Elemi Számelmélet

Gyarmati Katalin

katalin.gyarmati@ttk.elte.hu

Eötvös Loránd Tudományegyetem

Egyetemi Jegyzet

ELTE TTK Matematikai Intézet

2022

Tartalomjegyzék

Bevezetés

Az elemi számelmélet története az ókorig nyúlik vissza, de a terület mai napig használatos, gondolhatunk itt akár modern titkosítási algoritmusokra.

A jegyzet első része teljes egészében tartalmazza az első éves matematikus hallgatóknak tartott számelmélet kurzusomat, azonban egy kissé meg is haladja azt.

Célom volt, hogy a modern számítógépes kornak megfelelően, a jegyzetet úgy írjam, hogy az vetíthető legyen előadótermekben, illetve otthon, számítógépen olvasva is, kényelmesen el tudjunk merülni az elemi számelmélet különböző történelmi fejezeteiben.

Főképp a következő forrásokra támaszkodtam:

Martin Aigner, Günter M. Ziegler, *Bizonyítások a könyvből*, link.

Gyarmati Edit, Turán Pál, *Számelmélet*, link.

Erdős Pál, Surányi János, *Válogatott Fejezetek a Számelméletből*, link.

Freud Róbert, Gyarmati Edit, *Számelmélet*, link.

Fried Katalin, Korándi József, Török Judit, *Számelmélet*, link.

Fuchs László, *Bevezetés az Algebrába és Számelméletbe*, link.

G. H. Hardy - E. M. Wright, *An Introduction to the Theory of Numbers*, link.

Sárközy András, *Számelmélet és Alkalmazásai*, link.

Szalay Mihály, *Számelmélet*, link.

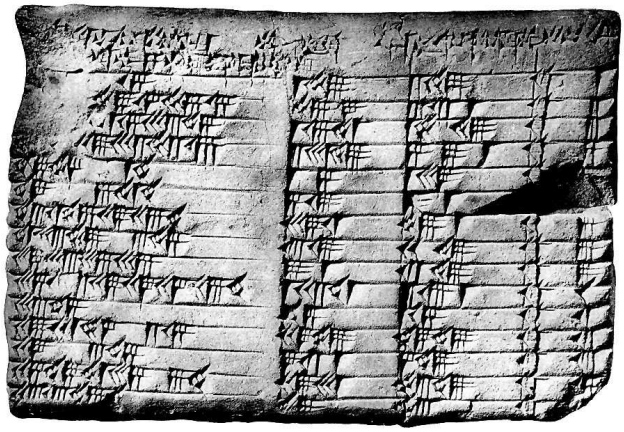
Wikipedia, link.

A jegyzetben ezekre a könyvekre általában nem hivatkozok külön többet (a többszörös hivatkozás elkerülése okán), viszont az egyes fejezetek végén megpróbáltam a matematikai eredmények eredeti forrását megnevezni, ahol tudtam. Azonban ez sokszor reménytelen vállalkozás, hiszen gyakran jó pár száz éves eredményekről van szó (de olyan tétel is van, amely 2000 éves). A könyvben az illusztráló ábrák, képek forrását az adott fejezet végén, a referenciajegyzékben adtam meg.

Az olvasóknak, hallgatóknak kellemes időtöltést kívánok.

1. Természetes számok

A legkorábbi számelméleti emlékünk egy agyag táblatöredék kb. i.e. 1800-ból való és Mezopotámiából származik. Úgynevezett pitagoraszi számhármasokat tartalmazott, azaz olyan a, b, c egész számokat, amelyre $a^2 + b^2 = c^2$. A számhármasok túl nagyok ahhoz, hogy egyszerű próbálgatással találták volna őket. A Plimpton 322 névre keresztelt tábla, így nézett ki:



A babiloni számok helyett ma már arab számokat használunk.

A természetes számokat mindenki jól ismeri, ezek:

$$0, 1, 2, 3, 4, 5, 6, 7, \ldots .$$

A mai modern számelmélet kiinduló pontja a természetes számok összessége, ezt a halmazt $\mathbb{N}$ jelöli. Kevésbé ismert azonban, hogy a természetes számoknak van egy axióma-rendszere. Ez, az ún. Peano-féle axióma-rendszer a következő:

1. A 0 természetes szám.

2. Minden n természetes számnak van egy rákövetkezője (vagyis minden számnál van egy 1-gyel nagyobb szám), amely ismét természetes szám, és amelyet n'-vel jelölünk.

3. A 0 egyetlen természetes számnak se rákövetkezője.

4. Ha $n' = m'$, akkor $n = m$ (vagyis különböző természetes számok rákövetkezői nem lehetnek egyenlők).

5. Ha a természetes számok valamilyen M halmaza tartalmazza a 0-át, és ha $n \in M$-ből következik $n' \in M$, akkor az M halmaz tartalmazza az összes természetes számot.

Minden bizonnyal a legbonyolultabb axióma az 5. axióma, amelyet szokás a teljes indukció axiómájának is hívni.

Középiskolából ismert a teljes indukció, mint bizonyítási módszer, azonban az, hogy ez a bizonyítási módszer működik valójában az 5. axiómát használja.

Peano matematikus, logikatudós és nyelvész, 1858-ben született a matematika axiómarendszereinek egyik megalapítója.

Azonban az első explicit teljes indukciós bizonyítás jóval régebbi, és a görög matematikus és csillagász Francesco Maurolico-tól ([1], 1575) származik. A következő állítást igazolta teljes indukcióval:

1.1. ÁLLÍTÁS. *Az első n páratlan szám összege éppen n^2. Képlet formájában:*

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

A történelmi utat bejárva, mi is bebizonyítjuk az állítást teljes indukcióval.

Kezdő lépés: A tétel $n = 1$-re igaz.

$$1 = 1^2?$$

Igen...

Indukciós lépés: Feltesszük, hogy az állítás igaz $n = k$-ra, azaz

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2 \tag{1.1}$$

Ebből bebizonyítjuk, hogy $n = k + 1$-re is igaz, tehát, hogy

$$1 + 3 + 5 + \cdots + (2(k + 1) - 1) = (k + 1)^2. \tag{1.2}$$

Végből adjunk (1.1) mindkét oldalához $2k + 1$-et:

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + 2k + 1.$$

Itt a jobboldalon éppen $(k + 1)^2$ áll, így (1.1)-ből valóban következik (1.2). Ezzel az állítást teljes indukcióval igazoltuk.

A köztudatban az elemi számelmélet főképp oszthatóság vizsgálatával bizonyít egész számokkal kapcsolatos állításokat. Ugyan ritkábban használt, azonban nagyon erős módszer a teljes indukció is az elemi számelméletben. Lássunk erre egy feladatot:

1.2. FELADAT. *Mely pozitív egész n-ekre teljesül, hogy*

$$3^n + 4^n = 5^n?$$

A jegyzetben tipikusan kevés feladat van, érdemes azonban a megoldás elolvasása előtt önállóan próbálkozni. Nem mindig sikerül a legszebb megoldást megtalálnunk, de a megoldásra szánt idő mindig megéri a fáradtságot.

1.2. Feladat megoldása.

A megoldás során sokszor segít, ha megnézzük az állítást az első pár természetes számra. Most is tegyünk így:

$$3^0 + 4^0 = 1 + 1 = 2 \neq 5^0 = 1$$
$$3^1 + 4^1 = 3 + 4 = 7 \neq 5^1 = 5$$
$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$
$$3^3 + 4^3 = 27 + 64 = 91 \neq 5^3 = 125$$
$$3^4 + 4^4 = 81 + 256 = 337 \neq 5^4 = 625$$
$$3^5 + 4^5 = 243 + 1024 = 1267 \neq 5^5 = 3125$$
$$3^6 + 4^6 = 729 + 4096 = 2825 \neq 5^6 = 15625$$

Észrevehetjük, hogy $n \geq 3$-ra, 5^n értéke nagyobb mint $3^n + 4^n$. Így állításunk a következő:

1.3. Állítás.

$$3^n + 4^n < 5^n \qquad \textit{ha } n \geq 3.$$

Ez teljes indukcióval könnyen igazolható.

Kezdő lépés: Az állítás $n = 3$-ra igaz. Valóban:

$$3^3 + 4^3 = 27 + 64 = 91 < 5^3 = 125$$

Indukciós lépés: Feltesszük, hogy az állítás igaz $n = k$-ra, azaz, hogy

$$3^k + 4^k < 5^k. \tag{1.3}$$

Ebből bebizonyítjuk, hogy $n = k + 1$-re is igaz, tehát, hogy

$$3^{k+1} + 4^{k+1} < 5^{k+1}. \tag{1.4}$$

Ez pedig (1.3)-t használva a következőkből adódik:

$$3^{k+1} + 4^{k+1} < 4 \cdot 3^k + 4^{k+1} = 4 \cdot (3^k + 4^k) < 4 \cdot 5^k < 5^{k+1}.$$

Ezzel az állításunkat beláttuk. Az $n = 0, 1, 2$ eseteket megnézve, azt kaptuk, hogy az egyetlen megoldása a feladatnak az $n = 2$.

Elemi számelmélet feladatok megoldása során, ha egyszerű oszthatósági vizsgálatok nem, vagy csak részben vezetnek eredményre, akkor az előző példához hasonlóan, gyakran segítenek nagyságrendi becslések.

Hivatkozások

[1] Franciscus Maurolycus, *Arithmeticorum libri duo*, 1575, link.

[2] Fotó, Plimpton 322, link.

2. Prímszámok (alapok)

Az egész számok halmaza már nem csak a 0-t és pozitív számokat tartalmazza, hanem a negatívokat is, azaz:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Az egész számok körében definiáljuk az oszthatóságot:

2.1. DEFINÍCIÓ. *Legyen $a, b \in \mathbb{Z}$. Ekkor azt mondjuk, a osztható b-vel, ha létezik olyan $c \in \mathbb{Z}$, melyre*

$$a = bc.$$

Jelölése: $b \mid a$.

Gyakorta használt jelölések a következők:

$$\text{létezik} = \exists$$
$$\text{minden} = \forall$$

A definíciónk az új jelölésekkel felírva:

2.2. DEFINÍCIÓ. *Legyen $a, b \in \mathbb{Z}$. Ekkor azt mondjuk, a osztható b-vel, ha $\exists\, c \in \mathbb{Z}$, melyre*

$$a = bc.$$

Jelölése: $b \mid a$.

Az elkövetkezendőkben a prímszámok elemi tulajdonságairól lesz szó.

Az első pár prímszám:

$$2, 3, 5, 7, 11, 13, \ldots$$

A középiskolában a prímszámokat a következőképpen definiáltuk:

2.3. DEFINÍCIÓ. *A p egész szám prímszám, ha*

(i) $p > 1$,

(ii) *a p számnak nincs 1-en és p-n kívül más pozitív osztója.*

Ez a definíció Eukleidésztől [4] származik.

Azonban a mai modern számelméletben szükségessé vált az oszthatóságot az egészeknél bővebb számkörökben definiálni.

Ilyen számkör pl. az

$$S = \{a + b\sqrt{5} : \ a, b \in \mathbb{Z}\}.$$

Ahhoz, hogy ilyen típusú számkörökben is tudjuk vizsgálni a számkör elemeinek számelméleti tulajdonságait, a mai modern korban a prímszámokat kicsit másképp definiáljuk. Erről bővebben később lesz szó, egyelőre maradjunk a klasszikus definíciónál.

2.4. TÉTEL. *Az 1-et kivéve minden pozitív egész n szám felírható prímek szorzataként.*

2.4. TÉTEL BIZONYÍTÁSA. A tételt n-re vonatkozó teljes indukcióval igazoljuk.

Kezdő lépés: A tétel $n = 2$-re igaz. Valóban: a 2 prímtényezős felbontása önmaga, mivel a 2 prímszám.

Indukciós lépés: Tegyük fel, hogy az állítást beláttuk

$$n = 2, 3, 4, \ldots, k-1\text{-re.}$$

Bebizonyítjuk $n = k$-ra is.

Ha k prím, készen vagyunk (egytényezős szorzat).

Ha k-nak van 1-en és k-n kívül más osztója, akkor vegyük ezen osztók közül egyet:

$$m \mid k, \qquad \text{ahol } 2 \leq m \leq k-1.$$

Ekkor $\exists r \in \mathbb{N}$, amelyre

$$k = mr,$$

itt

$$r = \frac{k}{m}, \quad \text{ahol } r \neq 1 \text{ és } r \neq k.$$

Ezért

$$2 \leq r, m \leq k - 1$$

is fennáll. Az indukciós feltevés miatt m és r előáll prímek szorzataként, tehát

$$k = mr$$

is.

A „számelmélet alaptételének” hívjuk a következőt:

2.5. TÉTEL. *Az 1-nél nagyobb természetes számok felírhatók prímek szorzataként, és ez a felírása prímek sorrendjétől eltekintve egyértelmű.*

A tételt szokás SzAT-nak rövidíteni.

A tétel egyik részét már beláttuk, nevezetesen, hogy létezik ilyen felírás. Ami hiányzik az egyértelműség.

Az egyértelműség Eukleidész I. tételéből [4] következik.

2.6. TÉTEL. (Eukleidész I. tétele) *Ha p prím és $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$.*

Így láttuk, hogy már Eukleidész is igazolt a SzAT-tal ekvivalens állításokat, mégis azt először Gauss mondta ki explicit 1801-ben [6].

Az olvasót bátorítom, hogy próbálja meg könyvek és internet használata nélkül bebizonyítani Eukleidész I. tételét. Később a jegyzetben is be fogjuk bizonyítani, de előbb lássuk, hogyan következik Eukleidész I. tételéből a prímtényezős felbontás egyértelműsége.

Eukleidész I. tételét többtényezős szorzatra felírva kapjuk:

$$p \mid a_1 a_2 a_3 \cdots a_n \quad \Rightarrow \quad p \mid a_1 \text{ vagy } p \mid a_2 \ldots \text{ vagy } p \mid a_n.$$

Indirekten bizonyítunk. Tegyük fel, hogy van egy természetes szám, amelynek van két különböző felírása:

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_k}$$

Ekkor

$$p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_k}.$$

Eukleidész I. tételét használva:

$$p_1 \mid q_1 \text{ vagy } p_1 \mid q_2 \ldots \text{ vagy } p_1 \mid q_n.$$

Szimmetrikus okokból feltehető, hogy

$$p_1 \mid q_1.$$

Tudjuk q_1 prímszám, két darab pozitív osztója van: 1 és q_1.

$$\Rightarrow p_1 = q_1.$$

Továbbá $\alpha_1 = \beta_1$, mert ha $\alpha_1 > \beta_1$, akkor

$$p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_2^{\beta_2} \cdots q_\ell^{\beta_k}.$$

De ekkor

$$p_1 \mid q_2^{\beta_2} \cdots q_\ell^{\beta_k}.$$

Eukleidész I. tételét használva:

$$p_1 \mid q_2 \text{ vagy } p_1 \mid q_3 \ldots \text{ vagy } p_1 \mid q_n.$$

Itt $q_2, q_3, \ldots, q_n$ prímek, egynél nagyobb osztóik csak önmaguk, így azt kapjuk:

$$p_1 \in \{q_2, q_3, \ldots, q_n\}.$$

Ez pedig ellentmond $p_1 = q_1$-nek, hiszen a $q_1, q_2, \ldots, q_n$ prímek mind különbözőek.

Hasonlóan látható, hogy $\alpha_1 < \beta_1$ nem lehet. Így:

$$p_1 = q_1, \ \alpha_1 = \beta_1.$$

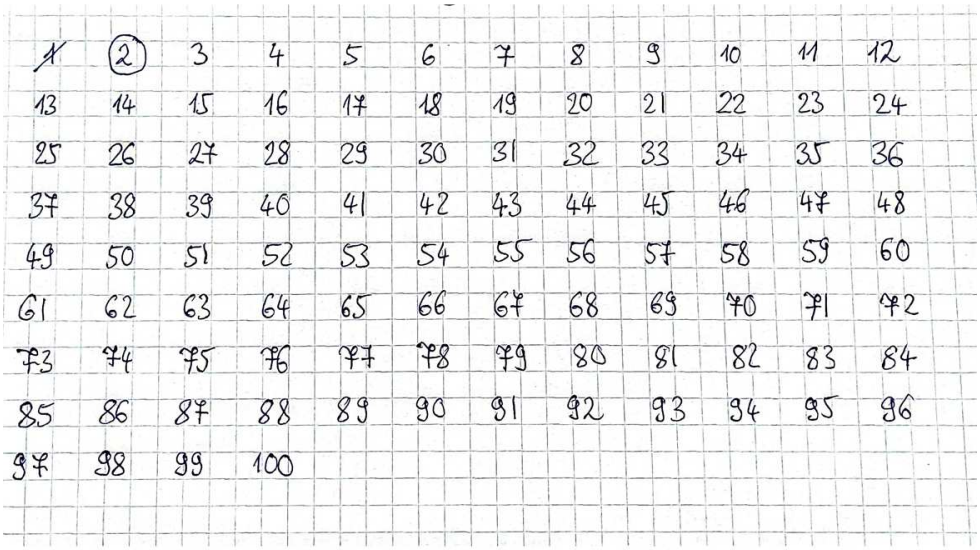
A prímtényezős felbontásban a többi tag, többi kitevő hasonlóan kezelhető.

2.1. Eratoszthenész Szitája

Eratoszthenész (i. e. 276 – i. e. 194) egyiptomi hellenisztikus matematikus, földrajztudós, csillagász, filozófus, költő, zenész. Fiatal korában „Bétának” is becézték, arra utalva, hogy sok mindennel foglalkozik ugyan, de mindenben csak a második legjobb tud lenni (a görög ábécében a béta a második betű). Később inkább az öttusázó atlétát jelentő „Pentatlosz” néven becézték sokoldalúságáért.

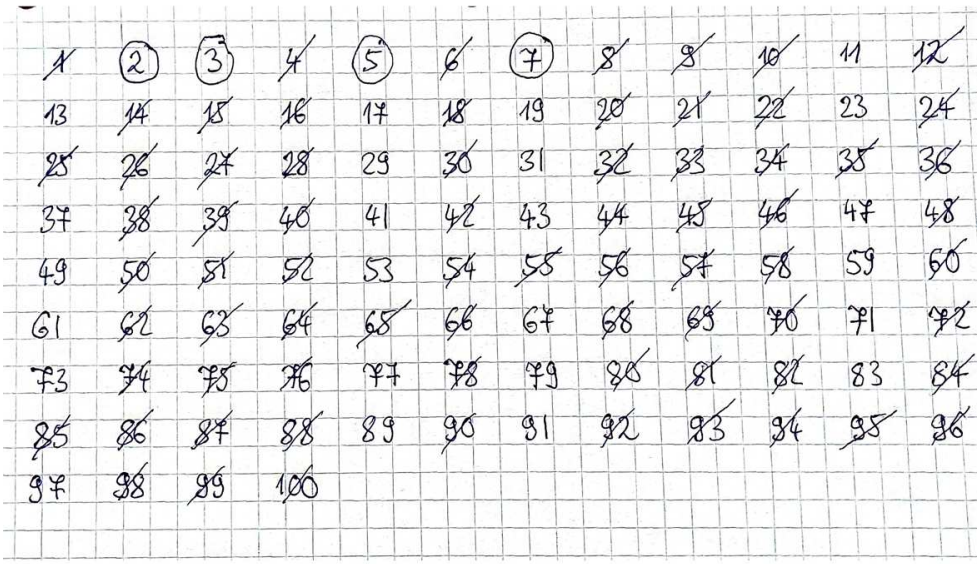
Eratoszthenész az első prímteszt megalkotója, sőt a mai napig leggyorsabb módszer, amely egy bizonyos határig megadja az összes prímszámot.

Lássunk erre egy példát. Írjuk fel a számokat 1-től 100-ig. Az 1 nem prímszám, húzzuk át. A következő egész szám, a 2-es prím, karikázzuk be.



Majd húzzuk át az összes páros számot. Az első át nem húzott szám a 3-as, karikázzuk be:

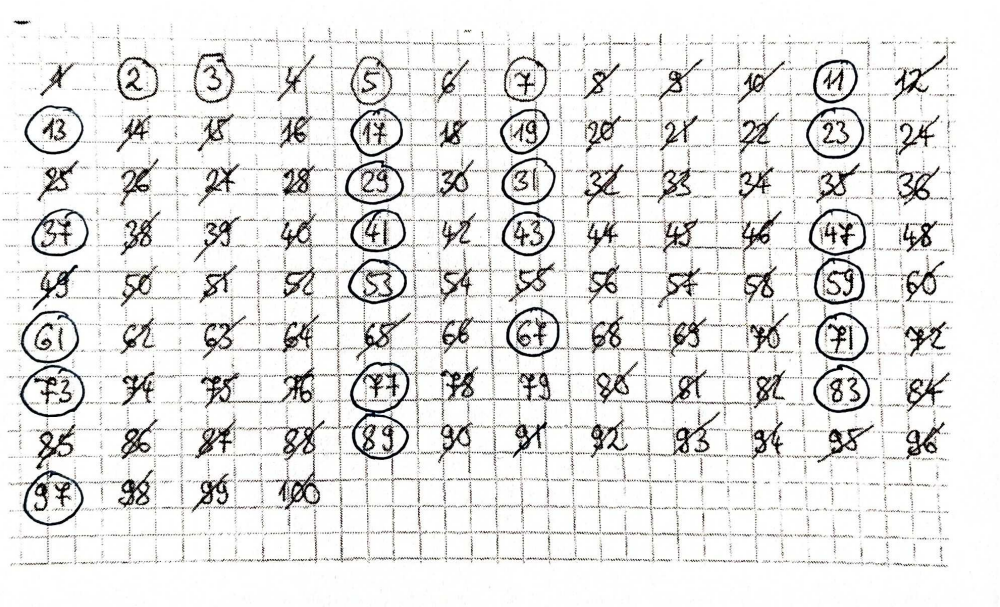
Folytassuk az algoritmust. Az összes 3-mal osztható számot áthúzzuk, majd bekarikázzuk az első át nem húzott számot, az 5-öt. Áthúzzuk az 5 többszöröseit, majd bekarikázzuk az első át nem húzott számot, az 7-et.



A következő lépésben úgy találjuk, hogy a 7 többszörösei közül csak

a 49 és 91 nincs áthúzva, ezeket húzzuk át. A következő prím a 11-es, de már nem kell áthúzni a 11-gyel osztható számokat.

A legkisebb szám, aminek nincs 11-nél kisebb prímosztója és összetett a $11^2 = 121$, ez pedig nagyobb mint 100. Vagyis az összes eddig jelöletlen számokat bekarikázva, megkapjuk a prímeket 100-ig.



Amennyiben n-ig szeretnénk meghatározni az összes prímet, elég $[\sqrt{n}]$-nél nem nagyobb prímekkel szitálni. Ez az algoritmus a mai napig a leggyorsabb, ha 1 és n között az összes prímet meg akarjuk határozni.

2.2. Elemi becslések prímszámok számára

Eukleidész [4] bebizonyította, hogy a prímszámok száma ∞. Ezt a tételt szokás Eukleidész II. tételének is hívni. Tétel formában megfogalmazva:

2.7. TÉTEL. (Eukleidész II. tétele) *A természetes számok között végtelen sok prím létezik.*

Aigner és Ziegler könyvében [1] hat különböző bizonyítást találunk arra, hogy a prímszámok száma végtelen.

Ismert egy anekdota Erdős Pálról, hogy sokszor emlegette azt, hogy Istennek van egy matematika könyve, amelyben minden tételnek megtalálható a legszebb bizonyítása.

Aigner és Ziegler [1] vállalkozott rá, hogy ebből a könyvből megismertet bennünket részletekkel, hogy ez mennyire volt sikeres és lehetséges, azt az olvasó döntésére bízzuk. Könyvük alapján a jegyzetben is szerepel több bizonyítás Eukleidész II. tételére, azonban először nézzük Eukleidész bizonyítását.

2.7. TÉTEL 1. BIZONYÍTÁSA. (Eukleidész)

Indirekten bizonyítunk. Tegyük fel, hogy csak véges sok prímszám $\exists$. Ezek: $p_1, p_2, \ldots, p_n$. Tekintsük az

$$A = p_1 p_2 \ldots p_n + 1$$

számot. A SzAT alapján A felírható prímek szorzataként:

$$q_1 q_2 \cdots q_\ell = A = p_1 p_2 \cdots p_n + 1.$$

Vegyük a q_1 prímet. Ekkor $q_1 \notin \{p_1, p_2, \ldots, p_n\}$, hiszen ha $q_1 = p_i$, akkor $q_1 = p_i \mid p_1 p_2 \cdots p_n$, másrészt $q_1 \mid q_1 q_2 \cdots q_\ell = A$. Így:

$$q_1 \mid A - p_1 p_2 \cdots p_n = 1,$$

ami ellentmondás, hiszen nincs olyan prímszám, amely 1-et osztaná.

Vagyis q_1 egy új prím, $p_1, p_2, \ldots, p_n$-től különböző. Azaz a bizonyítás elején mégsem soroltuk fel az összes prímet. Ellentmondásra jutottunk, és ezzel Eukleidész II. tételét igazoltuk.

Nézzük egy kicsit a prímek növekvő sorozatát:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5, \dots,$$

ahol p_n az n-edik prímszám. Eukleidész bizonyításából következik, hogy

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1.$$

Ebből teljes indukcióval bebizonyítható, hogy

$$p_n < 2^{2^n}.$$

A teljes indukció kivitelezése az olvasó házifeladata. A jegyzet további részében a házifeladatok rövidítésére a „HF” jelölést használjuk.

A HF-ek megoldása nem található meg a jegyzetben, ezek nagyon egyszerű gyakorló példák, az anyag önállóan való elmélyítésére szánt feladatok.

2.8. DEFINÍCIÓ. *Jelölje $\pi(x)$ az $\{1, 2, 3, \dots, x\}$ halmazban levő prímek számát.*

Nézzük meg $\pi(x)$ értékét az első pár x-re.

$\pi(1)$	$\{1\}$	$\pi(1) = 0$
$\pi(2)$	$\{1, ②\}$	$\pi(2) = 1$
$\pi(3)$	$\{1, ②, ③\}$	$\pi(3) = 2$
$\pi(4)$	$\{1, ②, ③, 4\}$	$\pi(4) = 2$
$\pi(5)$	$\{1, ②, ③, 4, ⑤\}$	$\pi(5) = 3$

2.9. ÁLLÍTÁS. *A $p_n < 2^{2^n}$ becslésből következik, hogy*

$$\pi(x) > \log_2 \log_2 x - 1.$$

Az állítás bizonyítása HF. A 2.9. Állítás eredménye nagyon gyenge becslés.

Jacques Hadamard [7] és Charles Jean de la Vallée Poussin [12] 1896-ban egymástól függetlenül (Bernard Riemann ötleteire támaszkodva) a következőt igazolta,

2.10. TÉTEL. (Prímszámtétel)

$$\pi(x) \sim \frac{x}{\log x}.$$

Hogy itt mit jelent a $\sim$ jelölés arra a jegyzet későbbi fejezeteiben térünk rá.

A bizonyítás komplex függvénytant, nevezetesen a Riemann-féle zeta függvényt használja. Ez a bizonyítás túl megy jelen jegyzet keretein.

De azért ebben a fejezetben adunk pár elemi becslést $\pi(x)$-re, illetve egy későbbi fejezetben is egyre élesebb becsléseket adunk $\pi(x)$-re.

A legjobb becslés amit be fogunk bizonyítani ebben a jegyzetben $\pi(x)$-re az Csebisev tételének [14], [15], [2] az eredetinél kissé gyengébb formája:

2.11. TÉTEL. *Ha $x \geq 2$, akkor*

$$0.34 \cdot \frac{x}{\log x} < \pi(x) < 4 \cdot \frac{x}{\log x}$$

Ez megközelíti a prímszámtétel állítását, de annál konstans szorzóval gyengébb.

A jegyzetben a felső becslésre adott bizonyítás Erdős Pál és Kalmár László munkája, mely teljesen elemi. Az alsó becslésre adott bizonyítás Landau [10] munkája.

Erdős Pál összes cikke megtalálható a Rényi Alfréd Matematikai Kutatóintézet honlapján, az alábbi helyen: link.

A webhelyet nézegetve nem találtam közös cikkét Erdős Pálnak és Kalmár Lászlónak, de ugyanakkor azt igen, hogy bár ők nem publikálták, bizonyításuk több könyvben is megjelent (természetesen az ő nevük alatt).

Szalay Mihály, Számelmélet [13] című tankönyvében könnyen olvasható ismertetést adott Erdős Pál, Kalmár László és Landau bizonyításáról, mi is ezt az ismertetőt követjük majd a 25. fejezetben.

Ezek után rátérhetünk Eukleidész II. tételének a második bizonyítására. Ez a bizonyítás az ún. Fermat-számokat használja.

2.12. DEFINÍCIÓ. *Az n-edik Fermat-szám:*

$$F_n \stackrel{def}{=} 2^{2^n} + 1.$$

A Fermat-számok nevüket Pierre de Fermat [5] francia jogász után kapták, aki bár rengeteget foglalkozott matematikával, foglalkozása szerint a toulouse-i fellebbviteli bíróság tagja volt.

Fermat foglalkozott először a 2.12. Definícióban megadott természetes számok számelméleti tulajdonságaival.

2.13. TÉTEL. *A Fermat-számok páronként relatív prímek.*

A bizonyítás a következő azonosságon múlik:

2.14. LEMMA.

$$F_n - 2 = 2^{2^n} - 1 = F_0 F_1 F_2 \cdots F_{n-1}.$$

2.14. LEMMA BIZONYÍTÁSA.

Valóban $2^{2^n} - 1$ az $a^2 - b^2 = (a-b)(a+b)$ azonosságot többszörösen használva szorzattá bomlik:

$$\begin{aligned} 2^{2^n} - 1 &= \left(2^{2^{n-1}} + 1\right)\left(2^{2^{n-1}} - 1\right) \\ &= \left(2^{2^{n-1}} + 1\right)\left(2^{2^{n-2}} + 1\right)\left(2^{2^{n-2}} - 1\right) \\ &\vdots \\ &= \left(2^{2^{n-1}} + 1\right)\left(2^{2^{n-2}} + 1\right)\cdots\left(2^{2^0} + 1\right)\left(2^{2^0} - 1\right). \end{aligned}$$

Itt a baloldalon $F_n - 2$, a jobboldalon $F_{n-1}F_{n-2}\cdots F_0$ szerepel, és ezzel az állítást beláttuk.

Lássuk most a tétel bizonyítását.

2.13. TÉTEL BIZONYÍTÁSA.

Legyen $n > k$. Belátjuk $(F_n, F_k) = 1$. Ehhez legyen

$$d = (F_n, F_k).$$

A Fermat-számok páratlanok, így d is páratlan. Mivel $0 \leq k \leq n-1$:

$$d \mid F_k, \quad F_k \mid F_0 F_1 \cdots F_{n-1} \quad \Rightarrow d \mid F_0 F_1 \cdots F_{n-1}.$$

Azaz a 2.14. Lemma szerint

$$d \mid F_n - 2.$$

De $d = (F_n, F_k)$, vagyis

$$d \mid F_n.$$

A fenti két oszthatóságból adódik:

$$d \mid F_n - (F_n - 2) = 2.$$

A 2-nek egyetlen pozitív páratlan osztója van az 1, így $d = 1$. Ezzel a tétel állítását beláttuk.

Ezután rátérhetünk Eukleidész II. tételének 2. bizonyítására.

2.7. TÉTEL 2. BIZONYÍTÁSA.

Az $F_0, F_1, F_2, \ldots$ Fermat-számok. Mindegyiknek vegyük egy-egy prímosztóját:

$$q_0 \mid F_0,\ q_1 \mid F_1,\ q_2 \mid F_2, \ldots.$$

Mivel az F_i Fermat-számok páronként relatív prímek, a $q_0, q_1, q_2 \ldots$ prímek között nem lehet két azonos.

Azaz végtelen sok prím létezik.

Fermat-számok kapcsán fontos fogalom a következő.

2.15. DEFINÍCIÓ. *Amennyiben az n-edik Fermat-szám*

$$F_n = 2^{2^n} + 1$$

prím, F_n-et Fermat prímnek nevezzük.

Itt mindjárt van egy az olvasónak szánt feladat:

2.16. FELADAT. *Igazolja, hogy ha $a \in \mathbb{N}$ esetén*

$$2^a + 1$$

prímszám, akkor szükségszerűen a kettőhatvány, azaz a számunk egy $2^{2^n} + 1$ alakú Fermat prím.

A megoldást később ismertetjük.

Az ismert Fermat-prímek a következők:

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537.$$

Jelenleg csak az első 12 Fermat-szám prímtényezőkre bontását ismerjük teljesen.

A Fermat-számokkal kapcsolatosan sok sejtés fogalmazódott meg:

2.17. SEJTÉS. *A Fermat-számok között F_0, F_1, F_2, F_3, F_4-en kívül nincs több prím.*

De sejthetjük ennek teljesen ellenkezőjét is:

2.18. SEJTÉS. *A Fermat-számok között végtelen sok prím van.*

De még a következő sem ismert:

2.19. SEJTÉS. *A Fermat-számok között végtelen sok összetett van.*

Ezen sejtések mindegyike reménytelenül nehéz. De ha próbálkozni akar az olvasó, én talán a 2.19. Sejtést javaslom.

Ha már szó esett a Fermat-prímekről, egy másik fontos csoportja a prímeknek a Mersenne-prímek. Nevüket Marin Mersenneről kapták, aki francia szerzetes, matematikus, fizikus volt. 13 évvel volt idősebb Fermat-nál, akivel levelezést folytatott. De sok más korabeli hírességgel is levelezett, többek között Galileo Galileivel. Fő munkáinak címei megtalálhatóak a kapcsolódó Wikipedia oldalon [20].

Mersenne rendszeresen találkozott korabeli tudósokkal, filozófusokkal, és hosszú levelekben tájékoztatta őket a tudomány és a filozófia területén történtekről. Az elterjedt mondás szerint: „Mersenne tudomására hozni valamit annyit jelent, mint egész Európa tudomására hozni”.

A számelméletben Mersenne-prímeknek nevezzük a következő számokat:

2.20. DEFINÍCIÓ. *Legyen p prímszám. Ekkor ha*

$$2^p - 1$$

is prímszám, akkor $2^p - 1$-et Mersenne-prímnek nevezzük.

A Mersenne-prímekkel kapcsolatos a következő feladat:

2.21. Feladat. *Legyen n természetes szám. Ekkor, ha 2^n-1 prímszám, akkor szükségszerűen n is prímszám.*

Mire az olvasó idáig eljutott, talán gondolkodott a 2.16. Feladat megoldásán. Amennyiben nem sikerült megoldania a feladatot, pici segítséget jelenthet, ha eláruljuk, hogy a 2.16. és 2.21. Feladatok megoldásához a következő nevezetes azonosságokat kell használni:

Minden n természetes számra:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}).$$

Páratlan n-ekre:

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1}),$$

ahol a $+/-$-ok felváltva követik egymást. Vigyázat, ez utóbbi egyenlőség csak páratlan n-ekre áll fenn. Gondoljunk csak arra, hogy páros n esetén, pl. $n = 2$-re, $a^2 + b^2$-ből nem emelhető ki $a + b$.

Mersenne-prímek kapcsán a leghíresebb sejtés a következő:

2.22. Sejtés. *Végtelen sok Mersenne-prím létezik.*

A Mersenne-prímek a modern számelméletben is fontos szerepet játszanak, hiszen a legnagyobb ismert prímszámok között nagyon sok Mersenne-prím van [17]. Ennek oka, hogy Mersenne-prímek vizsgálatára speciális, nagyon gyors prímtesztek vannak.

A 2.16. és 2.21. Feladatokat csak a fejezet végén igazoljuk.

Most inkább nézzük meg Eukleidész II. tételének 3. elemi bizonyítását. Ez a szép és trükkös bizonyítás Eulertől származik, aki 1737-ben igazolta a tételt.

A bizonyítást Erdős Pál [3] fedezte fel újra 1938-ban, egy német nyelven írt cikkben.

Elolvashatjuk a bizonyítást angolul is, Hardy és Wright [8] hatodik, Heath-Brown és Silverman által újradolgozott és kibővített kiadásában is. (Mindenképpen érdemes a számelmélet iránt érdeklődőnek ezt a könyvet is áttanulmányozni). Az apró betűs részben ott van, Euler és Erdős neve is...

A bizonyítás magyarul is elérhető [1]-ben, ahol összesen 6 bizonyítást is olvashatunk Eukleidész tételére.

Itt most a [8]-ban ismertetett módon bizonyítjuk be a tételt.

A bizonyításból következik, hogy a prímek reciprokösszege a végtelenbe tart.

2.7. Tétel 3. bizonyítása.

Jelölje $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ a prímek növekvő sorozatát.

Jelölje $N_j(x)$ azon 1 és x közé eső természetes számok számát, amelyek nem oszthatók a

$$p_{j+1},\ p_{j+2},\ \cdots$$

prímek egyikével sem, azaz prímtényezős felbontásuk

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j}$$

alakú. Képlettel:

$$N_j(x) = \left|\{m:\ 1 \le m \le x \ \text{ és } \ m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j}\}\right|.$$

Az 1. lépésben $N_j(x)$-re adunk felső becslést.

Egy $m \in \{m:\ 1 \le m \le x \ \text{ és } \ m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j}\}$-et írjunk fel

$$m = n^2 u$$

alakban, ahol n^2 a lehető legnagyobb négyzetszám osztója m-nek.

Ekkor u négyzetmentes, azaz nincs 1-nél nagyobb négyzetszám osztója, vagyis

$$u = p_1^{\beta_1} p_2^{\beta_2} \cdots p_j^{\beta_j}$$

alakú, ahol $\beta_i \in \{0, 1\}$.

Mivel minden i-re β_i csak kétféle értéket vehet fel, u értéke 2^j féle lehet.

Másrészt

$$\begin{aligned} n^2 &\le n^2 u = m \le x \\ n^2 &\le x \\ n &\le \sqrt{x}. \end{aligned}$$

Így $n \in \{1, 2, 3, \ldots, [\sqrt{x}]\}$. Tehát n legfeljebb $[\sqrt{x}]$ féle különböző értéket vehet fel.

Azaz $m = n^2 u$ pedig $[\sqrt{x}] \cdot 2^j$ féle értéket vehet fel. Így

$$N_j(x) \le [\sqrt{x}] \cdot 2^j \le \sqrt{x} \cdot 2^j.$$

A továbbiakban a bizonyítás minden x-re működik, így tetszőlegesen nagy x-re is.

Ha csak véges sok prím létezne, akkor ezek felsorolhatóak, legyen az összes prím:

$$p_1, p_2, \dots, p_j.$$

Az 1 és x közé eső számok mindegyike előáll ezek szorzataként, azaz

$$x = N_j(x).$$

Ezt összevetve az $N_j(x)$-re adott felső becsléssel:

$$\begin{aligned} x = N_j(x) &\leq \sqrt{x} \cdot 2^j \\ x &\leq \sqrt{x} \cdot 2^j \\ \sqrt{x} &\leq 2^j \\ x &\leq 2^{2j}. \end{aligned}$$

Azonban x tetszőlegesen nagynak választható a bizonyításban, így $x > 2^{2j}$-t választva ellentmondásra jutottunk.

2.23. TÉTEL. *A prímek reciprokösszege a ∞-be tart.*

2.23. TÉTEL BIZONYÍTÁSA.

Tegyük fel, hogy

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots = A. \tag{2.1}$$

Itt a baloldalon az összes prím reciprokösszege szerepel, de ez az összeg A-hoz tart, nem pedig egy A-nál kisebb számhoz. Így $\exists\, j$, hogy

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p_j} > A - \frac{1}{2}.$$

Vagyis (2.1) alapján:

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots < \frac{1}{2}.$$

Szorozzuk meg x-szel:

$$\frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \cdots < \frac{x}{2}.$$

Azaz azon 1 és x közé eső természetes számok száma, amelyek oszthatók a $p_{j+1}, p_{j+2}, \ldots$ prímek valamelyikével kevesebb mint $\frac{x}{2}$. Így azokra, amelyek ezek közül egyikkel sem oszthatóak:

$$\frac{x}{2} < N_j(x).$$

Az $N_j(x)$-re adott $2^j\sqrt{x}$ felső becslés alapján:

$$\begin{aligned} \frac{x}{2} &< N_j(x) \leq 2^j\sqrt{x} \\ \sqrt{x} &< 2^{j+1} \\ x &< 2^{2(j+1)} \end{aligned}$$

Így nagy x-ekre, akárcsak az előző bizonyításnál, ellentmondásra jutunk.

2.24. TÉTEL. *A prímszámok számára:*

$$\pi(x) \geq \frac{\log x}{2}.$$

Az n-edik prímet p_n-nel jelölve:

$$p_n < 4^n.$$

A 2.24. tételben nagyon gyenge becslések vannak. Valójában:

$$\pi(x) \sim \frac{x}{\log x},$$

$$p_n \sim n \log n.$$

De azért a 2.24. tételbeli eredmények már messze nem triviálisak, bizonyításuk komoly trükköket kíván.

2.24. Tétel bizonyítása.

Most is, az előző bizonyításokban már szereplő $N_j(x)$ és a rávonatkozó $2^j\sqrt{x}$ felső becslés a kulcspont.

Legyen most $j = \pi(x)$. Ekkor:

$$\begin{aligned} x = N_j(x) &\leq 2^j\sqrt{x} = 2^{\pi(x)}\sqrt{x} \\ \sqrt{x} &\leq 2^{\pi(x)} \\ \log_2 \sqrt{x} &\leq \pi(x) \\ \frac{1}{2\log 2}\log x &\leq \pi(x). \end{aligned}$$

Következzen $p_n < 4^n$ bizonyítása. Az x helyébe p_n-t írva:

$$\begin{aligned} \frac{\log p_n}{2\log 2} &\leq n = \pi(p_n) \\ \log p_n &\leq 2\log 2 \cdot n \\ p_n &\leq e^{2\log 2 \cdot n} \\ p_n &\leq 4^n. \end{aligned}$$

Ezzel a tétel állításait beláttuk.

Ebben a fejezetben már nem foglalkozunk többet $\pi(x)$ becslésével. De a későbbiekben, az utolsó fejezetben visszatérünk a témakörre, és bebizonyítjuk a 2.11. tételt.

2.3. Prímképletek

Vannak olyan polinomok, amelyek a változó sok egymás utáni értékére prímértékeket adnak [16],[21].

Például tekintsük az alábbi Eulertől [19] (1772) származó egész együtthatós polinomot:

$$x^2 + x + 41.$$

Valóban:

$$\begin{aligned} 1^2 + 1 + 41 &= 43 \quad \text{prím} \\ 2^2 + 2 + 41 &= 47 \quad \text{prím} \\ 3^2 + 3 + 41 &= 53 \quad \text{prím} \\ 4^2 + 4 + 41 &= 61 \quad \text{prím} \\ &\vdots \end{aligned}$$

Egy fiatalkoromban gyakran mondogatott mondás alapján: „Egy fizikus már rég rávágta volna, hogy minden egész helyen prímet vesz fel a polinom.”

Az $x^2 + x + 41$ polinom a $0 \leq x \leq 39$ helyeken prímeket ad, de $x = 40$-re:

$$40^2 + 40 + 41 = 1681 = 41^2 \quad \text{nem prím.}$$

Egy másik Legendre-től [18] (1798) származó hasonló polinom az

$$x^2 - x + 41,$$

amely szintén prímeket ad $x = 0$-tól kezdve $x = 40$-ig minden egész helyen, és pedig ugyanazt a 40 prímet mint az $f(x) = x^2 + x + 41$ polinom. (Miért? HF).

Szintén Legendre találta az x^2+x+17 polinomot, amely $x=0$-tól $x=15$-ig 16 darab különböző prímet vesz fel.

Itt szerepel egy az olvasónak szánt feladat:

2.25. FELADAT. *Létezik-e olyan egész együtthatós, egyváltozós polinom, amelynek a pozitív egész helyeken felvett értéke mindig prím?*

A feladat megoldása a 4. fejezetben, a kongruenciáknál lesz olvasható.

A következő oldalon egy nagyon érdekes tulajdonságú, de nagyon nagy méretű több változós polinom foglal helyet, melynek már a felírása is egy egész oldalt igénybe vesz.

Érdekességként megemlítjük, hogy 1970-ben Jurij Matyasevics [11] orosz matematikus szerkesztett egy olyan 25-ödfokú, 26 változós $p(x_1, x_2, \ldots, x_{26})$ polinomot, amely az $x_1, x_2, \ldots, x_{26}$ változók azon egész értékeire, amelyre $p(x_1, x_2, \ldots, x_{26})$ pozitív, akkor mindig prímszámot ad, és minden prímszám előállítható ilyen alakban.

A jelenleg ismert legegyszerűbb ilyen polinom (forrás: [9]):

$$
\begin{aligned}
&(k+2)(1- \\
&(wz+h+j-q)^2- \\
&((gk+2g+k+1)(h+j)+h-z)^2- \\
&(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2- \\
&(2n+p+q+z-e)^2- \\
&(e^3(e+2)(a+1)^2+1-o^2)^2- \\
&((a^2-1)y^2+1-x^2)^2- \\
&(16r^2y^4(a^2-1)+1-u^2)^2- \\
&(n+\ell+v-y)^2- \\
&((a^2-1)\ell^2+1-m^2)^2- \\
&(ai+k+1-\ell-i)^2- \\
&(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2- \\
&(p+\ell(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2- \\
&(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x)^2- \\
&(z+p\ell(a-p)+t(2ap-p^2-1)-pm)^2).
\end{aligned}
$$

A polinom tulajdonságainak alaposabb vizsgálatát az olvasóra bízzuk.

A számelmélet egyik leghíresebb sejtése Christian Goldbach-tól

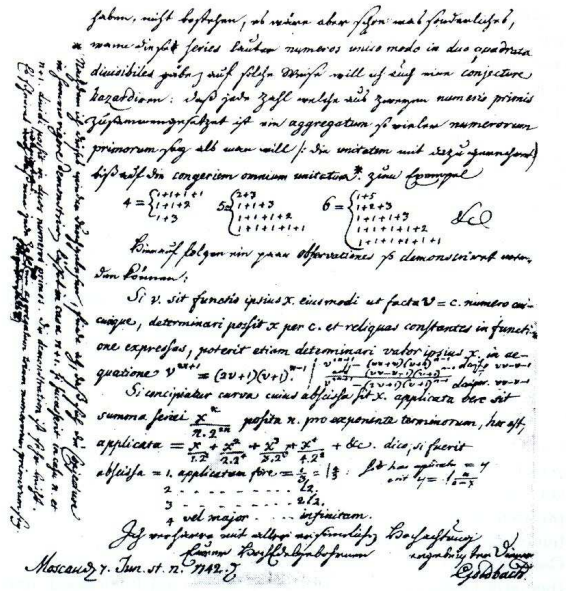
származik, aki egy Euler-hoz írt levelében a következőt fogalmazta meg:

2.26. SEJTÉS. (Goldbach-sejtés) (I.) *Minden* 2*-nél nagyobb páros szám előáll két prímszám összegeként.*

(II.) *Minden* 5*-nél nagyobb páratlan szám előáll három prímszám összegeként.*

Euler válaszában rámutatott, hogy (I.)-ből következik (II.).

Goldbach sok Eulerhez írt levele közül egyet megtaláltam a weben egy internetes könyvtárban (Fermat's library): link. Persze, akkoriban (és talán még ma is valamennyire), a kézírásos levelek voltak az elterjedtek. Goldbachnak Eulerhez írt levele az alábbi is:



Lassan a fejezet végén tartunk. Itt az idő, hogy ismertessük a 2.16. és 2.21. feladatok megoldását.

2.16. Feladat megoldása.

Tegyük fel, hogy a nem kettőhatvány. Ekkor a-nak $\exists$ egy egynél nagyobb páratlan osztója $t \geq 3$. Azaz $a = tm$, ekkor

$$2^a + 1 = 2^{tm} + 1 = (2^m)^t + 1^t$$
$$= (2^m + 1)\left((2^m)^{t-1} - (2^m)^{t-2} + \cdots - 2^m + 1\right)$$

Mivel $1 \leq m < a$, így $3 \leq 2^m + 1 < 2^a + 1$. Azaz $2^m + 1$ valódi osztója $2^a + 1$-nek, és így $2^a + 1$ összetett. Ezzel a feladat állítását beláttuk.

2.21. Feladat megoldása.

Tegyük fel, hogy n összetett. Ekkor n előáll $n = tm$ alakban, ahol $1 < t, m < n$. Ekkor

$$2^n - 1 = 2^{tm} - 1 = (2^m)^t - 1^t$$
$$= (2^m - 1)\left((2^m)^{t-1} + (2^m)^{t-2} + \cdots + 1\right)$$

Mivel $2 \leq m < n$, így $3 \leq 2^m - 1 < 2^n - 1$. Azaz $2^m - 1$ valódi osztója $2^n - 1$-nek, és így $2^n - 1$ összetett. Ezzel a feladat állítását beláttuk.

Hivatkozások

[1] Martin Aigner, Günter M. Ziegler, *Bizonyítások a könyvből*, link.

[2] Butzer (1999), *"P. L. Chebyshev (1821–1894): A Guide to his Life and Work"*, Journal of Approximation Theory, 96: 111–138, doi:10.1006/jath.1998.3289

[3] P Erdős, *Über die reihe* $\sum \frac{1}{p}$ link.

[4] Eukleidész, Elements (Book IX), link vagy link.

[5] *Oeuvres De Fermat*, Publiées Par Les Soins De Mm. Paul Tannery Et Charles Henry Sous Les Auspices Du Ministère De L'Instruction Publique, 2006, link.

[6] Gauss, *Disquisitiones Arithmeticae*, 1801, link.

[7] J. Hadamard, *Sur la distribution des zéros de la fonction* $\zeta(s)$ *et ses conséquences arithmétiques*, Bull. Soc. Math. France 24(1896), 199–220; reprinted in *Oeuvres de Jacques Hadamard*, C.N.R.S., Paris, 1968, vol 1, 189–210.

[8] G. H. Hardy - E. M. Wright, *An Introduction to the Theory of Numbers*, link.

[9] J. P. Jones, D. Sato, H. Wada, D. Wiens, *Diophantine representation of the set of prime numbers*, American Mathematical Monthly, Mathematical Association of America, 83 (6) (1976) 449–464.

[10] E. Landau, *Vorlesungen über Zahlentheorie* 1927, I. köt. 67. old.

[11] Y. V. Matiyasevich, *Enumerable sets are Diophantine*, Doklady Akademii Nauk SSSR (in Russian). 191: 279–282 (1970), English translation in Soviet Mathematics 11 (2), pp. 354–357.

[12] C.-J. de La Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Ann. Soc. Sci. Bruxelles 20 (1896), 183–256.

[13] Szalay Mihály, *Számelmélet*, link.

[14] Tchebychef, P. L. (1899), Markov, Andrey Andreevich; Sonin, N. (eds.), *Oeuvres, vol. I*, New York: Commissionaires de l'Académie impériale des sciences, MR 0147353, Reprinted by Chelsea 1962.

[15] Tchebychef, P. L. (1907), Markov, Andrey Andreevich; Sonin, N. (eds.), *Oeuvres, vol. II*, New York: Commissionaires de l'Académie impériale des sciences, MR 0147353, Reprinted by Chelsea 1962.

[16] Wikipedia, *Formula for primes*, link.

[17] Wikipedia, *Largest known prime*, link.

[18] Wikipedia, *Adrien-Marie Legendre*, link.

[19] Wikipedia,*Leonhard Euler*, link.

[20] Wikipedia, Marin Mersenne, link.

[21] Wolfram Mathworld, *Prime-Generating Polynomial*, link.

[22] Fotó, *Erasztoszthenesz*, link.

[23] Fotó, *Eukleidész*, színezett fametszet, 1584, link.

[24] Fotó, *Marin Mersenne*, link.

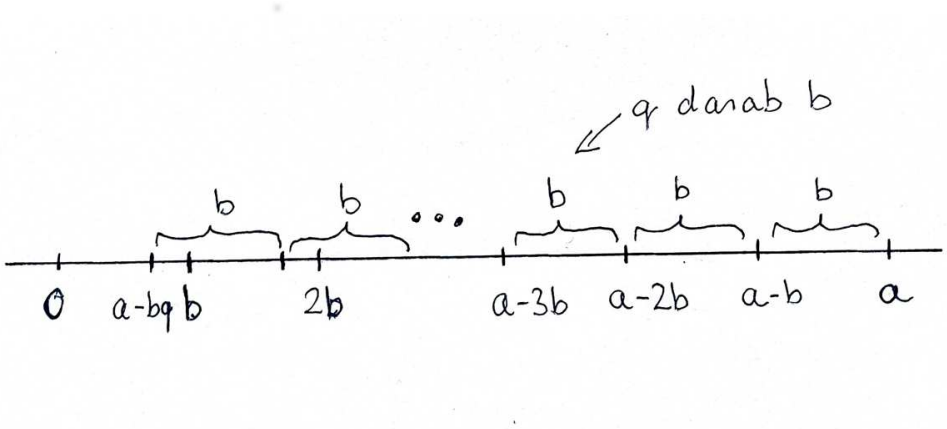
[25] Fotó, *Letter from Goldbach to Euler*, link.

3. Számelméleti alapfogalmak

Az egész számok körében az összeadás, kivonás, szorzás akárhányszor és egyértelműen végezhető el, az osztás azonban nem mindig. Két egész szám hányadosa már nem mindig lesz újból egész.

Az osztás általában kivezet az egész számok köréből. Van azonban az osztásnak olyan változata, amely nem igényel törtszámokat. Ez a maradékos osztás.

Legyen a és b két pozitív egész. Ha $a \geq b$, akkor vonjunk le b-t a-ból. Ha az $a - b$ különbség még mindig nagyobb vagy egyenlő b-nél, vonjunk le újból b-t. Ezt az eljárás folytassuk addig, amíg egy 0 és $b - 1$ közé eső számra nem jutunk.



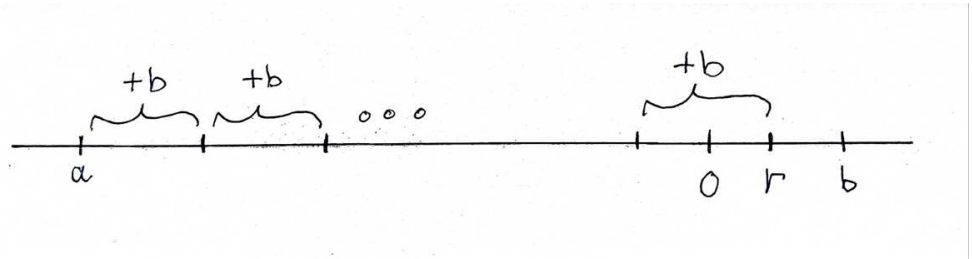
Az algoritmussal beláttuk olyan egész q és r létezését, amelyre

$$a = bq + r, \qquad 0 \leq r < b.$$

Ez esetben azt mondjuk a-t b-vel osztva a hányados q és a maradék r.

Ha $a < b$, akkor a hányados $q = 0$, a maradék $r = a$.

A maradékos osztás kiterjeszthető negatív számokra is. Ha a negatív, b pozitív, akkor a-hoz addig adunk b-ket, amíg 0 és b közé eső számhoz nem jutunk. Ábrával szemléltetve:



Általában a következő igaz:

3.1. TÉTEL. (Eukleidész, maradékos osztás lemma) *Adott a és $b \neq 0$ egész számokhoz léteznek olyan q és r egész számok, hogy*

$$a = bq + r, \qquad \text{ahol} \quad 0 \leq r < |b|.$$

Ez a felírás egyértelmű.

Azt hogy ilyen q és r létezik, már láttuk. A bizonyításból annyi hiányzik, hogy q és r egyértelmű a felírásban.

Előbb azonban, ha az alapoktól akarjuk kezdeni a bizonyítást szükségünk van pár nagyon egyszerű állítás igazolására.

Nyilvánvaló, hogy a 0-nak minden szám osztója, vagyis tetszőleges a-ra:

$$a \mid 0 \qquad \text{ugyanis} \quad 0 = 0 \cdot a.$$

Itt megjegyezendő, hogy $0 \mid 0$ is teljesül, noha 0-val nem szabad osztani...

Most megmutatjuk, hogy 0 az egyetlen olyan szám, amely végtelen sok osztóval rendelkezik.

3.2. TÉTEL. *Tetszőleges $a \neq 0$ számnak véges sok osztója van.*

A tétel bizonyítása az alábbi lemmán alapul:

3.3. LEMMA. *Ha $a \neq 0$ és $b \mid a$, akkor*

$$|b| \leq |a|.$$

3.3. LEMMA BIZONYÍTÁSA.

Mivel $b \mid a$ tehát van olyan q egész szám, amellyel

$$a = bq \tag{3.1}$$

Mivel $a \neq 0$, így $q \neq 0$, vagyis

$$|q| \geq 1.$$

Vagyis $|b|$-vel beszorozva az egyenlőtlenséget azt nyerjük, hogy

$$|b|\,|q| \geq |b|\,.$$

De ebből

$$|bq| \geq |b| \tag{3.2}$$

adódik, és (3.1) valamint (3.2) alapján:

$$|a| \geq |b|\,.$$

Ezzel a lemma állítását bebizonyítottuk.

3.2. TÉTEL BIZONYÍTÁSA.

Most $a \neq 0$ és $b \mid a$. A 3.3. Lemma alapján:

$$|b| \leq |a|\,.$$

Vagyis

$$-a \leq b \leq a.$$

De a $[-a, a]$ intervallumban csak véges sok egész szám van, tehát $a \neq 0$-nak véges sok osztója van, amivel tételünk bizonyítását befejeztük.

Ezután rátérhetünk Eukleidész maradékos osztás lemmájának bizonyítására.

3.1. Tétel bizonyítása.

A q és r létezését már a maradékos osztás bevezetésénél bebizonyítottuk (abban az esetben, ha b pozitív. A negatív b-k esete nagyon egyszerűen visszavezethető a pozitív b-k esetére, egyszerűen q helyett $-q$-t írunk...)

Most rátérünk az egyértelműség bizonyítására. Tegyük fel, hogy az állítással ellentétben, adott a és b-hez legalább két különböző q_1 és q_2 ill. r_1 és r_2 tartozik. Ekkor:

$$\begin{aligned} a &= bq_1 + r_1, \qquad \text{ahol} \quad 0 \leq r_1 < |b|\,, \\ a &= bq_2 + r_2, \qquad \text{ahol} \quad 0 \leq r_2 < |b| \end{aligned} \tag{3.3}$$

is teljesülne. De ebből:

$$bq_1 + r_1 = bq_2 + r_2$$
$$b(q_1 - q_2) = r_2 - r_1.$$

Vagyis

$$b \mid r_2 - r_1. \tag{3.4}$$

Azonban (3.3) miatt

$$|r_2 - r_1| < |b|\,.$$

Tegyük fel, hogy $r_2 - r_1 \neq 0$. Ekkor (3.4)-ból és 3.3. Lemmából adódóan

$$|b| \leq |r_2 - r_1|$$

következik. Így

$$|r_2 - r_1| < |b| \leq |r_2 - r_1|\,,$$

ami ellentmondás.

Tehát $r_2 - r_1 = 0$, vagyis $r_1 = r_2$. De ekkor

$$bq_1 = bq_2,$$

illetve $b \neq 0$-val való osztás után

$$q_1 = q_2,$$

ami ellentmondás.

Most az oszthatósági reláció legalapvetőbb tulajdonságaival fogunk foglalkozni.

3.1. Egységek

3.4. DEFINÍCIÓ. *Ha egy szám minden egész számnak osztója, akkor egységnek nevezzük.*

Az egységeket ezentúl ε-nal fogjuk jelölni.

3.5. TÉTEL. *A egész számok között két egység van: 1 és -1.*

3.5. TÉTEL BIZONYÍTÁSA.

(i) A -1 és $+1$ valóban egység, ugyanis $\forall a \in \mathbb{Z}$-re

$$a = 1 \cdot a$$

$$a = (-1) \cdot (-a).$$

(ii) A -1 és $+1$-en kívül nincs más egység:

Tegyük fel, hogy ε egység. Ekkor $\forall a \in \mathbb{Z}$-re

$$\varepsilon \mid a.$$

Speciálisan, $a = 1$-re is:

$$\varepsilon \mid 1.$$

A 3.3. Lemma alapján

$$|\varepsilon| \leq 1,$$

az $\varepsilon \in \{-1, 0, 1\}$ eseteket vizsgálva (a nulla egyetlen számnak: a nullának osztója), azt kapjuk, hogy $\varepsilon = 1$ vagy $\varepsilon = -1$.

Az oszthatóságot nem csak az egészek között, hanem más számkörökben is, pl. a Gauss egészek között, azaz

$$\mathcal{G} = \{a + bi : \ a, b \in \mathbb{Z}\},$$

vagy $\mathbb{Z}[\sqrt{2}]$-ben is vizsgálhatjuk.

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}.$$

Ehhez kapcsolódik a következő két feladat:

3.6. FELADAT. *Bizonyítsuk be, hogy $\mathcal{G}$-ben négy egység van: $1, -1, i, -i$.*

3.7. FELADAT. *Bizonyítsuk be, hogy $\mathbb{Z}[\sqrt{2}]$-ben:*

(i) *Az $1 + \sqrt{2}$ egység.*

(ii) *Végtelen sok egység létezik.*

A feladatok megoldásához először azt kell átgondolni, hogy egy S számkörben, hogyan érdemes definiálni az oszthatóságot.

Egyáltalán mi a számkör definíciója? Az algebrában már járatos olvasónak eláruljuk, hogy a számkör most kommutatív gyűrűt jelent.

De, ha valaki nem tanult még mélyebben haladó algebrát, akkor a példáinkban szereplő számkörökre úgy érdemes gondolni mint a valós vagy komplex számoknak olyan részhalmazaira, amelyből az összeadás, szorzás nem vezet ki. Ilyen a $\mathcal{G}$ is, és a $\mathbb{Z}[\sqrt{2}]$ is.

3.8. DEFINÍCIÓ. *Legyen S egy számkör $a, b \in S$. Ekkor azt mondjuk, a osztható b-vel, ha $\exists\, c \in S$, melyre*

$$a = bc.$$

Jelölése: $a \mid b$.

Meglepő tény, ha S a páros számok halmaza, akkor

$$2 \nmid 2 \qquad S\text{-ben},$$

mert hányadosuk $1 \notin S$.

Szerencsére 1 a legtöbb számkörnek eleme. Ez alapján megfogalmazható a következő tétel.

3.9. TÉTEL. *Legyen S egy számkör, és $1 \in S$. Ekkor $\varepsilon \in S$ akkor és csak akkor egység S-ben, ha*

$$\varepsilon \mid 1.$$

3.9. TÉTEL BIZONYÍTÁSA

Ha ε egység, akkor $\forall a \in S$-re $\varepsilon \mid a$. Ez $a = 1 \in S$-re is teljesül, vagyis $\varepsilon \mid 1$.

Fordítva, ha $\varepsilon \mid 1$, akkor $\exists c \in S$, hogy

$$1 = \varepsilon c.$$

Tehát tetszőleges $a \in S$-re

$$a = \varepsilon(ca),$$

vagyis $\varepsilon \mid a$.

Nem minden számkör tartalmazza az 1-et (ld. páros számok). De ha egy számkör nem tartalmazza az 1-et, akkor abban nincs egység, hiszen ekkor minden $a \in S$-re $a \nmid a$.

3.10. DEFINÍCIÓ. *A számkör egy a elemének egységszereseit a asszociáltjainak nevezzük.*

A 3.6. és 3.7. feladatok megoldását a fejezet végén adjuk meg.

3.2. Oszthatóság alaptulajdonságai

Először megnézzük, hogy az oszthatóságnak mint relációnak, milyen alaptulajdonságai vannak.

3.11. TÉTEL. *Ha az S számkörnek az 1 eleme, akkor az oszthatóság reflexív, antiszimmetrikus és tranzitív.*

3.11. TÉTEL BIZONYÍTÁSA.

1) Az oszthatóság reflexív, azaz $a \mid a$ $\forall a \in S$-re. Valóban a és a hányadosa 1, ami eleme a számkörnek.

2) Az oszthatóság antiszimmetrikus, azaz ha $a \mid b$ és $a \neq \varepsilon b$, ahol ε egység, akkor $b \nmid a$.

Tegyük fel ugyanis, hogy $a \mid b$ és $b \mid a$ egyszerre fenn áll. Ekkor alkalmas q-val és q'-vel:

$$b = aq,$$
$$a = bq'.$$

Így:

$$b = b(qq'),$$

vagyis $b \neq 0$ esetén $qq' = 1$, amiből a 3.9. Tétel értelmében, következik, hogy q és q' egység.

Ha pedig $b = 0$, akkor ebből már $a = 0$ adódik, ami ellentmond annak, hogy $a \neq \varepsilon b$ (ahol ε egység).

3) Ha $a \mid b$ és $b \mid c$, akkor $a \mid c$ (tranzitivitás), ugyanis

$$b = aq, \quad c = bq',$$

tehát

$$c = (aq)q' = a(qq').$$

3.12. Tétel. *Ha $a \mid b$ és $a \mid c$, akkor*

$$a \mid b + c, \quad a \mid b - c, \quad a \mid bk,$$

ahol k tetszőleges egész.

3.12. Tétel bizonyítása.

Tudjuk, hogy alkalmas q és q' egészekkel

$$b = aq, \quad c = aq',$$

tehát

$$b + c = a(q + q'),$$

$$b - c = a(q - q'),$$
$$bk = a(qk),$$

amiből az állítás már következik.

A 3.12. Tétel állítását ne próbáljuk meg megfordítani:

$$a \mid b + c \quad \not\Rightarrow \quad a \mid b \quad \text{és} \quad a \mid c.$$

Pl.: $7 \mid 10 + 4$, de $7 \nmid 10$ és $7 \nmid 4$.

A következő tételt a középiskolában már tanultuk:

3.13. TÉTEL. *Tetszőleges $A > 0$ egész szám felírható*

$$A = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0,$$

alakban, ahol

$$0 \leq a_i \leq 9, \quad \text{és} \quad a_n \neq 0.$$

Ebben a felírásban az a_i számjegyek egyértelműen vannak meghatározva.

Természetesen ez a tétel 10-es számrendszerről, tetszőleges b-alapú számrendszerre is általánosítható (ahol $b \geq 2$ egész szám):

3.14. TÉTEL. *Tetszőleges $A > 0$ egész szám felírható*

$$A = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0,$$

alakban, ahol

$$0 \leq a_i \leq b - 1, \quad \text{és} \quad a_n \neq 0.$$

Ebben a felírásban az a_i számjegyek egyértelműen vannak meghatározva.

A számjegyek meghatározására két módszer is ismert.

Egyrészt vehetjük a legnagyobb b-hatványt, amely A-nál nagyobb (legyen ez b^{n+1}), majd beszoríthatjuk A-t $a_n b^n$ és $(a_n+1)b^n$ közé:

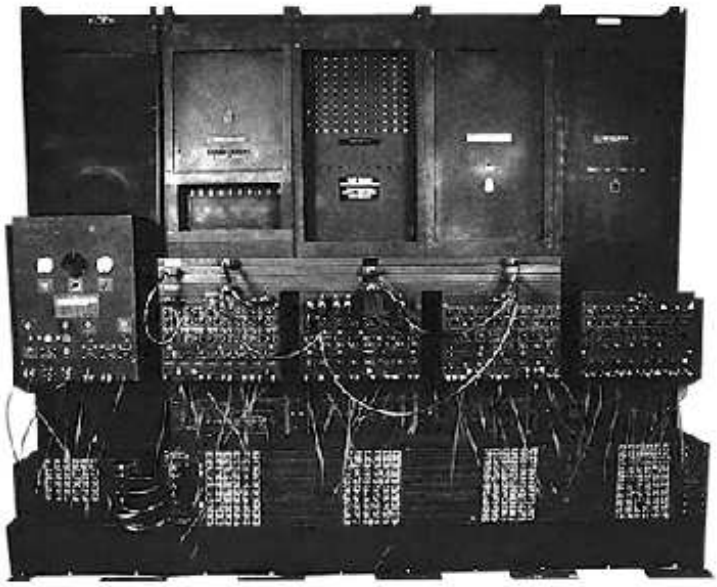
$$a_n b^n \leq A < (a_n+1)b^n,$$

meghatározva ezzel az a_n számjegyet. Majd rendre, hasonló módon meghatározzuk az $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$ számjegyeket.

Vagy pedig először az a_0 számjegyet határozzuk meg, észrevéve, hogy az A-nak a b-vel vett osztási maradéka. Majd rendre, hasonló módon meghatározzuk az $a_1, a_2, \ldots, a_n$ számjegyeket. Ennél bővebben a 3.13. és 3.14. Tételeket nem bizonyítjuk.

A történelem során sokféle számrendszert használtak. Manapság a 10-es számrendszeren kívül a legismertebb számrendszer a kettes, de az már kevésbé ismert, hogy a kettes számrendszer már ókori kínai írásokban is megjelent.

A kettes számrendszer leggyakoribb alkalmazása a számítógépekhez fűződik. Az első teljesen elektronikus számítógép, az ENIAC, a magyar származású Neumann János nevéhez fűződik.



Nagyon fontos számelméleti alapfogalom a legnagyobb közös osztó:

3.15. DEFINÍCIÓ. *Az a és b egész számok, ahol nem mindkettő 0, legnagyobb közös osztójának nevezzük azt a d számot, amelyre*

1. $d \mid a, d \mid b$ *tehát d közös osztó.*
2. d *a legnagyobb a közös osztók közül.*

Jelölése: $d = (a, b)$.

Gyakran azonban nem a természetes számok között keressük a legnagyobb közös osztót, hanem más számkörökben (az algebrát ismerő olvasó számára itt kommutatív gyűrűket is említhetünk), ahol nem mindig egyértelmű, hogy mit is jelent a „legnagyobb” kifejezés. Ennek megértéséhez jöjjön egy feladat:

3.16. FELADAT. *A $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : \ a, b \in \mathbb{Z}\}$ számkörben semelyik két számnak nincs legnagyobb közös osztója.*

A feladat megoldását a fejezet végén ismertetjük.

Tehát azért, hogy más számkörökben is tudjunk vizsgálódni, érdemes kiterjeszteni a legnagyobb közös osztó definícióját.

3.17. DEFINÍCIÓ. *Az a és b egész számok, ahol nem mindkettő 0, kitüntetett közös osztójának nevezzük azt a δ számot, amelyre*

1. $\delta \mid a$, $\delta \mid b$ *tehát δ közös osztó.*
2. *Ha $c \mid a$ és $c \mid b$, akkor $c \mid \delta$, vagyis δ az a és b összes közös osztójának többszöröse.*

Nyilvánvaló, hogy két egész számnak (most $\mathbb{Z}$-ben) mindig van legnagyobb osztója, de a kitüntetett közös osztó létezése már nem magától értendő.

Sőt, nem minden számkörben létezik kitüntetett közös osztó...

De szerencsénkre, a szokott egész számaink között jól definiált a kitüntetett közös osztó, sőt, egységszorzótól eltekintve megegyezik a legnagyobb közös osztóval. Ennek bizonyítása azonban egyáltalán nem könnyű.

Először csak azt látjuk be, hogyha δ létezik, akkor $\delta = \pm d$. Feltehetjük, hogy δ pozitív. Ha $\delta < d$, akkor δ nem lehetne többszöröse a d közös osztónak. Mivel d a legnagyobb közös osztó $\delta > d$ sem lehet, így $\delta = d$.

Az is világos, hogy tetszőleges számkörben, ha a kitüntetett közös osztó létezik, akkor az egységszorzótól eltekintve egyértelmű, ugyanis, ha van két különböző kitüntetett közös osztó: δ_1 és δ_2, akkor

$$\delta_1 \mid \delta_2 \quad \text{és} \quad \delta_2 \mid \delta_1.$$

Ez utóbbiból pedig következik, hogy δ_1 és δ_2 egymás egységszeresei, ld. 3.12. Tétel bizonyítását.

Vagyis a fő nehézség, hogy a kitüntetett legnagyobb közös osztó $\mathbb{Z}$-ben létezik.

Ennek bizonyítása az Euklideszi algoritmussal történik.

3.3. Euklideszi algoritmus

Az euklideszi algoritmus, nevét az ókori görög matematikusról, Eukleidészről kapta, aki az Elemekben írta le (Kr. e. 300 körül) [1]. Az egyik legrégibb, gyakran használt algoritmus.

Ez az algoritmus a következő:

Tegyük fel, hogy a és b két egész szám (nem mindkettő 0). Először elosztjuk a-t maradékosan b-vel. Majd b-t a maradékkal, és így tovább, mindig az osztót, az előző maradékkal:

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

Eljárásunk biztosan véges sok lépésen belül véget ér, előbb-utóbb eljutunk a 0 maradékhoz, hiszen a

$$|b| > r_1 > r_2 > \cdots \geq 0$$

sorozat korlátos, szigorúan monoton csökken és nemnegatív egész számokból áll.

Bebizonyítjuk, hogy az utolsó nem nulla maradék, azaz r_n lesz a kitüntetett közös osztó.

Először csak azt látjuk be, hogy r_n közös osztó. Ehhez alulról fölfele haladunk. Az algoritmus utolsó egyenlete alapján:

$$r_n \mid r_{n-1}.$$

Az utolsó előtti egyenletben $r_n \mid r_{n-1}$ és $r_n \mid r_n$, vagyis

$$r_n \mid r_{n-2}.$$

Hasonlóan haladva visszafele az eljárás végén megkapjuk

$$r_n \mid a \quad \text{és} \quad r_n \mid b,$$

azaz r_n közös osztó.

Az is világos, hogy r_n kitüntetett közös osztó. Most felülről lefele haladunk. Legyen c az a és b számok közös osztója: $c \mid a$ és $c \mid b$. Az algoritmus első egyenlete alapján:

$$c \mid a - bq_1 = r_1.$$

Lefele haladva, hasonlóan adódik rendre, hogy

$$c \mid r_2,\ c \mid r_3, \ldots, c \mid r_n.$$

Tehát r_n tetszőleges közös osztónak a többszöröse, azaz r_n kitüntetett közös osztó.

Összefoglalva az eddigiek $\mathbb{Z}$-re vonatkozó állításait:

3.18. TÉTEL. *Az egész számok között mindig létezik kitüntetett közös osztó, és az előjeltől eltekintve megegyezik a legnagyobb közös osztóval.*

Ez nem minden számkörben van így, de mivel az egészek között így van, ezért ezentúl, ha $\mathbb{Z}$ elemeiről beszélünk, akkor az egyszerűbb legnagyobb közös osztó kifejezést használjuk a kitüntetett közös osztóra is.

Szintén az euklideszi algoritmussal igazolható a következő tétel:

3.19. TÉTEL. *Legyen a és b egész számok (nem mindkettő 0). Ekkor a és b legnagyobb közös osztója felírható*

$$(a, b) = ax + by,$$

alakban, ahol x és y egész számok.

Megjegyezzük, hogy a fenti felírásban az x és y egész számok közül az egyik mindig pozitív a másik mindig negatív.

3.19. TÉTEL BIZONYÍTÁSA. Az eukliedszi algoritmusban felülről lefele haladunk. Ekkor:

$$a = a \cdot 1 + b \cdot 0,$$
$$b = a \cdot 0 + b \cdot 1.$$

Majd rendre az $r_1, r_2, \ldots, r_n$ maradékokat kifejezzük

$$r_m = ax_m + by_m$$

alakban. Ez teljes indukcióval igazolható.

$$a = bq_1 + r_1, \quad r_1 = a \cdot 1 + b(-q_1).$$

Azaz az indukció kezdőlépése $m = 1$ már készen is van. Azért nem egészen, mert van még egy kezdőlépés: $m = 2$. Ehhez:

$$\begin{aligned} b &= r_1 q_1 + r_2, \\ r_2 &= b - r_1 q_1, \\ &= b - (a \cdot 1 + b(-q_1)) q_2, \\ &= (1 + q_1 q_2) b - q_2 a. \end{aligned}$$

Ez is kész.

Az indukciós lépés a következő: ha $m = k-2$-re és $m = k-1$-re igaz az állítás, akkor $m = k$-ra is. Tudjuk:

$$\begin{aligned} r_{k-2} &= a x_{k-2} + b y_{k-2}, \\ r_{k-1} &= a x_{k-1} + b y_{k-1}. \end{aligned}$$

Azt is tudjuk, hogy:

$$r_{k-2} = r_{k-1} q_k + r_k.$$

Ezt átrendezve:

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1} q_k \\ &= (a x_{k-2} + b y_{k-2}) - (a x_{k-1} + b y_{k-1}) q_k \\ &= a(x_{k-2} - q_k x_{k-1}) + b(y_{k-2} - q_k y_{k-1}). \end{aligned}$$

Ezzel az állítást igazoltuk. Az összes r_m, nevezetesen az utolsó $r_n = (a, b)$ is előáll ilyen alakban. Ezzel a tétel állítását beláttuk.

Nagyon fontos megjegyezni, hogy az euklideszi algoritmus rendkívül gyors.

Ennek alapját a következő feladat adja:

3.20. FELADAT. *Az eukleideszi algoritmussal megadott* $r_1, r_2, \ldots, r_n$ *számokra mindig fennáll az*

$$r_i \leq \frac{r_{i-2}}{2}$$

összefüggés.

A 3.20. feladat alapján tetszőleges a és b egész számokra, az euklideszi algoritmus legfeljebb $2\log_2 |b| + 2$ lépésben véget ér.

Ezzel fejezetünk végére értünk. Nem maradt más hátra, mint a fejezetben megadott feladatok megoldásának ismertetése.

3.6. FELADAT MEGOLDÁSA.

Az világos, hogy $1, -1, i$ és $-i$ egységek $\mathcal{G}$-ben, hiszen mindegyik osztója az 1-nek:

$$1 = 1 \cdot 1 = (-1) \cdot (-1) = i \cdot (-i).$$

Most már csak azt kell bizonyítanunk, hogy más egység nincs $\mathcal{G}$-ben. Ehhez tegyük fel, hogy ε egység $\mathcal{G}$-ben. Ekkor

$$\varepsilon \mid 1.$$

Azaz $\exists\ \delta \in \mathcal{G}$, amelyre

$$\varepsilon \cdot \delta = 1.$$

A komplex számok konjugáltját véve

$$\overline{\varepsilon} \cdot \overline{\delta} = 1.$$

adódik. A fenti két egyenletet összeszorozva pedig

$$|\varepsilon| \cdot |\delta| = 1.$$

Így $|\varepsilon| = 1$. Ha $\varepsilon = a + bi$, akkor ez azt jelenti, hogy $a^2 + b^2 = 1$, vagyis

$$a = \pm 1, \ b = 0, \quad \text{vagy}$$
$$a = 0, \quad b = \pm 1.$$

Így $\varepsilon = a + bi$ valóban csak $\pm 1, \ \pm i$ lehet.

3.7. Feladat Megoldása.

(i): Az $1 + \sqrt{2}$ szám egység, hiszen $1 + \sqrt{2} \mid 1$, mivel

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1.$$

(ii): Ahhoz, hogy végtelen sok egység van elég belátni, hogy $(1 + \sqrt{2})^n$ egység $\forall \ n$-re. Az biztos, hogy $(1 + \sqrt{2})^n$ eleme a számkörnek, hiszen a binomiális tétel alapján

$$\begin{aligned}(1 + \sqrt{2})^n &= \sum_{i=0}^{n} \binom{n}{i} (\sqrt{2})^i \\ &= a + b\sqrt{2}\end{aligned} \tag{3.5}$$

alakú, ahol $a, b \in \mathbb{Z}$. Valóban, (3.5)-ben $(\sqrt{2})^i \in \mathbb{Z}$, ha i páros. Amennyiben i páratlan $(\sqrt{2})^i = r_i\sqrt{2}$, ahol $r_i \in \mathbb{Z}$.

Hasonlóan látható, hogy $(1 - \sqrt{2})^n$ is eleme a számkörnek. Ekkor:

$$(1 + \sqrt{2})^n (1 - \sqrt{2})^n = \Big((1 + \sqrt{2})(1 - \sqrt{2})\Big)^n = (-1)^n,$$
$$(1 + \sqrt{2})^n \mid (-1)^n,$$
$$(1 + \sqrt{2})^n \mid 1.$$

Vagyis $(1+\sqrt{2})^n$ egység.

3.16. Feladat megoldása.

Két számnak nincs legnagyobb közös osztója, mert minden közös osztónál található egy még nagyobb közös osztó. A 3.7. Feladat megoldása során láttuk $(1+\sqrt{2})^n$ egység, tehát $\forall a, b \in \mathbb{Z}[\sqrt{2}]$-re

$$(1+\sqrt{2})^n \mid a, \qquad (1+\sqrt{2})^n \mid b.$$

Vagyis $(1+\sqrt{2})^n$ mindegyik (a,b) számpárra közös osztó. De $n \to \infty$ esetén $(1+\sqrt{2})^n \to \infty$, vagyis a közös osztók minden határon túl nőnek, nincsen közöttük legnagyobb.

3.20. Feladat Megoldása.

Két eset: Ha $r_{i-1} \leq \frac{r_{i-2}}{2}$, akkor valóban $r_i < r_{i-1} \leq \frac{r_{i-2}}{2}$.

Ha viszont $r_{i-1} > \frac{r_{i-2}}{2}$, akkor nézzük az i-edik maradékos osztást:

$$r_{i-2} = r_{i-1}q_i + r_i,$$
$$r_i = r_{i-2} - r_{i-1}q_i < r_{i-2} - r_{i-1} < r_{i-2} - \frac{r_{i-2}}{2} = \frac{r_{i-2}}{2}.$$

Hivatkozások

[1] Eukleidész, Elements (Book IX), link vagy link.

[2] Fotó, *ENIAC*, link.

4. Prímek és Felbonthatatlanok

Eukleidész következőképpen definiálta a prímeket: $p > 1$ prím, ha 1-n és p-n kívül nincs más pozitív osztója.

Ezután rátérhetünk Eukleidész I. tételének [1] bizonyítására, mely szerint, ha p prím és a, b egész számok, akkor $p \mid ab$-ből következik $p \mid a$ vagy $p \mid b$.

2.6. TÉTEL BIZONYÍTÁSA. A fenti bizonyítás alapja az Eukleidészi algoritmus. Tudjuk:

$$p \mid ab.$$

Ha $p \mid a$ készen vagyunk. Ha $p \nmid a$, akkor tekintsük p és a legnagyobb közös osztóját: (a, p)-t. Ekkor

$$(a, p) \mid p,$$

de p-nek két pozitív osztója van 1 és p. Ha $(a, p) = p$, akkor $p \mid a$, de most $p \nmid a$. Így

$$(a, p) = 1.$$

Az Eukleidészi algoritmusnál tanultuk (a, p) felírható a és p lineáris kombinációjaként (ld. 3.19. Tétel):

$$1 = (a, p) = ax + py,$$

ahol $x, y \in \mathbb{Z}$. Ezt az egyenletet b-vel szorozva:

$$b = abx + pby.$$

De itt $p \mid ab$ és $p \mid py$, vagyis $p \mid b$. Ezzel Eukleidész I. tételét beláttuk.

A modern számelméletben azonban nem a klasszikus módon definiáljak a prímeket, avégből, hogy megkülönböztessük azt a két tulajdonságot, amiről eddig szó volt, nevezetesen, hogy p-nek egységen és önmaga asszociáltján kívül nincs osztója illetve $p \mid ab$-ből következik $p \mid a$ vagy $p \mid b$. Az alábbi két definíció tetszés szerinti számkörben értelmezhető:

4.1. DEFINÍCIÓ. *Az f 0-tól és egységtől különböző szám felbonthatatlan, ha $f = ab$ esetén (ahol a és b eleme a számkörnek) a vagy b mindig egység.*

4.2. DEFINÍCIÓ. *A p 0-tól és egységtől különböző szám prím, ha $p \mid ab$ esetén (ahol a és b eleme a számkörnek) mindig teljesül, hogy $p \mid a$ vagy $p \mid b$.*

Eukleidész klasszikus definíciója a felbonthatatlan számokkal van szinkronban.

4.3. TÉTEL. *Ha egy számkörnek eleme az 1, akkor igaz az, hogy a prímszámok mind felbonthatatlanok is.*

4.3. TÉTEL BIZONYÍTÁSA. Tegyük fel, hogy p prím. Bebizonyítjuk, hogy p felbonthatatlan. Ehhez az kell, hogy $p = ab$ esetén a vagy b egység. Mivel 1 eleme a számkörnek, ekkor

$$p \mid ab$$

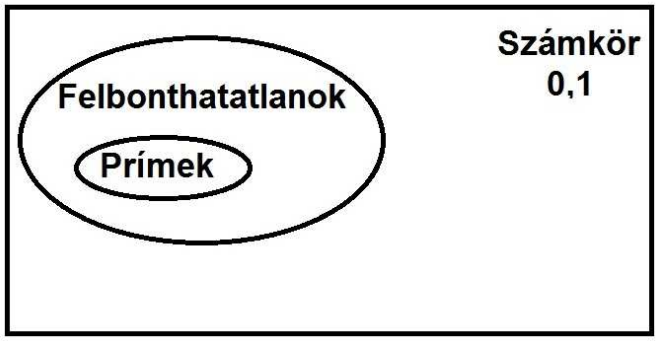
is teljesül. Mivel p prím, így $p \mid a$ vagy $p \mid b$. Szimmetrikus okokból feltehetjük $p \mid a$. Így $a = pa_0$. Azaz:

$$p = ab$$

$$p = pa_0b$$
$$1 = a_0b,$$

vagyis $b \mid 1$, így b egység.

Tételünk a következő ábrával szemléltethető:



Eukleidész I. tétele szerint:

4.4. TÉTEL. *A prímek és felbonthatatlanok $\mathbb{Z}$-ben egybeesnek.*

De $\mathbb{Z}$-n kívül más számkörök is vannak, ahol a két fogalom nem esik egybe. Pl.:

4.5. FELADAT. *Az*

$$S = \{a + b\sqrt{5} : \ a, b \in \mathbb{Z}\} \text{ számkörben}$$

a 2 felbonthatatlan, de nem prím.

Ennek bizonyítása az olvasónak szánt HF. Segítségként annyit adunk meg, hogy érdemes a norma fogalmát, és annak multiplikativitását használni, ahol is $N(a + b\sqrt{5}) = a^2 + 5b^2$. Az is igaz, hogy a fenti számkörben nem igaz a SzAT.

Hivatkozások

[1] Eukleidész, Elements (Book IX), link vagy link.

5. Polinomok racionális gyökei

Hogyan határozzuk meg egy egész együtthatós polinom racionális gyökeit?

Például a

$$6x^5 + x^4 - 2x^3 + 6x^2 + x - 2 = 0$$

egyenlet megoldásait keressük. Érdemes megnézni, van-e racionális gyök. Legyen $x = \frac{p}{q}$, ahol $(p, q) = 1$. Ekkor

$$6\left(\frac{p}{q}\right)^5 + \left(\frac{p}{q}\right)^4 - 2\left(\frac{p}{q}\right)^3 + 6\left(\frac{p}{q}\right)^2 + \frac{p}{q} - 2 = 0 \qquad / \cdot q^5.$$

Azaz

$$6p^5 + p^4q - 2p^3q^2 + 6p^2q^3 + pq^4 - 2q^5 = 0$$

Itt p a jobb és baloldalt is osztja, igen ám, de a baloldalon minden tag osztható p-vel kivéve $2q^5$-t. Mivel p az egész baloldalon álló kifejezést osztja, így $p \mid 2q^5$. Hasonló gondolatmenetet q-ra alkalmazva kapjuk:

$$p \mid 2q^5, \qquad q \mid 6p^5.$$

De $(p, q) = 1$ miatt:

$$p \mid 2, \qquad q \mid 6.$$

Így:

$$p \in \{-2, -1, 1, 2\}, \qquad q \in \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Végigpróbálva az összes esetet, látjuk, hogy

$$x = \frac{p}{q} = +\frac{1}{2},\ -\frac{2}{3},\ -1$$

a racionális megoldások. Ezt az eljárást racionális gyöktesztnek is nevezik.

Kiemelve $x - \frac{1}{2}$, $x + \frac{2}{3}$, $x + 1$-et a következőt is megkapjuk:

$$\begin{aligned} &6x^5 + x^4 - 2x^3 + 6x^2 + x - 2 \\ &\quad = 6\left(x - \frac{1}{2}\right)\left(x + \frac{2}{3}\right)(x+1)(x^2 - x + 1). \end{aligned}$$

Befejezésképp polinomok maradékos osztásának menetét ismertetjük. Az osztandó polinom legmagasabb fokú tagját elosztjuk az osztó polinom legmagasabb fokú tagjával. Majd visszaszorzunk és kivonunk, egészen addig ismételve az eljárást, amíg megkapjuk a hányadost és a maradékot. Az algoritmust az alábbi ábrával szemléltetjük:

$$\begin{array}{rl} & (6x^3 - 2x^2 + 6x + 3) \;:(x^2 - x + 1) = 6x + 4 \\ - & \underline{6x^3 - 6x^2 + 6x} \\ & \quad 4x^2 - 0x + 3 \\ - & \underline{\quad 4x^2 - 4x + 4} \\ & \quad\quad 4x - 1. \end{array}$$

Azaz

$$6x^3 - 2x^2 + 6x + 3 = (x^2 - x + 1)(6x + 4) + 4x - 1.$$

6. Kongruenciák (alapok)

A kongruenciák ma is használatos, kidolgozott elmélete Carl Friedrich Gauss [2] nevéhez fűződik

Magát a kongruencia fogalmat már Christian Goldbach is ismerte, csak ő Eulerhez írt levelében a $\equiv$ szimbólum helyett a $\mp$ jelet használta.

Sőt, közvetve, kongruenciát használ a több mint 2000 éves kínai maradéktétel is, amelyet a jegyzet 13. fejezetében ismertetünk.

6.1. DEFINÍCIÓ. *Azt mondjuk:*

$$a \equiv b \pmod{m}, \tag{6.1}$$

ha az m-mel vett osztási maradékuk ugyanaz. Más szóval:

$$m \mid a - b.$$

Szóban kifejezve (6.1)*-et: a kongruens b-vel modulo m.*

Példa:

$$15 \equiv 27 \pmod{6},$$

de

$$16 \not\equiv 27 \pmod{6}.$$

A $(\mathbf{mod\ 6})$ helyett lehet egyszerűen (6)-ot is írni.

Előfordul, hogy a való életben is megjelennek a modulusok.

Tegyük fel, hogy egy előadás minden második napon van (beleértve a vasárnapot is), és az első előadás hétfőre esik. Melyik előadás lesz először kedden?

Ha a szóban forgó előadás az $x+1$-edik, akkor a

$$2x \equiv 1 \qquad (\mathbf{mod}\ 7)$$

kongruenciát kell megoldanunk, megkeresni a legkisebb pozitív egész megoldást.

Ha nézzük az $x = 1, 2, 3, 4, \ldots$ eseteket, azt látjuk, a legkisebb pozitív egész megoldás az

$$x = 4.$$

Így az ötödik előadás esik keddre.

Előfordulnak magasabb fokú kongruenciák is, pl.

$$x^2 \equiv 1 \qquad (\mathbf{mod}\ 8)$$

-nak négy megoldása van:

$$x \equiv 1, 3, 5, 7 \qquad (\mathbf{mod}\ 8).$$

Néha akkor is használunk kongruenciákat, ha a kongruencia két oldalán nem egész számok vannak. Pl.:

$$\frac{3}{2} \equiv \frac{1}{2} \qquad (\mathbf{mod}\ 1),$$

vagy

$$-\pi \equiv \pi \qquad (\mathbf{mod}\ 2\pi).$$

Néhány elemi tulajdonság:

(i) $a \equiv b\ (m) \implies b \equiv a\ (m)$

(ii) $a \equiv b\ (m),\ b \equiv c\ (m) \implies a \equiv c\ (m)$

(iii) $a \equiv a'\ (m),\ b \equiv b'\ (m) \implies a+b \equiv a'+b'\ (m)$
$\implies ab \equiv a'b'\ (m)$

(iv) $x, y \in \mathbb{Z}$
$a \equiv a'\ (m)\ b \equiv b'\ (m) \implies xa+yb \equiv xa'+yb'\ (m)$

Ezeknek az alaptulajdonságoknak a bizonyítását az olvasóra bízzuk. Továbbá:

Ha $p(a,b,c,\ldots)$ egy többváltozós egész együtthatós polinom

$$a \equiv a'\ \ (m),\ b \equiv b'\ \ (m),\ c \equiv c'\ \ (m), \ldots,$$

akkor

$$p(a,b,c,\ldots) \equiv p(a',b',c',\ldots)\ \ (m).$$

Ezeket az alaptulajdonságokat használva már rátérhetünk a következő feladat megoldására:

2.25. Feladat megoldása. Tegyük fel, hogy van ilyen polinom: $f(x)$. Feltehető, hogy $f(x)$ főegyütthatója pozitív. Legyen $f(1) = q$. Tudjuk, hogy q prím. Tekintsük az $f(1+tq)$ alakú egész számokat. Ahogy $t \to \infty$ tudjuk, hogy $f(1+tq) \to \infty$, mivel $f(x)$ főegyütthatója pozitív. Mivel $f(1+tq)$ mindig prím és $f(1+tq) \equiv f(1) = q \equiv 0\ \pmod{q}$ (azaz $q \mid f(1+tq)$), ezért $f(1+tq)$ csak $\pm q$ lehet. De ez ellentmond $f(1+tq) \to \infty$-nak.

Láttuk, hogy kongruenciák esetében az összeadással, kivonással, szorzással ugyanúgy bánhatunk mint az egyenleteknél. Az osztással azonban lehetnek gondok! Például:

$$8 \equiv 20 \pmod{6} \quad / : 4.$$

De

$$2 \not\equiv 5 \pmod{6}.$$

Hogyan oszthatunk?

6.2. TÉTEL. *Legyen* $a, b, k \in \mathbb{Z}$ *és* $k \neq 0$. *Ekkor:*

$$\begin{aligned} ka &\equiv kb \pmod{m} \\ &\Downarrow \\ a &\equiv b \pmod{\frac{m}{(k,m)}}. \end{aligned}$$

Vagyis az előző példát tekintve:

$$\begin{aligned} 8 &\equiv 20 \pmod{6} \quad : 4 \\ 2 &\equiv 5 \pmod{\frac{6}{(6,4)}} \\ 2 &\equiv 5 \pmod{3} \end{aligned}$$

6.2. TÉTEL BIZONYÍTÁSA: Legyen $(k, m) = d$, $k = k_1 d$ és $m = m_1 d$. Ekkor $(k_1, m_1) = 1$. Így:

$$
\begin{aligned}
& ka \equiv kb \qquad (m) \\
& \Updownarrow \\
& m \mid ka - kb \\
& \Updownarrow \\
& \frac{k(a-b)}{m} \in \mathbb{Z} \\
& \Updownarrow \\
& \frac{k(a-b)}{m} = \frac{k_1 d(a-b)}{m_1 d} = \frac{k_1(a-b)}{m_1} \in \mathbb{Z}, \\
& \text{de mivel } (k_1, m_1)=1 \Updownarrow \\
& \frac{a-b}{m_1} \in \mathbb{Z} \\
& \Updownarrow \\
& m_1 \mid a - b \\
& \Updownarrow \\
& a \equiv b \pmod{m_1} = \pmod{\frac{m}{(k,m)}}.
\end{aligned}
$$

6.3. DEFINÍCIÓ. **Mod m** *teljes maradékrendszernek nevezzük azon számok halmazát, amelyeket úgy nyerünk, hogy az összes* mod m *maradékosztályból egy és csak egy reprezentáns elemet választunk.*

Példa.

$$1,\ 16,\ 24,\ 37,\ 42,\ 59,\ 63,\ 75,\ 88,\ 1000\ (10).$$

6.4. TÉTEL. *Adott egész számok akkor és csak akkor alkotnak teljes maradékrendszert* mod m*, ha*

a) számuk m*;*

b) közülük bármely két szám inkongruens mod m*.*

6.4. TÉTEL BIZONYÍTÁSA. A szükségesség nyilvánvaló.

Az elégségesség is azonnal adódik abból, hogy a b) tulajdonság teljesülése maga után vonja azt, hogy az adott számok mind más-más maradékosztályból valók. Az a) tulajdonság miatt pedig, az is világos, hogy valóban minden maradékosztályból van az adott számok között reprezentáns elem. Tehát teljes maradékrendszert alkotnak.

Gyakran használjuk a teljes maradékrendszerekre vonatkozó alábbi tételt.

6.5. TÉTEL. *Legyen*

$$r_1, r_2, \ldots, r_m$$

teljes maradékrendszer mod m*. Legyen továbbá*

$$(a, m) = 1 \quad \text{és} \quad b \quad \text{tetszőleges.}$$

Ekkor

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

is teljes maradékrendszer mod m*.*

6.5. TÉTEL BIZONYÍTÁSA. Mivel az új rendszer elemeinek száma is m, tehát az előző tétel alapján csak azt kell még bizonyítani, hogy páronként inkongruensek mod m.

Ez fennáll, ha ugyanis az állítással ellentétben volna köztük két kongruens szám mod m, pl.

$$ar_i + b \equiv ar_j + b \qquad (m),$$

akkor

$$\begin{aligned} ar_i &\equiv ar_j \qquad (m) \\ r_i &\equiv r_j \qquad \left(\frac{m}{(a,m)}\right) \\ r_i &\equiv r_j \qquad (m) \end{aligned}$$

következne, ami ellentmond annak, hogy az $r_1, r_2, \ldots, r_m$ számok mod m teljes maradékrendszert alkotnak.

(Megjegyezzük, hogy a tétel $(a,m) \neq 1$ esetén nem érvényes.)

6.6. Definíció. *Az (a) maradékosztályt* mod m redukált maradékosztálynak *nevezzük, ha*

$$(a,m) = 1.$$

6.7. Definíció. Mod m *redukált maradékrendszernek nevezzük a számok olyan halmazát, amelyet úgy nyerünk, hogy egy és csak egy reprezentánst választunk a* mod m *redukált maradékosztályokból.*

Példa: Mod 30 redukált maradékrendszer:

$$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29.$$

6.8. Definíció. *A* mod m *redukált maradékrendszer elemeinek számát $\varphi(m)$-mel jelöljük.*

Ezzel ekvivalens definíció a következő:

6.9. Definíció. *Az m-nél nem nagyobb, m-hez relatív prím pozitív egészek száma: $\varphi(m)$.*

Példa: $\varphi(30) = 8$.

6.10. Tétel. *Ha az n pozitív egész prímtényezős felbontása $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, akkor*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

Az általános képlet és a definíció alapján is könnyen látható, hogy ha p prím, akkor $\varphi(p) = p - 1$, illetve $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, ha $\alpha \in \mathbb{Z}^+$.

6.10. Tétel bizonyítása. A 17. fejezetben bizonyítjuk.

Példa:

$$\begin{aligned}
\varphi(30) &= 30 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \\
&= 30 \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{3} \cdot \frac{4}{5} = 8. \\
\varphi(45) &= 45 \cdot \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 24.
\end{aligned}$$

6.11. Tétel. *Adott számok akkor és csak akkor alkotnak redukált maradékrendszert* mod m*, ha*

a) *számuk $\varphi(m)$,*

b) *közülük bármely két szám inkongruens* mod m*,*

c) *mindannyian relatív prímek m-hez.*

6.11. Tétel bizonyítása. A szükségesség nyilvánvaló. Az elégségesség következik abból, hogy b) alapján minden szám más maradékosztályhoz tartozik (tehát minden maradékosztályból legfeljebb egy elemet választottunk ki), továbbá csak redukált maradékosztályból vannak elemek c) miatt.

Mivel a halmaz elemszáma pont $\varphi(m)$, ez csak úgy lehet, ha minden redukált maradékosztályból pontosan egy elemet választunk ki, tehát ekkor ezek a számok valóban redukált maradékrendszert alkotnak mod m.

6.12. Tétel. *Ha $r_1, r_2, \ldots, r_{\varphi(m)}$ mod m redukált maradékrendszer, továbbá $(a, m) = 1$, akkor az*

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

is redukált maradékrendszer mod m.

6.12. Tétel bizonyítása. A rendszer elemeinek száma nyilván $\varphi(m)$, páronként inkongruensek mod m, ugyanis ha

$$ar_i \equiv ar_j \qquad (m),$$

akkor $(a, m) = 1$ miatt

$$r_i \equiv r_j \qquad (m)$$

következne, ami ellentmond a feltételeknek. Továbbá

$$(r_i, m) = 1 \quad \text{és} \quad (a, m) = 1$$

miatt

$$(ar_i, m) = 1 \qquad (i = 1, 2, \ldots, \varphi(m)).$$

Ezzel a bizonyítást teljes egészében befejeztük.

Ezután rátérhetünk a számelmélet egyik legnevezetesebb tételének ismertetésére:

6.13. TÉTEL. (Euler-Fermat) *Legyen*

$$(a, m) = 1.$$

Ekkor

$$a^{\varphi(m)} \equiv 1 \qquad (m).$$

A tétel speciális esete, a kis-Fermat tétel eredete 1640-ig nyúlik vissza, amikor is Fermat bizonyítás nélkül megfogalmazta prímekre vonatkozó állítását. Euler 1736-ban bizonyította be tételét [1].

Euler 14 éves korától teológiát tanult, apja lelkésznek szánta. De Eulert a matematika sokkal jobban érdekelte. Magánúton, könyvekből tanult. Johann Bernoulli győzte meg Euler apját, hogy fiából neves matematikus lehet.

6.13. TÉTEL BIZONYÍTÁSA. Legyen

$$r_1, r_2, \ldots, r_{\varphi(m)} \tag{6.2}$$

redukált maradékrendszer mod m. Ekkor $(a, m) = 1$ miatt, a 6.12. tételt használva

$$ar_1, ar_2, \ldots, ar_{\varphi(m)} \tag{6.3}$$

is redukált maradékrendszer lesz mod m. Így (6.2)-ben és (6.3)-ban az elemek szorzata kongruens modulo m, azaz

$$r_1 r_2 \ldots r_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \qquad (m)$$

adódik.

Mivel $(r_i, m) = 1$, az összes r_i-vel lehet egyszerűsíteni, és így azt nyerjük, hogy

$$a^{\varphi(m)} \equiv 1 \qquad (m),$$

amivel az állításunkat bebizonyítottuk.

FONTOS: A tételben $(a, m) = 1$!

Amikor az m prím és $\varphi(m) = \varphi(p) = p - 1$, akkor a tétel speciális esete a kis-Fermat tétel.

6.14. TÉTEL. (kis Fermat-tétel) *Ha*

$$(a, p) = 1,$$

akkor

$$a^{p-1} \equiv 1 \qquad (p).$$

A kis Fermat-tételt

$$a^p \equiv a \qquad (\mathrm{mod}\ p)$$

alakban is szokás kimondani, ahol a tetszőleges természetes szám.

Az Euler–Fermat-tétel és a kis-Fermat-tétel számtalan bizonyításban, feladatban szerepel.

Lássunk egy példát, amely a már szóba került „Prímképletek” témakörhöz kapcsolódik.

6.15. TÉTEL. *Legyen P egy több- (k-változós) egész együtthatós polinom, és definiáljuk az f függvényt*

$$f(n) = P(n, 2^n, 3^n, \ldots, k^n)$$

képlettel. Amennyiben $f(n) \to \infty$, ha $n \to \infty$, akkor $f(n)$ függvény végtelen sok egész n értékre összetett.

6.16. MEGJEGYZÉS. *Itt valóban szükséges az $f(n) \to \infty$ feltétel. Gondoljunk arra az esetre, amikor*

$$f(n) = 2^n \cdot 3^n - 6^n + 5.$$

Bizonyítás: Tegyük fel, hogy az állítás nem igaz, és $\exists\, N_0$ küszöbérték, hogy

$$n > N_0$$

esetén $f(n)$ mindig prímszám.

Legyen n olyan, hogy

$$f(n) = p, \ \text{ ahol } \ p \ \text{ prím, és } \ p > k.$$

Tekintsük azokat az m-eket, amelyek felírhatók

$$m = n + tp(p-1)$$

alakban, ahol t egész szám. Nyilván

$$t \to \infty \text{ esetén } f\big(n + tp(p-1)\big) \to \infty.$$

Ekkor

$$m \equiv n \pmod{p}.$$

Másrészt

$$\begin{aligned} 2^m &\equiv 2^{n+tp(p-1)} = 2^n \cdot 2^{tp(p-1)} \\ &= 2^n (2^{p-1})^{tp} \equiv 2^n \cdot 1^{tp} \equiv 2^n \pmod{p} \end{aligned}$$

a kis Fermat-tétel miatt. Hasonlóan

$$\begin{aligned} 3^m &\equiv 3^n \pmod{p}, \\ 4^m &\equiv 4^n \pmod{p}, \\ &\vdots \\ k^m &\equiv k^n \pmod{p}. \end{aligned}$$

Itt mindig azt használtuk $2 < a \leq k$ esetén:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ehhez szükséges feltétel $(a, p) = 1$, ami azért igaz, mert $2 \leq a \leq k < p$. Vagyis

$$n \equiv m,\ 2^n \equiv 2^m,\ 3^n \equiv 3^m, \ldots,\ k^n \equiv k^m \pmod{p}.$$

Azaz

$$P(n, 2^n, 3^n, \ldots, k^n) \equiv P(m, 2^m, 3^m, \ldots, k^m) \pmod{p}$$

$$f(n) \equiv f(m) \pmod{p}.$$

De $f(n) = p$, azaz $0 \equiv f(n) \pmod{p}$. Vagyis

$$\begin{aligned} 0 &\equiv f(m) \qquad \bmod p \\ p &\mid f(m). \end{aligned}$$

Amennyiben $m = n + tp(p-1) > N_0$ $f(m)$ prím, de $p \mid f(m)$ miatt ez csak úgy lehet, ha

$$f(m) = \pm p,$$

viszont $t \to \infty$ esetén

$$f(m) = f\big(n + tp(p-1)\big) \to \infty,$$

ellentmondás.

Hivatkozások

[1] Leonhard Euler (presented: August 2, 1736; published: 1741) "Theorematum quorundam ad numeros primos spectantium demonstratio" (A proof of certain theorems regarding prime numbers), Commentarii academiae scientiarum Petropolitanae, 8 : 141–146.

[2] Carl Gauss, *Disquisitiones Arithmeticae* 1798, link.

[3] Fotó, *Leonard Euler, (Emanuel Handmann festménye 1752)*, link.

[4] Fotó, *Gauss portréja (Gottlieb Biermann, 1887)*, link.

7. Moduláris hatványozás

Példa. Határozzuk meg 2^{331} 17-es maradékát!

Nézzük a számolás menetét. A kis-Fermat tétel miatt:

$$2^{16} \equiv 1 \ (17).$$

Így:

$$2^{160} \equiv 1 \ (17) \quad 2^{320} \equiv 1 \ (17).$$

Továbbá:

$$2^{331} = 2^{320} \cdot 2^{11} \equiv 2^{11} \ (17).$$

Írjuk fel a 2^{2^k} alakú hatványok 17-es maradékát egy táblázatban. Az elkészítés során minden rubrikánál az előzőt négyzetre emeljük, majd redukáljuk mod 17:

Hatvány	1	2^1	2^2	2^4	2^8
mod 17	1	2	4	-1	1

Majd 2^{11}-ben a kitevőt kettőhatványok összegeként felírva kapjuk a következőt:

$$2^{11} \equiv 2^{8+2+1} \equiv 2^8 \cdot 2^2 \cdot 2^1 = 1 \cdot 4 \cdot 2 \equiv 8 \qquad (17).$$

8. Lineáris kongruencia

Lineáris kongruenciákkal sokoldalú alkalmazhatósága miatt már az ókori Indiában is foglalkoztak (pl. csillagászatban az égitestek mozgásának kiszámolása során). A fejezet első részében szó lesz arról, hogy a φ segítségével, hogyan oldható meg a lineáris kongruencia. Majd rátérünk Brahmagupta (598-668) indiai matematikus módszerére, amely az előbbinél lényegesen gyorsabb. Brahmagupta-ról érdemes még megjegyezni, hogy ő vezette be a nulla használatát, és ismertette a negatív számokkal való műveleteket is. Az alábbi kép hindu csillagászt ábrázol:

Először a lineáris kongruencia megoldhatóságról szóló tételt ismertetjük:

8.1. TÉTEL. *Az*

$$ax \equiv b \qquad (m)$$

kongruencia megoldhatóságának szükséges és elégséges feltétele az

$$(a, m) \mid b.$$

A megoldások száma (megoldhatóság esetén) (a, m).

A tételben a megoldások számát mindig az eredeti modulus szerint értjük.

8.1. Tétel bizonyítása.

a) Szükségesség: Tegyük fel, hogy van olyan x_0, amely megoldása a kongruenciának, vagyis

$$ax_0 \equiv b \qquad (m).$$

Ekkor

$$m \mid ax_0 - b,$$

tehát létezik olyan y_0 egész szám, hogy

$$ax_0 - b = my_0,$$

vagyis

$$ax_0 - my_0 = b.$$

De

$$(a, m) \mid a, \qquad (a, m) \mid m,$$

tehát

$$(a, m) \mid ax_0 - my_0 = b$$

is teljesül.

b) Elégségesség:

Jelöljük a és m legnagyobb közös osztóját d-vel. Így feltételünk szerint

$$d \mid b,$$

vagyis

$$b = db'$$

alakú. Mivel

$$d = (a, m),$$

ezért a 3.19. Tételt alkalmazva látható, hogy léteznek olyan x^* és y^* egészek, melyekre

$$d = ax^* + my^*.$$

Így

$$b = (ax^* + my^*)b'.$$

Vagyis

$$m \mid b - ab'x^*,$$

azaz

$$a(b'x^*) \equiv b \qquad (m)$$

következik. Ezzel bebizonyítottuk, kongruenciánkat az

$$x \equiv x^*b' \qquad (m)$$

szám kielégíti, tehát a kongruenciánk megoldható.

c) A megoldások száma:

Tegyük fel, hogy kongruenciánk megoldható, vagyis $(a, m) = d$ jelöléssel

$$d \mid b.$$

Ekkor

$$a = a'd, \;\; m = m'd, \;\; b = b'd \;\text{ és }\; (a', m') = 1$$

teljesül. Így a kongruencia

$$a'dx \equiv b'd \qquad (\mathrm{mod}\ m'd) \tag{8.1}$$

alakra hozható. Itt d-vel egyszerűsítve

$$a'x \equiv b' \qquad (\mathrm{mod}\ m'). \tag{8.2}$$

Vagyis (8.1) összes megoldása a (8.2) megoldásai közül kerül ki.

Megmutatjuk, hogy (8.2)-nek mod m' pontosan 1 megoldása van. (Azt, hogy van megoldása, az előbbiekből tudjuk.)

Legyen $r_1, r_2, \ldots, r_{m'}$ teljes maradékrendszer. Ekkor $a'r_1, a'r_2, \ldots, a'r_{m'}$ is teljes maradékrendszer (ld. 6.12. tétel). Tehát az r_i számok között pontosan 1 van, amelyre

$$a'r_i \equiv b' \qquad (m').$$

Azaz az eredeti (8.1) kongruencia megoldásai az

$$x = r_i + km' \qquad (k = 0, \pm 1, \pm 2, \ldots)$$

számok közül kerülhetnek ki. Nyilván minden

$$x = r_i + km'$$

alakú szám megoldása (8.1)-nek, hiszen (8.1) ekvivalens (8.2)-vel. Azonban az

$$x = r_i + km' \qquad (k = 0, \pm 1, \pm 2, \ldots)$$

alakú számok között $\frac{m}{m'} = d = (a, m)$ inkongruens van modulo m. Ugyanis

$$\begin{gathered} r_i + k_1 m' \equiv r_i + k_2 m' \qquad (m) \\ \Updownarrow \\ k_1 m' \equiv k_2 m' \qquad (m) \end{gathered}$$

$$\Updownarrow$$

$$k_1 m' \equiv k_2 m' \qquad (dm')$$

$$\Updownarrow$$

$$k_1 \equiv k_2 \qquad (d).$$

Ezzel a megoldások számára vonatkozó állítást is igazoltuk.

8.1. Lineáris kongruencia megoldása φ-vel

A lineáris kongruencia megoldására a legkönnyebben megjegyezhető módszer az alábbi:

8.2. TÉTEL. *Legyen* $(a, m) = 1$. *Ekkor az*

$$ax \equiv b \qquad (\mathrm{mod}\ m)$$

kongruencia egyetlen megoldása

$$x \equiv a^{\varphi(m)-1} b \qquad (\mathrm{mod}\ m).$$

8.2. TÉTEL BIZONYÍTÁSA. Az előző tételt alkalmazva adódik, hogy pontosan egy megoldás van modulo m. Ez az egy megoldás pedig

$$x \equiv a^{\varphi(m)-1} b \pmod{m},$$

ugyanis ekkor

$$ax \equiv a^{\varphi(m)} b \pmod{m}. \tag{8.3}$$

Az Euler–Fermat-tétel szerint

$$a^{\varphi(m)} \equiv 1 \qquad (\mathrm{mod}\ m),$$

ezt (8.3)-mal összevetve

$$ax \equiv b \pmod{m}$$

adódik.

Példa: Oldjuk meg a

$$21x \equiv 14 \qquad (35)$$

kongruenciát!

Mivel $(21, 35) = 7 \mid 14$, a kongruencia megoldható, és 7 inkongruens megoldása van mod 35. A kongruenciát 7-tel egyszerűsítve

$$3x \equiv 2 \qquad \left(\frac{35}{(7,\ 35)}\right)$$

$$3x \equiv 2 \qquad (5)$$

adódik, amelyben már $(3,\ 5) = 1$. Ennek a kongruenciának egyetlen megoldása

$$x_0 \equiv 3^{\varphi(5)-1} \cdot 2 \qquad (5),$$

vagyis

$$x_0 \equiv 3^3 \cdot 2 \qquad (5),$$

tehát

$$x_0 \equiv 4 \qquad (5).$$

Tehát az eredeti kongruencia megoldásai:

$$x \equiv 4,\ 9,\ 14,\ 19,\ 24,\ 29,\ 34 \qquad (35).$$

8.2. Lineáris kongruencia megoldása eukleidészi algoritmussal

Az alábbiakban Brahmagupta módszerét ismertetjük, de a modern terminológiát követve. Brahmagupta módszerét Diophantosz munkáját folytatva vezette le.

Tekintsük az

$$ax \equiv b \pmod{m} \tag{8.4}$$

kongruenciát, ahol $(a, m) = 1$.

Ha $(a, m) = 1$, akkor létezik egy mod m egyértelműen meghatározott a^* vagy a^{-1} elem, amelyre

$$aa^* \equiv 1 \pmod{m}.$$

Erre az a^*-ra teljesül:

$$a^* \equiv a^{\varphi(m)-1} \pmod{m},$$

de a^* az eukleidészi algoritmussal is meghatározható. Ezt fogjuk most megtanulni...

Ha egyszer a^*-ot meghatároztuk, akkor (8.4)-et a^*-gal szorozva a következőt kapjuk:

$$\begin{aligned} ax &\equiv b \pmod{m} \quad / \cdot a^* \\ aa^*x &\equiv ba^* \pmod{m} \\ x &\equiv ba^* \pmod{m}. \end{aligned}$$

Ez megadja a lineáris kongruencia megoldását.

Írjuk fel a-ra és m-re az eukleidészi algoritmust:

$$
\begin{aligned}
a &= q_1 m + r_1, && \text{ahol } 0 < r_1 < |m|\,, \\
m &= q_2 r_1 + r_2, && \text{ahol } 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, && \text{ahol } 0 < r_3 < r_3, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, && \text{ahol } 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_{n+1} && (r_{n+1} = 0).
\end{aligned}
$$

Láttuk $\forall\ r_i$ felírható $r_i = ax_i + my_i$ alakban, ezek az x_i, y_i-k rekurzívan adódnak az eukleidészi algoritmus lépéseinek átrendezésével (ld. 3.19. Tétel bizonyítása). Azaz

$$
\begin{aligned}
1 = (a, m) = r_n &= ax_n + my_n, \\
ax_n + my_n &\equiv 1 \pmod{m} \\
ax_n &\equiv 1 \pmod{m}
\end{aligned}
$$

Vagyis x_n-nek m-mel vett osztási maradéka megadja a^*-ot.

Brahmagupta módszere azért jóval gyorsabb mint a φ-re épülő módszer, mert nem szükséges faktorizációs algoritmusokat használni (ami a φ kiszámításához nélkülözhetetlen). A módszer az eukleideszi algoritmusra alapozódik, amely nagyon gyors: ha m a modulus az algoritmus kevesebb mint $3 \log_2 m$ lépésben véget ér.

Hivatkozások

[1] "The Hindoos" vol. II, The Library of Entertaining Knowledge (1835), facing page 318, link.

[2] Veronica Mate, *Ancient India: Linear Congruences*, link.

9. Lineáris Diofantikus egyenletek

Diofantikus (vagy diofantoszi) egyenletnek általában olyan egész együtthatós algebrai egyenletet nevezünk, melynek a megoldásait az egész számok körében, vagy esetleg a racionális számok körében keressük.

Egy többismeretlenes magasabb-fokú egyenlet összes egész megoldásait megkeresni általában nehéz feladat, de bizonyos speciális esetekben, azonban mégis könnyen megtalálhatjuk a megoldásokat.

Diophantosz korának híres probléma megoldója volt, de a diofantikus egyenletek esetében ő is legtöbbször csak arra szorítkozott, hogy felírta az egyenletet, és mutatott hozzá egy egész megoldást.

Egy ókori feladvány Diophantosz sírfelirata is, amelynek megfejtését az olvasóra bízzuk:

„Az istenek kegyelméből élete egyhatodát gyermekként töltötte. Eltelt életének még egytizenketted része, és kiserkent szakálla. További hetedrész múltán esküvői gyertyái égtek. Öt évvel a lakodalom után fia született, de ó, jaj! A későn született, gyenge gyermeket elragadta a kegyetlen sors, alighogy apja életének felét leélte. Gyászoló apja a számelméletben keresett vigaszt, ám négy év múlva az ő élete is véget ért.”

Példa. Oldjuk meg a

$$43x + 25y = 98 \tag{9.1}$$

lineáris diofantikus egyenletet. Azaz határozzuk meg az összes x és y egész számot, amelyre (9.1) fennáll.

Lineáris diofantoszi egyenletek megoldása többféleképpen is történhet, azonban mielőtt rátérnénk a leggyorsabb általános módszer ismertetésére, lássuk előbb példánk egy lehetséges megoldását: Ha

$$43x + 25y = 98,$$

akkor

$$\begin{aligned} 43x &\equiv 98 \pmod{25}, \\ 18x &\equiv 23 \pmod{25}. \end{aligned}$$

A lineáris kongruenciát megoldva kapjuk:

$$x \equiv 11 \pmod{25}.$$

Vagyis a lineáris diofantikus egyenlet összes megoldásai az $x = 11 + 25t$ alakú számok között keresendők. Ekkor:

$$\begin{aligned} 43\,(11 + 25t) + 25y &= 98 \\ 473 + 43 \cdot 25t + 25y &= 98 \\ 25y &= -375 - 43 \cdot 25t \\ y &= -15 - 43t. \end{aligned}$$

Tehát az összes megoldás $x = 11 + 25t$, $y = -15 - 43t$, ahol t egész szám.

Lineáris kongruenciánk általános megoldására a következő tétel vonatkozik.

9.1. TÉTEL. *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:*

$$x' = x_0 + t\frac{b}{(a,b)}, \qquad y' = y_0 - t\frac{a}{(a,b)},$$

ahol $t = 0, \pm 1, \pm 2, \ldots$

(iii) *Az egyenlet egy megoldását az eukleidészi algoritmussal kapjuk meg.*

9.1. TÉTEL BIZONYÍTÁSA.

(i) Ha $\exists$ megoldás, akkor $(a, b) \mid c$: Legyen x_0, y_0 egy megoldás. Ekkor:

$$ax_0 + by_0 = c.$$

Vagyis:

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

Ha $(a, b) \mid c$, akkor $\exists$ megoldás: Legyen $c = (a, b)c_0$. Az eukleidészi algoritmussal található x^* és y^* (ld. 3.19. Tétel), amelyre

$$(a, b) = ax^* + by^* \qquad / \cdot c_0$$

$$(a,b)c_0 = a(x^*c_0) + b(y^*c_0)$$
$$c = a(x^*c_0) + b(y^*c_0).$$

Azaz $x_0 = x^*c_0$, $y_0 = y^*c_0$ megoldás. Ez egyúttal a tétel (iii) részét is igazolja.

(ii) Legyen x', y' egy megoldás, és x_0, y_0 egy rögzített megoldás.

$$\begin{aligned} ax' + by' &= c \qquad (= ax_0 + by_0) \\ ax' + by' &= ax_0 + by_0 \\ a(x' - x_0) &= b(y_0 - y') \\ \frac{a}{(a,b)}(x' - x_0) &= \frac{b}{(a,b)}(y_0 - y') \end{aligned} \tag{9.2}$$

Ekkor:

$$\frac{a}{(a,b)} \mid \frac{b}{(a,b)}(y_0 - y').$$

De $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$ miatt

$$\frac{a}{(a,b)} \mid y_0 - y'.$$

Vagyis $\exists\, t \in \mathbb{Z}$

$$y_0 - y' = \frac{a}{(a,b)}t,$$
$$y' = y_0 - \frac{a}{(a,b)}t.$$

Ezt (9.2)-be írva

$$\frac{a}{(a,b)}(x' - x_0) = \frac{b}{(a,b)}\frac{a}{(a,b)}t,$$
$$x' = x_0 + \frac{b}{(a,b)}t.$$

Ezzel a tétel állítását igazoltuk.

A lineáris diofantikus egyenletek elmélete kiterjeszthető több ismeretlenre is. Így például a megoldhatóságra vonatkozó tétel analogonja a következő:

9.2. TÉTEL. *Az*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$$

lineáris diofantikus egyenlet akkor és csak akkor oldható meg, ha

$$(a_1, a_2, \ldots, a_n) \mid c.$$

Ezt a tételt nem bizonyítjuk.

Hivatkozások

[1] Fotó, Diophantosz, Matematikus, 210 - 290 B.C., Alexandria, link.

10. Racionális, Irracionális?

Általában Hippaszosznak, Püthagorasz egyik tanítványának tulajdonítják az irracionális számok felfedezését azáltal, hogy megadta az első (talán geometriai) bizonyítást a $\sqrt{2}$ irracionalitására. A legenda szerint Püthagorasz nem tudta elfogadni az irracionális számok létezését, ezért Hippaszoszt fulladásos halálra ítélte. De van olyan történet is, amely szerint Hippaszoszt megfojtották Püthagorasz tanítványai, vagy az is lehet, hogy csak egyszerűen kizárták a csoportjukból.

10.1. TÉTEL. *A $\sqrt{2}$ irracionális.*

10.1. TÉTEL BIZONYÍTÁSA. A bizonyításhoz nem szükséges használni a SzAT-t. Indirekten bizonyítunk. Tegyük fel, hogy $\sqrt{2}$ racionális. Azaz:

$$\sqrt{2} = \frac{a}{b} \qquad \text{ahol } (a,b) = 1$$
$$\sqrt{2}b = a$$
$$2b^2 = a^2$$

Vagyis a^2 páros. Ekkor a nem lehet páratlan, ugyanis egy a páratlan szám négyzete is páratlan. Tehát a páros.

$$a = 2a_0$$
$$2b^2 = (2a_0)^2 = 4{a_0}^2$$
$$b^2 = 2{a_0}^2$$

Így b is páros, azaz $2 \mid (a,b)$, ami ellentmond $(a,b) = 1$-nek.

Hasonlóan, de a SzAT-nek felhasználásával könnyen igazolhatóak az alábbiak is:

10.2. Tétel. *Ha N nem m-edik hatvány, $\sqrt[m]{N}$ irracionális.*

10.3. Tétel. $\log_{10} 2$ *irracionális.*

A fenti két tétel bizonyítását az olvasóra bízzuk. A következő konstansokról is tudjuk, hogy irracionális:

$$e, \pi, e^{\sqrt{2}}, e^{\sqrt{5}}, e^{\sqrt{7}}, e^{3\sqrt{2}}, \ldots, p(e), p(\pi)$$

ahol $p \not\equiv c$, $p \in \mathbb{Q}[x]$.

Mostanában:

$$e^{\pi},\ 2^{\sqrt{2}},\ e^{\pi\sqrt{2}},\ e^{\pi}+\pi, \ldots$$

Bizonyítatlan:

$$2^{e},\ \pi^{e},\ \pi^{\sqrt{2}},\ e+\pi$$

vagy az Euler-konstans.

Az érdeklődő olvasók a kapcsolódó Wikipédia oldalon [3] olvashatnak további eredményekről.

Elemileg és viszonylag könnyen bizonyítható az e irracionalitása. Az alábbi szép bizonyítás Fouriertől [1] származik.

10.4. Tétel. *Az e irracionális.*

10.4. Tétel bizonyítása.

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

Tegyük fel, e racionális.

$$e = \frac{a}{b}, \quad \text{ahol} \quad (a, b) = 1.$$

Legyen $k \geq b$. Ekkor $k!e$ egész szám. De:

$$k!e = \left(k! + \frac{k!}{1!} + \frac{k!}{2!} + \frac{k!}{3!} + \ldots + \frac{k!}{k!}\right) + \frac{k!}{(k+1)!} + \frac{k!}{(k+2)!} + \cdots$$

$$k!e = A + B,$$

ahol $A = k! + \frac{k!}{1!} + \frac{k!}{2!} + \frac{k!}{3!} + \ldots + \frac{k!}{k!}$ egész szám, B-re pedig

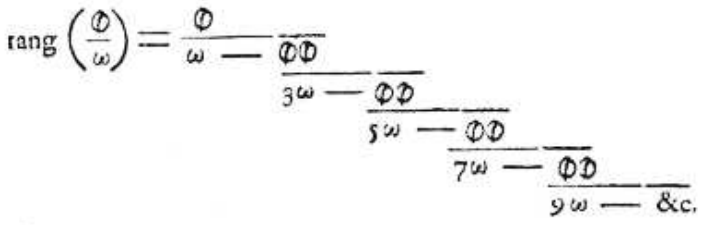
$$\begin{aligned} B &= \frac{k!}{(k+1)!} + \frac{k!}{(k+2)!} + \cdots \\ &= \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \cdots \\ &< \frac{1}{(k+1)} + \frac{1}{(k+1)^2} + \frac{1}{(k+1)^3} + \cdots \\ &= \frac{1}{k}. \end{aligned}$$

Így:

$$\begin{array}{ccc} k!e = A + B & & \\ \nwarrow \quad \nearrow & \wedge & \\ \text{egész} & \frac{1}{k}, & \end{array}$$

ami ellentmondás.

A π irracionalitását az 1760-as években Johann Heinrich Lambert bizonyította, aki korának neves polihisztora volt. Bár 12 évesen otthagyta az iskolát, önerőből tovább tanult, és később a Porosz Akadémia tagja lett. Az alábbiakban egy szkennelt formulát láthatunk Lambert bizonyításából:



A π irracionalitásának egy bizonyítását mi is ismertetjük, sőt, picit többet igazolunk, nevezetesen, hogy π^2 irracionális. Ez a bizonyítás Niventől [2] származik.

10.5. TÉTEL. *π^2 irracionális.*

10.6. KÖVETKEZMÉNY. *π irracionális.*

10.5. TÉTEL BIZONYÍTÁSA.

Előkészületek:

Legyen n pozitív egész.

$$f = f(x) \stackrel{\text{def}}{=} \frac{x^n(1-x)^n}{n!} = \frac{1}{n!}\sum_{m=n}^{2n} c_m x^m,$$

ahol c_m egész szám.

Ekkor $0 < x < 1$ esetén

$$0 < f(x) < \frac{1}{n!}$$

Tudjuk: $f(0) = 0$ és $f^{(m)}(0) = 0$, ha $m < n$ vagy $m > 2n$.

De ha

$$n \leq m \leq 2n,$$

akkor

$$f^{(m)}(0) = \frac{m!}{n!}c_m \in \mathbb{Z},$$

Így f deriváltjai 0-nál egészek. Ugyanez igaz 1-re is, mert

$$f(1-x) = f(x).$$

Tegyük fel, hogy π^2 racionális:

$$\pi^2 = \frac{a}{b} \qquad a, b \in \mathbb{Z}^+ \qquad (a, b) = 1,$$

Legyen:

$$\mathcal{G}(x) \stackrel{\text{def}}{=} b^n \left\{ \pi^{2n} f(x) - \pi^{2n-2} f''(x) + \pi^{2n-4} f^{(4)}(x) - \ldots + (-1)^n f^{(2n)}(x) \right\}.$$

De $\pi^{2j} = \dfrac{a^j}{b^j}$, így $0 \leq j \leq n$ esetén $b^n \pi^{2j}$ egész szám.

Vagyis $\mathcal{G}(0)$ és $\mathcal{G}(1)$ egész szám.

Nézzük a következő deriváltat:

$$\begin{aligned} \frac{d}{dx} \{ \mathcal{G}'(x) \sin \pi x - \pi \mathcal{G}(x) \cos \pi x \} \\ &= \left\{ \mathcal{G}''(x) + \pi^2 \mathcal{G}(x) \right\} \sin \pi x \\ &= \left\{ b^n \pi^{2n+2} f(x) \right\} \sin \pi x \\ &= \pi^2 a^n f(x) \sin \pi x. \end{aligned}$$

Ebből adódóan:

$$\pi \int_0^1 a^n \sin(\pi x) f(x) dx = \left[\frac{\mathcal{G}'(x) \sin \pi x}{\pi} - \mathcal{G}(x) \cos \pi x \right]_0^1$$

$$= \mathcal{G}(0) + \mathcal{G}(1)$$

egész szám.

De $0 < f(x) < \frac{1}{n!}$, ha $0 < x < 1$ miatt

$$0 < \pi \int_0^1 a^n \sin(\pi x) f(x) dx < \frac{\pi a^n}{n!} \underset{\uparrow}{<} 1$$

ha n elegendően nagy.

Ezzel ellentmondásra jutottunk, és beláttuk a tétel állítását.

Hivatkozások

[1] de Stainville, Janot (1815). Mélanges d'Analyse Algébrique et de Géométrie [A mixture of Algebraic Analysis and Geometry]. Veuve Courcier. pp. 340–341.

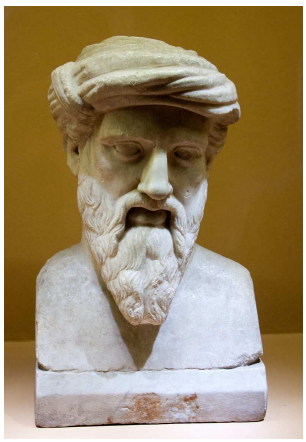
[2] I. Niven, *A simple proof that* π *is irrational*, Bullatin Amer. Math. Soc. 53 (1947), 509.

[3] Wikipedia, Transcendental number, link.

[4] Fotó, Lambert emlékirataiból a lánctörtek szkennelt formája, eredeti mű: "Mémoire sur quelques propriétés remarquables des quantités transcendentes [sic], circulaires et logarithmiques" (1761, nyomtatásban 1768), 288. oldal, link.

11. Pitagoraszi számhármasok

Az ókorban Krotón városában Püthagorasz vezetésével egy híres filozófiai iskola és társaság jött létre. A Pitagoraszi iskola szigorú életelvekhez kötődött, pl. vegetarianizmus, mi több szigorú felvételi rendszerrel is rendelkezett, s amely egyszerre volt matematikai iskola és misztériumvallási iskola is. Férfiakat és nőket egyaránt szívesen láttak.



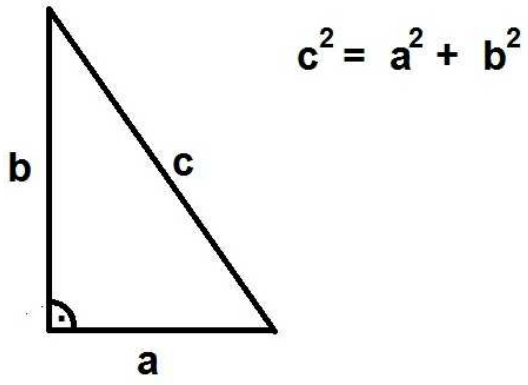
Pitagorasz tétele szerint, ha a és b egy derékszögű háromszög befogói és c az átfogója, akkor

$$a^2 + b^2 = c^2.$$

A tétel neve után kapták elnevezésüket a pitagoraszi számhármasok, amelyek olyan a, b és c pozitív egész számok, amelyre

$$a^2 + b^2 = c^2.$$

Ekkor ugyanis, az a, b, c egész számokhoz tartozik egy egész oldalú derékszögű háromszög.



A legrégebbi emlékünk pitagoraszi számhármasokról a Plimpton 322-es babiloni kőtábla, amely i.e. 1800 körül keletkezett. Erről a kőtábláról a jegyzet elején közöltünk képet. A pitagoraszi számhármasok az első és egyben egyik legrégebbi példa nem lineáris diofantikus egyenletekre.

Minden pitagoraszi számhármas visszavezethető egy olyan esetre, amikor a háromszög oldalait alkotó egész számok páronként relatív prímek. Legyen ugyanis

$$a^2 + b^2 = c^2, \tag{11.1}$$

és jelölje d az a, b és c számok legnagyobb közös osztóját. Ekkor:

$$a = da_0,\ b = db_0,\ c = dc_0,$$

ahol $(a_0, b_0, c_0) = 1$. A (11.1) egyenletet d^2-tel leosztva kapjuk, hogy

$$a_0^2 + b_0^2 = c_0^2.$$

A fentiek alapján egy új elnevezést vezetünk be, az a, b, c pozitív egészekből álló számhármas primitív pitagoraszi számhármas, ha $(a, b, c) = 1$ és $a^2 + b^2 = c^2$.

Ha a, b, c primitív pitagoraszi számhármas, akkor $(a, b) = (a, c) = (b, c) = 1$ is teljesül. Ugyanis, tegyük fel, hogy pl.

$(a, b) > 1$. Ekkor a-nak és b-nek létezik egy közös p prímosztója.

Vagyis $p \mid a$ és $p \mid b$. De $a^2 + b^2 = c^2$ miatt $p \mid c^2$. Ekkor azonban $p \mid c$ is teljesül. Tehát $p \mid (a, b, c)$, viszont $(a, b, c) = 1$, így ellentmondásra jutottunk. Hasonlóan bizonyítható, hogy $(a, c) = (b, c) = 1$.

Tudjuk, hogy 1 és 100 között 16 primitív pitagoraszi számhármas van. Ezek:

(3, 4, 5)	(5, 12, 13)	(8, 15, 17)	(7, 24, 25)
(20, 21, 29)	(12, 35, 37)	(9, 40, 41)	(28, 45, 53)
(11, 60, 61)	(16, 63, 65)	(33, 56, 65)	(48, 55, 73)
(13, 84, 85)	(36, 77, 85)	(39, 80, 89)	(65, 72, 97)

A pitagoraszi számhármasoknak van egy paraméteres alakja. Először lássuk a primitív pitagoraszi számhármasokra vonatkozó tételt:

11.1. TÉTEL. *Legyen a, b, c primitív pitagoraszi számhármas, azaz $a, b, c \in \mathbb{Z}^+$*

$$a^2 + b^2 = c^2$$

és

$$(a, b, c) = 1.$$

Ekkor $\exists\, u, v \in \mathbb{Z}^+$, $u > v$, $(u, v) = 1$, $u \not\equiv v \pmod 2$, hogy

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

vagy fordítva

$$a = 2uv, \quad b = u^2 - v^2, \quad c = u^2 + v^2.$$

11.1. Tétel bizonyítása. Azt már láttuk, hogy $(a,b,c)=1$ és $a^2+b^2=c^2$ esetén

$$(a,b)=(a,c)=(b,c)=1$$

is teljesül.

Vagyis a és b nem lehet egyszerre páros, mert ekkor

$$1=(a,b)=\text{ páros } \geq 2 \text{ teljesülne. } \lightning$$

Ha a és b mindkettő páratlan, akkor

$$a^2\equiv b^2\equiv 1 \pmod 4,$$

mivel

$$(2k+1)^2=4k^2+4k+1\equiv 1 \pmod 4.$$

De ha $a^2\equiv b^2\equiv 1 \pmod 4$, akkor

$$c^2=a^2+b^2\equiv 2 \pmod 4.$$

Vagyis c^2 páros $\Rightarrow$ c páros $\Rightarrow$ c^2 4-gyel osztható $\Rightarrow$ $c^2\equiv 0\ (4)$, ami ellentmond $c^2\equiv 2 \pmod 4$-nek.

Azaz a és b közül az egyik páros, a másik páratlan. Feltehető, hogy b páros és a páratlan. Ekkor c is páratlan ($a^2+b^2=c^2$ miatt), így

$$b^2=c^2-a^2$$
$$\left(\frac{b}{2}\right)^2=\frac{c-a}{2}\cdot\frac{c+a}{2},$$

ahol $\frac{b}{2}\in\mathbb{Z}$, $\frac{c-a}{2}\in\mathbb{Z}$, $\frac{c+a}{2}\in\mathbb{Z}$.

Legyen

$$d=\left(\frac{c-a}{2},\frac{c+a}{2}\right).$$

Itt

$$d \mid \frac{c-a}{2}, \frac{c+a}{2} \quad \Rightarrow d \mid \frac{c-a}{2} + \frac{c+a}{2}, \frac{c+a}{2} - \frac{c-a}{2}$$

$$d \mid (c, a) = 1$$

$$d = 1$$

$$\left(\frac{b}{2}\right)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$$

relatív prímek, ami csak úgy lehet, ha négyzetszámok:

Ha egy p prím $\left(\frac{b}{2}\right)^2$-ben 2α kitevővel szerepel.

$$\left(\frac{b}{2}\right)^2 = \ldots\ p^{2\alpha}\ \ldots$$

$\frac{c-a}{2}$	$\frac{c+a}{2}$
nem osztható p-vel	$p^{2\alpha}$-val osztható

vagy

$p^{2\alpha}$-val osztható	nem osztható p-vel

$\frac{c-a}{2}$-ben és $\frac{c+a}{2}$-ben is minden prím kitevője páros. Így:

$$\frac{c-a}{2} = v^2, \qquad \frac{c+a}{2} = u^2,$$

ahol u és v pozitív egészek és $v < u$. Ekkor $1 = \left(\frac{c-a}{2}, \frac{c+a}{2}\right) = (u^2, v^2) \Rightarrow (u, v) = 1$

$$a = \frac{c+a}{2} - \frac{c-a}{2} = u^2 - v^2$$

$$c = \frac{c+a}{2} + \frac{c-a}{2} = u^2 + v^2$$

$$\left(\frac{b}{2}\right)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2} = u^2 v^2$$

$$\Downarrow$$

$$\frac{b}{2} = uv$$

$$b = 2uv$$

Mivel a páratlan és $a = u^2 - v^2$, u és v paritása nem lehet azonos. Ezzel a tétel állítását beláttuk.

Mivel minden pitagoraszi számhármas egy primitív pitagoraszi számhármas többszöröse, ezért általában az alábbi igaz:

11.2. TÉTEL. *Legyen a, b, c pitagoraszi számhármas. Ekkor $\exists\, t, u, v \in \mathbb{Z}^+$, melyekre $u > v$, $(u, v) = 1$, $u \not\equiv v \ (2)$ és*

$$a = (u^2 - v^2)t, \qquad b = 2uvt, \qquad c = (u^2 + v^2)t,$$

vagy

$$a = 2uvt, \qquad b = (u^2 - v^2)t, \qquad c = (u^2 + v^2)t.$$

Hivatkozások

[1] Pitagorasz, Roman copy of a Greek original from the 2nd-1st century BC, Photo by Szilas, 2013-03-04.

12. Nagy Fermat-tétel

A matematikának minden bizonnyal egyik legrégebbi, ma már megoldott sejtése az ún. Fermat-sejtés (későbbi nevén nagy Fermat tétel). A fejezet alapja a kapcsolódó Wikipedia oldal [2] lerövidített változata.

A sejtés legelső forrásának eredete a homályba vész... Vélhetően a 17. század egy kedvelt problémája volt, a sejtés mai elnevezése Pierre de Fermat nevű fiatal francia matematikus (polgári foglalkozását tekintve jogász) nevéhez fűződik.

Fermat éppen Diophantosz Arithmeticae című művét olvasgatta, amikor is úgy gondolta megtalálta a sejtés bizonyítását, és ennek örömére a következőt írta a könyv margójára:

„Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.”

Azaz:

”Lehetetlen egy köbszámot felírni két köbszám összegeként, vagy egy negyedik hatványt felírni két negyedik hatvány összegeként, általában lehetetlen bármely magasabb hatványt felírni két ugyanolyan hatvány összegeként igazán csodálatos bizonyítást találtam erre a tételre. A margó azonban túlságosan keskeny, semhogy ideírhatnám.”

Fermat bizonyítását a mai napig nem sikerült megtalálni. A kutatók nem találták a jegyzetei között. Számtalan matematikus kísérelte rekonstruálni a bizonyítást, és bár bizonyos speciális esetekben sikerült eredményre jutni, Fermat által említett egyszerű és csoda szép bizonyítást senkinek sem sikerült megtalálnia a mai napig. Talán ez a szép bizonyítás nem is létezik. Fermat tévedett, és talán bizonyításában egy nehéz részt nem számolt elég precízen.

A sejtés formulákkal felírva a következőképpen szól:

12.1. SEJTÉS. *Az $x^n + y^n = z^n$ egyenletnek $n \geq 3$ esetén nincs pozitív egész számokból álló megoldása.*

Egyszerűen látható, hogy a sejtés teljes bizonyításához elég az állítást $n = 4$-re és páratlan prímekre belátni.

12.1. Az $n = 4$ eset

Fermat egyik nagy felfedezése a végtelen leszállás módszere. Ennek segítségével igazolta, hogy az $x^4 + y^4 = z^4$ egyenletnek nincs pozitív egészekből álló megoldása. Sőt, ennél többet igazolt, nevezetesen az $x^4 + y^4 = z^2$ egyenletnek nincs pozitív egészekből álló megoldása.

A módszer lényege, hogy ha létezik egy pozitív egészekből álló

megoldás, amelyre z minimális, akkor találhatunk egy másik megoldást is, amelyre z értéke az előbbinél kisebb és még mindig pozitív. Az eljárást folytatva pozitív egészeknek egy végtelen szigorúan monoton csökkenő sorozatát kapjuk, amely sose éri el a nullát, ami nyilvánvalóan ellentmondás.

Legyen tehát $x^4 + y^4 = z^2$. Belátjuk, hogy van olyan megoldás is, amiben z értéke kisebb. Ha $(x, y) > 1$, akkor x-nek és y-nak létezik közös prímosztója p. Ekkor $p^4 \mid x^4, y^4, z^2 = x^4 + y^4$, amiből $p^2 \mid z$. Így:

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2$$

egyenlettel máris egy kisebb megoldáshoz jutottunk. Hasonlóan kezelhető az $(x, z) > 1$ és $(y, z) > 1$ eset. Így a továbbiakban feltehetjük $(x, y) = (x, z) = (y, z) = 1$.

Először csak annyit látunk be, hogy z páratlan. Ellenkező esetben, ha z páros, akkor x és y páratlan, hiszen $(z, y) = (z, x) = 1$. De ekkor $x^4 + y^4 \equiv 2 \pmod 4$, viszont $z^2 \equiv 0 \pmod 4$, ami ellentmondás.

Tehát z páratlan, és így x és y közül pontosan az egyik, mondjuk x páros. Átrendezve

$$x^4 = (z - y^2)(z + y^2).$$

Itt a jobb oldal két tényezőjének ugyanaz a paritása, tehát mindkettő páros. Ha 2-nél nagyobb közös osztójuk lenne, akkor az osztaná a két tényező összegét ($2z$-t) és különbségét ($2y^2$-et) is, ami lehetetlen, hiszen y és z relatív prímek. Így a két tényező legnagyobb közös osztója 2.

Ez kétféleképpen valósulhat meg.

Első eset. $z-y^2=2a^4$, $z+y^2=8b^4$ alkalmas a, b egész számokkal, ahol a páratlan. Ekkor $y^2=4b^4-a^4$, de ez nem lehet, mert $4b^4-a^4\equiv -1 \pmod 4$, viszont négyzetszám négyes maradéka csak 0 vagy 1 lehet.

Második eset. $z-y^2=8a^4$, $z+y^2=2b^4$ alkalmas a, b pozitív egész számokkal, ahol b páratlan. Ekkor

$$4a^4=b^4-y^2=(b^2-y)(b^2+y).$$

A két tényezőnek 2 nyilván közös osztója. Ha 2-nél nagyobb közös osztójuk lenne, akkor az osztaná $2y$-t és $2b^2$-et is, így teljesülne $(b,y)>1$, tehát $(y,z)>1$ is (hiszen $z=2b^4-y^2$), amit kizártunk.

Így $b^2-y=2c^4$, $b^2+y=2d^4$ alkalmas c, d pozitív egész számokra. Ebből: $c^4+d^4=b^2$. Ezzel az eredeti egyenlethez hasonlót kaptunk, továbbá $y^4<z^2$ miatt $y^2<z$, s mivel $z+y^2=2b^4$ teljesül, $2b^4<2z$, így $b<z$.

12.2. A Fermat-tétel bizonyítása

A Fermat sejtést Andrew Wilesnak sikerült bebizonyítania 1995-ben. A bizonyításon egyedül teljes titokban dolgozott 7 évig.

A bizonyítás első, 1993-as bemutatása után egy elsőre végzetesnek tűnő hibát fedeztek fel, de szerencsére Wilesnak egy tanítványa segítségével 1994 őszére sikerült kijavítania a bizonyítást, amelyet végül 1995-ben fogadtak el.

A teljes bizonyítás 129 oldal hosszú, Galois-elméletet és elliptikus görbéket használ, tehát messze túlmegy az elemi számelmélet területén.

12.3. Érdekességek

Egy legenda szerint Paul Friedrich Wolfskehl német matematikus életét a Fermat-sejtés mentette meg. Lánykérőbe ment, de kikosarazták, ezért – pontban éjfélkor – öngyilkos akart lenni.

Hogy éjfélig gyorsabban teljen az idő, a könyvtárában lévő matematikai könyveket és cikkeket olvasgatta, és kezébe akadt Kummer írása, amely egy hibát mutatott ki Cauchynak Fermat-sejtésre adott bizonyításában.

Wolfskehl hajnalig próbálta kijavítani Cauchy hibás bizonyítását, és reggelre visszanyerte az életkedvét. Sőt, 100 000 márka jutalmat ajánlott fel annak, aki bebizonyítja a tételt (ld. pl. [1]).

1994. április 1-jén a matematikusok között körbejárt egy e-mail, ami bejelentette, hogy Noam Elkies, a Harvard Egyetem professzora igen nagy számokból álló ellenpéldát talált a sejtésre. Sok matematikus nem figyelt a dátumra és összes kollégájának elküldte a jól megfogalmazott szakszövegnek álcázott tréfát.

Hivatkozások

[1] Simon Singh, A nagy Fermat-sejtés (Park Könyvkiadó, Budapest, 1998, ISBN 9635304234; 2004, ISBN 9635306970).

[2] Wikipedia, Nagy-Fermat tétel, link.

[3] Fotó, Pierre de Fermat, Musée d'art et d'histoire de Narbonne, link.

13. Kínai Maradéktétel

Az egyik legrégebbi számelmélet a kínai maradéktétel, amely több mint 2000 éves. A kínai maradéktétel a több kongruenciából álló szimultán kongruencia-rendszerek megoldhatóságára ad választ. Sőt, van olyan változata is, amelyben a bizonyítás meg is konstruálja a megoldást. A jegyzetben egy ilyen bizonyítást fogunk mutatni. A tételt már több mint 2000 éve megfogalmazta egy ókori kínai matematikus, Szun Cu; innen a tétel mai elnevezése.

A tétel a következőképpen szól:

13.1. TÉTEL. (Kínai maradéktétel.) *Legyenek* $m_1, m_2, \ldots, m_k > 0$ *páronként relatív prímek,* $c_1, c_2, \ldots, c_k$ *pedig tetszőleges egészek. Ekkor az*

$$\begin{aligned} x &\equiv c_1 \qquad (m_1) \\ x &\equiv c_2 \qquad (m_2) \\ &\vdots \end{aligned}$$

$$x \equiv c_k \qquad (m_k)$$

kongruencia-rendszer bármilyen $c_1, c_2, \ldots, c_k$ *esetén megoldható, és a megoldás egyetlen maradékosztály* mod M*, ahol* $M = m_1 m_2 \ldots m_k$*.*

13.1. Tétel bizonyítása. A megoldás egyértelműsége mod M:

Tegyük fel, hogy x_1 és x_2 is megoldások. Ekkor

$$\begin{aligned} x_1 \equiv x_2 \equiv c_i \pmod{m_i} \\ 0 \equiv x_1 - x_2 \pmod{m_i} \\ m_i \mid x_1 - x_2. \end{aligned} \tag{13.1}$$

Mivel (13.1) fennáll $i = 1, 2, \ldots, k$ esetén, és $m_1, m_2, \ldots, m_k$ páronként relatív prímek,

$$\begin{aligned} m_1 m_2 \ldots m_k \mid x_1 - x_2 \\ M \mid x_1 - x_2 \\ x_1 \equiv x_2 \pmod{M}, \end{aligned}$$

így mod M csak 1 megoldása van a kongruencia-rendszernek.

A megoldás létezése: Legyen

$$M_i = \frac{M}{m_i}.$$

A megoldást

$$x = a_1 M_1 + a_2 M_2 + \ldots + a_k M_k$$

alakban keressük. Mivel

$$M_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \cdot \ldots \cdot m_k,$$

ezért $j \neq i$-re

$$M_i \equiv 0 \qquad (m_j). \tag{13.2}$$

Amennyiben a fenti módon megkonstruált x-re

$$x \equiv c_j \qquad (m_j)$$

akkor

$$a_1M_1 + a_2M_2 + \ldots + a_kM_k \equiv c_j \qquad (m_j).$$

Azonban ez (13.2) miatt

$$a_jM_j \equiv c_j \qquad (m_j)$$

-vel ekvivalens. Az

$$M_jy \equiv c_j \qquad (m_j)$$

kongruencia akkor oldható meg, ha $(m_j, M_j) \mid c_j$. De

$$(m_j, M_j) = (m_j, m_1m_2 \ldots m_{j-1}m_{j+1} \ldots m_k) = 1,$$

mert $(m_j, m_1) = (m_j, m_2) = \ldots = (m_j, m_k) = 1$. Így a lineáris kongruencia megoldhatóságáról tanultak alapján valóban létezik a_j, amelyre

$$a_jM_j \equiv c_j \qquad (m_j)$$

Ezzel beláttuk, hogy létezik a tétel feltételeinek eleget tevő x, mégpedig

$$x = a_1M_1 + \ldots + a_kM_k.$$

Mivel a bizonyítás előző részében beláttuk, hogy a megoldás egyértelmű mod $m_1m_2 \ldots m_k$, így az összes megoldás

$$x \equiv a_1M_1 + \ldots + a_kM_k \pmod{m_1m_2 \cdots m_k}$$

alakú.

Példa: Oldjuk meg az alábbi szimultán kongruencia-rendszert:

$$\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 2x &\equiv 3 \pmod 5 \\ 5x &\equiv 2 \pmod 7 \end{aligned} \tag{13.3}$$

Megoldás: Fontos megnézni, hogy mindegyik kongruencia külön-külön megoldható-e. Mivel ez így van, alkalmazhatjuk a Kínai maradéktételt, mely szerint létezik közös megoldás is, mivel a modulusok páronként relatív prímek. Sőt, a bizonyítás alapján ez a megoldás az

$$x \equiv 4 \cdot 5 \cdot A + 4 \cdot 7 \cdot B + 5 \cdot 7 \cdot C \pmod{4 \cdot 5 \cdot 7} \tag{13.4}$$

alakban keresendő. Ezt (13.3)-be írva, kapjuk, hogy

$$\begin{aligned} 3\,(4 \cdot 5 \cdot A + 4 \cdot 7 \cdot B + 5 \cdot 7 \cdot C) &\equiv 1 \pmod 4 \\ 2\,(4 \cdot 5 \cdot A + 4 \cdot 7 \cdot B + 5 \cdot 7 \cdot C) &\equiv 3 \pmod 5 \\ 5\,(4 \cdot 5 \cdot A + 4 \cdot 7 \cdot B + 5 \cdot 7 \cdot C) &\equiv 2 \pmod 7. \end{aligned}$$

Azaz:

$$\begin{aligned} 3 \cdot 5 \cdot 7 \cdot C &\equiv 1 \pmod 4 \\ 2 \cdot 4 \cdot 7 \cdot B &\equiv 3 \pmod 5 \\ 5 \cdot 4 \cdot 5 \cdot A &\equiv 2 \pmod 7. \end{aligned}$$

Mivel $3 \cdot 5 \cdot 7 \equiv 1 \pmod 4$, $2 \cdot 4 \cdot 7 \equiv 1 \pmod 5$ és $5 \cdot 4 \cdot 5 \equiv 2 \pmod 7$, így

$$C \equiv 1 \pmod 4$$

$$B \equiv 3 \pmod{5}$$
$$2 \cdot A \equiv 2 \pmod{7}$$

adódik. Az utolsó kongruenciát megoldva (2-vel osztva)

$$A \equiv 1 \pmod{7}$$

az eredmény. Az A, B és C számokra vonatkozó eredményt (13.4)-be írva, kapjuk, hogy

$$\begin{aligned} x &\equiv 4 \cdot 5 \cdot A + 4 \cdot 7 \cdot B + 5 \cdot 7 \cdot C \\ &\equiv 4 \cdot 5 \cdot 1 + 4 \cdot 7 \cdot 3 + 5 \cdot 7 \cdot 1 \\ &\equiv 139 \pmod{140}. \end{aligned}$$

Hivatkozások

[1] Joel Danielson fotója az Unsplash-en, Kínai nagy fal, link.

14. Magasabb fokú kongruenciák

14.1. TÉTEL. *Legyen* $n \in \mathbb{N}$, $n > 1$ *és* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *az* n *prímtényezős felbontása, továbbá*

$$f(x) \in \mathbb{Z}[x].$$

Az

$$f(x) \equiv 0 \qquad (n) \tag{14.1}$$

kongruencia pontosan akkor oldható meg, ha megoldható az

$$\begin{aligned} f(x) &\equiv 0 \qquad \left(p_1^{\alpha_1}\right) \\ f(x) &\equiv 0 \qquad \left(p_2^{\alpha_2}\right) \\ &\vdots \\ f(x) &\equiv 0 \qquad \left(p_k^{\alpha_k}\right) \end{aligned} \tag{14.2}$$

szimultán kongruencia-rendszer. Ha ezek közül valamelyik kongruenciának nincs megoldása, akkor az (14.1) *kongruenciának sincs megoldása. Ha a* (14.2)*-t alkotó kongruenciáknak* $h_1, h_2, \dots, h_k$ *egy-egy megoldása, akkor a* (14.1) *megoldásai*

$$\begin{aligned} x &\equiv h_1 \qquad \left(p_1^{\alpha_1}\right) \\ x &\equiv h_2 \qquad \left(p_2^{\alpha_2}\right) \\ &\vdots \\ x &\equiv h_k \qquad \left(p_k^{\alpha_k}\right) \end{aligned}$$

szimultán kongruencia-rendszer megoldásai között keresendők.

14.1. TÉTEL BIZONYÍTÁSA. A kongruenciát oszthatósággá átírva azonnal látszik.

Azaz a kínai maradéktétel miatt a megoldás megkeresése visszavezethető

$$f(x) \equiv 0 \qquad (p^\alpha)$$

típusú kongruenciák vizsgálatára, ahol p prím $\alpha \geq 1$ egész szám.

14.1. Prímhatvány modulusú kongruenciák

A prímhatvány modulusú kongruencia egyszerűen visszavezethető prímmodulusú kongruenciára. Ezt egy példán keresztül illusztráljuk.

Példa: Oldjuk meg az

$$x^3 + 4x \equiv 21 \qquad (\mathrm{mod}\ 125)$$

kongruenciát. Vagyis $125 \mid x^3 + 4x - 21$. Ebből adódóan:

$$x^3 + 4x \equiv 21 \pmod{125} \tag{14.3}$$

$$x^3 + 4x \equiv 21 \pmod{25} \tag{14.4}$$

$$x^3 + 4x \equiv 1 \pmod{5} \tag{14.5}$$

Megoldási stratégiánk a következő: Először (14.5)-t akarjuk megoldani. Majd a megoldások közül kikeressük azokat, amik (14.4)-nek is eleget tesznek. Végül megoldjuk (14.3)-at.

Először tehát (14.5)-t akarjuk megoldani. Prímmodulusú kongruencia esetén az általános esetben nincs jobb módszer mint végig nézni egy teljes maradékrendszer elemeit. Tehát az $x \in \{0, \pm 1, \pm 2\}$ elemeket végigpróbálva látjuk, hogy egyedül

$$x \equiv 2 \qquad (5)$$

a megoldás. Írjuk x-et $x = 5t + 2$ alakba, ahol $t \in \mathbb{Z}$. Ekkor (14.4):

$$(5t + 2)^3 + 4(5t + 2) \equiv 21 \qquad (25)$$

A 25-tel osztható tagok 0-val kongruensek, így ezekről elfeledkezhetünk:

$$\begin{aligned} 60t + 8 + 20t + 8 &\equiv 21 \qquad (25) \\ 80t + 16 &\equiv 21 \qquad (25) \\ 80t &\equiv 5 \qquad (25) \\ 16t &\equiv 1 \qquad (5) \\ t &\equiv 1 \qquad (5) \end{aligned}$$

Tehát $t = 5\ell + 1$ alakú, ahol ℓ egész szám. Viszont a megoldást x-ben keressük, ezért nézzük meg, mit ad ez x-re:

$$\begin{aligned} x &= 5t + 2 = 5(5\ell + 1) + 2 \\ &= 25\ell + 7 \end{aligned}$$

Végül megoldjuk (14.3)-at:

$$(25\ell + 7)^3 + 4(25\ell + 7) \equiv 21 \qquad (125)$$

A 125-tel osztható tagok 0-val kongruensek, így ezekről elfeledkezhetünk:

$$\begin{aligned} 3 \cdot 7^2 \cdot 25\ell + 7^3 + 4 \cdot 25\ell + 28 &\equiv 21 \qquad (125) \\ (3 \cdot 49 + 4) \cdot 25\ell + 371 &\equiv 21 \qquad (125) \\ 151 \cdot 25\ell &\equiv -350 \qquad (125) \\ 151\ell &\equiv -14 \qquad (5) \\ \ell &\equiv 1 \qquad (5) \end{aligned}$$

Vagyis ℓ egy $\ell = 5k + 1$ alakú szám, ahol k egész szám. Visszahelyettesítve x-be:

$$x = 25(5k + 1) + 7$$
$$= 125k + 32$$

Tehát az eredeti kongruencia megoldásai:

$$x \equiv 32 \pmod{125}.$$

Általában, az eljárás során extrém esetekben több megoldást is kaphatunk, vagy éppen az is lehet, hogy nincs megoldás. Fontos, hogy a diszkusszió során minden esetet alaposan végignézzünk.

14.2. Fokszám redukció

Egy magas fokú kongruencia esetében a fokszám a modulusnál kisebb számmá redukálható, az alábbi tétel alapján:

14.2. TÉTEL. *Ha p prím és $f(x) \in \mathbb{Z}[x]$, akkor létezik (egyetlen) olyan g egész együtthatós polinom, amelynek foka legfeljebb $p-1$ (vagy nem létezik foka – azaz az összes együttható 0), és minden $c \in \mathbb{Z}$-re*

$$f(c) \equiv g(c) \pmod{p}.$$

14.3. MEGJEGYZÉS. *A tételből következik, hogy*

$$f(x) \equiv 0 \ (p) \quad \text{és} \quad g(x) \equiv 0 \ (p)$$

kongruenciának ugyanazok a megoldásai.

14.2. TÉTEL BIZONYÍTÁSA. Az f polinomban x^p helyére mindenhol írjunk x-et, amíg lehetséges. Ezt az eljárást ismételjük, amíg lehetséges. Az így kapott polinom foka $\leq p-1$ (vagy minden együttható

0). Mivel p prím, ezért a kis Fermat-tétel szerint bármely $c \in \mathbb{Z}$-re $c^p \equiv c$, s ezért

$$f(c) \equiv g(c) \pmod{p}.$$

14.3. Fokszám tétel

A fokszám tétel megalkotója Joseph-Louis Lagrange, olasz eredetű francia matematikus. Nem csak matematikával foglalkozott, hanem csillagászattal és fizikával is. Legfontosabb műve a Mécanique analitique (Analitikus mechanika; 1788) című kötet, amely hamar alapművé vált. Apja a szárd király kincstárnoka volt, ám úgy alakult, hogy a bizonytalan, rizikós üzletekbe belemenve elveszítette vagyonát. Lagrange később megemlítette: „Gazdagon alighanem sohasem adtam volna matematikára a fejem."

14.4. TÉTEL. (Fokszám tétel) *Legyen p prímszám. Ha $f(x) \in \mathbb{Z}[x]$ egy n-edfokú polinom és van olyan együtthatója, ami nem osztható p-vel, akkor az*

$$f(x) \equiv 0 \qquad (p)$$

kongruenciának legfeljebb n megoldása van.

14.4. Tétel bizonyítása. A bizonyítás n-re vonatkozó teljes indukcióval történik. Kezdőlépés: $n = 1$-re nyilván igaz az állítás.

Indukciós lépés: Ha $n = k - 1$-re igaz, $n = k$-ra is. Legyen ugyanis $f(x)$ egy k-adfokú polinom. Ha nincs megoldása az

$$f(x) \equiv 0 \qquad (p) \tag{14.6}$$

kongruenciának, akkor a tétel nyilván igaz. Tegyük fel most, hogy (14.6)-nak van egy x_1 megoldása.

$$f(x_1) \equiv 0 \qquad (p). \tag{14.7}$$

Írjuk fel az $f(x)$ polinomot $f(x) = a_k x^k + \ldots + a_0$ alakban, ahol $p \nmid a_k$. Ekkor

$$f(x) - f(x_1) = a_k(x^k - {x_1}^k) + a_{k-1}(x^{k-1} - {x_1}^{k-1}) + \ldots + a_1(x - x_1)$$

Vagyis a jobboldalból $x - x_1$ kiemelhető, így

$$f(x) - f(x_1) = (x - x_1)g(x),$$

ahol $g(x) \in \mathbb{Z}[x]$ egy $k - 1$-edfokú polinom x-ben.

$$p \mid f(x)$$

esetén (14.7) miatt

$$p \mid f(x) - f(x_1)$$
$$p \mid (x - x_1)g(x)$$

$$p \mid x - x_1 \quad \text{vagy} \quad p \mid g(x) \tag{14.8}$$

Ekkor $g(x) \equiv 0 \pmod{p}$-nek az indukciós feltétel miatt legfeljebb $k-1$ gyöke van, így (14.8) miatt $p \mid f(x)$-nek legfeljebb k megoldása van, s ezzel a tételt igazoltuk.

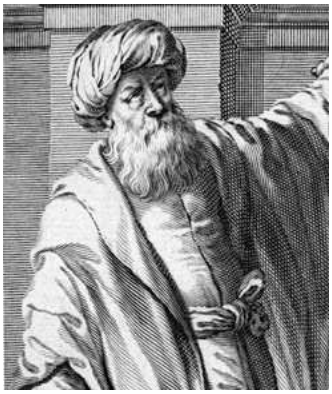
14.5. MEGJEGYZÉS. *A Fokszám tételben nagyon fontos, hogy a modulus prímszám, ellenkező esetben nem igaz a tétel. Tekintsük pl. az* $x^2 - 1 \equiv 0 \pmod{8}$ *kongruenciát. Itt a baloldalon álló polinom foka* 2*, viszont a kongruenciának* 4 *megoldása is van modulo* 8*, ezek:* $x \equiv 1, 3, 5, 7 \pmod{8}$.

Hivatkozások

[1] Fotó, Joseph-Louis Lagrange, 19. század, THE GRANGER COLLECTION, New York, link.

15. Wilson-tétel

A Wilson tétel első írásos formája Abu Ali Muhammad ibn al-Haszan ibn al-Hajszam al-Baszri arab matematikus, fizikus és csillagásztól származik (úgy 1000 körül). Ibn al-Hajszam-t az egyiptomi kalifa megbízta, hogy segítsen abban, hogy a Nílusnak (a terméshez szükséges) évenkénti áradásait folyamszabályozási munkálatokkal garantálják. Amikor a munka nem járt sikerrel, ibn al-Hajszam őrültséget színlelt, hogy a kalifa haragját elkerülje. A kalifa halála után elkobzott vagyonát visszakapta, és haláláig Egyiptomban élt.



Jóval később, a 18. században került újra napfényre a tétel, amikor is Edward Waring [3] bejelentette tanítványa John Wilson tételét. Eredetileg sem ő, sem tanítványa nem tudta bebizonyítani a tételt. Annak igazolását először Lagrange adta meg 1771-ben [2].

Nézzük tehát a tételt:

15.1. TÉTEL. (Wilson) *Ha p prím, akkor $(p-1)! \equiv -1 \pmod{p}$.*

15.1. TÉTEL BIZONYÍTÁSA. Ha $p = 2$ vagy 3, a kongruencia könnyen ellenőrizhető.

Feltehetjük tehát $p \geq 5$. Vesszük az $1, 2, \ldots, p-1$ számokat, és megpróbáljuk úgy párosítani, hogy az egy párban álló számok szorzata kongruens legyen 1-gyel modulo p.

Határozzuk meg j párját, ahol $1 \leq j \leq p-1$. A

$$jx \equiv 1 \qquad (p)$$

kongruencia egyértelműen megoldható, mert $(j,p) = 1 \mid 1$. Nyilván $x \not\equiv 0 \ (p)$ ekkor.

Nézzük meg, hogy j párja mikor különbözik j-től.

$$jx \equiv 1 \qquad (p) \tag{15.1}$$

Ha $x \equiv j \ \ (p)$, akkor (15.1)-ből

$$j^2 \equiv 1 \qquad (p)$$

Oszthatósággá átírva:

$$\begin{aligned} &p \mid j^2 - 1 \\ &p \mid (j-1)(j+1) \\ &p \mid j-1 \ \text{ vagy } \ p \mid j+1 \\ &j \equiv 1 \quad (p) \ \text{ vagy } \ j \equiv p-1 \quad (p) \end{aligned}$$

következik.

Azaz csak az 1 és a $p-1$ számoknak lehet „önmaga” a párja. Vagyis a $2, 3, \ldots, p-2$ számok párosíthatók oly módon, hogy az egy párban lévő számok szorzata 1-gyel kongruens, és a párban álló számok különbözőek.

Összeszorozva ezen párok szorzatát

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p} \qquad / * (p-1)$$
$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

adódik, ami a bizonyítandó állítás volt.

II. bizonyítás. Legyen

$$f(x) = x^{p-1} - 1,$$
$$g(x) = (x-1)(x-2)\ldots(x-(p-1)).$$

Az Euler–Fermat-tétel miatt f-nek gyöke az $1, 2, \ldots, p-1 \mod p$ maradékosztályok, $g(x)$-nek is gyöke ugyanezek a maradékosztályok. Vagyis

$$f(x) - g(x)\text{-nek is gyöke } 1, 2, 3, \ldots, p-1.$$

De $f(x) - g(x)$ foka $\leq p-2$, így a fokszámtétel miatt vagy legfeljebb $p-2$ gyöke van, vagy minden együtthatója osztható p-vel. Most van $p-1$ gyök $(1, 2, 3, \ldots, p-1) \Rightarrow \forall$ együttható osztható p-vel:

$$f(x) - g(x) \equiv 0 \pmod{p},$$

azaz

$$f(x) \equiv g(x) \pmod{p}.$$

A két polinom konstans tagjai kongruensek modulo p, azaz

$$-1 \equiv (-1)(-2)\ldots(-(p-1)) \qquad (p)$$

$$-1 \equiv (-1)^{p-1}(p-1)! \qquad (p)$$
$$-1 \equiv (p-1)! \qquad (p).$$

Ezzel a tételt bebizonyítottuk.

Wilson prímnek nevezünk egy p prímszámot, ha

$$p^2 \mid (p-1)! + 1.$$

A jelenleg ismert Wilson prímek az 5, 13 és 563. Számítógépek segítségével bebizonyították, hogy az $[1, 10^{13}]$ intervallumban nincs is több Wilson prím [1]. Az a sejtés, hogy végtelen sok Wilson prím létezik.

Hivatkozások

[1] E. Costa, R. Gerbicz, D. Harvey, *A search for Wilson primes*, Mathematics of Computation 83 (290) (2014), 3071–3091.

[2] J. L. Lagrange, *Demonstration d'un théorème nouveau concernant les nombres premiers*, Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres (Berlin), vol. 2, pages 125–137 (1771).

[3] E. Waring, *Meditationes Algebraicae* (Cambridge, Anglia: 1770) (latinul). Waring, Meditationes című munkájának harmadik kiadásában Wilson tétele az 5. probléma a 380. oldalon. Waring a következőt írja: "Hanc maxime elegantem primorum numerorum proprietatem invenit vir clarissimus, rerumque mathematicarum peritissimus Joannes Wilson Armiger." (Egy ember, aki a legkiválóbb és legügyesebb a matematikában, John Wilson Squire találta meg a prímszámok legelegánsabb tulajdonságát.)

[4] Cropped version of the frontispiece of Johannes Hevelius, Selenographia, depicting Ibn al-Haytham (Alhazen), artwork drawn by Adolph Boy, engraved by Jeremias Falck - Johannes Hevelius, Selenographia link.

[5] Fotó, John Wilson (1741-1793), angol matematikus és ügyvéd, link.

16. Wolstenholme tétele

Ismert egy jellegében a Wilson tételhez hasonló állítás, amelynek szerzője Wolstenholme.

Ő a következőt bizonyította [3]:

16.1. TÉTEL. (Wolstenholme) *Legyen $p \geq 5$ prím. Az*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

tört számlálója osztható p^2-tel.

16.1. TÉTEL BIZONYÍTÁSA. Legyen $f(x)$ és $g(x)$ polinom definíciója olyan, mint az előbb:

$$f(x) = x^{p-1} - 1,$$
$$g(x) = (x-1)(x-2)\ldots(x-(p-1)).$$

$g(x)$-ben a zárójelek felbontása után

$$g(x) = x^{p-1} + A_1 x^{p-2} + \ldots + A_{p-1}.$$

Nyilván $A_{p-1} = (p-1)!$

x helyébe p-t írva

$$g(p) = (p-1)(p-2)\dots(p-(p-1))$$
$$g(p) = (p-1)!$$

Másrészt

$$g(p) = p^{p-1} + A_1 p^{p-2} + \dots + A_{p-2}p + A_{p-1}.$$

Vagyis

$$(p-1)! = p^{p-1} + A_1 p^{p-2} + \dots + A_{p-2}p + (p-1)!$$
$$0 = p^{p-1} + A_1 p^{p-2} + \dots + A_{p-2}p.$$

Láttuk

$$f(x) \equiv g(x) \qquad (\mathrm{mod}\ p)$$
$$x^{p-1} - 1 \equiv x^{p-1} + A_1 x^{p-2} + \dots + A_{p-2}x + A_{p-1} \quad (\mathrm{mod}\ p)$$

A fokszám tétel miatt a kongruencia két oldalán lévő polinomban az együtthatók kongruensek modulo p. Azaz:

$$p \mid A_1, A_2, \dots, A_{p-2}, \quad -1 \equiv A_{p-1} \quad (p)$$

Visszatérve a

$$0 = p^{p-1} + A_1 p^{p-2} + \dots + A_{p-3}p^2 + A_{p-2}p$$

egyenlethez, itt a baloldalra $p^3 \mid 0$, a jobboldalon pedig az első $p-2$ darab tag osztható p^3-bel, mert $p \mid A_i$. De így $p^3 \mid A_{p-2}p$ is teljesül, vagyis $p^2 \mid A_{p-2}$.

Viszont A_{p-2} az $(x-1)(x-2)\dots(x-(p-1))$ törtben x együtthatója, és ez azonos

$$1 + \frac{1}{2} + \dots + \frac{1}{p-1}$$

számlálójával. Ezzel a tételt beláttuk.

Az alábbi érdekes binomiális együtthatókra vonatkozó tételek szintén Wolstenholme-tól származnak. Ezeket a jegyzetben nem bizonyítjuk:

16.2. TÉTEL. (Wolstenholme) *Ha $p \geq 5$ prímszám, akkor fennáll a következő:*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$$

.

Egy ekvivalens formája a tételnek az alábbi, amely Wilhelm Ljunggren-től [1] származik:

16.3. TÉTEL. *Ha $p \geq 3$ prímszám, akkor fennáll a következő:*

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}$$

Egy p prímszám Wolstenholme prímszám, ha fennáll a

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}.$$

Jelenleg, csak 16843 és 2124679 prímekről tudjuk, hogy Wolstenholme prímek. Számítógépek segítségével megvizsgálták az összes prímet 10^9-ig [2], eddig a határig biztosan nincs több.

Érdekes tulajdonsága a binomiális együtthatóknak még Lucas 1878-ban bizonyított tulajdonsága is. Eszerint, ha $a = n_1 p + n_0$ és $b = m_1 p + m_0$, akkor

$$\binom{a}{b} \equiv \binom{n_1}{m_1}\binom{n_0}{m_0} \pmod{p}.$$

Többszörösen alkalmazva a fenti kongruenciát, az is adódik, ha $a = n_r p^r + n_{r-1} p^{r-1} + \cdots + n_1 p + n_0$ és $b = m_r p^r + m_{r-1} p^{r-1} + \cdots + m_1 p + m_0$, akkor

$$\binom{a}{b} \equiv \binom{n_r}{m_r}\binom{n_{r-1}}{m_{r-1}} \cdots \binom{n_0}{m_0} \pmod{p}.$$

Hivatkozások

[1] A. Granville, *Binomial coefficients modulo prime powers*, Canadian Mathematical Society Conference Proceedings 20 (1997), 253–275, link.

[2] R. J.McIntosh, E.L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Mathematics of Computation, 76 (260) (2007) 2087–2094.

[3] J. Wolstenholme, *On certain properties of prime numbers*, The Quarterly Journal of Pure and Applied Mathematics, 5: 35–39 (1862).

[4] Fotó, Joseph Wolstenholme, link.

17. Számelméleti függvények

Számelméleti függvényekkel már sokszor találkoztunk, csak nem nevesítettük őket. A pontos definíció a következő:

17.1. DEFINÍCIÓ. *Az $f(n)$ függvényt számelméleti függvénynek nevezzük, ha értelmezési tartománya a természetes számok összessége. Értékkészlete lehet komplex vagy valós.*

Számelméleti függvény pl. tetszőleges polinomfüggvény, de a logaritmus függvény is, vagy a már definiált Euler-féle φ függvény. További nevezetes számelméleti függvényeket a fejezet második részében definiálunk.

Számelméleti függvények közül bizonyos speciális típusúakat többször használunk mint másokat. A leggyakrabban multiplikatív és additív számelméleti függvényeket használunk. Ezek definíciója az alábbi:

17.2. DEFINÍCIÓ. *Az $f(n)$ számelméleti függvényt multiplikatívnak nevezzük, ha*

$$f(ab) = f(a)f(b)$$

minden $(a, b) = 1$ számpárra.

Ha az

$$f(ab) = f(a)f(b)$$

összefüggés tetszőleges a, b természetes számok mellett is érvényes, akkor a függvényt teljesen multiplikatív függvénynek nevezzük.

17.3. DEFINÍCIÓ. *Az $f(n)$ számelméleti függvényt additívnak nevezzük, ha*

$$f(ab) = f(a) + f(b)$$

minden $(a, b) = 1$ számpárra. Ha az

$$f(ab) = f(a) + f(b)$$

összefüggés tetszőleges a, b természetes számok mellett is érvényes, akkor a függvényt teljesen additív függvénynek nevezzük.

Multiplikatív függvény pl. az Euler-féle φ függvény, additív a logaritmus függvény.

Az első tételünk a következő:

17.4. TÉTEL. *Legyen $f(n)$ nem azonosan nulla multiplikatív függvény. Ekkor*

$$f(1) = 1.$$

17.4. TÉTEL BIZONYÍTÁSA. Mivel minden a természetes számra

$$(a, 1) = 1,$$

tehát a függvény multiplikativitása miatt

$$f(a) = f(1 \cdot a) = f(1)f(a). \tag{17.1}$$

De mivel $f(n) \not\equiv 0$, $\exists\, a \;\; f(a) \neq 0$. Ekkor (17.1)-et $f(a)$-val osztva azonnal adódik az állítás.

Additív függvényekre a következő igaz:

17.5. TÉTEL. *Legyen $g(n)$ additív függvény. Ekkor*

$$g(1) = 0.$$

17.5. TÉTEL BIZONYÍTÁSA. Mivel minden a természetes számra $(a, 1) = 1$, tehát a függvény additivitása miatt

$$g(a) = g(1 \cdot a) = g(1) + g(a).$$

Mindkét oldalról $g(a)$-t kivonva adódik az állításunk.

A következők alapján multiplikatív illetve additív függvény kiterjeszthető prímhatvány helyekről az összes egész számra:

17.6. TÉTEL. *A multiplikatív $f(n)$, illetve az additív $g(n)$ függvény értékét elegendő prímszámhatvány helyeken meghatározni, ahhoz, hogy az összes értékük adott legyen. Nevezetesen érvényes a következő: Ha $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r}$, akkor*

$$f(n) = f\left({p_1}^{\alpha_1}\right) \cdots f\left({p_r}^{\alpha_r}\right)$$

és

$$g(n) = g\left({p_1}^{\alpha_1}\right) + g\left({p_2}^{\alpha_2}\right) + \ldots + g\left({p_r}^{\alpha_r}\right).$$

17.6. TÉTEL BIZONYÍTÁSA. Mindkét állítás a számelmélet alaptételének és a multiplikatív, ill. additív függvény definíciójának közvetlen következménye.

Teljesen additív és multiplikatív függvényekre az alábbi igaz:

17.7. TÉTEL. *A teljesen multiplikatív $s(n)$ és teljesen additív $t(n)$ függvény értékét elegendő prímszám helyeken meghatározni, ahhoz, hogy az összes értékük adott legyen. Nevezetesen érvényes a következő:*

Ha

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

akkor

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

és

$$t(n) = \alpha_1 t(p_1) + \alpha_2 t(p_2) + \dots + \alpha_r t(p_r).$$

17.7. TÉTEL BIZONYÍTÁSA. A számelmélet alaptételének és a teljesen multiplikatív, ill. teljesen additív függvény definíciójának közvetlen következménye.

17.8. TÉTEL. *Két multiplikatív függvény szorzata és hányadosa is multiplikatív függvény.*

17.8. TÉTEL BIZONYÍTÁSA. HF.

17.9. TÉTEL. *Két additív függvény összege és különbsége is additív függvény.*

17.9. TÉTEL BIZONYÍTÁSA. HF.

17.1. Nevezetes függvények

Az egyik eddig már ismertetésre került nevezetes számelméleti függvény az Euler-féle φ függvény, amelynek definícióját most átismételjük. A legelterjedtebb nevezetes számelméleti függvények a következők:

$$d(n), \sigma(n), \mu(n), \omega(n), \Omega(n), \varphi(n).$$

Lássuk a fenti függvények definícióját:

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

17.11. DEFINÍCIÓ. *Egy $n > 0$ egész pozitív osztóinak összege $\sigma(n)$.*

17.12. DEFINÍCIÓ. *Legyen n prímtényezős felbontása $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\dots{p_r}^{\alpha_r}$, ahol $p_1, p_2, \dots, p_r$ különböző prímek és $\alpha_1 \geq 1, \alpha_2 \geq 1, \dots, \alpha_r \geq 1$. Ekkor $\mu(n)$ Möbius-függvényt a következő módon értelmezzük:*

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1, \\ (-1)^r, & \text{ha } \alpha_1 = \alpha_2 = \dots = \alpha_r = 1, \\ 0, & \text{ha } \exists\, p \text{ prím, hogy } p^2 \mid n \text{ (azaz } \exists\, \alpha_i \geq 2) \end{cases}$$

A fenti definíciót egy új fogalommal a négyzetmentes számokkal is megadhatjuk. Egy n szám négyzetmentes, ha nincs 1-nél nagyobb négyzetszám osztója (azaz $\nexists\, p$ prím, hogy $p^2 \mid n$). Ekkor a $\mu(n)$

Möbius függvény a következő:

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1, \\ (-1)^r, & \text{ha } \alpha_1 = \alpha_2 = \ldots = \alpha_r = 1, \\ 0, & \text{ha } n \text{ nem négyzetmentes.} \end{cases}$$

Példa:

$$\mu(10) = (-1)^2, \qquad \mu(20) = 0, \qquad \mu(30) = (-1)^3.$$

17.13. DEFINÍCIÓ. *Az $\omega(n)$ az n különböző pozitív prímosztóinak száma. Amennyiben n prímtényezős felbontása $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_r}^{\alpha_r}$, akkor $\omega(n) = r$, az $\Omega(n)$ függvény pedig a prímosztók száma multiplicitással számolva, vagyis:*

$$\Omega(n) = \alpha_1 + \alpha_2 + \ldots + \alpha_r.$$

17.14. DEFINÍCIÓ. (Euler-féle φ–függvény) *Tetszőleges n pozitív egész esetén $\varphi(n)$ az $1, 2, \ldots, n$ számok közül az n-hez relatív prímek számát jelenti.*

17.15. TÉTEL. *A*

$$d(n), \sigma(n), \mu(n), \varphi(n)$$

függvények multiplikatív számelméleti függvények.

17.15. TÉTEL BIZONYÍTÁSA. Egyszerre bizonyítjuk, hogy $d(n)$ és $\sigma(n)$ multiplikatív.

Legyen $(a, b) = 1$. Ekkor bizonyítandó

$$d(ab) = d(a)d(b),$$
$$\sigma(ab) = \sigma(a)\sigma(b).$$

A következő lemmát használjuk:

17.16. LEMMA. *Legyen* $(a,b)=1$. *Ekkor* ab *tetszőleges* d *osztója egyértelműen előállítható a következő alakban:*

$$d=a'b', \quad \text{ahol} \quad a' \mid a,\ b' \mid b.$$

17.16. LEMMA BIZONYÍTÁSA. Legyen

$$a=p_1{}^{\alpha_1}\dots p_r{}^{\alpha_r}, \qquad b=q_1{}^{\beta_1}q_2{}^{\beta_2}\dots q_s{}^{\beta_s}. \tag{17.2}$$

Mivel $(a,b)=1$, tehát $p_i\neq q_j$, és így ab prímtényezős felbontása

$$ab=p_1{}^{\alpha_1}\dots p_r{}^{\alpha_r}q_1{}^{\beta_1}\dots q_s{}^{\beta_s}. \tag{17.3}$$

Ha tehát

$$d \mid ab,$$

akkor d prímtényezős felbontása

$$d=p_1{}^{\alpha'_1}\dots p_r{}^{\alpha'_r}q_1{}^{\beta'_1}\dots q_s{}^{\beta'_s},$$

ahol $0\le\alpha'_i\le\alpha_i,\ \ 0\le\beta'_j\le\beta_j$.

Így az egyértelműen meghatározott

$$a'=p_1{}^{\alpha'_1}\dots p_r{}^{\alpha'_r} \quad \text{és} \quad b'=q_1{}^{\beta'_1}\dots q_s{}^{\beta'_s}$$

mellett teljesül állításunk.

Ezután visszatérünk a tétel bizonyításához.

Legyen

$$(a,b)=1 \quad \text{és} \quad d \mid ab.$$

Ekkor a 17.16. Lemma alapján d egyértelműen

$$d=a'b'$$

alakba írható, ahol

$$a' \mid a \quad \text{és} \quad b' \mid b.$$

Így, ha

$$d(a) = k, \qquad d(b) = \ell,$$

akkor a osztóit $a_1, a_2, \ldots, a_k$-val, b osztóit $b_1, b_2, \ldots, b_\ell$-lel jelölve ab összes osztója a következő alakban írhatóak fel:

$$a_1b_1, \ldots, a_1b_\ell, a_2b_1, \ldots, a_2b_\ell, a_kb_1, \ldots, a_kb_\ell. \tag{17.4}$$

Ezek az osztók valóban különbözők, hiszen

$$a_{i_1}b_{j_1} = a_{i_2}b_{j_2}$$

-ből, $(a_{i_1}, b_{j_2}) \leq (a, b) = 1 \Rightarrow (a_{i_1}, b_{j_2}) = 1$ miatt tudjuk, hogy

$$a_{i_1} \mid a_{i_2},$$

s hasonlóan

$$a_{i_2} \mid a_{i_1},$$

azaz $a_{i_1} = a_{i_2}$ adódik. Hasonlóan $b_{j_1} = b_{j_2}$.

Azaz $a_{i_1}b_{j_1} = a_{i_2}b_{j_2}$ akkor és csak akkor, ha $i_1 = i_2$ és $j_1 = j_2$.

Így (17.4) alapján:

$$d(ab) = k\ell = d(a)d(b)$$

és

$$\begin{aligned}\sigma(ab) &= \sum_{i=1}^{k}\sum_{j=1}^{\ell} a_ib_j \\ &= \sum_{i=1}^{k} a_i \sum_{j=1}^{\ell} b_j\end{aligned}$$

$$= \sigma(a)\sigma(b).$$

Ezután bebizonyítjuk, hogy $\mu(n)$ multiplikatív.

1) Legyen $a = b = 1$

$$\mu(1 \cdot 1) = \mu(1) = 1 = \mu(1) \cdot \mu(1).$$

2) $a = 1,\ b \neq 1$.

Ekkor $\mu(1) = 1$ felhasználásával

$$\mu(ab) = \mu(1 \cdot b) = \mu(b) = \mu(1)\mu(b).$$

3) $a \neq 1$, $b \neq 1$.

I. eset: $\exists\, p^2 \mid a$:

$\mu(ab) = 0$, mert $p^2 \mid ab$.

$\mu(a)\mu(b) = 0$, mert $\mu(a) = 0$.

II. eset: $\exists\, p^2 \mid b$:

I. esethez hasonlóan.

III. eset: a és b négyzetmentes:

Mivel $(a, b) = 1$,

$$\begin{aligned} a &= p_1 p_2 \dots p_r, \\ b &= q_1 q_2 \dots q_s, \end{aligned} \qquad p_i \neq q_j$$

alakba írhatók, de ekkor

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

és így felhasználva $\mu(n)$ definícióját:

$$\mu(ab) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(a)\mu(b),$$

amivel állításunkat teljes egészében bebizonyítottuk.

Végül bebizonyítjuk, hogy $\varphi(n)$ multiplikatív.

$\varphi(ab)$ az ab-nél nem nagyobb pozitív egészek között az ab-hez relatív prímek számát jelenti. De ab-hez $(a,b)=1$ miatt azok és csak azok a számok relatív prímek, amelyek külön-külön a-hoz is és b-hez is relatív prímek.

Tehát $\varphi(ab)$ meghatározásához az ab-nél nem nagyobb pozitív egészek közül azoknak a számát kell meghatározni, amelyek relatív prímek a-hoz is és b-hez is.

Először felírjuk az ab-nél nem nagyobb pozitív egészek közül azokat, amelyek a-hoz relatív prímek. Ezek mindannyian egy mod a redukált maradékosztályhoz tartoznak.

Ha tehát $r_1, r_2, \ldots, r_{\varphi(a)}$ jelöli a mod a redukált maradékosztályok legkisebb pozitív elemeit, akkor az ab-nél nem nagyobb a-hoz relatív prím számok a következők lesznek:

$$\begin{array}{rll} r_1, & r_2, \ldots & , r_{\varphi(a)} \\ a+r_1, & a+r_2, \ldots & , a+r_{\varphi(a)} \\ 2a+r_1, & 2a+r_2, \ldots & , 2a+r_{\varphi(a)} \\ \vdots & & \\ (b-1)a+r_1, & (b-1)a+r_2, \ldots & , (b-1)a+r_{\varphi(a)}. \end{array} \tag{17.5}$$

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

Tekintsük evégből az (17.5) táblázatban az egy oszlopban álló számokat. Pl. az i-edik oszlopbeliek a következők:

$$r_i,\ a+r_i,\ 2a+r_i, \ldots, (b-1)a+r_i. \tag{17.6}$$

Látható, hogy ha a mod b teljes maradékrendszert a legkisebb nem negatív maradékokkal, a

$$0, 1, 2, \ldots, b-1 \tag{17.7}$$

számokkal adjuk meg, akkor (17.7)-ből a (17.6) úgy jön létre, hogy (17.7) elemeit a b-hez relatív prím a-val beszorozzuk, majd az így kapott számokhoz hozzáadjuk az r_i számot.

A 6.5. Tétel alapján újra teljes maradékrendszert kapunk mod b. (A tétel, amit itt használunk:

Ha $r_1, r_2, \ldots, r_m$ teljes maradékrendszer és $(a, m) = 1$, b tetszőleges egész, akkor

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

is teljes maradékrendszer mod m.)

Tehát az (17.5) táblázat minden oszlopában mod b egy teljes maradékrendszer áll.

Mivel egy mod b teljes maradékrendszerben $\varphi(b)$ számú b-hez relatív prímszám van, ezért az (17.5) táblázat minden oszlopában $\varphi(b)$ számú b-hez relatív prímszám van.

Mivel pedig az (17.5)-beli oszlopok száma $\varphi(a)$, tehát az (17.5) táblázatban összesen $\varphi(a)\varphi(b)$ számú b-hez relatív prímszám található.

Ezek a számok mindannyian relatív prímek voltak a-hoz is, tehát ezek lesznek azok a számok, amelyek ab-hez relatív prímek. Ezzel a tétel bizonyítását befejeztük.

Nevezetes additív függvények a következők:

17.17. Tétel. *Az $\Omega(n)$ függvény teljesen additív, az $\omega(n)$ függvény pedig additív függvény.*

17.17. Tétel bizonyítása: HF.

17.18. Tétel. *Az Euler-féle $\varphi(n)$ függvény explicit alakja:*

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)\\ &= n\prod_{p|n}\left(1-\frac{1}{p}\right),\end{aligned}$$

ahol az n szám prímtényezős felbontása

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

és

$$\varphi(1) = 1.$$

17.18. Tétel bizonyítása. A $\varphi(n)$ függvény multiplikativitása miatt elegendő $\varphi(p^k)$ meghatározása, ahol p prím, k pedig egész szám. Ugyanis ha n prímtényezős felbontása

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

akkor

$$\varphi(n) = \varphi\left({p_1}^{\alpha_1}\right)\varphi\left({p_2}^{\alpha_2}\right)\dots\varphi\left({p_r}^{\alpha_r}\right). \tag{17.8}$$

Most meghatározzuk $\varphi(p^k)$ értékét!

$$\varphi(p^k) = \left|\left\{x : 1 \le x \le p^k,\ \ (x, p^k) = 1\right\}\right|$$

$$
\begin{aligned}
&= \left|\left\{x : 1 \le x \le p^k,\ \ (x,p) = 1\right\}\right| \\
&= p^k - \left|\left\{x : 1 \le x \le p^k,\ \ (x,p) \neq 1\right\}\right| \\
&= p^k - \left|\left\{x : 1 \le x \le p^k,\ \ p \mid x\right\}\right| \\
&= p^k - p^{k-1} \\
&= p^k \left(1 - \frac{1}{p}\right).
\end{aligned}
$$

Így (17.8)-ból

$$
\begin{aligned}
\varphi(n) &= {p_1}^{\alpha_1} \left(1 - \frac{1}{p_1}\right) {p_2}^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots {p_r}^{\alpha_r} \left(1 - \frac{1}{p_r}\right) \\
&= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).
\end{aligned}
$$

17.19. TÉTEL. *A $d(n)$ függvény explicit alakja*

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1),$$

ahol az n szám prímtényezős felbontása

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

és $d(1) = 1$.

17.19. TÉTEL BIZONYÍTÁSA. $d(n)$ függvény multiplikativitása miatt elegendő $d(p^k)$ meghatározása, ahol p prím, k pedig egész szám.

Ugyanis ha

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

akkor

$$d(n) = d\left({p_1}^{\alpha_1}\right) d\left({p_2}^{\alpha_2}\right) \dots d\left({p_r}^{\alpha_r}\right). \tag{17.9}$$

De $d(p^k)$ értéke $k + 1$, hiszen p^k osztói $1, p, p^2, \dots, p^k$.

Így (17.9) alapján

$$d(n) = (\alpha_1 + 1) \dots \qquad (\alpha_r + 1).$$

17.20. TÉTEL. *$\sigma(n)$ függvény explicit alakja:*

$$\sigma(n) = \frac{{p_1}^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{{p_2}^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{{p_r}^{\alpha_r+1} - 1}{p_r - 1},$$

ahol az n szám prímtényezős felbontása

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

és

$$\sigma(1) = 1.$$

17.20. TÉTEL BIZONYÍTÁSA. A $\sigma(n)$ függvény multiplikativitása miatt elegendő $\sigma(p^k)$ meghatározása, ahol p prím, k pedig egész szám. Ugyanis ha

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

akkor

$$\sigma(n) = \sigma\left({p_1}^{\alpha_1}\right) \sigma\left({p_2}^{\alpha_2}\right) \dots \sigma\left({p_r}^{\alpha_r}\right), \tag{17.10}$$

de

$$\sigma(p^k) = 1 + p + p^2 + \dots + p^k = \frac{p^{k+1} - 1}{p - 1},$$

amit (17.10)-re alkalmazva adódik a tétel.

Példa. Adjuk meg

$$d(2000),\ \sigma(2000),\ \mu(2000),\ \omega(2000),\ \Omega(2000),\ \varphi(2000)$$

értékeit!

$2000 = 2^4 \cdot 5^3$.

Tehát

$$d(2000) = (4+1)(3+1) = 20$$

$$\sigma(2000) = \frac{2^{4+1}-1}{2-1} \cdot \frac{5^{3+1}-1}{5-1} = 4836$$
$$\mu(2000) = 0$$
$$\omega(2000) = 2$$
$$\Omega(2000) = 4+3 = 7$$
$$\varphi(2000) = 2000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 800.$$

17.2. Multiplikatív függvények összegzési függvénye is multiplikatív

A fejezet alapja a következő tétel:

17.21. TÉTEL. *Legyen $f(n)$ multiplikatív függvény. Ekkor*

$$g(n) = \sum_{d|n} f(d)$$

függvény is multiplikatív.

17.21. TÉTEL BIZONYÍTÁSA. Legyen

$$(n_1, n_2) = 1.$$

Ekkor

$$g(n_1 n_2) = \sum_{c|n_1 n_2} f(c).$$

Minden $c \mid n_1 n_2$ pontosan egyféleképpen írható

$$c = d_1 d_2$$

alakban, ahol $d_1 \mid n_1$ és $d_2 \mid n_2$. Azaz

$$g(n_1 n_2) = \sum_{d_1|n_1} \sum_{d_2|n_2} f(d_1 d_2).$$

Mivel $d_1 \mid n_1$, $d_2 \mid n_2$ és $(n_1, n_2) = 1$, így

$$(d_1, d_2) = 1$$

is fennáll. Azaz

$$f(d_1 d_2) = f(d_1) f(d_2),$$

s így

$$\begin{aligned} g(n_1 n_2) &= \sum_{d_1 \mid n_1} \sum_{d_2 \mid n} f(d_1) f(d_2) \\ &= \sum_{d_1 \mid n_1} f(d_1) \sum_{d_2 \mid n} f(d_2) \\ &= g(n_1) g(n_2). \end{aligned}$$

Ezzel a tétel állítását beláttuk.

Az alábbi tétel fontos és hasznos példa arra, hogy hogyan határozható meg explicit képlettel egy összegzési függvény. A tétel később is használjuk, egy a rendre vonatkozó tétel bizonyításánál (ld. 20.4. Tétel).

17.22. TÉTEL.

$$\sum_{d \mid n} \varphi(d) = n.$$

17.22. TÉTEL BIZONYÍTÁSA. Multiplikatív függvény összegzési függvénye is multiplikatív. $\varphi(x)$ multiplikatív függvény, tehát

$$g(n) \stackrel{\text{def}}{=} \sum_{d \mid n} \varphi(d)$$

is multiplikatív. Vagyis ha n prímtényezős felbontása

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

akkor

$$g(n) = g\left({p_1}^{\alpha_1}\right) \cdots g\left({p_r}^{\alpha_r}\right). \tag{17.11}$$

Határozzuk meg $g(p^\alpha)$-t!

$$\begin{aligned} g(p^\alpha) &\overset{\text{def}}{=} \sum_{d|p^\alpha} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \ldots + \varphi(p^\alpha) \\ &= 1 + p\left(1 - \frac{1}{p}\right) + p^2\left(1 - \frac{1}{p}\right) + \ldots + p^\alpha\left(1 - \frac{1}{p}\right) \\ &= 1 + (p-1) + (p^2 - p) + \ldots + (p^\alpha - p^{\alpha-1}) \\ &= p^\alpha. \end{aligned}$$

Ezt (17.11)-be írva

$$g(n) = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r} = n$$

valóban.

Fontos még ismerni a Möbius-féle megfordítási formulát is. Ez a következő:

17.23. Tétel. *Legyen $f(n)$ egy számelméleti függvény. Definiáljuk a $g(n)$ számelméleti függvényt a*

$$g(n) = \sum_{d|n} f(d)$$

Ekkor $g(n)$ függvény értékéből meghatározható $f(n)$, a következő képlettel:

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

17.23. Tétel bizonyítása. Multiplikatív függvény összegzési függvényére vonatkozó tételünk alapján kiszámolható (ld. 17.21.

Tétel), hogy

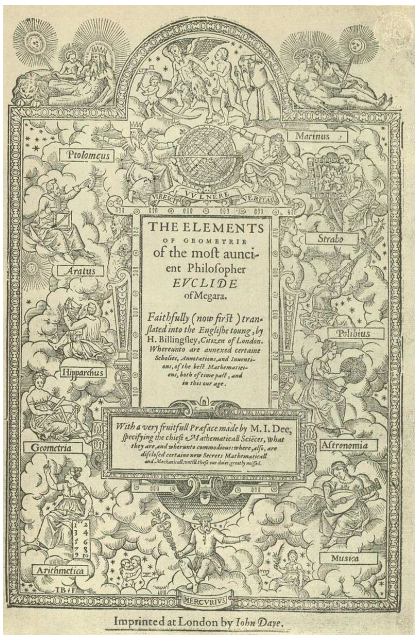
$$\sum_{d|n} \mu(d) = \delta(n) = \begin{cases} 1 & \text{ha } n = 1 \\ 0 & \text{ha } n > 1 \end{cases}$$

Eszerint

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) \\ &= \sum_{d'|n} f(d') \delta\left(\frac{n}{d'}\right) = f(n). \end{aligned}$$

18. Tökéletes számok

A tökéletes számok definíciója már Eukleidész: Elemek [2] című művében is felbukkan. Az alábbiakban az Elemek első, 1570-es, Sir Henry Billingsley-féle angol nyelvű kiadásának címlapja látható:



Eukleidész következőképpen definiálta a tökéletes számokat:

18.1. DEFINÍCIÓ. *Az n szám tökéletes, ha pozitív osztóinak összege egyenlő a szám kétszeresével. Vagyis*

$$\sigma(n) = 2n.$$

Tökéletes szám pl. a $6, 28, 496, 8128$. Az első két számra ellenőrizzük is gyorsan:

$$2 \cdot 6 = 1 + 2 + 3 + 6,$$
$$2 \cdot 28 = 1 + 2 + 4 + 7 + 14 + 28.$$

A sor természetesen tovább folytatható. Az első 48 tökéletes szám a $2^{p-1}(2^p-1)$ alakú számok, pontosan azokra a p prímekre, amelyekre 2^p-1 Mersenne prím. Ezek:

$$\begin{aligned} p = {} & 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, \\ & 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, \\ & 21701, 23209, 44497, 86243, 110503, 132049, 216091, \\ & 756839, 859433, 1257787, 1398269, 2976221, 3021377, \\ & 6972593, 13466917, 20996011, 24036583, 25964951, \\ & 30402457, 32582657, 37156667, 42643801, 43112609, \\ & 57885161. \end{aligned}$$

(Ez a A000043 sorozat az OEIS-ben.)

A következőt már Eukleidész is tudta:

18.2. Tétel. (Eukleidész) *Ha 2^p-1 Mersenne-prím, akkor $2^{p-1}(2^p-1)$ tökéletes szám.*

18.2. Tétel bizonyítása. Legyen $q = 2^p-1$, ekkor $m = 2^{p-1}(2^p-1)$ prímtényezős felbontása

$$m = 2^{p-1} \cdot q.$$

Tehát

$$\begin{aligned} \sigma(m) &= \frac{2^p-1}{2-1} \cdot \frac{q^2-1}{q-1} \\ &= (2^p-1)(q+1) \\ &= (2^p-1)2^p \\ &= 2 \cdot (2^{p-1}(2^p-1)) \\ &= 2m. \end{aligned}$$

Ennél azonban több is mondható. Ibn al-Haytham azt sejtette, hogy minden páros tökéletes szám a fenti alakba írható. Ezt a sejtést csak Euler bizonyította be, a 18. században:

18.3. TÉTEL. (Euler) *Minden páros tökéletes szám felírható* $2^{p-1}(2^p-1)$ *alakban, ahol* 2^p-1 *Mersenne-prím.*

Mielőtt rátérnénk a bizonyításra, megjegyezzük, hogy ha 2^p-1 Mersenne-prím, akkor szükségszerűen p is prím (ld. 2.21. Feladat).

18.3. TÉTEL BIZONYÍTÁSA. Legyen m egy páros tökéletes szám.

Írjuk fel m-et

$$m = 2^\alpha \cdot b$$

alakban, ahol b páratlan és $\alpha \geq 1$. Mivel σ multiplikatív,

$$\sigma(m) = \sigma(2^\alpha b) = \sigma(2^\alpha)\sigma(b),$$
$$\sigma(m) = (2^{\alpha+1}-1)\sigma(b).$$

Másrészt m tökéletes szám, tehát

$$\sigma(m) = 2m = 2^{\alpha+1}b.$$
$$2^{\alpha+1}b = (2^{\alpha+1}-1)\sigma(b)$$
$$\frac{b}{\sigma(b)} = \frac{2^{\alpha+1}-1}{2^{\alpha+1}} \longleftarrow \text{ Ez a tört nem egyszerűsíthető.}$$
$$b = (2^{\alpha+1}-1)c, \qquad \sigma(b) = 2^{\alpha+1}c,$$

ahol $c \in \mathbb{Z}$.

Így b-nek osztói $1, b$ és c. Ha $c \neq 1$:

$$\sigma(b) \geq b + c + 1 = (2^{\alpha+1}-1)c + c + 1$$
$$= 2^{\alpha+1}c + 1.$$

Ez ellentmondás.

Azaz $c = 1$. Ekkor $b = 2^{\alpha+1} - 1$ és $\sigma(b) = 2^{\alpha+1}$. Ekkor:

$$m = 2^{\alpha} b = 2^{\alpha}(2^{\alpha+1} - 1)$$

Ha $2^{\alpha+1} - 1$ nem prím, akkor az alábbi egy határozott egyenlőtlenség:

$$\sigma(2^{\alpha+1} - 1) > 1 + (2^{\alpha+1} - 1) = 2^{\alpha+1}.$$

Vagyis

$$\begin{aligned}
\sigma(m) &= \sigma(2^{\alpha}(2^{\alpha+1} - 1)) \\
&= \sigma(2^{\alpha})\sigma(2^{\alpha+1} - 1) \\
&= (2^{\alpha+1} - 1)\sigma(2^{\alpha+1} - 1) \\
&> 2^{\alpha+1}(2^{\alpha+1} - 1) = 2m.
\end{aligned}$$

Azaz m nem tökéletes. Ezzel ellentmondásra jutottunk.

Vagyis $2^{\alpha+1} - 1$ Mersenne-prím. Ekkor $\alpha + 1$ is prím (ld. 2.21. Feladatot) és $\alpha + 1$ helyébe p-t írva, megkaptuk

$$m = 2^{p-1}(2^p - 1)$$

alakú, ahol $2^p - 1$ Mersenne-prím.

Páratlan tökéletes számot a mai napig nem találtak. Így úgy gondoljuk, hogy a következő sejtés igaz:

18.4. SEJTÉS. *Nem létezik páratlan tökéletes szám.*

A tökéletes számokhoz kapcsolódó fogalom a barátságos számok.

18.5. DEFINÍCIÓ. *Az a és b természetes számok barátságos számok, ha az egyik szám önmagánál kisebb osztóinak összege éppen a másik szám és ez fordítva is igaz. Másképpen megfogalmazva:*

$$\sigma(a) - a = b \quad \text{és} \quad \sigma(b) - b = a.$$

Például a 220 és 284 barátságos számok, hiszen a 220 megfelelő osztói $1, 2, 4, 5, 10, 11, 20, 22, 44, 55$ és 110, ezek összege 284. Fordítva pedig, 284 megfelelő osztói $1, 2, 4, 71$ és 142, ezek összege 220.

Az első 10 barátságos számpár a következő:

$$(220, 284), (1184, 1210), (2620, 2924), (5020, 5564),$$
$$(6232, 6368), (10744, 10856), (12285, 14595), (17296, 18416),$$
$$(63020, 76084), (66928, 66992).$$

(Ez az A259180 sorozat a OEIS-ben.)

Szábit ibn Kurra (9. század) megadott barátságos számpároknak egy paraméteres alakját (ld. pl. [1]). Természetesen ezzel nem sorolta fel az összes barátságos számpárt, de azt könnyű belátni, hogy az ilyen alakú számok valóban barátságosak.

18.6. TÉTEL. (Szábit ibn Kurra) *Legyen n rögzített, $x = 3 \cdot 2^n - 1$, $y = 3 \cdot 2^{n-1} - 1$ és $z = 9 \cdot 2^{2n-1} - 1$. Ha x, y és z prímek, akkor az*

$$a = 2^n \cdot x \cdot y \ \text{ és } \ b = 2^n \cdot z$$

számok barátságos számpárt alkotnak.

A tétel bizonyítását az olvasóra bízzuk.

Érdemes még megemlíteni a hiányos és bővelkedő számok definícióját:

18.7. DEFINÍCIÓ. *Az n természetes szám hiányos, ha $\sigma(n) < 2n$, és bővelkedő, ha $\sigma(n) > 2n$.*

A hiányos és bővelkedő számoknak sok érdekes tulajdonsága van, de ezeknek a vizsgálata túl megy a jelen jegyzet keretein.

Hivatkozások

[1] Dickson, L. E. History of the Theory of Numbers, Vol. 1: Divisibility and Primality. New York: Dover, 2005.

[2] Eukleidész, Elements (Book IX), link vagy link.

[3] Eukleidész, Elemek első, 1570-es, Sir Henry Billingsley-féle angol nyelvű kiadásának címlapja, link.

[4] Fotó, barátságos számok, szerkesztett az alábbiból: link.

19. Rend

Az Euler–Fermat-tételből következik, hogy ha $(a, m) = 1$, akkor van olyan t pozitív egész, amelyre

$$a^t \equiv 1 \qquad (m). \tag{19.1}$$

Például ilyen $t = \varphi(m)$ vagy $t = \varphi(m)k$. De az már egyáltalán nem biztos, hogy a legkisebb pozitív ilyen t az mindig $\varphi(m)$, sőt az esetek többségében van $\varphi(m)$-nél kisebb pozitív t a fenti tulajdonsággal.

A (19.1)-nek eleget tevő pozitív egész t-k közül a legkisebbet rendnek fogjuk nevezni. A precíz definíció az alábbi:

19.1. DEFINÍCIÓ. *Legyen $(a, m) = 1$. A t pozitív egészet az a rendjének nevezzük modulo m, ha*

$$a^t \equiv 1 \qquad (m),$$

de bármely $0 < i < t$ esetén

$$a^i \not\equiv 1 \qquad (m).$$

Jelölés: $o_m(a)$. Szóban: ordo a modulo m.

Példa. $o_{10}(3) = 4$, ugyanis

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 7, \quad \boxed{3^4 \equiv 1} \pmod{10}$$

A következő ábrán egy olyan táblázatot mutatunk, amelyen az $a = 1, 2, 3, \ldots, 16$ esetekre megmutatja az a egész hatványainak a modulo 17 maradékát. A sorokban lévő első egyes adja meg a rend pontos értékét:

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

Euler–Fermat-tétel következménye:

19.2. Állítás. *Ha* $(a,m)=1$, *akkor* $o_m(a) \le \varphi(m)$.

A rend definíciójából világos:

19.3. Állítás. *Ha* $(a,m)=(b,m)=1$, $a \equiv b \pmod m$, *akkor* $o_m(a)=o_m(b)$.

Amennyiben $(a,m)>1$ a rend nem létezik, hiszen ekkor $d=(a,m)>1$ esetén $d \mid a^t$ minden t-re, ezért $d \nmid a^t-1$. Viszont ha $a^t \equiv 1 \pmod m$, akkor $d \mid m \mid a^t-1$, s itt az ellentmondás.

19.1. A rend alaptulajdonságai

19.4. Tétel. *Legyen* $(a,m)=1$ *és* $t \in \mathbb{N}$, *ekkor*

$$a^t \equiv 1 \pmod m \iff o_m(a) \mid t.$$

19.4. Tétel bizonyítása. Először tegyük fel, hogy $o_m(a) \mid t$. Bebizonyítjuk, hogy $a^t \equiv 1 \pmod m$. Legyen

$$t = o_m(a)x.$$

Ekkor:

$$a^t \equiv \left(a^{o_m(a)}\right)^x \equiv 1^x \equiv 1 \qquad (m).$$

Ezután tegyük fel, hogy $a^t \equiv 1 \pmod{m}$. Bebizonyítjuk, hogy $o_m(a) \mid t$. Osszuk el t-t maradékosan $o_m(a)$-val:

$$t = o_m(a)x + y,$$

ahol $0 \leq y < o_m(a)$.

$$a^t \equiv a^{o_m(a)x} \cdot a^y \equiv \left(a^{o_m(a)}\right)^x \cdot a^y \equiv a^y \qquad (m). \qquad (19.2)$$

Feltevésünk szerint

$$a^t \equiv 1 \qquad (m),$$

így (19.2) alapján:

$$a^y \equiv 1 \qquad (m).$$

De $y < o_m(a)$, ezért a rend definíciója miatt (ugyanis a rend a legkisebb pozitív egész t, amelyre $a^t \equiv 1 \pmod{m}$), csak $y = 0$ lehetséges, s ekkor

$$t = o_m(a)x, \quad \text{azaz} \qquad o_m(a) \mid t.$$

19.5. TÉTEL. *Legyen $u, v \in \mathbb{N}$, $(a, m) = 1$. Ekkor*

$$a^u \equiv a^v \qquad (m) \;\Leftrightarrow\; u \equiv v \qquad (o_m(a)).$$

19.5. TÉTEL BIZONYÍTÁSA. Szimmetrikus okokból feltehetjük, hogy $u \geq v$. A kongruenciát a^v-val leosztva (itt használjuk, hogy $(a, m) = 1$). majd az 19.4. Tételt felhasználva, kapjuk, hogy

$$a^u \equiv a^v \qquad (m) \;\Leftrightarrow\; a^{u-v} \equiv 1 \qquad (m)$$

$$\Leftrightarrow o_m(a) \mid u - v \;\Leftrightarrow\; u \equiv v \qquad (o_m(a))$$

Végül bebizonyítjuk, hogy a rend mindig osztója $\varphi(m)$-nek, ahol m a modulus.

19.6. TÉTEL. *Legyen* $(a, m) = 1$, $o_m(a) \mid \varphi(m)$.

19.6. TÉTEL BIZONYÍTÁSA. Az Euler–Fermat-tétel miatt

$$a^{\varphi(m)} \equiv 1 \qquad (m),$$

s így az 19.4. Tétel alapján

$$o_m(a) \mid \varphi(m).$$

Példa: Számítsuk ki a 13 rendjét modulo 59.

$(13, 59) = 1$, ezért $o_{59}(13)$ $\exists$. Tudjuk:

$$o_{59}(13) \mid \varphi(59) = 58$$
$$o_{59}(13) \in \{1, 2, 29, 58\}$$

Végignézve az eseteket:

$$13^1 \not\equiv 1 \qquad (59)$$
$$13^2 \equiv -8 \not\equiv 1 \qquad (59)$$

Végül $13^{29} \pmod{59}$-et ismételt négyzetre-emeléssel számoljuk ki:

$$13^4 \equiv (-8)^2 \equiv 5 \qquad (59)$$
$$13^8 \equiv 5^2 \equiv 25 \qquad (59)$$
$$13^{16} \equiv 25^2 \equiv -24 \qquad (59)$$

$$13^{29} \equiv 13^{16} \cdot 13^{8} \cdot 13^{4} \cdot 13 \equiv (-24) \cdot 25 \cdot 5 \cdot 13 \equiv -1$$
$$\not\equiv 1 \quad (59)$$

Így kizárásos alapon:

$$o_{59}(13) = 58.$$

Hivatkozások

[1] Ábra, Steven Gordon, Cryptography Study Notes, Part II, Number Theory, Discrete Logarithms, link.

20. Primitív gyökök

A primitív gyököket Gauss definiálta a Disquisitiones Arithmeticae (1801)-ben. Gyakorlatilag ez az egyetlen műve Gaussnak, ahol következesen (definíció, tétel, bizonyítás) ismerteti eredményeit. A fogalomnak a mai napig fontos jelentősége van a kriptográfiai alkalmazások miatt. De használható maradékosztályok gyors összeszorzása során is. A fentiekről bővebben a következő fejezetekben lesz szó.

20.1. Definíció. *Egy g számot primitív gyöknek nevezünk modulo m, ha*

$$o_m(g) = \varphi(m).$$

Azt, hogy egy szám primitív gyök-e úgy ellenőrizzük, hogy kiszámoljuk a rendjét.

Az előző fejezetben mutattunk egy ábrát, az $a = 1, 2, 3, \ldots, 16$ hatványaival modulo 17. Ha megint ránézünk erre a táblázatra, látható, hogy a rend a zöld sorokban maximális (azaz $= \varphi(17) = 16$). Így modulo 17 összesen 8 darab primitív gyök van. Ezek: $3, 5, 6, 7, 10, 11, 12$ és 14.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1
3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1
5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1
6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1
7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1
8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1
9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1
10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1
11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1
12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1
13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1
14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1
15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1
16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1

Amikor egy a számról, ahol $(a, m) = 1$ el akarjuk dönteni, hogy primitív gyök-e modulo m, akkor

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

-et fölösleges ellenőrizni, hiszen ennek az állításnak az igazságát tudjuk az Euler–Fermat-tétel miatt. Így az $o_m(a) \mid \varphi(m)$ miatt csak azt kell ellenőrizni, hogy

$$d \mid \varphi(m) \qquad d < \varphi(m)$$

esetén

$$a^d \not\equiv 1 \qquad (m).$$

20.2. TÉTEL. *Egy g szám akkor és csak akkor primitív gyök modulo m, ha $1, g, g^2, \ldots, g^{\varphi(m)-1}$ redukált maradékrendszer modulo m.*

20.2. TÉTEL BIZONYÍTÁSA. Tegyük fel, hogy g primitív gyök.

Ahhoz, hogy belássuk az $1, g, g^2, \ldots, g^{\varphi(m)-1}$ redukált maradékrendszer a 6.11. Tétel miatt három dolgot kell ellenőriznünk:

$1, g, g^2, \ldots, g^{\varphi(m)-1}$ páronként inkongruensek modulo m, számuk $\varphi(m)$ és ($(g, m) = 1$ miatt) valamennyien relatív prímek az m modulushoz. Az, hogy a halmazban a g hatványok páronként inkongruensek onnan látszik, ha $0 \leq i < j \leq \varphi(m) - 1$, akkor

$$g^i \equiv g^j \pmod{m}$$

esetén a 19.5. Tétel miatt

$$i \equiv j \pmod{\varphi(m)},$$

ami $0 \leq i < j \leq \varphi(m) - 1$, csak úgy lehet, ha $i = j$. A másik két tulajdonság triviális. Így a halmaz valóban redukált maradékrendszer.

A megfordításhoz tegyük fel, hogy a fenti g-hatványok redukált maradékrendszert alkotnak mod m. Ekkor $(g, m) = 1$, tehát $o_m(g)$ létezik, $o_m(g) \leq \varphi(m)$. Továbbá $g, g^2, \ldots, g^{\varphi(m)-1}$ egyike sem lehet 1-gyel kongruens, mivel az $1, g, g^2, \ldots, g^{\varphi(m)-1}$ halmazban az elemek páronként inkongruensek. Tehát $o_m(g) = \varphi(m)$.

20.3. TÉTEL. *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 $\alpha > 0$ egész szám.*

20.3. TÉTEL BIZONYÍTÁSA. A tételt teljes általánosságában nem igazoljuk. Először vázlatosan belátjuk, hogy ha m nem írható fel $m = p^\alpha$, $2p^\alpha$, 2 vagy 4 alakban (ahol $p > 2$ prím és $\alpha > 0$ egész szám), akkor nem létezik primitív gyök. Azt viszont, hogy ha m ilyen alakú, akkor létezik primitív gyök csak abban az esetben látjuk be,

ha m prím. Ez utóbbi a következő tételnek a speciális esete, ennek megfelelően a 20.4. Tétel ismertetése után egy mondat erejéig visszatérünk erre az állításra.

Lássuk tehát annak bizonyítását, hogy ha m nem írható fel $m = p^\alpha$, $2p^\alpha$, 2 vagy 4 alakban (ahol $p > 2$ prím és $\alpha > 0$), akkor nem létezik primitív gyök. Tekintsük m prímtényezős felbontását:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Paritás vizsgálattal (és külön választva a kettőhatványokat és azt az esetet, amikor $p_i^{\alpha_i}$ felírásában p_i páratlan prím) belátható, hogy ha $m \neq 2, 4, p^\alpha, 2p^\alpha$, akkor $\frac{\varphi(m)}{\varphi(p_i^{\alpha_i})}$ egész szám, sőt mindig páros is, így

$$\varphi(p_i^{\alpha_i}) \mid \frac{\varphi(m)}{2}$$

teljesül. Tehát $\frac{\varphi(m)}{2} = \varphi(p_i^{\alpha_i}) x_i$ alakú, ahol x_i pozitív egész. Az Euler-Fermat tétel szerint minden $(g, p_i^{\alpha_i}) = 1$ egész számra:

$$g^{\varphi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}.$$

Ezt x_i-edik hatványra emelve:

$$\begin{gathered} g^{\varphi(p_i^{\alpha_i}) x_i} \equiv 1 \pmod{p_i^{\alpha_i}} \\ g^{\varphi(m)/2} \equiv 1 \pmod{p_i^{\alpha_i}} \\ p_i^{\alpha_i} \mid g^{\varphi(m)/2} - 1. \end{gathered}$$

Ez utóbbi m minden $p_i^{\alpha_i}$ prímhatvány osztójára teljesül, így:

$$\begin{gathered} m \mid g^{\varphi(m)/2} - 1 \\ g^{\varphi(m)/2} \equiv 1 \pmod{m}. \end{gathered}$$

Azaz g rendje $\varphi(m)/2$-nél nem nagyobb, így g nem lehet primitív gyök. Mivel ez minden $(g, m) = 1$ maradékosztályra teljesül, ezért nem létezik primitív gyök.

Ezek után rátérünk következő tételünkre, mely adott rendű elemek számát pontosan meghatározza.

20.4. TÉTEL. *Legyen p prímszám. Jelölje $h(d)$ az $1, 2, \dots, p-1$ elemek közül azoknak az x-eknek a számát, amelyekre*

$$o_p(x) = d.$$

Ekkor nyilván $h(d) = 0$, ha $d \nmid p-1$, továbbá

$$h(d) = \varphi(d), \quad \text{ha} \quad d \mid p-1.$$

E tételből következik az előző tétel speciális esete, nevezetesen: ha m prím, akkor $\exists$ primitív gyök. Sőt, az is világos, hogy ebben az esetben a primitív gyökök száma $\varphi(\varphi(m))$.

20.4. TÉTEL BIZONYÍTÁSA. Mivel a rend osztója $\varphi(p) = p-1$-nek, így $h(d) = 0$, ha $d \nmid p-1$.

A bizonyítás során fontos szerepet fog játszani a következő azonosság:

$$\begin{aligned}\sum_{d=1}^{p-1} h(d) &= \sum_{d=1}^{p-1} \big|\{x : o_p(x) = d\}\big| \\ &= \sum_{x=1}^{p-1} \big|\{x : 1 \le o_p(x) \le p-1\}\big| \\ &= p-1.\end{aligned}$$

Mivel $d \nmid p-1$ esetén $h(d)=0$, így egyúttal

$$\sum_{d \mid p-1} h(d) = p-1 \tag{20.1}$$

egyenletet is igazoltuk.

A következő lépésben megmutatjuk, hogy

$$h(d) \leq \varphi(d).$$

Ha nincs d-edrendű elem, akkor

$$0 = h(d) \leq \varphi(d)$$

valóban. Következik az az eset, amikor van egy d-edrendű elem, mondjuk: a. Az

$$x^d \equiv 1 \pmod{m} \tag{20.2}$$

kongruenciának a fokszámtétel (14.4. Tétel) miatt $\leq d$ megoldása van, s a hatványai $a^0, a^1, \ldots, a^{d-1}$ páronként inkongruens számok (lásd 19.5. Tétel) valóban megoldásai (20.2)-nek, hiszen

$$(a^t)^d \equiv (a^d)^t \equiv 1^t \equiv 1 \qquad (p).$$

Így (20.2) megoldásai: $x = a^0, a^1, \ldots, a^{d-1} \ \ (p)$. Ezután belátjuk, hogy $0 \leq t \leq d-1$ esetén a^t rendje pontosan $\dfrac{d}{(t,d)}$. Valóban, ha

$$\begin{gathered}
(a^t)^x \equiv 1 \pmod{p} \\
\Updownarrow \\
a^{tx} \equiv 1 \pmod{p} \\
\Updownarrow \quad \text{(ld. 19.4. Tétel)} \\
o_p(a) \mid tx \\
\Updownarrow
\end{gathered}$$

$$d \mid tx$$
$$\Updownarrow$$
$$\frac{d}{(t,d)} \mid x.$$

A legkisebb pozitív egész x amire a fentiek teljesülnek az a^t rendje modulo p, és ez pedig pont $\frac{d}{(t,d)}$.

Így a^t rendje d, akkor és csak akkor, ha $(t,d) = 1$. Ez alapján $h(d) = \varphi(d)$. Következésképp $h(d) \leq \varphi(d)$.

Így (20.1) alapján tudjuk:

$$p - 1 = \sum_{d|p-1} h(d) \leq \sum_{d|p-1} \varphi(d).$$

Ezután a következőt fogjuk használni.

20.5. Lemma.

$$\sum_{d|n} \varphi(d) = n.$$

20.5. Lemma bizonyítása. A Lemma megegyezik a 17.22. Tétellel, ahol is már ismertettük a bizonyítást.

A lemma alapján:

$$p - 1 = \sum_{d|p-1} h(d) \leq \sum_{d|p-1} \varphi(d) = p - 1.$$

Itt egyenlőség kell, hogy fennálljon, ami csak akkor lehet, ha $\forall d \mid p-1$-re $h(d) = \varphi(d)$, ami éppen a bizonyítandó állítás volt.

20.6. Tétel. *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 $\varphi(p-1)$.*

20.6. TÉTEL BIZONYÍTÁSA. g^x primitív gyök $\Leftrightarrow g^x, g^{2x}, \ldots, g^{(p-1)x}$

RMR mod $p \Leftrightarrow x, 2x, \ldots, (p-1)x$ TMR mod $p-1 \Leftrightarrow (x, p-1) = 1$.

Végezetül egy megjegyzés:

$$g^{(p-1)/2} \equiv -1 \pmod{p},$$

ha p páratlan prím, hiszen $g^{(p-1)/2} \not\equiv 1 \pmod{p}$, mivel g rendje $p-1$, és a kis Fermat tételből adódóan pedig $p \mid g^{p-1} - 1 = (g^{(p-1)/2} - 1)(g^{(p-1)/2} + 1)$.

Vagyis $g^{(p-1)/2+a} \equiv -g^a \pmod{p}$ is teljesül páratlan prímek esetén.

Hivatkozások

[1] Carl Friedrich Gauss, Disquisitiones Arithmeticae (1801),

[2] Ábra, Steven Gordon, Cryptography Study Notes, Part II, Number Theory, Discrete Logarithms, link.

[3] Ábra, g betű, link.

21. Diszkrét logaritmus (index)

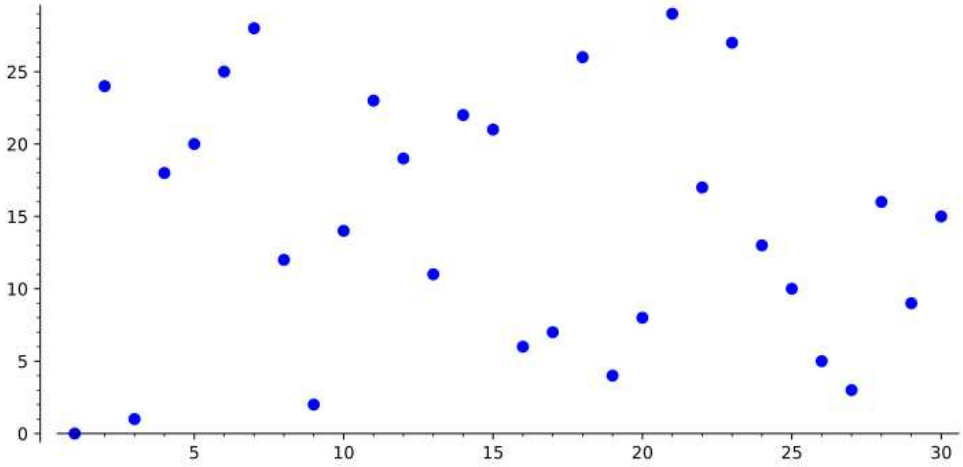
Gauss [1] megfogalmazta a „logaritmus függvény” moduláris analogonját, a következőkkel:

21.1. DEFINÍCIÓ. *Legyen p prím, g primitív gyök modulo p és $(a,p) = 1$. Ekkor a-nak a g alapú diszkrét logaritmusán vagy indexén azt a $0 \leq k \leq p-2$ számot értjük, amelyre*

$$a \equiv g^k \qquad (p).$$

Jelölés: $k = \operatorname{ind}_g a$.

Azonban, ha ábrázoljuk a diszkrét logaritmus függvényt, akkor a logaritmus függvény esetében jól megszokott folytonos ábra helyett egy diszkrét pontokból álló ábrát kapunk, amelyen a pontok eloszlása véletlenszerűnek tűnik. Például, a következő ábrán a $g = 3$ modulo 31 primitív gyökre ábrázoljuk az $x \to \operatorname{ind}_g(x)$ függvényt:



Ha $a \equiv b \ \ (p)$, akkor nyilván

$$\operatorname{ind}_g a = \operatorname{ind}_g b.$$

A 19.5. tétel miatt (hiszen $o_p(g) = \varphi(p) = p - 1$)

$$g^s \equiv g^t \pmod{p} \Leftrightarrow s \equiv t \pmod{p-1}.$$

Illusztrációként mellékelünk egy „hatvány” és egy „indextáblázatot” modulo 13:

Ekkor $g = 2$ primitív gyök. A hatványtáblázat a következő

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

Az indextáblázatot úgy kapjuk, hogy a moduláris hatványozás inverz műveletét végezzük, azaz az ábrán az alsó és felső sor megcserélődik (pl. ha a hatványtáblázatban a 9 alatt az 5 van, akkor az indextáblázatban az 5 alatt van a 9):

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2 a$	0	1	4	2	9	5	11	3	8	10	7	6

21.1. Binom kongruencia megoldása indextáblázattal

Az alfejezetben ismertetésre kerülő módszert egy példával illusztráljuk:

Példa: Oldjuk meg az

$$5x^{22} \equiv 6 \qquad (13)$$

kongruenciát.

Először megnézzük, hogy $x \equiv 0 \pmod{13}$ megoldás-e vajon. Mivel a válasz nem, ezért elég a $(x, 13) = 1$ esetet nézni a továbbiakban. Ekkor ind x létezik, tehát nem kerülünk gondba, ha minden számot egy primitív gyök hatványaként írunk fel.

Ehhez keresünk egy g primitív gyököt mod 13. Ilyen a $g = 2$ például. Elkészítjük a hatvány és indextáblázatot, esetünkben az előzőleg megadott két táblázat. Ekkor:

$$\begin{aligned} 5x^{22} &\equiv 6 && (13) \\ 2^{\operatorname{ind}_2 5} \cdot \left(2^{\operatorname{ind}_2 x}\right)^{22} &\equiv \left(2^{\operatorname{ind}_2 6}\right) && (13) \\ 2^{\operatorname{ind}_2 5 + 22 \operatorname{ind}_2 x} &\equiv 2^{\operatorname{ind}_2 6} && (13) \\ \operatorname{ind}_2 5 + 22 \operatorname{ind}_2 x &\equiv \operatorname{ind}_2 6 && (o_{13}(2)), \end{aligned}$$

ahol $o_{13}(2) = \varphi(13) = 12$. Az indextáblázatot használva:

$$\begin{aligned} 9 + 22 \operatorname{ind}_2 x &\equiv 5 && (12) \\ 22 \operatorname{ind}_2 x &\equiv 8 && (12) \\ 10 \operatorname{ind}_2 x &\equiv 8 && (12) \end{aligned}$$

Itt $(10, 12) \mid 8$ miatt a kongruencia megoldható. A kongruenciát 2-vel osztva:

$$5 \operatorname{ind}_2 x \equiv 4 \qquad (6).$$

A lineáris kongruencia megoldása

$$\begin{aligned} \operatorname{ind}_2 x &\equiv 2 && (6) \\ \operatorname{ind}_2 x &\equiv 2, \ \ 8 && (12) \\ x &\equiv 2^2, \ \ 2^8 && (13). \end{aligned}$$

A hatványtáblázat alapján:

$$x \equiv 4,\ 9 \qquad (13).$$

Régebben előre elkészített indextáblázatokat használtak maradékosztályok szorzásához. Ennek alapja a következő: $(a, m) = (b, m) = 1$ esetén:

$$ab \equiv g^{\text{ind}a} \cdot g^{\text{ind}b} \equiv g^{\text{ind}a+\text{ind}b} \pmod{m}.$$

Így a szorzás egy összeadássá redukálódik.

Az indextáblázatokat adott modulusra elég volt egyszer elkészíteni, és aztán tetszőleges szorzáshoz használhatóak voltak tekintve az adott modulust. Természetesen ez a módszer csak akkor alkalmazható, ha modulo m létezik primitív gyök, azaz $m = p^\alpha$, $2p^\alpha$, 2 vagy 4 alakú, ahol $p > 2$ prím és $\alpha > 0$ egész szám.

A következőkben a binom kongruenciák megoldhatóságára vonatkozó tételt ismertetjük:

21.2. TÉTEL. *Legyen p prím és $(a, p) = 1$. Az*

$$x^k \equiv a \pmod{p} \tag{21.1}$$

kongruencia akkor és csak akkor oldható meg, ha

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}. \tag{21.2}$$

Megoldhatóság esetén a páronként inkongruens megoldások száma $(k, p-1)$.

21.2. TÉTEL BIZONYÍTÁSA. Keressük a megoldást

$$x \equiv g^{\operatorname{ind} x} \qquad (p)$$

alakban, ahol g egy rögzített primitív gyök. Ekkor (21.1) kongruencia

$$g^{k \operatorname{ind} x} \equiv g^{\operatorname{ind} a} \qquad (p)$$

alakba írható, amiből

$$k \operatorname{ind} x \equiv \operatorname{ind} a \qquad (p-1) \tag{21.3}$$

következik. A (21.3) egy lineáris kongruencia, ami akkor oldható meg, ha

$$(k, p-1) \mid \operatorname{ind} a, \tag{21.4}$$

s ebben az esetben a megoldások száma $(k, p-1)$.

Végül megmutatjuk, hogy (21.4) ekvivalens a következővel:

$$a^{\frac{p-1}{(k,p-1)}} \equiv 1 \pmod{p}.$$

Valóban

$$a^{\frac{p-1}{(k,p-1)}} \equiv \left(g^{\operatorname{ind} a}\right)^{\frac{p-1}{(k,p-1)}} \equiv g^{(p-1)\frac{\operatorname{ind} a}{(k,p-1)}} \qquad (p).$$

Ezért a 19.4. Tételt használva látható, hogy $a^{\frac{p-1}{(k,p-1)}} \equiv 1$ ekvivalens azzal, hogy

$$p-1 \mid (p-1)\frac{\operatorname{ind} a}{(k, p-1)} \;\Leftrightarrow\; (k, p-1) \mid \operatorname{ind} a.$$

Hivatkozások

[1] Carl Friedrich Gauss, Disquisitiones Arithmeticae (1801),

[2] Ábra, diszkrét logaritmus mod 31, saját készítésű a Software for Algebra and Geometry Experimentation programmal.

22. Diffie–Hellman kulcscsere

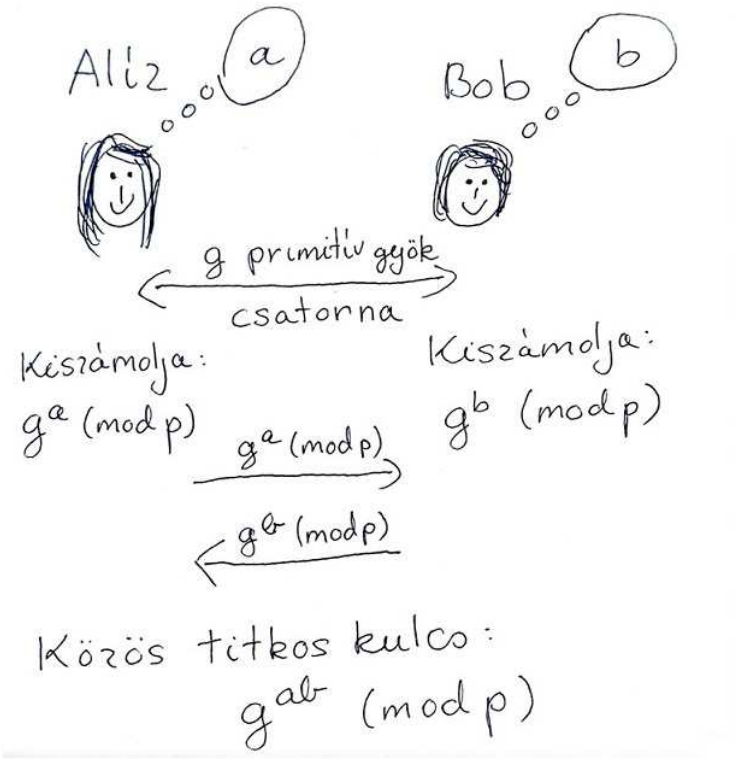
Amennyiben a modulus nagyon nagy, a diszkrét logaritmus, más néven index lassú kiszámíthatóságán múlik az egyik leghíresebb kulcscserélő eljárás a kriptográfiában.

A Diffie-Hellman [1], [2] kulcscsere a nyilvános kulcsú kriptográfia egyik legfontosabb fejezete, melyben a felek úgy szeretnének megállapodni egy közös titkos kulcsban, hogy ha minden kommunikációjuk nyilvános, mások akkor se tudják kitalálni a közös titkos kulcsot. Az eljárás Merkle egy ötletén [2] alapul.

Tegyük fel, hogy Alíz és Bob, akik most egymástól távol vannak (mondjuk más-más országban), félnek attól, hogy a csatornát, amelyen kommunikálnak (telefon vagy email), lehallgatják. Hogyan állapodhatnak meg egy közös titkos kulcsban?

Tekintsük a legegyszerűbb esetet, amikor a közös kulcs $\mathbb{Z}_p^*$-nek egy (véletlen) eleme kell, hogy legyen. Alíz választ egy titkos $1 \leq a \leq p-1$, Bob választ egy titkos $1 \leq b \leq p-1$ egész számot, és ezt soha nem mondják ki, titokban tartják.

Megállapodnak egy közös g primitív gyökben mod p, ezt akár nyilvánosságra is hozhatják. Az se feltétlen szükséges, hogy g primitív gyök legyen (bár ideális esetben az), elég, hogy g rendje nagyon nagy.



Alíz gyorsan ki tudja számolni g^{ab}-t, hiszen Bob elküldte neki $g^b \pmod p$-t, $a \in \mathbb{Z}$-t pedig ő találta ki, így $g^{ab} \pmod p$ gyorsan számolható egy egyszerű moduláris hatványozással:

$$\text{Alíz: } g^{ab} \equiv (g^b)^a \pmod p$$

Bob hasonlóan jár el, tehát mindketten ki tudják számolni $g^{ab} \pmod p$-t.

Tegyük fel, hogy Éva lehallgatja a csatornát. Ekkor a-t és b-t ő nem ismeri, ezeket Alíz és Bob fejben tartotta, viszont esetleg megszerzi

$$g, g^a, g^b \pmod p$$

értékét. Évának ekkor $g^{ab} \pmod p$ kiszámolásához, ekkor az ún. Diffie–Hellman problémát kell megoldania. Ez:

Diffie–Hellman-probléma: A p prím, g primitív gyök, valamint g^a és $g^b \pmod p$ ismeretében számítsuk ki $g^{ab} \pmod p$-t. Rövidítése: DHP.

Sejtés. A Diffie–Hellman-probléma megoldására nincs gyors algoritmus.

A Diffie-Hellman kulcscsere eljárás biztonsága azon múlik, hogy Éva (elegendően nagynak választott p prím esetén) még nagyon gyors számítógépek segítségével sem tudja belátható időn megoldani a DHP-t.

Egy kapcsolódó probléma a diszkrét logaritmus probléma, melyet a következő

Diszkrét logaritmus probléma: Adott $c \in {\mathbb{Z}_p}^*$ és g primitív gyök esetén számítsuk ki azt az x-et, melyre

$$c \equiv g^x \pmod p.$$

Rövidítése: DLP.

Világos, hogy ha a DLP-re ismert gyors megoldás, akkor DHP-re is, hiszen

$$g^a, g^b \rightsquigarrow a, b \text{ adott } \rightsquigarrow (g^a)^b \equiv g^{ab} \text{ (mod } p)$$

DLP-vel Moduláris hatványozás

Nem világos azonban, hogy ha DHP-re ismert gyors megoldás, akkor DLP-re is. Az az általános feltételezés, hogy ez a két probléma ekvivalens. De ez csak sejtés.

Az eljárás könnyen általánosítható $\mathbb{Z}_p^*$-ról, n-ed rendű ciklikus csoportokra, ahol a primitív gyök szerepét a csoport generátoreleme veszi át.

Hivatkozások

[1] W. Diffie, M. E. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory. 22 (6) (1976).

[2] R. C. Merkle, *Secure Communications Over Insecure Channels*, Communications of the ACM. 21 (4) (1978), 294–299.

[3] Ábra, Diffie-Hellman kulcscsere, saját készítésű.

23. Másodfokú kongruenciák

Másodfokú kongruenciákat sokan tanulmányoztak a történelem során: Fermat, Euler, Lagrange, Legendre, de a szisztematikus leírásukat Gauss adta meg először. Mivel pl. Fermat korában nem voltak matematikai újságok, sok akkori eredmény levelezésekből maradt ránk.

Kiindulópontunk a binom kongruenciák megoldhatóságára vonatkozó 21.2. Tétel. Ezt a tételt a $k = 2$ kitevőre alkalmazva a következőt kapjuk:

23.1. Tétel. *Legyen p páratlan prím és $(a, p) = 1$. Ekkor az*

$$x^2 \equiv a \qquad (p) \tag{23.1}$$

kongruencia megoldhatóságának szükséges és elégséges feltétele

$$a^{\frac{p-1}{2}} \equiv 1 \qquad (p) \tag{23.2}$$

teljesüljön. Ha (23.2) fennáll, akkor a megoldások száma 2.

De vajon mely a maradékosztályokra oldható meg az (23.1) kongruencia? A fenti kérdés motiválta a következő definíciót:

23.2. Definíció. *Legyen m tetszőleges természetes szám, a egy modulo m maradékosztály. Amennyiben az*

$$x^2 \equiv a \pmod{m}$$

kongruenciának van megoldása, akkor azt mondjuk, a kvadratikus maradék mod m*. Ha a fenti kongruenciának nincs megoldása, akkor azt mondjuk, a kvadratikus nem-maradék modulo m.*

Példa. Határozzuk meg a kvadratikus maradékokat modulo 7. Ehhez készítünk egy táblázatot:

x	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1

A fenti ábrából leolvasható, hogy a mod 7 kvadratikus maradékok az $0, 1, 2$ és 4 maradékosztályok modulo 7, a kvadratikus nemmaradékok a $3, 5$ és 6 maradékosztályok modulo 7.

Hasonló táblázatot készíthetünk 11 esetén is:

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{11}$	0	1	4	9	5	3	3	5	9	4	1

Most azt látjuk, hogy a mod 11 kvadratikus maradékok az $0, 1, 3, 4, 5$ és 9 maradékosztályok modulo 11, a kvadratikus nemmaradékok a $2, 6, 7, 8$ és 10 maradékosztályok modulo 11.

Ilyen táblázatokat összetett modulus esetén is készíthetünk, de a legérdekesebb és legtöbbet vizsgált esetek azok, amikor a modulus prímszám.

Az alábbi táblázat a Wikipédiából származik [7], és $m \leq 75$ esetén meghatározza a kvadratikus maradékokat. A piros színnel jelölt maradékosztályok olyan kvadratikus maradékokat jelölnek, amelyek nem relatív prímek a modulushoz.

n	quadratic residues mod n	n	quadratic residues mod n	n	quadratic residues mod n
1	0	26	0, 1, 3, 4, 9, 10, 12, 13, 14, 16, 17, 22, 23, 25	51	0, 1, 4, 9, 13, 15, 16, 18, 19, 21, 25, 30, 33, 34, 36, 42, 43, 49
2	0, 1	27	0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25	52	0, 1, 4, 9, 12, 13, 16, 17, 25, 29, 36, 40, 48, 49
3	0, 1	28	0, 1, 4, 8, 9, 16, 21, 25	53	0, 1, 4, 6, 7, 9, 10, 11, 13, 15, 16, 17, 24, 25, 28, 29, 36, 37, 38, 40, 42, 43, 44, 46, 47, 49, 52
4	0, 1	29	0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28	54	0, 1, 4, 7, 9, 10, 13, 16, 19, 22, 25, 27, 28, 31, 34, 36, 37, 40, 43, 46, 49, 52
5	0, 1, 4	30	0, 1, 4, 6, 9, 10, 15, 16, 19, 21, 24, 25	55	0, 1, 4, 5, 9, 11, 14, 15, 16, 20, 25, 26, 31, 34, 36, 44, 45, 49
6	0, 1, 3, 4	31	0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28	56	0, 1, 4, 8, 9, 16, 25, 28, 32, 36, 44, 49
7	0, 1, 2, 4	32	0, 1, 4, 9, 16, 17, 25	57	0, 1, 4, 6, 7, 9, 16, 19, 24, 25, 28, 30, 36, 39, 42, 43, 45, 49, 54, 55
8	0, 1, 4	33	0, 1, 3, 4, 9, 12, 15, 16, 22, 25, 27, 31	58	0, 1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 23, 24, 25, 28, 29, 30, 33, 34, 35, 36, 38, 42, 45, 49, 51, 52, 53, 54, 57
9	0, 1, 4, 7	34	0, 1, 2, 4, 8, 9, 13, 15, 16, 17, 18, 19, 21, 25, 26, 30, 32, 33	59	0, 1, 3, 4, 5, 7, 9, 12, 15, 16, 17, 19, 20, 21, 22, 25, 26, 27, 28, 29, 35, 36, 41, 45, 46, 48, 49, 51, 53, 57
10	0, 1, 4, 5, 6, 9	35	0, 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30	60	0, 1, 4, 9, 16, 21, 24, 25, 36, 40, 45, 49
11	0, 1, 3, 4, 5, 9	36	0, 1, 4, 9, 13, 16, 25, 28	61	0, 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58, 60
12	0, 1, 4, 9	37	0, 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36	62	0, 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28, 31, 32, 33, 35, 36, 38, 39, 40, 41, 45, 47, 49, 50, 51, 56, 59
13	0, 1, 3, 4, 9, 10, 12	38	0, 1, 4, 5, 6, 7, 9, 11, 16, 17, 19, 20, 23, 24, 25, 26, 28, 30, 35, 36	63	0, 1, 4, 7, 9, 16, 18, 22, 25, 28, 36, 37, 43, 46, 49, 58
14	0, 1, 2, 4, 7, 8, 9, 11	39	0, 1, 3, 4, 9, 10, 12, 13, 16, 22, 25, 27, 30, 36	64	0, 1, 4, 9, 16, 17, 25, 33, 36, 41, 49, 57
15	0, 1, 4, 6, 9, 10	40	0, 1, 4, 9, 16, 20, 24, 25, 36	65	0, 1, 4, 9, 10, 14, 16, 25, 26, 29, 30, 35, 36, 39, 40, 49, 51, 55, 56, 61, 64
16	0, 1, 4, 9	41	0, 1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40	66	0, 1, 3, 4, 9, 12, 15, 16, 22, 25, 27, 31, 33, 34, 36, 37, 42, 45, 48, 49, 55, 58, 60, 64
17	0, 1, 2, 4, 8, 9, 13, 15, 16	42	0, 1, 4, 7, 9, 15, 16, 18, 21, 22, 25, 28, 30, 36, 37, 39	67	0, 1, 4, 6, 9, 10, 14, 15, 16, 17, 19, 21, 22, 23, 24, 25, 26, 29, 33, 35, 36, 37, 39, 40, 47, 49, 54, 55, 56, 59, 60, 62, 64, 65
18	0, 1, 4, 7, 9, 10, 13, 16	43	0, 1, 4, 6, 9, 10, 11, 13, 14, 15, 16, 17, 21, 23, 24, 25, 31, 35, 36, 38, 40, 41	68	0, 1, 4, 8, 9, 13, 16, 17, 21, 25, 32, 33, 36, 49, 52, 53, 60, 64
19	0, 1, 4, 5, 6, 7, 9, 11, 16, 17	44	0, 1, 4, 5, 9, 12, 16, 20, 25, 33, 36, 37	69	0, 1, 3, 4, 6, 9, 12, 13, 16, 18, 24, 25, 27, 31, 36, 39, 46, 48, 49, 52, 54, 55, 58, 64
20	0, 1, 4, 5, 9, 16	45	0, 1, 4, 9, 10, 16, 19, 25, 31, 34, 36, 40	70	0, 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30, 35, 36, 39, 44, 46, 49, 50, 51, 56, 60, 64, 65
21	0, 1, 4, 7, 9, 15, 16, 18	46	0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 23, 24, 25, 26, 27, 29, 31, 32, 35, 36, 39, 41	71	0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 19, 20, 24, 25, 27, 29, 30, 32, 36, 37, 38, 40, 43, 45, 48, 49, 50, 54, 57, 58, 60, 64
22	0, 1, 3, 4, 5, 9, 11, 12, 14, 15, 16, 20	47	0, 1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42	72	0, 1, 4, 9, 16, 25, 28, 36, 40, 49, 52, 64
23	0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18	48	0, 1, 4, 9, 16, 25, 33, 36	73	0, 1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 19, 23, 24, 25, 27, 32, 35, 36, 37, 38, 41, 46, 48, 49, 50, 54, 55, 57, 61, 64, 65, 67, 69, 70, 71, 72
24	0, 1, 4, 9, 12, 16	49	0, 1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46	74	0, 1, 3, 4, 7, 9, 10, 11, 12, 16, 21, 25, 26, 27, 28, 30, 33, 34, 36, 37, 38, 40, 41, 44, 46, 47, 48, 49, 53, 58, 62, 63, 64, 65, 67, 70, 71, 73
25	0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24	50	0, 1, 4, 6, 9, 11, 14, 16, 19, 21, 24, 25, 26, 29, 31, 34, 36, 39, 41, 44, 46, 49	75	0, 1, 4, 6, 9, 16, 19, 21, 24, 25, 31, 34, 36, 39, 46, 49, 51, 54, 61, 64, 66, 69

23.3. Definíció. *Legyen p páratlan prím, és $(a, p) = 1$. Ha a kvadratikus maradék modulo p, akkor az $\left(\frac{a}{p}\right)$* Legendre-szimbólum *értéke legyen 1; ha az a kvadratikus nem-maradék modulo p, akkor az $\left(\frac{a}{p}\right)$ Legendre-szimbólum értéke legyen -1.*

Ha $p \mid a$, akkor az $\left(\frac{a}{p}\right) = \left(\frac{0}{p}\right)$ Legendre-szimbólumot vagy nem értelmezik, vagy azt mondják, hogy az értéke legyen 0.

A Legendre-szimbólumnak számos számelméleti bizonyításban fontos szerepe van, de túl az elméleti eredményeken kriptográfiai alkalmazásai is vannak.

Legyen p páratlan prím. Tekintsük a következő számokat $1^2, 2^2, 3^2, \ldots, (p-1)^2$ modulo p. Ebben a sorozatban

$$x^2 \equiv y^2 \pmod{p},$$

akkor és csak akkor áll fenn, ha

$$\begin{aligned} p &\mid x^2 - y^2 \\ p &\mid (x-y)(x+y) \\ p &\mid x-y \text{ vagy } p \mid x+y \\ x &\equiv \pm y \pmod{p} \\ x &= y \text{ vagy } p-y \end{aligned}$$

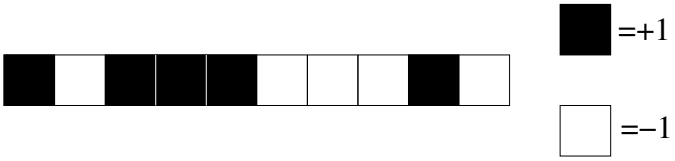
Azaz az $1^2, 2^2, 3^2, \ldots, (p-1)^2$ sorozat $\frac{p-1}{2}$ darab különböző elemet tartalmaz modulo p. Vagyis a nem-nulla kvadratikus maradékok száma: $\frac{p-1}{2}$. Ebből adódóan a kvadratikus nem-maradékok száma $\frac{p-1}{2}$.

Ez az egyszerű tény motiválta, hogy a Legendre szimbólum jól alkalmazható pszeudovéletlen objektumok konstruálása során.

1997-ben Christian Mauduit és Sárközy András [1] a következő konstrukciót adta meg véges bináris pszeudovéletlen sorozatok konstrukciójára:

$$E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right) \right).$$

Például, ha $p = 11$ ez a sorozat a következőképp illusztrálható:



Az eddigiek alapján, annak eldöntésére, hogy egy szám kvadratikus maradék-e vagy sem modulo m, egy x számot végigfuttatunk egy teljes maradékrendszeren modulo m, és megnéztük x^2 lehetséges maradékait.

Ha csak egy darab a számról szeretnénk eldönteni, hogy kvadratikus maradék-e, ez a módszer meglehetősen lassú.

1761-ben Euler talált egy ennél gyorsabb módszert abban az esetben, ha a modulus prím, amelyben a Legendre szimbólum kiszámításának alapja egy moduláris hatványozás (ld. 7. fejezet). A későbbiekben lesz szó egy ennél is gyorsabb módszerről, de előbb lássuk az ún. Euler lemmát:

23.4. LEMMA. (Euler-lemma) *Legyen p páratlan prím, $(a,p)=1$. Ekkor*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

23.4. LEMMA BIZONYÍTÁSA. Amennyiben $\left(\frac{a}{p}\right)=1$, akkor a 23.1. Tétel alapján valóban teljesül

$$\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \quad (p).$$

Nézzük, mi a helyzet, ha $\left(\frac{a}{p}\right)=-1$ esetén. A 23.1. Tételben láttuk:

$$\left(\frac{a}{p}\right) = 1 \;\Leftrightarrow\; a^{\frac{p-1}{2}} \equiv 1 \quad (p).$$

Vagyis ha $\left(\frac{a}{p}\right) = -1$, akkor $a^{\frac{p-1}{2}} \not\equiv 1 \ \ (p)$, azaz

$$p \nmid a^{\frac{p-1}{2}} - 1.$$

A kis Fermat-tétel alapján

$$a^{p-1} \equiv 1 \quad (p).$$

Így:

$$\begin{aligned} p \mid a^{p-1} - 1 \\ p \mid \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right), \end{aligned}$$

de $p \nmid a^{\frac{p-1}{2}} - 1 \ \Rightarrow \ p \mid a^{\frac{p-1}{2}} + 1$. Azaz:

$$a^{\frac{p-1}{2}} \equiv -1 \quad (p).$$

Vagyis valóban ekkor is

$$\left(\frac{a}{p}\right) = -1 \equiv a^{\frac{p-1}{2}} \quad (p).$$

Az Euler-lemma következményei az alábbiak.

23.5. TÉTEL. *Legyen p páratlan prím, $(a,p) = (b,p) = 1$. Ekkor:*

(a) $a \equiv b \quad (p)$ *esetén* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

(c) $\left(\frac{1}{p}\right) = 1$, *általában is* $\left(\frac{a^2}{p}\right) = 1$,

(d) $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p = 4k+1 \text{ alakú,} \\ -1, & \text{ha } p = 4k+3 \text{ alakú.} \end{cases}$$

23.5. TÉTEL BIZONYÍTÁSA A bizonyítás teljes kivitelezését az olvasóra bízzuk, az igazolás során az Euler-lemmát kell használni, a kis Fermat tételt, és azt, hogy a Legendre szimbólum értéke a tételben csak $+1$ vagy -1 lehet.

A fejezetben (kicsit később) a következőket fogjuk igazolni.

23.6. TÉTEL. (Gauss) *Ha p páratlan prím, akkor*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p = 8k \pm 1 \text{ alakú,} \\ -1, & \text{ha } p = 8k \pm 3 \text{ alakú.} \end{cases}$$

23.7. TÉTEL. (Gauss kvadratikus reciprocitási tétele) *Ha p és q egymástól különböző páratlan prímek, akkor*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{ha } p \text{ vagy } q = 4k+1 \text{ alakú,} \\ -\left(\frac{q}{p}\right), & \text{ha } p \text{ és } q \text{ is } = 4k+3 \text{ alakú.} \end{cases}$$

Gauss 8 különböző bizonyítást adott a kvadratikus reciprocitási tételére. Ma már azonban ennél sokkal több létezik. Például a következő weboldalon 334 különböző bizonyítást találhatunk összegyűjtve, sok közülük teljes részletességgel megadva: link.

Mielőtt a tételeket belátnánk, lássunk egy példát:

Példa. Megoldható-e az $x^2 \equiv -42 \ (61)$ kongruencia?

Ehhez meg kell határozni a $\left(\frac{-42}{61}\right)$ Legendre-szimbólum értékét. Ha ez az érték 1, akkor a kongruencia megoldható, ha -1, akkor nem oldható meg. Az első lépés során faktorizálunk:

$$\left(\frac{-42}{61}\right) = \left(\frac{-1}{61}\right) \cdot \left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right) \qquad (23.3)$$

Itt kiszámoljuk a jobboldalon álló Legendre szimbólumokat a 23.5., 23.6. és 23.7. Tételek segítségével:

$$\left(\frac{-1}{61}\right) = (-1)^{\frac{61-1}{2}} = 1$$
$$\left(\frac{2}{61}\right) = (-1)^{\frac{61^2-1}{8}} = -1$$
$$\left(\frac{3}{61}\right) = (-1)^{\frac{61-1}{2}\cdot\frac{3-1}{2}} \cdot \left(\frac{61}{3}\right) = \left(\frac{61}{3}\right) \underset{\text{mivel } 61\equiv 1\ (3)}{=} \left(\frac{1}{3}\right) = 1$$
$$\left(\frac{7}{61}\right) = (-1)^{\frac{61-1}{2}\cdot\frac{7-1}{2}} \cdot \left(\frac{61}{7}\right) = \left(\frac{61}{7}\right) \underset{\text{mivel } 61\equiv 5\ (7)}{=} \left(\frac{5}{7}\right)$$
$$= (-1)^{\frac{5-1}{2}\cdot\frac{7-1}{2}} \left(\frac{7}{5}\right) = \left(\frac{7}{5}\right) \underset{\text{mivel } 7\equiv 2\ (5)}{=} \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

Ezeket az eredményeket (23.3)-ba írva

$$\left(\frac{-42}{61}\right) = 1 \cdot (-1) \cdot 1 \cdot (-1) = 1.$$

Vagyis az $x^2 \equiv -42\ \ (61)$ kongruencia megoldható.

Látható, hogy a fenti algoritmusnak van egy lassú lépése, nevezetesen, amikor faktorizálunk, ugyanis a faktorizációs algoritmusok nagy számok esetében nagyon lassúak. Ezen Jacobi-szimbólumok használatával segíthetünk, ld. a fejezet utolsó részét.

Visszatérve az előző két tételhez, vagyis $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ és Gauss kvadratikus reciprocitási tételéhez, azok bizonyítása Gauss következő lemmáján alapul.

23.8. LEMMA. (Gauss-lemma.) *Legyen p páratlan prím, $(a,p) = 1$. Tekintsük az $a, 2a, 3a, \ldots, \frac{p-1}{2}a$ egészeket és legkisebb nemnegatív maradékaikat modulo p. Ha n jelöli azoknak a maradékoknak a számát, amelyek nagyobbak, mint $\frac{p}{2}$, akkor*

$$\left(\frac{a}{p}\right) = (-1)^n.$$

23.8. LEMMA BIZONYÍTÁSA. Legyenek $r_1, r_2, \ldots, r_n$ azok a maradékok, amelyek nagyobbak, mint $\frac{p}{2}$, a többi pedig $s_1, s_2, \ldots, s_k$.

$$n + k = \frac{p-1}{2}$$

$p - r_1, p - r_2, p - r_3, \ldots, p - r_n$ számok különbözőek és 1 és $\frac{p}{2}$ közé esnek.

$p - r_i \neq s_j$. Mivel ha $p - r_i = s_j$ valamely j-re, akkor $r_i \equiv \varrho a$ (p), $s_j \equiv \sigma a$ (p), ahol $1 \leq \varrho, \sigma \leq \frac{p-1}{2}$.

$$\begin{aligned} p - r_i &\equiv s_j, \\ p - \varrho a &\equiv \sigma a \quad (p), \\ \varrho a + \sigma a &\equiv p \equiv 0 \quad (p), \quad / : a, \text{ ahol } (a,p) = 1, \\ \varrho + \sigma &\equiv 0 \quad (p). \end{aligned}$$

Ez lehetetlen $1 \leq \sigma, \varrho \leq \frac{p-1}{2}$ miatt. Vagyis

$$p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_k$$

páronként különbözők, 1 és $\frac{p}{2}$ közé esnek, azaz $1, 2, \ldots, \frac{p-1}{2}$ számok más sorrendben. Összeszorozva

$$(p - r_1)(p - r_2)\ldots(p - r_n)s_1 s_2 \ldots s_k = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}.$$

Ez utóbbi egyenletet modulo p nézve:

$$\begin{aligned}(-r_1)(-r_2)\dots(-r_n)s_1s_2\dots s_k &\equiv 1\cdot 2\cdot\dots\cdot\frac{p-1}{2} \qquad (p),\\ (-1)^n r_1r_2\dots r_ns_1\dots s_k &\equiv 1\cdot 2\cdot\dots\cdot\frac{p-1}{2} \qquad (p),\\ (-1)^n\cdot a\cdot(2a)\dots\left(\frac{p-1}{2}a\right) &\equiv 1\cdot 2\cdot\dots\cdot\frac{p-1}{2} \qquad (p),\\ (-1)^n a^{\frac{p-1}{2}} &\equiv 1 \qquad (p),\\ a^{\frac{p-1}{2}} &\equiv (-1)^n \qquad (p).\end{aligned}$$

Végül az Euler-lemmát alkalmazva kapjuk:

$$\begin{aligned}\left(\frac{a}{p}\right) &\equiv a^{\frac{p-1}{2}} \equiv (-1)^n \qquad (p),\\ \left(\frac{a}{p}\right) &= (-1)^n,\end{aligned}$$

amivel tételünket bebizonyítottuk.

23.6. Tétel bizonyítása. A tételünk következik az alábbi lemmából, amely később Gauss kvadratikus reciprocitási tételének bizonyítása során is fontos szerepet játszik:

23.9. Lemma. *Ha p páratlan és $(a,2p)=1$, akkor $\left(\frac{a}{p}\right)=(-1)^t$, ahol $t=\sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right]$, továbbá $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$.*

23.9. Lemma bizonyítása. Ugyanazt a jelölést használjuk, mint az előző tételben. Az r_i és s_i egészek a legkisebb pozitív maradékok, amelyeket ja-nak p-vel való osztásánál kapunk. A hányados, mint könnyen látható, $\left[\frac{ja}{p}\right]$. Akkor:

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$$

és

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j,$$

és innen kivonással kapjuk

$$(a-1)\sum_{j=1}^{(p-1)/2} j = p\left(\sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] - n\right) + 2\sum_{j=1}^{n} r_j.$$

De

$$\sum_{j=1}^{(p-1)/2} j = \frac{p^2-1}{8}.$$

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] - n \pmod 2.$$

Ha a páratlan, akkor $n \equiv \sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] \pmod 2$. Ha $a = 2$, akkor $n \equiv \frac{p^2-1}{8} \pmod 2$, mivel $\left[\frac{2j}{p}\right] = 0$, ha $1 \le j \le \frac{p-1}{2}$. Ezek után lemmánk következik az előző lemmából. Ezzel egyúttal a 23.6. Tétel bizonyítását is befejeztük.

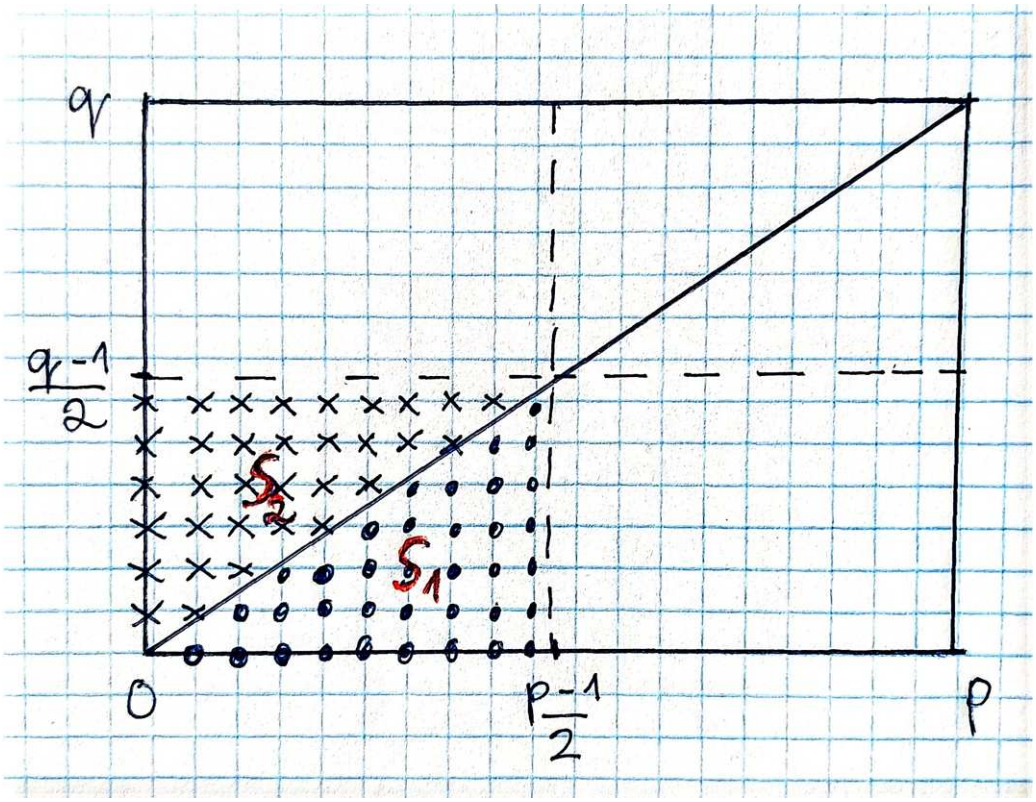
Ezután rátérhetünk Gauss kvadratikus reciprocitási tételének bizonyítására.

23.8. Tétel bizonyítása. Legyen S azon (x, y) párok halmaza, amelyekre $1 \le x \le \frac{p-1}{2}$, $1 \le y \le \frac{q-1}{2}$.

Az S halmazt két diszjunkt részhalmazra bontjuk:

S_1 elemei legyenek azok a párok, amelyekre $qx > py$, S_2 elemei pedig azok a párok, amelyekre $qx < py$.

Mivel $qx = py$ nem lehet, ez valódi felbontása az S halmaznak. Az eddigiek a következő ábrával illusztrálhatóak:



S_1 az olyan (x, y) párok halmaza, amelyekre $1 \leq x \leq \frac{p-1}{2}$, $1 \leq y < \frac{qx}{p}$. Ezért S_1 elemeinek száma $\sum_{x=1}^{(p-1)/2} \left[\frac{qx}{p}\right]$,

S_2 pedig az olyan (x, y) párokból áll, amelyekre $1 \leq y \leq \frac{q-1}{2}$, $1 \leq x < \frac{py}{q}$. Ezért S_2 elemeinek száma $\sum_{y=1}^{(q-1)/2} \left[\frac{py}{q}\right]$.

Ebből adódik, hogy

$$\sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] + \sum_{j=1}^{(p-1)/2} \left[\frac{pj}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Innen az előző tétel szerint $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

23.1. Jacobi-szimbólum

A Legendre-szimbólum kiszámításánál a leglassabb lépés az, amikor a számlálót prímtényezőkre bontjuk. Ez megkerülhető, ha úgynevezett Jacobi-szimbólumot használunk.

23.10. DEFINÍCIÓ. *Ha $P > 2$ páratlan szám, a hozzá relatív prím egész, akkor*

$$\left(\frac{a}{P}\right) \stackrel{\text{def}}{=} \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_k}\right)^{\alpha_k},$$

ahol $P = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$ a P prímtényezős felbontása. Az egyenlet jobb oldalán Legendre-szimbólumokat szorzunk össze.

Ha P prím (a definícióból következőleg), a Jacobi- és Legendre-szimbólum egybeesik.

Összetett P-re, az $X^2 \equiv a \ (P)$ kongruencia megoldhatóság nem kapcsolódik az $\left(\frac{a}{P}\right)$ Jacobi-szimbólum értékéhez.

Például

$$x^2 \equiv 2 \qquad (15)$$

nem oldható meg:

$$\begin{aligned} 15 \mid x^2 - 2 \\ 3 \mid x^2 - 2 \\ x^2 \equiv 2 \quad (3), \end{aligned}$$

ami nem oldható meg. De

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

A Jacobi-szimbólum tulajdonságait a következő tételben foglaljuk össze::

23.11. Tétel. *Legyen P páratlan szám, és $(a,P)=(b,P)=1$. Ekkor:*

(a) $a \equiv b \ (P)$ *esetén* $\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right)$;

(b) $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\cdot\left(\frac{b}{P}\right)$;

(c) $\left(\frac{1}{P}\right)=1, \quad \left(\frac{a^2}{P}\right)=1$;

(d) $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}=\begin{cases}1, & \text{ha } P \ 4k+1 \text{ alakú},\\ -1, & \text{ha } P \ 4k+3 \text{ alakú}\end{cases}$;

(e) $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}=\begin{cases}1, & \text{ha } P \ 8k\pm 1 \text{ alakú},\\ -1, & \text{ha } P \ 8k\pm 3 \text{ alakú}\end{cases}$;

(f) Ha P és Q páratlan számok, akkor

$$\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{Q}{P}\right).$$

Mivel most (f) nemcsak prímekre, de páratlan összetett számokra is fennáll, nem szükséges a számlálót prímtényezőkre bontani, csak a kettőhatványt kell leválasztani.

Példa: Számítsuk ki $\left(\frac{-42}{61}\right)$ Legendre-szimbólum értékét.

Mivel 61 prím: $\left(\frac{-42}{61}\right)_{\text{Jacobi}}=\left(\frac{-42}{61}\right)_{\text{Legendre}}$.

Ezentúl Jacobi-szimbólumokkal számolunk:

$$\begin{aligned}\left(\frac{-42}{61}\right) &= \left(\frac{-1}{61}\right)\cdot\left(\frac{2}{61}\right)\left(\frac{21}{61}\right) = (1)\cdot(-1)\left(\frac{21}{61}\right)\\ &= -\left(\frac{21}{61}\right) = -\left(\frac{61}{21}\right) = -\left(\frac{19}{21}\right) = -\left(\frac{21}{19}\right)\\ &= -\left(\frac{2}{19}\right) = +1.\end{aligned}$$

23.11. Tétel bizonyítása. A Tétel a), b) és c) része egyszerű következménye a Jacobi-szimbólum multiplikativitásának, ezeket itt nem részletezzük.

A d) rész igazolásához lássuk a következőt: Legyen $P = {p_1}^{\alpha_1}\dots{p_r}^{\alpha_r}$. Ekkor:

$$\begin{aligned}\left(\frac{-1}{P}\right) &= \left(\frac{-1}{p_1}\right)^{\alpha_1}\dots\left(\frac{-1}{p_r}\right)^{\alpha_r}\\ &= \left((-1)^{\frac{p_1-1}{2}}\right)^{\alpha_1}\dots\left((-1)^{\frac{p_r-1}{2}}\right)^{\alpha_r}\\ &= (-1)^{\alpha_1\cdot\frac{p_1-1}{2}+\dots+\alpha_r\frac{p_r-1}{2}}.\end{aligned}$$

Ez pontosan akkor $+1$, ha a $\sum_{p_i\equiv 3 \pmod 4}\alpha_i$ páros, ami viszont ekvivalens azzal, hogy P egy $4k+1$ alakú természetes szám.

Következőleg rátérünk az e) rész bizonyítására:

$$\begin{aligned}\left(\frac{2}{P}\right) &= \left(\frac{2}{p_1}\right)^{\alpha_1}\dots\left(\frac{2}{p_r}\right)^{\alpha_r}\\ &= \left((-1)^{\frac{{p_1}^2-1}{8}}\right)^{\alpha_1}\dots\left((-1)^{\frac{{p_r}^2-1}{8}}\right)^{\alpha_r}\end{aligned}$$

$$= (-1)^{\alpha_1 \cdot \frac{{p_1}^2-1}{8} + \ldots + \alpha_r \frac{{p_r}^2-1}{8}}.$$

Az, hogy ez a kifejezés -1 vagy $+1$, attól függ, hogy $\sum \alpha_i \frac{{p_i}^2-1}{8}$ páros-e vagy páratlan. Ha bebizonyítjuk, hogy

$$\sum \alpha_i \frac{{p_i}^2-1}{8} \equiv \frac{P^2-1}{8} \pmod 2,$$

készen vagyunk.

Ehhez

$$\frac{p^2-1}{8} = \begin{cases} 1 \pmod 2, & \text{ha } p \equiv \pm 3 \ (8), \\ 0 \pmod 2, & \text{ha } p \equiv \pm 1 \ (8). \end{cases}$$

Ez alapján

$$\sum \alpha_i \frac{{p_i}^2-1}{8} \equiv \sum_{\alpha_i \text{ páratlan}} \frac{{p_i}^2-1}{8} \pmod 2,$$
$$\equiv \sum_{p_i \equiv \pm 3 \ (8),\ \alpha_i \text{ páratlan}} 1 \pmod 2.$$

Másrészt

$$\frac{P^2-1}{8} = \frac{{p_1}^{2\alpha_i} \ldots {p_r}^{2\alpha_r} - 1}{8},$$

$$p^2 \equiv \begin{cases} 1 \pmod{16}, & \text{ha } p \equiv \pm 1 \ (8), \\ 9 \pmod{16}, & \text{ha } p \equiv \pm 3 \ (8), \end{cases}$$

$${p_i}^{2\alpha_i} \equiv \begin{cases} 1 \pmod{16}, & \text{ha } \alpha_i \text{ páros} \\ & \text{vagy } p \equiv \pm 1 \ (8), \\ 9 \text{ különben.} & \end{cases}$$

$${p_1}^{2\alpha_i} \ldots {p_r}^{2\alpha_r} \equiv 9^{\sum_{p_i \equiv \pm 3 \ (8),\ \alpha_i \text{ páratlan}} 1} \pmod{16}$$

$$\equiv \begin{cases} 1, & \text{ha } \sum_{p_i \equiv \pm 3 \ (8),\ \alpha_i \text{ páratlan}} 1 \text{ páros}, \\ 9, & \text{ha } \sum_{p_i \equiv \pm 3 \ (8),\ \alpha_i \text{ páratlan}} 1 \text{ páratlan } (\bmod 16). \end{cases}$$

$$\frac{{p_1}^{2\alpha_1} \ldots {p_r}^{2\alpha_r} - 1}{8} \equiv \begin{cases} \text{páros}, & \text{ha } \sum_{p_i \equiv \pm 3 \ (8),\ \alpha_i \text{ páratlan}} 1 \text{ páros}, \\ \text{páratlan}, & \text{ha } \sum_{p_i \equiv \pm 3 \ (8),\ \alpha_i \text{ páratlan}} 1 \text{ páratlan}. \end{cases}$$

Ebből pedig következik az állítás.

Végül rátérünk az f) rész bizonyítására: Legyen $P = p_1 p_2 \ldots p_r$, ahol most a p_i prímek között azonosak is lehetnek. Továbbá, legyen $Q = q_1 q_2 \ldots q_s$, ahol most a q_i prímek között azonosak is lehetnek, fontos, hogy $p_i \neq q_j$. A Jacobi-szimbólum multiplikativitása miatt:

$$\left(\frac{P}{Q}\right) = \prod_{1 \leq i \leq r,\ 1 \leq j \leq s} \left(\frac{p_i}{q_j}\right), \quad \left(\frac{Q}{P}\right) = \prod_{1 \leq i \leq r,\ 1 \leq j \leq s} \left(\frac{q_j}{p_i}\right).$$

Legyen a p_i prímek között u darab, a q_j prímek között v darab $4k+3$ alakú egész szám. Gauss kvadratikus reciprocitási tétele alapján ekkor uv darab p_i, q_j párra teljesül, hogy

$$\left(\frac{p_j}{q_i}\right) = -\left(\frac{q_i}{p_j}\right),$$

a többi párra pedig azonos a kongruencia bal és jobb oldalán álló Legendre szimbólum. Vagyis:

$$\left(\frac{P}{Q}\right) = (-1)^{uv} \left(\frac{Q}{P}\right).$$

Viszont itt uv pontosan akkor páratlan, ha u és v is páratlan, ami azzal ekvivalens, hogy P és Q is $4k+3$ alakú. Ezzel a tétel állítását beláttuk.

23.2. Négyzetgyökvonás modulo p

Az eddigiekben szó volt arról, hogy egy $x^2 \equiv a \pmod{p}$ mikor oldható meg, de arról nem, hogy ha ha megoldható, hogyan lehet egy x megoldást megtalálni?

Elsőre talán meglepő, de erre is vannak gyors algoritmusok. Ilyen pl. az ún. Tonelli–Shanks algoritmus, melyet Shanks [6] 1973-ban publikált, aki kifejtette:

„Azért késtem leírni a történelmi utalásokat, mert kölcsönadtam egy barátomnak a Dickson's History 1. kötetét, és soha nem kaptam vissza."

Tehát Dickson könyve szerint az algoritmus redundánsabb változata már 1891-ben létezett, és Tonelli [3] nevéhez kötődik.

Ismert egy másik algoritmus is négyzetgyökvonásra, Perelta [5] algoritmusa, amelynek egy ügyes 2×2-es mátrixokra alapuló ismertetését Robin Chapman jegyzete [2] adott meg.

Mindkét algoritmus elolvasható Számítógépes Számelmélet című egyetemi jegyzetem [4] 6.4 és 6.5 fejezetében.

Hivatkozások

[1] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arithmetica (1997) 82 (4), 365-377.

[2] R. Chapman, *Perelta's algorithm*, link.

[3] L. E. Dickson, *History of the Theory of Numbers* Vol. 1 (1919). Washington, Carnegie Institution of Washington. pp. 215–216.

[4] K. Gyarmati, *Számítógépes Számelmélet*, Egyetemi jegyzet 2022, link.

[5] R. C. Perelta, *A simple and fast probabilistic algorithm for computing square roots modulo a prime number*, I. E. E. E. Trans. Inform. Tehory 32 (1986), 846-847.

[6] D. Shanks, *Five Number-theoretic Algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics, 51–70. 1973.

[7] Kvadratikus maradékok táblázata, Wikipedia, Quadratic residue link.

[8] Ábra, Legendre sorozat illusztrálása, saját készítésű.

[9] Ábra, Gauss kvadratikus reciprocitási tételének bizonyításának illusztrálásához, saját készítésű.

24. Titkosítások

24.1. Mono-alfabetikus rejtjel

Régebben a történelem során az egyik leggyakoribb titkosítás az ún. mono-alfabetikus rejtjel volt, amikor minden betűt egy szimbólummal helyettesítünk, de ugyanazt a betűt mindig ugyanazzal a szimbólummal. Ennek egy kissé egyszerűsített formáját már Caesar is használta.

Kutatók, rejtjelfejtők a mai napig gyakran kerülnek abba a helyzetbe, hogy egy mono-alfabetikus rejtjelet kell megfejteniük, és nem csak akkor, amikor titkosításról van szó, hanem például, ha egy új, eddig nem ismert történelmi írásmódot szeretnének megfejteni.

A mono-alfabetikus rejtjel illusztrálásra, nézzük meg pl. a magyar rovásírást:

Amennyiben valaki nem ismeri, hogy melyik szimbólum melyik betűnek felel meg, a rejtjel megfejtése akár órákba is beletelhet. De a megfejtetés nem lehetetlen; pl. a magyar ábécében a leggyakoribb betű az E betű, a titkosított szövegben legtöbbször előforduló szimbólum az E betűnek felel meg. Hasonlóan megtalálható az ábécé második majd harmadik leggyakoribb betű kódja is, ez a magyar ábécében az A majd a T betű.

Ezek után lehet még rövid szavacskákat is vizsgálni, pl. a magyar nyelvben nagyon gyakori az „AZ” szócska, vagyis az A betűt kódját gyakran követi a Z betű kódja.

Ha az olvasónak van kedve és ideje, érdemes elolvasni a rejtjelezés talán legkorábbi és minden bizonnyal leghíresebb irodalmi megjelenését, Edgar Allan Poe Aranybogár című novelláját [5], melyben lényegében egy monoalfabetikus rejtjel megfejtése történik.

24.2. Vernam-féle titkosító eljárás

Tegyük fel, hogy titkosítani szeretnénk egy szöveget. A modern titkosítási rendszerek legelső lépése, hogy a szöveget egy számsorozattal írjuk le.

Például, a szöveg minden betűjéhez hozzárendelünk egy 0,1 sorozatot:

A: 000001	B: 000010	C: 000011	D: 000101	E: 000110	É: 000111
F: 001000	G: 001001	H: 001010	I: 001011	Í: 001100	J: 001101
K: 001110	L: 001111	M: 010000	N: 010001	O: 010011	Ó: 010100
Ö: 010101	Ő: 010110	P: 010111	Q: 011000	R: 011001	S: 011010
T: 011011	U: 011100	Ú: 011101	Ü: 011110	Ű: 011111	V: 100000
X: 100001	Y: 100010	Z: 110011			

Az ily módon kódolt szöveget könnyű visszafejteni betű gyakoriságelemzéssel. (Például a magyar nyelvben az E betű a leggyakoribb, így a kódolt szövegben a 000110 fog előfordulni leggyakrabban.)

Ezért ezt a számsorozatot muszáj titkosítani.

A Vernam-féle titkosító eljárás [7] során a számsorozatként leírt szöveget úgy titkosítjuk, hogy bitenként összeadjuk egy pszeudovéletlen sorozattal.

$$\begin{aligned} \text{Üzenet} &: (a_1, \ldots, a_N) \in \{0,1\}^N \\ \oplus\ \text{Titkos kulcs} &: \underline{(e_1, \ldots, e_N)} \in \{0,1\}^N \\ \text{Kódolt üzenet} &: (f_1, \ldots, f_N) \in \{0,1\}^N. \end{aligned}$$

Összeadási szabály:

$$\begin{aligned} 0 \oplus 0 = 0, \quad 1 \oplus 1 = 0, \\ 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1. \end{aligned}$$

Az eljárást az I. világháború során találta ki Vernam, de a mai napig a legbiztonságosabb titkosítási módszerek közé tartozik.

Ha a kulcs valódi véletlen sorozat, akkor a titkosítás során az üzenet minden bitje (egymástól függetlenül) azonos valószínűséggel változik meg illetve marad ugyanaz. Ezért ekkor ez a titkosítási mód tökéletes biztonságot ad.

A Vernam-féle titkosító eljárás egyetlen hátránya, hogy a titkos kulcsnak ugyanolyan hosszúnak kell lenni mint az üzenetnek.

A valódi véletlen sorozat generálás hosszú, fáradságos és költséges folyamat. Ezen manapság úgy segítenek, hogy számítógépek és számelméleti algoritmusokkal definiálnak véletlennek tűnő ún. pszeudovéletlen sorozatokat.

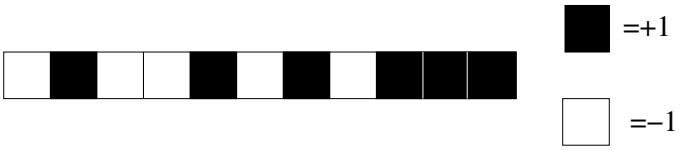
A területen írt első cikkükben, 1997-ben Mauduit és Sárközy [4] a következő konstrukciót adta meg a Legendre szimbólum felhasználásával:

$$E_{p-1} = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)\right).$$

Ez az konstrukció azonban minden p prímre csak egyetlen sorozatot ad meg. Egy ügyes ötlettel Hoffstein és Lieman [2] ezt a konstrukciót úgy terjesztette ki, hogy minden egyes p prímre több sorozatot tudunk generálni egyszerre, megadva ezzel pszeudovéletlen sorozatoknak egy nagy családját:

$$E_p(f) = \left(\left(\frac{f(1)}{p}\right), \left(\frac{f(2)}{p}\right), \ldots, \left(\frac{f(p)}{p}\right)\right) \quad \text{ahol most } \left(\frac{0}{p}\right) \stackrel{\text{def}}{=} 1.$$

Például, ha $p = 11$, $f(x) = x^2+1$ ez a sorozat a következőképp illusztrálható:



A fentiekkel megadott sorozat minden egyes polinomra megad egy pszeudovéletlen sorozatot. Hoffstein és Lieman azonban

nem bizonyítottak semmit a sorozat pszeudovéletlen tulajdonságairól, csak állították, hogy erős pszeudovéletlen tulajdonságokkal rendelkezik. Goubin, Mauduit és Sárközy [3] belátták, hogy néhány nem túl erős kikötést téve az f polinomra ezek a sorozatok statisztikai vizsgálatok segítségével nem különböztethető meg a valódi véletlen sorozattól.

Amennyiben a Vernam-féle titkosító eljárás során a fenti Legendre szimbólummal megadott pszeudovéletlen sorozatot használjuk kulcsként, a kommunikációban résztvevő feleknek elegendő a p prímben és az f polinom együtthatóiban megállapodni. Ezekben a számokban megállapodhatnak pl. a Diffie-Hellman kulcscserélő eljárás keretében (ld. 22. fejezet), vagy pedig a híres RSA-eljárás keretében, melyről bővebben a következő alfejeztben lesz szó.

24.3. RSA

Ron Rivest, Adi Shamir és Len Adleman [6] az 1970-es évek közepe táján megalkotta az egyik legismertebb titkosítási eljárást, az RSA-t. (Az RSA elnevezés a szerzők nevének kezdőbetűiből ered...)

Az RSA jó ideig számtalan informatikai, számítógépes, kommunikációs rendszerben jelentős szerepet játszott. Az alkalmazások során nagyon fontos a körültekintő implementálás, és hogy az alapvető biztonsági szempontok mellett, az apróságoknak tűnő dolgokra is ügyeljünk. Ilyen pl., hogy az algoritmusban szereplő két prím p és q nem lehet közel egymáshoz, de más fontos feltételek is vannak, melyek részletezésére a fejezetben nem térünk ki.

A következőkben ismertetjük az RSA titkosítási algoritmust.

Legyen $N = pq$ két nagy prím szorzata ($n/2$ darab számjegyből áll mindkettő), ezt az N-et nevezzük RSA modulusnak. Napjainkban N tipikus hosszúsága 2048 bit, amely 617 decimális jegyet jelent. Eleinte az $n = 128$ bites modulus is biztonságosnak bizonyult, majd a támadások és technika fejlődésének hatására folyamatosan növekedett: 256, 512, 1024 majd 2048 bitre.

Legyen e, d két egész szám, ahol

$$ed \equiv 1 \pmod{\varphi(N)}.$$

Itt $N = pq$ miatt $\varphi(N) = (p-1)(q-1)$. Az e-t nyilvános, míg a d-t privát exponensnek nevezzük.

Az (N, e) páros a publikus kulcs, míg az (N, d) páros a privát vagy másképp titkos kulcs. Ez utóbbit csak az a személy ismeri, akinek a titkosított üzenetet küldjük, és aki dekódolja majd az üzeneteinket.

Az üzenetet tekinthetjük egy egész számnak, amelyre $0 < M < N$. (Az egyszerűség kedvéért most feltesszük, hogy $(M, N) = 1$ teljesül az üzenetre. Ez az üzenet esetleges kis módosításával könnyen elérhető. Valójában azonban nincs szükség erre a feltételre, csak az általános esetben a dekódolás bizonyítása pár sorral hosszabb a lentieknél.)

A titkosított üzenet

$$C \equiv M^e \pmod{N} \qquad \leftarrow \text{RSA függvény.}$$

A dekódolás

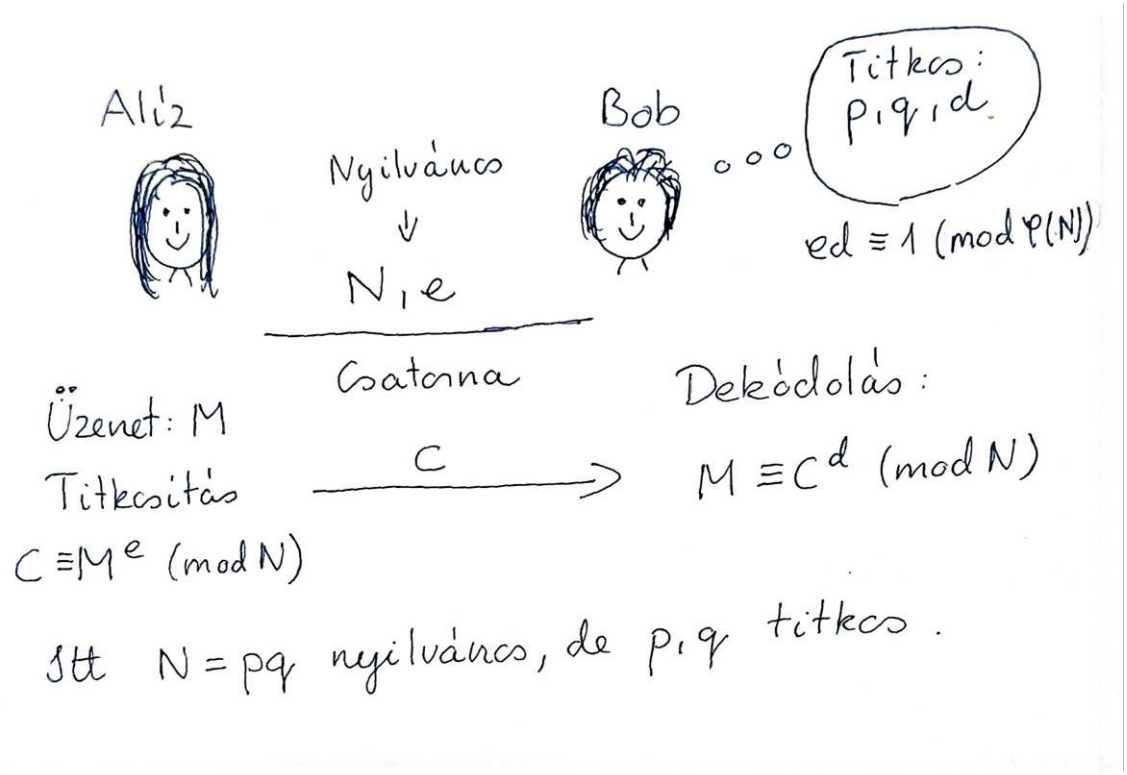
$$ed \equiv 1 \pmod{\varphi(N)} \quad \text{miatt}$$

$\exists k \in \mathbb{Z}^+$, melyre $ed = k\varphi(N) + 1$. Az Euler-Fermat tétel alapján

$$M \equiv C^d \pmod{N} \quad \text{ez a dekódolás,}$$

ugyanis

$$C^d \equiv (M^e)^d = M^{k\varphi(N)+1} = M\left(M^{\varphi(N)}\right)^k \equiv M \cdot 1^k$$
$$\equiv M \pmod{N}.$$



Az RSA algoritmusban $M \to M^e \pmod{N}$ egy egyirányú függvény, mivel a titkosítás a publikus kulcs (N, e) ismeretében könnyen elvégezhető moduláris hatványozással, melynek időigénye $O(\log e(\log N)^2)$ bitoperáció, azonban az invertálás d (azaz a privát) kulcs ismerete nélkül nagyon nehéz.

Az RSA támadások nagyobb része arra irányul, hogy d ismeret nélkül, hogyan lehetne invertálni az RSA függvényt. Pontosabban

fogalmazva, ha csupán (N, e, C) hármas adott (és p, q, d titkos) akkor képesek vagyunk-e az eredeti M üzenetet C-ből visszaállítani.

Megjegyzés: p, q, e-ből d számolható, ekkor ugyanis d az

$$ex \equiv 1 \pmod{(p-1)(q-1)}$$

lineáris kongruencia megoldása. De p, q titkos, csak $N = pq$ adott, p, q ismeretéhez N-et faktorizálni kell, ez azonban nagy N számok esetén nagyon-nagyon lassú. Amennyiben a p és q prímek elég nagyok, akkor az N faktorizálása annyi időbe telne még modern számítógépekkel is (pl. több évezred), amely valójában kivárhatatlan.

Míg a faktorizásra nem ismert gyors algoritmus, a fordított irányú műveletre, azaz p és q ismeretében a szorzat $N = pq$ kiszámolására vannak nagyon gyors algoritmusok.

Az RSA-ról a fentieknél bővebben a Számítógépes Számelmélet [1] jegyzetben írtam, beleértve azt is, hogy a helytelen alkalmazások során milyen buktatók lehetnek.

Hivatkozások

[1] K. Gyarmati, *Számítógépes Számelmélet*, Egyetemi jegyzet 2022, link.

[2] J. Hoffstein, D. Lieman, *The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher*, Progress in Computer Science and Applied Logic, Vol. 20, Birkhäuser, Verlag, Basel, 2001; pp. 59-68.

[3] L. Goubin, C. Mauduit, A. Sárközy, *Construction of large families of pseudorandom binary sequences*, Journal of Number Theory 106 (1) (2004), 56-69

[4] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arithmetica 82 (4) (1997), 365-377

[5] E. A. Poe, *Aranybogár*, http://vmek.oszk.hu/03500/03575/.

[6] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM. 21 (2) (1978), 120–126.

[7] G. S. Vernam, *Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications*, Transactions of the American Institute of Electrical Engineers 55 (1926), 109–115.

[8] Ábra, Székely-magyar rovásírás, link.

[9] Ábra, RSA eljárás, saját készítésű.

25. Prímszámok száma

A fejezetben főként $\pi(x)$-re adunk minél élesebb becsléseket, bár a létező legélesebb becslések bizonyítása messze túl megy a jelen jegyzet keretein, ugyanis mély és technikás analízisbeli eszközöket kiván.

A fejezetbeli bizonyítások és történeti áttekintés egyrészét Szalay Mihály, Számelmélet [18] tankönyve alapján készítettem, néhol azonban apróbb kiegészítésekkel és ábrákkal.

Legendre már 1798-ban azt sejtette, hogy $\pi(x)$ becsülhető egy $\frac{x}{A\log x+B}$ alakú kifejezéssel, ahol A és B állandók.

A sejtés igazolása felé Csebisev [19], [20] tette meg az első nagy lépést (1848 és 1852 között), mégpedig annak bizonyításával, hogy $\pi(x)$ az $x/\log x$ két konstansszorosa közé esik. Tételét az alábbi formában mi is igazoljuk:

25.1. TÉTEL. (Csebisev) *Ha* $x \geq 2$*, akkor*

$$0.34 \cdot \frac{x}{\log x} < \pi(x) < 4 \cdot \frac{x}{\log x}.$$

Csebisevnek azonban nem sikerült bizonyítania a

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\log x}}$$

határérték létezését, csupán azt, amennyiben létezik ez a határérték, akkor az szükségszerűen 1.

Több mint 40 évet kellett várni addig, amíg ezt az állítást sikerült belátni.

Azt, hogy a határérték létezik (és akkor 1), először Jacques Salomon Hadamard [7] és Jean de la Vallée Poussin igazolta [14] egymástól függetlenül 1896-ban, melyet ma prímszámtételnek hívunk:

25.2. TÉTEL. (Prímszámtétel)

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

J. S. Hadamard

C.-J. de La Vallée Poussin

A prímszámtétel segítségével becslést nyerhetünk az n-edik prímszám nagyságára is:

25.3. TÉTEL. *Jelölje $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ a prímek növekvő sorozatát. Ekkor*

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

Sőt, a prímszámtételnél de la Vallée Poussin [15] többet is igazolt, nevezetesen:

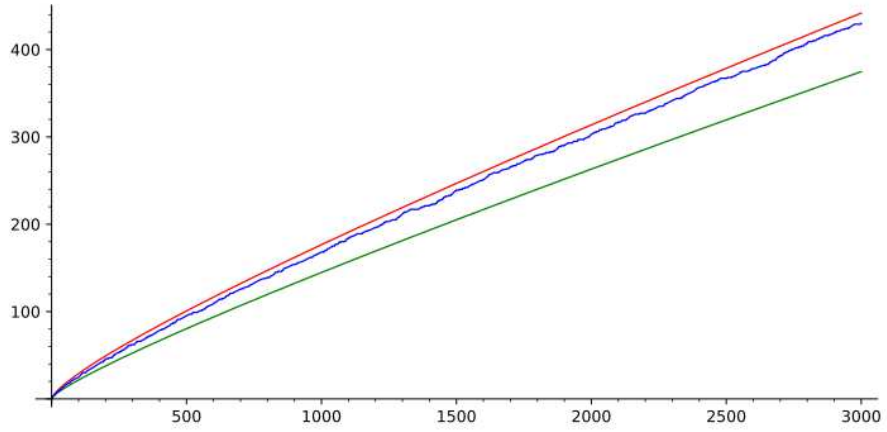
25.4. TÉTEL. *Létezik olyan c_1 és c_2 pozitív állandó, hogy*

$$\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| < c_1 x e^{-c_2\sqrt{\log x}}.$$

Elsőre talán rejtélyes, hogy miért jobb közelítése $\pi(x)$-nek az $\int_2^x \frac{dt}{\log t}$ mint a $\frac{x}{\log x}$.

Azt, hogy a prímszámok száma jól közelíthető $\int_2^x \frac{dt}{\log t}$-vel még Gauss sejtette 1792 tájékán (15 évesen) [5], igaz erre csupán egy 72 éves korában írt levélben utalt. A továbbiakban az $\int_2^x \frac{dt}{\log t}$ kifejezést $\mathrm{Li}(x)$-szel jelöljük.

A következő ábrán a $\pi(x)$-et ábrázoljuk (kék vonal), a $\mathrm{Li}(x)$-et (piros vonal) és az $\frac{x}{\log x}$ függvényt (zöld vonal) a $[2, 3000]$ intervallumon.



Az ábrán látható, hogy a $\mathrm{Li}(x)$ függvény közelebb van a $\pi(x)$ függvényhez mint a $\frac{x}{\log x}$ függvény. De ez akkor derül ki igazán, ha parciálisan integráljuk a $\mathrm{Li}(x)$ függvényt:

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} - \frac{2}{\log 2}.$$

Mégegyszer parciálisan integrálva pedig

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \int_2^x \frac{dt}{(\log t)^3} - \frac{2}{\log 2} - \frac{2}{(\log 2)^2}.$$

Az eljárást folytatva egyre finomabb közelítéseit kapjuk $\mathrm{Li}(x)$-nek.

Gauss [5] 15 évesen azt sejtette, hogy minden x-re $\pi(x) < \mathrm{Li}(x)$, és sejtését ellenőrizte is az $x < 3000000$ esetén. Ez a sejtés hosszú évszázadokon át fennállt.

Csak 1914-ben sikerült J. E. Littlewoodnak [10] megcáfolnia a sejtést. Deléglise és Rivat [2] eredményei szerint a legkisebb ellenpélda is nagyobb mint 10^{20}. 2005-ben pedig Chao és Plymen [1] igazolta olyan ellenpélda létezését, amely $< 10^{317}$.

A jegyzetben az eddig említett tételek közül csupán Csebisev tételét igazoljuk, hiszen csak annak bizonyítása érhető el elemileg. A 25.1. Tételbeli felső becslésnek a bizonyítása a következő önmagában is érdekes tételen alapul:

25.5. Tétel. *Tetszőleges $x \geq 2$ szám esetén az x-nél nem nagyobb prímek szorzatára:*

$$\prod_{p \leq x} p < 4^x.$$

25.5. Tétel bizonyítása. A következő becslés Erdős Pál és Kalmár László munkája (bár ők maguk a bizonyítást nem publikálták, az több ismeretterjesztő írásban megjelent).

Erdős Pál

Kalmár László

A bizonyítás során feltehetjük, hogy x egész szám.

Teljes indukcióval bizonyítjuk a tételt. Az indukció kezdőlépései az $x = 1$ és $x = 2$ eset, melyek nyilvánvalóak.

Legyen $n \geq 3$. Feltesszük, hogy a n-nél kisebb egészekre fennáll az egyenlőtlenség, és bebizonyítjuk, hogy $x = n$-re is.

Ez nagyon egyszerű, ha n páros, mert ekkor a $n \geq 3$ feltevés miatt n összetett, és így

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p < 4^{n-1} < 4^n.$$

Legyen a továbbiakban $n = 2k + 1 > 4$ páratlan szám. Ekkor a szorzat

$$\prod_{p \leq 2k+1} p = \left(\prod_{p \leq k+1} p \right) \left(\prod_{k+2 \leq p \leq 2k+1} p \right). \qquad (25.1)$$

Az indukciós feltevés miatt az első zárójelben lévő szorzat kisebb mint 4^{k+1}. A második zárójelben lévő szorzat osztója a

$$(k+2)(k+3)\cdots(2k+1) = \frac{(2k+1)!}{(k+1)!} = k! \binom{2k+1}{k}$$

számnak, de mivel ez a szorzat $k!$-hoz relatív prím, ezért osztója $\binom{2k+1}{k}$-nak. A következőkben $\binom{2k+1}{k}$-t becsüljük.

$$\begin{aligned}\binom{2k+1}{k} &= \frac{2\cdot 4\cdot 6\cdot\dots 2k\cdot 3\cdot 5\cdot\dots\cdot(2k+1)}{k!(k+1)!}\\ &= 2^k\cdot\frac{3\cdot 5\cdot\dots\cdot(2k+1)}{2\cdot 3\cdot\dots\cdot(k+1)}\\ &< 2^k\cdot\frac{4\cdot 6\cdot\dots\cdot(2k+2)}{2\cdot 3\cdot\dots\cdot(k+1)}\\ &= 4^k.\end{aligned}$$

Így (25.1) alapján:

$$\prod_{p\le 2k+1} p < 4^{k+1}\cdot 4^k = 4^{2k+1},$$

ami éppen a bizonyítandó állítás.

25.1. Tétel bizonyítása. Először a felső becslést igazoljuk. (Az alábbi bizonyítás Erdős Páltól és Kalmár Lászlótól származik.) A 25.5. Tételt felhasználva azt kapjuk tehát, hogy

$$4^x > \prod_{\sqrt{x}\le p\le x} p > (\sqrt{x})^{(\pi(x)-\pi(\sqrt{x}))} > (\sqrt{x})^{(\pi(x)-\sqrt{x})}.$$

A két szélső mennyiség logaritmusát véve és $\pi(x)$-et kifejezve

$$\pi(x) < \frac{(2\log 4)x}{\log x} + \sqrt{x} = \frac{\left(2\log 4 + \frac{\log x}{\sqrt{x}}\right)x}{\log x}.$$

Könnyen ellenőrízhető, hogy $\frac{\log x}{\sqrt{x}} < 0.8$, hiszen ez $x = 2,3,4,\dots,8$-ra ez kiszámolható, $x\ge 8$ esetén pedig a $\frac{\log x}{\sqrt{x}}$ függvény monoton csökken, mert a deriváltja negatív. Tehát:

$$\pi(x) < \frac{(2\log 4 + 0.8)\,x}{\log x} < 4\frac{x}{\log x},$$

ami a bizonyítandó felső becslés volt.

Ezután rátérünk az alsó becslés igazolására. Az itt ismertetésre kerülő bizonyítás Landau [9] munkája.

A bizonyítás az ún. Legendre formulát használja, mely a következő:

25.6. Lemma. (Legendre formula) *Legyen n és k pozitív egész számok, p pozitív prím, melyre $p^k \leq n < p^{k+1}$. Ekkor $n!$ prímtényezős felbontásában p kitevője:*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots + \left[\frac{n}{p^k}\right]$$

25.6. Lemma bizonyítása. Az $n!$ az $1, 2, 3, \ldots, n$ számok szorzata, ezek között $\left[\frac{n}{p}\right]$ darab p-vel osztható van. De a számok között p^2-tel is oszthatók vannak, mégpedig $\left[\frac{n}{p^2}\right]$ darab, ezek hozzáadnak a kitevőhöz $\left[\frac{n}{p^2}\right]$ darab egyest. Az eljárást folytatva a kitevőhöz hozzádjuk még a $p^3, p^4, \ldots, p^k$-nal osztható számok számát, és ezzel készen vagyunk, hiszen p^{k+1}-nel osztható szám már nincs.

Tekintsük a $\binom{2n}{n}$ binomiális kitevőt:

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{\beta_p}, \tag{25.2}$$

ahol az előző lemma miatt β_p-re tudjuk, hogy

$$\beta_p = \sum_{j=1}^{k_p} \left(\left[\frac{2n}{p^j} \right] - 2 \left[\frac{n}{p^j} \right] \right).$$

A fenti képletben k_p-re pedig $p^{k_p} \leq 2n < p^{k_p+1}$.

Mivel tetszőleges y-ra $[2y] - 2[y] \leq 1$, így

$$\beta_p \leq \sum_{j=1}^{k_p} 1 = k_p,$$

s ebből adódoan $p^{\beta_p} \leq p^{k_p} \leq 2n$. Ezt (25.2)-be írva:

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\beta_p} \leq (2n)^{\pi(2n)}.$$

Azután alulról is becsüljük ugyanezt a binomiális együtthatót:

$$\begin{aligned} \binom{2n}{n} &= \frac{2 \cdot 4 \cdot \ldots \cdot (2n) \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)}{1 \cdot 2 \cdot \ldots \cdot n \cdot n!} \\ &= 2^n \cdot \frac{3 \cdot 5 \cdot \ldots \cdot (2n-1)}{n!} \\ &> 2^n \cdot \frac{2 \cdot 4 \cdot \ldots \cdot (2n-2)}{1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n} \\ &= \frac{2^{2n-1}}{n} = \frac{2^{2n}}{2n}. \end{aligned}$$

A két becslés egybevetéséből

$$(2n)^{\pi(2n)} > \frac{2^{2n}}{2n},$$

ahonnan

$$\pi(2n) + 1 > \log 2 \cdot \frac{2n}{\log(2n)}.$$

Ezzel páros egészekre be is bizonyítottuk az alsó becslést. Páratlan számokra kicsit tovább kell számolni:

$$\begin{aligned}
\pi(x) &\geq \pi\left(2\left[\frac{x}{2}\right]\right) \\
&> \log 2 \cdot \frac{2\left[\frac{x}{2}\right]}{\log\left(2\left[\frac{x}{2}\right]\right)} - 1 \\
&> \log 2 \cdot \frac{2\left(\frac{x}{2}-1\right)}{\log x} - 1 \\
&= \log 2 \cdot \frac{x}{\log x} - \left(\frac{2\log 2}{\log x} + 1\right) \\
&\geq \log 2 \cdot \frac{x}{\log x} - 3 \\
&> 0.34\frac{x}{\log x}.
\end{aligned}$$

Ezzel a 25.1. Tétel bizonyítását befejeztük.

Ha a 25.1. Tételnél kicsit élesebb becslést tudnánk adni $\pi(x)$-re, (mondjuk $0.75\frac{x}{\log x} < \pi(x) < 1.5\frac{x}{\log x}$), akkor abból kijön, hogy $\pi(n) < \pi(2n)$, azaz n és $2n$ közé mindig esik prím. Az, hogy ez így van Bertrand sejtett először 1845-ben, azóta úgy ismerik, hogy Bertrand-féle posztulátum. A sejtést Csebisev igazolta először.

25.7. TÉTEL. (Csebisev) *Ha n pozitív egész, akkor n és $2n$ közé mindig esik prím.*

A Csebisev tételnek egy elemi bizonyítását az érdeklődők pl. itt tudják elolvasni: link.

A prímszámok számának becsléséhez kapcsolódik a számelmélet egyik leghíresebb sejtése a Riemann-sejtés, melyet Bertrand Riemann fogalmazott meg egyetlen számelmélet témájú

dolgozatában, a doktori értekezésében. Eredményei, noha jórészüket nem bizonyította a lehető legnagyobb hatással volt a számelmélet területére.

A Riemann-sejtés ismertetése túl megy a jelen jegyzet keretein, csak annyit említünk meg, hogy az azt állítja, hogy ha a nem triviális gyökeit nézzük a $\sum_{n=1}^{\infty} \frac{1}{n^s}$ sor analítikus kiterjesztésének a komplex számsíkra, akkor azok az $x = \frac{1}{2}$ egyenesen helyezkednek el.

Koch [8] eredménye szerint a sejtéssel ekvivalens, hogy létezik c pozitív konstans, amelyre:

$$|\pi(x) - \mathrm{Li}(x)| < c\sqrt{x}\log x.$$

A Riemann-sejtésről bővebben pl. itt olvashatnak: link.

Noha $\mathrm{Li}(x)$ lényegesen jobb közelítés $\pi(x)$-re mint az $\frac{x}{\log x}$ függvény, előfordulhatnak olyan alkalmazások, bizonyítások, amikor elegendő $\pi(x)$-et $\frac{x}{\log x}$ függvénnyel közelíteni. Azonban az ilyen típusú becslések között is vannak élesek és kevésbé élesek. Ezek közül említünk most néhányat.

Így pl. ha $x \geq 17$:

$$\frac{x}{\log x} < \pi(x) < 1.25506\frac{x}{\log x}$$

A bizonyítás megtalálható [17]-ben. Felső becslésként $x \geq 1$-re Dusart [4] bebizonyította, hogy

$$\pi(x) \leq \frac{x}{\log x}\left(1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + \frac{7.59}{\log^3 x}\right).$$

Az n-edik prímszám értékére elég éles becslések a következők:

$$n(\log(n \log n) - 1) < p_n < n\log(n \log n),$$

ha $n \geq 6$. Itt a felső becslés Rosser-től származik [16], míg az alsó Dusart-tól [3]. További becslések olvashatóak a kapcsolódó Wikipédia oldalon [22].

Érdemes még ismerni néhány prímek eloszlásával kapcsolatos további fontos eredményt is, pl. Mertens három tételét, melynek az olvasók pl. itt tudnak utánanézni: link.

Nevezetes még Dirichlet tétel is, mely a következőt állítja:

25.8. TÉTEL. (Dirichlet) *Ha a és b relatív prím egész számok $b \neq 0$, akkor az $a,\ a+b,\ a+2b, \ldots$ számtani sorozat végtelen sok prímet tartalmaz.*

A bizonyítás nagyon mély, messze túl megy a jelen jegyzet keretein, de megemlítjük még a modern számelmélet egyik legfontosabb prímekkel kapcsolatos eredményét is (szintén bizonyítás nélkül), mely Ben Greentől és Terence Taotól [6] származik:

25.9. TÉTEL. (Green - Tao) *A prímszámok között van tetszőlegesen hosszú számtani sorozat.*

Fontos modern eredmény kapcsolódik a prímhézagok becsléséhez is. Jelölje d_n az $n+1$-edik és n-edik prím különbségét, azaz:

$$d_n = p_{n+1} - p_n.$$

A prímszámtételből azonnal következik, hogy d_n végtelen sokszor kisebb mint $(1+\varepsilon)\log n$. Ezt a becslést folyamatosan javítgatták, egyre jobb eredmények születtek pl. Erdős, Bombieri-Davenport, Maier tollából.

2009-ben átütő eredményt ért el Pintz János és Yıldırım, Cem Y. [11] bebizonyítva, hogy végtelen sokszor fennáll

$$d_n < (\log n)^{1/2+\varepsilon},$$

akármilyen pozitív ε-ra.

Ezután sikerült bebizonyítani, hogy d_n végtelen sokszor kisebb mint egy konstans! Zang [21] bebizonyította, hogy d_n végtelen sokszor kisebb mint 70 millió. Ez a becslés is folyamatosan javult, a ma ismert legjobb eredmény a Polymath Project 8B [12], [13] keretében elért eredmény, nevezetesen

$$d_n \leq 246$$

végtelen sok n-re.

Tehát már megközelítettük, de még nem bizonyítottuk be, a híres ikerprím-sejtést, azaz, hogy végtelen sok p prím létezik, amelyre $p+2$ is prím.

Ezzel a jegyzet végére értünk... További kellemes időtöltést kívánok!

Hivatkozások

[1] K.F. Chao, R Plymen, *A new bound for the smallest x with* $\pi(x) > \mathrm{Li}(x)$, Int. J. Number Theory 6 (2010) 681-690.

[2] M. Deléglise, J. Rivat, *Computing* $\pi(x)$*: The Meissel, Lehmer, Lagarias, Miller, Odlyzkomethod method*, Math. Comp. 65 (1996), 235-245.

[3] P. Dusart, Pierre, *The* k *kth prime is greater than* $k(\ln k + \ln\ln k - 1)$ *for* $k \geq 2$, Mathematics of Computation. 68 (225) (1999) 411–415.

[4] P. Dusart, *Explicit estimates of some functions over primes*. Ramanujan Journal. 45 (1) (2018), 225–234.

[5] H. M. Edwards, *Riemann's zeta function*, Academic Press, New York, 1974.

[6] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics, 167 (2) (2008), 481–547, link.

[7] J. Hadamard, *Sur la distribution des zéros de la fonction* $\zeta(s)$ *et ses conséquences arithmétiques*, Bulletin de la Société Mathématique de France, Société Mathématique de France, 24 (1896) 199–220.

[8] N. H. von Koch, *Sur la distribution des nombres premiers*, Acta Mathematica, 24: 159–182.

[9] E. Landau, *Vorlesungen über Zahlentheorie* 1927, I. köt. 67. old.

[10] J. E. Littlewood, *Sur la distribution des nombres premiers*, C. R. Acad.Sci. Paris 158 (1914) 1869-1872.

[11] J. Pintz, C. Yıldırım, C Yalçin Primes in tuples. II. Acta Math. 204 (1) (2010), 1–47.

[12] Polymath, D. H. J., *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. 1 (2014), Art. 12, 83 pp.

[13] Polymath, D. H. J., *Erratum to: Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. 2 (2015), Art. 15, 2 pp.

[14] C. J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Annales de la Société scientifique de Bruxelles, Imprimeur de l'Académie Royale de Belgique, 20 B, 21 B (1896), 183–256, 281–352, 363–397, 351–368.

[15] C. J. de la Vallée Poussin, *Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs a une limite donnée*, Mémoires couronnés de l'Académie de Belgique, Imprimeur de l'Académie Royale de Belgique (1899) 59, 1–74.

[16] J. B. Rosser, *Explicit bounds for some functions of prime numbers*, American Journal of Mathematics. 63 (1) (1941), 211–232.

[17] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. 6 (1962), 64-94.

[18] Szalay Mihály, *Számelmélet*, link.

[19] Tchebychef, P. L. (1899), Markov, Andrey Andreevich; Sonin, N. (eds.), *Oeuvres, vol. I*, New York: Commissionaires de l'Académie impériale des sciences, MR 0147353, Reprinted by Chelsea 1962.

[20] Tchebychef, P. L. (1907), Markov, Andrey Andreevich; Sonin, N. (eds.), *Oeuvres, vol. II*, New York: Commissionaires de l'Académie impériale des sciences, MR 0147353, Reprinted by Chelsea 1962.

[21] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. (2) 179 (2014), 1121–1174

[22] Wikipedia, *Prime-counting function*, (2022, September 14), link.

[23] Fotó, Pafnutyij Lvovics Csebisev, Wikipedia link.

[24] Fotó, Peter Gustav Lejeune Dirichlet, Wikipedia link.

[25] Fotó, Erdős Pál, KÖMAL Arcképcsarnok, link.

[26] Fotó, Jacques Salomon Hadamard, Wikipedia, link.

[27] Fotó, Kalmár László, Wikipedia, link.

[28] Fotó, Edmund Landau, Wikipedia, link.

[29] Fotó, Adrien-Marie Legendre, Wikipedia, link.

[30] Fotó, Charles-Jean de La Vallée Poussin, Wikipedia, link.

[31] Fotó, Georg Friedrich Bernhard Riemann, Wikipedia, link.

[32] Ábra, $\pi(x)$, $\mathrm{Li}(x)$, $\frac{x}{\log x}$, saját készítésű a Software for Algebra and Geometry Experimentation programmal.