Mivel $d = \alpha - r/s \neq 0$, ezért elég nagy k esetén $|d| > 1/(ks)^2$.

8.1.3

a) Bármely $s > 1$-re legfeljebb egy darab s nevezőjű tört lehet megfelelő.

b) Az a) részből következik.

8.1.4

a) Bármely k-ra vagy egy 2^k, vagy pedig egy 2^{k+1} nevezőjű tört megfelel.

b) $\alpha = 1/3$.
c) Bármely k-ra van ilyen 3^k nevezőjű tört.
d) $\alpha = 1/2$.
e) A $\sqrt{\alpha}$-t jól approximáló r/s törtek négyzetei megfelelnek.
f) $\alpha = (1+\sqrt{5})^2/4$.

8.1.5 Használjuk fel, hogy az α-t jól közelítő törtekre $r^2 \sim \alpha s^2$.

8.1.6 A 8.1.6 Tételhez hasonlóan bizonyíthatunk. A „gyökteleníteshez" a feladatban szereplő különbséget $\sqrt{2} + r/s$-sel érdemes beszorozni.

8.1.7 Ha r/s jól közelíti α-t, akkor
a) $a(r/s) + b$ jól közelíti $a\alpha + b$-t;
b) r^2/s^2 jól közelíti α^2-et.

8.1.8 a) 0 és 1. — b) és c) A teljes $(-1, 1)$ intervallum.

8.1.9
a) Az i-edik elem köré rajzoljunk egy $\varepsilon/2^i$ hosszúságú intervallumot.
b) Számosság: Kölcsönösen egyértelmű megfeleltetés létesíthető az ilyen „harmados" törtek és a $[0, 1)$-beli összes valós szám kettes alapú számrendszer szerinti „kettedes" törtként való felírása között (a 2-es jegy helyett 1-est kell írni). — Nullmértékűség: A Cantor-halmazt úgy kapjuk, hogy a $[0, 1)$ intervallumból elhagyjuk a középső harmadát, majd mindkét megmaradt intervallumnak a középső harmadát, majd a négy megmaradt intervallumnak a középső harmadát stb. Az első m lépés után a megmaradt intervallumok összhossza

$$1 - \frac{1}{3} - \frac{2}{9} - \ldots - \frac{2^{m-1}}{3^m} = 1 - \frac{1}{3} \cdot \frac{1 - (\frac{2}{3})^m}{1 - \frac{2}{3}} \to 0, \qquad \text{ha } m \to \infty.$$

8.1.10
a) Azonnal következik a definícióból.
b) A k darab halmaz mindegyikét fedjük le ε/k összhosszúságú intervallumsorozattal.
c) Az i-edik halmazt fedjük le $\varepsilon/2^i$ összhosszúságú intervallumsorozattal $(i = 1, 2, \ldots)$.
d) Bármely halmaz előáll az egy pontból álló részhalmazainak egyesítéseként, és ezek a részhalmazok nyilván nullmértékűek. Ez az egyesítés például a Cantor-halmaz esetén is nullmértékű, a $[0, 1]$ intervallum esetén viszont nem az.

8.2.

8.2.1

a) A 8.2.1 Tétel mindkét bizonyítása átvihető a térbeli esetre is, a második bizonyításnál ehhez természetesen a 8.2.2 Lemma térbeli változatára van szükség.

b) Az n-dimenziós esetben azt kell feltenni, hogy H térfogata legalább $2^n\Delta$. (Ekkor Δ az alapparalelepipedon n oldalának koordinátavektoraiból képzett determináns abszolút értékét jelenti.)

8.2.2 A 8.2.1 Tételre adott mindkét bizonyítás gondolatmenete alkalmas az állítás igazolására, a második bizonyításnál ehhez a 8.2.2 Lemma alábbi általánosítására van szükség (ezt az ottani jelölések segítségével fogalmazzuk meg): Ha a K_P halmazok közül bármely $r+1$ darab metszete az üres halmaz, akkor $t \le r\Delta$. Bármelyik bizonyítás gondolatmenetéből r darab olyan nemtriviális rácspont adódik, amelyek közül semelyik kettő sem egymás tükörképe az O középpontra, a további r darabot pedig ennek az r rácspontnak az O-ra vonatkozó tükörképei biztosítják.

8.2.3 Kövessük a 8.2.4 Tétel gondolatmenetét. Ha $p = 3k+1$ alakú prímszám, akkor alkalmas c-vel $c^2 \equiv -3 \pmod p$. Ekkor a 8.2.4 Tétel bizonyításában szereplő (6) rács pontjaira $p \mid x^2 + 3y^2$. A Minkowski-tételt a megfelelő ellipszisre alkalmazva egy olyan nemtriviális rácspontot kapunk, amelyre $x^2 + 3y^2 < 3p$. Mivel $x^2 + 3y^2 = 2p$ a modulo 3 feltétel miatt nem teljesülhet, így szükségképpen $x^2 + 3y^2 = p$.

8.2.4 A 8.2.1 Tétel jelölései szerint most L a szokásos négyzetrács, tehát $\Delta = 1$, H pedig az

$$a_{11}x_1 + a_{12}x_2 = \pm b_1, \qquad a_{21}x_1 + a_{22}x_2 = \pm b_2$$

egyenesek által határolt paralelogramma, ennek területe $4b_1b_2/|D|$. A feladat állítása ezért Minkowski tételéből következik.

8.2.5 A térbeli Minkowski-tétel (lásd a 8.2.1a feladatot) felhasználásával a 8.2.3 Tétel bizonyításához hasonló gondolatmenetet lehet alkalmazni. Ehhez tekintsük az

$$x = s\alpha_1 - r_1, \qquad y = s\alpha_2 - r_2, \qquad z = s$$

rácsot, itt az alapparalelepipedon térfogata $\Delta = 1$. Az approximációs feltételt átírhatjuk a $|zx^2| < c^2$, $|zy^2| < c^2$ alakba, ahol $c = 2/3$. Ezen nem konvex (és nem korlátos) térbeli halmaz helyett a számtani és mértani közép közötti egyenlőtlenséget is felhasználva vegyük alkalmas $a > 1$

értékekre az

$$\frac{1}{a^2}|z| + 2a|x| \le \sqrt[3]{12}, \qquad \frac{1}{a^2}|z| + 2a|y| \le \sqrt[3]{12}$$

oktaédereket.

8.3.

8.3.1 a) 4, 1, 4, 2. b) 1, 1, 2, 1, 2, 1, 2, ... c) 2, 4, 4, 4, ...
d) 1, 1, 1, 1, ...

8.3.2 a) 43/30. b) $(1 + \sqrt{3})/2$.

8.3.3 Használjuk fel a 8.3.3 Tételben megadott r_n/s_n törtek jó közelítését, és azt, hogy (11) alapján $(s_{n-1}, s_n) = 1$.

8.3.4 A 8.3.1d feladat szerint $(1+\sqrt{5})/2$ minden lánctörtjegye 1-es, és így a 8.3.3 Tételben szereplő r_n/s_n törtekre a (8a)–(8b) rekurzió szerint $r_n = \varphi_{n+2}$ és $s_n = \varphi_{n+1}$.

8.3.5 Használjuk fel a 8.3.4 Lemmában szereplő (8a), (8b) és (10) képleteket.

8.3.6 Az eredeti számot α-val, a „tisztán" periodikus részből nyert számot β-val jelölve az

$$\alpha = L(c_0, c_1, \ldots, c_{M-k}, \beta) \qquad \text{és} \qquad \beta = L(c_{M-k+1}, \ldots, c_M, \beta)$$

véges lánctörteket kapjuk. Ezekből a feladat állítása az emeletes törtek lebontása és további átrendezések után adódik.

8.4.

8.4.1 Sűrűek: b), d), f), g).

8.4.2 Rajzoljunk minden egyes $0 < r < 1$ racionális szám körül megszámlálható sok olyan zárt intervallumot, amelyek benne vannak $[0, 1)$-ben és a hosszuk 0-hoz tart, majd az összes így kapott intervallumot rendezzük egyetlen $J_1, J_2, \ldots$ intervallumsorozatba. Egy u_i számsorozat törtrészeinek mindenütt sűrűségéhez azt kell igazolni, hogy mindegyik J_s intervallumban található legalább egy $\{u_i\}$.

Ezek után az α-t egymásba skatulyázott zárt intervallumok közös pontjaként fogjuk megkapni. A kiindulási intervallum legyen (mondjuk) $H_0 = [2, 3]$. Ha a H_{k-1} intervallum már adott, akkor H_k-t a H_{k-1} következő részintervallumának definiáljuk: választunk egy olyan n_k kitevőt, amelyre a H_{k-1}-beli x elemek n_k-adik hatványai kitöltenek egy

két egész szám közötti teljes T intervallumot, és H_k-ba azokat az x-eket tesszük, amelyekre

$$x \in H_{k-1}, \qquad x^{n_k} \in T \qquad \text{és} \qquad \left\{x^{n_k}\right\} \in J_k\,.$$

Az így gyártott H_k intervallumok közös pontja megfelel α-nak.

8.4.3 Ha egy P_n pont „nagyon közel" van a k-dimenziós egységkocka egy $Q = (v_1, \ldots, v_k)$ pontjához, akkor minden $1 \le j \le k$-ra $\{n\alpha_j\} - v_j$ „kicsi" abszolút értékű, és így ezek tetszőleges lineáris kombinációjának az abszolút értéke is kicsi. Az $1, \alpha_1, \ldots, \alpha_k$ lineáris összefüggősége esetén ily módon a v_i-k alkalmas lineáris kombinációjára egy olyan feltétel nyerhető, amely nem teljesülhet tetszőleges Q-ra.

8.4.4

a) Képezzük az új sorozat elemeit úgy, hogy mindig a régi sorozat legelső olyan, még fel nem használt tagját vesszük, amelynek törtrésze rendre az alábbi intervallumokba esik:

$$\left[0, \frac{1}{2}\right), \ \left[\frac{1}{2}, 1\right), \ \left[0, \frac{1}{3}\right), \ \left[\frac{1}{3}, \frac{2}{3}\right), \ \left[\frac{2}{3}, 1\right), \ \left[0, \frac{1}{4}\right), \ \ldots$$

b) Például minden második tagnak olyan elemet vegyünk, amelynek nagyon kicsi a törtrésze.

8.4.5 Igaz: b), c).

8.4.6

a) Legyen k tetszőleges egész szám. Ha $10^k \le m < 10^{k+1}$, akkor

$$\{\lg m\} > \frac{1}{2} \iff m > 10^k\sqrt{10}.$$

Ez azt jelenti, hogy az $(1/2, 1)$ intervallumba a törtrészeknek jóval több, mint a fele esik, ha $n = 10^{k+1}$ (és jóval kevesebb, mint a fele, ha $n = \left\lfloor 10^k\sqrt{10}\right\rfloor$).

b) Az $1/(2\pi)$ arány irracionális, ezért az (ívmértékben mért) n szögek a 8.4.5 Tétel szerint egyenletes eloszlásúak az egységkörön. Ennek alapján a $\{\sin n\}$ értékek egyenletes eloszlása azt jelentené, hogy azok az x *valós* számok, amelyekre $\{\sin x\}$ a $[0, 1]$ intervallum egy előre megadott d hosszúságú I részintervallumába esik, az egységkör kerületének a d-szeresét foglalják el. Könnyen látható azonban, hogy ez például az $I = [1/2, \sqrt{3}/2]$ intervallumra nem teljesül.

8.4.7 Azt kell igazolni, hogy $54321 \cdot 10^v \le t^n < 54322 \cdot 10^v$ teljesül alkalmas n és v természetes számokra. Térjünk át tízes alapú logaritmusra, és $\alpha = \lg t$-re alkalmazzuk a 8.4.1 Tételt.

9. Algebrai és transzcendens számok

9.1.

9.1.1

a) Egy jó polinom $x^{20} - 7$.

b) Emeljük négyzetre az $\alpha - 3 = \sqrt{2}$ egyenlőséget.

c) Az $\alpha - \sqrt{3} = \sqrt{2}$ egyenlőséget négyzetre emelve, majd az eredményt átrendezés után ismét négyzetre emelve egy megfelelő egész együtthatós polinomot olvashatunk le.

d) Az $\alpha - \sqrt{2} = \sqrt[3]{4}$ egyenlőséget emeljük köbre, majd az eredményt átrendezés után emeljük négyzetre.

e) Az $\alpha = \sqrt[3]{2} + \sqrt[3]{4}$ egyenlőséget emeljük köbre, ezután a jobb oldalon keletkező „köbgyökös" rész átalakítható:

$$3\sqrt[3]{2}\sqrt[3]{4}(\sqrt[3]{2} + \sqrt[3]{4}) = 3 \cdot 2\alpha\,.$$

f) Az előzőkhöz hasonló módon, többszöri négyzetre emeléssel „kiküszöbölhetjük" a gyökjeleket.

9.1.2 Tegyük fel, hogy α gyöke az $f(x) = a_0 + a_1x + \ldots + a_nx^n$ racionális együtthatós polinomnak, ahol $a_n \neq 0$. Ekkor a megadott számok rendre gyökei az alábbi, szintén az előírt tulajdonságú polinomoknak:

a) $f(-x) = a_0 - a_1x + a_2x^2 + \ldots + (-1)^n x^n$;

b) $f(x)$ (egy valós együtthatós polinomnak α-val együtt $\overline{\alpha}$ is gyöke);

c) $xf(1/x) = a_n + a_{n-1}x + \ldots + a_0x^n$ ($\alpha \neq 0$ miatt feltehető, hogy $a_0 \neq 0$);

d) $f(x - r) = a_0 + a_1(x - r) + \ldots + a_n(x - r)^n$;

e) $f(x/r) = a_0 + a_1(x/r) + \ldots + a_n(x/r)^n$ (nyilván feltehető, hogy $r \neq 0$);

f) $f(x^k) = a_0 + a_1x^k + \ldots + a_nx^{kn}$.

9.1.3 Ha $\zeta(2) = \pi^2/6$ algebrai lenne, akkor az előző feladat e) és f) része szerint π is algebrai lenne.

9.1.4 Tegyük fel indirekt, hogy $f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$ algebrai, azaz léteznek olyan nem csupa nulla $b_0, b_1, \ldots, b_s$ racionális számok, amelyekre

$$b_0 + b_1(a_0 + a_1\alpha + \ldots + a_n\alpha^n) + \ldots + b_s(a_0 + a_1\alpha + \ldots + a_n\alpha^n)^s = 0\,.$$

A műveleteket elvégezve kapjuk, hogy α gyöke egy racionális együtthatós, nemnulla polinomnak, ami ellentmondás.

9.1.5 Ha van ilyen h, akkor h minden gyöke, így speciálisan g minden gyöke is algebrai. Megfordítva, ha g (multiplicitással számolt) gyökei az $\alpha_1, \ldots, \alpha_r$ algebrai számok, és α_j gyöke egy f_j egész együtthatós, nemnulla polinomnak ($j = 1, \ldots, r$), akkor a $h = f_1 \ldots f_r$ polinom megfelel a feltételeknek.

9.1.6 Az állítás azonnal következik az algebrai szám és a lineáris összefüggés definíciójából.

9.1.7 Az α komplex szám gyöke az alábbi komplex, illetve valós együtthatós polinomnak: a) $x-\alpha$; b) $(x-\alpha)(x-\overline{\alpha})$.

9.2.

9.2.1

a)–e) A fokszám megegyezik $\deg\alpha$-val, kivéve ha e)-ben $r=0$. Ennek igazolásához válasszuk a 9.1.2 feladat útmutatásában szereplő f polinomot m_α-nak, és lássuk be, hogy ekkor az útmutatásban az f segítségével megadott $f(-x)$ stb. polinomok is irreducibilisek $\mathbf{Q}$ felett.

f) $\deg\sqrt[k]{\alpha}\le k\deg\alpha$.

9.2.2 Először keressünk egy olyan f racionális együtthatós (nemnulla) polinomot, amelynek az adott α szám gyöke, majd vizsgáljuk meg, hogy f irreducibilis-e $\mathbf{Q}$ felett. Ha f irreducibilis, akkor $f=m_\alpha$ és így $\deg\alpha=\deg f$. Ha f reducibilis, akkor bontsuk irreducibilisek szorzatára, és keressük meg, melyik tényezőnek gyöke az α. — Az irreducibilitást gyakran ellenőrizhetjük a Schönemann–Eisenstein-kritérium segítségével, illetve másod- vagy harmadfokú polinom esetén elég azt megvizsgálni, hogy a polinomnak létezik-e racionális gyöke.

a) 7.

b) 3. — Fejezzük ki $1/2=\cos 60°$-ot $\cos 20°$ segítségével.

c) 3. — Lásd a 9.1.1e feladatnál szereplő útmutatást.

d) 2. — A „nagy” négyzetgyök alatt „teljes négyzet” szerepel.

e) 4.

f) 4. — A számhoz adjunk hozzá 1-et, és az így kapott négytagú összegre alkalmazzuk a mértani sorozat összegképletét.

9.2.3 Ha $\alpha=r+\sqrt{s}$, akkor α gyöke az $(x-r)^2-s$ másodfokú, a $\mathbf{Q}$ felett irreducibilis polinomnak. A megfordításhoz használjuk fel a másodfokú egyenlet megoldóképletét.

9.2.4

a) Használjuk fel, hogy ha α algebrai és r racionális, akkor $\deg(\alpha+r)=$ $=\deg\alpha$ (lásd a 9.2.1d feladatot).

b) Ha az α komplex szám nem valós, akkor az $s(\alpha+r)$ számok mindenütt sűrűek a komplex számsíkon, ahol r és s végigfutnak a racionális számokon.

9.2.5

a) Bármely i-re $\deg \alpha_i \leq \deg f$.

b) Egyenlőség pontosan akkor teljesül, ha f irreducibilis $\mathbf{Q}$ felett.

c) Írjuk fel f-et (a $\mathbf{Q}$ felett) irreducibilis polinomok szorzataként: $f = f_1 \dots f_k$, ahol f reducibilitása miatt $k \geq 2$. Legyen $\deg f_j = n_j$. Ekkor $n_1 + \dots + n_k = n$ és

$$\sum_{i=1}^{n} \deg \alpha_i = \sum_{j=1}^{k} n_j^2 \,. \tag{1}$$

Lássuk be, hogy az (1) jobb oldalán szereplő összeg akkor maximális, ha $k = 2$, és n_1 és n_2 közül az egyik 1, a másik $n - 1$.

9.2.6 $m_\alpha = x^6 + 5x^5 + 10x^2 + 5x - 10$. — Útmutatás: A feltételekből $f = g m_\alpha$, ahol $\deg g = 1$. Ebből következik, hogy f-nek van racionális gyöke. Határozzuk meg ezt a gyököt, ezután osszuk le f-et a megfelelő gyöktényezővel (ez utóbbit a leggyorsabban a Horner-elrendezéssel végezhetjük el).

9.2.7 Használjuk fel, hogy $[m_\alpha, m_\beta] \mid f$, továbbá ha $m_\alpha \neq m_\beta$, akkor a minimálpolinomok irreducibilitása miatt $(m_\alpha, m_\beta) = 1$.

9.2.8 Ha f irreducibilis lenne, akkor a feltételekből $f = m_\alpha \mid g$ következne.

9.3.

9.3.1

a) Legyen α algebrai és β transzcendens. Ha $\alpha + \beta$ algebrai lenne, akkor $\beta = (\alpha + \beta) - \alpha$ is algebrai lenne, ami ellentmondás.

b) Például $\pi + (1 - \pi)$ algebrai, $\pi + (1 + \pi)$ transzcendens.

c) Az összeghez képest annyi a változás, hogy egy algebrai és egy transzcendens szám szorzata lehet algebrai is, mégpedig abban a kivételes esetben, amikor az egyik tényező 0.

9.3.2

a) α és β algebrai.

b) α és β transzcendens.

c) α és β közül legalább az egyik transzcendens (mutassunk példát a többféle lehetőség mindegyikére).

d) α és β algebrai, vagy $\alpha = 0$ és β transzcendens.

e) α és β transzcendens.

f) α és β transzcendens, vagy pedig közülük az egyik 0 és a másik transzcendens.

g) α és β közül legalább az egyik transzcendens.

h) α és β algebrai. — Útmutatás: az $\alpha+\beta=c$, $\alpha\beta=d$ „egyenletrendszert" oldjuk meg, ekkor a másodfokú egyenlet megoldóképletéből (vagy a 9.3.6 Tétel alapján) kapjuk, hogy α és β is algebrai.

A racionális-irracionális esetben csak d)-nél és h)-nál van változás; ekkor az alábbi megoldásokat kapjuk, ahol $r>0$ és s racionális számok:

d) $\alpha=0$ és $\beta(\neq 0)$ tetszőleges, vagy $\alpha=\sqrt{r}$ és $\beta=s\sqrt{r}(\neq 0)$;

h) $\alpha=s+\sqrt{r}$ és $\beta=s-\sqrt{r}$.

9.3.3 Algebrai: b).

9.3.4

a) Legfeljebb egy lehet közülük algebrai; használjuk a 9.3.2a,d,h feladatot.

b) (b1) következik a 9.3.3 Tételből, (b2) pedig $e^{i\pi}=-1$ alapján a 9.3.5 Tételből.

9.3.5 Algebrai: a), b).

9.3.7 Lássuk be, hogy $\lg n$ irracionális, majd használjuk fel a 9.3.5 Tételt.

9.3.8 Tegyük fel, hogy valamely $k\neq m$ pozitív egészekre $\alpha^k+\beta^k=c$ és $\alpha^m+\beta^m=d$, ahol c és d algebrai számok, amelyek közül legalább az egyik nem nulla. Innen

$$(c-\beta^k)^m=(d-\beta^m)^k\,,$$

és így β gyöke egy algebrai együtthatós nemnulla polinomnak, azaz a 9.3.6 Tétel alapján maga is algebrai. Ugyanígy kapjuk, hogy α is algebrai, és ekkor valóban minden n-re $\alpha^n+\beta^n$ is algebrai.

9.3.9 *Algebrai*: Mutassuk meg, hogy végtelen sok olyan pozitív egész létezik, amely az α-nak nem racionális hatványa. Ezek a 9.3.5 Tétel szerint az α-nak szükségképpen transzcendens kitevőjű hatványai.
Transzcendens: Az α-nak kontinuum sok transzcendens kitevőjű hatványa van, és ezek közül csak megszámlálható sok lehet algebrai szám.

9.4.

9.4.1 b) A 9.4.2 Tételben megadott szám Liouville-szám, és így az a) részből következik, hogy végtelen sok Liouville-szám van. — Kontinuum: A 9.4.2 Tétel bizonyításához hasonlóan adódik, hogy a $10^{-k!}$ sorozat tetszőleges végtelen részsorozatából képzett végtelen sor is Liouville-szám.

9.4.2

a) Legyen $f = f_1 \dots f_k$ az f felbontása $\mathbf{Q}$ felett irreducibilis polinomok szorzatára. Ekkor a szóban forgó (12) diofantikus egyenlet a

$$g_j(y,z) = y^{n_j} f_j\Big(\frac{z}{y}\Big) = b_j, \qquad j = 1, 2, \dots, k$$

egyenletrendszerekre vezethető vissza, ahol $\prod_{j=1}^{k} b_j = b$. Így $b \neq 0$ esetén csak véges sok ilyen egyenletrendszert kapunk, és ezek mindegyikének (sőt már akármelyik egyenletnek is) a(z eredeti) 9.4.4 Tétel szerint csak véges sok megoldása lehet. Ha $b = 0$, akkor legalább az egyik $b_j = 0$, tehát ismét csak véges sok egyenletet kell nézni, és ezek mindegyikének csak véges sok megoldása lehet.

b) A 9.4.4 Tétel bizonyításában csak ezeket a tulajdonságokat használtuk fel.

9.4.3 Kövessük a 9.4.4 Tétel bizonyításának a gondolatmenetét. Ha z_i/y_i-nek nincs korlátos részsorozata, akkor cseréljük meg z_i és y_i szerepét, azaz $f(z_i/y_i)$ helyett tekintsük $f(y_i/z_i)$-t. A 9.4.3 Tétel (ii) állítását elég (például a $\kappa = 0{,}99$ speciális esetben alkalmazni.

9.4.4 Használjuk fel, hogy ha az f polinomnak α többszörös gyöke, akkor α gyöke az f deriváltjának is.

9.5.

9.5.1 Alkalmazzunk a 9.5.1 Tétel bizonyításához hasonló gondolatmenetet.

9.5.2

a) Írjuk fel $\sin 1$-re, illetve $\cos 1$-re a $\sin x$, illetve $\cos x$ hatványsorából adódó végtelen sort, és alkalmazzuk a 9.5.1 Tétel gondolatmenetét.

b) Bizonyítsunk indirekt a 9.5.2 Tétel bizonyításának a mintájára: az ottani I integrálban $\sin(\pi x)$ helyére tegyünk $\sin(rx)$-et, és a legyen most az $1/r$, $\cos r$ és $\sin r$ racionális számok közös nevezője.

c) Fejezzük ki $\sin(2x)$-et és $\cos(2x)$-et $\operatorname{tg} x$ segítségével. Innen látszik, hogy ha $\operatorname{tg} r$ racionális, akkor $\sin(2r)$ és $\cos(2r)$ mindketten racionálisak, ami ellentmond a b) résznek.

9.5.3 Használjuk fel, hogy a 9.5.2 Tétel bizonyításában minden második parciális integrálásnál $\sin \pi = \sin 0 = 0$ miatt a „kiintegrált rész” 0. Ebből adódik, hogy két parciális integrálást együttesen egy lépésnek tekintve, tulajdonképpen mindig csak összesen egy új „kiintegrált tag” keletkezik,

amelynek „nevezője” mindig π^2-szerese az előzőnek. Így a $\pi^2 = a/b$ indirekt feltevésből kiindulva a

$$\pi a^{n+1} \int_0^1 \sin(\pi x) f(x) dx$$

integrál vizsgálatával a 9.5.2 Tétel gondolatmenetét követve ellentmondásra fogunk jutni.

9.6.

9.6.1 Az $\overline{\alpha}$ minimálpolinomja ugyanaz, mint az α minimálpolinomja, a másik három szám pedig rendre előállítható α-ból és $\overline{\alpha}$-ból a következő műveletek segítségével: összeadás; kivonás és i-vel való szorzás; szorzás és négyzetgyökvonás.

9.6.2 Csak c) algebrai egész. — Útmutatás d)-hez: Tegyük fel indirekt, hogy $\cos 1^\circ$ algebrai egész, és mutassuk meg, hogy ekkor $\sin 1^\circ$ is az, sőt az összegzési képletek alapján bármely k egészre $\cos k^\circ$ és $\sin k^\circ$ is algebrai egész. Ez azonban például $k = 30$-ra nem igaz.

9.6.3 Igaz: a), c), e), f), h).

9.6.4 Létezik, például $x = y = 1$, $z = \sqrt[n]{2}$ megfelel.

9.6.5 Igaz: a), c), d).

9.6.6 Mivel α algebrai szám, ezért alkalmas a_i egész számokra

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0, \qquad \text{ahol} \qquad a_n \neq 0.$$

Ezt a_n^{n-1}-gyel szorozva és átalakítva kapjuk, hogy $a_n\alpha$ algebrai egész, azaz α előáll egy algebrai egész és az a_n egész szám hányadosaként. Ha ezt α helyett $1/\alpha$-ra alkalmazzuk, akkor az adódik, hogy α felírható egy egész számnak és egy algebrai egésznek a hányadosaként (ha $\alpha = 0$, akkor pedig ez triviálisan igaz).

9.6.7 Az α (normált, egész együtthatós) minimálpolinomjában a konstans tag ± 1.

9.6.8

a) Megfelel például $\beta_n = (\sqrt{2} - 1)^n$.

b) Legyen $\beta_n = \sqrt[n]{\alpha}$.

c) Legyen az α algebrai egész minimálpolinomja $a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ (ahol minden a_i egész), ekkor α/b minimálpolinomja $a_0 + a_1bx + \ldots + a_{n-1}b^{n-1}x^{n-1} + b^nx^n$. Ezt normálva a konstans tag csak úgy lesz egész, ha $b^n \mid a_0$, tehát csak véges sok ilyen b egész létezik (hiszen $\alpha \neq 0$ miatt $a_0 \neq 0$).

9.6.9 Mindkét kérdésre igenlő a válasz, megfelel például $\cos\varphi + i\sin\varphi$, ahol a) $\cos\varphi = 1/3$; b) $\cos\varphi = \sqrt{2} - 1$.

9.6.10

a) A 8.4.1 Tétel alapján például az $a + b\sqrt[n]{2}$ alakú számok, ahol a és b egész szám, mindenütt sűrűek a számegyenesen.

b) A másodfokú egyenlet megoldóképletéből adódik, hogy bármely nem valós másodfokú algebrai egész valós része csak 2 nevezőjű tört lehet, ezért a másodfokú algebrai egészek nem lesznek mindenütt sűrűek a számsíkon. A negyedfokúak viszont igen: az $(a + b\sqrt{2}) + i(c + d\sqrt{2})$ alakú számok, ahol a, b, c és d egész szám, „általában" negyedfokú algebrai egészek, és mindenütt sűrűek a síkon.

9.6.11

a) Mivel racionális r esetén $\alpha = \cos r^\circ + i\sin r^\circ$ egységgyök, és így algebrai egész, ezért $2\mathrm{Re}\,\alpha = 2\cos r^\circ$ is algebrai egész. Ha $2\cos r^\circ$ emellett még racionális is, akkor csak egész szám lehet. Így $\cos r^\circ$ értéke 0, $\pm 1/2$ vagy ± 1. — A feladatot megoldhatjuk az algebrai egészek felhasználása nélkül is. Ha r racionális, akkor van olyan n pozitív egész, amelyre nr a 360-nak egész számú többszöröse, azaz $\cos(nr^\circ) = 1$. A

$$\cos(n\alpha) = 2\cos\big((n-1)\alpha\big)\cos\alpha - \cos\big((n-2)\alpha\big)$$

összefüggés alapján igazoljuk teljes indukcióval, hogy $2\cos(n\alpha)$ a $2\cos\alpha$-nak egy egész együtthatós, normált polinomja. Ebből következik, hogy ha $\cos(nr^\circ) = 1$, akkor $2\cos r^\circ$ gyöke egy egész együtthatós, normált polinomnak. Egy ilyen polinom racionális gyökei csak egészek lehetnek, tehát $2\cos r^\circ$ egész szám.

b) Az r és $\sin r^\circ$ értékek közül legalább az egyik irracionális, kivéve ha r olyan egész szám, amely a 30-nak páratlan többszöröse vagy pedig osztható 180-nal.

Tegyük fel, hogy $\mathrm{tg}\, r^\circ$ értelmezve van, azaz az r nem páratlan többszöröse 90-nek. Ekkor az r és $\mathrm{tg}\, r^\circ$ értékek közül legalább az egyik irracionális, kivéve ha r olyan egész szám, amely a 45-nek páratlan többszöröse vagy pedig osztható 180-nal.

A szinuszra vonatkozó állítás azonnal adódik az a) részből és a $\sin r^\circ = \cos(90 - r)^\circ$ összefüggésből, a tangensre vonatkozó állítás pedig ezután a 9.5.2c) feladathoz adott útmutatás szerint következik.

10. Algebrai számtestek

10.1.

10.1.1 Az $L \subseteq T \subseteq M$ bővítéslláncban a fokszámtétel szerint valamelyik láncszem elsőfokú.

10.1.2 a) 2. b) ∞. c) ∞.

10.1.3

a) Az egyik irány nyilvánvaló, a másik pedig következik a 9.3.6 Tételből.

b) (b1) 1. (b2) 2. (b3) 2. (b4) 3.

10.1.4

a) Igaz: (a1).

b) $m_{\vartheta,M} \mid m_{\vartheta,L}$ és $\deg_M \vartheta \le \deg_L \vartheta$.

10.2.

10.2.1 A 10.2.2 Tétel alapján a $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$ egyenlőséghez elég azt igazolni, hogy $\alpha \in \mathbf{Q}(\beta)$ és $\beta \in \mathbf{Q}(\alpha)$.

10.2.2

a) Ez legegyszerűbben a 10.2.2 Tételből következik.

b) $\mathbf{Q}(\alpha)$ altér a $\mathbf{Q}$ feletti $\mathbf{Q}(\vartheta)$ véges dimenziós vektortérben, és egy véges dimenziós V vektortér egy U alterére $U = V$ pontosan akkor teljesül, ha $\dim U = \dim V$.

c) A ϑ és α számok pontosan a megadott feltétel esetén fejezhetők ki kölcsönösen egymással a 10.2.1 Definícióban megadott módon.

10.2.3 Igaz: b), d). (Ezek igazolásánál ne felejtkezzünk el arról, hogy ϑ transzcendens szám is lehet.)

10.2.4 a) $12 + 2\sqrt[3]{2} + 9\sqrt[3]{4}$. b) $\frac{1}{2}\sqrt[3]{4}$. c) $\frac{9}{17} - \frac{1}{17}\sqrt[3]{2} + \frac{2}{17}\sqrt[3]{4}$.

10.2.5 a) 4. b) 10. c) 7. d) 4.
Útmutatás: Az alábbi két észrevételt érdemes felhasználni: (i) Ha α eleme egy véges bővítésnek, akkor $\deg \alpha$ osztója a bővítés fokának.
(ii) Ha α algebrai és egy k-adfokú szám eleme $\mathbf{Q}(\alpha)$-nak, akkor $k \mid \deg \alpha$.

10.2.6 a) $\emptyset$. b) $\mathbf{Q}(\sqrt[3]{7})$. c) $\mathbf{Q}(\sqrt{5})$.
Útmutatás b)-hez: Használjuk fel, hogy $\mathbf{Q}(\sqrt[3]{7})$ része a metszetnek, és a metszet ($\mathbf{Q}$ feletti) foka osztója mindkét bővítés fokának. — Másik lehetőség: A metszet egy tetszőleges elemét írjuk fel a 10.2.3 Tételnek megfelelően egyrészt mint $\mathbf{Q}(\sqrt[6]{7})$-beli, másrészt mint $\mathbf{Q}(\sqrt[9]{7})$-beli elemet.

Mindkét előállítást tekintsük most mint ugyanannak a $\mathbf{Q}(\sqrt[18]{7})$-beli elemnek a 10.2.3 Tétel szerinti felírását, ekkor ennek az előállításnak az egyértelműségéből adódik a jelzett eredmény.

10.2.7 a) $\mathbf{Q}$. b) $\mathbf{Q}(\sqrt[3]{3})$. c) $\mathbf{Q}(\sqrt{2})$.

10.2.8 Induljunk ki a $|\vartheta| = 1$-ből adódó

$$\operatorname{Re}\vartheta = \frac{\vartheta + \overline{\vartheta}}{2} = \frac{1}{2}\big(\vartheta + \frac{1}{\vartheta}\big)$$

összefüggésből. (A bizonyítás során ne feledkezzünk el arról, hogy ϑ transzcendens szám is lehet.)

10.2.9 A bővítések és a fokszámok vizsgálatából vezessük le, hogy $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt[7]{5})$. (Használjuk fel a 10.2.5 és 10.2.3 Tételeket, valamint a 10.2.2 feladatot.)

10.2.10 Válasz: k, illetve $k/2$ (ez utóbbi nyilván csak páros k esetén fordulhat elő). — Útmutatás: Alkalmazzuk a fokszámtételt a $\mathbf{Q} \subseteq \mathbf{Q}(\beta^2) \subseteq \mathbf{Q}(\beta)$ bővítésláncra. (Páros k esetén mutassunk példát mindkét lehetőség megvalósulására.)

10.2.11 Válasz: ± 1. — Útmutatás: A 10.2.8 feladathoz hasonló gondolatmenetet alkalmazva tekintsük a $\mathbf{Q} \subseteq \mathbf{Q}(\operatorname{Re}\vartheta) \subseteq \mathbf{Q}(\vartheta)$ bővítésláncot. — Másik lehetőség: Mutassuk meg, hogy ϑ-nak és $1/\vartheta$-nak ugyanaz a minimálpolinomja, és ennek felhasználásával lássuk be, hogy az 1 vagy a -1 gyöke ennek a minimálpolinomnak.

10.2.12 Az a) rész a 10.2.6 (vagy a 9.3.1), a b) rész pedig a 10.2.7 (vagy a 9.3.6) Tételre adott bizonyításból következik.

10.2.13

a) A $\Leftarrow$ irány nyilvánvaló, a $\Rightarrow$ irány pedig abból adódik, hogy ϑ transzcendenciája miatt $(g_1h_2 - g_2h_1)(\vartheta) = 0$ csak a $g_1h_2 - g_2h_1 = 0$ esetben lehetséges.

b) Az a) rész alapján a

$$\frac{g(x)}{h(x)} \mapsto \frac{g(\vartheta)}{h(\vartheta)}$$

megfeleltetés bijekció a $\mathbf{Q}$ feletti algebrai törtek és $\mathbf{Q}(\vartheta)$ között, a művelettartás pedig nyilvánvaló.

10.3.

10.3.1

a) A 10.3.5 Tétel bizonyításának $E(\sqrt{2})$ részéhez hasonlóan igazoljuk, hogy $E(\sqrt{3})$-ban a norma abszolút értéke szerint elvégezhető a maradékos osztás.

(b1) Mindkét felbontásban felbonthatatlanok szerepelnek, ezek azonban csak egységtényezőkben különböznek:

$$5+3\sqrt{3}=(2+\sqrt{3})(1+\sqrt{3}) \qquad \text{és} \qquad -4+3\sqrt{3}=(2-\sqrt{3})(1+2\sqrt{3}).$$

(b2) Mindkét felbontásban szerepel olyan tényező, amely nem felbonthatatlan.

c) Alkalmazzuk a 10.3.8 Tételt. — Az összes prímet (egységszerestől eltekintve) a pozitív prímszámok felbontásából nyerjük:

(c1) $3=(\sqrt{3})^2$; $2=\varepsilon(1+\sqrt{3})^2$, ahol $\varepsilon=2-\sqrt{3}$ egység.

(c2) Ha $p\equiv\pm5 \pmod{12}$, akkor p prím.

(c3) Ha $p\equiv\pm1 \pmod{12}$, akkor p két prím szorzata, amelyek nem egymás egységszeresei.

d) Megoldhatóság esetén a megoldásszám végtelen, lásd a 7.8.3 feladatot. Az egyenlet akkor és csak akkor oldható meg, ha n kanonikus alakjában minden $12k\pm5$ alakú prímszám kitevője páros, továbbá a 2, a 3 és a $12k-1$ alakú prímszámok kitevőjének az összege is páros. — Útmutatás: Használjuk fel a c) rész eredményét, és kövessük a két-négyzetszám-tétel bizonyításának gondolatmenetét. Vegyük figyelembe, hogy minden egység normája $+1$. A 2, a 3 és a $12k-1$ alakú prímszámok kitevőjét azért kell vizsgálni, mert az ezeknek a prímszámoknak a felbontásából származó $E(\sqrt{3})$-beli prímek normája negatív, így ha a szóban forgó kitevőösszeg páratlan, akkor n helyett $-n$ áll elő x^2-3y^2 alakban.

10.3.2

a) A Gauss-egészekhez hasonlóan igazolható, hogy a norma szerint elvégezhető a maradékos osztás.

b) A 10.3.8 Tételből következik, hogy az összes prímet (egységszerestől eltekintve) a pozitív prímszámok felbontásából nyerjük, a következőképpen:

(b1) $2=-(\sqrt{-2})^2$.

(b2) Ha $p\equiv5$ vagy $7 \pmod{8}$, akkor p prím.

(b3) Ha $p\equiv1$ vagy $3 \pmod{8}$, akkor p két prím szorzata, amelyek nem egymás egységszeresei.

c) Válasz: $x=\pm5$, $y=3$. — Útmutatás: Az $(x+\sqrt{-2})(x-\sqrt{-2})=y^3$ bal oldalán a két tényező közös prímosztója csak $\sqrt{-2}$ lehet, ebből azonban következik, hogy x páros, ami az eredeti egyenlet modulo 4 vizsgálatával ellentmondásra vezet. A két tényező így relatív prím, és mivel az egységek

csak a ± 1, amelyek maguk is köbszámok, ezért mindkét tényező teljes köb. Az eredmény ezután az $x + \sqrt{-2} = (a + b\sqrt{-2})^3$ egyenlőségben a $\sqrt{-2}$ együtthatójának összehasonlításából adódik.

10.3.3 Tekintsük például az alábbi felbontásokat:

a) $(1 + \sqrt{15})(1 - \sqrt{15}) = (-2) \cdot 7$.

b) $(1 + \sqrt{26})(1 - \sqrt{26}) = (-5) \cdot 5$.

c) $(2 + \sqrt{-6})(2 - \sqrt{-6}) = 2 \cdot 5$.

d) $(2 + \sqrt{-10})(2 - \sqrt{-10}) = 2 \cdot 7$.

10.3.4 Kövessük a Gauss-, illetve Euler-egészeknél látott gondolatmenetet (7.4.8 Tétel). Ha $t \not\equiv 1 \pmod 4$, akkor $E(\sqrt{t})$ elemei egy téglalaprácsot alkotnak a komplex számsíkon, ahol az „alaptéglalap" vízszintes oldala 1, függőleges oldala pedig $\sqrt{|t|}$ hosszúságú. A maradékos osztáshoz arra van szükség, hogy a rácspontok köré rajzolt egységkörök belseje tartalmazza $\mathbf{Q}(\sqrt{t})$ minden elemét. Ez biztosan teljesül, ha a körök lefedik az egész síkot, azaz $\sqrt{|t|} < \sqrt{3}$, vagyis $t = -1$ vagy -2, továbbá biztosan nem teljesül, ha az $1/2$ abszcisszájú függőleges egyenesen egy szakasz lefedetlen marad, azaz $\sqrt{|t|} > \sqrt{3}$, vagyis $t < -3$ (mivel $-3 \equiv 1 \pmod 4$, ezért $t = -3$ most nem jöhet szóba). Hasonlóan okoskodhatunk a $t \equiv 1 \pmod 4$ esetben is, ekkor egy olyan paralelogrammarácsról van szó, ahol az alapparalelogramma vízszintes oldala 1 hosszúságú, a magassága $\frac{1}{2}\sqrt{|t|}$, és a vízszintes oldalhoz tartozó magasság talppontja az oldal felezőpontjában van.

10.3.5 Használjuk fel a 10.3.8/(vii) Tételt.

10.3.6 Lássuk be, hogy bármely $0 \leq n \leq k - 2$ esetén $n^2 + n + k = N(\alpha_n)$, ahol α_n felbonthatatlan $E(\sqrt{-4k+1})$-ben. Ebből vezessük le, hogy ha valamely n-re $N(\alpha_n)$ nem lenne prímszám, akkor $N(\alpha_n)$ kétféleképpen bomlana felbonthatatlanok szorzatára.

10.3.7 A felbonthatatlanság azonnal adódik a norma tulajdonságaiból. — Az állítás másik részéhez először lássuk be, hogy a feltétel alapján minden $\beta \in E(\sqrt{t})$-hez létezik olyan b egész szám, amelyre $\alpha \mid \beta - b$. Ekkor α prím volta a következőképpen igazolható:

$$\alpha \mid \beta\gamma \Longrightarrow \alpha \mid bc \Longrightarrow \pm p = N(\alpha) \mid b^2c^2 \Longrightarrow$$
$$\Longrightarrow p \mid b \text{ vagy } p \mid c \Longrightarrow \alpha \mid b \text{ vagy } \alpha \mid c \Longrightarrow \alpha \mid \beta \text{ vagy } \alpha \mid \gamma.$$

10.3.8 Mivel β^2/α^2 algebrai egész, ezért a négyzetgyöke, β/α is az. Emellett $\beta/\alpha \in \mathbf{Q}(\sqrt{t})$, tehát $\beta/\alpha \in E(\sqrt{t})$ is teljesül.

10.3.9

a) $5 = -(\sqrt{-5})^2$.

b) A 10.3.5 Tétel bizonyításában láttuk, hogy a 2 felbonthatatlan, továbbá

$$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5}), \qquad \text{de} \qquad 2 \nmid 1 \pm \sqrt{-5},$$

tehát a 2 nem prím.

c) Használjuk fel a 10.3.7 Tételt, és azt, hogy $\left(\frac{-5}{p}\right) = -1$ pontosan a megadott alakú p prímszámokra teljesül.

d) Az, hogy ezek nem prímek, az előzőkből következik, a felbonthatatlanság pedig azért igaz, mert egy ilyen p (sőt általában egy $10s \pm 3$ alakú szám) nem lehet egy $E(\sqrt{-5})$-beli elem normája.

e) Azt kell igazolni, hogy ezek a p prímek előállnak normaként, azaz (egész a, b-vel) $p = a^2 + 5b^2$ alakban, hiszen ekkor $p = (a + b\sqrt{-5})(a - b\sqrt{-5})$. Az $x^2 \equiv -5 \pmod{p}$ kongruencia megoldhatóságát felhasználva a 8.2.4 Tétel bizonyításának a mintájára vagy a 7.5.21a feladatban szereplő Thue-lemma segítségével mutassuk meg, hogy a p-nek egy kis többszöröse előáll a^2+5b^2 alakban, majd ebből vezessük le, hogy akkor maga a p is felírható így.

10.4.

10.4.1

a) $\pm\sqrt{2} \pm \sqrt{3}$.

b) $\sqrt{2}(\pm 1 \pm i)$.

c) $\cos 20^\circ$, $\cos 140^\circ$, $\cos 260^\circ$.

d) $\cos k^\circ + i \sin k^\circ$, ahol $1 \le k \le 360$, k egész és $(k, 360) = 1$.

10.4.2

a) A ϑ minimálpolinomjára a gyökök és együtthatók közötti összefüggést alkalmazva kapjuk, hogy $\vartheta_{(1)} + \vartheta_{(2)}$ racionális, és így $\vartheta_{(2)} \in \mathbf{Q}(\vartheta_{(1)})$.

b) Létezik olyan $\vartheta_{(j)}$, amely valós szám, tehát $\mathbf{Q}(\vartheta_{(j)}) \subseteq \mathbf{R}$, és így $\mathbf{Q}(\vartheta_{(j)}) \neq \neq \mathbf{Q}(\vartheta)$.

c) A $\mathbf{Q} \subseteq \mathbf{Q}(\vartheta_{(j)}) \cap \mathbf{Q}(\vartheta_{(k)}) \subseteq \mathbf{Q}(\vartheta_{(j)})$ bővítéslánccban a két láncszem fokának a szorzata 3, így az állításhoz csak azt kell igazolni, hogy bármelyik két $\mathbf{Q}(\vartheta_{(j)})$ különböző. Lássuk be, hogy ha a három $\mathbf{Q}(\vartheta_{(j)})$ közül valamelyik kettő megegyezik, akkor a harmadik is ugyanez kell hogy legyen. Ez azonban ellentmond a feladat b) részének.

10.4.3 (Az R.K. rövidítés a relatív konjugáltakat jelöli.)

a) R.K.: $1 \pm \sqrt[4]{2}$, $1 \pm i\sqrt[4]{2}$. $\quad N(\alpha) = -1$.

b) R.K.: $1 \pm \sqrt{2}$ kétszeres multiplicitással. $\quad N(\beta) = 1$.

c) R.K.: $(1 \pm \sqrt[4]{2})(1 + \sqrt{2})$, $(1 \pm i\sqrt[4]{2})(1 - \sqrt{2})$. $\quad N(\gamma) = -1$.

10.4.4 Kövessük a 10.3.4 Tétel bizonyításának a gondolatmenetét. (Figyeljünk arra, hogy az ε relatív konjugáltjai általában nem elemei $\mathbf{Q}(\vartheta)$-nak, viszont a szorzatuknak az ε-nal vett hányadosa már igen.)

10.4.5

a) Például $(3+4i)/5$ megfelel.

b) Legyen a másodfokú bővítés $\mathbf{Q}(\sqrt{t})$ alakú, ahol t négyzetmentes egész és $t \neq 1$, és legyen $p > 2$ egy olyan prím, amelyre $\left(\frac{t}{p}\right) = 1$. Ekkor az $x^2 - t \equiv 0 \pmod{p}$, és így az $x^2 - t \equiv 0 \pmod{p^2}$ kongruencia is megoldható, azaz létezik olyan c egész szám, amelyre $(c+\sqrt{t})/p$ nem algebrai egész, de a normája egész szám.

10.5.

10.5.1 a) -4. b) -3. c) -108. d) $2^{n-1}n^n(-1)^{(n-1)(n-2)/2}$.
Útmutatás d)-hez: A keresett diszkrimináns egy Vandermonde-determináns négyzete, ezt a determináns önmagával való (sor-oszlop) szorzásával érdemes kiszámítani.

10.5.2

a) Ekkor

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = C \begin{pmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{pmatrix},$$

ahol C egész elemű mátrix, és így a 10.5.3/(iii) Tétel szerint

$$\Delta(\beta_1, \ldots, \beta_n) = \Delta(\omega_1, \ldots, \omega_n)(\det C)^2 .$$

b) Az a) rész szerint a két diszkrimináns egymásnak kölcsönösen pozitív egész számszorosa.

10.5.3 A másodfokú bővítések $\mathbf{Q}(\sqrt{t})$ alakúak, ahol t négyzetmentes egész szám és $t \neq 1$. A keresett diszkrimináns $4t$, ha $t \not\equiv 1 \pmod 4$, és t, ha $t \equiv 1 \pmod 4$.

10.5.4 A 10.5.2 feladatnál látott gondolatmenetet érdemes alkalmazni.

10.5.5

a) A keresett feltétel: $a, b, c, d \in \mathbf{Z}$ és $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1$.

b) Legyen $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$. Ekkor az $a + b\omega$ és $c + d\omega$ Euler-racionálisok pontosan akkor alkotnak egész bázist, ha a, b, c, d-re teljesül az a) résznél megadott feltétel.

10.5.6 Azokban a $\mathbf{Q}(\sqrt{t})$ bővítésekben, ahol (t négyzetmentes egész szám, $t \neq 1$ és) $t \equiv 1 \pmod 4$.

10.5.7 Közvetlenül következik a diszkrimináns definíciójából. — Másik lehetőség: Alkalmazzuk a 10.5.3/(iii) Tételt az $\alpha_i = \vartheta^{i-1}$ szereposztással, és használjuk ki, hogy $\Delta(1, \vartheta, \dots, \vartheta^{n-1})$ egy olyan Vandermonde-determináns négyzete, amelynek a generátorai valós számok.

10.5.8

a) Például $\mathbf{Q}(i)$-ben $1/2$ és $2i$ megfelel.

b) Használjuk fel, hogy ha az $r_1, \dots, r_n$ racionális számok szorzata 1, akkor $\Delta(r_1\alpha_1, \dots, r_n\alpha_n) = \Delta(\alpha_1, \dots, \alpha_n)$.

11. Ideálok

11.1.

11.1.1 a) (2). b) $(1 + i)$. c) Nem ideál.
d) $(1 + i)$. e) Nem ideál. f) (7).

11.1.2 a) $(2x - 1)$. b) $([x^2 - 2][x^2 - 3])$. c) Nem ideál.
d) $(x - 3, 2)$. e) Nem ideál.

11.1.3 Legyen R test és $I \neq 0$ ideál R-ben. Azt kell igazolni, hogy $I = R$. Ha $a \neq 0$ eleme I-nek és b tetszőleges eleme R-nek, akkor az osztás elvégezhetősége miatt van olyan $c \in R$, amelyre $ca = b$, azaz $b \in I$, vagyis $I = R$. — A megfordításnál vegyünk R-ben egy $a \neq 0$ elemet. Ekkor a feltétel szerint $(a) = R$, tehát bármely $b \in R$-re $b \in (a)$. Ez azt jelenti, hogy alkalmas c-vel $ca = b$ teljesül, vagyis elvégezhető R-ben az osztás, és így R valóban test.

11.1.4 Legyen $I = (\xi_1 2^{1/k_1}, \dots, \xi_n 2^{1/k_n})$, ahol $\xi_1, \dots, \xi_n \in E$. Ekkor I minden eleme $\xi 2^{1/m}$ alakú, ahol $\xi \in E$ és $m = [k_1, \dots, k_n]$. Mivel (például) $2^{1/(m+1)}$ nem lehet ilyen alakú, ezért $I \neq K$, vagyis K nem generálható véges sok elemmel.

11.1.5 Mutassuk meg, hogy az egyik ideál generátorai kifejezhetők a másik generátorainak a segítségével, és viszont.

11.1.6

a) a1: 4, a2: 9, a3: 5.
Test: a2, a3.

b) Ha $\alpha \neq 0$, akkor $G/(\alpha)$ elemszáma $N(\alpha)$, és $G/(\alpha)$ akkor és csak akkor test, ha α Gauss-prím. — Útmutatás: A „modulo α maradékosztályok" számának meghatározásához lásd a 7.7.12 feladathoz adott útmutatást. A másik állítás ahhoz hasonlóan bizonyítható, ahogyan azt igazoltuk, hogy $\mathbf{Z}/(m)$ akkor és csak akkor test, ha m prím (2.8.4 Tétel, természetesen azt is végig kell gondolni, hogy az ehhez felhasznált valamennyi korábbi tétel megfelelője is átvihető a Gauss-egészekre).

11.1.7

a) Alkalmazzunk ahhoz hasonló gondolatmenetet, mint amikor (a 11.1.3 Tétel utáni Példák között) azt igazoltuk, hogy $\mathbf{Z}[x]$-ben $(2, x)$ nem főideál.

b) b1: 2, test. b2: 6, nem test. b3: 121, test.

11.1.8

a) Test: a2.

b) $T[x]/(f)$ test $\iff$ f irreducibilis T felett.

c) A faktorgyűrűnek 4 eleme van (a maradékosztályok az $a_0 + a_1 x$ maradékokkal reprezentálhatók, ahol $a_i = 0$ vagy 1), és egyszerűen ellenőrizhető, hogy a három darab $\neq 0$ elemnek létezik inverze. — Másik lehetőség: A faktorgyűrű izomorf $S = \mathbf{Z}_2[x]/(x^2 + x + 1)$-gyel, ahol $\mathbf{Z}_2$ a modulo 2 maradékosztályok teste. Ekkor S a feladat b) része alapján test.

11.1.9

a) Kövessük a 11.1.6 Tétel utáni Példánál a $\vartheta = \sqrt{2}$ speciális esetben látott gondolatmenetet. A bizonyítás lényege: $\mathbf{Q}[x]$-nek az (m_ϑ) főideál szerinti egy-egy maradékosztályát egyértelműen jellemzi az adott osztályba eső polinomoknak az m_ϑ polinommal való osztási maradéka, és az ezekkel a maradékokkal való számolásnál az egyetlen „szabály" az, hogy az m_ϑ többszörösei „nem számítanak". Ez pontosan megfelel a $\mathbf{Q}(\vartheta)$-beli elemek szokásos felírásának és az ottani (kizárólag az $m_\vartheta(\vartheta) = 0$ összefüggést felhasználó) számolásnak. — Másik lehetőség: A $\mathbf{Q}[x]$-ből $\mathbf{Q}(\vartheta)$-ba az $f \mapsto f(\vartheta)$ leképezés gyűrűhomomorfizmus, amelynek a képe $\mathbf{Q}(\vartheta)$, a magja pedig az m_ϑ által generált főideál. Így az állítás következik a gyűrűk homomorfizmustételéből.

b) Az a) rész általánosítását szem előtt tartva legyen $M = L[x]/(f)$. Az f irreducibilitását felhasználva igazolható, hogy M test, a konstans+(f) maradékosztályok halmaza megfelel L^*-nak, az $x + (f)$ maradékosztály pedig ϑ-nak.

11.1.10

a) Az állítást elég főideálokra igazolni, ugyanis ha $\alpha \in I$, akkor $(\alpha) \subseteq I$ miatt az I szerinti maradékosztályok száma legfeljebb annyi, mint az (α) szerinti maradékosztályok száma. Legyen tehát $\alpha \neq 0$, és mutassuk meg, hogy „modulo α" csak véges sok maradék létezik. Legyen $\omega_1, \ldots, \omega_n$ egész bázis $E(\vartheta)$-ban. Ekkor bármely $\xi \in E(\vartheta)$ felírható $\xi = k_1\omega_1 + \ldots + k_n\omega_n$ alakban, ahol $k_i \in \mathbf{Z}$, $i = 1, \ldots, n$. Mivel $\alpha \mid N(\alpha)$, ezért minden modulo α maradékosztálynak van olyan ξ reprezentánsa, ahol $0 \leq k_i < |N(\alpha)|$, $i = 1, \ldots, n$.

b) Ekkor az R/A_j faktorgyűrűk elemszáma szigorúan monoton csökken. Ez azonban lehetetlen, hiszen $A_2 \neq 0$ miatt R/A_2-nek csak véges sok eleme van.

c) Ha egy $I \neq 0$ ideál nem lenne végesen generált, akkor létezne benne ideáloknak egy szigorúan növő

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \ldots$$

lánca.

11.2.

11.2.1 a) (5). b) (60).

11.2.2 a) 4. b) 16.

11.2.3 Fogalmazzuk át a feladatot oszthatóságra a 11.2.1 Tétel felhasználásával.

11.2.4

a) A 2 és az $1+\sqrt{-5}$ egyaránt közös osztók, nincs azonban olyan közös osztó, amely ezeknek többszöröse lenne.

b) (2), $(1+\sqrt{-5})$, (1).

c) Például $\alpha = 2$, $\beta = 1 + \sqrt{-5}$.

11.3.

11.3.1

a) A normált minimálpolinomjuk egész együtthatós és a konstans tag 1 vagy -1 (lásd a 9.6.7 feladatot).

b) $\alpha = \sqrt{\alpha}\sqrt{\alpha}$.

11.3.2

a) Ha $a \neq 0$ és b tetszőleges, valamint ha $a = b = 0$.

b) Minden $a \neq 0$ egység, és így eleve nem léteznek felbonthatatlanok, illetve prímek.

c) Alaptétel: az állítás „üres”, hiszen a 0-tól és egységektől különböző elemekre vonatkozik, ilyenek azonban testben nincsenek. — Főideálgyűrű: testben csak a triviális (0) és (1) ideálok léteznek (lásd a 11.1.3 feladatot), és ezek valóban főideálok. — Euklideszi gyűrű: mivel elvégezhető az osztás, ezért mindig elérhető, hogy a maradék 0 legyen (és így „tetszőleges” függvény megfelel f-nek).

11.3.3

a) Ez a 2.

b) Az eljárással most egy egységet kapunk, és annak nincs felbonthatatlan osztója.

c) Az 1.5.5c feladat útmutatásához hasonlóan konstruálhatunk megfelelő f-et.

d) (0), (1), (2), (2^2), (2^3), ...

11.3.4 A 11.1.1 Definíció követelményeinek a teljesülését kell ellenőrizni.

11.3.5 Útmutatás a szükségességhez: Ha $R[x]$ főideálgyűrű, akkor tetszőleges a konstans polinommal (a, x) is főideál.

11.3.6 Mutassuk meg, hogy ha $c \neq 0$ olyan elem, amelyre $f(c)$ minimális, akkor c egység. Ekkor $c \mid c$ is teljesül, azaz alkalmas e-vel $ec = c$. A nullosztómentesség felhasználásával igazoljuk, hogy e egységelem.

11.3.7 Igaz: a).

11.3.8 A legkisebb abszolút értékű maradék szerinti maradékos osztás kielégíti a feltételt, azaz ha ($b \neq 0$ és) $a = bq + r$, ahol $|r| \leq |b|/2$, akkor $f(r) < f(b)$.

11.3.9

a) Először mutassuk meg, hogy R minden ideálja végesen generált, majd lássuk be, hogy $(a, b) = (d)$, ahol $d = \text{lnko}\{a, b\}$.

b) Következik az a) részből a 11.1.10a feladat alapján.

11.3.10 Az „akkor” részre vonatkozóan lásd a 10.3.4 feladatot és az ahhoz tartozó útmutatást. Megfordítva, ha valamely $t < -3$-ra $E(\sqrt{t})$ euklideszi gyűrű, akkor tekintsünk egy olyan $\beta \neq 0, \pm 1$ elemet, amelyre $f(\beta)$ minimális. Mutassuk meg, hogy $N(\beta) \leq 3$. Ebből már következik, hogy ($t < -3$ esetén) csak $t = -7$ és $t = -11$ lehetséges.

11.4.

11.4.1

a) A 11.4.3 Definíció előtti P1 vagy P2 példákban szereplő A és B ideálok esetén H nem ideál. (P1 esetén például $2 \cdot 3 + [x+3][x-2] = x^2 + x$, P2 esetén pedig $3 \cdot 3 - [1+\sqrt{-5}][1-\sqrt{-5}] = 3$ nem áll elő ab alakban.)

b) Ha $A = (\alpha)$, akkor

$$\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} [r_i \alpha] b_i = \alpha \sum_{i=1}^{n} r_i b_i = \alpha b.$$

11.4.2

a), b) A bizonyítás ugyanúgy történik, mint az egész számoknál.

c) A 11.4.2 Tétel (iv) állításából következik.

d) Használjuk fel c)-t.

e) A szükségességhez legyen $A = (1)$, és használjuk fel c)-t.

11.4.3

a) Ha $\alpha = \beta\gamma$, akkor a 11.4.2 Tételben a (iii) állítás bizonyításából kapjuk, hogy $(\alpha) = (\beta)(\gamma)$. Megfordítva, ha $(\beta)C = (\alpha)$, akkor a 11.4.1b feladathoz adott útmutatás szerint $(\beta)C$ minden eleme, így speciálisan α is osztható β-val.

b) Az a) részből adódó $\gamma = \alpha/\beta$ elem megfelel a feltételeknek.

11.4.4

a) Azt kell igazolni, hogy D ideál, D tartalmazza A-t és B-t, valamint ha C tetszőleges olyan ideál, amelynek része A és B, akkor $D \subseteq C$.

b) Ellentett: $A \subseteq A + B = (0) \Longrightarrow A = (0)$.

c) Az $A(B, C)$ ideál elemei $\sum_{i=1}^{n} a_i[b_i + c_i]$ alakúak, így a zárójelek felbontása után kapjuk, hogy ezek (AB, AC)-nek is elemei. A másik irányú tartalmazáshoz vegyük észre, hogy (AB, AC) elemeit

$$\sum_{i=1}^{n} a_i b_i + \sum_{j=1}^{k} a'_j c_j = \sum_{i=1}^{n} a_i[b_i + 0] + \sum_{j=1}^{k} a'_j[0 + c_j]$$

alakba írva $A(B, C)$-beli elemeket kapunk.

11.4.5 A legkisebb közös többszörös olyan közös többszöröse A-nak és B-nek, amely minden közös többszörösnek osztója. Ezt (5) alapján a tartalmazásra átfogalmazva M a legbővebb olyan ideál, amely része A-nak és B-nek, azaz $M = A \cap B$.

11.4.6 Például $\mathbf{Z}[x]$-ben $A = (x)$, $B = (2, x)$ megfelel.

11.4.7 A (12) $\Rightarrow$ (11) irányt bizonyítsuk indirekt, a megfordításhoz pedig alkalmazzuk (11)-et az $A = (a)$, $B = (b)$ szereposztással.

11.4.8

a1) Csak a két triviális osztója létezik.
a2) Az egyetlen nemtriviális osztó az a1-beli ideál.
a3) Két nemtriviális osztója van: $(2, 1 + \sqrt{-5})$ és $(3, 1 + \sqrt{-5})$.
b) b1: $(2, 1 + \sqrt{-5})$; b2: (1).
c) Felbonthatatlan ideál: c1, c3.

11.4.9 Igaz: b), c), d).

11.4.10

a) $A = (2, x)$, $B = (4, x^2)$, $C = (4, 2x, x^2)$.
b) A 11.4.1b feladat alapján $(\alpha)B = \{\alpha b \mid b \in B\}$, $(\alpha)C = \{\alpha c \mid c \in C\}$, és $\alpha \neq 0$, valamint R nullosztómentessége miatt $\alpha b = \alpha c \Rightarrow b = c$.

11.4.11

a) Ellenőrizzük az ideál definíciójában foglaltak teljesülését.
b) Lássuk be, hogy I maximális ideál, azaz rendelkezik a (9) tulajdonsággal. Ebből könnyen adódik, hogy a megadott hármon kívül I-nek nincs több felbontása. Végül, az $I \cdot I = I$ egyenlőség igazolásához használjuk fel, hogy $x^\alpha = x^{\alpha/2}x^{\alpha/2}$.

11.4.12

a) Ha $P = AB$, akkor egyrészt $P \subseteq A$ és $P \subseteq B$, másrészt a (12)-vel ekvivalens (11) tulajdonság miatt $A \subseteq P$ vagy $B \subseteq P$. Innen kapjuk, hogy $P = A$ vagy $P = B$.
b) Ilyen például $\mathbf{Z}[x]$-ben a $(4, x)$ ideál.
c) Tegyük fel indirekt, hogy M maximális ideál és mégis van olyan $a \notin M$, $b \notin M$, amelyre $ab \in M$. Jelölje (a, M), illetve (b, M) az a-t és az M-et, illetve a b-t és az M-et tartalmazó legszűkebb ideált. Az M maximalitása folytán $(a, M) = (b, M) = R$. Ekkor

$$R = RR = (a, M)(b, M) \subseteq (ab, M) = M,$$

ami ellentmondás.
d) Ilyen például $\mathbf{Z}[x]$-ben az (x) ideál.
e) A maximális ideálra vonatkozó állításhoz mutassuk meg, hogy általában bijekció létesíthető az R-nek az I-t tartalmazó ideáljai és az R/I faktorgyűrű ideáljai között, majd használjuk fel a 11.1.3 feladatot. A prímideálra vonatkozó állítás azonnal adódik a (12) feltételnek az R/I faktorgyűrűre történő átfogalmazásából.

11.5.

11.5.1 Mindkét feltétel ekvivalens $A \mid (\alpha)$ fennállásával.

11.5.2

a) A $N(\alpha)/\alpha$ hányados egyrészt algebrai egész, másrészt eleme $\mathbf{Q}(\vartheta)$-nak.

b) Az a) rész (vagy a 11.5.5 Tétel) szerint A-ban található nemnulla egész szám, így ekkor ennek az egész számú többszörösei is elemei A-nak. Az állítás másik részéhez lássuk be, hogy az összes A-beli egész számot a legkisebb ilyen pozitív egész (egész számú) többszöröseként kapjuk.

11.5.3 Következik a 11.5.8 Tételből.

11.5.4

a) A 11.5.2 feladat alapján bármely P prímideálban van $c > 1$ egész szám. Bontsuk fel c-t prímszámok szorzatára. Mivel P prímideál, ezért ezen prímszámok valamelyike szükségképpen eleme P-nek. Ha P tartalmazna két különböző pozitív prímszámot, akkor az ezek alkalmas egész számokkal képzett kombinációjaként előálló 1-et is tartalmazná, ami lehetetlen.

b) Következik az a) részből.

c) Igen.

d) Nem, ez következik a 11.5.3 feladatból.

11.5.5 Használjuk fel az ideálok legnagyobb közös osztójáról és legkisebb közös többszöröséről tanultakat.

11.5.6 Írjuk fel többféleképpen az $(\alpha)^2$ és $(\beta)^2$ ideálok legnagyobb közös osztóját.

11.5.7

a) $(21) = (3, 4+\sqrt{-5})(3, 4-\sqrt{-5})(7, 4+\sqrt{-5})(7, 4-\sqrt{-5})$. [Természetesen ezek a prímideálok más generátorokkal is megadhatók, például $(3, 4+\sqrt{-5}) = (3, 1+\sqrt{-5}) = (3, 1-2\sqrt{-5}) = (2-\sqrt{-5}, 1+\sqrt{-5})$ stb.]

b) $p = 2$ és 3.

c) $p = 2$, 5, valamint a $20k+1$, $20k+3$, $20k+7$ és $20k+9$ alakú prímek.

11.5.8 Mindkét tulajdonság azzal ekvivalens, hogy $E(\vartheta)$ minden ideálja főideál (lásd a 11.3.9b feladatot, a 11.4.2/(iii) Tételt és a 11.5.8 Tételt).

11.6.

11.6.1 $(2\,,\,\sqrt{-6})(3+\sqrt{-6}) = (3\,,\,\sqrt{-6})(2-\sqrt{-6})$.

11.6.2 Mindkét feltétel ekvivalens azzal, hogy $E(\vartheta)$ főideálgyűrű (vö. a 11.3.9b feladattal).

11.6.3 Használjuk fel, hogy alkalmas u és v pozitív egészekkel $ku = 1 + hv$.

11.6.4
a) Nincs megoldás.
b) $x = 0$, $y = 1$.
c) $x = \pm 985$, $y = 99$.
d) $x = \pm 36$, $y = 11$. — Ne felejtsük el, hogy $-35 \equiv 1 \pmod 4$ miatt $a + b\sqrt{-35} \in E(\sqrt{-35})$ esetén a és b nem feltételenül egész számok.

12. Kombinatorikus számelmélet

12.1.

12.1.1
a) $\lfloor n/2 \rfloor + 1$, azaz $h + 1$, ha $n = 2h$ vagy $2h + 1$. — Útmutatás: Megfelelő számhalmazt alkotnak az $[n/2, n]$ intervallum összes egészei. Annak igazolásához, hogy ennél több szám már nem adható meg, vegyük észre, hogy ha $u + v = a_k$, ahol $0 < u < v$, akkor u és v közül legfeljebb az egyik szerepelhet az a_i-k között.
b) Álljon rögzített r mellett az A_r sorozat az $a_1 + a_2 + \ldots + a_r + a_s$ számokból, ahol $s = r + 1, r + 2, \ldots$ (így A_0 az eredeti sorozat), és jelölje $A_r(n)$ az A_r sorozat n-nél nem nagyobb elemeinek a számát. A feltétel szerint az A_r sorozatok páronként diszjunktak, ezért

$$n \geq \sum_{i=0}^{t} A_i(n) \geq (t+1) A_t(n)$$

bármely n-re és t-re. Másrészt

$$A_t(n) = A\Big(n - \sum_{i=1}^{t} a_i\Big) - t \geq A(n) - \sum_{i=1}^{t} a_i - t.$$

A két egyenlőtlenségből

$$A(n) \leq \frac{n}{t+1} + \sum_{i=1}^{t} a_i + t\,,$$

amit n-nel leosztva, $n \to \infty$ esetén a jobb oldal $1/(t+1)$-hez tart, és mivel t tetszőleges volt, ezért valóban $A(n)/n \to 0$.

12.1.2 Ilyen tulajdonságú és a kívánt „sűrűségű” halmazt alkotnak a 3-mal nem osztható számok. Annak igazolásához, hogy nagyobb sűrűség már nem

lehetséges, vegyük észre, hogy bármely $[r, 4r]$ intervallumban legfeljebb $2r+1$ darab a_i lehet, mert a $2r$-nél nem nagyobb a_j-kre az $a_j + a_{j+1}$-ek, kivéve esetleg az utolsót, a $[2r+1, 4r]$ részbe esnek, és a feltétel szerint különböznek az itt levő a_i-ktől. Ezután bontsuk fel az $[1, n]$ intervallumot ilyen típusú részintervallumokra.

12.1.3 A konstrukcióhoz vegyünk először $\lceil k/2 \rceil$ számot, és legyen t ezek összege. Ha most az első két tagot elhagyjuk, és egy olyan új tagot hozzáveszünk, amely éppen az elhagyott tagok összegével egyenlő, akkor az összeg nem változott. Ezután ugyanezt az eljárást ismételgessük, ameddig csak lehet. Annak igazolásához, hogy ennél nagyobb előállításszám nem létezik, használjuk fel, hogy t minden előállításában más az utolsó tag, valamint más a tagszám.

12.1.4 A feltétel szerint bármely $1 \le j \le n$ egész legfeljebb egy a_i-vel lehet osztható, ezért $\sum_{i=1}^{k} \lfloor n/a_i \rfloor \le n$, és így $n \sum_{i=1}^{k} 1/a_i < n + k$.

12.1.5 $$\frac{1}{[a_i, a_{i+1}]} = \frac{(a_i, a_{i+1})}{a_i a_{i+1}} \le \frac{a_{i+1} - a_i}{a_i a_{i+1}} = \frac{1}{a_i} - \frac{1}{a_{i+1}}.$$

12.1.6

a) Az alsó becsléshez használjuk fel, hogy a $3j+1$ alakú egészek kielégítik a feltételt. A felső becsléshez vegyük észre, hogy ha t^2 a legnagyobb négyzetszám n-ig és $u + v = t^2$, akkor u és v közül legfeljebb az egyik szerepelhet az a_i-k között.

b) Keressünk 11 olyan maradékot modulo 32, amelyek közül semelyik kettőnek az összege sem lehet kongruens egy négyzetszámmal mod 32.

12.1.7 Megfelelnek azok a számok, amelyek ötös számrendszerbeli alakjában a (hátulról nézve) páratlanadik helyeken 0 vagy 2 áll (a többi jegy tetszőleges). Ekkor k értéke kb. n^c, ahol $c = (1 + \log_5 2)/2 = 0.71\ldots$

12.1.8 A prímek egy ilyen tulajdonságú halmazt alkotnak, tehát $s(n) \ge \pi(n)$. Az $s(n) < \pi(n) + 2n^{2/3}$ becslés igazolásához legyen C az 1 és $n^{2/3}$ közötti egész számok halmaza, továbbá D a C-nek az n-ig terjedő prímszámokkal való egyesítése. Először lássuk be, hogy n-ig minden szám felírható $n = cd$ alakban, ahol $c \in C$, $d \in D$ (a felírás általában nem egyértelmű). Ezután az a_i számoknak rögzítsük egy ilyen $a_i = c_i d_i$ alakú előállítását, majd készítsünk el egy $|C| + |D| \le \pi(n) + 2n^{2/3}$ csúcsú páros gráfot, amelynél a csúcsok egyik csoportja a C halmaz, a másik pedig a D, és az a_i számnak a c_i és d_i csúcsot összekötő él felel meg. Ha az élek száma legalább annyi, mint a csúcsok száma, akkor a gráfban van kör. A párosság miatt ennek a körnek páros sok éle van, és a konstrukció alapján a minden második élnek megfelelő a_i-k szorzata megegyezik a kör többi élének megfelelő a_j-k

szorzatával (hiszen mindkét szorzat a kör összes csúcsaiban szereplő számok szorzata).

12.1.9 $\pi(n)$. — Útmutatás: A prímek nyilván rendelkeznek ezzel a tulajdonsággal, tehát a maximum legalább $\pi(n)$. Indirekt tegyük fel, hogy $\pi(n)+1$ ilyen tulajdonságú a_i is megadható lenne. Ekkor minden a_i-hez lenne olyan prím, amelynek a kitevője a_i kanonikus alakjában nagyobb lenne, mint az összes többi a_j kanonikus alakjában együttvéve. A skatulyaelv szerint lenne olyan prím, amely két a_i-nél is ezt a szerepet játszaná, és ez könnyen láthatóan ellentmondás.

12.1.10 $2n/3$. — Útmutatás: A 6-hoz nem relatív prím (azaz a 2 és a 3 közül legalább az egyikkel osztható) $2n/3$ darab szám megfelel a feltételnek. Ha viszont több, mint $2n/3$ elemet veszünk, akkor a skatulyaelv szerint lesz olyan s, hogy a $6s+1,\dots,6s+6$ számok között legalább öt darab a_i fordul elő; lássuk be, hogy ezek között biztosan található három olyan, amelyek páronként relatív prímek. — Megjegyzés: A feladatot három helyett r-re a következőképpen általánosíthatjuk: Mennyi k maximuma, ha bármely r darab a_i között található kettő olyan, amelyek nem relatív prímek. Ilyen halmazt alkotnak például azok a számok, amelyek az első $r-1$ prím közül legalább az egyikkel oszthatók. (Miért?) Erdős azt sejtette, hogy (minden, az r-től függően elég nagy n esetén) ez adja a maximumot. Ezt a sokáig megoldatlan sejtést Ahlswede és Khachatrian igazolták 1994-ben.

12.1.11 Az a_i-k lnkojával végigosztva elérhető, hogy az a_i-k relatív prímek legyenek. Ha van köztük k-val osztható, pl. $k \mid a_i$ és $k \nmid a_j$, akkor (k prím volta miatt) $k \mid \dfrac{a_i}{(a_i,a_j)}$, tehát $\dfrac{a_i}{(a_i,a_j)} \geq k$. Ha egyik a_i sem osztható k-val, akkor van közöttük kettő, amelyek kongruensek mod k. Ha a_i és a_j ilyenek, akkor $\dfrac{a_i}{(a_i,a_j)} \equiv \dfrac{a_j}{(a_i,a_j)} \pmod{k}$, és így a két hányados közül a nagyobbik nagyobb, mint k.

12.1.12 Legyen az $n=2^j$ esetre $a_1,\dots,a_k$ egy megfelelő konstrukció. Ekkor $2^{j+t} \leq n < 2^{j+t+1}$ esetén jó lesz az $1,2,\dots,2^{t-1},2^t a_1,\dots,2^t a_k$ számhalmaz.

12.1.13 A Csebisev-egyenlőtlenségben az optimális választás $c=\sqrt{3}$, ekkor (9)-ben és (10)-ben $8/3$ helyett $3\sqrt{3}/2$ adódik. További javítási lehetőség, hogy (10)-ből elég nagy n-re a (6)-nál erősebb $k \leq (1+\varepsilon)\log_2 n$ következik, ahol $\varepsilon > 0$ tetszőlegesen kicsi lehet, és így (7) jobb oldalán az 1 összeadandó „lényegében” elhagyható. Mindezek alapján a (2) becslésben a képlet végén álló 2 helyett a $\log_2(3\sqrt{3}/2) = 1{,}377\ldots$-nál akármilyen kicsivel nagyobb konstans írható (elég nagy n-et feltételezve).

12.2.

12.2.1 A mohó algoritmussal mindig a legelső olyan elemet választjuk, amelyik nem rontja el a Sidon–tulajdonságot. Tegyük fel, hogy $a_1 < a_2 < \ldots < a_s < n$ már megvan. Egy d elem akkor rossz, ha valamilyen $i\,, j\,, k \leq s$-re $d + a_i = a_j + a_k$, azaz $d = a_j + a_k - a_i$. (A $d + d = a_j + a_k$ esetet nem kell külön számításba venni, mert ha d-vel csak ilyen probléma lenne, akkor $d < a_k$ miatt korábban az a_k helyett a d-t kellett volna a sorozatba választanunk.) Ezzel legfeljebb s^3 (sőt tulajdonképpen kevesebb mint $s^3/2$) elemet zártunk ki, azaz $s < n^{1/3}$ esetén még találunk n-nél kisebb további jó elemet.

12.2.2 A Sidon-tulajdonság igazolásához tegyük fel, hogy $a_i + a_j = a_k + a_l$, azaz

$$2p(i+j-k-l) + (\langle i^2 \bmod p\rangle + \langle j^2 \bmod p\rangle - \langle k^2 \bmod p\rangle - \langle l^2 \bmod p\rangle) = 0.$$

Itt a második tag osztható $2p$-vel, de abszolút értéke $2p$-nél kisebb, tehát csak 0 lehet. Emiatt az első tag is 0. Vagyis $i-k = l-j$ és $i^2-k^2 \equiv l^2-j^2 \pmod p$. Innen egyszerű számolással adódik, hogy vagy $i = k$ és $j = l$ vagy pedig $i = l$ és $j = k$.

12.2.3 A p^2 elemű testtel és a benne levő p elemű résztesttel hasonlóan (csak egyszerűbben) kell okoskodni, mint a 12.2.2 Tétel bizonyításában tettük.

12.2.4 Vegyünk egy g primitív gyököt modulo p, és legyen a_i az $x \equiv i \pmod{p-1}$, $x \equiv g^i \pmod p$ szimultán kongruenciarendszer megoldása modulo $p(p-1)$, $i = 1, 2, \ldots, p-1$.

12.2.5 A 12.2.1 Tétel szerint vegyünk 1 és n_1 között egy kb. $\sqrt{n_1}$ elemszámú S_1 Sidon-sorozatot. Legyen n_2 jóval nagyobb n_1-nél. Az $[n_1, n_1 + n_2]$ intervallumban ne vegyünk elemeket, viszont $n_1 + n_2$ és $n_1 + 2n_2$ között helyezzünk el egy kb. $\sqrt{n_2}$ elemszámú Sidon-halmazt, és abból hagyjuk el azokat az elempárokat, amelyeknek a különbsége $< n_1$, a maradékot jelölje S_2. (Megfelelne céljainknak az is, ha minden elempárból csak az egyik elemet hagynánk el.) A Sidon-tulajdonság miatt az elhagyott elemek száma $< 2n_1$. Így $n_1 + 2n_2$-ig összesen kb. $\sqrt{n_2} + \sqrt{n_1} - 2n_1 \approx$ $\approx \sqrt{n_2}$ elemünk van. Lássuk be, hogy $S_1 \cup S_2$ Sidon-tulajdonságú. Ezután válasszunk egy, az $n_1 + 2n_2$-nél jóval nagyobb n_3-at, $n_1 + 2n_2 + n_3$ és $n_1 + 2n_2 + 2n_3$ között helyezzünk el egy kb. $\sqrt{n_3}$ elemszámú Sidon-halmazt, abból töröljük azokat az elemeket, amelyeknek a különbsége $< n_1 + 2n_2$ stb. Az eljárást folytatva a feladat feltételeit teljesítő végtelen Sidon-sorozatot kapunk.

12.2.6

a) Általánosítsuk a 12.2.3 feladat módszerét a p^h elemű testre.

b) Az elemekből képezhető h-tagú összegek egyrészt mind különbözők, másrészt valamennyien 1 és nh közé esnek.

12.2.7 Nyilván elég belátni, hogy minden pozitív egész egyértelműen előáll $a_i - a_j$ alakban, ahol $i > j$. A sorozatnak mindig két-két új elemét definiáljuk úgy, hogy ezek egyrészt olyan nagyok legyenek, hogy a korábbi elemekkel alkotott különbségeik ne egyezhessenek meg semelyik két korábbi elem különbségével, másrészt az ő különbségük legyen az a legkisebb pozitív egész, amely még nem állt elő két korábbi elem különbségeként.

12.2.8 Álljon A, illetve B azokból a számokból, amelyek kettes számrendszerbeli alakjában (hátulról nézve) minden páros, illetve minden páratlan helyen 0 számjegy áll.

12.3.

12.3.1

a) Legyen $A = \{a_1 < a_2 < \ldots < a_k\}$, ekkor $a_1 + a_1 < a_1 + a_2 < a_2 + a_2 < a_2 + a_3 < \ldots < a_k + a_k$ éppen $2k - 1$ különböző összeg. Ha $|A + A| = 2k - 1$, akkor minden $a_i + a_j$, speciálisan $a_i + a_{i+2}$ is a fenti összegek valamelyike, és nagyságrendi megfontolások miatt csak $a_{i+1} + a_{i+1}$-gyel egyezhet meg, vagyis $a_{i+1} = (a_i + a_{i+2})/2$.

b) Ha $A = \{a_1 < a_2 < \ldots < a_k\}$, $B = \{b_1 < b_2 < \ldots < b_r\}$ és $k \geq r$, akkor $a_1 + b_1 < a_1 + b_2 < a_2 + b_2 < a_2 + b_3 < \ldots < a_r + b_r < a_{r+1} + b_r < \ldots < a_k + b_r$ a kívánt számú különböző összeg. Egyenlőség esetén minden további $a_i + b_j$ a fenti összegek valamelyike. Az $a_2 + b_1$, $a_1 + b_3$, $a_3 + b_2$ stb. összegeket nagyságrendi megfontolásokkal rendre „beazonosíthatjuk", és innen egyszerűen adódik, hogy A első r eleme és B azonos differenciájú számtani sorozatot alkot. A kiindulási $k + r - 1$ tagú összegsorozat alkalmas módosításával ugyanezt A bármely r szomszédos elemére hasonlóan igazolhatjuk.

c) Bizonyítsunk t szerinti teljes indukcióval.

12.3.2 Hagyjuk el B-ből a 0-n kívül az m-hez nem relatív prím elemeket, és ezután kövessük a 12.3.1 Tétel első bizonyítását. A becslés élességének igazolásához legyen például $m = p^2$, $A = \{0, p, 2p, \ldots, (p-1)p\}$, $B = \{0, p, 2p, \ldots, 1, p+1, 2p+1, \ldots, (p-1)p+1\}$.

12.3.3

a) Kövessük a 12.3.1 Tétel első bizonyítását. A megadott feltételt ott kell felhasználni, amikor $b \neq 0$ esetén $A + b = A$ lehetetlenségét mutatjuk meg.

b) Például az $A = \{0, 1, \ldots, k-1\}$ és $B = \{0, 1, \ldots, r-1\}$ halmazokra (ahol $k + r \leq m + 1$) egyenlőség teljesül.

c) Ugyanaz a bizonyítás elmondható az általános esetben is.

12.3.4 A 12.3.1 Tétel második bizonyításához hasonlóan okoskodhatunk: legyen $A = B$, $C = A \hat{+} A$ és

$$f_1(x, y) = (x + y)^m (x - y)^2 \prod_{c \in C} (x + y - c),$$

ahol $m + |C| = 2k - 4$.

12.3.5

a) A 12.3.1 Tétel második bizonyításában látottakhoz hasonlóan „redukáljuk" azokat az $x^i y^j$ tagokat, amelyekben $i \geq k$ vagy $j \geq r$, majd használjuk a 12.3.2 Lemmát.

b) Legyen $|A_i| = k_i$, $i = 1, \ldots, n$, továbbá $F(x_1, \ldots, x_n)$ olyan T feletti n-változós polinom, amelynek a foka $\sum_{i=1}^{n} (k_i - 1)$, és amelyben a $\prod_{i=1}^{n} x_i^{k_i - 1}$ tag együtthatója nem nulla. Ekkor van olyan $a_i \in A_i$, $i = 1, \ldots, n$, amelyre $F(a_1, \ldots, a_n) \neq 0$.

12.3.6 Ha $C = D = \mathbf{Z}_p$, akkor a $c = d$ párosítás jó, hiszen $\mathbf{Z}_p$-ben $2u = 2v$-ből p páratlansága miatt $u = v$ következik. Ha $|C| = |D| = n < p$, akkor alkalmazzuk a 12.3.5b feladatot $A_1 = \ldots = A_n = D$ és

$$F(x_1, \ldots, x_n) = \prod_{1 \leq j < i \leq n} (x_i - x_j)(x_i + c_i - x_j - c_j)$$

szereposztással.

12.3.7 Legyen p prím, $A_i \subseteq \mathbf{Z}_p$, $i = 1, \ldots, n$. Ekkor

$$|A_1 + \ldots + A_n| \geq \min(p\,,\ |A_1| + \ldots + |A_n| + 1 - n).$$

Ezt a 12.3.1 Tételből n szerinti teljes indukcióval igazolhatjuk.

12.3.8

a) Azt kell igazolni, hogy $2n-1$ egész számból mindig kiválasztható n olyan, amelyek összege osztható n-nel. A 3.6.6 feladatban látott módon elég ezt arra az esetre bizonyítani, amikor az n egy p prímszám. Feltehető, hogy a számainkra $0 \leq a_1 \leq a_2 \leq \ldots \leq a_{2p-1} \leq p - 1$ teljesül. Ha van p darab egyforma a_i, akkor ezek összege osztható p-vel. Egyébként — áttérve $\mathbf{Z}_p$-re — legyen $A_i = \{a_i, a_{i+p-1}\}$, $i = 1, \ldots, p - 1$, ekkor $|A_i| = 2$. A 12.3.7 feladat alapján $|A_1 + \ldots + A_{p-1}| = p$, tehát $\mathbf{Z}_p$ minden

eleme, így a_{2p-1} is előáll $a^{(1)} + \ldots + a^{(p-1)}$ alakban, ahol $a^{(i)} \in A_i$, azaz $a^{(1)} + \ldots + a^{(p-1)} + a_{2p-1}$ osztható p-vel.

b) A P és Q rácspontok F felezőpontja akkor és csak akkor rácspont, ha P és Q első, illetve második kordinátái is azonos paritásúak. A skatulyaelv alapján 5 rácspont között biztosan lesz két ilyen tulajdonságú.

c) Tekintsünk olyan rácspontokat, amelyek koordinátáit modulo n redukálva $(0,0)$, $(0,1)$, $(1,0)$, illetve $(1,1)$ adódik, és vegyünk mindegyik fajtából $n-1$ darabot. Ekkor ezen $4n-4$ rácspont közül nem választható ki n olyan, amelyek első és második koordinátáinak az átlaga is egész szám lenne.

d) (i) Az alsó becslés a (c)-beli konstrukció általánosításával igazolható. A felső becslés következik abból, hogy ennyi rácspont között a skatulyaelv alapján biztosan található n olyan, amelyek bármelyik koordinátáját tekintve, ezek azonos maradékot adnak modulo n. — (ii) Ahhoz hasonlóan érdemes eljárni, mint amikor a 3.6.6 feladatban azt mutattuk meg, hogy ha az ottani állítás két számra érvényes, akkor igaz ezek szorzatára is.

12.3.9 Legyen $|A| = k$, c kvadratikus nemmaradék mod p, és tekintsük az $a_i + ca_j$ összegeket, ezek száma k^2. Ha $k^2 > p$, akkor az összegek között biztosan van két egyenlő, amit átrendezve $a_i - a_r = c(a_s - a_j)$ adódik. Itt $a_i - a_r$ és $a_s - a_j$ közül (pontosan) az egyik kvadratikus maradék mod p.

12.3.10 Általánosítsuk a 12.3.3 Tétel kimondása előtti meggondolásokat.

12.4.

12.4.1 Az utolsó három egyenlőség nyilvánvaló, az elsőnél $R(3,2) \leq 6$-ot már igazoltuk, így csak azt kell belátni, hogy egy 5 szögpontú teljes gráf élei kiszínezhetők két színnel úgy, hogy ne keletkezzék egyszínű háromszög. Erre megfelel, ha egy ötszög oldalait pirosra, az átlóit pedig kékre festjük.

12.4.2 A 12.4.1 Tétel bizonyításának I. részében az

$$R(3,t) \leq t\big(R(3,t-1)-1\big) + 2 \qquad (*)$$

egyenlőtlenséget igazoltuk. Innen $R(3,t) \leq tR(3,t-1)$, és (a) azonnal adódik teljes indukcióval. Az élesebb (b) becslésnél az indukcióhoz használjuk (*)-ot és az e sorfejtéséből kapott

$$\lceil et! \rceil = t!\Big(1 + \frac{1}{1!} + \frac{1}{2!} + \ldots + \frac{1}{t!}\Big) + 1$$

alakot.

12.4.3

a) Következik az előző feladat (b) része alapján $S(t) < R(3,t)$-ből (lásd a 12.4.2 Tétel bizonyítását).

b) Vegyük az $1, 2, \ldots, n = S(t)$ számoknak egy „rossz" színezését t színnel (azaz, amikor az $x + y = z$ egyenletnek nincs egyszínű megoldása), majd használjuk a $t+1$-edik színt az $n+1, \ldots, 2n+1$ számok mindegyikénél, végül színezzük ki a $2n+2, \ldots, 3n+1$ számokat ugyanúgy, mint az első n-et (azaz $2n+1+i$ színe legyen ugyanaz, mint az i színe). Mutassuk meg, hogy ez az $1, 2, \ldots, 3n+1$ számoknak egy rossz színezése $t+1$ színnel.

c) Bizonyítsunk teljes indukcióval (b) alapján.

d) A (b)-beli konstrukciót általánosítjuk. Legyen ν az $1, \ldots, n = S(t)$ egy rossz színezése t színnel és ϱ az $1, \ldots, r = S(v)$ egy rossz színezése v másik színnel. Ekkor az alábbi konstrukció az $1 \leq m \leq 2nr + n + r$ számok egy rossz színezése lesz $t+v$ színnel: legyen $m = i(2n+1)+j$, ahol $1 \leq j \leq 2n+1$, és legyen m színe $\nu(j)$, ha $1 \leq j \leq n$, illetve $\varrho(i)$, ha $n+1 \leq \leq j \leq 2n+1$ (azaz a $2n+1$ hosszúságú intervallumok első felében mindig ismételjük meg az $1, 2, \ldots, n$-nek a ν szerinti színezését, az intervallumok második fele pedig legyen egyszínű, ahol a színt az intervallum $1, 2, \ldots, r$ *sorszámának* a ϱ szerinti színezése adja).

12.4.4 $5n - 1$.

12.4.5 Alkalmazzuk a 12.4.2 Tétel bizonyításának gondolatmenetét $R(3,t)$ helyett $R(4,t)$-vel.

12.4.6 Ha $B^t + C^t \equiv D^t \pmod{p}$, ahol $BCD \not\equiv 0 \pmod{p}$, és $CF \equiv 1 \pmod{p}$, akkor $(BF)^t + 1 \equiv (DF)^t \pmod{p}$.

12.4.7

a) Használjunk váltakozva egyre hosszabb piros, illetve kék intervallumokat.

b) Az összes számtani sorozatot sorozatba rendezzük, és rendre mindegyikbe beteszünk egy kék elemet, arra vigyázva, hogy a következő kék szám mindig legalább a duplája legyen az előzőnek. — „Konkrétabb" konstrukció: az $n! + n$ alakú számok legyenek a kékek, ekkor minden $a + md$, $m = 1, 2, \ldots$ számtani sorozatban lesz kék elem, mert pl. $n = a + d$-re $(a+d)! + a + d \equiv a \pmod{d}$, tehát nincs végtelen piros számtani sorozat, és a gyors növekedés miatt 3-tagú kék sincs.

12.4.8 Legyen $m = w(k,t) + 1$, ekkor a 12.4.4A Tétel alapján kapunk egy m-nél kisebb k-tagú egyszínű számtani sorozatot (a továbbiakban k-ESZ). Tekintsük most az $m, 2m, \ldots, (m-1)m$ számokat, és alkalmazzuk újra a 12.4.4A tételt (mintha az m „együtthatói" lennének így színezve), ekkor

az m többszöröseiből kapunk egy újabb k-ESZ-t, ami kisebb m^2-nél, stb. Az így nyert végtelen sok k-ESZ közül végtelen soknak azonos a színe, mert csak véges sok szín lehetséges.

12.4.9 Alkalmazzuk a Van der Waerden-tételt a kettőhatványok kitevőire.

12.4.10 PPKKPPKK mutatja, hogy 8 szám még kevés. Azt, hogy 9 már elég, (minél kevesebb) esetszétválasztással lehet igazolni; érdemes a (szín- és szám)szimmetriákat felhasználni: az 1,5,9 közül az 5 piros, az 1 kék és a 9 vagy kék, vagy piros, majd a 3 és a 7 színét nézzük stb.

12.4.11

a) Az $1, 2, \ldots, n$ számokat 2^n-féleképpen színezhetjük ki két színnel. Számoljuk most meg azokat a színezéseket, amelyeknél előfordul k-tagú egyszínű számtani sorozat (k-ESZ). A k-ESZ-ek száma (pl. a kezdőtag és a differencia szerint összeszámolva) legfeljebb $n^2/2(k-1)$, egy k-ESZ színe kétféle lehet, a többi szám színezése pedig 2^{n-k}-féle. Ennélfogva összesen legfeljebb $n^2 2^{n-k}/(k-1)$ színezésnél fordulhat elő k-ESZ (persze így számos rossz színezést többszörösen is megszámoltunk). Ezért, ha $n^2 2^{n-k}/(k-1) < 2^n$, azaz $n < 2^{k/2}\sqrt{k-1}$, akkor biztosan van olyan színezés, amelyben nem fordul elő k-ESZ.

b) Tekintsük a 2^p elemű T véges testet, legyen Δ a multiplikatív csoport generátoreleme és W egy $p-1$-dimenziós altér T-ben (mint $\mathbf{Z}_2$ feletti vektortérben). A színezés: k piros, ha $\Delta^k \in W$. Az $1, 2, \ldots, p(2^p-1)$ számokat ily módon kiszínezve nem fordul elő $p+1$-tagú egyszínű számtani sorozat.

12.4.12 Írjuk fel a számokat d alapú számrendszerben, ahol d értékét később alkalmasan megválasztjuk. Tekintsük most azokat a számokat n-ig, amelyek felírásában minden számjegy $< d/2$ és a számjegyek négyzetösszege egy adott q érték. Mutassuk meg, hogy egy ilyen számhalmazban nem fordul elő háromtagú számtani sorozat, továbbá q és d alkalmas megválasztásával elérhető, hogy a halmaz elemszáma a feladat állításának megfelelően nagy legyen.

12.5.

12.5.1 Az $1, 2, \ldots, M = [m_1, \ldots, m_k]$ számok közül az $a_i \pmod{m_i}$ maradékosztály M/m_i elemet tartalmaz, és mivel minden szám benne van legalább az egyik maradékosztályban, ezért $\sum_{i=1}^{k} M/m_i \geq M$.

12.5.2 Az új maradékosztálynak részhalmaza a régi.

12.5.3 Legyen m_i tetszőleges és L a többi m_j legkisebb közös többszöröse. A

feltétel szerint van olyan c, amely nincs benne a $j \neq i$-hez tartozó maradékosztályok egyikében sem. Ekkor $c + L$ is ilyen tulajdonságú. Ez azt jelenti, hogy mindkét számot az $a_i \pmod{m_i}$ maradékosztálynak kell tartalmaznia, azaz $c \equiv c + L \pmod{m_i}$, és így $m_i \mid L$.

12.5.4 Használjuk fel az előző három feladatot.

12.5.5 Válassszuk például modulusnak a 120 osztóit (az 1 és a 2 kivételével).

12.5.6

a) Járjunk el hasonlóan, mint a 12.5.1 feladatnál.
b) Ez a 12.5.1 Tétel bármelyik bizonyításából leolvasható.
c) Legyen $m_i = 2^i$, ha $1 \leq i \leq k-1$.

12.5.7 Ilyenek például a 3-mal osztható páros számok, a $3^n + 3$ alakúak kivételével. Ha az $n = 0$ kitevőt is megengedjük, akkor az $1 + p$ alakúakat is le kell számítani, ahol p (egy $6k-1$ alakű) prímszám, de még így is végtelen sok nem előálló marad, a prímek „ritkasága" miatt. Az általános esetben hasonlóan kell eljárni a 3 helyett az a-val, illetve $b/2$-vel. (Ez mutatja, hogy $b = 2$ volt az egyetlen nehéz eset, lásd a 12.5.2 Tételt.)

12.6.

12.6.1 A pontos megfogalmazás a következő. Tekintsük a nemnegatív egészek egy tetszőleges felbontását az I és J végtelen részhalmazok diszjunkt egyesítésére, és írjuk fel az n számot c alapú számrendszerben: $n = \sum_{v=0}^{V} \gamma_v c^v$, $0 \leq \gamma_v < c$. Legyen $A = \{n \mid \gamma_i = 0 \text{ minden } i \in I\}$ és $B = \{n \mid \gamma_j = 0 \text{ minden } j \in J\}$. A komplementumságot az biztosítja, hogy minden szám felírható c alapú számrendszerben. Minden ilyen konstrukciónál $\liminf_{n\to\infty} A(n)B(n)/n = 1$ (de könnyen láthatóan $\limsup_{n\to\infty} A(n)B(n)/n > 1$).

12.6.2 Nem, ez a 12.5.2 Tételből következik.

12.6.3 (a) Szükséges és elégséges. — (b) Elégséges, de nem szükséges, lásd pl. a 12.4.7b feladat piros halmazát. — (c) Szükséges, de nem elégséges. — (d) Se nem szükséges, se nem elégséges.

12.6.4 A 12.6.1 Tétel bizonyításához hasonlóan érdemes eljárni. Mivel $a_t \equiv t \pmod{2^i 3^j}$, ha $i, j \leq t$, ezért az a_{k-s} számok, $\log_6 k + 1 \leq s \leq \log_6 k + d_k$, teljes maradékrendszert alkotnak mod d_k, ha $d_k = 2^i 3^j$ és $d_k < k - 5\log_6 k$. Az elemszámbecslésekhez később felhasználandó $d_k \sim k$ és $d_k \leq d_{k+1}$ további feltételek azért biztosíthatók, mert a nagyság szerint rendezett $2^i 3^j$ alakú számok sorozatában a szomszédos elemek hányadosa

1-hez tart, ugyanis a $\log_2(2^i 3^j)$ értékek törtrésze a 8.4.1 Tétel szerint mindenütt sűrű $[0,1]$-ben.

Ha most $a_k \le n < a_{k+1}$, akkor $n = a_{k-s} + rd_k$, ahol $6^k(1-1/k) < < rd_k < 6^{k+1}$, tehát az ilyen rd_k-kat választva B-nek, az A komplementumát kapjuk. Az elemszámbecsléseknél $A(n) = k$, és $B(n)$-nél azoknak az rd_j-knek a számát kell viszonylag pontosan becsülni, amelyekre $k \ge j \ge v = \lfloor k - 2\log_6 k \rfloor$, majd ezek kezeléséhez használjuk a d_v „közös nevezőt", a $j < v$-hez tartozó tagok száma pedig legfeljebb 6^v.

12.6.5 Mivel ekkor $A(n) = \pi(n) \sim n/\log n$, ezért

$$S(n) <\sim 10 \sum_{i=2}^{n} \frac{\log^2 n}{n} \sim 10 \int_2^n \frac{\log^2 x}{x} dx \sim \frac{10(\log n)^3}{3}\,.$$

12.6.6 Használjuk a 12.6.4 Tételt. Mivel $(\log A(i))/A(i) \to 0$, ezért bármely $\varepsilon > 0$-hoz van olyan i_0, hogy $i \ge i_0$-ra $(\log A(i))/A(i) < \varepsilon/20$. Ekkor

$$B(n) < 10 \sum_{i=a_1}^{n} \frac{\log A(i)}{A(i)} < C + 10 \sum_{i=i_0}^{n} \frac{\log A(i)}{A(i)} < C + \frac{10n\varepsilon}{20} < \varepsilon n.$$

MEGOLDÁSOK

1. Számelméleti alapfogalmak

• **1.1.18** Mivel bármely n-re csak véges sok „játék" lehetséges, és mindegyik játék az egyik játékos győzelmével végződik, ezért valamelyik játékosnak biztosan van nyerő stratégiája. Megmutatjuk, hogy ez mindig az első játékos. Indirekt tegyük fel, hogy valamilyen n-re a második játékosnak, Tündének lenne nyerő stratégiája. Ez azt is jelenti, hogy ha Csongor $d_1 = 1$-gyel kezd, akkor Tünde tud olyan $d_2 = r$-et mondani, majd tovább úgy játszani, hogy nyerjen. Ekkor viszont Csongor $d_1 = r$-rel kezdve nyerne, hiszen pontosan ugyanúgy kell játszania, mint Tündének az előbb (az előző játékhoz képest legfeljebb a még fel nem használt 1-es szám okozhatna eltérést, azonban az 1 most sem választható későbbi lépésben, hiszen már $d_1 = r$-nek osztója). Ellentmondásra jutottunk, tehát bármely $n > 1$-re a kezdő játékosnak van nyerő stratégiája. — Vegyük észre, hogy a bizonyítás csak a nyerési lehetőség tényét adja a kezdő részére, a konkrét stratégia megtervezésére semmilyen információt sem nyújt. Bonyolult szerkezetű n-ek esetén nem is ismeretes, hogyan kell Csongornak optimálisan játszania (és ebben az esetek óriási számára tekintettel egy számítógép sem tud rajta segíteni).

• **1.1.22 f)** Mivel az $1 + \sqrt{2}$ egység, továbbá egy egység negatívja és minden (egész kitevőjű) hatványa is egység, ezért a megadott számok valóban egységek. A megfordításhoz indirekt tegyük fel, hogy ezeken kívül is létezik egy ε egység. Ezt szükség esetén -1-gyel beszorozva egy $\delta > 0$ egységet kapunk. Ekkor létezik olyan k egész, amelyre $(1 + \sqrt{2})^k < \delta < (1 + \sqrt{2})^{k+1}$. Az egyenlőtlenséget az $(1 + \sqrt{2})^{-k}$ egységgel beszorozva egy olyan $u + v\sqrt{2}$ egységhez jutunk, amelyre $1 < u + v\sqrt{2} < 1 + \sqrt{2}$. Itt u és v előjele nyilván nem lehet azonos (és egyikük sem lehet nulla). A továbbiakban felhasználjuk, hogy $|u^2 - 2v^2| = 1$. Ha $u^2 - 2v^2 = -1$, akkor $\varrho = v\sqrt{2} - u = 1/(u + v\sqrt{2})$ miatt $0 < \varrho < 1$. Ugyanakkor $v > 0, u < 0$ esetén $\varrho > 1$, illetve $v < 0, u > 0$ esetén $\varrho < 0$ adódik, ami ellentmondás. Ugyanígy jutunk ellentmondásra az $u^2 - 2v^2 = 1$ esetben is.

• **1.1.23 a)** Ha e egységelem, akkor e nyilván egység is. Megfordítva, legyen ε egység. Ekkor $\varepsilon \mid \varepsilon$, azaz van olyan q, amelyre $\varepsilon = \varepsilon q$. Megmutatjuk, hogy q egységelem. Tetszőleges c-re $\varepsilon c = \varepsilon qc$, azaz $\varepsilon(c - qc) = 0$. A nullosztómentesség miatt $c = qc$, azaz q valóban egységelem.

• **1.3.11** Mivel $(a,b) \mid a$, ezért $c(a,b) \mid ca$, ugyanígy $c(a,b) \mid cb$. Ez azt jelenti, hogy $c(a,b)$ közös osztója ca-nak és cb-nek, ennélfogva $c(a,b)$ osztója ca és cb kitüntetett közös osztójának, (ca,cb)-nek is. Ennek alapján alkalmas q egésszel $c(a,b)q = (ca,cb)$. Azt kell még megmutatnunk, hogy q egység.

Mivel $c(a,b)q = (ca,cb) \mid ca$, ezért $q(a,b) \mid a$, ugyanígy $q(a,b) \mid b$. Ez azt jelenti, hogy $q(a,b)$ közös osztója a-nak és b-nek, ennélfogva osztója a kitüntetett közös osztójuknak is, azaz $q(a,b) \mid (a,b)$. Innen $q \mid 1$, tehát q valóban egység.

• **1.3.13** Mivel $(n,k) \mid n$, ezért $a^{(n,k)}-1 \mid a^n-1$, ugyanígy $a^{(n,k)}-1 \mid a^k-1$. Ez azt jelenti, hogy $a^{(n,k)}-1$ közös osztója a^n-1-nek és a^k-1-nek.

Most a kitüntetett tulajdonságot igazoljuk, vagyis azt, hogy a^n-1 és a^k-1 bármely d közös osztója osztja $a^{(n,k)}-1$-et is. Az $(n,k) = nu+kv$ előállításban u és v nyilván ellentétes előjelűek, ezért feltehető, hogy $(n,k) = nr-ks$, ahol r,s pozitív egészek. Ekkor

$$d \mid a^n-1 \mid a^{nr}-1 \qquad \text{és} \qquad d \mid a^k-1 \mid a^{ks}-1,$$

innen

$$d \mid (a^{nr}-1)-(a^{ks}-1) = a^{nr}-a^{ks} = a^{ks}(a^{nr-ks}-1) = a^{ks}(a^{(n,k)}-1)\,.$$

Itt d az utolsó szorzat első tényezőjéhez, a^{ks}-hez relatív prím, hiszen $d \mid a^{ks}-1$. Ezért d szükségképpen osztja a második tényezőt, $a^{(n,k)}-1$-et.

• **1.4.5** Arra fogunk támaszkodni, hogy a k páratlansága miatt bármely c esetén $c^k+(t+1-c)^k$ osztható $c+(t+1-c) = t+1$-gyel. Legyen először t páros. Ekkor az

$$\big(1^k+t^k\big)+\big(2^k+(t-1)^k\big)+\ldots+\big((t/2)^k+(1+(t/2))^k\big)$$

csoportosításból az előzőek alapján látszik, hogy a szóban forgó összeg osztható $t+1$-gyel. Ezért csak úgy lehet prím, ha értéke éppen $t+1$. Azonban

$$1^k+2^k+3^k+\ldots+t^k \geq 1+2+\ldots+t = t(t+1)/2 \geq t+1\,,$$

és egyenlőség csak akkor teljesül, ha $t=2$ és $k=1$, és ekkor $1^1+2^1 = 3$ valóban prím.

Ha t páratlan, akkor a helyzet csak annyiban változik, hogy az összegnek van középső tagja, $\big((t+1)/2\big)^k$, tehát az előző gondolatmenet alapján az összeg

osztható $(t+1)/2$-vel. Ugyanakkor az összeg nagyobb, mint $(t+1)/2$, vagyis sohasem lehet prím.

A feladat egyetlen megoldása tehát $t=2$, $k=1$.

Hasonló gondolatmenettel érhetünk célhoz úgy is, hogy $t+1$ helyett a t-vel való oszthatóságot vizsgáljuk.

• **1.5.8** Legyen p felbonthatatlan és tegyük fel, hogy $p \mid ab$. Azt kell igazolnunk, hogy ekkor $p \mid a$ és $p \mid b$ közül legalább az egyik fennáll.

Ha $a=0$, akkor $p \mid a$. Ha a egység, akkor $p \mid b$.

Ha a és b nullától és egységtől különbözők, akkor bontsuk fel őket felbonthatatlanok szorzatára:

$$a = u_1 \dots u_k, \qquad b = v_1 \dots v_m.$$

Innen kapjuk, hogy $ab = u_1 \dots u_k v_1 \dots v_m$.

A $p \mid ab$ feltételből $ab = ps$ alkalmas s egésszel. Bontsuk fel s-et felbonthatatlanok szorzatára: $s = w_1 \dots w_n$, ekkor $ab = pw_1 \dots w_n$.

A számelmélet alaptétele szerint az ab-re kapott két felbontás lényegében ugyanaz, tehát a p meg kell hogy egyezzen valamelyik u_i vagy v_j alkalmas egységszeresével. Ennek megfelelően $p \mid a$ vagy $p \mid b$ teljesül.

• **1.5.10** A 2 és a 3 megfelel, például $2 = 1^3 + 1^3$, illetve $3^2 = 2^3 + 1^3$.

Megfordítva, tegyük fel, hogy $x^3 + y^3 = p^\alpha$. Az egyenletet $(x,y)^3$-nal leosztva egy hasonló típusú egyenlet keletkezik, ahol (az új) x és y már relatív prímek (és az új α esetleg kisebb, mint az eredeti volt).

Szorzattá bontás után $(x+y)(x^2-xy+y^2) = p^\alpha$ adódik, ahonnan a számelmélet alaptétele (és a pozitivitási feltételek) szerint azt kapjuk, hogy

$$x+y = p^\beta, \qquad x^2-xy+y^2 = p^\gamma, \qquad \beta > 0, \quad \gamma \geq 0, \quad \beta+\gamma = \alpha. \tag{1}$$

Az $(x+y)^2 - (x^2-xy+y^2) = 3xy$ azonosságba (1)-et beírva nyerjük, hogy

$$p^{2\beta} - p^\gamma = 3xy\,. \tag{2}$$

Ha $\gamma = 0$, akkor

$$1 = x^2 - xy + y^2 = (x-y)^2 + xy \geq xy \geq 1 \cdot 1 = 1$$

alapján $x = y = 1$ és $p = 2$.

Ha $\gamma > 0$, akkor (2) szerint $p \mid 3xy$. Ha itt $p \mid x$, akkor $p \mid x + y (= p^\beta)$ miatt $p \mid y$ is teljesül, ami ellentmond annak, hogy x és y relatív prímek.

Ugyanígy $p \mid y$ is ellentmondásra vezet. Ezért csak $p \mid 3$, azaz $p = 3$ lehetséges.

• **1.6.3 a)** Indirekt tegyük fel, hogy valamilyen $x, z > 0$ és $k \geq 2$ egészekre $x(x+1) = z^k$. Mivel $(x, x+1) = 1$, ezért az 1.6.2a feladat szerint léteznek olyan u és v pozitív egészek, amelyekkel $x = u^k$ és $x + 1 = v^k$. Innen $v^k - u^k = 1$. Ez azonban lehetetlen, hiszen

$$v^k - u^k \geq (u+1)^k - u^k > ku^{k-1} > 1.$$

• **b)** Az előző gondolatmenetet kell egy kicsit módosítani. A három tényező általában nem lesz páronként relatív prím, azonban a középső szám relatív prím a másik kettőhöz, és így $(x-1)x(x+1) = z^k$, $(x, x^2-1) = 1$ alapján $x = u^k, x^2 - 1 = v^k$. Ekkor $(u^2)^k - v^k = 1$, ami lehetetlen.

• **c)** Először megmutatjuk, hogy négy egymást követő pozitív egész szorzata nem lehet négyzetszám, azaz ($x \geq 2$-re)

$$(x-1)x(x+1)(x+2) = z^2 \tag{1}$$

nem teljesülhet. Legyen $x(x+1) = 2y$, ekkor $(x-1)(x+2) = 2y-2$, és így (1) átírható $y(y-1) = (z/2)^2$ alakba. Az a) részben láttuk, hogy két szomszédos pozitív egész szorzata nem lehet négyzetszám, és ezért (1) sem állhat fenn.

A továbbiakban legyen $k \geq 3$, és tegyük fel indirekt, hogy négy egymást követő pozitív egész szorzata k-adik hatvány. A négy tényező között található olyan, amelyik a másik háromhoz relatív prím: a két középső szám közül a páratlan biztosan megfelel. Ekkor a b)-ben látott gondolatmenet szerint mind ez a tényező, mind pedig a másik három tényező szorzata k-adik hatvány. Ez azt jelenti, hogy

$$(u^k - 1)(u^k + 1)(u^k + 2) = v^k \tag{2}$$

vagy

$$(u^k - 1)(u^k + 1)(u^k - 2) = v^k\,. \tag{3}$$

Megmutatjuk azonban, hogy $k \geq 3$-ra (2) és (3) bal oldala két szomszédos egész szám k-adik hatványa közé esik, vagyis nem lehet k-adik hatvány.

Vizsgáljuk először (2) bal oldalát, ez $u^{3k} + 2u^{2k} - u^k - 2$. Belátjuk, hogy

$$(u^3)^k < u^{3k} + 2u^{2k} - u^k - 2 < (u^3+1)^k\,.$$

Itt az első egyenlőtlenség nyilvánvaló, a második pedig az alábbi módon következik ($k \geq 3$):

$$(u^3+1)^k > u^{3k} + ku^{3(k-1)} > u^{3k} + 2u^{2k} > u^{3k} + 2u^{2k} - u^k - 2.$$

Tekintsük most (3) bal oldalát, ez $u^{3k} - 2u^{2k} - u^k + 2$. Azt igazoljuk, hogy

$$(u^3)^k > u^{3k} - 2u^{2k} - u^k + 2 > (u^3 - 1)^k \,.$$

Az első egyenlőtlenség most is nyilvánvaló. A második egyenlőtlenség $k = 3$ esetén $(u^3-1)(u^3-3) > 0$-val ekvivalens, ami igaz. Ha $k \geq 4$, akkor a második egyenlőtlenséget írjuk át

$$(u^3)^k - (u^3 - 1)^k > 2u^{2k} + u^k - 2$$

alakba. Ennek fennállását a következőképpen láthatjuk be:

$$\begin{aligned}(u^3)^k - (u^3 - 1)^k = u^{3(k-1)} + u^{3(k-2)}(u^3 - 1) + \ldots + (u^3 - 1)^{k-1} > \\ > u^{3k-3} + u^{3k-6} > u \cdot u^{2k} + u^k > 2u^{2k} + u^k - 2\,.\end{aligned}$$

• **1.6.4** Tegyük fel, hogy $2^{p-1} - 1 = n^2 p$. Mivel $p = 2$ nem megfelelő, ezért $p - 1$ páros, és az egyenlet átírható

$$(2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1) = n^2 p$$

alakba.

A bal oldalon a két tényező relatív prím, ezért a következő két eset lehetséges:

$$2^{(p-1)/2} - 1 = u^2 \qquad \text{és} \qquad 2^{(p-1)/2} + 1 = pv^2\,, \tag{i}$$

illetve

$$2^{(p-1)/2} - 1 = pu^2 \qquad \text{és} \qquad 2^{(p-1)/2} + 1 = v^2\,. \tag{ii}$$

Az (i) esetben az első egyenlőség bal oldala $p > 3$-ra 4-gyel osztva 3-at ad maradékul, és így nem lehet négyzetszám. Vagyis csak $p = 3$ lehetséges, ami valóban ki is elégíti a feladat feltételeit.

A (ii) esetben a második egyenlőség átírható $2^{(p-1)/2} = (v - 1)(v + 1)$ alakba. Ez csak úgy lehet, ha $v-1$ és $v+1$ mindketten kettőhatványok. Mivel a különbségük kettő, ezért csak a 2 és 4, azaz $v = 3$ jöhet szóba. Az innen adódó $p = 7$ valóban ki is elégíti a feladat feltételeit.

A feladat összes megoldása tehát $p = 3$ és $p = 7$.

• **1.6.10** *Első megoldás*: Ha $n = 1$, akkor $A(1) = B(1) = d(1) = 1$, tehát ekkor egyenlőség teljesül. Legyen $n > 1$, és legyen az n kanonikus alakja $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, ahol $\alpha_i > 0$. A négyzetmentes osztókat az jellemzi, hogy bennük minden p_i kitevője 0 vagy 1, tehát $A(n) = 2^r$. A négyzetszámosztókban minden p_i kitevője páros, tehát $B(n) = (1 + \lfloor \alpha_1/2 \rfloor) \ldots (1 + \lfloor \alpha_r/2 \rfloor)$.

Az a) rész állítása azonnal adódik a $2(1+\lfloor\alpha_i/2\rfloor) \geq \alpha_i+1$ egyenlőtlenségből (páros α_i esetén itt $>$, páratlan α_i esetén $=$ áll), hiszen $i = 1, 2, \ldots, r$-re a bal oldalakat összeszorozva $A(n)B(n)$, a jobb oldalakat összeszorozva $d(n)$ adódik. Így az is látszik, hogy egyenlőség pontosan akkor teljesül, ha minden i-re $2(1 + \lfloor\alpha_i/2\rfloor) = \alpha_i + 1$, azaz ha minden α_i páratlan.

• *Második megoldás*: Egy számból a maximális négyzetszám osztóját leválasztva a számelmélet alaptétele alapján kapjuk, hogy minden pozitív egész egyértelműen írható fel egy négyzetszám és egy négyzetmentes szám szorzataként. Így n minden osztója is egyértelműen írható fel n egy négyzetszám osztójának és egy négyzetmentes osztójának a szorzataként, tehát $d(n) \leq$ $\leq A(n)B(n)$. Egyenlőség akkor áll fenn, ha az ilyen szorzatként adódó számok valamennyien osztói az n-nek. Ha n-ben valamelyik p_i prím kitevője páros $\alpha_i = 2m$, akkor a $p_i^{2m}p_i$ szorzat már nem lesz osztója n-nek. Hasonlóan látható, hogy ha viszont n-ben minden prím kitevője páratlan, akkor minden ilyen szorzat n-nek osztója. Vagyis egyenlőség pontosan akkor teljesül, ha n kanonikus alakjában minden prím kitevője páratlan.

• **1.6.28** A megfelelő rozmárlétszámok éppen a kettőhatványok. Ha a fejet -1-nek, az írást $+1$-nek vesszük, akkor a feladatot a következőképpen fogalmazhatjuk át. Legyen $x_1, x_2, \ldots, x_n$ mindegyike 1 vagy -1, és képezzük az $x_1x_2, x_2x_3, \ldots, x_nx_1$ számokat, majd ugyanezt az eljárást ismételgessük. A feladat azt kérdezi, hogy milyen n esetén jutunk el garantáltan a csupa 1-ből álló sorozathoz.

Lássuk be először, hogy páratlan $n > 1$-re a játék nem feltétlenül ér véget. A számok szorzata minden lépésben az előző számok szorzatának a négyzete, tehát a második lépéstől kezdve biztosan $+1$. Emiatt a -1-ek száma minden lépésben páros kell legyen. Ha eredetileg nem a csupa 1-esből és nem a csupa -1-esből indultunk ki, akkor a játék véget érése előtt minden számnak -1-nek kell lennie, ami páratlan sok -1 lenne, tehát nem valósulhat meg. (Innen az is látszik, hogy páratlan n-re a játék csakis akkor ér véget, ha a csupa $+1$ vagy a csupa -1 sorozat volt a kezdő helyzet.)

Legyen most $n = rt$, ahol $t > 1$ páratlan. Ha a kiinduló helyzet periodikus t szerint (és nem minden elem azonos), akkor a páratlan esetre látottak biztosítják, hogy a játék nem ér véget.

Végül megmutatjuk, hogy $n = 2^k$ esetén a játék biztosan véget ér. Néhány lépést felírva megsejthető, majd r szerinti teljes indukcióval vagy a Pascal-háromszög alapján bizonyítható, hogy az r-edik lépésben a sorozatunk első tagja

$$x_1^{\binom{r}{0}} x_2^{\binom{r}{1}} \ldots x_{r+1}^{\binom{r}{r}}\ , \tag{1}$$

ahol x_i-t $i > n$-re az $x_1 = x_{n+1} = x_{2n+1} = \ldots, x_2 = x_{n+2} = \ldots$ stb. módon értelmezzük (mindez nemcsak kettőhatványokra, hanem bármely n-re érvényes). Ezt most $r = n = 2^k$-ra alkalmazva kapjuk, hogy (1)-ben minden kitevő páros, hiszen x_1-é 2, a többi x_i-nél pedig $\binom{2^k}{i-1}$, ami páros (lásd az 1.6.27 feladat (c2) részét). Így a szorzat négyzetszám, vagyis $+1$. Hasonlóan kapjuk, hogy az n-edik lépésben kapott többi szám is $+1$, tehát a játék (legkésőbb ekkorra biztosan) véget ért.

• **1.6.29** *Első megoldás*: Legyen $1 \leq k \leq n$. Ekkor $n! + k > k$ miatt választhatunk olyan p prímszámot, hogy $n!+k$ a p-nek magasabb hatványával osztható, mint k. Legyen például $p^\alpha \mid k$, $p^{\alpha+1} \nmid k$, és $p^{\alpha+1} \mid n! + k$ (ahol $\alpha \geq 0$ egész). Állítjuk, hogy p nem osztója az $n! + t$ ($t = 1, 2, \ldots, n$, $t \neq k$) számoknak.

Ha $p > n$, akkor ez nyilvánvaló, hiszen ekkor n darab egymás utáni szám közül p legfeljebb egynek lehet osztója. Tegyük fel tehát, hogy $p \leq n$. Ha még $p \mid n!+t$ is fennállna (ahol $1 \leq t \leq n$ és $t \neq k$), akkor $p \mid n!$ miatt $p \mid t$, és így $kt \mid n!$ miatt $p^{\alpha+1} \mid n!$ következne, ami ellentmond annak, hogy $p^{\alpha+1} \mid n!+k$ és $p^{\alpha+1} \nmid k$.

• *Második megoldás*: Először megmutatjuk, hogy mindegyik $n! + k$ számnak ($1 \leq k \leq n$) van $n/2$-nél nagyobb prímosztója. Sőt, belátjuk, hogy az $n!+k = k(n!/k+1)$ alakban a második tényező egy tetszőleges p prímosztójára $p > n/2$. Tegyük fel indirekt, hogy $p \leq n/2$. Az $n!/k$ szám az 1-től n-ig terjedő számok közül a k kivételével a többi $n-1$-nek a szorzata. Mivel $p \leq n/2$ miatt $n!$ tényezői között p és $2p$ is szerepel, így $n!/k$-ban ezek közül legalább az egyik megmarad ($k = 2p$ esetén a p, $k = p$ esetén a $2p$, más k-ra pedig mindkettő), tehát $n!/k$ osztható p-vel. Emiatt $n!/k + 1$ nem lehet osztható p-vel, ami ellentmondás.

Most belátjuk, hogy az $n!+k$ számok egy-egy $n/2$-nél nagyobb tetszőleges prímosztója megfelel a feladat feltételeinek. Ehhez elég azt igazolni, hogy egy $n/2$-nél nagyobb q prímszám legfeljebb egy darab $n! + j$-nek lehet osztója ($1 \leq j \leq n$). Ha $q \geq n$, akkor ez abból következik, hogy n szomszédos szám közül legfeljebb egy osztható q-val. Ha $n/2 < q < n$, akkor q szerepel $n!$-ban, tehát ha q osztója $n! + j$-nek, akkor osztója $(n! + j) - n! = j$-nek is. Mivel $2q > n \geq j > 0$, ezért ez csak úgy lehetséges, ha $q = j$, tehát a j most is egyértelműen meghatározott.

• **1.6.30** A keresett maximum értéke 9.

Először megmutatjuk, hogy a 9 elérhető. Legyenek $p_1, p_2, \ldots, p_{4991}$ különböző prímszámok, és jelölje P ezek szorzatát. Ekkor az alábbi 5000 szám

megfelel a feltételeknek:

$$a_i = P/p_i, i = 1, 2, \ldots, 4991; \quad b_j = p_j, j = 1, 2, \ldots, 8 \text{ és } b_9 = p_9 \cdot p_{10} \cdot \ldots \cdot p_{4991}\,.$$

Itt a $b_1, b_2, \ldots, b_9$ számok páronként relatív prímek. Belátjuk továbbá, hogy bármely tíz számnak a legkisebb közös többszöröse éppen P. Egyrészt P mindegyik a_i-vel és b_j-vel osztható, így P-nél nagyobb érték nem jöhet szóba, másrészt két (vagy több) a_i-nek, illetve az összes b_j-nek a legkisebb közös többszöröse P, és bármely tíz szám között vagy megtalálható az összes b_j, vagy pedig szerepel legalább két a_i.

Most bebizonyítjuk, hogy tíz páronként relatív prím szám már nem fordulhat elő. Tegyük fel indirekt, hogy a $c_1, c_2, \ldots, c_{5000}$ különböző pozitív egészek közül bármely tíznek a legkisebb közös többszöröse ugyanaz a C szám, és (mondjuk) $c_1, c_2, \ldots, c_{10}$ páronként relatív prímek. Ekkor $c_1, c_2, \ldots, c_{10}$ legkisebb közös többszöröse $C = c_1 \cdot c_2 \cdot \ldots \cdot c_{10}$. Tekintsük most c_{11}-et. A feltétel szerint $c_2, c_3, \ldots, c_{10}, c_{11}$ legkisebb közös többszöröse is C. Ez azt jelenti, hogy c_{11}-nek csak olyan prímosztói lehetnek, amelyek $c_1, \ldots, c_{10}$ valamelyikében már előfordultak, továbbá c_{11} a c_1 prímtényezőit pontosan ugyanazon a hatványon kell hogy tartalmazza, mint amelyiken azok a c_1-ben szerepeltek (hiszen ezekkel a prímekkel — a páronként relatív prímség miatt — a $c_2, \ldots, c_{10}$ számok egyike sem osztható). Ismételjük meg ugyanezt a gondolatmenetet arra a tíz számra, amikor a c_{11}-hez a $c_1, c_2, \ldots, c_{10}$ számok közül rendre mindig másik kilencet veszünk hozzá, és így képezzük a legkisebb közös többszöröst. Innen kapjuk, hogy csak $c_{11} = C$ lehetséges. Ugyanez adódik c_{12}-re is, ami ellentmondás, hiszen a számainknak különbözőknek kell lenniük.

• **1.6.34** I. Először belátjuk, hogy az $S(i)$ értékek között ($i \geq 2$ esetén) csak (pozitív) összetett számok szerepelnek. $S(i) \neq 1$, mert $S(i) \geq i \geq 2$. Továbbá $S(i)$ nem lehet prím, mert egy olyan, különböző pozitív egészekből képezett szorzat, amelynek a legnagyobb tényezője prím, nem lehet négyzetszám, hiszen a szorzat ennek a prímnek csak az első hatványával osztható.

II. Most megmutatjuk, hogy $i < j$ esetén $S(i) \neq S(j)$. Indirekt tegyük fel, hogy $S(i) = S(j) = n$. Ekkor vannak olyan $i = b_1 < b_2 < \ldots < b_r = n$ és $j = c_1 < c_2 < \ldots < c_s = n$ számok, hogy a $b_1 b_2 \ldots b_r$ szorzat és a $c_1 c_2 \ldots c_s$ szorzat is négyzetszám. Szorozzuk ezeket össze, majd hagyjuk el a kétszer előforduló tényezők mindkét példányát (azaz a $b_1 b_2 \ldots b_r c_1 c_2 \ldots c_s$ szorzatot leosztjuk azon számok szorzatának a négyzetével, amelyek mind a b-k, mind pedig a c-k között szerepelnek).

Az így kapott szorzat tényezői között $i < j$ miatt biztosan megtalálható az i, ugyanakkor hiányzik az n. Nyilván ez a szorzat is négyzetszám, amelynek

a legkisebb tényezője i, legnagyobb tényezője viszont n-nél kisebb. Ez azonban ellentmond $S(i)$ definíciójának.

III. Végül azt igazoljuk, hogy minden n összetett szám fellép az $S(i)$ értékek között. Tekintsük ehhez az összes olyan $u_1 < u_2 < \ldots < u_k$ számhalmazt, amelyre $u_k = n$ és az $u_1 u_2 \ldots u_k$ szorzat négyzetszám. Ilyen számhalmaz biztosan létezik: ha n négyzetszám, akkor a $k = 1$, $u_1 = n$ választás megfelel, egyébként pedig vegyük hozzá n-hez azokat a prímeket, amelyek n prímtényezős felbontásában páratlan hatványon szerepelnek.

Tekintsük most u_1 lehető *legnagyobb* értékét, legyen ez m. Bebizonyítjuk, hogy $S(m) = n$.

Indirekt tegyük fel, hogy vannak olyan $v_1 < v_2 < \ldots < v_q$ egészek, amelyekre $v_1 = m$, $v_1 v_2 \ldots v_q$ négyzetszám és $v_q < n$. Ekkor a II. pontban látott gondolatmenethez hasonlóan képezzük az u-k és a v-k szorzatát, majd ebből elhagyjuk a kétszer előforduló tényezők mindkét példányát. Az így kapott szorzat tényezői között megmarad az n, de hiányzik az m. Vagyis ez a szorzat egy olyan négyzetszám, amelynek a legnagyobb tényezője n, de a legkisebb tényezője nagyobb m-nél. Ez viszont ellentmond m választásának.

• **1.6.35 a)** Nem létezik.

•*Első bizonyítás*: Indirekt tegyük fel, hogy az $a + kd$, $k = 0, 1, 2, \ldots$ számtani sorozat megfelelne. Legyen p olyan prím, amely nem osztója d-nek. Ekkor könnyen láthatóan az $a + kd$ számok $k = 1, 2, \ldots, p^2$-re csupa különböző maradékot adnak p^2-tel osztva. Ez azt jelenti, hogy ezek a számok minden lehetséges maradékot kiadnak p^2-tel osztva, így speciálisan a p maradékot is. Egy teljes hatvány azonban nem lehet $mp^2 + p$ alakú, hiszen egy ilyen szám p-nek pontosan az első hatványával osztható.

• *Második bizonyítás*: Egy d differenciájú számtani sorozatnak N-ig kb. N/d eleme van, azonban N-ig csak ennél jóval kevesebb teljes hatvány található: legfeljebb $N^{1/2} + N^{1/3} + N^{1/4} + \ldots \leq N^{1/2} + \log_2 N \cdot N^{1/3} < 2\sqrt{N}$, ha N nagy. Ez azt jelenti, hogy ha N-et megfelelően nagyra választjuk, akkor „nincs elég sok" teljes hatvány ahhoz, hogy a számtani sorozat minden tagja az legyen.

• *Harmadik bizonyítás*: Felhasználjuk a számtani sorozatok prímszámaira vonatkozó Dirichlet-tételt, amely szerint $(A, D) = 1$ esetén az $A + kD$ számtani sorozat végtelen sok prímszámot tartalmaz (5.3.1 Tétel). Eszerint $a + kd$-ből $m = (a, d)$-t kiemelve $a + kd = m(A + kD)$ végtelen sokszor lesz mp alakú, amely elég nagy p prím esetén nem lehet teljes hatvány.

• *Negyedik bizonyítás*: Ha a számtani sorozat első tagja (amelyről feltehetjük, hogy 1-nél nagyobb) $a = b^r$, ahol $r > 1$ a lehető legnagyobb hatványkitevő,

akkor némi számolás után adódik, hogy az $a + (a^2 d^{r-1})d$ tag nem lehet teljes hatvány.

• **b)** Létezik. Teljes indukcióval bizonyítunk: Tegyük fel, hogy $a_1^{k_1}, \ldots, a_n^{k_n}$ egy d differenciájú számtani sorozat, és legyen ennek $n+1$-edik tagja $s = a_n^{k_n} + d$. Ekkor minden tagot $s^{k_1 k_2 \ldots k_n}$-nel beszorozva egy teljes hatványokból álló $n+1$ tagú számtani sorozatot nyerünk.

2. Kongruenciák

• **2.2.4 f)** Akkor és csak akkor létezik modulo m teljes maradékrendszer csupaegyekből, ha $m = 3^k$ alakú.

Tegyük fel először, hogy m-nek van egy $p \neq 3$ prímosztója, és mégis lennének olyan csupaegyek, amelyek minden lehetséges maradékot kiadnának modulo m. Ekkor nyilván modulo p is létrejönne minden lehetséges maradék, vagyis létezne modulo p is teljes maradékrendszer csupaegyekből.

Ennek a modulo p teljes maradékrendszernek az elemeit szorozzuk meg 9-cel, és az eredményhez adjunk hozzá 1-et. Mivel $(9, p) = 1$, ezért így ismét egy teljes maradékrendszert kapunk modulo p, amelynek az elemei tízhatványok. Ezek azonban nem adhatnak ki minden maradékot p-vel osztva: ha $p = 2$ vagy 5, akkor csak a nulla maradék jön létre, más p esetén pedig a nulla maradék biztosan nem jön létre.

Ez az ellentmondás mutatja, hogy ha m nem háromhatvány, akkor ilyen csupaegyek nem léteznek.

Legyen most $m = 3^k$. Belátjuk, hogy ekkor az első m darab csupaegy mind különböző maradékot ad m-mel osztva (és így a megfelelő darabszám miatt teljes maradékrendszert alkot modulo m).

Tegyük fel indirekt, hogy valamely $1 \leq i < j \leq m$-re a j-edik és az i-edik csupaegy különbsége osztható lenne 3^k-val. Ekkor $(3^k, 10) = 1$ miatt ennek a különbségnek a 10^i-edrésze, ami éppen a $j - i$-edik csupaegy, is osztható lenne 3^k-val. Másrészt viszont r szerinti teljes indukcióval igazolható, hogy 3^r-rel legelőször a 3^r-edik csupaegy osztható (lásd az 1.3.12b feladatot). Ebből $3^k = m \leq j - i < m$ következik, ami ellentmondás.

Így $m = 3^k$ valóban megfelel a feladat feltételeinek.

• **g)** Akkor és csak akkor létezik modulo m teljes maradékrendszer teljes hatványokból, ha m négyzetmentes, azaz csupa különböző prímszám szorzata (vagy $m = 1$).

Ha m nem négyzetmentes, tehát valamely p prímre m osztható p^2-tel, akkor például a p maradék nem jöhet létre: ennek a maradékosztálynak min-

den eleme p-nek pontosan az első hatványával osztható, és így nem lehet teljes hatvány.

Az állítás másik felének igazolásához először megmutatjuk, hogy bármely p prímhez és bármely c-hez van olyan $s > 0$, hogy $c^{s+1} - c$ osztható p-vel. Ha c osztható p-vel, akkor ez tetszőleges s-re nyilvánvaló. Minden más esetben is c hatványai csak véges sokféle maradékot adhatnak p-vel osztva, ezért van olyan $r < t$, hogy p osztója $c^t - c^r = c^{r-1}(c^{t-r+1} - c)$-nek és így $(p, c) = 1$ miatt $c^{t-r+1} - c$-nek is.

Legyen most $m = p_1 \dots p_r$, $p_i \neq p_j$. Belátjuk, hogy tetszőleges c-hez van olyan $T > 0$, hogy c^{T+1} és c azonos maradékot adnak m-mel osztva, azaz $c^{T+1} - c$ osztható m-mel. Tekintsük a c-hez és a p_i-khez tartozó előző bekezdésbeli s_i kitevőket, ezek szorzata megfelel T-nek.

Végül tekintsünk egy $c_1, \dots, c_m$ teljes maradékrendszert modulo m, ahol $c_i > 1$. Az előbbiek szerint minden c_i-hez létezik olyan $k_i > 1$, amelyre $c_i \equiv c_i^{k_i} \pmod{m}$. Ekkor a $c_i^{k_i}$ teljes hatványok teljes maradékrendszert alkotnak modulo m.

• **2.2.8 a)** Pontosan akkor tudnak összegyűlni, ha m páratlan vagy osztható 4-gyel.

Ha m páratlan, akkor a legnagyobb fán levő mókus maradjon ott, a két szomszédja egy lépésben odaugrik, a két másodszomszédja két lépésben odaugrik stb.

Ha m osztható 4-gyel, akkor a fenti lépések után csak a legnagyobb fával szemközti fán marad egy mókus, amely páros sok ugrással eljut a legnagyobb fára, miközben egy másik mókus ide-oda ugrál a legnagyobb fa és valamelyik szomszédja között.

Végül, ha m páros, de 4-gyel nem osztható, akkor a mókusok nem tudnak összegyűlni. Tekintsük ugyanis, hány ugrással juthat el egy-egy mókus valamely kijelölt fára. Ezeknek az ugrásszámoknak az összege mindenképpen páratlan, tehát a feladat feltételei szerint nem valósítható meg.

• **b)** Pontosan a páratlan m-ekre lesz mókusgyűlés.

Az a)-beli gondolatmenetek továbbra is érvényesek, ha m nem osztható 4-gyel.

A 4-gyel osztható (illetve tetszőleges páros) m-ekre számozzuk meg a fákat sorban 1-től m-ig. Minden helyzetben adjuk össze azoknak a fáknak a sorszámait, amely fákon mókus ül, mégpedig minden sorszámot annyiszor, ahány mókus található az adott fán. Ennek az összegnek az m-mel vett maradéka nem változik az ugrálás során. A kiindulási helyzetben ez a maradék $1 + 2 + \dots + m = m(m+1)/2 = m \cdot (m/2) + m/2$ maradéka, ami $m/2$ (itt hivatkozhattunk volna a 2.2.7a feladat eredményére is). Ha minden mókus

ugyanazon a fán tanyázik, akkor a maradék nyilván 0, tehát ez az állapot nem jöhet létre.

• **2.2.12 a)** Ha $(a, m) = 1$, akkor az ar_i számok redukált maradékrendszert alkotnak, tehát páronként inkongruensek modulo m.

Belátjuk, hogy $m = 4k+2$ esetén $(a, m) = 2$ mellett is fennáll a páronkénti inkongruencia. Tegyük fel, hogy $ar_i \equiv ar_j \pmod{m}$. A 2.1.3 Tétel egyszerűsítési szabálya szerint ekkor

$$r_i \equiv r_j \pmod{\frac{m}{2}}. \tag{1}$$

Továbbá $(r_i, m) = (r_j, m) = 1$ miatt r_i és r_j páratlanok, tehát

$$r_i \equiv r_j \pmod{2}. \tag{2}$$

Mivel $(m/2, 2) = 1$, ezért az (1) és (2) kongruenciákból $r_i \equiv r_j \pmod{m}$, vagyis $i = j$ következik.

Most azt mutatjuk meg, hogy a fentiektől eltekintve az ar_i számok nem lesznek páronként inkongruensek modulo m.

A vizsgálatot két esetre bontjuk: (A) Az m-nek és az a-nak létezik egy közös $p > 2$ prímosztója; (B) $2 \mid a$ és $4 \mid m$.

Az (A) esetben

$$a \cdot \left(\frac{m}{p} + 1\right) \equiv a \cdot 1 \equiv a \cdot \left(\frac{2m}{p} + 1\right) \pmod{m}. \tag{3}$$

Ha itt $(m/p + 1, m) = 1$, akkor alkalmas $i \neq j$-re

$$r_i \equiv 1 \not\equiv \frac{m}{p} + 1 \equiv r_j \pmod{m}, \quad \text{de} \quad ar_i \equiv ar_j \pmod{m}.$$

Ha $(2m/p + 1, m) = 1$, akkor is ugyanígy kapjuk, hogy az ar_i számok nem lesznek páronként inkongruensek modulo m.

Így az (A) eset lezárásához elég azt igazolni, hogy $m/p + 1$ és $2m/p + 1$ közül legalább az egyik relatív prím az m-hez.

Legyen $(m/p+1, m) = d$. Ekkor $d \mid p(m/p+1) - m = p$, azaz csak $d = p$ vagy $d = 1$ lehetséges. Ugyanígy adódik, hogy $(2m/p + 1, m) = p$ vagy 1.

Mindkét legnagyobb közös osztó azonban nem lehet p, ugyanis

$$2(m/p + 1) - (2m/p + 1) = 1$$

miatt $m/p+1$ és $2m/p+1$ relatív prímek.

Végül, a (B) esetben $(m/2+1, 2) = 1$ miatt (3)-ból a fentiekhez hasonlóan kapjuk, hogy az ar_i számok nem lesznek páronként inkongruensek modulo m.

Most még egy bizonyítást mutatunk a feladat állításának arra a részére, hogy az ar_i számok csak a megadott esetekben lehetnek páronként inkongruensek modulo m. Ehhez az Euler-féle φ-függvényt fogjuk felhasználni.

Legyen p az m tetszőleges prímosztója. Az r_i számok száma $\varphi(m)$, és ezek (legfeljebb) $\varphi(m/p)$-féle maradékosztályba eshetnek modulo m/p. Ha tehát $\varphi(m) > \varphi(m/p)$, akkor biztosan van olyan r_i és r_j $(i \neq j)$, amelyek azonos maradékot adnak m/p-vel osztva, és így ha $p \mid a$, akkor $m \mid ar_i - ar_j$. Vagyis, ha az ar_i számok mind különböző maradékot adnak m-mel osztva, akkor az a-nak az m-mel csak olyan p közös prímosztója lehet, amelyre $\varphi(m) = \varphi(m/p)$.

A φ-függvény képletéből (lásd a 2.3.1 Tételt) könnyen adódik, hogy

$$\varphi(m) = p\varphi(m/p), \text{ ha } p^2 \mid m, \quad \text{és} \quad \varphi(m) = (p-1)\varphi(m/p), \text{ ha } (p, m/p) = 1\,.$$

Így a $\varphi(m) = \varphi(m/p)$ egyenlőség pontosan akkor teljesül, ha $p = 2$ és $(2, m/2) = 1$. Ez azt jelenti, hogy ha az ar_i számok páronként inkongruensek, és a és m nem relatív prímek, akkor csak az az eset lehetséges, hogy m páros és nem osztható 4-gyel, továbbá $(a, m) = 2$.

• **b)** Mivel az $r_i + b$ elemek száma $\varphi(m)$, és nyilván páronként inkongruensek modulo m, ezért akkor és csak akkor alkotnak redukált maradékrendszert, ha valamennyien relatív prímek m-hez.

Legyen az m összes különböző prímosztója $p_1, \ldots, p_s$. Először azt látjuk be, hogy ha $p_1 \cdot \ldots \cdot p_s \mid b$, akkor $(r_i + b, m) = 1$.

Ez valóban igaz, hiszen bármely $1 \leq j \leq s$ esetén

$$p_j \mid b, \;\; p_j \nmid r_i \Longrightarrow p_j \nmid r_i + b\,,$$

vagyis $r_i + b$-nek és m-nek nincs közös prímosztója.

Most megmutatjuk, hogy más b értékek nem felelnek meg, azaz található hozzájuk olyan i, amelyre $(r_i + b, m) \neq 1$.

Tegyük fel, hogy a p_j prímek közül pontosan a $p_1, \ldots, p_k$ osztója a b-nek. Itt a feltétel szerint $k < s$. Ha a b egyik p_j-vel sem osztható, akkor ezt tekinthetjük a $k = 0$ esetnek.

Legyen $v = p_{k+1} \ldots p_s - b$. Ekkor $(v, m) = 1$, ugyanis v nem osztható egyik p_j-vel sem, hiszen bármegyik j-re a $p_{k+1} \ldots p_s - b$ különbségnek pontosan az egyik tagja osztható p_j-vel.

Ez azt jelenti, hogy van olyan i, amelyre $r_i \equiv v \pmod{m}$. Ugyanakkor $r_i + b \equiv v + b = p_{k+1} \ldots p_s \pmod{m}$, tehát $r_i + b$ nem relatív prím az m-hez.

• **2.2.13** Akkor és csak akkor léteznek ilyen maradékrendszerek, ha $(k, m) = 1$.

Elégségesség: Tegyük fel, hogy $(k, m) = 1$, és legyen

$$a_i = 1 + ki, \quad i = 1, 2, \ldots, m, \quad \text{illetve} \quad b_j = 1 + mj, \quad j = 1, 2, \ldots, k\,.$$

A 2.2.4 Tétel alapján ezek valóban teljes maradékrendszerek modulo m, illetve modulo k.

Megmutatjuk, hogy az $a_i b_j$ szorzatok teljes maradékrendszert alkotnak modulo mk. Mivel a számuk mk, tehát csak a páronkénti inkongruenciát kell belátni.

Tegyük fel, hogy

$$(1 + ki)(1 + mj) \equiv (1 + kr)(1 + ms) \pmod{mk}.$$

A beszorzások elvégzése után mindkét oldalból 1-et kivonva és az mk-val osztható tagokat elhagyva a

$$ki + mj \equiv kr + ms \pmod{mk} \tag{1}$$

kongruenciához jutunk.

Tekintsük (1)-et most csak modulo m, ekkor $ki \equiv kr \pmod{m}$ adódik. Mivel $(k, m) = 1$, ezért ezt k-val végigosztva $i \equiv r \pmod{m}$, azaz $i = r$ következik. Ugyanígy kapjuk, hogy $j = s$.

Szükségesség: Tegyük fel, hogy $(m, k) \neq 1$. Azt kell igazolnunk, hogy az $a_1, \ldots, a_m$ (modulo m), illetve $b_1, \ldots, b_k$ (modulo k) teljes maradékrendszerekből képzett $a_i b_j$ szorzatok nem alkothatnak teljes maradékrendszert modulo mk.

Legyen p az m és a k egy közös prímosztója. Ekkor az a_i, illetve b_j elemek között m/p, illetve k/p darab p-vel osztható található.

Az $a_i b_j$ szorzat pontosan akkor osztható p-vel, ha egy tetszőleges a_i-t egy p-vel osztható b_j-vel szorzunk meg, vagy fordítva, de így kétszer számoltuk azokat a szorzatokat, ahol mindkét tényező osztható volt p-vel. Ebből következik, hogy az $a_i b_j$ szorzatok közül

$$m \cdot \frac{k}{p} + k \cdot \frac{m}{p} - \frac{m}{p} \cdot \frac{k}{p} = \frac{2mk}{p} - \frac{mk}{p^2} \tag{2}$$

a p-vel oszthatók száma. Ugyanakkor egy modulo mk teljes maradékrendszerben a p-vel oszthatók száma mk/p, ami ($p > 1$ miatt) nem egyenlő (2)-vel, tehát az $a_i b_j$ szorzatok nem alkothatnak teljes maradékrendszert modulo mk.

• **2.2.14 a)** *Szükségesség*: Ha $(a,b) = d > 1$, akkor T-ben csak d-vel osztható számok szerepelnek, tehát például a redukált maradékosztályok egyáltalán nincsenek reprezentálva.

Elégségesség: T elemszáma ab, így csak a páronkénti inkongruenciát kell igazolni. Ha

$$i_1 b + j_1 a \equiv i_2 b + j_2 a \pmod{ab},$$

akkor ez a kongruencia modulo a is teljesül: $i_1 b \equiv i_2 b \pmod{a}$. Itt $(a,b) = 1$ miatt egyszerűsíthetünk b-vel, ekkor $i_1 \equiv i_2 \pmod{a}$, vagyis $i_1 = i_2$ adódik. Hasonlóan kapjuk, hogy $j_1 = j_2$.

• **b)** A szükségesség, valamint az elégségességnél a páronkénti inkongruencia igazolása ugyanúgy történik, mint az a) részben. Az elégségességnél azt kell még belátni, hogy $(a,b) = 1$ esetén R minden eleme valamelyik redukált maradékosztályba tartozik, és valamennyi redukált maradékosztálynak valóban szerepel reprezentánsa R-ben. Más szóval:

(A) R elemei relatív prímek ab-hez; és

(B) ha $(u, ab) = 1$, akkor van R-nek olyan v eleme, amelyre $u \equiv v \pmod{ab}$.

(A) igazolásához tekintsük ab egy tetszőleges p prímosztóját, és mutassuk meg, hogy p nem osztója $r_i b + s_j a$-nak.

Mivel p prím és $(a,b) = 1$, ezért az alábbi két eset lehetséges:

$$(\alpha)\ p \mid a \ \text{ és } \ p \nmid b, \qquad (\beta)\ p \nmid a \ \text{ és } \ p \mid b\,.$$

Az (α) esetben $p \nmid b$ és $p \nmid r_i$, és ezért p prím volta miatt $p \nmid r_i b$, ugyanakkor $p \mid s_j a$, tehát valóban $p \nmid r_i b + s_j a$. Hasonlóan intézhető el a (β) eset is.

Végül (B) igazolásához legyen $(u, ab) = 1$, és írjuk fel az u számot

$$u = rb + sa \tag{1}$$

alakban. Ez megtehető, hiszen $(a,b) = 1$ miatt az $u = bx + ay$ diofantikus egyenlet megoldható.

Az (1) előállításban $(r,a) = 1$, hiszen különben (r,a) nemtriviális közös osztója lenne u-nak és ab-nek. Ezért van olyan i, amelyre $r \equiv r_i \pmod{a}$. Hasonlóan kapjuk, hogy van olyan j, amelyre $s \equiv s_j \pmod{b}$.

Megmutatjuk, hogy R-nek az így adódó $v = r_i b + s_j a$ eleme kongruens u-val modulo ab. A

$$v - u = (r_i b + s_j a) - (rb + sa) = (r_i - r)b + (s_j - s)a$$

előállítás végén szereplő összeg első tagjában $r_i - r$ osztható a-val, a második tagban pedig $s_j - s$ osztható b-vel, tehát $v - u$ valóban osztható ab-vel.

• **c)** Egyrészt a b)-beli R halmaz elemszáma $\varphi(a)\varphi(b)$, másrészt $(a,b)=1$ esetén R redukált maradékrendszer modulo ab, tehát elemszáma $\varphi(ab)$.

• **2.3.18** Az $n \le 3$ egészek nyilván megfelelők.

Megmutatjuk, hogy $n > 3$-ra $\varphi(n!) = k!$ nem teljesülhet. Ez $n = 4$-re nyilvánvaló, a továbbiakban legyen $n \ge 5$.

Jelöljük $A(j)$-vel a 2 kitevőjét a j kanonikus alakjában.

Mivel a feltétel szerint $k < n$, ezért

$$A(k!) \le A(n!)\,. \tag{1}$$

Másrészt $\varphi(n!)$-ban biztosan szerepelnek a $2^{A(n!)-1}$, $3-1$ és $5-1$ tényezők, ezért

$$A\big(\varphi(n!)\big) \ge (A(n!)-1)+1+2 > A(n!)\,. \tag{2}$$

Az (1) és (2) egyenlőtlenségekből $A\big(\varphi(n!)\big) > A(k!)$ adódik, így a $\varphi(n!) = k!$ egyenlőség valóban nem teljesülhet.

• **2.3.19** Akkor és csak akkor létezik olyan számtani sorozat, amely redukált maradékrendszer modulo m, ha m kettőhatvány, prím vagy egy prímszám kétszerese.

Elégségesség: Ha $m = 2^k$, akkor $1, 3, \dots, 2^k-1$, ha $m = p$, akkor $1, 2, \dots, p-1$, ha pedig $m = 2p$ (ahol $p > 2$), akkor $p+2, p+4, \dots, 2p-1, 2p+1, \dots, 3p-2$ megfelel.

Szükségesség: Indirekt, tegyük fel, hogy m nem a fenti alakú, és mégis találtunk egy olyan

$$a, a+d, \dots, a+(\varphi(m)-1)d \tag{1}$$

számtani sorozatot, amely redukált maradékrendszer modulo m.

Legyen p az m egy páratlan prímosztója.

Ha $p \mid d$, akkor az (1) számtani sorozat, vagyis a redukált maradékrendszer minden eleme a-val kongruens modulo p. Ez azonban az $(1)_m$ és a $(-1)_m$ redukált maradékosztályokat reprezentáló elemekre egyszerre nem teljesülhet, ugyanis $1 \not\equiv -1 \pmod{p}$.

Ha $(p,d) = 1$, akkor az $a, a+d, \dots, a+(p-1)d$ elemek teljes maradékrendszert alkotnak modulo p. Így ezek között lesz p-vel osztható is, ami nem relatív prím az m-hez. Ez azt jelenti, hogy ez az elem nem szerepelhet (1)-ben. Ez csak úgy lehetséges, ha $p-1 \ge \varphi(m)-1$, azaz

$$p \ge \varphi(m)\,. \tag{2}$$

Írjuk fel m-et $m = tp$ alakban, ahol a feltételek szerint $t > 2$. Ekkor $\varphi(t) \geq 2$ és a 2.3.10a feladat felhasználásával kapjuk, hogy

$$\varphi(m) = \varphi(tp) \geq \varphi(t)\varphi(p) \geq 2(p-1) > p\,,$$

ami ellentmond (2)-nek.

• **2.5.7** *Első megoldás*: Ha $(a, m) = d$, akkor a $b = d, 2d, \ldots, (m/d)d$, összesen m/d darab b értékre $f(b) = d$, a többi $1 \leq b \leq m$-re pedig nincs megoldás, tehát $f(b) = 0$. Ezért a keresett összeg $\sum_{b=1}^{m} f(b) = (m/d)d = m$.

• *Második megoldás*: Az $x = 1, 2, \ldots, m$ számok mindegyike pontosan egy darab b esetén lesz az $ax \equiv b \pmod{m}$ kongruencia megoldása, ennélfogva $\sum_{b=1}^{m} f(b) = m$. Ez a meggondolás nemcsak lineáris kongruenciákra, hanem tetszőleges magasabb fokú h polinomot véve a $h(x) \equiv b \pmod{m}$ kongruenciáknál is ugyanígy érvényes.

• **2.6.9** Az útmutatásnak megfelelően az $x \equiv 39^{38^{37}} \pmod{1440}$ kongruenciáról van szó, és $1440 = 2^5 \cdot 3^2 \cdot 5$ alapján ehelyett a 2^5, 3^2 és 5 modulusokra adódó kongruenciarendszert vizsgáljuk.

Mivel $39 \equiv -1 \pmod{5}$ és 38^{37} páros, így $x \equiv 1 \pmod{5}$.

Mivel $3 \mid 39$, ezért $x \equiv 0 \pmod{9}$.

Végül, $39 \equiv 7 \pmod{32}$ és $7^4 = 49^2 \equiv 17^2 \equiv 1 \pmod{32}$, továbbá $4 \mid 38^{37}$, ennélfogva $x \equiv 1 \pmod{32}$.

Ennek megfelelően az

$$x \equiv 1 \pmod{5}, \quad x \equiv 0 \pmod{9}, \quad x \equiv 1 \pmod{32}$$

szimultán kongruenciarendszert kell megoldani.

Az első és utolsó kongruenciából $x \equiv 1 \pmod{5 \cdot 32 = 160}$, azaz $x = 160z + 1$. Ezt a középső kongruenciába visszahelyettesítve $160z + 1 \equiv 0 \pmod{9}$, ahonnan $z \equiv 5 \pmod{9}$, vagyis $z = 9t + 5$. Innen

$$x = 160(9t + 5) + 1 = 1440t + 801, \quad \text{tehát} \quad x \equiv 801 \pmod{1440}\,.$$

A keresett pontos idő tehát 13 óra 21 perc.

• **2.8.5 c)** Az útmutatásban jelzett négy állítást bizonyítjuk.

(i) A műveletek „jósága”, az azonosságok teljesülése, a nullelem és az ellentett létezése az a) pontban látottak mintájára igazolható.

(ii) Legyen $m = tk$, ahol a feltételek szerint $t > 1$ és $(t, k) = 1$. A szóban forgó maradékosztályok $(rk)_m$, ahol $0 \leq r \leq t-1$. (Ha más r-eket veszünk, akkor is ugyanezeket a maradékosztályokat kapjuk, csak más reprezentánsokkal.)

Az $(sk)_m$ maradékosztály pontosan akkor lesz egységelem, ha

$$(sk)_m(rk)_m = (rk)_m, \quad \text{azaz} \quad srk^2 \equiv rk \pmod{tk}, \quad r = 0, 1 \ldots, t-1. \tag{1}$$

Ha az (1)-beli kongruencia $r = 1$-re teljesül, vagyis

$$sk^2 \equiv k \pmod{tk}, \tag{2}$$

akkor (2)-t r-rel beszorozva kapjuk, hogy (1) minden r-re fennáll. Ez azt jelenti, hogy (2) is ekvivalens azzal, hogy az $(sk)_m$ maradékosztály egységelem.

A (2) kongruenciát k-val elosztva a vele ekvivalens $sk \equiv 1 \pmod{t}$ kongruenciát kapjuk. Az egységelem létezéséhez tehát azt kell belátnunk, hogy az $xk \equiv 1 \pmod{t}$ lineáris kongruencia megoldható. Ez pedig $(t, k) = 1$ miatt valóban igaz.

(iii) A feltétel szerint $(t, k) = 1$ és t prím. (i) és (ii) alapján már csak azt kell igazolni, hogy minden $1 \leq r \leq t-1$ esetén az $(rk)_m$ maradékosztálynak létezik inverze. Legyen $(sk)_m$ az egységelem, és keressük $(rk)_m$ inverzét $(uk)_m$ alakban:

$$(rk)_m(uk)_m = (sk)_m, \qquad \text{azaz} \qquad ruk^2 \equiv sk \pmod{tk}. \tag{3}$$

A (3)-beli kongruenciát k-val elosztva a vele ekvivalens $ukr \equiv s \pmod{t}$ kongruenciához jutunk. Így azt kell belátnunk, hogy az $xkr \equiv s \pmod{t}$ lineáris kongruencia megoldható. Mivel $(t, k) = 1$ és t prím volta miatt $(t, r) = 1$, ezért $(t, kr) = 1$ is teljesül, tehát a kongruencia valóban megoldható.

Megjegyzés: A fenti gondolatmenet finomításával az is belátható, hogy ha $(t, k) = 1$, de t összetett, akkor nem kapunk testet. Sőt, ennél általánosabban az is igaz, hogy bármely $(t, k) = 1$ esetén az R gyűrű „teljesen ugyanolyan”, mint a modulo t maradékosztályok gyűrűje (pontos megfogalmazásban ez azt jelenti, hogy a két gyűrű *izomorf*, azaz létezik közöttük egy kölcsönösen egyértelmű, művelettartó leképezés).

(iv) Használjuk a korábbi jelöléseket. Az $(rk)_m \neq (0)_m$ maradékosztály pontosan akkor nullosztó, ha van olyan $(vk)_m \neq (0)_m$, amelyre

$$(rk)_m(vk)_m = (0)_m, \qquad \text{azaz} \qquad rvk^2 \equiv 0 \pmod{tk}. \tag{4}$$

A (4)-beli kongruenciát k-val elosztva a vele ekvivalens $vkr \equiv 0 \pmod{t}$ kongruenciát kapjuk. Így azt kell belátnunk, hogy az $xkr \equiv 0 \pmod{t}$ lineáris kongruenciának van $v \not\equiv 0 \pmod{t}$ megoldása is. Mivel a megoldásszám $(t, kr) > 1$, ez valóban teljesül.

3. Magasabb fokú kongruenciák

• **3.2.6** Tegyük fel, hogy $o_p(a) = o_p(-a) = k$. Ekkor

$$1 \equiv a^k \equiv (-a)^k = (-1)^k a^k \equiv (-1)^k \pmod{p}, \tag{1}$$

tehát k páros, $k = 2t$. Innen adódik, hogy $p \mid a^{2t} - 1 = (a^t - 1)(a^t + 1)$, amiből p prím tulajdonsága és $t < o_p(a)$ miatt $p \mid a^t + 1$, azaz $a^t \equiv -1 \pmod{p}$ következik. Ugyanígy kapjuk, hogy $(-a)^t \equiv -1 \pmod{p}$. Innen az (1)-hez hasonló gondolatmenettel azt nyerjük, hogy t is páros, azaz valóban $4 \mid o_p(a)$.

A megfordításhoz legyen $o_p(a) = 4s$. Ekkor $(-a)^{4s} = a^{4s} \equiv 1 \pmod{p}$ miatt $r = o_p(-a) \mid 4s$. Tegyük fel indirekt, hogy $r < 4s$. Ha r páros, akkor $1 \equiv (-a)^r = a^r \pmod{p}$ ellentmond $o_p(a) = 4s$-nek. Ha r páratlan, akkor $r \mid s$ és $1 \equiv (-a)^{2r} = a^{2r} \pmod{p}$ miatt ugyanígy ellentmondásra jutunk.

Megjegyezzük, hogy a megfordítás összetett modulus esetén is igaz (a bizonyításban sem használtuk ki, hogy a modulus prím), a másik irány azonban nem igaz, például $o_{21}(8) = o_{21}(-8) = 2$.

• **3.2.9** A feltételből $(a, p) = 1$, tehát $o_p(a)$ létezik. A kis Fermat-tétel szerint $1 \equiv a^{2p-2} = a^{2p-10}a^8 \equiv -a^8 \pmod{p}$, tehát $a^8 \equiv -1 \pmod{p}$. Ezt négyzetre emelve kapjuk, hogy $a^{16} \equiv 1 \pmod{p}$. A 3.2.2 Tétel (i) állítását (és a $p > 2$ miatt fennálló $1 \not\equiv -1 \pmod{p}$ inkongruenciát) felhasználva azt nyerjük, hogy $o_p(a) \mid 16$, de $o_p(a) \nmid 8$, tehát $o_p(a) = 16$.

• **3.3.10** Ha $a \equiv b^r \pmod{p}$ és $b \equiv a^s \pmod{p}$, akkor a 3.2.4a feladat alapján $o_p(a)$ és $o_p(b)$ kölcsönösen osztják egymást, tehát egyenlők.

A megfordításhoz vegyünk egy g primitív gyököt, legyen $a \equiv g^u \pmod{p}$, illetve $b \equiv g^v \pmod{p}$. A 3.2.4c feladat alapján ekkor $o_p(a) = (p-1)/(p-1, u)$, illetve $o_p(b) = (p-1)/(p-1, v)$. A rendek egyenlősége miatt innen $(p-1, u) = (p-1, v)$ következik.

Az a és b szerepe szimmetrikus, így elég olyan r létezését igazolnunk, amelyre $a \equiv b^r \pmod{p}$. Ez a kongruencia átírható $g^u \equiv g^{vr} \pmod{p}$ alakba, amely az $u \equiv vr \pmod{p-1}$ lineáris kongruenciával ekvivalens (ahol r az

ismeretlen). Ez a lineáris kongruencia a $(p-1, v) = (p-1, u) \mid u$ feltétel teljesülése miatt valóban megoldható.

Az r létezését az alábbi módon is beláthatjuk: Legyen $o_p(b) = k$. Ekkor egyrészt a 3.3.9 feladat (vagy a 3.3.3 Tétel második bizonyítása) szerint az összes k-adrendű elem száma $\varphi(k)$, másrészt a 3.2.4b feladat alapján a $b, b^2, \ldots, b^k$ elemek között is $\varphi(k)$ darab k-adrendű elem található, tehát ezek adják az összes k-adrendű elemet.

Megjegyzés: Hasonlóan igazolható a következő általánosabb eredmény is: $o_p(a) \mid o_p(b)$ akkor és csak akkor teljesül, ha van olyan r pozitív egész, amelyre $a \equiv b^r \pmod{p}$.

• **3.4.9** Először tegyük fel, hogy $\operatorname{ind}_g a = \operatorname{ind}_h b$. A 3.2.4c feladat alapján ekkor

$$o_p(a) = \frac{p-1}{\big(\operatorname{ind}_g a\,,\, p-1\big)} = \frac{p-1}{\big(\operatorname{ind}_h b\,,\, p-1\big)} = o_p(b)\,.$$

Most tegyük fel megfordítva, hogy $o_p(a) = o_p(b)$, és legyen g egy tetszőleges primitív gyök mod p, $\operatorname{ind}_g a = r$, $\operatorname{ind}_g b = s$. Ismét a 3.2.4c feladat alapján kapjuk, hogy ekkor $(r, p-1) = (s, p-1)$.

Az $\operatorname{ind}_h b = r$ feltételt teljesítő h primitív gyököt $h \equiv g^k \pmod{p}$ alakban keressük, ahol $(k, p-1) = 1$ a 3.3.4 Tétel (i) állítása szerint. Ekkor a feltétel átírható a

$$g^s \equiv b \equiv h^r \equiv (g^k)^r = g^{kr} \pmod{p}$$

alakba, ami

$$s \equiv kr \pmod{p-1} \tag{1}$$

fennállásával ekvivalens. Az (1) összefüggés a k-ra nézve egy lineáris kongruencia, amely $(r, p-1) = (s, p-1) \mid s$ miatt megoldható.

Azt kell még megmutatnunk, hogy van olyan k megoldás is, amely $p-1$-hez relatív prím.

Jelöljük az $(r, p-1) = (s, p-1)$ számot d-vel. Ekkor (1)-et d-vel egyszerűsítve a vele ekvivalens

$$\frac{s}{d} \equiv k \cdot \frac{r}{d} \quad \Big(\operatorname{mod} \frac{p-1}{d}\Big) \tag{2}$$

kongruenciához jutunk. A (2) bal oldala relatív prím a modulushoz, hiszen $(s/d, (p-1)/d) = 1$. Ezért a jobb oldal is relatív prím a modulushoz, tehát $(k, (p-1)/d) = 1$ is teljesül.

Ha $p-1$ minden prímosztója szerepel már $(p-1)/d$-ben is, akkor innen $(k, p-1) = 1$ következik, tehát készen vagyunk. Ellenkező esetben legyen Q

a $p-1$ azon prímosztóinak szorzata, amelyek relatív prímek $(p-1)/d$-hez és k_0 a (2) kongruencia egy tetszőleges megoldása. Ekkor az

$$x \equiv k_0 \pmod{\frac{p-1}{d}}, \qquad x \equiv 1 \pmod{Q}$$

szimultán kongruenciarendszer megoldásaként kapott k minden feltételnek eleget tesz: továbbra is kielégíti az (1) kongruenciát és emellett relatív prím $p-1$-hez.

• **3.5.12** *Első bizonyítás*: Ha az a szám 100-adik hatványmaradék, azaz $p \nmid a$ és van olyan w, amelyre $a \equiv w^{100} \pmod{p}$, akkor $a \equiv (w^5)^{20} \equiv (w^2)^{50} \pmod{p}$, tehát a egyben 20-adik és 50-edik hatványmaradék is.

A megfordításhoz tegyük fel, hogy az a szám 20-adik és 50-edik hatványmaradék is, vagyis $p \nmid a$ és van olyan u és v, amelyre $u^{20} \equiv v^{50} \equiv a \pmod{p}$. Ekkor $u^{100} \equiv a^5 \pmod{p}$ és $v^{100} \equiv a^2 \pmod{p}$. Ezeket az $a \cdot (a^2)^2 = a^5$ egyenlőségbe beírva $a(v^2)^{100} \equiv u^{100} \pmod{p}$ adódik. Mindkét oldalt $(v^{p-3})^{100}$-zal szorozva a kis Fermat-tétel miatt kapjuk, hogy $a \equiv (v^{p-3}u)^{100} \pmod{p}$, tehát az a valóban 100-adik hatványmaradék.

• *Második bizonyítás*: A 3.5.3 Tétel „indexes" kritériuma szerint az alábbi ekvivalenciát kell igazolni:

$$(100, p-1) \mid \operatorname{ind} a \iff \begin{cases} (20, p-1) \mid \operatorname{ind} a \\ (50, p-1) \mid \operatorname{ind} a \end{cases}$$

Itt $(20, p-1) \mid (100, p-1)$, illetve $(50, p-1) \mid (100, p-1)$ miatt az egyik irány nyilvánvaló.

A megfordításhoz azt kell megmutatnunk, hogy ha $(20, p-1) \mid \operatorname{ind} a$ és $(50, p-1) \mid \operatorname{ind} a$, akkor $(100, p-1) \mid \operatorname{ind} a$ is teljesül. Ha $25 \nmid p-1$, illetve $4 \nmid p-1$, akkor $(100, p-1) = (20, p-1)$, illetve $(100, p-1) = (50, p-1)$, tehát készen vagyunk. Ha $25 \mid p-1$ és $4 \mid p-1$, akkor $(50, p-1) = 50 \mid \operatorname{ind} a$ és $(20, p-1) = 20 \mid \operatorname{ind} a$, tehát $[50, 20] = 100 = (100, p-1) \mid \operatorname{ind} a$.

• Hasonló módon nyerhetünk egy harmadik bizonyítást a 3.5.3 Tétel „hatványos" kritériuma alapján, ezt nem részletezzük.

• Az útmutatásoknál már megfogalmaztuk a feladat általánosítását: a akkor és csak akkor lesz egyszerre k-adik és n-edik hatványmaradék, ha $[k, n]$-edik hatványmaradék.

Mindhárom bizonyítás átvihető az általános esetre is. Ekkor a „nehezebb iránynál" az első bizonyításban az $a \cdot (a^2)^2 = a^5$ alapjául szolgáló $1 = 1 \cdot 5 - 2 \cdot 2$

egyenlőség helyére az $1 = b([k,n]/k) - c([k,n]/n)$ előállítás lép, a második (és harmadik) bizonyításnál pedig a $[(k,p-1),(n,p-1)] = ([k,n],p-1)$ összefüggést lehet felhasználni (lásd az 1.6.19b feladatot).

• **3.7.3 b)** Bebizonyítjuk, hogy páratlan a és $k \geq 3$ esetén az

$$x^2 \equiv a \pmod{2^k} \tag{1}$$

kongruencia akkor és csak akkor oldható meg, ha

$$a \equiv 1 \pmod{8}, \tag{2}$$

és megoldhatóság esetén a megoldásszám 4.

Mivel páratlan c-re $c^2 \equiv 1 \pmod 8$, ezért (2) az (1) kongruencia megoldhatóságának szükséges feltétele.

Most azt igazoljuk, hogy megoldhatóság esetén a megoldásszám 4. Tegyük fel, hogy egy rögzített (páratlan) a-ra $x \equiv c \pmod{2^k}$ megoldása (1)-nek. Ebben az esetben d akkor és csak akkor megoldás, ha

$$2^k \mid d^2 - c^2 = (d-c)(d+c)\,. \tag{3}$$

Mivel c és d páratlan, ezért mindkét tényező páros szám. Megmutatjuk azonban, hogy $c+d$ és $d-c$ nem lehet egyszerre 4-gyel osztható. Ellenkező esetben ugyanis $4 \mid (d-c)+(d+c) = 2d$ is teljesülne, ami ellentmond d páratlanságának.

Ebből az következik, hogy (3) pontosan akkor érvényes, ha a $d-c$ és $d+c$ közül (pontosan) az egyik osztható 2^{k-1}-gyel. Innen $d \equiv \pm c \pmod{2^{k-1}}$, azaz (1)-re valóban négy (páronként inkongruens) megoldást kapunk mod 2^k:

$$x \equiv c, \qquad x \equiv c + 2^{k-1}, \qquad x \equiv -c, \qquad x \equiv -c + 2^{k-1}\,.$$

Végül belátjuk, hogy (1) megoldhatóságához a (2) feltétel nemcsak szükséges, hanem egyben elégséges is.

Nyilván elég a mod 2^k páronként inkongruens $1 \leq a < 2^k$ értékekre szorítkozni. Ekkor egy mod 2^k redukált maradékrendszer minden eleme pontosan egy ilyen a esetén lesz az (1) kongruenciának megoldása. Ez azt jelenti, hogy a kongruencia $\varphi(2^k)/4 = 2^{k-3}$ darab a-ra lesz megoldható. Mivel a (2) feltételt éppen ennyi a teljesíti, ezért az (1) kongruenciának ezek mindegyikére megoldhatónak kell lennie.

4. Legendre- és Jacobi-szimbólum

• **4.1.13 a)** (Valamennyi kongruencia a 13 modulusra vonatkozik.) Először elérjük, hogy a másodfokú tag együtthatója 1 legyen. Ehhez a kongruenciát megszorozzuk -4-gyel (mivel $(4,13)=1$, ezért ez ekvivalens lépés): $-12x^2-20x-20\equiv 0$, azaz $x^2+6x+6\equiv 0$. Most alakítsunk teljes négyzetté:

$$(x+3)^2\equiv 3\equiv 16 \iff x+3\equiv\pm 4 \iff x\equiv 1 \text{ és } 6.$$

A -4-gyel való szorzás helyett oszthatunk is 3-mal, ha előtte a többi tag együtthatóját 3-mal oszthatókra cseréljük: $3x^2+5x+5\equiv 3x^2+18x+18\equiv 0$, és így $x^2+6x+6\equiv 0$.

Egy újabb lehetőség, hogy az eredeti kongruenciát beszorozzuk $4\cdot 3$-mal, és ezután alakítunk teljes négyzetté:

$$36x^2+60x+60=(6x+5)^2+35\equiv 0 \iff (6x+5)^2\equiv 4 \iff 6x+5\equiv\pm 2\,.$$

Ezután a $6x\equiv -3$ és $6x\equiv -7$ lineáris kongruenciákat kell megoldani.

• **4.2.8** Az útmutatásban szereplő $f=(x^2+1)(x^2-17)(x^2+17)$ polinomnak nyilván nincs racionális gyöke.

Az $f(x)\equiv 0 \pmod m$ kongruencia megoldhatóságához a kínai maradéktétel szerint elég igazolni, hogy az $f(x)\equiv 0 \pmod{p^k}$ kongruencia megoldható minden p^k prímhatványra.

Az $x^2\equiv 17 \pmod{2^k}$ kongruencia megoldható, mert $17\equiv 1 \pmod 8$, lásd a 3.7.3b feladat megoldását.

Ha $p>2$ és $p\neq 17$, akkor

$$\left(\frac{-1}{p}\right)\left(\frac{17}{p}\right)\left(\frac{-17}{p}\right)=\left(\frac{-17}{p}\right)^2=1$$

miatt az f-et alkotó három tényező közül legalább az egyiknek létezik megoldása mod p. Innen p páratlansága miatt a 3.7.2 feladat (vagy a 3.7.1 Tétel) alapján adódik, hogy mod p^k is létezik megoldás.

Végül $p=17$ esetén az $x^2\equiv -1 \pmod{17}$ kongruencia megoldható, mert $17\equiv 1 \pmod 4$, és így mod 17^k is van megoldás.

• **4.3.7 b)** Megmutatjuk, hogy éppen a négyzetszámok a keresett a értékek.

A négyzetszámok valóban megfelelők, ugyanis ha $a=s^2$, akkor

$$\left(\frac{a}{m}\right)=\left(\frac{s^2}{m}\right)=\left(\frac{s}{m}\right)^2=1\,.$$

A megfordításhoz tegyük fel, hogy a nem négyzetszám. Legyen először $a > 0$. Ekkor van olyan prím, amely páratlan hatványon szerepel az a kanonikus alakjában.

Ha a 2 ilyen prím, azaz $a = 2^i t$, ahol i és t páratlan, akkor legyen m az $x \equiv 5 \pmod 8$, $x \equiv 1 \pmod t$ szimultán kongruenciarendszer egy (pozitív) megoldása. Ekkor ($t > 1$-re)

$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^i \left(\frac{t}{m}\right) = (-1)\left(\frac{m}{t}\right) = (-1)\left(\frac{1}{t}\right) = -1\,.$$

Ha egy $p > 2$ prím kitevője páratlan, azaz $a = 2^i p^j v$, ahol $i \geq 0$, j páratlan és $(v, 2p) = 1$, akkor legyen m az $x \equiv 1 \pmod 8$, $x \equiv 1 \pmod v$, $x \equiv c \pmod p$ szimultán kongruenciarendszer egy (pozitív) megoldása, ahol c egy kvadratikus nemmaradék mod p. Ekkor

$$\left(\frac{a}{m}\right) = \left(\frac{2}{m}\right)^i \left(\frac{v}{m}\right)\left(\frac{c}{p}\right)^j = 1 \cdot \left(\frac{m}{v}\right)(-1) = (-1)\left(\frac{1}{v}\right) = -1\,.$$

Legyen végül $a < 0$. Ha $|a|$ nem négyzetszám, akkor járjunk el a fentiek szerint. Ha $a = -s^2$, akkor bármely $4k+3$ alakú m megfelel (amely páratlan, 1-nél nagyobb és relatív prím a-hoz):

$$\left(\frac{-s^2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{s}{m}\right)^2 = -1\,.$$

5. Prímszámok

• **5.1.5 c)** Indirekt tegyük fel, hogy $p < n$ a legkisebb olyan prím, amelyre $(p, d) = 1$. Ekkor a prímekből álló számtani sorozat első p tagja, $a, a+d, \ldots, a+(p-1)d$ teljes maradékrendszer modulo p, és így van közöttük p-vel osztható, ami a feltétel szerint csak maga a p lehet, azaz $p = a + jd$. Ha itt $j > 0$, akkor p minimalitása miatt az a prím osztója d-nek, tehát a osztója minden tagnak, ami ellentmond ezek prím voltának. Ezért csak $p = a$ lehetséges, ekkor viszont a számtani sorozat $p+1$-edik tagja, $a + pd = p(1+d)$ nem prím.

• **5.2.5** Gauss tétele szerint azt kell megvizsgálnunk, mely $2^k - 1$ alakú számok írhatók fel különböző Fermat-prímek szorzataként.

Először megmutatjuk, hogy k szükségképpen kettőhatvány. Indirekt tegyük fel, hogy k-nak létezik egy q páratlan prímosztója. Ekkor $2^q - 1 \mid 2^k - 1$ is teljesül. Továbbá az 5.2.3 Tétel szerint $2^q - 1$ minden prímosztója $2rq + 1$ alakú, ami q páratlansága miatt nem lehet Fermat-prím. Ez viszont ellentmond annak, hogy $2^k - 1$ minden prímosztója Fermat-prím.

Legyen tehát $k = 2^{n+1}$. Ekkor az 5.2.1a feladat alapján $2^k - 1 = F_0F_1 \dots F_n$. Ha $0 \le n \le 4$, akkor kapjuk, hogy $2^k - 1$ valóban csupa különböző Fermat-prím szorzata, tehát ez az öt k érték megfelel. Ha azonban $n \ge 5$, akkor $2^k - 1$ osztható F_5-tel, és így 641-gyel is, ami nem Fermat-prím.

Összefoglalva, szabályos $2^k - 1$-szög akkor és csak akkor szerkeszthető, ha $k = 2, 4, 8, 16$ vagy 32.

• **5.2.7** Tegyük fel először, hogy $2p + 1 \mid M_p$, és legyen q a $2p + 1$ tetszőleges prímosztója. Ekkor $q \mid M_p$ is teljesül, ezért az 5.2.3 Tétel szerint $q = 2pk + 1$ alakú. Mivel $q \mid 2p+1$, így csak $q = 2p+1$ lehetséges, vagyis $2p+1$ prím. Azt kell még igazolni, hogy $p \equiv 3 \pmod 4$. Nyilván $p \ne 2$. Ha $p \equiv 1 \pmod 4$ állna fenn, akkor ebből $q = 2p + 1 \equiv 3 \pmod 8$ és így $\left(\frac{2}{q}\right) = -1$ következne. Ez azonban ellentmond annak, hogy a $2p+1 \mid M_p$ feltétel átírható a $2^{(q-1)/2} \equiv 1 \pmod q$ alakba.

A megfordításhoz legyen $q = 2p + 1$ prím és $p \equiv 3 \pmod 4$. Ekkor $q \equiv 7 \pmod 8$, ezért $\left(\frac{2}{q}\right) = 1$, azaz $2^{(q-1)/2} \equiv 1 \pmod q$, ami éppen a bizonyítani kívánt $2p + 1 \mid M_p$ oszthatóságot jelenti.

• **5.2.9** A számpár páros eleme csak kettőhatvány lehet.

Vizsgáljuk először azt az esetet, amikor $n + 1 = 2^\alpha$ és $n = q^\beta$ (ahol q páratlan prím, α, $\beta \ge 1$). Ekkor $2^\alpha = q^\beta + 1$.

Ha $\beta = 1$, akkor q Mersenne-prím.

Ha β páros, akkor a jobb oldal 2 maradékot ad 4-gyel osztva, ami lehetetlen.

Ha $\beta > 1$ páratlan, akkor a jobb oldal $(q+1)(q^{\beta-1} - q^{\beta-2} \pm \dots + 1)$ alakba írható. Mivel itt a második tényező egy 1-nél nagyobb páratlan szám, ez nem lehet kettőhatvány, tehát ismét ellentmondásra jutottunk.

Tegyük most fel, hogy $n = 2^\alpha$ és $n + 1 = q^\beta$. Ekkor $2^\alpha = q^\beta - 1$.

Ha $\beta = 1$, akkor q Fermat-prím.

Ha β páros, akkor a jobb oldal $(q^{\beta/2} - 1)(q^{\beta/2} + 1)$ alakba írható. Itt mindkét tényező maga is kettőhatvány, a különbségük kettő, tehát csak a $2 \cdot 4$ szorzatról lehet szó. Ekkor $2^\alpha = 8, q^\beta = 9$.

Végül, ha $\beta > 1$ páratlan, akkor a jobb oldal $(q-1)(q^{\beta-1} + q^{\beta-2} + \dots + 1)$ alakba írható. Mivel itt a második tényező egy 1-nél nagyobb páratlan szám, ez nem lehet kettőhatvány, tehát ellentmondásra jutottunk.

Az összes megfelelő számpár tehát a következő: (8,9); (M_p, M_p+1), ahol M_p Mersenne-prím; $(2^{2^n}, F_n)$, ahol F_n Fermat-prím.

• **5.5.9 a)** Ha $n = k^3$, akkor $(k+1)^3 = n+3n^{2/3}+3n^{1/3}+1 > n+n^{2/3}$. Az 5.5.4 Tétel (A) része szerint minden elég nagy n-re n és $n + n^{2/3}$ között található prímszám, tehát a $\left(k^3, (k+1)^3\right)$ intervallum is tartalmaz prímszámot.

• **b)** Az útmutatásban vázolt gondolatmenetet fogjuk követni. Előállítunk egy q_n prímszámsorozatot, amelyhez található lesz olyan α, hogy

$$q_n = \lfloor \alpha^{3^n} \rfloor \tag{1}$$

teljesüljön. Legyen

$$c_n = \sqrt[3^n]{q_n} \qquad \text{és} \qquad d_n = \sqrt[3^n]{q_n + 1}\,.$$

Ezzel a jelöléssel (1) éppen azt jelenti, hogy

$$c_n \le \alpha < d_n\,. \tag{2}$$

A q_n prímeket úgy fogjuk megválasztani, hogy $[c_n, d_n]$ egy egymásba skatulyázott zárt intervallumsorozatot alkosson, azaz minden n-re

$$\sqrt[3^n]{q_n} < \sqrt[3^{n+1}]{q_{n+1}} < \sqrt[3^{n+1}]{q_{n+1}+1} < \sqrt[3^n]{q_n+1} \tag{3}$$

teljesüljön. A (3) egyenlőtlenséget 3^{n+1}-edik hatványra emelve a

$$q_n^3 \le q_{n+1} < (q_n+1)^3 - 1 \tag{4}$$

feltételhez jutunk.

Ennek megfelelően legyen q_1 egy nagy prímszám, q_2 egy olyan prím, amely q_1^3 és $(q_1+1)^3$ közé esik, és általában, ha q_n-et már kiválasztottuk, akkor q_{n+1} legyen egy olyan prím, amely eleget tesz (4)-nek. Ilyen q_{n+1} prímet a feladat a) része szerint mindig találunk (ha q_1-et elegendően nagyra választottuk).

Ily módon tehát egy egymásba skatulyázott $[c_n, d_n]$ zárt intervallumsorozatot kaptunk. Ennek van közös pontja, jelöljük ezt α-val. Megmutatjuk, hogy α megfelel a feladat állításának.

Az α konstrukciója szerint minden n-re $c_n \le \alpha \le d_n$, és nekünk a hajszálnyival élesebb (2) egyenlőtlenségre van szükségünk. Az jelenthetne problémát, ha valamely n-re $\alpha = d_n$ teljesülne. Mivel azonban a d_j számok (3) és (4) miatt *szigorúan* monoton csökkennek, ezért $\alpha \le d_{n+1} < d_n$, tehát $\alpha = d_n$ nem fordulhat elő.

• **c)** A b) rész bizonyításában láttuk, hogy csak α létezését tudjuk garantálni, α konkrét értékét nem tudjuk megadni. Sőt, a helyzet tulajdonképpen ennél is sokkal furcsább: *előbb* „gyártanunk" kellett végtelen sok alkalmas prímet ahhoz, hogy olyan α-t biztosítsunk, amelynek segítségével *utána* az $\lfloor \alpha^{3^n} \rfloor$ „képletből" visszakapjuk *ugyanazokat* a prímeket, amelyeket az α elkészítéséhez fel kellett használnunk.

• **5.6.1** Jelölje az a), b), ... részekben szereplő számsorozatokat rendre $A = \{a_1, a_2, \ldots\}$, $B = \{b_1, b_2, \ldots\}$ stb., és ezekben az n-nél nem nagyobb elemek számát $A(n)$, $B(n)$ stb.

• **a)** Nyilván $a_n = Ln$, tehát

$$\sum_{n=1}^{\infty} \frac{1}{a_n} \;=\; \frac{1}{L} \sum_{n=1}^{\infty} \frac{1}{n} \;=\; \infty \qquad \text{és} \qquad A(n) \;=\; \left\lfloor \frac{n}{L} \right\rfloor \sim \frac{n}{L}\,.$$

• **b)** Mivel pozitív tagú sorról van szó, a tagokat tetszőlegesen átrendezhetjük. Csoportosítsuk a teljes hatványokat aszerint, hogy melyik számnak a hatványai (így bizonyos hatványokat többször is megszámolunk, pl. $64 = 4^3 = 8^2$). Ekkor

$$\sum_{n=1}^{\infty} \frac{1}{b_n} \;<\; \sum_{j=2}^{\infty} \sum_{k=2}^{\infty} \frac{1}{j^k} \;=\; \sum_{j=2}^{\infty} \frac{1}{j^2(1-\frac{1}{j})} \;=\; \sum_{j=2}^{\infty} \frac{1}{j(j-1)} = 1\,.$$

Rátérve $B(n)$ vizsgálatára, megmutatjuk, hogy itt lényegében csak a négyzetszámok számítanak, a magasabb hatványok száma ehhez képest elhanyagolható.

Rögzített $k > 1$ kitevőre az 1-nél nagyobb és n-nél kisebb vagy egyenlő k-adik hatványok száma $\lfloor \sqrt[k]{n} \rfloor - 1$. Így bizonyos számokat (például a 64-et) több k-nál is figyelembe vettünk, továbbá csak olyan k értékek jöhetnek szóba, amelyekre $2^k \le n$, azaz $k \le \lfloor \log_2 n \rfloor$. Ennek megfelelően

$$\lfloor \sqrt{n} \rfloor \;-\; 1 \;\le\; B(n) \;\le\; \sqrt{n} \;+\; \sum_{k=3}^{\lfloor \log_2 n \rfloor} \sqrt[k]{n} \;\le\; \sqrt{n} \;+\; (\log_2 n)\sqrt[3]{n}\,.$$

Innen $\sqrt{n}$-nel való osztással kapjuk, hogy $B(n) \sim \sqrt{n}$.

• **c)** A négyzetmentes számok között megtalálhatók a prímek is, és már ez utóbbiak reciprokösszege is divergens.

• **d)** Az 5.6.1 Tétel harmadik bizonyításának mintájára adódik, hogy

$$\sum_{d_j \le n} \frac{1}{d_j} \le \prod_{p<L} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{\nu_p}}\right),$$

ahol

$$p^{\nu_p} \le n < p^{\nu_p+1}, \qquad \text{azaz} \qquad \nu_p = \lfloor \log_p n \rfloor .$$

A mértani sorozatokat összegezve és felülről becsülve azt kapjuk, hogy

$$\sum_{d_j \le n} \frac{1}{d_j} \le \prod_{p<L} \frac{1}{1-\frac{1}{p}} .$$

Mivel itt a jobb oldal független az n-től, ezért a $\sum_{j=1}^{\infty} 1/d_j$ sor konvergens.

Áttérve $D(n)$ becslésére, legyenek $p_1, \ldots, p_k$ az L-nél kisebb prímek. Ekkor a D sorozat tagjainak kanonikus alakja

$$d = p_1^{\alpha_1} \ldots p_k^{\alpha_k} . \tag{1}$$

Ha $d \le n$, akkor (1)-ben nyilván minden i-re

$$p_i^{\alpha_i} \le n, \qquad \text{azaz} \qquad 0 \le \alpha_i \le \frac{\log n}{\log p_i} .$$

Ebből következik, hogy

$$D(n) \le \prod_{i=1}^{k} \Big(1 + \frac{\log n}{\log p_i}\Big) \le c(\log n)^k ,$$

ahol c alkalmas konstans.

A $D(n)$ alsó becsléséhez vegyük észre, hogy ha (1)-ben minden i-re

$$p_i^{\alpha_i} \le \sqrt[k]{n}, \qquad \text{azaz} \qquad 0 \le \alpha_i \le \frac{\log n}{k \log p_i} ,$$

akkor $d \le n$. Innen az előzőkhöz hasonlóan adódik, hogy alkalmas c' konstanssal $D(n) > c'(\log n)^k$.

Az aszimptotika igazolásához az (1) logaritmizált alakjával dolgozunk:

$$\log d = \alpha_1 \log p_1 + \ldots + \alpha_k \log p_k .$$

Ekkor $D(n)$ azoknak az $(\alpha_1, \ldots, \alpha_k)$ szám k-asoknak a száma, ahol

$$\alpha_1 \log p_1 + \ldots + \alpha_k \log p_k \leq \log n \quad \text{és mindegyik } \alpha_i \text{ nemnegatív egész.} \quad (2)$$

A bizonyítást először $L = 6$-ra részletezzük, utána pedig jelezni fogjuk, hogyan vihető át ez a gondolatmenet tetszőleges L-re.

Ha $L = 6$, akkor $k = 3$; a 2, 3 és 5 prímekről van szó. Ekkor (2) szerint $D(n)$ az

$$\alpha_1 \log 2 + \alpha_2 \log 3 + \alpha_3 \log 5 \leq \log n \quad (3)$$

egyenlőtlenség nemnegatív egész $(\alpha_1, \alpha_2, \alpha_3)$ megoldásainak a száma.

Az $x_1 \log 2 + x_2 \log 3 + x_3 \log 5 = \log n$ egyenlőséget úgy is felfoghatjuk, mint a térben egy síknak az egyenletét. Ekkor az

$$x_1 \log 2 + x_2 \log 3 + x_3 \log 5 \leq \log n, \qquad x_i \geq 0$$

egyenlőtlenségrendszert annak a G_n háromoldalú gúlának az (x_1, x_2, x_3) pontjai elégítik ki, amelyet a fenti sík és a koordinátatengelyek pozitív félegyenesei határolnak.

Az *egész* koordinátájú (x_1, x_2, x_3) pontok éppen a szokásos (egységnyi oldalú, az origót is tartalmazó) kockarács pontjai a térben. Eszerint (3) nemnegatív egész megoldásainak a száma éppen a G_n gúlába eső rácspontok száma.

Szemléletesen világos (és könnyen igazolható, vö. a 7.5.9 feladattal), hogy nagy n esetén a G_n gúlába eső rácspontok száma „körülbelül" a G_n gúla térfogata. Precíz fogalmazásban ez azt jelenti, hogy $n \to \infty$ mellett a rácspontok száma és a gúla térfogata aszimptotikusan egyenlő.

A G_n gúla $V(G_n)$ térfogata az origóból kiinduló három páronként merőleges él szorzatának az egyhatoda. Mindezek alapján

$$D(n) \sim V(G_n) = \frac{(\log n)^3}{6 \cdot \log 2 \cdot \log 3 \cdot \log 5} \,.$$

Tetszőleges L esetén is hasonlóan kell eljárni: (2) szerint ekkor a k-dimenziós térben keressük a megfelelő „gúla" (ún. szimplex) rácspontjainak a számát, ami aszimptotikusan egyenlő a gúla térfogatával. Ebben az esetben

$$D(n) \sim V(G_n) = \frac{(\log n)^k}{k! \prod_{p<L} \log p} \,.$$

• **e)** Ezek között a számok között megtalálhatók az L-nél nagyobb prímszámok is, és már ez utóbbiak reciprokösszege is divergens.

Az $E(n)$ becsléséhez vegyük észre, hogy itt éppen azokról a számokról van szó, amelyek az L-nél nem nagyobb prímek mindegyikéhez relatív prímek. Legyen $M = \prod_{p\le L} p$. Ekkor az előbbiek szerint bármely M egymást követő egész szám között az E sorozatnak pontosan $\varphi(M)$ eleme található. Ennek megfelelően

$$\text{ha} \quad tM \le n < (t+1)M, \quad \text{akkor} \quad t\varphi(M) \le E(n) \le (t+1)\varphi(M)\,.$$

Az $E(n)$-re és az n-re vonatkozó egyenlőtlenségekből kapjuk, hogy

$$\frac{t\varphi(M)}{(t+1)M} \le \frac{E(n)}{n} \le \frac{(t+1)\varphi(M)}{tM}\,.$$

Mivel $t = \lfloor n/M \rfloor$, ezért ha $n \to \infty$, akkor t is a végtelenhez, $t/(t+1)$ és $(t+1)/t$ pedig 1-hez tart. Ez azt jelenti, hogy

$$\lim_{n\to\infty} \frac{E(n)}{n} = \frac{\varphi(M)}{M} = \prod_{p\le L}\Big(1-\frac{1}{p}\Big)\,, \qquad \text{azaz} \qquad E(n) \sim n \prod_{p\le L}\Big(1-\frac{1}{p}\Big)\,.$$

• **f)** A négyzetteljes számok reciprokaiból képzett $\sum_{j=1}^{\infty} 1/f_j$ sor konvergenciáját kétféleképpen is bebizonyítjuk. (Egy harmadik bizonyítás az 5.6.7 feladat alapján adható.)

Első bizonyítás: Az 5.6.1 Tétel harmadik bizonyításához hasonlóan adódik, hogy

$$\sum_{f_j\le n} \frac{1}{f_j} \le \prod_{p^2\le n}\left(1+\frac{1}{p^2}+\frac{1}{p^3}+\ldots+\frac{1}{p^{\nu_p}}\right)\,,$$

ahol

$$p^{\nu_p} \le n < p^{\nu_p+1}\,, \qquad \text{azaz} \qquad \nu_p = \lfloor \log_p n \rfloor\,.$$

Itt az egyes tényezőkben az 1 után mértani sorozatok állnak, ezeket összegezve és felülről becsülve azt kapjuk, hogy

$$\sum_{f_j\le n} \frac{1}{f_j} \le \prod_{p\le\sqrt{n}}\Big(1+\frac{1}{p^2(1-\frac{1}{p})}\Big) = \prod_{p\le\sqrt{n}}\Big(1+\frac{1}{p(p-1)}\Big)\,. \tag{4}$$

Ha p_k a k-adik prím, akkor $k>1$ esetén $p_k(p_k-1) > p_{k-1}^2$. Ennek alapján a (4) jobb oldalán a $p = p_1 = 2$-nek megfelelő

$$1+\frac{1}{2\cdot 1} = \frac{3}{2}$$

tényezőt változatlanul hagyva és $k > 1$ esetén a $p = p_k$-nak megfelelő tényezőre az

$$1 + \frac{1}{p_k(p_k - 1)} < 1 + \frac{1}{p_{k-1}^2}$$

becslést alkalmazva a (4) jobb oldalára a következő felső becslést nyerjük:

$$\prod_{p \le \sqrt{n}} \Big(1 + \frac{1}{p(p-1)}\Big) \; < \; \frac{3}{2} \prod_{p \le \sqrt{n}} \Big(1 + \frac{1}{p^2}\Big) \; < \; 2 \sum_{j=1}^{\infty} \frac{1}{j^2} \, .$$

Második bizonyítás: Először megmutatjuk, hogy minden négyzetteljes szám felírható egy négyzetszám és egy köbszám szorzataként. Legyen az f négyzetteljes szám kanonikus alakja

$$f = q_1^{\mu_1} \dots q_r^{\mu_r} \, , \qquad \mu_i \ge 2, \quad i = 1, 2, \dots, r \, .$$

A μ_i kitevők felírhatók $\mu_i = 2\alpha_i + 3\beta_i$ alakban, ahol $\alpha_i, \beta_i \ge 0$ (például β_i aszerint legyen 0 vagy 1, hogy μ_i páros, illetve páratlan). Ekkor

$$f = a^2 b^3 \, , \qquad \text{ahol} \qquad a = \prod_{i=1}^{r} q_i^{\alpha_i} \quad \text{és} \quad b = \prod_{i=1}^{r} q_i^{\beta_i} \, . \tag{5}$$

(5)-ből következik, hogy a négyzetteljes számok reciprokösszege kisebb, mint a négyzetszámok reciprokösszegének és a köbszámok reciprokösszegének a szorzata, ami igazolja a konvergenciát.

Az $F(n)$ becsléséhez (5)-öt fogjuk felhasználni. Láttuk, hogy az is elérhető, hogy minden $\beta_i = 0$ vagy 1, vagyis a b négyzetmentes. Az is azonnal adódik, hogy ilyen feltételek mellett az $f = a^2 b^3$ előállítás már egyértelmű, vagyis minden négyzetteljes szám egyértelműen írható fel egy négyzetszámnak és egy négyzetmentes szám köbének a szorzataként. Nyilvánvaló továbbá, hogy az 1 kivételével az ilyen $a^2 b^3$ szorzatok valóban négyzetteljesek.

Mindezek alapján $F(n)$-et úgy kapjuk meg, hogy az n-nél nem nagyobb ilyen $a^2 b^3$ szorzatok számából 1-et levonunk. Egy ilyen szorzatban b négyzetmentes és $b \le \sqrt[3]{n}$, valamint rögzített b mellett $1 \le a \le \sqrt{n/b^3}$. Ennek megfelelően

$$F(n) \; = \; -1 + \sum_{b \le \sqrt[3]{n}}{}' \left\lfloor \sqrt{\frac{n}{b^3}} \right\rfloor \, , \tag{6}$$

ahol $\sum'$-vel azt jelöljük, hogy csak a négyzetmentes b értékekre kell az összegzést végezni.

A (6) jobb oldalát az egészrészek felbontása után

$$\sqrt{n}\sum_{b\le\sqrt[3]{n}}{}' \frac{1}{b^{3/2}} \;+\; U(n)$$

alakba írhatjuk, ahol az $U(n)$ hibatag a másik részhez képest elhanyagolható, ugyanis

$$|U(n)| \;\le\; 1+\sum_{b\le\sqrt[3]{n}}{}' 1 \;\le\; 1+\sqrt[3]{n}\,.$$

Ebből következik, hogy

$$F(n)\sim c\sqrt{n}\,, \qquad \text{ahol} \qquad c=\sum_{b=1}^{\infty}{}' \frac{1}{b^{3/2}}\,.$$

• **5.6.6** Az $(1-1/p^s)^{-1}$ tényezőket írjuk fel végtelen mértani sorként, és használjuk fel, hogy két pozitív tagú konvergens sor (vagy általában két abszolút konvergens sor) „ugyanúgy szorozható össze, mint azt a véges sok tagból álló összegek szorzásánál megszoktuk". Ebből következik, hogy

$$\prod_{p\le n}\frac{1}{1-\frac{1}{p^s}} \;=\; \prod_{p\le n}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots\right) \;=\; \sum_{j\in W_n}\frac{1}{j^s}\,,$$

ahol W_n azoknak a számoknak a halmaza, amelyek minden prímosztója kisebb vagy egyenlő, mint n. Nyilván

$$\sum_{j=1}^{n}\frac{1}{j^s} \;\le\; \sum_{j\in W_n}\frac{1}{j^s} \;<\; \sum_{j=1}^{\infty}\frac{1}{j^s}\,. \tag{7}$$

Mivel (7) bal oldala $n\to\infty$ esetén a jobb oldalhoz tart, ezért

$$\lim_{n\to\infty}\prod_{p\le n}\frac{1}{1-\frac{1}{p^s}} \;=\; \lim_{n\to\infty}\sum_{j\in W_n}\frac{1}{j^s} \;=\; \sum_{j=1}^{\infty}\frac{1}{j^s} \;=\; \zeta(s)\,.$$

• **5.7.4** A feltétel szerint az n összetett számra

$$2^{n-1}\equiv 1 \pmod{n} \tag{1}$$

teljesül. Azt kell belátnunk, hogy 2^n-1 is összetett, ez azonnal következik n összetettségéből (lásd az 1.4.4a feladatot), továbbá hogy

$$2^{2^n-2} \equiv 1 \pmod{2^n-1} \tag{2}$$

is fennáll.

Mivel nyilván $2^n \equiv 1 \pmod{2^n-1}$, ezért (2)-höz elég megmutatni, hogy $n \mid 2^n-2$. Ez azonban azonnal következik (1)-ből.

• **5.7.17** Legyen az $n>1$ páratlan szám kanonikus alakja

$$n = q_1^{\alpha_1} \dots q_s^{\alpha_s}, \qquad \text{és} \qquad n-1 = 2^k r, \text{ ahol } r \text{ páratlan.}$$

Azt kell igazolnunk, hogy ha egy a-ra

$$a^r,\ a^{2r},\ a^{4r},\ \dots,\ a^{2^{k-2}r} = a^{\frac{n-1}{4}},\ a^{2^{k-1}r} = a^{\frac{n-1}{2}}$$

jó sorozat, azaz ezek modulo n vett legkisebb abszolút értékű maradékai között előfordul -1 vagy pedig a^r maradéka 1, akkor

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{*}$$

is fennáll.

Ha $a^r \equiv 1 \pmod{n}$, akkor egyrészt ezt a kongruenciát 2^{k-1} hatványra emelve kapjuk, hogy $a^{(n-1)/2} \equiv 1 \pmod{n}$, másrészt

$$1 = \left(\frac{1}{n}\right) = \left(\frac{a^r}{n}\right) = \left(\frac{a}{n}\right)^r,$$

ahonnan r páratlansága miatt $\left(\frac{a}{n}\right) = 1$ következik. Így (*) ekkor valóban teljesül.

Tegyük most fel, hogy

$$a^{2^j r} \equiv -1 \pmod{n}, \quad \text{ahol} \quad 0 \le j \le k-2\,. \tag{3}$$

Ekkor ($j < k-1$ miatt) $a^{(n-1)/2} \equiv 1 \pmod{n}$. Azt kell igazolni, hogy $\left(\frac{a}{n}\right) = 1$ is teljesül.

A (3) kongruenciát mod q_i tekintve, majd négyzetre emelve kapjuk, hogy

$$a^{2^j r} \equiv -1 \pmod{q_i} \qquad \text{és} \qquad a^{2^{j+1} r} \equiv 1 \pmod{q_i}\,.$$

Ez azt jelenti, hogy

$$o_{q_i}(a) \not| 2^j r \qquad \text{és} \qquad o_{q_i}(a) \mid 2^{j+1} r\,,$$

vagyis

$$o_{q_i}(a) = 2^{j+1} r_i\,, \qquad \text{ahol} \qquad r_i \mid r\,. \tag{4}$$

Mivel q_i prím, ezért (4)-ből

$$a^{2^j r_i} \equiv -1 \pmod{q_i} \tag{5}$$

következik, továbbá $o_{q_i}(a) \mid q-1$ alapján azt is kapjuk, hogy alkalmas h_i-vel

$$q_i = 1 + 2^{j+1} r_i h_i\,. \tag{6}$$

Az (5) és (6) összefüggések felhasználásával

$$\left(\frac{a}{q_i}\right) \equiv a^{(q_i-1)/2} = a^{2^j r_i h_i} = \left(a^{2^j r_i}\right)^{h_i} \equiv (-1)^{h_i} \pmod{q_i} \tag{7}$$

adódik. A (7) alapján

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{s} \left(\frac{a}{q_i}\right)^{\alpha_i} = (-1)^{\sum_{i=1}^{s} \alpha_i h_i}\,,$$

vagyis $\left(\frac{a}{n}\right) = 1$-hez azt kell megmutatni, hogy $\sum_{i=1}^{s} \alpha_i h_i$ páros. Mivel minden r_i páratlan, ez azzal ekvivalens, hogy $\sum_{i=1}^{s} \alpha_i r_i h_i$ páros.

A (6) felhasználásával

$$n = \prod_{i=1}^{s} q_i^{\alpha_i} = \prod_{i=1}^{s} (1 + 2^{j+1} r_i h_i)^{\alpha_i}\,. \tag{8}$$

A (8) jobb oldalán a beszorzást elvégezve a legtöbb tag osztható lesz 2^{j+2}-vel:

$$n = 1 + 2^{j+1} \sum_{i=1}^{s} \alpha_i r_i h_i + 2^{j+2} C\,. \tag{9}$$

Mivel $n - 1 = 2^k r$, azaz $n = 1 + 2^k r$, ezért (9)-ből

$$2^k r = 2^{j+1} \sum_{i=1}^{s} \alpha_i r_i h_i + 2^{j+2} C\,,$$

majd 2^{j+1}-gyel történő egyszerűsítés után

$$2^{k-j-1}r - 2C = \sum_{i=1}^{s} \alpha_i r_i h_i \tag{10}$$

következik. A (10) bal oldala $j < k-1$ miatt páros, tehát a jobb oldalon álló $\sum_{i=1}^{s} \alpha_i r_i h_i$ összeg is valóban páros.

Végül az

$$a^{2^{k-1}r} = a^{\frac{n-1}{2}} \equiv -1 \pmod{q_i}$$

esetben is ugyanígy járhatunk el. Ekkor $\left(\frac{a}{n}\right) = -1$-et kell igazolnunk, ami $\sum_{i=1}^{s} \alpha_i r_i h_i$ páratlanságával ekvivalens. Ekkor $j = k-1$-nek megfelelően (10) bal oldalán $r - 2C$ áll, ami r páratlansága miatt valóban páratlan.

6. Számelméleti függvények

• **6.1.7 a)** Az $ab = (a,b)[a,b]$ egyenlőség és a teljes additivitás miatt az $f(ab)$ függvényértéket kétféleképpen kiszámítva éppen a kívánt

$$f(a) + f(b) = f((a,b)) + f([a,b]) \tag{1}$$

egyenlőséget kapjuk.

• **b)** Legyen a és b kanonikus alakja

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \quad \text{és} \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \quad \text{ahol} \quad \alpha_i \geq 0,\ \beta_j \geq 0\,.$$

Ekkor

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}$$

és

$$[a,b] = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}\,.$$

Innen a 6.1.7 Tétel alapján kapjuk, hogy

$$f(a) + f(b) = \sum_{i=1}^{r} f(p_i^{\alpha_i}) + f(p_i^{\beta_i}) \tag{2}$$

és

$$f((a,b)) + f([a,b]) = \sum_{i=1}^{r} f(p_i^{\min(\alpha_i,\beta_i)}) + f(p_i^{\max(\alpha_i,\beta_i)})\,. \tag{3}$$

(Mindez $f(1) = 0$ miatt akkor is érvényes, ha a kitevők között a 0 is előfordul.)

Mivel tetszőleges két valós szám egyike a két szám minimuma, másika pedig a két szám maximuma, ezért az α_i, β_i és $\min(\alpha_i, \beta_i), \max(\alpha_i, \beta_i)$ értékek bármely i esetén megegyeznek. Ennélfogva (2)-ből és (3)-ból azonnal következik (1).

• **c)** Megmutatjuk, hogy a feltételt az $f = g + c$ alakú függvények elégítik ki, ahol g additív, c pedig konstans.

Mivel az additív függvényekről már láttuk, hogy megfelelnek, ezért azonnal adódik, hogy a fenti alakú függvények is jók.

Megfordítva, tegyük fel, hogy az f függvényre (1) bármely a, b esetén teljesül, és próbáljuk előállítani f-et a keresett $f = g + c$ alakban, ahol g additív és c konstans.

A $g(1) = 0$ feltételből kapjuk, hogy c értéke csak $f(1)$ lehet. Ennélfogva azt kell igazolnunk, hogy a $g(n) = f(n) - f(1)$ függvény additív. Ez azt jelenti, hogy bármely $(a, b) = 1$ esetén

$$f(ab) - f(1) = \big(f(a) - f(1)\big) + \big(f(b) - f(1)\big)\,,$$

azaz

$$f(1) + f(ab) = f(a) + f(b)\,. \tag{4}$$

Mivel $(a, b) = 1$ miatt $[a, b] = ab$, ezért (4) bal oldalán $f(1)$, illetve $f(ab)$ helyére $f((a, b))$, illetve $f([a, b])$ írható. Ennélfogva (4) azonnal következik (1)-ből.

• **d)** Az előzőkhöz hasonlóan igazolhatjuk, hogy az

$$f(a)f(b) = f((a, b))f([a, b]) \tag{5}$$

egyenlőség minden a, b esetén teljesül a teljesen multiplikatív, sőt a multiplikatív függvényekre, valamint ezek konstansszorosaira, továbbá, hogy $f(1) \neq 0$ esetén ez utóbbiak adják az összes lehetséges f-et.

Vizsgáljuk most az $f(1) = 0$ esetet. Ha $f = 0$, akkor (5) nyilván teljesül. Tegyük fel, hogy $f \neq 0$ kielégíti (5)-öt, és legyen K a legkisebb pozitív egész, amelyre $f(K) \neq 0$.

Ha $K \nmid n$, akkor

$$f(K)f(n) = f((K, n))f([K, n]). \tag{6}$$

Mivel a feltétel szerint $(K, n) < K$, ezért $f((K, n)) = 0$, továbbá $f(K) \neq 0$, és így (6) alapján $f(n) = 0$.

Legyen most $h(n) = f(Kn)$. Ekkor h is kielégíti (5)-öt bármely a, b esetén:

$$h(a)h(b) = f(Ka)f(Kb) = f((Ka, Kb))f([Ka, Kb]) = \\ = f(K(a, b))f(K[a, b]) = h((a, b))h([a, b]).$$

Továbbá $h(1) = f(K) \neq 0$, ezért h egy multiplikatív függvény konstansszorosa.

Összefoglalva, azt kaptuk, hogy

$$f(n) = \begin{cases} 0, & \text{ha } K \nmid n; \\ cg\left(\frac{n}{K}\right), & \text{ha } K \mid n, \end{cases} \tag{7}$$

ahol $g(n)$ multiplikatív, c konstans és K rögzített pozitív egész. Megfordítva, könnyen adódik, hogy a (7)-beli f függvényekre (5) valóban teljesül minden a, b esetén. A (7) tartalmazza az $f(1) \neq 0$, illetve $f = 0$ eseteket is, amikor $K = 1$, illetve $c = 0$ (vagy $g = 0$). Ezzel beláttuk, hogy a (7) képlet adja az összes keresett függvényt.

• **6.1.9 d)** A feladat megoldásában az olyan additív függvények játszanak szerepet, amelyek egy vagy két prím hatványaitól eltekintve minden prímhatvány helyen 0 értéket vesznek fel.

Legyen p tetszőleges prímszám. Nevezzünk házi használatra egy h additív függvényt p-talpúnak, ha h a p hatványain tetszőleges értéket vehet fel, a többi prímhatvány helyen viszont csak 0-t. Egy általános n helyen felvett függvényértéket innen a következőképpen kapunk meg: az n felírható $n = tp^\alpha$ alakban, ahol $(t, p) = 1$, ekkor $h(n) = h(p^\alpha)$. (Ez az $\alpha = 0$ esetben is helyes, hiszen az additivitás miatt $h(1) = 0$.) Az ilyen függvényeket úgy is jellemezhetjük, hogy minden $(c, p) = 1$ esetén $h(c) = 0$.

Hasonlóképpen definiáljuk a (p, q)-talpú függvényeket, ahol p és q különböző prímek: ekkor a h additív függvény a p és q hatványain tetszőleges értéket vehet fel, a többi prímhatvány helyen viszont csak 0-t. Egy általános n helyen felvett függvényértéket innen a következőképpen kapunk meg: az n felírható $n = tp^\alpha q^\beta$ alakban, ahol $(t, pq) = 1$, ekkor $h(n) = h(p^\alpha) + h(q^\beta)$. Az ilyen függvényeket úgy is jellemezhetjük, hogy minden $(c, pq) = 1$ esetén $h(c) = 0$.

Rátérve a feladat megoldására, ha $f = 0$ vagy $g = 0$, akkor nyilván minden teljesül.

Most megmutatjuk, hogy ha f és g is p-talpú (ugyanazzal a p prímmel), akkor fg is additív.

Azt kell igazolni, hogy bármely $(a, b) = 1$ esetén fennáll

$$(fg)(ab) = (fg)(a) + (fg)(b). \tag{8}$$

Ha a és b egyike sem osztható p-vel, akkor a (8) mindkét oldala 0.

Ha $a = tp^\alpha$, ahol $\alpha > 0$, $(t,p) = 1$, akkor $(a,b) = 1$ miatt $p \nmid b$, és így

$$(fg)(b) = 0\,, \quad (fg)(a) = (fg)(ab) = f(p^\alpha)g(p^\alpha)\,,$$

tehát (8) ekkor is teljesül.

További megoldásokat kapunk, ha f és g is (p,q)-talpú (ugyanazokkal a p, q prímekkel), és létezik olyan c, hogy

$$g(p^\alpha) = cf(p^\alpha)\,, \qquad g(q^\beta) = -cf(q^\beta)\,, \qquad \alpha,\beta = 1,2,3,\ldots \tag{9}$$

Ekkor (8) igazolása az előzőek mintájára történhet, ha a és b közül legalább az egyik se p-vel, se q-val nem osztható.

A fennmaradó esetben $a = tp^\alpha$ és $b = sq^\beta$ (vagy fordítva), ahol $(ts, pq) = 1$. Ekkor (9)-et is felhasználva kapjuk, hogy

$$\begin{aligned}
(fg)(a) &= f(p^\alpha)g(p^\alpha) = cf(p^\alpha)^2\,,\\
(fg)(b) &= f(q^\beta)g(q^\beta) = -cf(q^\beta)^2\,,\\
(fg)(ab) &= \big(f(p^\alpha) + f(q^\beta)\big)\big(g(p^\alpha) + g(q^\beta)\big) =\\
&= \big(f(p^\alpha) + f(q^\beta)\big)\big(cf(p^\alpha) - cf(q^\beta)\big)\,,
\end{aligned}$$

ahonnan (8) leolvasható.

Összefoglalva, eddig a következő megoldásokat találtuk:

I. $f = 0$ vagy $g = 0$.

II. f és g tetszőleges p-talpú függvény.

III. f és g olyan (p,q)-talpú függvények, amelyek kielégítik (9)-et.

Most azt igazoljuk, hogy a fentiekben az összes megoldást megadtuk, vagyis ha f, g és fg is additív, akkor az f, g függvénypár ezen három típus valamelyikébe tartozik.

Tegyük fel, hogy f, g és fg is additív. Ekkor bármely $(a,b) = 1$ esetén fennáll

$$f(a)g(a) + f(b)g(b) = f(ab)g(ab) = \big(f(a) + f(b)\big)\big(g(a) + g(b)\big)\,,$$

azaz

$$f(a)g(b) + f(b)g(a) = 0\,. \tag{10}$$

Feltehetjük, hogy $f \neq 0$ és $g \neq 0$. Az f és g függvények prímhatvány helyeken felvett értékeit fogjuk vizsgálni. Két esetet különböztetünk meg:

(A) Van olyan p^α prímhatvány, amelyre $f(p^\alpha) \neq 0$ és $g(p^\alpha) = 0$.

(B) Bármely w prímhatványra $f(w) = 0 \iff g(w) = 0$.

Az (A) esetben alkalmazzuk (10)-et az $a = p^\alpha$ és $b = r^\gamma$ értékekre, ahol r a p-től különböző prím. Ekkor $g(r^\gamma) = 0$ adódik. Ez azt jelenti, hogy a g függvény p-talpú. Mivel $g \neq 0$, ezért van olyan κ, amelyre $g(p^\kappa) \neq 0$. Ekkor (10)-et az $a = p^\kappa$ és $b = r^\gamma$ értékekre alkalmazva kapjuk, hogy $f(r^\gamma) = 0$. Eszerint az f is p-talpú, vagyis egy II. típusú f, g párról van szó.

Térjünk át a (B) esetre, és legyen a p^α olyan prímhatvány, amelyre $f(p^\alpha) \neq 0$ és $g(p^\alpha) \neq 0$. Ha az f függvény p-talpú, akkor a (B) feltétel szerint a g is az, tehát ismét a II. típusú f, g párhoz jutottunk.

Így feltehetjük, hogy van egy q^β prímhatvány is, ahol q a p-től különböző prím és $f(q^\beta) \neq 0$, $g(q^\beta) \neq 0$.

Először megmutatjuk, hogy f és g is (p, q)-talpú, vagyis tetszőleges, a p-től és q-tól különböző r prím esetén minden γ-ra $f(r^\gamma) = g(r^\gamma) = 0$ teljesül.

Tegyük fel indirekt, hogy van olyan r^γ, amelyre $f(r^\gamma) \neq 0$.

Ha $f(a)f(b) \neq 0$, akkor (10) átírható a

$$\frac{g(a)}{f(a)} = -\frac{g(b)}{f(b)} \tag{11}$$

alakba. Alkalmazzuk (11)-et rendre a p^α, q^β és r^γ számokból képezett párokra:

$$\frac{g(p^\alpha)}{f(p^\alpha)} = -\frac{g(q^\beta)}{f(q^\beta)} = \frac{g(r^\gamma)}{f(r^\gamma)} = -\frac{g(p^\alpha)}{f(p^\alpha)},$$

ami ellentmond $g(p^\alpha) \neq 0$-nak.

Végül (9) igazolásához alkalmazzuk (11)-et először $a = p^\alpha$, $b = q^\beta$ szereposztással, és legyen a két oldal közös értéke c. Ezután az a változatlanul tartása mellett legyen $b = q^\nu$, ahol ν végigfut az összes olyan kitevőn, amelyre $f(q^\nu) \neq 0$, majd hasonló módon, rögzített $b = q^\beta$ mellett legyen $a = p^\mu$ az összes olyan μ-vel, amelyre $f(p^\mu) \neq 0$. Ekkor (11)-ből éppen a (9) összefüggések adódnak.

Ezzel megmutattuk, hogy az f, g függvénypár III. típusú.

• **6.1.13 a)** Tegyük fel, hogy az f additív függvény k különböző értéket vesz fel. Ezek között $f(1) = 0$ miatt szerepel a 0 is.

Először azt igazoljuk, hogy bármely k darab, páronként relatív prím $a_1, a_2, \ldots, a_k$ szám közül kiválasztható néhány (esetleg csak egy, esetleg az összes), amelyek szorzatán az f értéke 0.

Tekintsük az

$$f(a_1),\ f(a_1a_2),\ \ldots,\ f(a_1a_2\ldots a_k)$$

függvényértékeket. Ha ezek mind különbözők, akkor szerepel közöttük a 0 is, tehát készen vagyunk. Ha pedig van köztük két egyenlő, azaz valamilyen $1 \le i < j \le k$-ra $f(a_1a_2\ldots a_j) = f(a_1a_2\ldots a_i)$, akkor

$$\begin{aligned} 0 &= f(a_1a_2\ldots a_j) - f(a_1a_2\ldots a_i) = \\ &= \big(f(a_1) + f(a_2) + \ldots + f(a_j)\big) - \big(f(a_1) + f(a_2) + \ldots + f(a_i)\big) = \\ &= f(a_{i+1}) + \ldots + f(a_j) = f(a_{i+1}\ldots a_j)\,. \end{aligned}$$

Legyen most b tetszőleges. A b-nél nagyobb prímek sorozatát osszuk be k hosszúságú blokkokba. Ekkor az előzőek szerint bármely r-re az r-edik blokk néhány alkalmas prímjének a c_r szorzatát véve $f(c_r) = 0$. Így $(b, c_r) = 1$ miatt $f(bc_r) = f(b) + f(c_r) = f(b)$, tehát az $f(b)$ értéket a függvény végtelen sok helyen felveszi.

• **6.1.15** Nyilván $\varphi_2(1) = 1$. Egy $n = p^\alpha$ prímhatványra $(j, p^\alpha) \ne 1 \iff p \mid j$, ezért az $i = rp$, illetve $i = rp - 1$ alakú számok esetén lesz $(i, p^\alpha) \ne 1$, illetve $(i + 1, p^\alpha) \ne 1$. Ennek megfelelően $\varphi_2(p^\alpha)$ meghatározásához az $1, 2, \ldots, p^\alpha$ számok számából le kell vonni a

$$p - 1,\ p,\ 2p - 1,\ 2p,\ \ldots,\ p^\alpha - 1 = p^{\alpha-1}p - 1,\ p^\alpha = p^{\alpha-1}p$$

számok számát, vagyis

$$\varphi_2(p^\alpha) = p^\alpha - 2p^{\alpha-1}\,. \tag{12}$$

Most belátjuk, hogy $\varphi_2(n)$ multiplikatív. Legyen $(a, b) = 1$ és

$$1 \le u_1 < u_2 < \ldots < u_r \le a, \qquad \text{illetve} \qquad 1 \le v_1 < v_2 < \ldots < v_s \le b$$

az összes olyan szám (1 és a, illetve 1 és b között), amelyre

$$(u_i, a) = (u_i + 1, a) = 1, \qquad \text{illetve} \qquad (v_j, b) = (v_j + 1, b) = 1.$$

Ekkor tehát $r = \varphi_2(a)$ és $s = \varphi_2(b)$.

Tekintsük az

$$\begin{aligned} x &\equiv u_i \pmod a \\ x &\equiv v_j \pmod b \end{aligned} \tag{13}$$

szimultán kongruenciarendszert. Mivel $(a, b) = 1$, ezért ennek a rendszernek bármely $i = 1, \ldots, \varphi_2(a)$, $j = 1, \ldots, \varphi_2(b)$ esetén pontosan egy megoldása van modulo ab. Jelöljük w_{ij}-vel az $1 \le w_{ij} \le ab$ feltételt is kielégítő (egyértelműen

meghatározott) megoldást. Ezzel összesen $\varphi_2(a)\varphi_2(b)$ darab w_{ij} számot definiáltunk.

Megmutatjuk, hogy

$$(w_{ij}, ab) = (w_{ij} + 1, ab) = 1\,, \tag{14}$$

és ezek adják az összes ilyen tulajdonságú számot 1 és ab között. Ebből következik, hogy a w_{ij} értékek száma $\varphi_2(ab)$, amit az előzőkkel összevetve éppen a kívánt multiplikativitás adódik.

A (14)-hez azt kell belátni, hogy w_{ij} és $w_{ij}+1$ az a-hoz és b-hez is relatív prímek. Mivel $w_{ij} \equiv u_i \pmod a$, ezért

$$(w_{ij}, a) = (u_i, a) = 1 \qquad \text{és} \qquad (w_{ij} + 1, a) = (u_i + 1, a) = 1\,.$$

Hasonlóan adódik, hogy $(w_{ij}, b) = (w_{ij} + 1, b) = 1$ is teljesül.

Most tegyük fel, hogy $1 \le c \le ab$ és $(c, ab) = (c + 1, ab) = 1$. Azt kell igazolni, hogy alkalmas i-vel és j-vel $c = w_{ij}$. Legyen c legkisebb pozitív maradéka a-val, illetve b-vel osztva c', illetve c''. Ekkor

$$(c', a) = (c, a) = 1 \qquad \text{és} \qquad (c' + 1, a) = (c + 1, a) = 1\,.$$

Ez azt jelenti, hogy alkalmas i-vel $c' = u_i$. Hasonlóan kapjuk, hogy $c'' = v_j$.

Ebből következik, hogy c megoldása a (13) szimultán kongruenciarendszernek, tehát $c = w_{ij}$. Ezzel $\varphi_2(n)$ multiplikativitásának a bizonyítását befejeztük.

Végül, legyen az n kanonikus alakja $n = \prod_{i=1}^{t} p_i^{\alpha_i}$. Ekkor a multiplikativitás és (12) felhasználásával kapjuk, hogy

$$\varphi_2(n) = \prod_{i=1}^{t} \left(p_i^{\alpha_i} - 2p_i^{\alpha_i - 1}\right) = n \prod_{\substack{p \mid n \\ p \text{ prím}}} \left(1 - \frac{2}{p}\right)\,.$$

• **6.2.7** *Első megoldás*: Megmutatjuk, hogy $\sigma(n) \neq 2p$, ahol p egy tetszőleges $6k - 1$ alakú prím.

Tegyük fel indirekt, hogy valamilyen n pozitív egészre $\sigma(n) = 2p$. Legyen az n kanonikus alakja $n = q_1^{\alpha_1} \dots q_r^{\alpha_r}$, ekkor

$$2p = \sigma(n) = \prod_{i=1}^{r} \sigma(q_i^{\alpha_i})\,.$$

Mivel a 2 nem szerepel a σ-függvény értékkészletében, ezért $r = 1$, azaz $n = q^\alpha$ (ahol q prím), és

$$2p = 1 + q + q^2 + \ldots + q^\alpha . \tag{1}$$

Mivel (1) bal oldala páros, ezért $q > 2$ és α páratlan, így (1) jobb oldalán kiemelhető $1 + q$. Nyilván $1 + q \neq 1, 2, p$, tehát csak $1 + q = 2p$ lehetséges (és ekkor $\alpha = 1$). A feltétel szerint $2p \equiv 1 \pmod 3$, ezért innen $3 \mid q$ adódik. Ez azt jelenti, hogy $q = 3$, vagyis $p = 2$, ami ellentmondás.

Ugyanígy igazolható az is, hogy $\sigma(n) \neq 2p$, ahol p egy 3-nál nagyobb $5k - 2$ alakú prím vagy egy tetszőleges $7k - 3$ vagy $11k - 5$ alakú prím stb.

• *Második megoldás*: Megmutatjuk, hogy $\sigma(n) \neq 3^s$, ha $s > 1$.

Most is indirekt bizonyítunk. A σ-függvény multiplikativitásából adódik, hogy az n kanonikus alakjában szereplő bármely q^α prímhatványra $\sigma(q^\alpha) = 3^t$ (ahol $1 \leq t \leq s$), azaz

$$3^t = 1 + q + q^2 + \ldots + q^\alpha . \tag{2}$$

Vizsgáljuk először a $q = 2$ esetet, ekkor (2) átírható a

$$3^t = 2^{\alpha+1} - 1 \tag{3}$$

alakba. Ha $\alpha = 1$, akkor $t = 1$ és megoldást kapunk. Ha $\alpha > 1$, akkor (3) bal oldala 8-cal osztva 3-at vagy 1-et ad maradékul, a jobb oldal pedig 7-et, ami ellentmondás.

A továbbiakban feltehetjük tehát, hogy $q > 2$ és $t > 1$. A (2) egyenlőséget modulo 2, illetve modulo 3 tekintve azt kapjuk, hogy α páros, továbbá $q \equiv 1 \pmod 3$ és $\alpha \equiv 2 \pmod 3$. Ezért (2) jobb oldalán kiemelhető $1+q+q^2$, ami így szintén a 3-nak hatványa. Ez azonban lehetetlen, mert $1+q+q^2$ nem osztható már 9-cel sem (ezt például a $q \equiv 1, 4$ és $7 \pmod 9$ esetek behelyettesítésével ellenőrizhetjük).

Ezzel megmutattuk, hogy a 2 az egyetlen prímhatvány, és így a 2 az egyetlen olyan n is, amelyre $\sigma(n)$ a 3-nak hatványa. Ez azt jelenti, hogy $s > 1$-re $\sigma(n) = 3^s$ nem lehetséges.

• *Harmadik megoldás*: Azt mutatjuk meg, hogy a „legtöbb” páratlan szám nem szerepel a σ-függvény értékkészletében.

Legyen N tetszőleges („nagy”) egész szám, és vizsgáljuk meg, legfeljebb hány olyan x van, amelyre $\sigma(x)$ egy $2N$-nél kisebb páratlan szám. Ekkor egyrészt nyilván $x < 2N$, továbbá a 6.2.6a feladat szerint x csak négyzetszám vagy egy négyzetszám kétszerese lehet. A $2N$-nél kisebb négyzetszámok száma $\lfloor\sqrt{2N-1}\rfloor$, a $2t^2$ alakú számok száma pedig $\lfloor\sqrt{N-1}\rfloor$. Ennek megfelelően a

szóba jövő x-ek száma kisebb, mint $(\sqrt{2}+1)\sqrt{N}$. A $2N$-nél kisebb páratlan számok száma ugyanakkor N. Ez azt jelenti, hogy a $2N$-nél kisebb páratlan számok közül legalább

$$N-(\sqrt{2}+1)\sqrt{N} \tag{4}$$

nem szerepel a σ-függvény értékkészletében. (A (4)-beli függvény „nagyon erősen" tart a végtelenhez, mert a második tag „elhanyagolható" az N-hez képest.)

• *Negyedik megoldás*: Legyen N tetszőleges egész, és vizsgáljuk meg, legfeljebb hány olyan x van, amelyre $\sigma(x)\le N$. Ekkor egyrészt nyilván $x\le N$, másrészt a $2N/3$-nál nagyobb s páros számok nem jók, mert ezekre $\sigma(s)\ge s+s/2>N$. A $2N/3$ és N közötti páros számok száma

$$\left\lfloor\frac{N}{2}\right\rfloor-\left\lfloor\frac{N}{3}\right\rfloor>\frac{N}{6}-2\,,$$

ezért a szóba jövő x-ek száma legfeljebb $5N/6+2$. Ez azt jelenti, hogy az $1,2,\dots,N$ számok közül legalább $N/6-2$ nem szerepel a σ-függvény értékkészletében.

• *Ötödik megoldás*: A negyedik megoldáshoz hasonló gondolatmenetet alkalmazunk, de most nem azt használjuk ki, hogy bizonyos $x\le N$-ek esetén $\sigma(x)>N$, hanem azt, hogy „sok" olyan $x_i\ne x_j$ pár van, amelyre $\sigma(x_i)=\sigma(x_j)$. Ilyen párok például a $6t$ és a $11t$, ha $(t,66)=1$. Ezek száma N-ig körülbelül

$$N\frac{\varphi(66)}{66\cdot 11}=0{,}027\ldots N.$$

Mivel az $x\le N$ helyek közül legalább ennyi esetben a σ-függvény értéke „összeesik", ezért legalább ennyi szám ki kell hogy maradjon a függvény értékkészletéből.

• *Megjegyzés*: A feladat állítása jelentősen élesíthető: a „legtöbb" egész szám hiányzik a σ-függvény értékkészletéből, vagyis az értékkészlet a természetes számoknak egy „ritka" részsorozatát alkotja. Ez pontosan a következőt jelenti. Legyen $U(N)$ azoknak az $y\le N$ értékeknek a száma, amelyek előfordulnak a σ-függvény értékkészletében. Ekkor $\lim_{N\to\infty}U(N)/N=0$. A bizonyításhoz a prímszámoknak a számtani sorozatokban való eloszlásáról szóló eredményeket kell felhasználni, lásd a 6.4.8 és 6.4.9 feladatokat.

• **6.2.8** Az $n=1$ érték nyilván megfelel. Megmutatjuk, hogy más megoldás nincs. Ha $n\ge 2$, akkor

$$\frac{\sigma(n!)}{n!}=\prod_{p\le n}\left(1+\frac{1}{p}+\frac{1}{p^2}+\ldots+\frac{1}{p^{\alpha_p}}\right)<\prod_{p\le n}\frac{p}{p-1}\le\prod_{2\le v\le n}\frac{v}{v-1}=n\,.$$

Innen $n! < \sigma(n!) < n \cdot n! < (n+1)!$, azaz $\sigma(n!) \neq k!$.

• **6.2.17 b)** Megmutatjuk, hogy $g(n)$ értéke csak 0 és ± 1 lehet.

Ha n nem négyzetmentes, akkor az összeg minden tagja 0, tehát $g(n) = 0$.

A továbbiakban tegyük fel, hogy n négyzetmentes.

Ha n az összes 100-nál kisebb prímmel osztható, akkor $g(n) = \mu(n) = \pm 1$.

Egyébként legyen S az összes olyan 100-nál kisebb prím szorzata, amelyek nem osztói n-nek. Ha $(n,k) \neq 1$ vagy k nem négyzetmentes, akkor $\mu(nk) = 0$, ezért

$$g(n) = \sum_{k|S} \mu(nk) = \sum_{k|S} \mu(n)\mu(k) = \mu(n) \sum_{k|S} \mu(k) = 0$$

(az utolsó lépésben a 6.2.4 Tételt használtuk).

• **6.3.5 a)** Ha $n = 2^{p-1}$, ahol $2^p - 1$ Mersenne-prím, akkor $\sigma(n) = 2^p - 1$ és $\sigma(\sigma(n)) = 2^p = 2n$.

A megfordításhoz tegyük fel, hogy n páros és szupertökéletes. Legyen $n = 2^k t$, ahol $k \geq 1$ és t páratlan.

Ekkor $\sigma(n) = (2^{k+1} - 1)\sigma(t)$, ahonnan $k \geq 1$ miatt következik, hogy $(2^{k+1} - 1)\sigma(t)$ és $\sigma(t)$ a $\sigma(n)$-nek két különböző osztója. Így

$$2^{k+1}t = 2n = \sigma(\sigma(n)) \geq (2^{k+1} - 1)\sigma(t) + \sigma(t) = 2^{k+1}\sigma(t)\,.$$

Ez csak úgy lehetséges, ha $\sigma(t) = t$, azaz $t = 1$, továbbá $\sigma(n)$-nek a megadott két számon kívül nincs más pozitív osztója, azaz $\sigma(n) = 2^{k+1} - 1$ prím.

• **b)** A 6.2.6a feladat szerint egy páratlan n pontosan akkor négyzetszám, ha $\sigma(n)$ páratlan. Így elég belátni, hogy egy páratlan n szupertökéletes szám esetén $\sigma(n)$ páratlan.

Tegyük fel indirekt, hogy n szupertökéletes és $\sigma(n) = 2^v w$, ahol w páratlan és $v \geq 1$. Ekkor

$$2n = \sigma(\sigma(n)) = (2^{v+1} - 1)\sigma(w)\,,$$

ahonnan alkalmas z-vel $\sigma(w) = 2z$ és $n = (2^{v+1} - 1)z$ következik. Innen $v \geq 1$ alapján azt kapjuk, hogy

$$\sigma(n) \geq (2^{v+1} - 1)z + z = 2^{v+1}z,$$

ugyanakkor

$$\sigma(n) = 2^v w < 2^v \sigma(w) = 2^{v+1}z,$$

ami ellentmondás. (A $w < \sigma(w)$ egyenlőtlenség abból adódott, hogy $\sigma(w) = 2z$ miatt $w \neq 1$.)

• **c)** Tegyük fel, hogy p^α szupertökéletes, ahol p páratlan prím. Legyen $\sigma(p^\alpha)$ kanonikus alakja $\prod_{j=1}^{s} q_j^{\beta_j}$, azaz

$$\sigma(p^\alpha) = 1 + p + \ldots + p^\alpha = \prod_{j=1}^{s} q_j^{\beta_j} \,. \tag{5}$$

Ekkor

$$2p^\alpha = \sigma(\sigma(p^\alpha)) = \prod_{j=1}^{s} \left(1 + q_j + \ldots + q_j^{\beta_j}\right). \tag{6}$$

A (6) jobb oldalán szereplő tényezők közül pontosan egy páros, legyen ez mondjuk az első tényező. Ez azt jelenti, hogy

$$1 + q_1 + \ldots + q_1^{\beta_1} = \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} = 2p^{\gamma_1}, \tag{7a}$$

továbbá

$$1 + q_j + \ldots + q_j^{\beta_j} = \frac{q_j^{\beta_j+1} - 1}{q_j - 1} = p^{\gamma_j} \,, \qquad j = 2, \ldots, s \,, \tag{7b}$$

ahol a γ_j kitevők alkalmas pozitív egészek. (A bizonyítás lépései az $s = 1$ esetben is helyesek lesznek.)

A (7a) és (7b) egyenlőségekből következik, hogy

$$q_j^{\beta_j+1} \equiv 1 \pmod{p} \,, \qquad j = 1, 2, \ldots, s \,. \tag{8}$$

(7a)-ból azt is kapjuk, hogy β_1 páratlan, és így $1 + q_1 + \ldots + q_1^{\beta_1}$-ből kiemelhető $1 + q_1$. Ennek alapján $1 + q_1 = 2p^\delta$ alakú, ezért

$$q_1 \equiv -1 \pmod{p} \,. \tag{9}$$

(7b) szerint $j \geq 2$ esetén a β_j kitevő páros, tehát

$$K = (\beta_2 + 1) \ldots (\beta_s + 1) \text{ páratlan.} \tag{10}$$

Szorozzuk be (5)-öt $q_1 \ldots q_s$-sel:

$$\prod_{j=1}^{s} q_j^{\beta_j+1} = q_1 q_2 \ldots q_s (1 + p + \ldots + p^\alpha) \,. \tag{11}$$

Tekintsük (11)-et modulo p, ekkor (8) és (9) felhasználásával $1 \equiv -q_2 \dots q_s \pmod{p}$, azaz

$$q_2 \dots q_s \equiv -1 \pmod{p} \tag{12}$$

adódik. Emeljük (12)-t a K-adik hatványra. Ekkor (10) alapján

$$(q_2 \dots q_s)^K \equiv -1 \pmod{p}\,. \tag{13}$$

Ugyanakkor $j \geq 2 \Rightarrow \beta_j + 1 \mid K$ és (8) felhasználásával azt kapjuk, hogy

$$(q_2 \dots q_s)^K \equiv 1 \pmod{p}\,,$$

ami ($p > 2$ miatt) ellentmond (13)-nak.

• **6.4.8 b)** Az útmutatásban vázolt gondolatmenetet követjük.

Legyen $\varepsilon > 0$ tetszőleges. Azt kell igazolni, hogy ha N elég nagy, akkor az $1, 2, \dots, N$ számok közül legfeljebb εN darab szerepel a φ-függvény értékkészletében.

Rögzítsük le az r pozitív egész értékét úgy, hogy

$$2^r > \frac{2}{\varepsilon}$$

teljesüljön.

A $\varphi(n)$ értékkészletét osszuk két csoportba: H_1-be tartozzanak a 2^r-rel osztható függvényértékek, H_2-be pedig azok, amelyek nem oszthatók 2^r-rel.

A H_1 halmaz N-nél nem nagyobb elemeinek a száma nyilván

$$\left\lfloor \frac{N}{2^r} \right\rfloor < \frac{\varepsilon N}{2}\,.$$

A feladat állításához így elég megmutatni, hogy elég nagy N esetén a H_2 halmaz N-nél nem nagyobb elemeinek a száma szintén legfeljebb $\varepsilon N/2$.

Ha $\omega(n) \geq r+1$, akkor $2^r \mid \varphi(n)$, tehát minden ilyen n esetén $\varphi(n) \in H_1$.

Így a továbbiakban elég az olyan n-eket vizsgálni, amelyekre $\omega(n) \leq r$. Ebben az esetben

$$\frac{\varphi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right) \tag{14}$$

nyilván akkor a legkisebb, ha az n kanonikus alakjában éppen az első r prímszám, $p_1, \dots, p_r$ szerepel. Ekkor (14)-et a

$$\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = c$$

jelölés segítségével

$$\varphi(n) \geq nc \tag{15}$$

alakba írhatjuk.

A (15) egyenlőtlenségből az következik, hogy ha $\varphi(n) \leq N$, akkor

$$n \leq \frac{\varphi(n)}{c} \leq \frac{N}{c}\,,$$

vagyis H_2-nek az N-nél nem nagyobb elemei csak a

$$\varphi(1),\ \varphi(2),\ \ldots,\ \varphi(N')$$

függvényértékek közül kerülhetnek ki, ahol $N' = \lfloor N/c \rfloor$.

A feladat a) része szerint létezik olyan n_0, hogy ha $N' > n_0$, akkor az $1, 2, \ldots, N'$ számok között legfeljebb

$$\frac{c\varepsilon N'}{2} \leq \frac{\varepsilon N}{2}$$

olyan van, amelyre $\varphi(n)$ nem osztható 2^r-rel, és így nyilván legfeljebb $\varepsilon N/2$ darab H_2-be tartozó $\varphi(n)$ érték keletkezhet.

• **6.6.12 a)** Mivel $d(n) = (1*1)(n)$, ezért a 6.6.4 Tétel szerint a $d(n)$ Dirichlet-sora $D(s) = \zeta^2(s)$, és így speciálisan $s = 2$-re

$$D(2) = \sum_{n=1}^{\infty} \frac{d(n)}{n^2} = \zeta^2(2) = \Big(\frac{\pi^2}{6}\Big)^2\,.$$

• **b)** Jelöljük a $d^2(n)$ függvény Dirichlet-sorát $T(s)$-sel. Mivel $d^2(n)$ multiplikatív, ezért a 6.6.10a feladat szerint

$$T(s) = \sum_{n=1}^{\infty} \frac{d^2(n)}{n^s} = \prod_p \Big(\sum_{k=0}^{\infty} \frac{d^2(p^k)}{p^{ks}}\Big) = \prod_p \Big(\sum_{k=0}^{\infty} \frac{(k+1)^2}{p^{ks}}\Big)\,. \tag{16}$$

Legyen

$$H(x) = \sum_{k=0}^{\infty} (k+1)^2 x^k\,, \tag{17}$$

ekkor (16) és (17) alapján

$$T(s)=\prod_p H\Big(\frac{1}{p^s}\Big)\,. \tag{18}$$

Feltesszük, hogy $s>1$, ekkor $p\ge 2$ miatt $H(x)$-et a $0<x<1/2$ tartományban vizsgáljuk. A $H(x)$ végtelen sorhoz úgy jutunk el, ha a

$$\sum_{j=0}^{\infty} x^j=\frac{1}{1-x}$$

végtelen mértani sort tagonként deriváljuk:

$$\sum_{j=1}^{\infty} jx^{j-1}=\frac{1}{(1-x)^2}\,,$$

az eredményt megszorozzuk x-szel:

$$\sum_{j=1}^{\infty} jx^{j}=\frac{x}{(1-x)^2}\,,$$

majd ismét tagonként deriválunk:

$$\sum_{j=1}^{\infty} j^2x^{j-1}=\frac{1+x}{(1-x)^3}\,. \tag{19}$$

A hatványsorok deriválásáról szóló tétel szerint az előbbi levezetésben szereplő lépések például $|x|\le 1/2$ esetén helyesek voltak, és így a fenti egyenlőségek igazak.

A $k=j-1$ helyettesítés mutatja, hogy (19) bal oldalán éppen $H(x)$ áll. A jobb oldalon szereplő tört számlálóját és nevezőjét $1-x$-szel bővítve így

$$H(x)=\frac{1-x^2}{(1-x)^4} \tag{20}$$

adódik. A (20)-at (18)-ba beírva azt nyerjük, hogy

$$T(s)=\prod_p \frac{1-\frac{1}{p^{2s}}}{\big(1-\frac{1}{p^s}\big)^4}=\frac{\zeta^4(s)}{\zeta(2s)}\,. \tag{21}$$

A (21) képletet $s = 2$-re alkalmazva kapjuk, hogy

$$T(2) = \sum_{n=1}^{\infty} \frac{d^2(n)}{n^2} = \frac{\zeta^4(2)}{\zeta(4)} = \frac{\left(\frac{\pi^2}{6}\right)^4}{\frac{\pi^4}{90}} = \frac{5\pi^4}{72}\,.$$

• **6.7.4** Az útmutatásban jelzett gondolatmenetet követjük.

Először megmutatjuk, hogy ha n elég nagy, akkor az $1, 2, \ldots, n$ számok között több, mint $n/2$ olyan i van, amelyre $\sigma(i) \leq 2n$. Legyen t azoknak az i értékeknek a száma, amelyekre ez nem teljesül, ekkor azt kell igazolni, hogy $t < n/2$. Erre a t darab „rossz" i-re a $\sigma(i) > 2n$, a többi i-re pedig a triviális $\sigma(i) > 0$ becslést alkalmazva azt kapjuk, hogy

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) > 2tn\,. \tag{22}$$

Másrészt a 6.7.3 Tétel szerint elég nagy esetén

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) < n^2\,. \tag{23}$$

A (22) és (23) egyenlőtlenségekből azonnal adódik, hogy valóban $t < n/2$.

Legyen most k tetszőleges. A 6.4.9 feladat alapján elég nagy n esetén az $1, 2, \ldots, 2n$ számok között legfeljebb

$$\frac{2n}{4k}$$

olyan j érték szerepel, amely benne van a σ-függvény értékkészletében. Mivel az előző bekezdés szerint több, mint $n/2$ olyan i van, amelyre a $\sigma(i)$ egy ilyen j függvényérték, ezért a skatulyaelv alapján kell lennie olyan j-nek, amelyet a σ-függvény legalább

$$\frac{n}{2} \;:\; \frac{2n}{4k} \;=\; k$$

helyen vesz fel.

7. Diofantikus egyenletek

• **7.1.4** Jelöljük a szóban forgó huszadik századi évszámot M-mel. Először megmutatjuk, hogy A és B nem születhettek mindketten 1899 után.

Indirekt tegyük fel, hogy mégis ez lenne a helyzet. Legyen A születési éve $\overline{19uv}$, B születési éve pedig $\overline{19xz}$ (nyilván egyikük sem születhetett 2000-ben). Ekkor a feltétel szerint

$$M = 1900 + 10u + v + 1 + 9 + u + v = 1910 + 11u + 2v = 1910 + 11x + 2z.$$

Ezt átrendezve $11(u-x) = 2(z-v)$ adódik, amiből kapjuk, hogy $11 \mid z-v$. Mivel $|z - v| \leq 9$, ezért csak $z - v = 0$ lehetséges. Ha azonban $z = v$, akkor $u = x$ is teljesül, ami ellentmondás, hiszen A és B különböző korúak.

Hasonlóan adódik, hogy A és B nem születhettek mindketten 1900 előtt: ha a születési évszámuk $\overline{18uv}$, illetve $\overline{18xz}$, akkor

$$M = 1800 + 10u + v + 1 + 8 + u + v = 1809 + 11u + 2v = 1809 + 11x + 2z$$

ugyanígy ellentmondásra vezet.

Ez azt jelenti, hogy (mondjuk) A születési évszáma $\overline{19uv}$, B-é pedig $\overline{18xz}$. Ekkor

$$M = 1910 + 11u + 2v = 1809 + 11x + 2z, \quad \text{vagyis} \quad 101 = 11(x-u) + 2(z-v).$$

Innen egyrészt $x - u$ páratlan, másrészt $z - v \leq 9$ miatt

$$x - u \geq \frac{101 - 18}{11} > 7,$$

vagyis csak $x - u = 9$ lehetséges. Ebből

$$x = 9, \quad u = 0 \quad \text{és} \quad z = v + 1 \quad (v = 0, 1, \ldots, 8),$$

és ezek az értékek (alkalmas M mellett) ki is elégítik a feladat feltételeit. Így a korkülönbség

$$\overline{19uv} - \overline{18xz} = (1900 + v) - (1890 + v + 1) = 9 \text{ év}.$$

• **7.3.8** Megmutatjuk, hogy a triviális $x = y = s = t = 0$ értékrendszeren kívül nincs más megoldás.

• *Első megoldás*: Tegyük fel indirekt, hogy létezik egy nemtriviális racionális megoldás. Ekkor a nevezők legkisebb közös többszörösével végigszorozva, majd szükség esetén az így adódó egész számok legnagyobb közös osztójával végigosztva olyan egész megoldáshoz jutunk, ahol $(x, y, s, t) = 1$.

Vizsgáljuk a számok paritását. A feltétel alapján

$$t^2+s^2+x^2 \equiv t^2+(s+x)^2=(y+t)^2+x^2 \equiv y^2+t^2+x^2 \pmod 2,$$

tehát s és y azonos paritású.

Ekkor az egyenletrendszert modulo 4 nézve azt kapjuk, ugyanilyen paritású t, $s+x$, $y+t$ és x is.

Mind a hat szám nem lehet páratlan, mert ha y és t páratlan, akkor $y+t$ páros.

Mind a hat szám páros sem lehet, hiszen $(x,y,s,t)=1$.

Ezzel ellentmondásra jutottunk.

• *Második megoldás*: Most is indirekt bizonyítunk. Az előző megoldáshoz hasonlóan feltehetjük, hogy ekkor létezik egy nemtriviális egész megoldás is. Ennél a szóban forgó négyzetösszegek értéke nem lehet nulla.

Tekintsük az egész koordinátájú négyzetrácsban a $(0,0)$, az (s,y) és az $(s+x,-t)$ koordinátájú rácspontokat. A feltétel éppen azt jelenti, hogy ezek egy szabályos háromszöget alkotnak.

Rácspontok azonban nem alkothatnak szabályos háromszöget, ugyanis az őket befoglaló rácstéglalap és a „sarokháromszögek" területe is nyilvánvalóan racionális, ugyanakkor a szabályos háromszög területe az oldala négyzetének $\sqrt{3}/4$-szerese, az oldal négyzete pedig (Pitagorasz tétele alapján) egész szám.

• **7.3.10** Legyen a 8 szám számtani közepe s. Ekkor $2s=t$, ahol t páratlan egész, továbbá a 8 szám köbének összege

$$\left(s-\frac{7}{2}\right)^3+\left(s-\frac{5}{2}\right)^3+\left(s-\frac{3}{2}\right)^3+\left(s-\frac{1}{2}\right)^3+\left(s+\frac{1}{2}\right)^3+\left(s+\frac{3}{2}\right)^3+$$
$$+\left(s+\frac{5}{2}\right)^3+\left(s+\frac{7}{2}\right)^3=8s^3+126s=t^3+63t\,.$$

Így a $t^3+63t=v^3$ egyenlet olyan megoldásait keressük, ahol v egész és t páratlan egész. Ha a (v,t) pár megoldás, akkor a $(-v,-t)$ pár is megoldás, ezért elég a $t>0$ megoldásokat keresnünk.

Nyilván $v>t$, továbbá $(t+5)^3>t^3+63t=v^3$, tehát $v<t+5$. Ennek alapján (figyelembe véve, hogy v szükségképpen páros) csak $v=t+1$ és $v=t+3$ lehetséges.

Az elsőből nem kapunk megoldást, a másodikból $t=1$ és $t=3$ adódik. A keresett köbszámok ennek megfelelően $64=4^3, 216=6^3, -64=(-4)^3$ és $-216=(-6)^3$.

• **7.3.13 g)** Az $x = \pm 1$, $y = 0$ értékek nyilván kielégítik az egyenletet. Megmutatjuk, hogy más egész megoldás nincs.

Indirekt bizonyítunk. Nyilván feltehetjük, hogy $x > 1$.

Az egyenletet $(x+1)(x-1) = 2y^4$ alakba írva látszik, hogy x páratlansága miatt $x+1$ és $x-1$ páros, ezért y is az, $y = 2u$. Az egyenlet mindkét oldalát 4-gyel osztva

$$\frac{x+1}{2} \cdot \frac{x-1}{2} = 8u^4 \tag{1}$$

adódik. Az (1) bal oldalán két szomszédos pozitív egész szám szorzata áll, ezért a tényezők relatív prímek is. Így egyikük egy negyedik hatvány, a másik pedig egy negyedik hatvány 8-szorosa. Mivel a két szám eltérése 1, tehát

$$w^4 - 8z^4 = 1 \qquad \text{vagy} \qquad w^4 - 8z^4 = -1.$$

Az utóbbi eset nem lehetséges, mert egy négyzetszám nem adhat -1 maradékot 8-cal osztva. Az első esetben átrendezés és szorzattá bontás után a $(w^2+1)(w^2-1) = 8z^4$, azaz a

$$\frac{w^2+1}{2}(w^2-1) = (2z^2)^2 \tag{2}$$

összefüggéshez jutunk.

Megmutatjuk, hogy a (2) bal oldalán álló két (pozitív) tényező relatív prím. Jelölje a legnagyobb közös osztójukat d. Mivel $(w^2+1)/2$ páratlan, ezért d is csak páratlan lehet. Továbbá

$$d \mid 2\frac{w^2+1}{2} - (w^2-1) = 2,$$

tehát valóban $d = 1$.

Ez azt jelenti, hogy $(w^2+1)/2$ és w^2-1 külön-külön is négyzetszámok. Két pozitív négyzetszám különbsége azonban nem lehet 1, tehát w^2-1 nem lehet négyzetszám, és így ellentmondásra jutottunk.

• **h)** Megmutatjuk, hogy az összes megoldás: $x = y$, valamint $x = 2, y = 4$ és $x = 4$, $y = 2$.

Ezek nyilván megoldások. Így azt kell igazolni, hogy $y > x$ esetén $x = 2$ és $y = 4$.

• *Első bizonyítás*: Legyen $(x, y) = d$, ekkor $x = da$, $y = db$, ahol $(a, b) = 1$. Ezt az egyenletbe visszaírva, majd d-edik gyököt vonva

$$(da)^b = (db)^a, \qquad \text{azaz } b > a \text{ miatt} \qquad d^{b-a}a^b = b^a \tag{3}$$

adódik. Innen kapjuk, hogy $a \mid b^a$, de ez $(a,b)=1$ miatt csak $a=1$ esetén lehetséges. Ekkor (3) a

$$d^{b-1} = b \tag{4}$$

egyenletet jelenti. Itt $b > a = 1$, és így $d > 1$. Ha $d > 2$, akkor bármely $b > 1$-re $d^{b-1} > b$, és $d = 2$ esetén is csak úgy teljesülhet (4), ha $b = 2$. Innen valóban a kívánt

$$x = da = 2 \cdot 1 = 2 \qquad \text{és} \qquad y = db = 2 \cdot 2 = 4$$

értékeket kapjuk.

• *Második bizonyítás*: Ha $y > x > 1$, akkor az egyenlet ekvivalens az

$$\frac{x}{\log x} = \frac{y}{\log y}$$

egyenlettel. Mivel az $f(z) = z/\log z$ függvény az $1 < z < e$ intervallumban szigorúan monoton fogy, és $z > e$-re szigorúan monoton nő, így két különböző egész helyen csak akkor vehet fel azonos értéket, ha a kisebbik hely a 2. Ez azt jelenti, hogy csak $x = 2$ lehetséges. Ekkor $y = 4$ megfelel, továbbá az f függvény $z > e$-re szigorúan monoton, ezért más y már nem lehet jó.

• **i)** Az $x = 5$, $y = 1$ értékek nyilván megfelelnek. Megmutatjuk, hogy más megoldás nincs.

Az egyenlet fennállása esetén az

$$y^5 \equiv 2^x \pmod{31} \tag{5}$$

kongruenciának is teljesülnie kell. Mivel az eredeti egyenletből nyilvánvaló, hogy $31 \nmid y$, ezért (5) miatt a 2^x szükségképpen ötödik hatványmaradék modulo 31. Ekkor a 3.5.3 Tétel szerint

$$(2^x)^{\frac{30}{(5,30)}} = 2^{6x} \equiv 1 \pmod{31}. \tag{6}$$

A (6)-ból következik, hogy

$$o_{31}(2) = 5 \mid 6x, \qquad \text{ezért} \qquad 5 \mid x, \qquad \text{azaz} \qquad x = 5u\,.$$

Ezt az eredeti egyenletbe visszaírva azt kapjuk, hogy

$$(2^u)^5 - y^5 = 31, \tag{7}$$

tehát két (pozitív) ötödik hatvány különbsége 31. Azt, hogy (7) egyedül a $2^5 - 1^5$ esetben valósulhat meg, ahhoz hasonlóan igazolhatjuk, ahogyan a II. módszer példájának megoldása során az $a^3 - b^3 = 7$ egyenletet kezeltük: vagy azt használjuk fel, hogy minden más esetben két pozitív ötödik hatvány különbsége nagyobb, mint 31, vagy pedig a (7) bal oldalát szorzattá bontva bizonyítunk.

• **7.5.10** Az egyenlet bal oldalát bontsuk szorzattá: $(x + 2i)(x - 2i) = y^3$. Legyen $\delta = (x + 2i, x - 2i)$, ekkor

$$\delta \mid (x + 2i) - (x - 2i) = 4i = (-i)(1 + i)^4.$$

Ebből következik, hogy $\delta = (1 + i)^r$, ahol $0 \le r \le 4$.

A konjugálás tulajdonságaiból adódik (lásd a 7.4.2a feladatot), hogy

$$(1 + i)^s \mid x + 2i \iff (1 - i)^s \mid x - 2i\,. \tag{8}$$

Az $1 + i$ és $1 - i$ egymás egységszeresei, ezért (8)-ból következik, hogy az $1 + i$ kitevője $x + 2i$ és $x - 2i$ kanonikus alakjában egyaránt r. Az $(x + 2i)(x - 2i)$ szorzat (a Gauss-egészek körében is) köbszám, tehát a kanonikus alakjában minden Gauss-prím, így az $1 + i$ kitevője is osztható 3-mal. Ez azt jelenti, hogy $3 \mid 2r$, tehát $r = 3t$ (azaz $r = 0$ vagy 3).

A fentiek alapján

$$\frac{x + 2i}{(1 + i)^{3t}} \cdot \frac{x - 2i}{(1 - i)^{3t}} = \left(\frac{y}{2^t}\right)^3 \qquad \text{és} \qquad \left(\frac{x + 2i}{(1 + i)^{3t}}\,,\, \frac{x - 2i}{(1 - i)^{3t}}\right) = 1\,.$$

Innen a számelmélet alaptételéből következik, hogy $x + 2i$ és $x - 2i$ is „köbszámok" egységszeresei, és mivel a Gauss-egészek körében minden egység köbszám, így $x + 2i$ és $x - 2i$ maguk is köbszámok.

Ekkor

$$x + 2i = (c + di)^3 = c^3 - 3cd^2 + (3c^2d - d^3)i\,. \tag{9}$$

A képzetes részeket összehasonlítva $2 = d(3c^2 - d^2)$ adódik. Innen $d = \pm 1$ vagy ± 2, és ezeket visszahelyettesítve csak a $d = 1$ és $d = -2$ esetben kapunk c-re egész értéket, mindkétszer $c = \pm 1$.

Végül (9)-ből $x = c^3 - 3cd^2$, ahonnan az $x = \pm 2$, $y = 2$ és $x = \pm 11$, $y = 5$ megoldásokat nyerjük.

• **7.5.11** A $\xi^2 + \psi^2 = \alpha$ egyenletet vizsgáljuk, ahol α adott Gauss-egész, és ξ és ψ az „ismeretlen" Gauss-egészek.

Az egyenlet bal oldalát szorzattá bontva $(\xi+\psi i)(\xi-\psi i)=\alpha$ adódik, tehát

$$\xi+\psi i=\delta_1,\quad \xi-\psi i=\delta_2,\quad \text{ahol}\quad \delta_1\delta_2=\alpha.$$

Innen

$$\xi=\frac{\delta_1+\delta_2}{2},\qquad \psi=\frac{\delta_1-\delta_2}{2i}\,.$$

Mivel i egység, továbbá $\delta_1+\delta_2=(\delta_1-\delta_2)+2\delta_2$, ezért ξ és ψ pontosan akkor lesznek Gauss-egészek, ha

$$2\mid\delta_1-\delta_2\,. \tag{10}$$

Legyen $\alpha=a+bi$.

Először azokat az eseteket tekintjük, amikor alkalmas δ_1, δ_2 osztópárra (10) teljesül (tehát α felírható $\xi^2+\psi^2$ alakban).

Ha a páratlan és b páros, akkor a $\delta_1=\alpha, \delta_2=1$ választás kielégíti (10)-et: $2\mid(a-1)+bi$.

Ha $4\mid a$ és $4\mid b$, akkor a $\delta_1=\alpha/2, \delta_2=2$ választás megfelel, hiszen ekkor δ_1 és δ_2 külön-külön is oszthatók 2-vel.

Ha a és b párosak, és közülük pontosan az egyik osztható 4-gyel, akkor α kanonikus alakjában az $1+i$ Gauss-prím pontosan a második hatványon szerepel, tehát

$$\alpha=(1+i)^2(c+di),\quad \text{ahol}\quad 1+i\nmid c+di,\quad \text{azaz}\quad c\not\equiv d\pmod 2\,.$$

Ekkor a

$$\delta_1=\frac{\alpha}{1+i}=(c+di)(1+i),\qquad \delta_2=1+i$$

választás megfelelő. Ugyanis

$$\delta_1-\delta_2=(1+i)((c-1)+di)\,,$$

továbbá

$$c-1\equiv d\pmod 2\Longrightarrow 1+i\mid c-1+di,$$

tehát $\delta_1-\delta_2$ osztható $(-i)(1+i)^2=2$-vel.

Most megmutatjuk, hogy a többi esetben α nem áll elő $\xi^2+\psi^2$ alakban.

Ha $a\equiv b\equiv 2\pmod 4$, akkor α kanonikus alakjában az $1+i$ Gauss-prím pontosan a harmadik hatványon szerepel. Ez azt jelenti, hogy bármely δ_1, δ_2 osztópárnak pontosan az egyik eleme osztható $(-i)(1+i)^2=2$-vel, tehát (10) nem teljesülhet.

Végül, ha b páratlan, akkor $a+bi\neq(x_1+x_2i)^2+(y_1+y_2i)^2$, ugyanis a jobb oldal képzetes része páros, míg a bal oldalé páratlan.

Összefoglalva, azt láttuk be, hogy $\alpha = a + bi$ akkor és csak akkor *nem* írható fel $\xi^2 + \psi^2$ alakban, ha b páratlan, vagy $a \equiv b \equiv 2 \pmod 4$.

• **7.5.17** Azt igazoljuk, hogy n pontosan akkor áll elő a kívánt alakban, ha $2n$ felírható három négyzetszám összegeként. Ebből a három-négyzetszám-tétel alapján következik, hogy azok az n értékek „rosszak", amelyekre

$$2n = 4^{k+1}(8m + 7), \qquad \text{azaz} \qquad n = 4^k(16m + 14)\,.$$

Ha n előáll az előírt alakban, azaz $n = 2x^2 + y^2 + z^2$, akkor

$$2n = (2x)^2 + (y + z)^2 + (y - z)^2\,.$$

Megfordítva, ha $2n = a^2 + b^2 + c^2$, akkor feltehető, hogy a páros és b és c azonos paritású, és ekkor

$$n = 2\Big(\frac{a}{2}\Big)^2 + \Big(\frac{b+c}{2}\Big)^2 + \Big(\frac{b-c}{2}\Big)^2\,.$$

• **7.5.5 b)** A végtelen leszállás módszerét alkalmazzuk. Tegyük fel indirekt, hogy az

$$x^4 + y^4 = z^2 \tag{11}$$

diofantikus egyenletnek létezik pozitív egész megoldása (megoldáson a továbbiakban mindig csak pozitív egész megoldást fogunk érteni), és tekintsük azt az $x_0,\ y_0,\ z_0$ megoldást, ahol z_0 minimális. Megmutatjuk, hogy létezik egy olyan $x_1,\ y_1,\ z_1$ megoldás, amelyre $z_1 < z_0$, és ez ellentmond z_0 minimalitásának.

Ha $(x_0, y_0, z_0) = d > 1$, akkor

$$\frac{x_0}{d}\,, \qquad \frac{y_0}{d}\,, \qquad \frac{z_0}{d^2}$$

is kielégíti (11)-et, és $z_0/d^2 < z_0$ ellentmond z_0 minimalitásának.

Ebből következik, hogy $x_0,\ y_0$ és z_0 relatív prímek, és a szokásos módon igazolható, hogy páronként is relatív prímek.

A fentiek alapján $x_0^2,\ y_0^2$ és z_0 primitív pitagoraszi számhármast alkotnak. Ezért

$$x_0^2 = 2mn \tag{12a}$$
$$y_0^2 = m^2 - n^2 \tag{12b}$$
$$z_0 = m^2 + n^2 \tag{12c}$$

ahol

$$m > n > 0, \qquad (m, n) = 1 \qquad \text{és} \qquad m \not\equiv n \pmod 2 .$$

A (12b) egyenletet modulo 4 vizsgálva kapjuk, hogy az m és n közül most m a páratlan és n a páros; $n = 2n_1$. Ezt (12a)-ba beírva kapjuk, hogy

$$\left(\frac{x_0}{2}\right)^2 = mn_1, \qquad \text{ahol} \qquad (m, n_1) = 1.$$

Ebből következik, hogy

$$m = u^2 \qquad \text{és} \qquad n_1 = v^2 , \qquad \text{ahol} \qquad (u, v) = 1. \tag{13}$$

A (13)-at (12b)-be beírva kapjuk, hogy

$$y_0^2 = (u^2)^2 - (2v^2)^2 ,$$

azaz y_0, $2v^2$ és u^2 primitív pitagoraszi számhármast alkot. Ebből következik, hogy

$$2v^2 = 2rs \tag{14a}$$

$$u^2 = r^2 + s^2 \tag{14b}$$

ahol $(r, s) = 1$. A (14a)-ból így azt nyerjük, hogy $r = t^2$, $s = w^2$, és ekkor (14b) átírható az

$$u^2 = t^4 + w^4$$

alakba. Ez azt jelenti, hogy $x_1 = t, y_1 = w$, $z_1 = u$ megoldása (11)-nek, továbbá (12c) és (13) alapján

$$z_0 = m^2 + n^2 > m = u^2 \geq u = z_1,$$

ami ellentmond z_0 minimalitásának.

• **7.7.7** Legyen a számrendszer alapszáma x. Ekkor az

$$x^3 + x^2 + x + 1 = y^2 \tag{15}$$

diofantikus egyenlet olyan megoldásait keressük, ahol $x \geq 2$. Bebizonyítjuk, hogy az egyetlen ilyen megoldás $x = 7$, $y = 20$. (Könnyen látható, hogy $x \leq 1$ esetén csak az $x = 0$ és ± 1 értékekből kapunk egész megoldást.)

A (15) bal oldalát szorzattá bontva

$$(x+1)(x^2+1) = y^2 \tag{16}$$

adódik. Jelöljük a (16) bal oldalán szereplő két tényező legnagyobb közös osztóját h-val, ekkor

$$h \mid (x^2+1) - (x+1)(x-1) = 2, \qquad \text{tehát} \qquad h = 1 \text{ vagy } 2.$$

Ha $h = 1$, akkor x^2+1 (és $x+1$ is) négyzetszám: $x^2+1 = z^2$. Ez azonban ($x \neq 0$ miatt) lehetetlen.

A $h = 2$ esetben

$$x + 1 = 2u^2 \qquad \text{és} \qquad x^2 + 1 = 2v^2 \qquad (u > 1,\ v > 1). \tag{17}$$

Az első egyenletből $x = 2u^2 - 1$, ezt a második egyenletbe beírva kapjuk, hogy

$$(2u^2 - 1)^2 + 1 = 2v^2\,. \tag{18}$$

(18)-ból átrendezés és 2-vel való osztás után

$$(u^2)^2 + (u^2 - 1)^2 = v^2 \tag{19}$$

adódik. A (19) egyenletből $u > 1$, $v > 0$ és $(u^2, u^2 - 1) = 1$ alapján következik, hogy

$$u^2, \quad u^2 - 1 \quad \text{és} \quad v$$

primitív pitagoraszi számhármast alkotnak. Innen azt nyerjük, hogy (a „szokásos" tulajdonságú alkalmas m és n egészekkel) vagy

$$u^2 = m^2 - n^2 \tag{20a}$$

és

$$u^2 - 1 = 2mn, \tag{20b}$$

vagy pedig fordított szereposztással

$$u^2 = 2mn \tag{21a}$$

és

$$u^2 - 1 = m^2 - n^2 \tag{21b}$$

teljesül.

Nézzük először a (20a)–(20b) esetet. A (20a) egyenlet és $(m,n)=1$ alapján u, n és m primitív pitagoraszi számhármas. Mivel a feltételek szerint u páratlan, ezért

$$u=r^2-s^2, \qquad n=2rs \qquad \text{és} \qquad m=r^2+s^2.$$

Ebből következik, hogy

$$m-n=(r-s)^2. \tag{22}$$

A (20a) egyenletből (20b)-t kivonva

$$m^2-n^2-2mn=1, \qquad \text{azaz} \qquad (m-n)^2-2n^2=1 \tag{23}$$

adódik. (22) alapján (23) átírható a következő alakba:

$$(r-s)^4-1=2n^2\,. \tag{24}$$

Bontsuk (24) bal oldalát szorzattá:

$$\big((r-s)^2+1\big)\big((r-s)^2-1\big)=2n^2\,. \tag{25}$$

A (25) bal oldalán a két tényező különbsége 2, mindkét tényező páros, így a legnagyobb közös osztójuk 2. Mivel egy páratlan szám négyzete 4-gyel osztva 1 maradékot ad, ezért az első tényező (páros, de) 4-gyel már nem osztható. Mindebből következik, hogy

$$(r-s)^2+1=2t^2 \qquad \text{és} \qquad (r-s)^2-1=w^2\,.$$

Ez utóbbi azonban ($w\neq 0$ miatt) lehetetlen. Ezzel beláttuk, hogy a (20a)–(20b) eset nem valósulhat meg.

Rátérve a (21a)–(21b) esetre, most u páros, és így (21b) modulo 4 vizsgálatából kapjuk, hogy szükségképpen m páros és n páratlan. Mivel $(m,n)=$ $=1$, ezért (21a)-ból következik, hogy

$$m=2a^2, \qquad n=b^2, \qquad \text{és így} \qquad u^2=4a^2b^2. \tag{26}$$

A (26)-ot (21b)-be beírva a

$$4a^2b^2-1=4a^4-b^4$$

egyenlethez jutunk, amelyből átrendezés után

$$(2a^2+b^2)^2-1=8a^4 \tag{27}$$

adódik. A (27) bal oldalát szorzattá bontva a két tényező páros és különbségük 2, tehát a legnagyobb közös osztójuk 2. Így az alábbi két lehetőség van:

$$2a^2+b^2+1=2c^4 \qquad \text{és} \qquad 2a^2+b^2-1=4d^4\,, \tag{28}$$

vagy

$$2a^2+b^2+1=4d^4 \qquad \text{és} \qquad 2a^2+b^2-1=2c^4\,. \tag{29}$$

A (28)-beli két egyenletet egymásból kivonva 2-vel való osztás után

$$c^4-2d^4=1$$

adódik. A 7.3.13g feladat szerint ebből $d=0$ következik, ami most nem lehetséges.

(29)-ből hasonló módon a

$$c^4-2d^4=-1$$

egyenletet kapjuk. A 7.7.6 feladat szerint ekkor $c=\pm1$, $d=\pm1$. Ezt (29)-be visszaírva kapjuk, hogy $2a^2+b^2=3$, ahonnan $a^2=b^2=1$. Így (26) alapján $u^2=4$, és végül (17) miatt $x=7$.

• **7.7.10 a)** Tegyük fel először, hogy az

$$x^2+3y^2=n \tag{30}$$

diofantikus egyenlet megoldható, legyen $x=a$, $y=b$ egy megoldás. Ekkor

$$\begin{aligned} n=a^2+3b^2=a^2+(bi\sqrt{3})^2=N(a+bi\sqrt{3})=N(a+b(1+2\omega))=\\ =N(a+b+2b\omega)=(a+b)^2-(a+b)2b+(2b)^2\,, \end{aligned}$$

tehát $x=a+b$, $y=2b$ megoldása az

$$x^2-xy+y^2=n \tag{31}$$

diofantikus egyenletnek.

Legyen most $x=c$, $y=d$ megoldása (31)-nek. Ha van olyan a, b egész szám, amelyre

$$c=a+b \qquad \text{és} \qquad d=2b, \tag{32}$$

akkor az előző gondolatmenet megfordításával kapjuk, hogy $x=a$, $y=b$ megoldása (30)-nak. (32) pontosan akkor teljesül, ha d páros. Mivel az

$n = x^2 - xy + y^2$ egyenlet x-ben és y-ban szimmetrikus, ezért az is megfelel, ha c páros. Végül, ha c és d is páratlan, akkor

$$n = c^2 - cd + d^2 = N(c + d\omega) = N(c + d\omega^2) = \\ = N(c - d - d\omega) = (c - d)^2 - (c - d)(-d) + (-d)^2 ,$$

tehát $x = c - d$, $y = -d$ is megoldása (31)-nek, és itt $c - d$ már páros.

Természetesen a fentieket az Euler-egészek felhasználása nélkül, „trükkös" átalakítások formájában is el lehet mondani.

• **7.7.11** A 7.5.10 feladat megoldásának gondolatmenetét követjük. Az

$$x^2 + 243 = y^3 \tag{33}$$

egyenlet bal oldalát az Euler-egészek körében szorzattá bonthatjuk:

$$(x + 9i\sqrt{3})(x - 9i\sqrt{3}) = y^3 . \tag{34}$$

Legyen

$$\alpha = x + 9i\sqrt{3} = x + 9 + 18\omega, \quad \text{ekkor} \quad \overline{\alpha} = x - 9i\sqrt{3} .$$

Belátjuk, hogy α és $\overline{\alpha}$ relatív prímek, így szükségképpen egy-egy köbszám egységszeresei (köbszámokon most Euler-egészek köbét értjük).

Legyen $\delta = (\alpha, \overline{\alpha})$, ekkor

$$\delta \mid \alpha - \overline{\alpha} = 18i\sqrt{3} = 2(i\sqrt{3})^5 .$$

A (33) egyenlet modulo 8 vizsgálatából adódik, hogy x szükségképpen páros, tehát $2 \nmid x + 9$, és így $2 \nmid \alpha$. Ebből következik, hogy a 2 Euler-prím nem osztója δ-nak.

Ha $i\sqrt{5} \mid x + 9$, akkor $i\sqrt{3} \mid x$, tehát $3 \mid x$, és ezért $3 \mid y$. Legyen s és t a 3 kitevője x és y kanonikus alakjában. Ekkor (33) bal oldalán a 3 kitevője $\min(2s, 5)$, a jobb oldalon pedig $3t$, amelyek nem lehetnek egyenlők.

Ezzel igazoltuk, hogy $\delta = 1$, tehát α és $\overline{\alpha}$ egy-egy köbszám egységszeresei. (Az egységtényező nem hagyható el, mert az Euler-egészek körében nem minden egység köbszám.)

Ekkor

$$\alpha = x + 9 + 18\omega = \varepsilon(c + d\omega)^3 . \tag{35}$$

Mivel a -1 köbszám, ezért (35)-öt elég az $\varepsilon = 1$, ω és ω^2 esetekben megvizsgálni.

A $\varepsilon = 1$ esetben $\omega^3 = 1$ és $\omega^2 = -1 - \omega$ figyelembevételével kapjuk, hogy

$$(c + d\omega)^3 = c^3 + 3c^2 d\omega + 3cd^2\omega^2 + d^3\omega^3 = c^3 + d^3 - 3cd^2 + (3c^2 d - 3cd^2)\omega.$$

Ekkor (35)-ben az „ω-mentes rész", illetve ω együtthatóit összehasonlítva

$$x + 9 = c^3 + d^3 - 3cd^2 \tag{36a}$$

$$18 = 3c^2 d - 3cd^2 \tag{36b}$$

adódik. (36b) ekvivalens a $cd(c - d) = 6$ diofantikus egyenlettel, amelynek az alábbi (c, d) számpárok a megoldásai:

$$(3, 2); \qquad (3, 1); \qquad (-1, 2); \qquad (-1, -3); \qquad (-2, 1); \qquad (-2, -3).$$

Ezeket (36a)-ba behelyettesítve az $x = \pm 10$ értékeket kapjuk, és ekkor (33) szerint $y = 7$.

Az $\varepsilon = \omega$ esetben teljesen hasonlóan (36b) helyett a

$$18 = c^3 + d^3 - 3c^2 d \tag{37}$$

diofantikus egyenlethez jutunk. Ha c és d közül legalább az egyik páratlan, akkor (37) jobb oldala páratlan, ami nem lehet. Ha c és d mindketten párosak, akkor pedig a jobb oldal osztható 8-cal, ami szintén lehetetlen. Tehát (37)-nek nincs megoldása.

Végül az $\varepsilon = \omega^2$ eset (37) helyett a

$$18 = -c^3 - d^3 + 3cd^2$$

diofantikus egyenletre vezet, amelyről az előzővel egyező módon látható be, hogy nincs megoldása.

Összefoglalva, azt kaptuk, hogy az $x^2 + 243 = y^3$ diofantikus egyenlet összes megoldása: $x = \pm 10$, $y = 7$.

8. Diofantikus approximáció

• **8.1.8 c)** Megmutatjuk, hogy egy ϱ valós szám akkor és csak akkor írható fel $h(\alpha) = \{\alpha\}^2 - \{\alpha^2\}$ alakban, ha $-1 < \varrho < 1$.

A szükségesség azonnal adódik abból, hogy bármely c-re $0 \le \{c\} < 1$.

Az elégségességhez legyen $0 \le \vartheta < 1$, k pozitív egész és $\alpha = k + \vartheta$. Ekkor

$$\{\alpha\}^2 = \vartheta^2 \qquad \text{és} \qquad \{\alpha^2\} = \{\vartheta^2 + 2k\vartheta\}. \tag{1}$$

Ha

$$0 \le \vartheta^2 + 2k\vartheta < 1, \qquad \text{azaz} \qquad 0 \le \vartheta < -k + \sqrt{k^2+1}, \tag{2}$$

akkor (1) alapján

$$h(\alpha) = \{\alpha\}^2 - \{\alpha^2\} = \vartheta^2 - \{\vartheta^2 + 2k\vartheta\} = \vartheta^2 - (\vartheta^2 + 2k\vartheta) = -2k\vartheta. \tag{3}$$

Figyelembe véve (2)-t

$$0 \ge -2k\vartheta > -2k(-k + \sqrt{k^2+1}) \tag{4}$$

adódik. Ekkor (3) és (4) alapján a $h(\alpha) = -2k\vartheta$ értékek között a

$$\left(-2k(-k + \sqrt{k^2+1})\,,\ 0\right]$$

intervallum minden pontja előfordul. Mivel

$$-2k(-k + \sqrt{k^2+1}) = \frac{-2k}{k + \sqrt{k^2+1}} = \frac{-2}{1 + \sqrt{1+k^{-2}}} \to -1, \qquad \text{ha} \qquad k \to \infty,$$

ezért a $h(\alpha)$ értékek a teljes $(-1, 0]$ intervallumot kiadják.

Ha az előző gondolatmenetet (2) helyett a

$$2k \le \vartheta^2 + 2k\vartheta < 2k + 1, \qquad \text{azaz} \qquad -k + \sqrt{k^2+2k} \le \vartheta < 1$$

feltételt kielégítő ϑ-kra megismételjük, akkor azt kapjuk, hogy a $h(\alpha)$ értékek között a $[0, 1)$ intervalum minden eleme is fellép.

• **8.3.5** A 8.3.4 Lemma (8a), (8b) és (10) képletei alapján

$$\begin{aligned} r_n s_{n-2} - r_{n-2} s_n &= (c_n r_{n-1} + r_{n-2}) s_{n-2} - r_{n-2}(c_n s_{n-1} + s_{n-2}) = \\ &= c_n (r_{n-1} s_{n-2} - r_{n-2} s_{n-1}) = (-1)^n c_n\,. \end{aligned}$$

Ezt $s_n s_{n-2}$-vel osztva a feladat állítását kapjuk.

• **8.3.6** A feltétel szerint

$$\alpha = L(c_0, c_1, \ldots, c_{M-k}, c_{M-k+1}, \ldots, c_M, c_{M-k+1}, \ldots, c_M, \ldots)\,.$$

Legyen

$$\beta = L(c_{M-k+1}, \dots, c_M, c_{M-k+1}, \dots, c_M, \dots)\,.$$

Ekkor

$$\alpha = L(c_0, c_1, \dots, c_{M-k}, \beta) \qquad \text{és} \qquad \beta = L(c_{M-k+1}, \dots, c_M, \beta)\,.$$

Ezeket az „emeletes törteket kifejtve”

$$\alpha = \frac{u_1\beta + u_2}{u_3\beta + u_4}\,, \qquad \text{illetve} \qquad \beta = \frac{u_5\beta + u_6}{u_7\beta + u_8}$$

adódik, ahol az u_i-k alkalmas egész számok. Az első egyenlőségből fejezzük ki β-t α segítségével, és ezt helyettesítsük be a második egyenlőségbe. Ekkor átrendezés után egy olyan egész együtthatós másodfokú egyenlethez jutunk, amelynek az α gyöke. (Mivel végtelen lánctörtről van szó, ezért az α irracionális, és így elsőfokú egész együtthatós egyenletnek nem lehet gyöke.)

• **8.4.1 a)** Mivel $(1+\sqrt{2})^n + (1-\sqrt{2})^n$ egész szám és $\lim_{n\to\infty}(1-\sqrt{2})^n = 0$, ezért páros n-re az $\{(1+\sqrt{2})^n\}$ törtrészek (rész)sorozata 1-hez, páratlan n-re pedig 0-hoz tart, és így nem lehet mindenütt sűrű $[0,1]$-ben.

• **b)** A sorozat szomszédos elemeinek a különbsége 0-hoz tart:

$$\sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1}+\sqrt{n}} \to 0, \quad \text{ha} \quad n \to \infty\,.$$

Ezért a szomszédos elemek törtrészeinek a különbsége is 0-hoz tart, kivéve, amikor a törtrész „visszaugrik” az 1 közeléből a 0 közelébe. Ebből következik, hogy a törtrészek mindenütt sűrűek $[0,1]$-ben.

• **c)** Mivel

$$\{\sqrt{n^2+1}\} = \sqrt{n^2+1} - n = \frac{1}{\sqrt{n^2+1}+n} \to 0, \quad \text{ha} \quad n \to \infty\,,$$

ezért $\left\{\sqrt{n^2+1}\,\right\}$ nem lehet mindenütt sűrű $[0,1]$-ben.

• **d)** Mivel

$$\sqrt{2n^2+1} - n\sqrt{2} \to 0, \quad \text{ha} \quad n \to \infty\,,$$

és $\left\{n\sqrt{2}\,\right\}$ a 8.4.1 Tétel szerint mindenütt sűrű $[0,1]$-ben, ezért $\left\{\sqrt{2n^2+1}\,\right\}$ is mindenütt sűrű $[0,1]$-ben.

• **e)** A szinuszfüggvény periodikussága miatt a sorozat csak véges sok (181) különböző értéket vesz fel, ezért a törtrészek sorozata nem lehet mindenütt sűrű $[0,1]$-ben.

• **f)** Mivel π irracionalitása miatt az $1/(2\pi)$ arány is irracionális, ezért az (ívmértékben mért) n szögek a 8.4.1 Tétel szerint mindenütt sűrűn helyezkednek el az egységkörön. A szinuszfüggvény folytonossága miatt ezért a $\sin n$ értékek is mindenütt sűrűek a szinuszfüggvény $[-1,1]$ értékkészletében, és így a törtrészek mindenütt sűrűek $[0,1]$-ben.

• **g)** Mivel

$$\lg(n+1) - \lg n = \lg\bigl(1+\frac{1}{n}\bigr) \to 0, \quad \text{ha} \quad n \to \infty\,,$$

ezért a b) résznél adott indoklás szerint a törtrészek sorozata mindenütt sűrű $[0,1]$-ben.

• **8.4.3** Induljunk ki abból, hogy a $P_n = (\{n\alpha_1\}, \{n\alpha_2\}, \ldots, \{n\alpha_k\})$ pontok mindenütt sűrűek, vagyis a k-dimenziós egységkocka bármely $(v_1, \ldots, v_k)$ pontjának tetszőleges kicsi környezetében található egy P_n pont. Ez azt jelenti, hogy bármely $\varepsilon > 0$-hoz létezik olyan n, hogy

$$|\{n\alpha_j\} - v_j| < \varepsilon, \qquad j = 1, 2, \ldots, k,$$

vagyis alkalmas r_j egészekre

$$|n\alpha_j - v_j - r_j| < \varepsilon, \qquad j = 1, 2, \ldots, k. \tag{5}$$

Azt kell igazolnunk, hogy az $1, \alpha_1, \ldots, \alpha_k$ számok lineárisan függetlenek. Indirekt bizonyítunk: feltesszük, hogy léteznek olyan nem csupa nulla $c_0, \ldots, c_k$ racionális számok, amelyekre

$$c_0 + c_1\alpha_1 + \ldots + c_k\alpha_k = 0. \tag{6}$$

A (6) egyenlőséget a c_j-k nevezőinek legkisebb közös többszörösével beszorozva elérhető, hogy (6) egész c_j-kkel is teljesüljön.

A megoldás kulcsa az, hogy az (5) alapján „kicsi" abszolút értékű $n\alpha_j - v_j - r_j$ számoknak és $0 = n \cdot 1 - n$-nek a $c_1, \ldots, c_k, c_0$ számokkal vett lineáris kombinációja is kicsi abszolút értékű lesz:

$$|c_0(n \cdot 1 - n) + \sum_{j=1}^{k} c_j(n\alpha_j - v_j - r_j)| < \varepsilon \sum_{j=1}^{k} |c_j| = \varepsilon'. \tag{7}$$

Másrészt (7) bal oldala az abszolút érték nélkül

$$n(c_0 + \sum_{j=1}^{k} c_j\alpha_j) - \sum_{j=1}^{k} c_j v_j - M \tag{8}$$

alakba írható, ahol M egész szám. A (6), (7) és (8) alapján

$$|\sum_{j=1}^{k} c_j v_j + M| < \varepsilon'$$

adódik, tehát

$$\{\sum_{j=1}^{k} c_j v_j\} < \varepsilon' \qquad \text{vagy} \qquad \{\sum_{j=1}^{k} c_j v_j\} > 1 - \varepsilon'.$$

Ez tetszőleges $v_1, \ldots, v_k$ esetén nyilván lehetetlen, és így ellentmondásra jutottunk.

9. Algebrai és transzcendens számok

• **9.2.8** A feltétel szerint $f \neq 0$, továbbá f-nek létezik gyöke, tehát f nem lehet (nemnulla) konstans polinom.

Tegyük fel indirekt, hogy f irreducibilis $\mathbf{Q}$ felett. Ekkor f a gyökei minimálpolinomja, azaz

$$f = m_\alpha = m_\beta.$$

Mivel $g(\alpha) = 0$, ezért $m_\alpha = f \mid g$. Ekkor viszont f minden gyöke g-nek is gyöke, tehát $g(\beta) = 0$. Az így kapott ellentmondás bizonyítja, hogy f reducibilis $\mathbf{Q}$ felett.

(A feltételekből g reducibilitására vagy irreducibilitására nem tudunk következtetni, mindkét eset megvalósulhat.)

• **9.3.6** Tegyük fel, hogy r és $\cos\varphi$ algebrai. Ekkor $\sin\varphi = \pm\sqrt{1-\cos^2\varphi}$ és i is algebrai, tehát az r, $\cos\varphi$, $\sin\varphi$ és i számokból az összeadás és szorzás segítségével képzett α is algebrai.

Megfordítva, tegyük fel, hogy α algebrai. A 9.3.3 Tétel alapján ekkor $r\cos\varphi$ és $r\sin\varphi$ is algebrai. Innen $r = \sqrt{(r\cos\varphi)^2 + (r\sin\varphi)^2}$ is algebrai. Ezt felhasználva kapjuk, hogy $\cos\varphi = (r\cos\varphi)/r$ is algebrai.

• **9.4.1 a)** (a1) Legyen $h = a/b$, ahol $b > 0$ és a egész számok. Mivel α Liouville-szám, ezért tetszőleges n-hez létezik olyan r/s tört, amelyre

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{2n}}\,. \tag{1}$$

A már többször alkalmazott meggondolás szerint $n \to \infty$ mellett a megfelelő s értékek is a végtelenhez tartanak, így feltehetjük, hogy $s > b$.

Az (1) egyenlőtlenség átírható

$$\left|(h+\alpha) - \left(\frac{a}{b} + \frac{r}{s}\right)\right| < \frac{1}{s^{2n}}$$

alakba, és így az $s > b$ feltételt is felhasználva

$$\left|(h+\alpha) - \frac{as+br}{bs}\right| < \frac{1}{s^{2n}} < \frac{1}{(bs)^n}$$

adódik. Ez azt jelenti, hogy az

$$\frac{R}{S} = \frac{as+br}{bs}$$

törtre

$$\left|(h+\alpha) - \frac{R}{S}\right| < \frac{1}{S^n}$$

teljesül. Ezzel beláttuk, hogy $h+\alpha$ Liouville-szám.

• (a2) A $h\alpha$-ra vonatkozó állítást az előzőekhez hasonlóan igazolhatjuk.

• (a3) Megmutatjuk, hogy ha r/s „jól" közelíti α-t, akkor $(r/s)^k$ „majdnem ilyen jól" közelíti α^k-t. Induljunk ki az

$$\alpha^k - \left(\frac{r}{s}\right)^k = \left(\alpha - \frac{r}{s}\right)\left(\alpha^{k-1} + \alpha^{k-2}\left(\frac{r}{s}\right) + \ldots + \left(\frac{r}{s}\right)^{k-1}\right) \tag{2}$$

azonosságból. Ha r/s (bármilyen értelemben) közel van α-hoz, akkor (2) második tényezőjének értéke közel van $k\alpha^{k-1}$-hez, tehát abszolút értékben egy csak az α-tól és k-tól függő c korlát alatt marad. Ebből következik, hogy ha

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^{kn}}, \tag{3}$$

akkor

$$\left|\alpha^k - \frac{r^k}{s^k}\right| < \frac{c}{(s^k)^n}. \tag{4}$$

Mivel α Liouville-szám, ezért (3), és így (4) is tetszőleges n-re elérhető, azaz α^k is Liouville-szám.

• (a4) Azt fogjuk igazolni, hogy ha r/s „jól" közelíti α-t, akkor s/r „jól" közelíti $1/\alpha$-t. (Ha $r < 0$, akkor s/r helyett a $(-s)/(-r)$ alakot vesszük.)

Az (1) egyenlőtlenség

$$|s\alpha - r| < \frac{1}{s^{2n-1}}$$

alakját felhasználva

$$\left|\frac{1}{\alpha} - \frac{s}{r}\right| = \left|\frac{r - s\alpha}{r\alpha}\right| < \frac{1}{s^{2n-1}|r\alpha|} \tag{5}$$

adódik (nyilván feltehető $r \neq 0$). Tudjuk, hogy ha $n \to \infty$, akkor a megfelelő s értékek végtelenhez és az r/s törtek α-hoz tartanak, ezért feltehető, hogy

$$\left|\frac{r}{s}\right| < |\alpha| + 1 < s \qquad \text{és} \qquad s|\alpha| \geq 1. \tag{6}$$

Az (5) és (6) egyenlőtlenségekből kapjuk, hogy

$$\left|\frac{1}{\alpha} - \frac{s}{r}\right| < \frac{1}{|r|^n}. \tag{7}$$

Mivel α Liouville-szám, ezért (1), és így (7) is tetszőleges n-re elérhető, azaz $1/\alpha$ is Liouville-szám.

• **9.4.4** Tegyük fel indirekt, hogy egy α komplex szám többszörös gyöke az f polinomnak. Ekkor α gyöke az f deriváltjának, f'-nek is. Mivel f irreducibilis $\mathbf{Q}$ felett, ezért f az α (egyik) minimálpolinomja. Így $f'(\alpha) = 0$-ból következik, hogy $f \mid f'$. Ez azonban ($f' \neq 0$ és) $\deg f' < \deg f$ miatt lehetetlen.

• **9.6.5 a)** Az állítás igaz. Tegyük fel indirekt, hogy f minden gyöke algebrai egész, azaz f gyöktényezős alakja $\mathbf{C}[x]$-ben

$$f = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)\,,$$

ahol mindegyik α_j algebrai egész. A szorzást elvégezve kapjuk, hogy az f együtthatói az α_j-kből összeadás, kivonás és szorzás segítségével állnak elő. Mivel az algebrai egészek gyűrűt alkotnak, így f minden együtthatója algebrai egész. Az együtthatók egyben racionális számok is, tehát szükségképpen egész számok, ami ellentmond az f-re vonatkozó feltételnek.

• **b)** Az állítás hamis. Például az

$$f = (x^2-6)(x^2-\frac{1}{2}) = x^4 - \frac{13}{2}x^2 + 3$$

polinom normált, racionális együtthatós, nem minden együtthatója egész, és mégis van olyan gyöke, a $\sqrt{6}$ (és a $-\sqrt{6}$), amely algebrai egész.

• **c)** Az állítás igaz. Mivel f irreducibilis $\mathbf{Q}$ felett, ezért valamennyi gyökének minimálpolinomja. A 9.6.1 Definíció alapján így egyik gyök sem lehet algebrai egész.

• **d)** Az állítás igaz. Legyen α az f polinom egyetlen olyan gyöke, amely nem algebrai egész. Mivel $f(\alpha)=0$, ezért $m_\alpha \mid f$, és így m_α minden gyöke f-nek is gyöke. Az m_α egyik gyöke sem algebrai egész, továbbá m_α-nak (a 9.4.4 feladat szerint) nem lehet többszörös gyöke, ezért a feladat feltétele csak úgy teljesülhet, ha m_α elsőfokú. Ez azt jelenti, hogy α racionális szám, tehát f-nek valóban létezik racionális gyöke.

10. Algebrai számtestek

• **10.2.5 a)** Legyen $\alpha = \sqrt{7}+3i$ és $M = \mathbf{Q}(\alpha)$, ekkor $\deg\alpha = \deg(M:\mathbf{Q})$.

Tekintsük a következő bővítésláncot:

$$\mathbf{Q} \subseteq K \subseteq L, \qquad \text{ahol} \qquad K = \mathbf{Q}(\sqrt{7}) \qquad \text{és} \qquad L = K(i). \tag{1}$$

Belátjuk, hogy $M = L$ és így $\deg\alpha$ meghatározásához az $L:\mathbf{Q}$ bővítés fokát kell meghatároznunk.

Az L definíciója alapján $\sqrt{7} \in L$ és $3i \in L$, továbbá L test, ezért $\alpha = \sqrt{7}+3i \in L$, és így $M \subseteq L$.

A másik irányú, $L \subseteq M$ tartalmazáshoz azt kell igazolni, hogy $\sqrt{7} \in M$ és $3i \in M$. Mivel

$$(\sqrt{7} - 3i)(\sqrt{7} + 3i) = 16, \qquad \text{azaz} \qquad \overline{\alpha} = \frac{16}{\alpha},$$

ezért $\overline{\alpha} \in M$, tehát

$$\sqrt{7} = \operatorname{Re}\alpha = \frac{\alpha + \overline{\alpha}}{2} \in M \qquad \text{és} \qquad 3i = \frac{\alpha - \overline{\alpha}}{2} \in M.$$

Rátérve $\deg(L : \mathbf{Q})$ meghatározására, megmutatjuk, hogy az (1) bővítéslláncban mindkét láncszem foka 2. Nyilván $\deg(K : \mathbf{Q}) = \deg\sqrt{7} = 2$. Mivel $L \neq K$ (hiszen K minden eleme valós, L viszont tartalmazza az i-t), ezért $\deg(L : K) \geq 2$. Ugyanakkor $\deg(L : K) = \deg_K i \leq \deg i = 2$, tehát valóban $\deg(L : K) = 2$.

Ezután a fokszámtételből következik, hogy

$$\deg\alpha = \deg(L : \mathbf{Q}) = \deg(K : \mathbf{Q}) \cdot \deg(L : K) = 4.$$

• **10.2.7** Jelöljük $\mathbf{Q}(\vartheta)$ valós elemeinek halmazát V-vel: $V = \mathbf{Q}(\vartheta) \cap \mathbf{R}$.

• **a)** Mivel $\vartheta = \sqrt[5]{3}(\cos 144° + i \sin 144°)$ gyöke az $x^5 - 3$, a racionális test felett irreducibilis polinomnak, ezért a $\mathbf{Q}(\vartheta)$ bővítés foka 5.

Tekintsük a $\mathbf{Q} \subseteq V \subseteq \mathbf{Q}(\vartheta)$ bővítésláncot. A fokszámtétel alapján

$$5 = \deg(\mathbf{Q}(\vartheta) : \mathbf{Q}) = \deg(\mathbf{Q}(\vartheta) : V) \cdot \deg(V : \mathbf{Q}),$$

és így $\deg(\mathbf{Q}(\vartheta) : V) = 1$ vagy 5. Mivel V csak valós számokból áll, $\mathbf{Q}(\vartheta)$ pedig tartalmaz nem valós komplex számokat is, ezért $\mathbf{Q}(\vartheta) \neq V$. Ebből következik, hogy $\deg(\mathbf{Q}(\vartheta) : V) \neq 1$, vagyis csak $\deg(\mathbf{Q}(\vartheta) : V) = 5$ lehetséges. Ekkor $\deg(V : \mathbf{Q}) = 1$, azaz $V = \mathbf{Q}$.

• **b)** Megmutatjuk, hogy $V = \mathbf{Q}(\sqrt[3]{3})$.

Mivel $\sqrt[3]{3}$ valós és

$$\sqrt[3]{3} = -\left(i\sqrt[6]{3}\right)^2 = -\vartheta^2 \in \mathbf{Q}(\vartheta),$$

ezért $\mathbf{Q}(\sqrt[3]{3}) \subseteq V$.

Tekintsük a

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt[3]{3}) \subseteq V \subseteq \mathbf{Q}(\vartheta) \tag{2}$$

bővítésláncot.

Mivel $\vartheta = i\sqrt[6]{3}$ gyöke az x^6+3, a racionális test felett irreducibilis polinomnak, ezért $\deg(\mathbf{Q}(\vartheta):\mathbf{Q}) = 6$.

Hasonlóan adódik, hogy $\deg(\mathbf{Q}(\sqrt[3]{3}):\mathbf{Q}) = 3$.

Így a fokszámtételt a (2) bővítésláncra alkalmazva kapjuk, hogy

$$2 = \deg(\mathbf{Q}(\vartheta):\mathbf{Q}(\sqrt[3]{3})) = \deg(\mathbf{Q}(\vartheta):V)\cdot\deg(V:\mathbf{Q}(\sqrt[3]{3})).$$

Az a) résznél látott módon adódik, hogy $\mathbf{Q}(\vartheta)\neq\mathbf{Q}(\sqrt[3]{3})$, és így

$$\deg(V:\mathbf{Q}(\sqrt[3]{3}))=1, \qquad \text{azaz} \qquad V=\mathbf{Q}(\sqrt[3]{3}).$$

• **c)** Mivel a $\sqrt{i}$ két értéke egymás negatívja, ezért ugyanahhoz a bővítéshez jutunk bármelyik érték esetén. Válasszuk például a

$$\vartheta = \sqrt{i} = \frac{1+i}{\sqrt{2}} \tag{3}$$

értéket.

Megmutatjuk, hogy $V = \mathbf{Q}(\sqrt{2})$.

Első megoldás: Mivel

$$i = (\sqrt{i})^2 = \vartheta^2 \in \mathbf{Q}(\vartheta)\,,$$

ezért (3)-ból következik, hogy

$$\sqrt{2}\in\mathbf{Q}(\vartheta), \qquad \text{tehát} \qquad \mathbf{Q}(\sqrt{2})\subseteq V.$$

Tekintsük a

$$\mathbf{Q}\subseteq\mathbf{Q}(\sqrt{2})\subseteq V\subseteq\mathbf{Q}(\vartheta)$$

bővítésláncot. Az előző részekhez hasonlóan adódik, hogy

$$\deg(\mathbf{Q}(\vartheta):\mathbf{Q})=4, \qquad \deg(\mathbf{Q}(\sqrt{2}):\mathbf{Q})=2 \qquad \text{és} \qquad V\neq\mathbf{Q}(\vartheta).$$

Ebből a fokszámtétel felhasználásával kapjuk, hogy

$$\deg(V:\mathbf{Q}(\sqrt{2}))=1, \qquad \text{azaz} \qquad V=\mathbf{Q}(\sqrt{2}).$$

Második megoldás: A 10.2.3 Tétel szerint $\mathbf{Q}(\vartheta)$ elemei egyértelműen felírhatók racionális a_i számokkal

$$\alpha = a_0 + a_1\sqrt{i} + a_2(\sqrt{i})^2 + a_3(\sqrt{i})^3 = a_0 + a_1\frac{1+i}{\sqrt{2}} + a_2 i + a_3\frac{-1+i}{\sqrt{2}} \tag{4}$$

alakban.

Az α akkor és csak akkor valós, ha a képzetes része 0, azaz

$$\frac{a_1 + a_3}{\sqrt{2}} + a_2 = 0.$$

Mivel $\sqrt{2}$ irracionális, ez pontosan akkor teljesül, ha

$$a_3 = -a_1 \qquad \text{és} \qquad a_2 = 0.$$

Ezt (4)-be visszahelyettesítve kapjuk, hogy α akkor és csak akkor valós, ha

$$\alpha = a_0 + a_1\sqrt{2}, \qquad \text{azaz} \qquad \alpha \in \mathbf{Q}(\sqrt{2}).$$

Ezzel beláttuk, hogy $V = \mathbf{Q}(\sqrt{2})$.

Harmadik megoldás: Az állítás a 10.2.8 feladatból is következik.

• **10.2.8** Mivel $|\vartheta| = 1$, ezért $\overline{\vartheta} = 1/\vartheta$, és így

$$\operatorname{Re}\vartheta = \frac{\vartheta + \overline{\vartheta}}{2} = \frac{1}{2}\big(\vartheta + \frac{1}{\vartheta}\big)\,. \tag{5}$$

Ebből következik, hogy $\operatorname{Re}\vartheta \in \mathbf{Q}(\vartheta)$, és így $\mathbf{Q}(\operatorname{Re}\vartheta) \subseteq \mathbf{Q}(\vartheta)$. Mivel nyilván $\mathbf{Q}(\operatorname{Re}\vartheta) \subseteq \mathbf{R}$, ezért

$$\mathbf{Q}(\operatorname{Re}\vartheta) \subseteq \mathbf{Q}(\vartheta) \cap \mathbf{R}. \tag{6}$$

A másik irányú tartalmazáshoz legyen c a $\mathbf{Q}(\vartheta)$ tetszőleges valós eleme: $c = g(\vartheta)/h(\vartheta)$ (ahol g, $h \in \mathbf{Q}[x]$, $h(\vartheta) \neq 0$). Ekkor

$$h(\vartheta)c = g(\vartheta). \tag{7}$$

A (7) egyenlőséget konjugálva, $c \in \mathbf{R}$ alapján

$$h(\overline{\vartheta})c = g(\overline{\vartheta}) \tag{8}$$

adódik. Tegyük fel egyelőre, hogy $h(\vartheta) + h(\overline{\vartheta}) \neq 0$. Ekkor (7)-et és (8)-at összeadva, majd c-t kifejezve azt kapjuk, hogy

$$c \;=\; \frac{g(\vartheta) + g(\overline{\vartheta})}{h(\vartheta) + h(\overline{\vartheta})} \;=\; \frac{g(\vartheta) + g(1/\vartheta)}{h(\vartheta) + h(1/\vartheta)}\,. \tag{9}$$

Felhasználva, hogy $\vartheta^k + \vartheta^{-k}$ felírható $\vartheta + (1/\vartheta)$, azaz $2\mathrm{Re}\,\vartheta$ racionális együtthatós polinomjaként, (9)-ből azt nyerjük, hogy $c \in \mathbf{Q}(\mathrm{Re}\,\vartheta)$. Ezzel beláttuk, hogy

$$\mathbf{Q}(\vartheta) \cap \mathbf{R} \subseteq \mathbf{Q}(\mathrm{Re}\,\vartheta).$$

Hátravan még a

$$h(\vartheta) + h(\overline{\vartheta}) = h(\vartheta) + h(1/\vartheta) = 0 \tag{10}$$

eset vizsgálata. Ekkor azonnal adódik, hogy ϑ algebrai szám. Az alábbi gondolatmenet nemcsak (10) fennállása, hanem tetszőleges ϑ algebrai szám esetén érvényes.

Felhasználva (6)-ot, tekintsük a

$$\mathbf{Q}(\mathrm{Re}\,\vartheta) \subseteq \mathbf{Q}(\vartheta) \cap \mathbf{R} \subseteq \mathbf{Q}(\vartheta) \tag{11}$$

bővítésláncot. A feladat állítása $\vartheta = \pm 1$ esetén nyilvánvaló, így feltehetjük, hogy ϑ nem valós szám. Megmutatjuk, hogy ekkor (11)-ben az egész lánc is, és a második láncszem is másodfokú bővítés, ezért a fokszámtétel alapján az első láncszem elsőfokú, azaz a két szóban forgó bővítés megegyezik.

Mivel a (11) lánc első két eleme csak valós számokból áll, a harmadik viszont nem, ezért az egész lánc és a második láncszem is legalább másodfokú. Így elég belátni, hogy az egész lánc (legfeljebb) másodfokú bővítés.

A $|\vartheta| = 1$ feltétel miatt $\mathrm{Im}\,\vartheta = \pm\sqrt{1 - (\mathrm{Re}\,\vartheta)^2}$, ezért

$$\vartheta = \mathrm{Re}\,\vartheta + i\mathrm{Im}\,\vartheta = \mathrm{Re}\,\vartheta + \sqrt{(\mathrm{Re}\,\vartheta)^2 - 1}$$

($\mathrm{Im}\,\vartheta \neq 0$ miatt pontosan) másodfokú elem $\mathbf{Q}(\mathrm{Re}\,\vartheta)$ felett. Így valóban $\deg\big(\mathbf{Q}(\vartheta) : \mathbf{Q}(\mathrm{Re}\,\vartheta)\big) = 2$.

• **10.2.11** Megmutatjuk, hogy az egységkörön a ± 1-en kívül nincs páratlan fokú algebrai szám.

• *Első bizonyítás*: A 10.2.8 feladat megoldása során beláttuk, hogy ha ϑ algebrai szám és $|\vartheta| = 1$, akkor

$$\mathbf{Q}(\mathrm{Re}\,\vartheta) \subseteq \mathbf{Q}(\vartheta),$$

és $\vartheta \neq \pm 1$ esetén a bővítés foka 2.

Ez azt jelenti, hogy a

$$\mathbf{Q} \subseteq \mathbf{Q}(\mathrm{Re}\,\vartheta) \subseteq \mathbf{Q}(\vartheta)$$

bővítéslánc második láncszemének a foka 2, és így a fokszámtétel szerint

$$\deg \vartheta = \deg(\mathbf{Q}(\vartheta) : \mathbf{Q}) \text{ páros.}$$

• *Második bizonyítás*: Egy valós együtthatós polinomnak egy komplex szám és a konjugáltja ugyanannyiszoros gyöke, ezért $|\vartheta| = 1$ esetén $1/\vartheta = \overline{\vartheta}$ is gyöke a ϑ minimálpolinomjának. Ebből m_ϑ irreducibilitása miatt következik, hogy

$$m_\vartheta = m_{1/\vartheta}. \tag{12}$$

Könnyen adódik (lásd például a 9.1.2c feladathoz fűzött útmutatást), hogy ha ϑ minimálpolinomja

$$m_\vartheta = a_0 + a_1 x + \ldots + a_n x^n \qquad (a_n \neq 0), \tag{13a}$$

akkor $1/\vartheta$ (egyik) minimálpolinomja

$$m_{1/\vartheta} = a_n + a_{n-1} x + \ldots + a_0 x^n \qquad (a_0 \neq 0). \tag{13b}$$

A (12) feltételből következik, hogy a (13b) polinom a (13a) polinomnak egy c racionális számszorosa. A konstans tagok és a főegyütthatók összehasonlításából kapjuk, hogy

$$a_n = c a_0 \qquad \text{és} \qquad a_0 = c a_n\,,$$

és így $c = \pm 1$. Ennek felhasználásával a többi együttható összehasonlításából az adódik, hogy vagy

$$a_j = a_{n-j}, \qquad j = 0, 1, \ldots, n,$$

vagy pedig

$$a_j = -a_{n-j}, \qquad j = 0, 1, \ldots, n.$$

Ha $\deg \vartheta = n$ páratlan, akkor az első esetben

$$m_\vartheta(-1) = \sum_{j=0}^{n} a_j (-1)^j = \sum_{j=0}^{(n-1)/2} a_j \big((-1)^j + (-1)^{n-j}\big) = 0,$$

a második esetben pedig

$$m_\vartheta(1) = \sum_{j=0}^{n} a_j = \sum_{j=0}^{(n-1)/2} \big(a_j + a_{n-j}\big) = 0.$$

Ez azt jelenti, hogy m_ϑ-nak a -1 vagy az 1 racionális szám gyöke. Mivel m_ϑ irreducibilis $\mathbf{Q}$ felett, ezért ez csak úgy lehetséges ha $\vartheta = -1$, illetve 1.

• **10.3.5** Ha t négyzetmentes összetett szám, akkor létezik olyan $p > 2$ prímszám, amelyre $p \mid t$.

Indirekt tegyük fel, hogy $E(\sqrt{t})$-ben igaz a számelmélet alaptétele. Ekkor a 10.3.8 Tétel (vii) állítása szerint p felbomlik $E(\sqrt{t})$-ben, és így létezik olyan $\alpha = a+b\sqrt{t}$, amelyre $N(\alpha) = a^2+|t|b^2 = p$. Itt a és b egészek vagy 2 nevezőjű törtek, tehát $u = 2a$, $v = 2b$ biztosan egész, és

$$u^2 + |t|v^2 = 4p. \tag{14}$$

Ha $v = 0$, akkor $u^2 = 4p$, ami lehetetlen.

Legyen $|t| = kp$. Mivel $k \geq 2$, ezért $|v| \geq 2$ esetén (14) bal oldala nagyobb a jobb oldalnál.

Maradt a $|v| = 1$ eset. Ekkor $u^2 = (4-k)p$, ami $k = 2, 3$ és $k \geq 5$ mellett nyilván lehetetlen, továbbá t négyzetmentessége miatt $k \neq 4$.

Ezzel megmutattuk, hogy (14) nem teljesülhet, és így ellentmondásra jutottunk.

• **10.3.6** Az útmutatásban jelzett gondolatmenetet követjük.

Legyen $t = -4k+1$ és $\alpha_n = n + (1+\sqrt{t})/2$. Ekkor

$$N(\alpha_n) = N\Big(n + \frac{1+\sqrt{t}}{2}\Big) = \Big(n + \frac{1+\sqrt{t}}{2}\Big)\Big(n + \frac{1-\sqrt{t}}{2}\Big) = n^2 + n + k\,. \tag{15}$$

Megmutatjuk, hogy $0 \leq n \leq k-2$ esetén α_n felbonthatatlan. Tegyük fel indirekt, hogy (valamely n-re) $\alpha_n = \beta\gamma$, ahol β és γ egyike sem egység. Mivel α_n-nek nem lehet ± 1-től különböző olyan osztója, amely egész szám, ezért

$$\beta = b_0 + b_1\frac{1+\sqrt{t}}{2}, \quad \gamma = c_0 + c_1\frac{1+\sqrt{t}}{2}, \quad \text{ahol} \quad b_j, c_j \in \mathbf{Z}, \quad \text{és} \quad b_1c_1 \neq 0.$$

Ebből következik, hogy

$$N(\beta) = b_0^2 + b_0b_1 + b_1^2k = \Big(b_0 + \frac{b_1}{2}\Big)^2 + b_1^2\Big(k - \frac{1}{4}\Big) \geq k,$$

és ugyanígy $N(\gamma) \geq k$. Ekkor azonban

$$k^2 \leq N(\beta)N(\gamma) = N(\alpha_n) < N(\alpha_{k-1}) = (k-1)^2 + (k-1) + k = k^2\,,$$

ami ellentmondás.

Ezzel beláttuk, hogy $0 \le n \le k-2$ esetén α_n felbonthatatlan. Ebből következik, hogy $\overline{\alpha_n}$ is felbonthatatlan.

Tegyük fel most indirekt, hogy valamely $0 \le n \le k-2$-re $f(n)$ nem prímszám, azaz

$$N(\alpha_n) = n^2 + n + k = rs, \qquad \text{ahol} \qquad r,\, s > 1. \tag{16}$$

A (15) és (16) összefüggésekből ekkor

$$\left(n + \frac{1+\sqrt{t}}{2}\right)\left(n + \frac{1-\sqrt{t}}{2}\right) = rs \tag{17}$$

adódik. A (17) bal oldalán két felbonthatatlan szám szorzata áll. Így a számelmélet alaptétele szerint a jobb oldalon álló két, egységtől különböző tényező is felbonthatatlan, mégpedig valamelyik bal oldali tényező egységszerese kell hogy legyen. Ez azonban lehetetlen, hiszen a ± 1-től különböző r egész szám nem lehet osztója α_n-nek vagy $\overline{\alpha_n}$-nak.

• **10.3.9 e)** Az útmutatásnak megfelelően azt fogjuk igazolni, hogy ha $p \equiv 1$ vagy 9 (mod 20), akkor van olyan a, b egész, amelyre

$$p = a^2 + 5b^2 = (a + b\sqrt{-5})(a - b\sqrt{-5}).$$

Erre két bizonyítást adunk. Mindkettőben felhasználjuk, hogy $\left(\frac{-5}{p}\right) = 1$ miatt létezik olyan c egész, amelyre $p \mid c^2 + 5$.

• *Első bizonyítás*: A 8.2.4 Tétel bizonyításának gondolatmenetét követjük. Tekintsük a síkon az $x = pu + cv$, $y = v$ koordinátájú pontokat, ahol u és v egymástól függetlenül befutják az egész számokat. Ezek a pontok egy parelogrammarácsot alkotnak, amelyben az alapparalelogramma területe $\Delta = p$.

Bármely rácspont esetén

$$x^2 + 5y^2 = (pu + cv)^2 + 5v^2 = p(pu^2 + 2cuv) + v^2(c^2 + 5) \equiv 0 \pmod{p},$$

azaz $p \mid x^2 + 5y^2$.

Alkalmazzuk Minkowski tételét az $x^2 + 5y^2 \le 4\sqrt{5}p/\pi$ egyenletű, origó körüli $4p = 4\Delta$ területű (zárt) ellipszisre. A tétel szerint ez az ellipszis az origón kívül is tartalmaz legalább egy (x, y) rácspontot. Így erre a rácspontra teljesül

$$p \mid x^2 + 5y^2 \qquad \text{és} \qquad x^2 + 5y^2 \le \frac{4\sqrt{5}p}{\pi} < 3p,$$

tehát $x^2+5y^2=p$ vagy $2p$.

Az $x^2+5y^2=2p$ egyenlőség azonban nem állhat fenn, mert 5-tel osztva a bal oldal lehetséges maradékai 0 és ±1, a jobb oldalé pedig ±2, hiszen $p\equiv\pm1 \pmod 5$. Ezért szükségképpen $x^2+5y^2=p$.

• *Második bizonyítás*: Legyen $p \mid c^2+5$. Belátjuk, hogy a $cy\equiv x \pmod p$ kongruenciának létezik olyan x, y megoldása, ahol $0<|x|$, $|y|<\sqrt{p}$. Ez a 7.5.21a feladatban szereplő Thue-lemmából következik, a $k=1$, $u=v=\lceil\sqrt{p}\rceil$ és $C=c$ szereposztással.

Ekkor

$$x^2+5y^2\equiv c^2y^2+5y^2=(c^2+5)y^2\equiv 0 \pmod p \qquad \text{és} \qquad x^2+5y^2<6p\,.$$

Megmutatjuk, hogy van olyan a, b egész, amelyre $a^2+5b^2=p$.

Ha $x^2+5y^2=5p$, akkor $5\mid x$, azaz $x=5z$, és így $25z^2+5y^2=5p$, vagyis $5z^2+y^2=p$.

Ha $x^2+5y^2=4p$, akkor a modulo 4 maradékok alapján x és y is páros, $x=2a$, $y=2b$, és így $4a^2+20b^2=4p$, azaz $a^2+5b^2=p$.

Az $x^2+5y^2=3p$ vagy $2p$ egyenlőség a két oldal modulo 5 maradékainak különbözősége miatt nem teljesülhet.

Végül, az $x^2+5y^2=p$ eset azonnal a kívánt állítást jelenti.

• **10.5.6** Tekintsünk egy általános $\mathbf{Q}(\sqrt{t})$ másodfokú bővítést, ahol t négyzetmentes egész szám és $t\neq1$. Megmutatjuk, hogy $\mathbf{Q}(\sqrt{t})$-ben akkor és csak akkor létezik a kívánt tulajdonságú egész bázis, ha $t\equiv1 \pmod 4$.

Elégségesség: Ha $t\equiv1 \pmod 4$, akkor az

$$\omega_1=\frac{1+\sqrt{t}}{2} \qquad \text{és} \qquad \omega_2=\frac{1-\sqrt{t}}{2}$$

választás megfelel.

Ehhez azt alábbiakat kell megmutatni:

(i) minden $\alpha\in\mathbf{Q}(\sqrt{t})$ egyértelműen felírható racionális c_j számokkal

$$\alpha=c_1\omega_1+c_2\omega_2 \tag{18}$$

alakban;

(ii) α akkor és csak akkor algebrai egész, ha c_1 és c_2 egész szám;

(iii) ω_1-nek és ω_2-nek ugyanaz a minimálpolinomja.

(i) Tudjuk, hogy α egyértelműen előáll

$$\alpha=a+b\sqrt{t} \tag{19}$$

alakban, ahol a és b racionális számok. Hasonlítsuk össze (18)-at és (19)-et:

$$a+b\sqrt{t}=c_1\frac{1+\sqrt{t}}{2}+c_2\frac{1-\sqrt{t}}{2}=\frac{c_1+c_2}{2}+\frac{c_1-c_2}{2}\sqrt{t}\,.$$

A (19) előállítás egyértelműségéből látszik, hogy (18) pontosan akkor teljesül, ha

$$a=\frac{c_1+c_2}{2}\qquad\text{és}\qquad b=\frac{c_1-c_2}{2}\,,\tag{20a}$$

azaz

$$c_1=a+b\qquad\text{és}\qquad c_2=a-b.\tag{20b}$$

Ezzel a megfelelő (racionális) c_1 és c_2 létezését és egyértelműségét beláttuk.

(ii) A 10.3.2 Tétel szerint a $t\equiv 1 \pmod 4$ esetben α akkor és csak akkor algebrai egész, ha

$$a=\frac{u}{2}\,,\quad b=\frac{v}{2}\,,\quad\text{ahol}\quad u,\,v\in\mathbf{Z}\quad\text{és}\quad u\equiv v \pmod 2.\tag{21}$$

Azt kell igazolnunk, hogy a (21) feltétel ekvivalens azzal, hogy c_1 és c_2 egész számok.

Ha a és b a (21)-ben előírt alakú, akkor (20b)-ből következik, hogy

$$c_1=\frac{u+v}{2}\qquad\text{és}\qquad c_2=\frac{u-v}{2}$$

egész számok.

Megfordítva, ha c_1 és c_2 egész, akkor $u=c_1+c_2$ és $v=c_1-c_2$ azonos paritású, és így (20a) szerint a és b eleget tesz (21)-nek.

(iii) A két szám közös minimálpolinomja

$$(x-\omega_1)(x-\omega_2)=x^2-x+\frac{1-t}{4}\,.$$

Szükségesség: Indirekt tegyük fel, hogy valamely $t\not\equiv 1 \pmod 4$ esetén létezik a megadott tulajdonságú ω_1, ω_2 egész bázis.

Az ω_1 és ω_2 egymás $\mathbf{Q}$ feletti konjugáltjai, tehát

$$\omega_1=r+s\sqrt{t}\qquad\text{és}\qquad\omega_2=r-s\sqrt{t},\qquad r,\,s\in\mathbf{Q}.$$

Mivel ω_1 és ω_2 algebrai egész és $t\not\equiv 1 \pmod 4$, ezért (a 10.3.2 Tétel alapján) r és s egész számok, továbbá ω_1 és ω_2 lineáris függetlensége miatt $s\neq 0$.

Az 1 algebrai egész, tehát alkalmas c_1 és c_2 egész számokkal elő kell állnia

$$1 = c_1\omega_1 + c_2\omega_2 = (c_1 + c_2)r + (c_1 - c_2)s\sqrt{t}$$

alakban. Ez pontosan akkor teljesül, ha

$$(c_1 + c_2)r = 1 \qquad \text{és} \qquad (c_1 - c_2)s = 0.$$

Az $s \neq 0$ feltételből kapjuk, hogy $c_1 = c_2$, és így

$$1 = (c_1 + c_2)r = 2c_1r,$$

ami egész c_1 és r értékekre lehetetlen.

11. Ideálok

• **11.1.8 a)** Először megmutatjuk, hogy az a1 és a3 gyűrű nem test, mivel található bennük nullosztó.

Jelöljük I-vel $\mathbf{R}[x]$-ben az $x^2 - 2$ által generált főideált: $I = (x^2 - 2)$. Ekkor az $\mathbf{R}[x]/I$ faktorgyűrűben az $x + \sqrt{2}$ és $x - \sqrt{2}$ polinomok által reprezentált (nemnulla) maradékosztályok szorzata a nulla maradékosztály:

$$\big[x + \sqrt{2} + I\,\big]\big[x - \sqrt{2} + I\,\big] = \big[x + \sqrt{2}\,\big]\big[x - \sqrt{2}\,\big] + I = x^2 - 2 + I = 0 + I\,.$$

Ez azt jelenti, hogy $x + \sqrt{2} + I$ és $x - \sqrt{2} + I$ nullosztók $\mathbf{R}[x]/I$-ben, és így $\mathbf{R}[x]/I$ nem lehet test.

Hasonló a helyzet a $\mathbf{C}[x]/(x^2 + 1)$ faktorgyűrűben: itt az $x + i$ és $x - i$ polinomok által reprezentált (nemnulla) maradékosztályok szorzata nulla.

Most megmutatjuk, hogy az a2-ben megadott $\mathbf{R}[x]/(x^2 + 1)$ faktorgyűrű test, mégpedig a komplex számtesttel izomorf.

A 11.1.6 Tétel utáni példa gondolatmenetét követjük. Most azok a (valós együtthatós) polinomok kerülnek az $(x^2 + 1)$ főideál szerint egy maradékosztályba, amelyek ugyanazt a maradékot adják $x^2 + 1$-gyel osztva. Ily módon minden maradékosztály egyértelműen jellemezhető egy „maradékkal”, azaz egy legfeljebb elsőfokú $a + bx$ (valós együtthatós) polinommal (idesorolva a 0 polinomot is, amely magát az ideált reprezentálja).

A maradékosztálygyűrűben tulajdonképpen ezekkel a maradékokkal számolunk, azaz pl. két maradékosztály szorzásakor ezeket a maradékokat összeszorozzuk és vesszük a szorzatnak az x^2+1-gyel való osztási maradékát. Ennek megfelelően az összeadást az

$$[a + bx] + [c + dx] = [a + c] + [b + d]x,$$

a szorzást pedig az

$$[a+bx][c+dx] = ac + [ad+bc]x + bdx^2 = \\ = ac + [ad+bc]x - bd + bd[x^2+1] = [ac-bd] + [ad+bc]x$$

szabály szerint kell végezni, azaz pontosan ugyanúgy, ahogyan a komplex számoknál (képzeljünk az „x” betű helyére mindenhol „i” betűt).

Ezzel beláttuk, hogy az $\mathbf{R}[x]/(x^2+1)$ maradékosztálygyűrű test és izomorf $\mathbf{C}$-vel.

• **b)** Bebizonyítjuk, hogy az $R = T[x]/(f)$ faktorgyűrű akkor és csak akkor test, ha f irreducibilis T felett.

Szükségesség: Tegyük fel indirekt, hogy f nem irreducibilis T felett. Ekkor $f = 0$, vagy f egység, vagy pedig f reducibilis T felett. Megmutatjuk, hogy R egyik esetben sem test.

Ha f egység, akkor $(f) = (1) = T[x]$, tehát R-nek csak egy eleme van, ha pedig $f = 0$, akkor $(f) = (0)$, tehát R azonosnak tekinthető $T[x]$-szel, vagyis R ezekben az esetekben nyilván nem test.

Ha f reducibilis, azaz létezik olyan g és h nemkonstans polinom, amelyre $f = gh$, akkor R-ben a g és h polinomok által reprezentált maradékosztályok szorzata a nulla maradékosztály:

$$[g+(f)][h+(f)] = gh + (f) = f + (f) = 0 + (f)\,.$$

Ugyanakkor $g+(f)$ és $h+(f)$ egyike sem a nulla maradékosztály, hiszen $f \nmid g$ és $f \nmid h$.

Ez azt jelenti, hogy reducibilis f esetén R-ben találhatók nullosztók, és így R nem lehet test.

Elégségesség: Azt kell igazolni, hogy ha f irreducibilis T felett, akkor az $R = T[x]/(f)$ faktorgyűrű test.

Az R gyűrű kommutatív, továbbá az $1+(f)$ maradékosztály egységelem (a szorzásra nézve). Azt kell még belátni, hogy minden nemnulla elemnek létezik inverze.

A 10.2.3 Tétel bizonyításának I. részéhez hasonló gondolatmenetet alkalmazunk.

Legyen $u+(f)$ egy tetszőleges nemnulla maradékosztály, azaz $f \nmid u$. A $v+(f)$ maradékosztály pontosan akkor lesz az $u+(f)$ inverze, ha

$$[u+(f)][v+(f)] = uv + (f) = 1 + (f)\,, \qquad \text{vagyis} \qquad f \mid 1 - uv.$$

Ez azt jelenti, hogy létezik olyan $w \in T[x]$ polinom, amelyre

$$1 = uv + fw. \tag{1}$$

Az (1) egyenletben u és f adottak, v és w pedig az ismeretlenek; így az invertálhatóság kérdését egy polinomokra vonatkozó „diofantikus” egyenlet megoldhatóságára fogalmaztuk át.

Amint a 10.2.3 Tétel bizonyításában már megindokoltuk, az (1) diofantikus egyenlet (az egész számokra vonatkozó 1.3.6 Tétellel összhangban) akkor és csak akkor oldható meg, ha u és f legnagyobb közös osztója osztója az 1-nek, azaz u és f relatív prímek. Mivel f irreducibilis és $f \nmid u$, ezért ez valóban teljesül.

• **c)** Az $I = (2, x^2 + x + 1)$ ideál szerinti maradékosztályok reprezentálásához a polinomoknak az ideál mindkét generátoreleme szerint vesszük a maradékát. (Mivel $g = x^2 + x + 1$ normált polinom, ezért az egész együtthatós polinomok körében is el tudunk osztani bármely polinomot maradékosan g-vel.)

Ennek megfelelően minden maradékosztálynak van olyan reprezentánsa, amely legfeljebb elsőfokú (vagy a 0 polinom) és valamennyi együtthatója 0 vagy 1. Így az alábbi négy polinomot kapjuk:

$$0, \qquad 1, \qquad x, \qquad 1 + x.$$

Könnyen adódik, hogy ezek közül már semelyik kettő sem esik ugyanabba a maradékosztályba (azaz semelyik két polinom különbsége sem eleme az I ideálnak).

Ez azt jelenti, hogy az $R = \mathbf{Z}[x]/(2, x^2 + x + 1)$ faktorgyűrűnek négy eleme van, és ezek rendre a fenti négy polinommal reprezentálhatók.

Az R gyűrű nyilván kommutatív és az $1 + I$ maradékosztály egységelem. Az egységelem inverze önmaga, a másik két nemnulla elem pedig egymás inverze:

$$[x + I][1 + x + I] = x[1 + x] + I = 1 + [x^2 + x + 1 - 2] + I = 1 + I,$$

hiszen $x^2 + x + 1 - 2 \in I$.

Ezzel beláttuk, hogy az R gyűrű test.

Egy másik lehetséges bizonyítást a feladathoz adott útmutatásnál vázoltunk.

• **11.3.5** Ha R test, akkor $R[x]$ (a fokszám szerinti maradékos osztásra nézve) euklideszi gyűrű, és így a 11.3.5 Tétel alapján főideálgyűrű is.

A megfordításhoz tegyük fel, hogy $R[x]$ főideálgyűrű. Azt kell igazolni, hogy R test, azaz bármely $a \neq 0$ elemnek létezik inverze.

Tekintsük $R[x]$-ben az a nemnulla konstans polinom és az x által generált $I = (a, x)$ ideált. A feltétel szerint I főideál, azaz alkalmas $g \in R[x]$ polinommal $I = (g)$.

Mivel $x \in (a, x) = (g)$, ezért $g \mid x$. Így $g = \varepsilon$ vagy $g = \varepsilon x$, ahol ε egység (azaz olyan konstans polinom, amelynek létezik inverze $R[x]$-ben, vagy ami ugyanaz, az ε-nak mint R-beli elemnek létezik inverze R-ben). A $g \mid a$ feltétel miatt $g \neq \varepsilon x$, azaz csak $g = \varepsilon$ lehetséges. Ekkor $(g) = (1)$.

Mivel $(a, x) = (1)$, ezért alkalmas h, $t \in R[x]$ polinomokkal $1 = ah + xt$. Ebből következik, hogy h konstans tagjának és az a-nak a szorzata 1, tehát a-nak valóban létezik inverze.

• **11.3.9 a)** A 11.1.10b feladathoz adott útmutatás alapján azonnal adódik, hogy R minden ideálja végesen generált.

Ha $(a, b) = (d)$, akkor $(a, b, c) = (d, c)$. Ennek megfelelően elég azt belátni, hogy bármely, két elemmel generált (a, b) ideál főideál.

Ha itt valamelyik generátorelem 0, akkor az állítás nyilvánvaló. Így feltehetjük, hogy a és b egyike sem 0.

A számelmélet alaptételéből következik, hogy létezik $\operatorname{lnko}\{a, b\}$, jelöljük ezt d-vel. A 11.2.2/(iii) Tétel szerint $(a, b) = (d)$ fennállásához $d = \operatorname{lnko}\{a, b\}$ mellett azt kell még megmutatni, hogy alkalmas u, $v \in R$ elemekre $d = au + bv$. Ezt d-vel osztva a vele ekvivalens

$$1 = a_1 u + b_1 v, \qquad \operatorname{lnko}\{a_1, b_1\} = 1$$

egyenlőséghez jutunk, ami más megfogalmazásban azt jelenti, hogy alkalmas u-val az 1 és $a_1 u$ elemek ugyanabba a (b_1) szerinti maradékosztályba esnek. Ezt kell tehát belátnunk.

Vegyünk a (b_1) szerinti véges sok maradékosztály mindegyikéből egy-egy elemet (azaz egy teljes maradékrendszert modulo b_1), legyen ez $r_1, \ldots, r_n$. Megmutatjuk, hogy ekkor $a_1 r_1, \ldots, a_1 r_n$ is teljes maradékrendszer modulo b_1.

Ha $a_1 r_i$ és $a_1 r_j$ ugyanabba a (b_1) szerinti maradékosztályba esnek, akkor $a_1 r_i - a_1 r_j \in (b_1)$, azaz $b_1 \mid a_1(r_i - r_j)$. Mivel a_1 és b_1 relatív prímek, ezért a számelmélet alaptételéből következik, hogy ekkor $b_1 \mid r_i - r_j$. Ez azt jelenti, hogy $r_i - r_j \in (b_1)$, vagyis $i = j$.

Ezzel igazoltuk, hogy az $a_1 r_1, \ldots, a_1 r_n$ elemek különböző maradékosztályokba esnek, és így valóban minden maradékosztályt reprezentálnak. Ebből speciálisan az is következik, hogy van olyan i, amelyre $a_1 r_i$ ugyanabba a maradékosztályba esik, mint az 1, és ezt kellett igazolni.

• **11.3.10** A megadott öt t érték esetén $E(\sqrt{t})$-ben a norma szerint elvégezhető a maradékos osztás, ennek igazolását a 10.3.4 feladathoz adott útmutatásban vázoltuk.

A megfordításhoz tegyük fel, hogy $E(\sqrt{t})$ euklideszi gyűrű. Nyilván elég a $t < -3$ esettel foglalkozni, ekkor a ± 1-en kívül nincs más egység $E(\sqrt{t})$-ben.

Legyen β egy olyan, a 0-tól és az egységektől (azaz ±1-től) különböző elem, amelyre $f(\beta)$ (az $f(0)=0$ és az $f(\pm1)$ értékektől eltekintve) a legkisebb.

A β kiválasztásából következik, hogy bármely $\xi \in E(\sqrt{t})$ elemet β-val maradékosan osztva a maradék csak 0 vagy ±1 lehet. Ez más megfogalmazásban azt jelenti, hogy bármely ξ esetén ξ, $\xi+1$ vagy $\xi-1$ osztható β-val.

Speciálisan, ha $\xi=2$, akkor azt kapjuk, hogy $\beta \mid 2$ vagy $\beta \mid 3$ vagy $\beta \mid 1$. Az utolsó eset nem fordulhat elő, hiszen $\beta \neq \pm1$.

Ha $\beta \mid 2$, akkor $N(\beta) \mid N(2)=4$, azaz [$N(\beta)\neq 1$ miatt] $N(\beta)=2$ vagy $N(\beta)=4$. Belátjuk, hogy csak $N(\beta)=2$ lehetséges.

A $N(\beta)=4$ feltétel (a $\beta \mid 2$ oszthatósággal együtt) azt jelenti, hogy a β a 2 egységszerese. Ennek az eshetőségnek a kizárásához így elég egy olyan ξ-t mutatni, amelyre a 2 a ξ, $\xi+1$ és $\xi-1$ elemek egyikének sem osztója.

Ha $t \not\equiv 1 \pmod 4$, akkor $\xi=\sqrt{t}$, ha pedig $t\equiv 1 \pmod 4$, akkor $\xi=(1+\sqrt{t})/2$ nyilván ilyen tulajdonságú. (Felhasználtuk az $E(\sqrt{t})$ elemeinek előállítására vonatkozó 10.3.2 Tételt.)

Ezzel megmutattuk, hogy ha $\beta \mid 2$, akkor $N(\beta)=2$. Teljesen hasonlóan kapjuk, hogy a $\beta \mid 3$ esetben $N(\beta)=3$.

Legyen először $t\not\equiv 1 \pmod 4$. Ekkor $\beta=c+d\sqrt{t}$, ahol c és d egész. Mivel $N(\beta)$ nem négyzetszám, ezért $d\neq 0$, és így

$$3 \geq N(\beta)=c^2+|t|\cdot d^2 \geq 0+|t|\cdot 1=|t|, \qquad \text{azaz} \qquad t\geq -3,$$

amit kizártunk.

Ha $t\equiv 1 \pmod 4$, akkor $\beta=c+d(1+\sqrt{t})/2$ alakú, ahol c és d egész. Most is $d\neq 0$, és így

$$3 \geq N(\beta)=\Big(c+\frac{d}{2}\Big)^2+|t|\cdot\frac{d^2}{4} \geq \frac{1+|t|}{4}, \qquad \text{azaz} \qquad t\geq -11,$$

vagyis ($t<-3$-at és $t\equiv 1 \pmod 4$-et figyelembe véve) $t=-7$ vagy $t=-11$, amint állítottuk.

• **11.4.8 a)** Az alábbi két tényt többször is fel fogjuk használni:

(i) $E(\sqrt{-5})$ ideáljaira teljesül az oszthatóság és a fordított irányú tartalmazás ekvivalenciája, ezért elég azt megvizsgálnunk, hogy a megadott ideálokat mely ideálok tartalmazzák.

(ii) $-5\equiv 3 \pmod 4$, ezért a 10.3.2 Tétel szerint $E(\sqrt{-5})$ elemei $u+v\sqrt{-5}$ alakúak, ahol u és v egész számok.

• a1) Először megmutatjuk, hogy

$$a+b\sqrt{-5}\in(2,\,1+\sqrt{-5}) \iff a\equiv b \pmod 2. \qquad (*)$$

(Ennek a feladatnak a megoldásánál számok helyett más jeleket használunk a képletszámozáshoz, annak érdekében, hogy mondjuk a (2) főideál és a (2) képlet azonos jelölése ne okozhasson zavart.)

Ha a és b páros, akkor

$$a+b\sqrt{-5}=2\Big[\frac{a}{2}+\frac{b}{2}\sqrt{-5}\Big]\in(2)\subseteq(2,\,1+\sqrt{-5})\,,$$

ha pedig a és b páratlan, akkor

$$a+b\sqrt{-5}=2\Big[\frac{a-1}{2}+\frac{b-1}{2}\sqrt{-5}\Big]+\big[1+\sqrt{-5}\,\big]\in(2,\,1+\sqrt{-5})\,.$$

Tegyük fel megfordítva, hogy $a+b\sqrt{-5}\in(2,\,1+\sqrt{-5})$, azaz alkalmas $\alpha,\,\beta\in E(\sqrt{-5})$ elemekkel

$$a+b\sqrt{-5}=2\alpha+\big[1+\sqrt{-5}\,\big]\beta. \qquad (+)$$

A $(+)$ egyenlőséget $1-\sqrt{-5}$-tel beszorozva kapjuk, hogy

$$\big[a+b\sqrt{-5}\,\big]\big[1-\sqrt{-5}\,\big]=2\big[1-\sqrt{-5}\,\big]\alpha+6\beta.$$

Ebből következik, hogy

$$2\,\Big|\,\big[a+b\sqrt{-5}\,\big]\big[1-\sqrt{-5}\,\big]=[a+5b]+[b-a]\sqrt{-5}.$$

Ez azt jelenti, hogy $a+5b$ és $b-a$ páros szám, vagyis a és b azonos paritású.

Ezzel $(*)$-ot beláttuk.

Térjünk rá most az $I=(2,\,1+\sqrt{-5})$ ideál osztóira. Nyilván $I\mid I$ és $(1)\mid I$. Megmutatjuk, hogy I-nek nincs több osztója (vagyis I felbonthatatlan ideál, és így prímideál).

Tegyük fel, hogy egy A ideálra $A\mid I$ és $A\neq I$. Ekkor $I\subset A$ szigorú tartalmazással. Azt kell igazolnunk, hogy $A=(1)$, azaz $1\in A$.

Legyen $c+d\sqrt{-5}\in A\setminus I$. Ekkor $(*)$ miatt c és d különböző paritású.

Ha c páratlan és d páros, akkor ismét $(*)$ alapján kapjuk, hogy

$$c-1+d\sqrt{-5}\in I\subset A,$$

és így

$$1=\big[c+d\sqrt{-5}\,\big]-\big[c-1+d\sqrt{-5}\,\big]\in A.$$

Ha d páratlan és c páros, akkor hasonló módon adódik, hogy

$$\sqrt{-5} = \big[c + d\sqrt{-5}\,\big] - \big[c + [d-1]\sqrt{-5}\big] \in A,$$

és így

$$1 = \big[\sqrt{-5}\,\big]\big[\sqrt{-5}\,\big] + 3 \cdot 2 \in A.$$

• a2) A (2) főideálnak nyilván osztója önmaga és az (1) ideál. Emellett $(*)$ alapján a $(2,\, 1+\sqrt{-5})$ ideál egy nemtriviális osztó. Megmutatjuk, hogy (2)-nek nincs több osztója.

Tegyük fel, hogy egy B ideálra $B \mid (2)$ és $B \neq (2)$. Ekkor $(2) \subset B$ szigorú tartalmazással.

Legyen $u + v\sqrt{-5} \in B \setminus (2)$.

Ha u páratlan és v páros, akkor $u - 1 + v\sqrt{-5} \in (2)$, és így

$$1 = \big[u + v\sqrt{-5}\,\big] - \big[u - 1 + v\sqrt{-5}\,\big] \in B, \qquad \text{tehát} \qquad B = (1).$$

Ha u páros és v páratlan, akkor hasonló módon adódik, hogy

$$\sqrt{-5} = \big[u + v\sqrt{-5}\big] - \big[u + [v-1]\sqrt{-5}\big] \in B,$$

amiből ismét

$$1 = \big[\sqrt{-5}\,\big]\big[\sqrt{-5}\,\big] + 3 \cdot 2 \in B, \qquad \text{azaz} \qquad B = (1)$$

következik.

Végül, ha u és v is páratlan, akkor

$$1 + \sqrt{-5} = \big[u + v\sqrt{-5}\,\big] - 2\Big[\frac{u-1}{2} + \frac{v-1}{2}\sqrt{-5}\Big] \in B.$$

Ez azt jelenti, hogy $(2,\, 1+\sqrt{-5}) \subseteq B$, amiből az a1) rész felhasználásával következik, hogy $B = (2,\, 1+\sqrt{-5})$ vagy $B = (1)$.

• a3) Megmutatjuk, hogy az $(1+\sqrt{-5})$ főideálnak az alábbi négy (különböző) osztója van:

$$(1), \qquad (1+\sqrt{-5}), \qquad (2,\, 1+\sqrt{-5}) \qquad \text{és} \qquad (3,\, 1+\sqrt{-5}).$$

Ezek valamennyien osztók, hiszen tartalmazzák az $(1+\sqrt{-5})$ főideált.

A $(2,\, 1+\sqrt{-5})$ ideál nemtriviális osztó, ugyanis egyrészt

$$1 + \sqrt{-5} \not\mid 2 \Longrightarrow (2,\, 1+\sqrt{-5}) \neq (1+\sqrt{-5}),$$

másrészt az a1)-beli $(*)$ képlet szerint $(2,\, 1+\sqrt{-5}) \neq (1)$.

Ugyanígy adódik, hogy $(3,\, 1+\sqrt{-5})$ is nemtriviális osztó, ekkor $(*)$ helyett a hasonló módon igazolható

$$a+b\sqrt{-5}\in(3,\,1+\sqrt{-5}) \iff a\equiv b \pmod 3 \qquad (**)$$

összefüggést érdemes felhasználni.

Végül (például) $(*)$-ból és $(**)$-ból kapjuk, hogy

$$(2,\,1+\sqrt{-5})\neq(3,\,1+\sqrt{-5})\,.$$

Most belátjuk, hogy ha a C ideál osztója az $(1+\sqrt{-5})$ főideálnak, akkor C a fenti négy ideál valamelyikével egyenlő.

Tegyük fel, hogy $C\mid(1+\sqrt{-5})$ és $C\neq(1+\sqrt{-5})$, ekkor $(1+\sqrt{-5})\subset C$ szigorú tartalmazással. Legyen

$$r+s\sqrt{-5}\in C\setminus(1+\sqrt{-5}). \qquad (\nabla)$$

Ekkor egyrészt

$$r-s=\big[r+s\sqrt{-5}\,\big]-s\big[1+\sqrt{-5}\,\big]\in C, \qquad (\flat)$$

másrészt

$$6=\big[1+\sqrt{-5}\,\big]\big[1-\sqrt{-5}\,\big]\in(1+\sqrt{-5})\subset C. \qquad (\sharp)$$

Jelöljük d-vel a 6 és $r-s$ egész számok legnagyobb közös osztóját. Ekkor alkalmas t és w egész számokra $d=6t+[r-s]w$, és így $(\flat)$ és $(\sharp)$ alapján $d\in C$.

Ha $d=1$, akkor $1\in C$, tehát $C=(1)$.

Ha $d=2$, akkor $2\in C$, és így $(2,\,1+\sqrt{-5})\subseteq C$. Az a1) rész alapján ebből következik, hogy $C=(2,\,1+\sqrt{-5})$ vagy $C=(1)$.

Ha $d=3$, akkor $3\in C$, és így $(3,\,1+\sqrt{-5})\subseteq C$. Az a1) részhez hasonlóan, $(**)$ felhasználásával könnyen igazolható, hogy ekkor $C=(3,\,1+\sqrt{-5})$ vagy $C=(1)$.

Végül belátjuk, hogy $d\neq 6$. Ha ugyanis $d=6$, azaz $6\mid r-s$, akkor

$$r+s\sqrt{-5}=[r-s]+s\big[1+\sqrt{-5}\,\big]\in(1+\sqrt{-5}),$$

ami ellentmond (∇)-nak.

• **11.4.9 a)** Az állítás hamis, például $E(\sqrt{-5})$-ben a 2 felbonthatatlan elem, azonban a (2) nem felbonthatatlan ideál.

• **b)** Az állítás igaz. A feltétel alapján α nem lehet egység vagy 0. Tegyük fel, hogy $\alpha = \beta\gamma$. Ekkor $(\alpha) = (\beta)(\gamma)$, és így (α) felbonthatatlansága miatt $(\beta) = (1)$ vagy $(\gamma) = (1)$, azaz β vagy γ egység.

• **c)** és **d)** Mindkét állítás igaz. Mivel

$$(\alpha) \neq (0) \iff \alpha \neq 0 \qquad \text{és} \qquad (\alpha) \neq (1) \iff \alpha \text{ nem egység},$$

ezért a továbbiakban feltehetjük, hogy (α) nemtriviális ideál.

Felhasználjuk az oszthatóság és a fordított irányú tartalmazás ekvivalenciáját. Ennek megfelelően

$$\begin{aligned}(\alpha) \text{ prímideál} &\iff \big[\, \beta\gamma \in (\alpha) \Longrightarrow \beta \in (\alpha) \text{ vagy } \gamma \in (\alpha) \,\big] \iff \\ &\iff \big[\, \alpha \mid \beta\gamma \Longrightarrow \alpha \mid \beta \text{ vagy } \alpha \mid \gamma \,\big] \iff \alpha \text{ prímelem.}\end{aligned}$$

• **11.5.7 c)** Megmutatjuk, hogy egy $p > 0$ prímszámhoz akkor és csak akkor található olyan a egész szám, amelyre a $(p,\ a + \sqrt{-5})$ ideál prímideál, ha $p = 2$, $p = 5$, vagy pedig p a 20-szal osztva 1, 3, 7, illetve 9 maradékot ad.

• Először azt igazoljuk, hogy a felsorolt p értékek valóban rendelkeznek az előírt tulajdonsággal.

• A $p = 2$ esetben $a = 1$ megfelel: $I_2 = (2,\ 1 + \sqrt{-5})$ prímideál (lásd a 11.4.8 feladatot).

• A $p = 5$ esetben $a = 0$ megfelel: $I_5 = (5,\ \sqrt{-5}) = (\sqrt{-5})$ prímideál. Ez a 11.4.9c–d feladat alapján azzal ekvivalens, hogy $\sqrt{-5}$ prímelem $E(\sqrt{-5})$-ben. Így azt kell igazolnunk, hogy

$$\sqrt{-5} \,\Big|\, \big[a+b\sqrt{-5}\,\big]\big[c+d\sqrt{-5}\,\big] \Rightarrow \sqrt{-5} \,\Big|\, a+b\sqrt{-5} \text{ vagy } \sqrt{-5} \,\Big|\, c+d\sqrt{-5}\,. \quad (2)$$

Mivel $\sqrt{-5}$ önmagának osztója, ezért (2) ekvivalens az alábbi feltétel teljesülésével:

$$\sqrt{-5} \,\Big|\, ac \Longrightarrow \sqrt{-5} \,\Big|\, a \quad \text{vagy} \quad \sqrt{-5} \,\Big|\, c\,. \quad (3)$$

Egy egész szám könnyen láthatóan pontosan akkor osztható $\sqrt{-5}$-tel, ha 5-tel osztható, tehát (3) átírható a következő alakba:

$$5 \mid ac \Longrightarrow 5 \mid a \quad \text{vagy} \quad 5 \mid c\,. \quad (4)$$

Az 5 az egész számok körében prím, ezért (4), és így (2) is valóban teljesül. (Célhoz érhettünk volna a 10.3.7b feladat felhasználásával is.)

• Legyen most p egy $20k+1$, $20k+3$, $20k+7$ vagy $20k+9$ alakú pozitív prímszám. A Legendre-szimbólum tulajdonságainak a felhasználásával könnyen adódik, hogy ezek éppen azok a prímek, amelyekre $\left(\frac{-5}{p}\right) = 1$. Ez azt jelenti, hogy az

$$x^2 \equiv -5 \pmod{p}$$

kongruencia megoldható, vagyis létezik olyan a egész szám, amelyre

$$p \mid a^2 + 5. \tag{5}$$

Megmutatjuk, hogy az $I_p = (p,\, a + \sqrt{-5})$ ideál felbonthatatlan ideál, és így prímideál. Ehhez azt kell igazolni, hogy $I_p \neq (1)$, $I_p \neq (0)$, továbbá I_p csak triviális módon bontható két ideál szorzatára. Ez utóbbi teljesüléséhez a 11.4.6 Definíció után adott ekvivalens átfogalmazások szerint elég azt belátni, hogy bármely A ideálra

$$I_p \subseteq A \subseteq E(\sqrt{-5}) \Longrightarrow A = I_p \quad \text{vagy} \quad A = E(\sqrt{-5})\,. \tag{6}$$

Nyilván $I_p \neq (0)$.

Ha $I_p = (1)$ teljesülne, akkor alkalmas $\alpha,\ \beta \in E(\sqrt{-5})$ elemekkel az 1 előállna

$$1 = \alpha p + \beta\big[a + \sqrt{-5}\,\big] \tag{7}$$

alakban. A (7) egyenlőséget $a - \sqrt{-5}$-tel beszorozva kapjuk, hogy

$$a - \sqrt{-5} = \alpha\big[a - \sqrt{-5}\,\big]p + \beta[a^2 + 5]\,. \tag{8}$$

Mivel (5) alapján (8) jobb oldala osztható p-vel, ezért a bal oldal is, vagyis

$$\frac{a}{p} - \frac{1}{p}\sqrt{-5} \in E(\sqrt{-5})\,,$$

ami nyilván lehetetlen. Ezzel beláttuk, hogy $I_p \neq (1)$.

A (6) tulajdonság igazolásához tegyük fel, hogy egy A ideál valódi módon tartalmazza az I_p ideált. Megmutatjuk, hogy $1 \in A$, azaz $A = E(\sqrt{-5})$.

Vegyünk egy tetszőleges

$$c + d\sqrt{-5} \in A \setminus I_p \tag{9}$$

elemet. Ekkor

$$\big[c + d\sqrt{-5}\,\big] - d\big[a + \sqrt{-5}\,\big] = c - da \in A. \tag{10}$$

Ha $p \mid c - da$, azaz alkalmas u egész számmal

$$c = da + up, \qquad \text{akkor} \qquad c + d\sqrt{-5} = d\big[a + \sqrt{-5}\,\big] + up \in I_p\,,$$

ami ellentmond (9)-nek.

Ebből következik, hogy $c-da$ nem lehet osztható a p prímszámmal, vagyis $c - da$ és p (az egész számok körében) relatív prímek. Ekkor alkalmas v és w egész számokkal

$$1 = v[c - da] + wp\,. \tag{11}$$

Mivel $p \in A$ és (10) alapján $c - da \in A$, ezért (11) szerint $1 \in A$, amint állítottuk.

• Most megmutatjuk, hogy a felsorolásból kimaradt, azaz a $20k+11$, $20k+13$, $20k + 17$ és $20k + 19$ alakú (pozitív) p prímszámokhoz nem található olyan a egész szám, amelyre $(p,\, a + \sqrt{-5})$ prímideál.

Ezekre a p prímszámokra $\left(\frac{-5}{p}\right) = -1$, és így a 10.3.7 Tétel alapján ezek a p értékek $E(\sqrt{-5})$-ben is prímek. A 11.4.9c feladat szerint ekkor (p) prímideál.

Tegyük fel indirekt, hogy alkalmas a egész számra $(p,\, a+\sqrt{-5})$ prímideál lenne. Mivel

$$(p) \subseteq (p,\, a + \sqrt{-5}), \qquad \text{és így} \qquad (p,\, a + \sqrt{-5}) \,\Big|\, (p)\,,$$

továbbá $(p,\, a + \sqrt{-5})$ és (p) is prímideál, ezért csak $(p,\, a + \sqrt{-5}) = (p)$ lehetséges. Ez azt jelenti, hogy $a + \sqrt{-5} \in (p)$, és így

$$p \mid a + \sqrt{-5}, \qquad \text{azaz} \qquad \frac{a}{p} + \frac{1}{p}\sqrt{-5} \in E(\sqrt{-5}),$$

ami lehetetlen.

• **11.5.9** Előrebocsátjuk, hogy a 11.5.1 Tétel érvényes marad akkor is, ha algebrai egész helyett mindenhol egész számot írunk. Ez abból következik, hogy ha u és v egész számok, akkor az $u \mid v$ oszthatóság pontosan akkor teljesül az algebrai egészek körében, mint amikor az egész számok körében. Tekintsük ugyanis az $uw = v$ egyenlőséget. Ha w egész szám, akkor nyilván w algebrai egész is. Megfordítva, ha w algebrai egész, akkor mivel ($u \neq 0$ esetén) $w = v/u$ racionális is, ezért w szükségképpen egész szám.

A továbbiakban a 11.5.1 Tételnek ezt az egész számokra vonatkozó speciális esetét fogjuk használni.

• **a)** Legyen a két primitív polinom

$$f(x) = a_0 + a_1x + \ldots + a_mx^m \qquad \text{és} \qquad g(x) = b_0 + b_1x + \ldots + b_nx^n\,,$$

és a szorzatuk

$$f(x)g(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}\,.$$

Tegyük fel indirekt, hogy $f(x)g(x)$ nem primitív polinom, azaz létezik olyan p prímszám, amelyre

$$p \mid k, \qquad k = 0, 1, \ldots, m+n.$$

Ekkor a 11.5.1 Tétel (fent jelzett speciális esete) szerint

$$p \mid a_ib_j, \qquad i = 0, 1, \ldots, m, \qquad j = 0, 1, \ldots, n.$$

Mivel f és g is primitív polinom, ezért van olyan i, illetve j, amelyre

$$p \nmid a_i \qquad \text{és} \qquad p \nmid b_j\,.$$

Ebből p prímtulajdonsága szerint következik, hogy $p \nmid a_ib_j$, ami ellentmondás.

• **b)** Legyen az F, illetve G polinomban az együtthatók nevezőinek legkisebb közös többszöröse r, illetve s. A $H = FG$ egyenlőséget $t = rs$-sel beszorozva kapjuk, hogy

$$tH(x) = F_2(x)G_2(x), \qquad \text{ahol} \qquad F_2(x),\, G_2(x) \in \mathbf{Z}[x]\,. \tag{12}$$

Ha $t = 1$, akkor készen vagyunk. Ha $t > 1$, akkor legyen p a t egy tetszőleges prímosztója. Ekkor p osztója az $F_2(x)G_2(x)$ polinom minden együtthatójának.

Ha p nem osztója sem az $F_2(x)$ polinom minden együtthatójának, sem pedig $G_2(x)$ minden együtthatójának, akkor az a) részben látott módon ellentmondásba kerülünk a 11.5.1 Tétellel. Így p osztója mondjuk $F_2(x)$ minden együtthatójának, $F_2(x) = pF_3(x)$.

A (12) egyenletet p-vel egyszerűsítve

$$t_1H(x) = F_3(x)G_2(x), \qquad F_3(x),\, G_2(x) \in \mathbf{Z}[x], \qquad t_1 = \frac{t}{p}$$

adódik. Ha $t_1 = 1$, akkor készen vagyunk, egyébként ismételjük meg az eljárást mindaddig, amíg a H polinom egy kívánt előállítását kapjuk.

• **11.6.3 a)** Mivel k és h relatív prímek, ezért léteznek olyan u és v pozitív egészek, amelyekre $ku = 1 + hv$. Ekkor

$$A^k \sim B^k \Longrightarrow A^{ku} \sim B^{ku}\,,$$

azaz alkalmas (α) és (β) nemnulla főideálokra

$$(\alpha)A^{ku} = (\beta)B^{ku}\,. \tag{13}$$

Írjuk be (13)-ban A^{ku}, illetve B^{ku} helyére az AA^{hv}, illetve BB^{hv} előállítást, és használjuk fel, hogy A^{hv} és B^{hv} főideál, legyen $A^{hv} = (\gamma)$, $B^{hv} = (\delta)$. Innen kapjuk, hogy

$$(\alpha\gamma)A = (\beta\delta)B, \qquad \text{azaz} \qquad A \sim B.$$

• **b)** Az a) részt speciálisan $B = (1)$-ra alkalmazva $A \sim (1)$ adódik, és így a 11.6.2/(iv) Tétel alapján A főideál.

• **11.6.4 d)** Megmutatjuk, hogy az $x^2 + 35 = y^3$ diofantikus egyenlet összes megoldása $x = \pm 36,\ y = 11$.

A 11.6.5 Tétel bizonyításának a gondolatmenetét követjük. Fel fogjuk használni, hogy $E(\sqrt{-35})$-ben az ideálosztályok száma $h(\sqrt{-35}) = 2$ (lásd a 11.6.4 Tétel előtt megadott táblázatot). Ebből az is következik, hogy $E(\sqrt{-35})$-ben nem érvényes a számelmélet alaptétele.

Az egyenlet bal oldalát $E(\sqrt{-35})$-ben szorzattá bontjuk:

$$\big[x + \sqrt{-35}\,\big]\big[x - \sqrt{-35}\,\big] = y^3\,. \tag{14}$$

Mivel $E(\sqrt{-35})$-ben nem érvényes a számelmélet alaptétele, ezért (14)-ről át kell térni a megfelelő főideálok közötti egyenletre:

$$(x + \sqrt{-35})(x - \sqrt{-35}) = (y)^3\,. \tag{15}$$

Megmutatjuk, hogy az $(x + \sqrt{-35})$ és $(x - \sqrt{-35})$ ideálok relatív prímek. Tegyük fel indirekt, hogy van egy P prímideál közös osztójuk. Ekkor P osztója $(y)^3$-nak is, és mivel P prímideál, ezért (y)-nak is. Az oszthatóságoknak megfelelő tartalmazások alapján

$$x + \sqrt{-35} \in P, \qquad x - \sqrt{-35} \in P \qquad \text{és} \qquad y \in P.$$

Ekkor

$$\sqrt{-35}\big[[x - \sqrt{-35}\,] - [x + \sqrt{-35}\,]\big] = 2 \cdot 35 = 70 \in P$$

is igaz.

Megmutatjuk, hogy y és 70 relatív prímek (az egész számok körében).

Ha $7 \mid y$, akkor az eredeti egyenletből kapjuk, hogy x is osztható 7-tel, ekkor azonban a 7-nek x^2+35 pontosan az első, y^3 viszont legalább a harmadik hatványával osztható, ami lehetetlen.

Ugyanígy kapjuk, hogy $5 \nmid y$.

Ha $2 \mid y$, akkor x páratlan, és az egyenlet bal oldala 4, a jobb oldala viszont 0 maradékot ad 8-cal osztva, ami szintén lehetetlen.

Ezzel beláttuk, hogy y és 70 relatív prímek. Ekkor alkalmas r és s egész számokra $1 = yr + 70s$. Mivel 70 és y is eleme P-nek, ezért az 1 is eleme P-nek, azaz $P = (1)$, ami ellentmond annak, hogy P prímideál.

Így a (15) egyenlőség bal oldalán szereplő két (fő)ideál valóban relatív prím. Az ideálokra vonatkozó egyértelmű prímfaktorizációból (11.5.8 Tétel) következik, hogy mindkét ideál egy alkalmas ideál köbe, azaz (például)

$$(x + \sqrt{-35}) = A^3 \,. \tag{16}$$

Mivel $E(\sqrt{-35})$-ben az ideálosztályok száma $h(\sqrt{-35}) = 2$, ezért a 11.6.4 Tétel szerint A^2 főideál, $A^2 = (\gamma)$. Ezt a (16) egyenlőségbe beírva

$$(x + \sqrt{-35}) = (\gamma)A$$

adódik, amiből a 11.4.3b feladat alapján kapjuk, hogy A főideál, azaz $A = (\alpha)$. Ekkor (16) átírható az

$$(x + \sqrt{-35}) = (\alpha^3), \qquad \text{azaz} \qquad x + \sqrt{-35} = \varepsilon\alpha^3 \tag{17}$$

alakba, ahol ε egység $E(\sqrt{-35})$-ben. Az $E(\sqrt{-35})$ egységei csak a ± 1, és ezek maguk is köbszámok. Ezért (17) tovább ekvivalens azzal, hogy

$$x + \sqrt{-35} = \beta^3 = \left[a + b\sqrt{-35}\,\right]^3 , \tag{18}$$

ahol $-35 \equiv 1 \pmod 4$ miatt a és b egész számok vagy pedig $a = u/2$ és $v = b/2$, ahol u és v páratlan egészek.

A köbre emelést elvégezve és a képzetes részeket összehasonlítva

$$1 = 3a^2b - 35b^3 = b[3a^2 - 35b^2] \tag{19}$$

adódik.

Ha a és b egész számok, akkor innen $b = \pm 1$, azonban a-ra nem kapunk egész értéket.

Ha $a = u/2$ és $v = b/2$, ahol u és v páratlan, akkor (19)-et 8-cal szorozva adódik, hogy

$$8 = v[3u^2 - 35v^2].$$

Mivel v páratlan, ezért

$$v = \pm 1 \qquad \text{és} \qquad 3u^2 - 35v^2 = 3u^2 - 35 = \pm 8.$$

Innen $u = \pm 3$ és $v = -1$. Ezeket az értékeket (18)-ba visszahelyettesítve és a valós részeket összehasonlítva kapjuk, hogy

$$x = \frac{u[u^2 - 105v^2]}{8} = \mp 36 \qquad \text{és} \qquad y = \sqrt[3]{x^2 + 35} = 11.$$

12. Kombinatorikus számelmélet

• **12.1.3** Először egy konstrukciót adunk arra, hogy a megoldásszám elérheti $\lceil k/2 \rceil$-t. Legyen $k = 2j - 1$ vagy $2j$, ekkor $\lceil k/2 \rceil = j$. Az útmutatásban javasoltaknak megfelelően legyen

$$q > j, \;\; a_1 = q + 1, a_2 = q + 2, \ldots, a_j = q + j \text{ és } t = a_1 + a_2 + \ldots + a_j.$$

Ezután legyen $a_{j+1} = a_1 + a_2$, ekkor

$$t = a_3 + a_4 + \ldots + a_j + a_{j+1}$$

is igaz. Hasonlóan folytatva legyen $a_{j+2} = a_3 + a_4$, ekkor a

$$t = a_5 + a_6 + \ldots + a_{j+1} + a_{j+2}$$

előállítás is érvényes.

Általában legyen $a_{j+r} = a_{2r-1} + a_{2r}$, ha $r \leq j-1$ (és $k = 2j$ esetén legyen a_{2j} tetszőleges, a_{2j-1}-nél nagyobb szám). Ekkor

$$t = a_{2r+1} + a_{2r+2} + \ldots + a_{j+r}.$$

Ily módon $a_s < a_{s+1}$ minden s esetén fennáll: $s < j$-re az a_s-eket így választottuk, $s = j$-re $a_{j+1} = a_1 + a_2 = 2q + 3 > a_j = q + j$ (hiszen $q > j$), $j < s \leq 2j - 2$-re pedig a_{s+1} mindig két későbbi a_i-nek az összege, mint a_s.

Az eljárást végigvíve t előáll j, $j-1$, ... szomszédos a_i összegeként, míg végül egytagú összegként is megjelenik, ami összesen a kívánt j számú előállítás.

Most megmutatjuk, hogy ennél nagyobb előállításszám nem lehetséges. Vegyünk egy tetszőleges $a_1, \ldots, a_k$ rendszert és egy t számot, és tekintsük t-nek azt az előállítását, amelyben az utolsó (azaz a legnagyobb) tag a lehető legkisebb, legyen az indexe v.

Ha $v > j$, akkor legfeljebb $k-(v-1) \le k-j \le j$ előállítás lehetséges, hiszen mindegyiknek szükségképpen más az utolsó tagja.

Ha $v \le j$, akkor mivel minden előállítás tagszáma más és minden tagszám legfeljebb v, tehát legfeljebb $v \le j$ előállítás lehetséges.

• **12.2.3** Tekintsük a p^2 elemű T_2 véges testet és ebben a p elemű T_1 résztestet. Mivel egy véges test multiplikatív csoportja ciklikus, így van T_2-nek olyan Δ eleme, amelynek a hatványai T_2 minden nemnulla elemét előállítják.

Vegyünk egy tetszőleges $\Theta \in T_2 \setminus T_1$ elemet, és legyenek T_1 elemei $\gamma_1, \ldots, \gamma_p$. Írjuk fel a $\Theta+\gamma_i$ elemeket $\Theta+\gamma_i = \Delta^{a_i}$ alakban, ezzel kijelöltünk p darab a_i egész számot 1 és p^2-1 között.

Megmutatjuk, hogy ezek eleget tesznek a feltételnek, azaz az $a_i + a_j$ összegek páronként különböző maradékot adnak modulo p^2-1.

Tegyük fel, hogy $a_i + a_j \equiv a_k + a_l \pmod{p^2-1}$. Ekkor az a_i-k definíciója alapján $(\Theta+\gamma_i)(\Theta+\gamma_j) - (\Theta+\gamma_k)(\Theta+\gamma_l) = 0$ adódik. A bal oldal Θ-nak legfeljebb elsőfokú polinomja T_1-beli együtthatókkal, hiszen Θ^2 kiesik. Elsőfokú azonban nem lehet, mert akkor $\Theta \in T_1$ következne, így — mivel a Θ gyöke — csak az azonosan nulla polinom lehet. Ekkor azonban pl. a polinomok gyöktényezős alakjának az egyértelműsége miatt $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$, és így ugyanez áll az a_i-kre is, ami éppen a bizonyítandó állítás volt.

• **12.2.4** Az útmutatást követve vegyünk egy g primitív gyököt modulo p, és legyen a_i az $x \equiv i \pmod{p-1}$, $x \equiv g^i \pmod{p}$ szimultán kongruenciarendszer megoldása modulo $p(p-1)$, $i = 1, 2, \ldots, p-1$. Nyilván elég azt megmutatnunk, hogy bármely c-re a $c \equiv a_i + a_j \pmod{p(p-1)}$ kongruencia legfeljebb egyetlen $\{i, j\}$-vel teljesülhet. Az a_i definíciója alapján ez a kongruencia a $c \equiv i + j \pmod{p-1}$, $c \equiv g^i + g^j \pmod{p}$ szimultán kongruenciarendszerrel ekvivalens. Itt az első kongruencia átírható a $g^c \equiv g^i g^j \pmod{p}$ alakba, vagyis a g^i és g^j számok összegét és szorzatát is ismerjük modulo p. A gyökök és együtthatók közötti összefüggés alapján a g^i és g^j maradékosztályok a $z^2 - cz + g^c \equiv 0 \pmod{p}$ másodfokú kongruencia egyértelműen meghatározott gyökei (p prím), és így i és j is egyértelmű.

• **12.3.6** Az útmutatást követve legyen $|C| = |D| = n < p$, $C = \{c_1, \ldots, c_n\}$, $A_1 = \ldots = A_n = D$ és

$$F(x_1, \ldots, x_n) = \prod_{1 \le j < i \le n} (x_i - x_j)(x_i + c_i - x_j - c_j).$$

Ekkor F foka $n(n-1)$, így ha $\prod_{i=1}^n x_i^{n-1}$ együtthatója nem nulla, akkor a 12.3.5b feladat alapján van olyan $d_1, \ldots, d_n \in D$, amelyre

$$F(d_1, \ldots, d_n) = \prod_{1 \le j < i \le n} (d_i - d_j)(d_i + c_i - d_j - c_j) \neq 0.$$

Ekkor szükségképpen $d_i \neq d_j$, ha $i \neq j$, vagyis $d_1, \ldots, d_n$ kiadják a D összes elemét, továbbá $c_i + d_i \neq c_j + d_j$, ha $i \neq j$, azaz $c_i \longleftrightarrow d_i$ egy megfelelő párba állítás a C és D halmaz elemei között. Most igazoljuk, hogy F-ben a $\prod_{i=1}^n x_i^{n-1}$ tag együtthatója nem nulla. F-ben a $\deg F = n(n-1)$-edfokú tagokat $\prod_{1 \le j < i \le n} (x_i - x_j)^2$ adja (a többi tag ennél alacsonyabb fokú). Ez a rész nem más, mint a

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix}$$

Vandermonde-determináns négyzete. Írjuk fel $V(x_1, \ldots, x_n)$-et a determináns definíciója szerint, és vizsgáljuk meg, mi lesz az önmagával való szorzatában a kérdéses $\prod_{i=1}^n x_i^{n-1}$ tag együtthatója. Ilyen tagot akkor kapunk, ha az egyik determinánsból a

$$(-1)^{I(j_1, \ldots, j_n)} x_1^{j_1} \ldots x_n^{j_n}$$

tagot a másik determináns

$$(-1)^{I(n-1-j_1, \ldots, n-1-j_n)} x_1^{n-1-j_1} \ldots x_n^{n-1-j_n}$$

tagjával szorozzuk össze (ahol $I()$ a megfelelő oszlopindex-permutációk inverziószámát jelöli, az oszlopokat 0-tól $n-1$-ig számoztuk). Mivel az előjelet meghatározó két permutáció éppen egymás „komplementere”, ezért

$$I(j_1, \ldots, j_n) + I(n-1-j, \ldots, n-1-j_n) = \binom{n}{2},$$

vagyis minden ilyen szorzat

$$(-1)^{\binom{n}{2}} x_1^{n-1} \dots x_n^{n-1} .$$

Mivel $n!$ ilyen szorzat képezhető, így F-ben a $\prod_{i=1}^{n} x_i^{n-1}$ tag együtthatója $(-1)^{\binom{n}{2}} n!$, ami $n < p$ miatt valóban nem nulla, amint állítottuk.

• **12.4.11b** Tegyük fel indirekt, hogy az útmutatás szerinti színezésben az $1 \le b < b + d < b + 2d < \dots < b + pd \le p(2^p - 1)$ számok mind azonos színűek. Legyen $\Theta = \Delta^b , \Psi = \Delta^d$. A feltétel szerint ekkor a $\Theta, \Theta\Psi, \dots, \Theta\Psi^p$ „vektorok" vagy valamennyien a W altérbe esnek, vagy pedig egyikük sem esik W-be.

Ha a számtani sorozat piros, akkor tehát ezek a vektorok egy $p-1$-dimenziós altér elemei. Ezért közülük már az első p darab is lineárisan összefüggő, azaz alkalmas $\gamma_i \in \mathbf{Z}_2$ együtthatókkal $\sum_{i=0}^{p-1} \gamma_i (\Theta\Psi^i) = 0$ nemtriviálisan teljesül. Az egyenlőséget Θ-val elosztva azt kapjuk, hogy Ψ gyöke egy p-nél alacsonyabb fokú $\mathbf{Z}_2$ feletti polinomnak. Mivel Ψ foka osztója T fokának, vagyis p-nek, ezért Ψ foka csak 1 lehet, azaz $\Psi \in \mathbf{Z}_2$. Ez azonban ellentmondás, hiszen nyilván $\Psi \ne 0$ és $d < 2^p - 1$ miatt $\Psi \ne 1$.

Ha a számtani sorozat kék, akkor a $\Theta\Psi - \Theta, \Theta\Psi^2 - \Theta\Psi, \dots, \Theta\Psi^p - \Theta\Psi^{p-1}$ vektorokra kell megismételni az előző gondolatmenetet (csak Θ helyett most $\Theta(\Psi - 1)$-gyel kell a megfelelő egyenlőséget elosztani).

• **12.4.12** Az útmutatást követve tekintsük azokat a számokat n-ig, amelyeket a d alapú számrendszerben felírva minden számjegy $< d/2$ és a számjegyek négyzetösszege egy adott q érték. Ha három ilyen szám számtani sorozatot alkot, akkor minden számjegyükre ugyanez áll fenn, mert a jegyekre adott korlátozás miatt két szám összeadása során sohasem képződik átvitel a következő helyiértékre. Így a középső szám valamennyi jegye a másik két szám megfelelő jegyeinek számtani közepe. Felírva, hogy mindhárom szám jegyeinek négyzetösszege q, egyszerű számolással adódik, hogy a számok szükségképpen egyenlők. (Más megfogalmazásban: ha a három számot a számjegyeikből alkotott vektoroknak tekintjük, akkor a harmadik vektor az első kettő összegének a fele, továbbá mindhárom vektor euklideszi normája egyenlő. Ez csak úgy lehet, ha maguk a vektorok is megegyeznek.)

Adott d-re a felírásban szereplő számjegyek száma $u \approx (\log n)/(\log d)$, és q-nak legfeljebb $ud^2/4$-féle értéke lehet. Ha a halmazainkat minden lehetséges q-ra egyesítjük, akkor az összes olyan számot megkapjuk, amelyek valamennyi jegye $d/2$-nél kisebb. Ez összesen kb. $n/2^u$ szám. Ezért biztosan van olyan q, amelynek megfelelő halmaz elemszáma legalább $n/(2^{u-2}ud^2)$. Ez akkor veszi fel a maximumát ha $\log d \approx \sqrt{\log n}$, és ez a maximum éppen a feladat állításában előírt érték.

TÖRTÉNETI NÉVTÁR

A könyv során több helyen kitértünk a számelmélet történetének néhány vonatkozására. A következő összefoglalóban ábécérendben megadjuk a könyvben név szerint említett legtöbb matematikus születési és halálozási évszámát, nemzetiségét, valamint röviden utalunk számelméleti munkásságukra. Ez a kis történeti kitekintés szükségszerűen szubjektív, több okból is. Először is, csak olyan matematikusok szerepelnek benne, akik a számelméletnek a könyvben tárgyalt fejezeteivel kapcsolatba hozhatók, azok történetében szerepet játszottak. Ebből az is következik, hogy a számelmélet sok jelentős kutatója kimaradt. Másodszor, a felsorolt matematikusoknak sem feltétlenül a legjelentősebb eredményeit tudjuk említeni, még kevésbé méltatni, nem beszélve a matematika egyéb területein végzett munkásságukról. Így az alábbi összefoglaló semmiképpen sem tekinthető az adott matematikusok fontosságát, szerepét bemutató elemző értékelésnek, hanem csak olyan válogatásnak, amely a könyvben tárgyalt számelméleti anyaghoz némi történeti hátteret kölcsönöz.

Chevalley, Claude (ejtsd: svalé), 1909–1984, francia. Jelentős eredményeket ért el az algebrai számelméletben.

Csebisev, Pafnutyij Lvovics, 1821–1894, orosz. Elsőként igazolta, hogy $(2 \leq)n$ és $2n$ között mindig található prímszám, és meghatározta az x-nél nem nagyobb prímek számának nagyságrendjét. A valószínűségszámításban fontos szerepet játszó Csebisev-egyenlőtlenség, amelyhez a Hardy–Ramanujan-tétel Turán-féle bizonyítása is kapcsolódik, később a valószínűségszámítás számelméleti alkalmazásainak egyik kiindulópontjává vált.

Dedekind, Richard, 1831–1916, német. A Kummer által bevezetett ideálfogalmat a gyűrűk mind algebrai, mind pedig számelméleti szempontból történő vizsgálatának egyik alapvető eszközévé fejlesztette tovább.

Diophantosz, i.sz. 250 körül élt Alexandriában, görög. Róla nevezték el az olyan (általában) egész együtthatós algebrai egyenleteket, amikor a megoldásokat az egész (esetleg a racionális) számok körében keressük. Az ő nevét őrzi a diofantikus egyenletek vizsgálatában fontos szerepet játszó diofantikus approximáció is.

Dirichlet, Peter Lejeune (ejtsd: dirislé vagy dirichlé), 1805–1859, német. Hatékonyan alkalmazta az analízis módszereit a számelméletben. Bebizonyította azt a később róla elnevezett tételt, hogy ha egy számtani sorozat első eleme és differenciája relatív prímek, akkor a sorozat végtelen sok prímszámot

tartalmaz. A Dirichlet-sorok a számelméleti függvények vizsgálatának ma is fontos eszközei.

Eratoszthenész, i.e. 276?–194?, görög. A számelméletben a prímszámtáblázatok készítésére használt eratoszteneszi szita őrzi a nevét.

Erdős Pál, 1913–1996, magyar. A XX. századi matematika egyik legnagyobb hatású alakja. Már 18 éves korában nemzetközi ismertségre tett szert Csebisev tételére adott egyszerű bizonyításával. A számelmélet területén nevéhez fűződik többek között az ún. véletlen módszerek bevezetése, a kombinatorikus számelmélet számos kérdéskörének és a számelméleti függvények karakterizációjának elindítása.

Euklidész, i.e. 300 körül élt, görög. Elemek című hatalmas munkáján több évezred matematikusai nevelkedtek. Az Elemek 13 könyvéből 3 teljesen számelméleti témájú. Ezekben szerepel többek között a páros tökéletes számok előállítására vonatkozó képlet, valamint annak a bizonyítása, hogy a prímszámok száma végtelen. Nagy számok legnagyobb közös osztójának a meghatározására ma is az euklideszi algoritmust használjuk.

Euler, Leonhard, 1707–1783, svájci. Hatalmas formátumú matematikai polihisztor, az analitikus módszerek mestere. A számelméletben ő vezette be a φ-függvényt, a kis Fermat-tétel általánosításaként felfedezte az Euler–Fermat-tételt, és felépítette a másodfokú kongruenciák elméletét. Megoldotta a Fermat-sejtés köbökre vonatkozó speciális esetét. Megmutatta, hogy a prímszámok reciprokösszege divergens. Jelentős eredményeket ért el a partíciók vizsgálatában.

Fermat, Pierre (ejtsd: fermá), 1601–1665, francia. A modern számelmélet megteremtője (noha „hivatalos” foglalkozását tekintve jogász volt). Híres sejtése több, mint 350 évig megoldatlan maradt, miközben a bizonyítására indított kísérletek számos hatékony, új módszerrel gazdagították a matematikát. Végül Andrew Wiles igazolta a Fermat-sejtést 1994-ben. Fermat nevét őrzi a kongruenciák elméletében alapvető kis Fermat-tétel (amelyet később Euler általánosított), valamint a Fermat-prím fogalma is. Lényegében Fermat oldotta meg először, mely számok állnak elő két négyzetszám összegeként, valamint ő mutatta meg, hogy a Pell-egyenletnek végtelen sok megoldása van.

Gauss, Carl Friedrich, 1777–1855, német. Minden idők talán legnagyobb, legsokoldalúbb matematikusa. 1801-ben jelent meg Disquisitiones arithmeticae c. könyve, amelyben többek között a másodfokú kongruenciák elméletének részletes tárgyalása szerepel. Gauss vezette be a kongruenciáknál ma is használatos jelölésrendszert, valamint a róla elnevezett Gauss-egészeket, amelyek

később mintául szolgáltak az algebrai számtestek vizsgálatához. Gausstól származik a három-négyzetszám-tétel, valamint a szabályos sokszögek euklideszi szerkeszthetőségére vonatkozó tétel is.

Gelfond, Alekszandr Oszipovics, 1906–1968, orosz. Ő és Schneider igazolták (egyidejűleg, de egymástól függetlenül) Hilbertnek azt a sejtését, hogy egy (0-tól és 1-től különböző) algebrai szám irracionális algebrai kitevős hatványa mindig transzcendens.

Goldbach, Christian, 1690–1764, német. Eulerhez írott egyik levelében szerepel a prímszámokra vonatkozó híres Goldbach-sejtés.

Hadamard, Jacques (ejtsd: ádámár), 1865–1963, francia. Ő és de la Vallée Poussin igazolták elsőként (egyidejűleg, de egymástól függetlenül) a prímszámtételt.

Hardy, Geoffrey, 1877–1947, angol. Analitikus módszerek alkalmazásával jelentős eredményeket ért el a prímszámelméletben és az additív számelméletben. Ramanujan felfedezője és munkatársa.

Hermite, Charles (ejtsd: ermit), 1822–1901, francia. Elsőként igazolta 1873-ban, hogy e transzcendens.

Hilbert, David, 1862–1943, német. Az 1900-as párizsi matematikai kongresszuson tartott híres előadásában 23 problémakört vázolt fel, amelyeket a matematikai kutatások szempontjából kiemelkedő fontosságúnak tartott, és ezzel (is) óriási hatást gyakorolt a huszadik század matematikájára. A Hilbert-problémák között több számelméleti is található. Hilbert bizonyította be elsőként a Waring-problémakörben szereplő $g(k)$ létezését.

Jacobi, Carl, 1804–1851, német. A számelméletben a Legendre-szimbólum általánosításaként kapott Jacobi-szimbólum őrzi a nevét.

Kalmár László, 1905–1976, magyar. Kutatási területe elsősorban a matematikai logika volt. Erdős Pállal közösen egyszerű bizonyítást adtak az x-ig terjedő prímszámok számának felső becslésére.

Kőnig Gyula, 1849–1913, magyar. Elsősorban halmazelmélettel foglalkozott. Legérdekesebb számelméleti eredménye a Rados Gusztávval közösen elért Kőnig–Rados-tétel, amely a prím modulusú magasabb fokú kongruenciák megoldhatóságára, illetve megoldásszámára vonatkozik.

Kronecker, Leopold, 1823–1891, német. Az algebrai bővítések ideáljaival kapcsolatban ért el jelentős eredményeket.

Kummer, Ernst, 1810–1893, német. Bevezette az ideálokat, amelyek segítségével jelentős előrehaladást ért el a Fermat-sejtéssel kapcsolatban.

Lagrange, Joseph Louis (ejtsd: lágranzs), 1736–1813, francia. Nevezetes számelméleti munkássága a négy-négyzetszám-tétel első bizonyítása.

Lamé, Gabriel, 1795–1870, francia. Az utókor számára leginkább egy, a Fermat-sejtésre adott hibás bizonyítása által vált híressé.

Legendre, Adrien-Marie (ejtsd: lözsandr), 1752–1833, francia. Nevét őrzi a másodfokú kongruenciáknál szereplő Legendre-szimbólum, valamint az $n!$ kanonikus alakjára vonatkozó Legendre-formula.

Lindemann, Ferdinand, 1852–1939, német. Bebizonyította 1882-ben, hogy π transzcendens, és ezzel lezárta a(z euklideszi értelemben vett) körnégyszögesítés kétezer éves problémáját.

Liouville, Joseph (ejtsd: liuvil), 1809–1882, francia. Elsőként konstruált transzcendens számot. Nagy érdemeket szerzett azzal, hogy (a 21 éves korában párbajban megölt) Galois (ejtsd: galoá) hevenyészett matematikai hagyatékának feldolgozásával felismerte és közkinccsé tette Galois korszakalkotó felfedezéseit.

Lucas, Edouard (ejtsd: lüká), 1842–1891, francia. Hatékony eljárást dolgozott ki a Mersenne-számok prímtesztelésére. A számítógépek ma is ennek a Lehmer által továbbfejlesztett változatát használják nagy Mersenne-prímek kereséséhez.

Mersenne, Marin (ejtsd: merszen), 1588–1648, francia. Kiváló tudományszervező, aki kiterjedt levelezést folytatott Fermat-val, Descartes-tal és a kor számos más kiemelkedő tudósával. A később róla elnevezett prímek elsősorban a tökéletes számokkal való kapcsolatuk miatt érdekelték. Az ilyen prímekről 1644-ben közzétett listája meglepően kevés hibát tartalmaz (a lista ellenőrzésének matematikai és technikai eszközeire több, mint kétszáz évet kellett várni).

Minkowski, Hermann, 1864–1909, német. Nevezetes rácsgeometriai tételével a geometriai számelmélet megteremtője.

Möbius, Ferdinand, 1790–1868, német. Az általa bevezetett μ-függvény igen fontos szerepet játszik a számelméleti függvények vizsgálatánál, valamint a prímszámelméletben (emellett a Möbius-szalag is az ő nevét viseli).

Poussin, Charles de la Vallée (ejtsd: pusszen, dö la valé), 1866–1962, belga. Ő és Hadamard igazolták elsőként (egyidejűleg, de egymástól függetlenül) a prímszámtételt.

Rados Gusztáv, 1862–1942, magyar. Legérdekesebb számelméleti eredménye a Kőnig Gyulával közösen elért Kőnig–Rados-tétel.

Ramanujan, Srinivasa (ejtsd: ramanudzsan), 1887–1920, indiai. Zseniális intuíciójú matematikus, aki valószínűleg elsősorban képzési hiányosságai miatt nem volt képes matematikai eredményeit a szokásos bizonyítási lépésekre bontva megindokolni. Hardy segítségével a cambridge-i egyetemen ki tudta bontakoztatni képességeit. Naplói még ma is új kutatások forrásait jelentik.

Ramsey, Frank Plumpton (ejtsd: remzi), 1903–1930, angol. Rövid élete során közgazdászként, filozófusként és matematikusként egyaránt kiválót alkotott. Matematikai logikai vizsgálatok kapcsán fedezte fel híres gráftételét.

Rényi Alfréd, 1921–1970, magyar. A Magyar Tudományos Akadémia Matematikai Kutató Intézetének megalapítója és első igazgatója, a magyar valószínűségszámítási iskola megteremtője. A számelmélet területén a Goldbach-sejtéssel kapcsolatban ért el jelentős új eredményeket.

Riemann, Bernhard, 1826–1866, német. A prímszámtétel bizonyításához vezető út kidolgozója, az ő elvei alapján igazolta a tételt egymástól függetlenül Hadamard és de la Vallée Poussin 1896-ban. Euler gondolatait továbbfejlesztve Riemann rámutatott a róla elnevezett zétafügvény központi jelentőségére a prímszámok eloszlásának vizsgálatában. Ehhez a függvényhez kapcsolódik a ma is megoldatlan Riemann-sejtés.

Schneider, Theodor, 1911–1988, német. Ő és Gelfond igazolták (egyidejűleg, de egymástól függetlenül) Hilbertnek az algebrai számok irracionális algebrai kitevős hatványaira vonatkozó problémáját.

Schur, Issai, 1875–1941, (a nácik által zsidó származása miatt elűzött) német. Híres tétele, hogy véges sok színnel kiszínezve a természetes számok elég nagy kezdőszeletét, mindig lesz az $x + y = z$ egyenletnek egyszínű megoldása.

S(ch)nirelmann, Lev Gyemidovics, 1905–1938, orosz. Az általa bevezetett sűrűségfogalom segítségével jelentős eredményeket ért el a Goldbach-sejtés vizsgálatában.

Thue, Axel, 1863–1922, norvég. Fontos eredményeket ért el a diofantikus approximációban és a diofantikus egyenletek területén.

Turán Pál, 1910–1976, magyar. Első jelentős eredménye a Hardy–Ramanujan-tételre adott egyszerű bizonyítása volt, amely később a valószínűségszámítás számelméleti alkalmazásainak kiindulópontjává vált. Elsősorban az analitikus számelmélet és a partíciók területén végzett kiemelkedő munkásságot.

Vinogradov, Ivan Matvejevics, 1891–1975, orosz. Lényegében bebizonyította a „páratlan" Goldbach-sejtést, azaz, hogy minden elég nagy páratlan szám előáll három prímszám összegeként. Jelentősen javította a Waring-problémakörben szereplő $G(k)$ függvényre korábban adott becsléseket is.

Waerden, Bartel Leendert van der, 1903–1996, holland. Bebizonyította, hogy a természetes számok véges sok színnel történő tetszőleges színezése esetén keletkeznek akármilyen hosszú (véges) egyszínű számtani sorozatok.

Waring, Edward, 1736–1798, angol. Az ő nevét viseli az egész számok k-adik hatványok összegeként történő előállíthatóságát vizsgáló Waring-problémakör.

Wilson, John, 1741–1793, angol. Nevét a $(p-1)!$ modulo p maradékáról szóló tétel őrzi.

TÁBLÁZATOK

Prímszámok 2–1733

2	127	283	467	661	877	1087	1297	1523
3	131	293	479	673	881	1091	1301	1531
5	137	307	487	677	883	1093	1303	1543
7	139	311	491	683	887	1097	1307	1549
11	149	313	499	691	907	1103	1319	1553
13	151	317	503	701	911	1109	1321	1559
17	157	331	509	709	919	1117	1327	1567
19	163	337	521	719	929	1123	1361	1571
23	167	347	523	727	937	1129	1367	1579
29	173	349	541	733	941	1151	1373	1583
31	179	353	547	739	947	1153	1381	1597
37	181	359	557	743	953	1163	1399	1601
41	191	367	563	751	967	1171	1409	1607
43	193	373	569	757	971	1181	1423	1609
47	197	379	571	761	977	1187	1427	1613
53	199	383	577	769	983	1193	1429	1619
59	211	389	587	773	991	1201	1433	1621
61	223	397	593	787	997	1213	1439	1627
67	227	401	599	797	1009	1217	1447	1637
71	229	409	601	809	1013	1223	1451	1657
73	233	419	607	811	1019	1229	1453	1663
79	239	421	613	821	1021	1231	1459	1667
83	241	431	617	823	1031	1237	1471	1669
89	251	433	619	827	1033	1249	1481	1693
97	257	439	631	829	1039	1259	1483	1697
101	263	443	641	839	1049	1277	1487	1699
103	269	449	643	853	1051	1279	1489	1709
107	271	457	647	857	1061	1283	1493	1721
109	277	461	653	859	1063	1289	1499	1723
113	281	463	659	863	1069	1291	1511	1733

Prímszámok 1741–3907

1741	1993	2221	2437	2689	2909	3187	3433	3659
1747	1997	2237	2441	2693	2917	3191	3449	3671
1753	1999	2239	2447	2699	2927	3203	3457	3673
1759	2003	2243	2459	2707	2939	3209	3461	3677
1777	2011	2251	2467	2711	2953	3217	3463	3691
1783	2017	2267	2473	2713	2957	3221	3467	3697
1787	2027	2269	2477	2719	2963	3229	3469	3701
1789	2029	2273	2503	2729	2969	3251	3491	3709
1801	2039	2281	2521	2731	2971	3253	3499	3719
1811	2053	2287	2531	2741	2999	3257	3511	3727
1823	2063	2293	2539	2749	3001	3259	3517	3733
1831	2069	2297	2543	2753	3011	3271	3527	3739
1847	2081	2309	2549	2767	3019	3299	3529	3761
1861	2083	2311	2551	2777	3023	3301	3533	3767
1867	2087	2333	2557	2789	3037	3307	3539	3769
1871	2089	2339	2579	2791	3041	3313	3541	3779
1873	2099	2341	2591	2797	3049	3319	3547	3793
1877	2111	2347	2593	2801	3061	3323	3557	3797
1879	2113	2351	2609	2803	3067	3329	3559	3803
1889	2129	2357	2617	2819	3079	3331	3571	3821
1901	2131	2371	2621	2833	3083	3343	3581	3823
1907	2137	2377	2633	2837	3089	3347	3583	3833
1913	2141	2381	2647	2843	3109	3359	3593	3847
1931	2143	2383	2657	2851	3119	3361	3607	3851
1933	2153	2389	2659	2857	3121	3371	3613	3853
1949	2161	2393	2663	2861	3137	3373	3617	3863
1951	2179	2399	2671	2879	3163	3389	3623	3877
1973	2203	2411	2677	2887	3167	3391	3631	3881
1979	2207	2417	2683	2897	3169	3407	3637	3889
1987	2213	2423	2687	2903	3181	3413	3643	3907

Prímtényezős felbontás

Az alábbi táblázatban megadjuk az 1100-nál kisebb, 2-vel, 3-mal és 5-tel nem osztható pozitív összetett számok prímtényezős felbontását.

$49 = 7^2$	$377 = 13 \cdot 29$	$637 = 7^2 \cdot 13$	$871 = 13 \cdot 67$
$77 = 7 \cdot 11$	$391 = 17 \cdot 23$	$649 = 11 \cdot 59$	$889 = 7 \cdot 127$
$91 = 7 \cdot 13$	$403 = 13 \cdot 31$	$667 = 23 \cdot 29$	$893 = 19 \cdot 47$
$119 = 7 \cdot 17$	$407 = 11 \cdot 37$	$671 = 11 \cdot 61$	$899 = 29 \cdot 31$
$121 = 11^2$	$413 = 7 \cdot 59$	$679 = 7 \cdot 97$	$901 = 17 \cdot 53$
$133 = 7 \cdot 19$	$427 = 7 \cdot 61$	$689 = 13 \cdot 53$	$913 = 11 \cdot 83$
$143 = 11 \cdot 13$	$437 = 19 \cdot 23$	$697 = 17 \cdot 41$	$917 = 7 \cdot 131$
$161 = 7 \cdot 23$	$451 = 11 \cdot 41$	$703 = 19 \cdot 37$	$923 = 13 \cdot 71$
$169 = 13^2$	$469 = 7 \cdot 67$	$707 = 7 \cdot 101$	$931 = 7^2 \cdot 19$
$187 = 11 \cdot 17$	$473 = 11 \cdot 43$	$713 = 23 \cdot 31$	$943 = 23 \cdot 41$
$203 = 7 \cdot 29$	$481 = 13 \cdot 37$	$721 = 7 \cdot 103$	$949 = 13 \cdot 73$
$209 = 11 \cdot 19$	$493 = 17 \cdot 29$	$731 = 17 \cdot 43$	$959 = 7 \cdot 137$
$217 = 7 \cdot 31$	$497 = 7 \cdot 71$	$737 = 11 \cdot 67$	$961 = 31^2$
$221 = 13 \cdot 17$	$511 = 7 \cdot 73$	$749 = 7 \cdot 107$	$973 = 7 \cdot 139$
$247 = 13 \cdot 19$	$517 = 11 \cdot 47$	$763 = 7 \cdot 109$	$979 = 11 \cdot 89$
$253 = 11 \cdot 23$	$527 = 17 \cdot 31$	$767 = 13 \cdot 59$	$989 = 23 \cdot 43$
$259 = 7 \cdot 37$	$529 = 23^2$	$779 = 19 \cdot 41$	$1001 = 7 \cdot 11 \cdot 13$
$287 = 7 \cdot 41$	$533 = 13 \cdot 41$	$781 = 11 \cdot 71$	$1003 = 17 \cdot 59$
$289 = 17^2$	$539 = 7^2 \cdot 11$	$791 = 7 \cdot 113$	$1007 = 19 \cdot 53$
$299 = 13 \cdot 23$	$551 = 19 \cdot 29$	$793 = 13 \cdot 61$	$1027 = 13 \cdot 79$
$301 = 7 \cdot 43$	$553 = 7 \cdot 79$	$799 = 17 \cdot 47$	$1037 = 17 \cdot 61$
$319 = 11 \cdot 29$	$559 = 13 \cdot 43$	$803 = 11 \cdot 73$	$1043 = 7 \cdot 149$
$323 = 17 \cdot 19$	$581 = 7 \cdot 83$	$817 = 19 \cdot 43$	$1057 = 7 \cdot 151$
$329 = 7 \cdot 47$	$583 = 11 \cdot 53$	$833 = 7^2 \cdot 17$	$1067 = 11 \cdot 97$
$341 = 11 \cdot 31$	$589 = 19 \cdot 31$	$841 = 29^2$	$1073 = 29 \cdot 37$
$343 = 7^3$	$611 = 13 \cdot 47$	$847 = 7 \cdot 11^2$	$1079 = 13 \cdot 83$
$361 = 19^2$	$623 = 7 \cdot 89$	$851 = 23 \cdot 37$	$1081 = 23 \cdot 47$
$371 = 7 \cdot 53$	$629 = 17 \cdot 37$	$869 = 11 \cdot 79$	$1099 = 7 \cdot 157$

Mersenne-számok

Mersenne-számoknak az $M_p = 2^p - 1$ alakú számokat nevezzük, ahol $p > 0$ prímszám. Ezekkel részletesen foglalkozunk az 5.2 pontban, és ott megtalálható a 2023-ban ismert 51 ilyen alakú prím listája is.

Az alábbi táblázatban megadjuk a 10 és 100 közötti kitevőkhöz tartozó Mersenne-számok prímtényezős felbontását.

$$2^{11} - 1 = 23 \cdot 89$$

$$2^{13} - 1 = 8191$$

$$2^{17} - 1 = 131071$$

$$2^{19} - 1 = 524287$$

$$2^{23} - 1 = 47 \cdot 178481$$

$$2^{29} - 1 = 233 \cdot 1103 \cdot 2089$$

$$2^{31} - 1 = 2147483647$$

$$2^{37} - 1 = 223 \cdot 616318177$$

$$2^{41} - 1 = 13367 \cdot 164511353$$

$$2^{43} - 1 = 431 \cdot 9719 \cdot 2099863$$

$$2^{47} - 1 = 2351 \cdot 4513 \cdot 13264529$$

$$2^{53} - 1 = 6361 \cdot 69431 \cdot 20394401$$

$$2^{59} - 1 = 179951 \cdot 3203431780337$$

$$2^{61} - 1 = 2305843009213693951$$

$$2^{67} - 1 = 193707721 \cdot 761838257287$$

$$2^{71} - 1 = 228479 \cdot 48544121 \cdot 212885833$$

$$2^{73} - 1 = 439 \cdot 2298041 \cdot 9361973132609$$

$$2^{79} - 1 = 2687 \cdot 202029703 \cdot 1113491139767$$

$$2^{83} - 1 = 167 \cdot 57912614113275649087721$$

$$2^{89} - 1 = 618970019642690137449562111$$

$$2^{97} - 1 = 11447 \cdot 13842607235828485645766393$$

Fermat-számok

Fermat-számoknak az $F_n = 2^{2^n} + 1$ alakú számokat nevezzük, ahol $n \geq 0$ egész, ezekkel részletesen foglalkozunk az 5.2 pontban.

A $0 \leq n \leq 4$ értékekre F_n prím:

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65\,537.$$

Egyelőre $n \geq 5$-re nem találtak prímet a Fermat-számok között.

Az F_5, F_6 és F_7 prímtényezős felbontása a következő:

$$F_5 = 641 \cdot 6700417$$

$$F_6 = 274177 \cdot 67280421310721$$

$$F_7 = 59649589127497217 \cdot 5704689200685129054721$$

Ezeken kívül 2023-ban még $8 \leq n \leq 11$ esetén ismert az F_n prímtényezős felbontása.

F_{20}-ról megmutatták, hogy összetett, de nem tudták még egyetlen nemtriviális osztóját sem meghatározni.

F_{33} a legkisebb olyan Fermat-szám, amelyről nem ismert, hogy prím-e vagy összetett.

TÁRGYMUTATÓ

A tárgymutató elsődleges célja, hogy segítséget nyújtson a könyvben (több helyen) előforduló fogalmak, elnevezések, jelölések magyarázatának visszakeresésében.

Ennek megfelelően a tárgymutatóban (általában) csak az első előfordulási hely adatai szerepelnek. A fogalom, elnevezés után megadjuk a könyvben használt tipikus jelölését (ha van ilyen), majd annak a definíciónak, tételnek stb. a számát, ahol a fogalom, elnevezés, jelölés magyarázata megtalálható, végül zárójelben odaírjuk az oldalszámot is.

A definíción kívül gyakran a szóban forgó fogalomhoz kapcsolódó fontos tételeket is jelzünk, például „$\sigma(n)$" esetében a 6.2.1 Definíció mellett a függvény képletét tartalmazó 6.2.2 Tételre is utalunk. Más esetekben a fogalomhoz kapcsolódó tételeket külön sorokban listázzuk, például az „átlagérték"-nél rendre megadjuk, hogy a nevezetesebb számelméleti függvények átlagértékeiről mely tételek szólnak.

Ha egy fontos fogalom több területen is előjön, akkor általában ezek mindegyikét felsoroljuk, lásd például az „egység" vagy a „norma" esetében. (Ha a jelölésben nincs eltérés, akkor azt nem ismételjük meg minden sorban.)

A definíciószám, tételszám stb. után egy „$-$", illetve „$+$" jel szerepel, ha az adott fogalmat nem a jelzett definícióban, tételben stb., hanem (közvetlenül) azt megelőzően, illetve követően a szövegben (külön számozás nélkül) vezetjük be. Így pl. a „triviális osztó"-nál D1.4.1$-$ arra utal, hogy a triviális osztó értelmezése az 1.4.1 Definíció *előtt* (az előző oldal alján) történik.

A tárgymutatóban D3.2.1 jelenti a 3.2.1 Definíciót, és a D betű helyett T, L, F rendre a megfelelő számú tételre, lemmára, feladatra utal. Az 1.3.3 Tétel bizonyítását B1.3.3-mal, az 1.2 pontban szereplő 3. példát 1.2.P3-mal, az 5.8 pontot 5.8-cal jelezzük. Ez utóbbi jelentheti akár az egész pontot, akár annak egy részét, az eligazodásban ilyenkor a megjelölt oldalszámok segíthetnek. Például a „titkosírás" esetén az 5.8 pont (feladatok nélküli) teljes 214–217 oldalszáma fel van tüntetve, ugyanakkor a „Diffie–Hellman-elv"-nél csak a 214–215 oldal szerepel. Az „RSA-séma" konkrétan össze van foglalva az 5.8.1 Tételben, így a tárgymutató is azt jelzi.

A $\sigma(n)$ függvényre vonatkozó „átlagos nagyságrend"-nél T6.7.3$+$ azt mutatja, hogy a magyarázat a tétel *kimondása után* (még a *bizonyítás előtt*) található, ugyanakkor az „algebrailag zárt test" esetében B9.3.6$+$ arra utal, hogy az értelmezés a 9.3.6 Tétel *bizonyítása után* keresendő.

A jelölésekkel kapcsolatos legfontosabb információkat a 12–13. oldalon a „Technikai tudnivalók" c. rész is tartalmazza, de az alábbiakban ezeket is

megismételjük.

A definíciók stb. számozásánál az első szám mindig a fejezetet, a második a fejezeten belül a pontot, a harmadik pedig a ponton belül a sorszámot jelöli. A definíciók és tételek sorszámozása egy ponton belül folyamatos, tehát pl. az 1.1.2 Definíció után az 1.1.3 Tétel következik. Az illusztrációs példák, képletek stb. (sima, egy számmal történő) számozása pontonként újrakezdődik.

Külön is kiemelünk néhány fontos jelölést, amelyek a könyvben leggyakrabban szereplő fogalmakat érintik. Megkülönböztetjük a (valós) számok alsó és felső egészrészét, és ezeket $\lfloor\ \rfloor$, illetve $\lceil\ \rceil$ jelöli, így pl. $\lfloor\pi\rfloor = 3$, $\lceil\pi\rceil = 4$, a $[\pi]$ jelölést nem használjuk. A számok törtrészét $\{\ \}$ jelöli, tehát $\{c\} = c - \lfloor c\rfloor$. Az oszthatóságra, a legnagyobb közös osztóra és a legkisebb közös többszörösre a szokásos jelöléseket használjuk, tehát pl. $7 \mid 42$, $(9, 15) = 3$, $[9, 15] = 45$. A $[\ ]$ szögletes zárójel legkisebb közös többszöröst, zárt intervallumot vagy egyszerűen zárójelet jelöl (ez utóbbi különösen a 11. fejezetben jellemző, ahol a $(\ )$ kerek zárójel ideált jelent; a megkülönböztetés érdekében itt a legnagyobb közös osztóra is az $\mathrm{lnko}\{a, b\}$ jelölést használjuk).

A polinomok és függvények jelölésére többnyire az (argumentum nélküli) f, g stb. jelölés szerepel, de helyenként az $f(x)$, $g(x)$ stb. írásmód is előfordul. A polinomok fokszámát (az angol degree szónak megfelelően „deg"-gel jelöljük, tehát pl. $\deg(x^3 + x) = 3$. A szokásos módon $\mathbf{Q}$, $\mathbf{R}$, illetve $\mathbf{C}$ rendre a racionális, a valós, illetve a komplex számok testét, $\mathbf{Z}$, $\mathbf{Z}_m$, illetve $T[x]$ pedig az egész számok, a modulo m maradékosztályok, illetve a T feletti polinomok gyűrűjét jelenti. A testbővítéseknél $\mathbf{Q}(\vartheta)$, illetve $E(\vartheta)$ a racionális test ϑ-val való egyszerű bővítését, illetve (algebrai ϑ esetén) az ebben található algebrai egészek gyűrűjét jelenti, E-vel pedig az összes algebrai egész gyűrűjét jelöljük. A p betűt szinte kizárólag a (pozitív) prímszámok jelölésére tartjuk fenn. A sima (index nélküli) log jelölés a természetes (e alapú) logaritmust jelenti.

A (véges vagy végtelen) szorzatok és összegek jelölésére gyakran használjuk a $\prod$ és $\sum$ jeleket, például

$$\prod_{i=1}^{r} p_i^{\alpha_i}, \qquad \prod_{p \le n} p, \qquad \sum_{p} \frac{1}{p^2}$$

rendre a $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ szorzatot, az n-nél nem nagyobb (pozitív) prímszámok szorzatát, illetve a (pozitív) prímszámok négyzetének reciprokösszegét jelenti.

Megemlítjük még, hogy a könyvben a definíciók, illetve a tételek megfogalmazásának a végén ♣ áll, a bizonyítások befejezését pedig ■ jelzi. A feladatok kitűzésénél szereplő *, **, illetve **M** jelek rendre arra utalnak, hogy a feladat nehéz, kiemelkedően nehéz, illetve részletes megoldás található hozzá a „Megoldások" c. fejezetben.

additív bázis T12.3.3– (521), F12.3.10 (530)
— komplementum 12.6 (541)
— számelméleti függvény D6.1.4 (221)
— — — karakterizációja T6.8.1 (275)
Agrawal–Kayal–Saxena-teszt (AKS) 5.7 (209–210)
alapparalelogramma (rácsé) T8.2.1 (358)
alaptételes gyűrű T11.3.1 (461)
algebrai egész D9.6.1 (403)
— elem D10.1.4 (410)
— — foka $\deg \vartheta$ D10.1.5 (411)
— — minimálpolinomja m_ϑ 10.1.5 (411)
algebrai szám D9.1.1 (377)
— — approximációja T9.4.1 (390), T9.4.3 (393)
— — foka $\deg \alpha$ D9.2.4 (382)
— — minimálpolinomja m_α D9.2.1 (381)
— — normája ($\mathbf{Q}(\vartheta)$-ban) $N(\alpha)$ D10.4.4, T10.4.5 (437)
— — $\mathbf{Q}$ feletti konjugáltja $\vartheta_{(j)}$ D10.4.1 (434)
— — relatív konjugáltja $f(\vartheta_{(j)})$ D10.4.2, T10.4.3 (434–436)
algebrai számtest = $\mathbf{Q}$ egyszerű algebrai bővítése
algebrailag zárt test B9.3.6+ (388)
álprím (a alapú) D5.7.3 (204)
— (univerzális) D5.7.3 (204)
alsó egészrész $\lfloor\ \rfloor$ B1.2.1 (20)
approximáció (diofantikus) 8.1 (349–356)
— , algebrai számé T9.4.1 (390), T9.4.3 (393)
— , irracionális számé 8.1 (349–356)
— , racionális számé F8.1.1 (356)
— , szimultán T8.1.3, T8.1.4 (351–352)
átlagérték, átlagértékfüggvény D6.7.1 (260)
— , $d(n)$-é T6.4.3 (239), T6.4.4 (241)
— , $\varphi(n)$-é T6.7.4 (263)
— , $\omega(n)$-é T6.7.6 (267)
— , $\Omega(n)$-é F6.7.5 (274)
— , $\sigma(n)$-é T6.7.3 (261)
átlagos nagyságrend, $\varphi(n)$-é T6.7.4+ (263)
— — , $\sigma(n)$-é T6.7.3+ (261)

barátságos számok F6.3.7 (237)
bázis (additív) T12.3.3– (521), F12.3.10 (530)
Bertrand-posztulátum (Csebisev-tétel) T5.5.3+ (181)

binom kongruencia T3.5.1 (122)
bővelkedő szám F6.3.3 (236)

C=komplex számok
Carmichael-szám D5.7.3 (204)
Cauchy–Davenport–Chowla-tétel T12.3.1 (518)
Chevalley-tétel T3.6.1 (126)
cinkos B5.7.4 (206)

Csebisev-egyenlőtlenség B6.7.7+ (273), B12.1.1 (498)
Csebisev-tétel T5.5.3 (181)
csoport B2.8.5+ (99)
csupaegy F1.3.12 (33)

$d(n) = n$ (pozitív) osztóinak a száma T1.6.3 (44)
$d_k(n)$ D6.2.6, T6.2.7 (228)
deg = fok(szám)
Diffie–Hellman-elv 5.8 (214–215)
diofantikus approximáció 8.1 (349–356)
— egyenlet T1.3.6– (29)
— — , lineáris T1.3.6 (30), T7.1.1 (281)
Dirichlet-sor $F(s)$ D6.6.3 (256)
Dirichlet-tétel (prímszámok számtani sorozatokban) T5.3.1 (168)
diszjunkt fedőrendszer (DFR) F12.5.6 (541)
diszkrét logaritmus = index $\operatorname{ind} a$, $\operatorname{ind}_g a$ D3.4.1 (119)
diszkrimináns ($\mathbf{Q}(\vartheta)$-é) B10.5.4+ (445)
— ($\mathbf{Q}(\vartheta)$-beli elem-n-eseké) $\Delta(\alpha_1, \dots, \alpha_n)$ D10.5.2 (441)

E = összes algebrai egész gyűrűje
e irracionalitása T9.5.1 (397)
e transzcendenciája T9.5.3 (400)
$E(\vartheta)$ = a $\mathbf{Q}(\vartheta)$ bővítés algebrai egészeinek gyűrűje
egész bázis ($\mathbf{Q}(\vartheta)$-ban) $\omega_1, \dots, \omega_n$ D10.5.1 (439), T10.5.4 (443)
egészrész (alsó) $\lfloor\ \rfloor$ B1.2.1 (20)
— , felső $\lceil\ \rceil$ B1.2.1 (21)
egyenletes eloszlás D8.4.3, T8.4.4 (374–375)
egyértelmű prímfaktorizáció,
egyértelmű prímfelbontás = számelmélet alaptétele
egyiptomi tört F7.3.6 (294)

egység ε D1.1.2 (15), D7.4.6 (297)
— (egész számoknál) D1.1.2, T1.1.3 (15–16)
— (Euler-egészeknél) T7.7.6 (326)
— (Gauss-egészeknél) D7.4.6, T7.4.7 (297–298)
— (másodfokú bővítéseknél) T10.3.4 (424)
egységelem (szorzásnál) 1, e F1.1.23a (20)
egyszerű algebrai bővítés $\mathbf{Q}(\vartheta)$ D10.2.1 (413), T10.2.3 (414)
— bővítés D10.2.1, T10.2.2 (413)
ekvivalenciareláció B2.1.2+ (55)
ekvivalens ideálok D11.6.1 (490)
elemi szimmetrikus polinom T9.3.1+ (384)
eratoszteneszi szita T5.1.2 (153)
euklideszi algoritmus B1.3.3 (27)
— gyűrű D11.3.4 (464), T11.3.5 (465)
Euler-egész $\alpha = a + b\omega$ D7.7.4 (324)
Euler-féle φ-függvény $\varphi(n)$ D2.2.7 (62), T2.3.1 (67)
Euler–Fermat-tétel T2.4.1 (71)
Euler partíciós tétele T 7.9.5 (344)
Euler-prím T7.7.7 (326)
Euler-racionális 9.6.P3 (404)

faktorgyűrű = maradékosztálygyűrű R/I T11.1.6 (452)
fedőrendszer 12.5 (536–537)
— , diszjunkt (DFR) F12.5.6 (541)
felbonthatatlan ideál D11.4.6 (473)
— szám D1.4.1 (34)
felső egészrész $\lceil\ \rceil$ B1.2.1 (20)
Fermat-prím F_n F1.4.4 (36), 5.2 (158)
Fermat-sejtés T7.7.1 (320)
— a 3 kitevőre T7.7.10 (328)
— a 4 kitevőre T7.7.2 (322)
Fermat-szám F_n 5.2 (158)
— (prím)osztói T5.2.1 (159)
— prímtesztje T5.2.2 (160)
Fermat-tétel („kis”) T2.4.1A, T2.4.1B (72)
$\varphi(n)$ = Euler-féle φ-függvény D2.2.7 (62), T2.3.1 (67)
Fibonacci-szám φ_n F1.2.5 (23)
fok, fokszám (algebrai elemé) $\deg\vartheta$ D10.1.5 (411)
— (algebrai számé) $\deg\alpha$ D9.2.4 (382)
— (polinomé modulo m) D3.1.1 (102)

fok (testbővítésé) $\deg(M:L)$ D10.1.2 (409)
fokszámtétel T10.1.3 (409)
főideál (a) D11.1.2 (449)
főideálgyűrű D11.3.2, T11.3.3 (462–463)
Frobenius-probléma F7.1.11 (285)

$g(k)$ D7.6.1 (315)
$G(k)$ D7.6.3 (316)
Gauss-egész $\alpha = a + bi$ D7.4.1 (296)
Gauss-felbonthatatlan π D7.4.10 (300)
Gauss-lemma (másodfokú kongruenciáknál) T4.2.1 (141)
— (primitív polinomoknál) F11.5.9 (489)
Gauss-prím π D7.4.11 (300), T7.4.15 (302)
Gauss-racionális 9.6.P3 (404)
Gelfond–Schneider-tétel T9.3.5 (387)
generátorfüggvény (partícióknál) 7.9 (341–342)
Goldbach-sejtés 5.1 (154)

gyűrű R B2.8.2+ (97)
— , alaptételes T11.3.1 (461)
— , euklideszi D11.3.4 (464), T11.3.5 (465)

hányados (maradékos osztásnál) q B1.2.1+ (21)
Hardy–Ramanujan-tétel T6.7.7, T6.7.7A (269)
harmonikus szám F6.3.6 (237)
három-négyzetszám-tétel T7.5.2 (307)
hatványmaradék (k-adik) D3.5.2, T3.5.3 (124)
hatvány-nemmaradék (k-adik) D3.5.2 (124)
hatványozás ismételt négyzetre emeléssel 3.2.P (107–108), B5.7.1 (200–201)
hegytétel T6.4.2 (238)
hézag a szomszédos prímek között 5.5 (180–185)
hiányos szám F6.3.3 (236)

ideál I D11.1.1 (448)
— , elem(ek) által generált (a), $(a_1, \ldots, a_k)$ D11.1.2, D11.1.4 (449–450)
— , felbonthatatlan D11.4.6 (473)
— , legszűkebb T11.1.3 (449), T11.1.5 (451)
— , maximális D11.4.6+ (473)
— , triviális 11.1.P4 (449)
— , végesen generált $(a_1, \ldots, a_k)$ D11.1.4 (450)

ideál szerinti maradékosztály $a + I$ T11.1.6 (452)
ideálok ekvivalenciája D11.6.1 (490)
— legkisebb közös többszöröse F11.4.5 (476)
— legnagyobb közös osztója (A, B) D11.4.4, T11.4.5 (472)
— oszthatósága $B \mid A$ D11.4.3 (471)
— összege $A + B$ F11.4.4b (475)
— szorzata AB D11.4.1, T11.4.2 (468–469)
ideálosztály T11.6.3– (491)
ikerprímek 5.1 (154)
Im = képzetes rész (komplex számé)
index $\operatorname{ind} a$, $\operatorname{ind}_g a$ D3.4.1 (119)
inkongruens = nem kongruens $\not\equiv$ D2.1.1+ (54)
integritási tartomány F1.1.23 (19)
inverz (szorzásnál) T2.8.3– (98)
irracionális szám approximációja 8.1 (349–356)
irracionalitás bizonyítása, e T9.5.1 (397)
— — , $\sqrt[k]{n}$ F1.6.33a (53)
— — , $\log_a b$ F1.6.33b (53)
— — , $\sqrt{2}$ (geometriailag) F1.3.17e (33)
— — , π T9.5.2 (397)
irreducibilis = felbonthatatlan
ismételt négyzetre emelés módszere 3.2.P (107–108), B5.7.1 (200–201)
izolált prím T5.5.2 (180)

Jacobi-szimbólum $\left(\frac{a}{m}\right)$ D4.3.1 (147)

k-adik hatványmaradék D3.5.2, T3.5.3 (124)
k-adik hatvány-nemmaradék D3.5.2 (124)
kanonikus alak T1.6.1 (43)
— — (Gauss-egészeknél) B7.5.1 (306)
— — (ideáloknál) T11.5.9– (486)
— — (legkisebb közös többszörösé) T1.6.6 (46)
— — (legnagyobb közös osztóé) T1.6.4 (44)
— — (módosított) T1.6.1+ (43)
— — (n!-é) T1.6.8 (48)
— — (osztóé) T1.6.2 (43)
karakterizáció (additív számelméleti függvényeké) T6.8.1 (275)
képzetes másodfokú bővítés T10.3.6– (427–428)
két-négyzetszám-tétel T7.5.1 (305)

kínai maradéktétel T2.6.2 (84)
kis Fermat-tétel T2.4.1A, T2.4.1B (72)
kitüntetett közös osztó (a, b) D1.3.2 (26)
kommutatív csoport B2.8.5+ (99)
— test T T2.8.3+ (98)
komplementum (additív) 12.6 (541)
— , teljesen gazdaságos (TGK) T12.6.2− (545)
kongruencia $a \equiv b \pmod m$ D2.1.1 (54)
— ($a + b\sqrt{3}$ alakú számoknál) B5.2.4 (164)
— (Euler-egészeknél) D7.7.8 (327)
— , binom T3.5.1 (122)
— , lineáris $ax \equiv b \pmod m$ D2.5.1, T2.5.3–T2.5.5 (74–77)
— , másodfokú D4.1.1 (137)
— , prímhatvány modulusú T3.7.1 (133)
kongruencia fedőrendszer 12.5 (536–537)
kongruencia megoldásszáma D2.5.2 (75)
konjugált (**Q** feletti) $\vartheta_{(j)}$ D10.4.1 (434)
— (relatív) $f(\vartheta_{(j)})$ D10.4.2, T10.4.3 (434–436)
konvolúció $f * g$ D6.6.1 (253)
Kőnig–Rados-tétel T3.6.2 (129)
körosztási polinom Φ_m B5.3.4 (169)
középérték(függvény) = átlagérték(függvény) D6.7.1 (260)
közös osztó, legnagyobb (a, b), $\operatorname{lnko}\{a, b\}$ D1.3.1 (25), D7.4.9 (299)
— — , kitüntetett (a, b) D1.3.2 (26)
közös többszörös, legkisebb $[a, b]$, $\operatorname{lkkt}(a, b)$ D1.6.5 (46)
Kronecker-tétel (ideáloknál) T11.5.5 (481)
kvadratikus maradék D4.1.1 (137)
— nemmaradék D4.1.1 (137)
— reciprocitási tétel T4.2.3 (143)
kvázitökéletes szám F6.3.4 (236)

lánctört 8.3 (365)
lánctörtjegy D8.3.1 (365)
Legendre-formula = $n!$ kanonikus alakja T1.6.8 (48)
Legendre-szimbólum $\left(\frac{a}{p}\right)$ D4.1.3 (138)
legkisebb abszolút értékű maradék r T1.2.1A+ (21)
— közös többszörös $[a, b]$, $\operatorname{lkkt}(a, b)$ D1.6.5 (46)
— — — kanonikus alakja T1.6.6 (46)
legkisebb nemnegatív maradék r B1.2.1+ (21)

legnagyobb közös mérték F1.3.17d (33)
— — osztó (a,b), $\operatorname{lnko}\{a,b\}$ D1.3.1 (25), D7.4.9 (299)
— — — (egész számoknál) (a,b), $\operatorname{lnko}\{a,b\}$ D1.3.1 (25)
— — — (Gauss-egészeknél) (α,β) D7.4.9 (299)
— — — (ideáloknál) (A,B) D11.4.4, T11.4.5 (472)
— — — kanonikus alakja T1.6.4 (45)
legszűkebb ideál T11.1.3 (449), T11.1.5 (451)
— (rész)test T10.2.2 (413)
lineáris diofantikus egyenlet $ax+by=c$ T1.3.6 (30), T7.1.1 (281)
— kongruencia $ax\equiv b \pmod m$ D2.5.1, T2.5.3–T2.5.5 (74–77)
Liouville approximációs tétele T9.4.1 (390)
Liouville-szám F9.4.1 (396)
Lucas–Lehmer-teszt = Mersenne-számok prímtesztje T5.2.4 (164)

maradék (maradékos osztásnál) r B1.2.1+ (21)
— , kvadratikus D4.1.1 (137)
— , legkisebb abszolút értékű T1.2.1A+ (21)
— , legkisebb nemnegatív B1.2.1+ (21)
maradékos osztás (egész számoknál) T1.2.1, T1.2.1A (20–21)
— (euklideszi gyűrűben) D11.3.4 (464)
— (Gauss-egészeknél) T7.4.8 (298)
maradékosztály (faktorgyűrűnél) $a+I$ T11.1.6 (452)
— (kongruenciánál) (a), $(a)_m$ D2.2.1 (60)
— , redukált D2.2.6 (62)
maradékosztálygyűrű (ideál szerinti) R/I T11.1.6 (452)
— (modulo m) $\mathbf{Z}_m$ T2.8.2 (97)
maradékrendszer, redukált D2.2.8, T2.2.9 (63)
— , teljes D2.2.2, T2.2.3 (60–61)
maradékszámrendszer 2.6.P2− (88–89)
másodfokú bővítés $\mathbf{Q}(\sqrt{t})$ 10.3 (419–432)
— — , képzetes T10.3.6− (427–428)
— — , valós T10.3.6− (427)
másodfokú bővítés algebrai egészei T10.3.2 (421)
— kongruencia D4.1.1 (137)
másodrendű additív bázis T12.3.3− (521)
maximális ideál D11.4.6+ (473)
megfordítási formula T6.5.3 (249)
— függvény $\tilde f$ T6.5.2 (248)
megoldásszám (kongruenciáé) D2.5.2 (75)
Mersenne-prím M_p F1.4.4 (36), 5.2 (158)

Mersenne-szám M_p 5.2 (158)
— (prím)osztói T5.2.3 (163)
— prímtesztje T5.2.4 (164)
Miller–Lenstra–Rabin-teszt T5.7.5 (208)
minimálpolinom (algebrai elemé) m_ϑ D10.1.5 (411)
— (algebrai számé) m_α D9.2.1 (381)
Minkowski-tétel T8.2.1 (358)
modulus (kongruenciáé) m D2.1.1+ (54)
Möbius-féle megfordítási formula T6.5.3 (249)
Möbius-függvény $\mu(n)$ D6.2.3 (227)
multiplikatív inverz T2.8.3− (98)
— számelméleti függvény D6.1.2 (221)
$\mu(n)$ = Möbius-függvény D6.2.3 (227)

$n!$ kanonikus alakja (Legendre-formula) T1.6.8 (48)
négy-négyzetszám-tétel T7.5.3 (308)
négyzetmentes szám F1.6.10 (50)
négyzetteljes szám F5.6.1f (196)
norma (egyszerű algebrai bővítésben) $N(\alpha)$ D10.4.4 (437)
— (Euler-egészé) D7.7.5 (325)
— (Gauss-egészé) D7.4.2, T7.4.3 (296)
— (kvaternióé) B7.5.4+ (309)
— (másodfokú bővítésben) D10.3.3 (423)
nullmértékű halmaz D8.1.7 (354)
nullosztó T2.8.5− (98)

nyilvános jelkulcsú titkosírás 5.8 (214–217)

$\omega(n) = n$ különböző (pozitív) prímosztóinak a száma D6.2.5 (228)
$\Omega(n) = n$ „összes” (pozitív) prímosztóinak a száma D6.2.5 (228)
Ore-szám F6.3.6 (237)
osztályszám T11.6.3 (491)
osztható(ság), osztó $b \mid a$ D1.1.1 (15), D7.4.4 (297)
— , — (egész számoknál) $b \mid a$ D1.1.1 (15)
— , — (Gauss-egészeknél) $\beta \mid \alpha$ D7.4.4 (297)
— , — (ideáloknál) $B \mid A$ D11.4.3 (471)
osztók összege $\sigma(n)$ D6.2.1, T6.2.2 (226)
— száma $d(n)$ T1.6.3 (44)
osztókra vonatkozó összegzési függvény f^+ D6.5.1 (248)

összegzési függvény f^+ D6.5.1 (248)
összemérhetőség F1.3.17 (33)

p_n: általában az n-edik prímszámot jelöli
$p(n) = n$ partícióinak a száma D7.9.1 (340)
páronként relatív prím D1.3.8 (31)
páros számok számelmélete B1.1.3+ (16), B1.4.3+ (35), B1.5.1− (38)
partíció D7.9.1 (340)
Pell-egyenlet T7.8.1 (335), T7.8.2 (337)
Pepin-teszt = Fermat-számok prímtesztje T5.2.2 (160)
π irracionalitása T9.5.2 (397)
$\pi(x)$ T5.4.1− (172)
— alsó és felső becslése T5.4.3 (174)
pitagoraszi számhármas T7.2.1 (286)
polinom, körosztási Φ_m B5.3.4 (169)
— , primitív F11.5.9 (489)
polinom deriváltja f' T3.7.1 (133), B5.3.4 (170)
— fok(szám)a modulo m D3.1.1 (102)
— többszörös gyöke B5.3.4 (170)
prím, prímszám p D1.4.2 (34)
prímhatvány modulusú kongruencia megoldása T3.7.1 (133)
prímideál D11.4.7 (473)
primitív gyök (modulo m) g D3.3.1, T3.3.2 (110-111)
— pitagoraszi számhármas T7.2.1 (286)
— polinom F11.5.9 (489)
prímképletek 5.1 (156)
prímosztók száma („különbözők”) $\omega(n)$ D6.2.5 (228)
— — („összes”) $\Omega(n)$ D6.2.5 (228)
prímszámok számtani sorozatokban 5.1 (155), T5.3.1 (168)
prímszámtétel T5.4.1 (172)
prímteszt (Agrawal–Kayal–Saxena) 5.7 (209–210)
— (Fermat-számé) T5.2.2 (160)
— (kis Fermat-tétel alapján) T5.7.2 (203)
— (Mersenne-számé) T5.2.4 (164)
— (Miller–Lenstra–Rabin) T5.7.5 (208)
— (Solovay–Strassen) T5.7.4 (204)
pszeudoprím = álprím D5.7.3 (204)

$\mathbf{Q}$ = racionális számok
$\mathbf{Q}$ egyszerű (algebrai) bővítése $\mathbf{Q}(\vartheta)$ D10.2.1, T10.2.2, T10.2.3 (413–414)

Q feletti konjugált (algebrai számé) $\vartheta_{(j)}$ D10.4.1 (434)

R = valós számok
racionális szám approximációja F8.1.1 (356)
Ramsey-számok T12.4.1+ (531)
Ramsey tétele T12.4.1 (531)
Re = valós rész (komplex számé)
reciprocitási tétel T4.2.3 (143)
redukált maradékosztály D2.2.6 (62)
— maradékrendszer D2.2.8, T2.2.9 (63)
relatív konjugált (**Q**(ϑ)-ban) $f(\vartheta_{(j)})$ D10.4.2, T10.4.3 (434–436)
— prím D1.3.7 (30)
— — , páronként D1.3.8 (31)
relatív prímség valószínűsége T6.7.5 (264)
rend (modulo m) $o(a)$, $o_m(a)$ D3.2.1 (106)
Riemann-féle zéta-függvény $\zeta(s)$ F5.6.6 (197), T6.6.4− (256)
Riemann-sejtés T6.6.4− (257)
Roth approximációs tétele T9.4.3 (393)
RSA-séma T5.8.1 (217)

Schur-számok T12.4.2+ (532)
Schur tétele T12.4.2 (532)
Sidon-sorozat 12.2 (506–507)
Smith-determináns T6.5.4 (250)
Solovay–Strassen-teszt T5.7.4 (204)

szakaszok összemérhetősége F1.3.17 (33)
számelmélet alaptétele T1.5.1 (37), T7.4.13 (301), 11.3 (460–466)
— — (egész számoknál) T1.5.1 (37)
— — (Gauss-egészeknél) T7.4.13 (301)
— — (gyűrűben általában) 11.3 (460–466)
— — (ideáloknál) T11.5.8 (484)
— — (másodfokú bővítések algebrai egészeire) T10.3.5 (425), T10.3.6 (428)
számelméleti algoritmusok lépésszáma T5.7.1 (200)
— függvény D6.1.1 (220)
számrendszeres felírás T1.2.2 (21)
számtani sorozatok prímszámai 5.1 (155), T5.3.1 (168)
$\sigma(n) = n$ (pozitív) osztóinak az összege D6.2.1, T6.2.2 (226)
szimmetrikus polinom T9.3.1+ (384)
— polinomok alaptétele T9.3.2 (384)

szimultán approximáció T8.1.3, T8.1.4 (351–352)
— kongruenciarendszer 2.6 (81–90)
szupertökéletes szám F6.3.5 (237)

T: általában kommutatív testet jelöl
$T[x]$ = a T test feletti polinomok gyűrűje
tanú B5.7.4 (206)
teljes maradékrendszer D2.2.2, T2.2.3 (60–61)
teljesen additív számelméleti függvény D6.1.5 (221)
— gazdaságos komplementum(TGK) T12.6.2− (545)
— multiplikatív számelméleti függvény D6.1.3 (221)
test T T2.8.3+ (98)
— , algebrailag zárt B9.3.6+ (388)
testbővítés $M : L$ D10.1.1 (408)
— , egyszerű $\mathbf{Q}(\vartheta)$ D10.2.1, T10.2.2 (413)
— , egyszerű algebrai D10.2.1 (413), T10.2.3 (414)
— , másodfokú $\mathbf{Q}(\sqrt{t})$ 10.3 (419–432)
— , véges D10.1.2 (409)
testbővítés foka $\deg(M : L)$ D10.1.2 (409)
testbővítések fokszámtétele T10.1.3 (409)
Thue approximációs tétele T9.4.3 (393)
Thue-lemma F7.5.21a (314)
titkosírás 5.8 (214–217)
tizedes tört F3.2.20 (110)
totálisan additív számelméleti függvény D6.1.5 (221)
— multiplikatív számelméleti függvény D6.1.3 (221)
többszörös D1.1.1+ (15), D7.4.4+ (297)
tökéletes szám D6.3.1, T6.3.2 (235)
törtrész $\{\ \}$ B8.1.2 (350)
transzcendencia bizonyítása, e T9.5.3 (400)
— — , $\lg n$ F9.3.7 (389)
transzcendens szám D9.1.2 (378)
— — létezése T9.1.3 (378), T9.4.2 (392)
triviális ideál 11.1.P4 (449)
— osztó D1.4.1− (34)

univerzális álprím D5.7.3 (204)

valós másodfokú bővítés T10.3.6− (427)
Van der Waerden-számok T12.4.4A+ (534)

Van der Waerden tétele T12.4.4, T12.4.4A (534)
véges bővítés D10.1.2 (409)
végtelen leszállás B7.5.3+ (311)
— szorzat F5.6.6, F5.6.7 (198)
völgytétel T6.4.1 (238)

Waring-problémakör 7.6 (314–319)
Weyl tétele T8.4.4 (375)
Wiles tétele (Fermat-sejtés) T7.7.1 (320)
Wilson-tétel T2.7.1 (93), B3.1.2+ (103)

$\mathbf{Z}$ = egész számok
$\mathbf{Z}_m$ = modulo m maradékosztálygyűrű T2.8.2 (97)
zéta-függvény $\zeta(s)$ F5.6.6 (197), T6.6.4− (256)