Számelmélet 2

Gyarmati Katalin

katalin.gyarmati@ttk.elte.hu

Sárközy András

andras.sarkozy@ttk.elte.hu

Eötvös Loránd Tudományegyetem
Egyetemi Jegyzet

ELTE TTK, Matematikai Intézet

2024

Tartalomjegyzék

Bevezetés

A bevezető elemi számelmélet egyetemi kurzus után se érdemes a számelmélet tanulmányozását abbahagyni, számos olyan téma van, ami még viszonylag egyszerűen elérhető, és amelyeket akár érdemes megismerni a mélyebb számelméleti tanulmányok előtt. Jelen jegyzetben pár ilyen fejezetet gyűjtöttünk össze.

Irodalom

A jegyzet megírása során széles körű irodalmat használtunk, kiemelnénk ezek közül pár könyvet az alábbiakban.

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

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

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

Gyarmati Katalin, *Elemi Módszerek a Kombinatorikus Számelméletben*, link.

Gyarmati Katalin, *Elemi Számelmélet*, link.

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

Sárközy András, *Számelmélet*, link

Sárközy András, *Számelmélet és Alkalmazásai*, link.

Wikipédia, link.

A részletesebb (további) irodalmat mindig az adott fejezet végén a referenciajegyzékben tüntettük fel, akárcsak az illusztráló ábrák forrását (kivételt képeznek ez alól a saját készítésű ábrák).

Most nem építettünk rá ugyan, de az érdeklődőknek szívesen ajánljuk a következő könyveket is:

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

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

Szalay Mihály, *Számelmélet*, link

Az olvasóknak kellemes időtöltést kívánunk!

1. Pár szó a Riemann sejtésről

Hol hagytuk abba az előző számelmélet kurzust?

Akkor az alapokból indultunk ki; most: modern számelmélet fejezeteinek ismertetése következik. Valahogy így:

Adódna, hogy lineárisan haladjunk:

Így is fogunk haladni, de nem rögtön, felsőbb éven lesz pár speciális számelmélet tárgyunk, de előtte azért még mindig szükséges bizonyos előismeret.

Ahhoz, hogy a fenti fejezetekbe betekintést nyerjünk két lehetőségünk is van:

1. Újra végigmenni az egyes fejezeteken, de most kicsit mélyebbre ásni mint első éven

2. Elmélyedni 1 vagy 2 viszonylag hozzáférhetőbb területben (pl. kombinatorikus számelméletben vagy geometriai számelméletben.

Alapjában az első utat fogjuk választani: végigmegyünk az egyes fejezeteken, de súlyozva azokat.

Először a prímszámelmélettel kezdjük. A területen az egyik legfontosabb eredmény a következő:

1.1 TÉTEL. (Prímszámtétel)

$$\lim_{x\to\infty} \frac{\frac{\pi(x)}{x}}{\frac{}{\log x}} = 1$$

A fenti tétel nagyon sokáig csak sejtés volt... Csebisev több részeredménye után, végül azt, hogy a fenti határérték létezik (és akkor 1), először Jacques Salomon Hadamard [2] és Jean de la Vallée Poussin igazolta [3] egymástól függetlenül 1896-ban.

J. S. Hadamard

C.-J. de La Vallée Poussin

Még régebben, a 15 éves Gauss 1792 tájékán azt sejtette, hogy a prímszámok számára van $\frac{x}{\log x}$-nél van egy még pontosabb közelítés, nevezetesen $\int_2^x \frac{dt}{\log t}$, igaz erre csupán egy 72 éves korában írt levélben utalt [1].

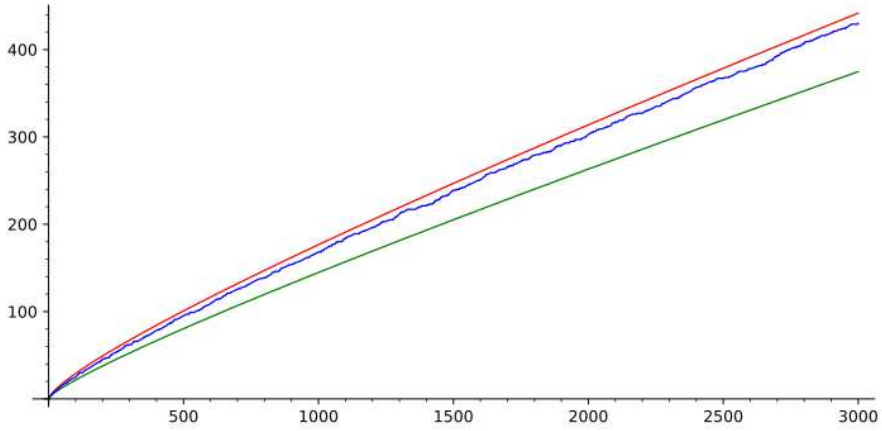
A továbbiakban legyen

$$\mathrm{Li}(x) \stackrel{\text{def}}{=} \int_2^x \frac{dt}{\log t},$$

az ún. integrál-logaritmus függvény.

Elsőre talán rejtélyes, hogy miért jobb közelítése $\pi(x)$-nek az $\int_2^x \frac{dt}{\log t}$ mint az $\frac{x}{\log x}$.

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.

Az $\frac{x}{\log x}$ és $\mathrm{Li}(x)$ függvény kapcsolata, akkor látszik jól, ha parciálisan integráljuk a $\mathrm{Li}(x)$ függvényt:

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} - \frac{2}{\log 2}.$$

Még egyszer 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.

Tehát a prímszámtétel bizonyítása után következő lépésnek

$$\left|\pi(x) - \frac{x}{\log x}\right|$$

„különbség” vizsgálata adódott volna; de mivel kiderült, hogy $\pi(x)$ jobban közelíthető a $\frac{x}{\log x}$ helyett a $\mathrm{Li}(x)$-szel, így a

$$\Delta(x) = |\pi(x) - \mathrm{Li}(x)|$$

„hiba” becslése lett a számelmélet egyik legfontosabb problémája.

Tudjuk például, hogy tetszőleges nagy A számot megadva, elég nagy x-re

$$\Delta(x) < \frac{x}{(\log x)^A},$$

sőt

$$\Delta(x) < \frac{x}{e^{(\log x)^c}}, \quad c \to 3/5.$$

Itt megjegyezendő, hogy de La Vallée Poussin nem csak a prímszámtételt bizonyított anno, hanem a fenti állítást is $c = \frac{1}{2}$-del.

Másik irányból azt tudjuk, hogy

$$\Delta(x) > c\sqrt{x} \quad (\infty \text{ sok } x\text{-re}).$$

Sejtés:

$$\Delta(x) < x^{1/2+\varepsilon},$$

bármely pozitív ε-ra. Összefügg az ún. Riemann-sejtéssel. A $\Delta(x) = |\pi(x) - \mathrm{Li}(x)|$ értékéről bővebben a kapcsolódó Wikipédia oldalon is olvashatunk: link.

Egy-két szó $\Delta(x)$ becsléséhez kapcsolódó eszközökről, az analitikus számelméletről.

Tekintsük a

$$\sum_{n=1}^{+\infty} \frac{1}{n^s}$$

∞ sort, ez $s > 1$ esetén abszolút konvergens (az ún. hiperharmonikus sor). Az összegfüggvényt jelöljük $\zeta(s)$-sel:

$$\zeta(s) \stackrel{\text{def}}{=} \sum_{n=1}^{+\infty} \frac{1}{n^s} \qquad (s > 1).$$

Ez az ún. Riemann-féle ζ-függvény.

A modern számelméletben meghatározó szerepet játszó azonosság:

1.2 TÉTEL. (A Riemann-féle ζ-függvény Euler-féle szorzat-előállítása)

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}} \qquad (\mathrm{Re}\, s > 1).$$

A 1.2 Tétel bizonyítása. Először csak egy vázlatot ismertetünk. A végtelen mértani sor összegképlete szerint $|x| < 1$ esetén:

$$\frac{1}{1-x} = 1 + x + x^2 + \ldots + x^n + \ldots \qquad (|x| < 1),$$

$$\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots + \frac{1}{p^{ns}} + \ldots \quad \left(\frac{1}{p^s} \leq \frac{1}{2} < 1\right).$$

Így

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \left(1 + \frac{1}{{p_1}^s} + \frac{1}{{p_1}^{2s}} + \ldots + \frac{1}{{p_1}^{\alpha_1 s}} + \ldots\right)$$
$$\left(1 + \frac{1}{{p_2}^s} + \frac{1}{{p_2}^{2s}} + \ldots + \frac{1}{{p_2}^{\alpha_2 s}} + \ldots\right) \cdots$$
$$\left(1 + \frac{1}{{p_r}^s} + \frac{1}{{p_r}^{2s}} + \ldots + \frac{1}{{p_r}^{\alpha_r s}} + \ldots\right).$$

Itt $\forall\ \infty$ sor $\forall$ tagja nem negatív, így lehet tagonként szorozni (pontosítás később):

$$\prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{\alpha_1=0}^{+\infty} \cdots \sum_{\alpha_r=0}^{+\infty} \underbrace{\frac{1}{\left({p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r}\right)^s}}$$

itt valahonnan kezdve $\forall$ kitevő 0,
$\forall$ véges n természetes szám
egy és csak egyféleképpen
írható fel ebben az alakban

$$= \sum_{n=1}^{\infty} \frac{1}{n^s},$$

kész. A teljes bizonyításhoz annyi pontosítás kell, hogy

$$\left|\zeta(s) - \prod_{p \leq z} \frac{1}{1-\frac{1}{p^s}}\right| < \sum_{n=z+1}^{\infty} \frac{1}{n^s} \longrightarrow 0,$$

amint $z \to \infty$, ha $\operatorname{Re} s > 1$.

Alkalmazásul egy újabb bizonyítás arra, hogy ∞ sok prím $\exists$:

1.3 TÉTEL. ∞ *sok prímszám* $\exists$.

A 1.3 Tétel bizonyítása. Tegyük fel indirekt, hogy csak véges sok prím létezik, legyenek ezek $p_1, p_2, \ldots, p_k$. Ekkor

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}} = \frac{1}{1 - \frac{1}{{p_1}^s}} \cdot \frac{1}{1 - \frac{1}{{p_2}^s}} \cdots \frac{1}{1 - \frac{1}{{p_k}^s}}.$$

Nézzük, hogy mi történik itt, ha $s \to 1+$? Baloldal:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \to \infty, \tag{1.1}$$

hiszen a $\sum_{n=1}^{\infty} \frac{1}{n}$ harmonikus sor divergens. A jobboldalon:

$$\frac{1}{1 - \frac{1}{{p_i}^s}} \to \frac{1}{1 - \frac{1}{{p_i}^1}} = \frac{1}{1 - \frac{1}{p_i}}$$

Így:

$$\prod_p \frac{1}{1 - \frac{1}{p^s}} \to \underbrace{\frac{1}{1 - \frac{1}{p_1}} \cdot \frac{1}{1 - \frac{1}{p_2}} \cdot \ldots \cdot \frac{1}{1 - \frac{1}{p_k}}}$$

Ez egy véges szám, ellentmond (1.1)-nek.

Hasonlóan azt is bebizonyíthatnánk akár, hogy

$$\sum_{p \le n} \frac{1}{p} \to \infty.$$

Hogy lehet ebből továbbmenni?

1.4 DEFINÍCIÓ. *Egy* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *alakú végtelen sort, ahol* $a_1, a_2, \ldots, a_n, \ldots$ *adott valós vagy komplex számok,* s *valós vagy komplex változó, Dirichlet-sornak nevezünk.*

Kidolgozható a Dirichlet-sorok elmélete (pl. formula adható a $\sum_{n\le x} a_n$ együttható összegre). Ezt alkalmazva a ζ-függvényre pontosabban

$$(\log \zeta(s))' = \frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\text{-re,}$$

becslést nyerünk e Dirichlet-sor együttható összegére:

$$\sum_{n\le x} \Lambda(n) \sim \sum_{p\le x} \log p \sim \pi(x)\log x\text{-re.}$$

Itt $\Lambda(n)$ a Mangoldt-szimbólum:

$$\Lambda(n) = \begin{cases} \log p, & \text{ha } n = p^\alpha, \\ 0, & \text{ha } n \neq p^\alpha. \end{cases}$$

De: Dirichlet-sorok vizsgálatához – így együttható összeg formulához is, ki kell terjeszteni a $\zeta(s)$ függvény értelmezését komplex változókra is.

Riemann kiterjesztette a definíciót komplex számsíkra is (azaz értelmezési tartomány a komplex számsík, és $\operatorname{Re} s > 1$-re megegyezik az általunk definiált ζ-függvénnyel).

Egy lehetséges kiterjesztés a következő:

$$\zeta(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1}}{e^x - 1}\,\mathrm{d}x\,,$$

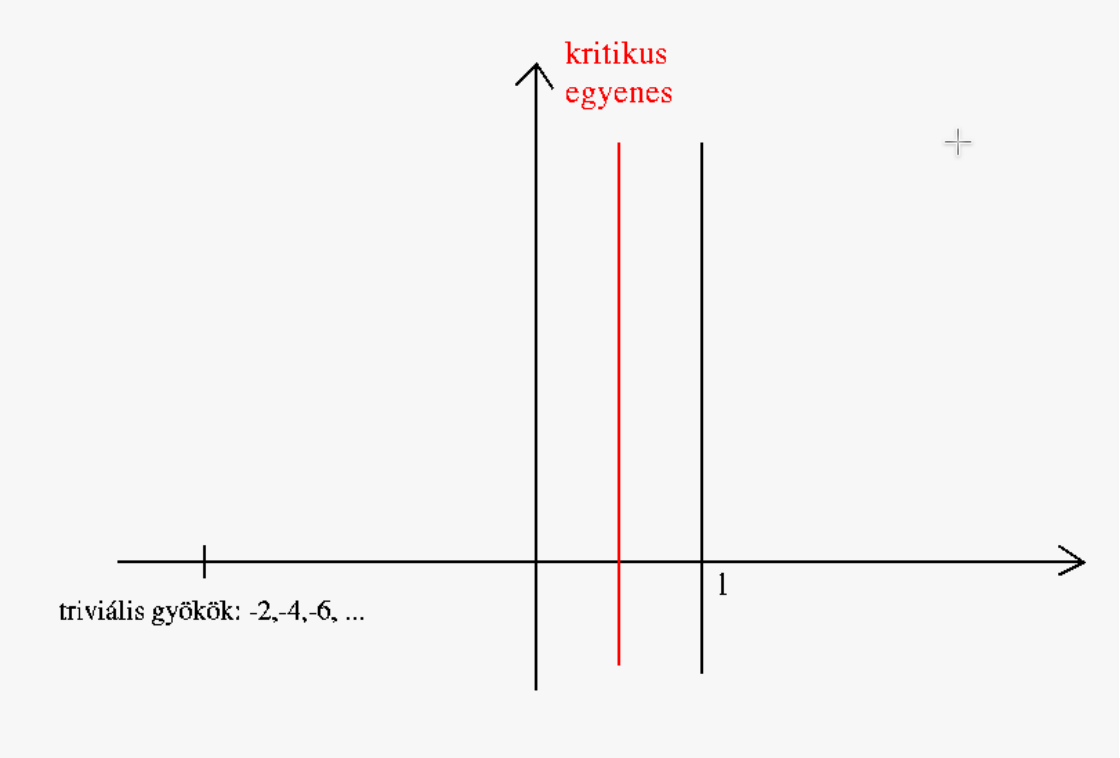
ahol

$$\Gamma(s) = \int_0^\infty x^{s-1}\, e^{-x}\, \mathrm{d}x$$

a gamma függvény.

A híres Riemann sejtés azt mondja ki, hogy a $\zeta(x)$ függvény nem triviális gyökei az $x = \frac{1}{2}$ egyenesen vannak.

Szokás a $0 \leq x \leq 1$ sávot kritikus sávnak hívni (ebben keressük a nem triviális gyököket), az $x = \frac{1}{2}$ egyenest kritikus egyenesnek hívni. Azt tudjuk, hogy a kritikus sávon kívül a ζ függvény gyökei a negatív páros számok, és egy egyszeres pólusa van 1-ben, más pólusa pedig nincs.



Sok Riemann sejtéssel ekvivalens állítás létezik, és sok állítás következik belőle. Például, Schoenfeld [5] igazolta, hogyha igaz a Riemann sejtés, akkor

$$\Delta(x) = |\pi(x) - \mathrm{Li}(x)| < \frac{1}{8\pi}\sqrt{x}\log(x), \qquad \text{ha } x \geq 2657.$$

Prímszámelméleti vizsgálódásainkkal, akkor jutunk igazán előbbre, ha ezt a kiterjesztett $\zeta(s)$ komplex függvényt vizsgáljuk, a komplex függvénytan eszközeivel. Ez az analitikus számelmélet és komplex függvénytan kapcsolata.

Hivatkozások

[1] H. M. Edwards, *Riemann's zeta function*, Academic Press, New York, 1974.

[2] 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.

[3] 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.

[4] 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.

[5] L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\Psi(x)$ II*, Mathematics of Computation, 30 (134) (1976), 337-360.

[6] Kép, Jacques Salomon Hadamard, Wikipédia, link.

[7] Kép, Charles-Jean de La Vallée Poussin, Wikipédia, link.

[8] Kép, Georg Friedrich Bernhard Riemann, Wikipédia, link.

2. Dirichlet tétele

Továbbiakban Prímszámok eloszlásával kapcsolatos kérdésekkel foglalkozunk.

Első kérdéskör: olyan tételek keresése, hogy bizonyos speciális alakú természetes számok közt végtelen sok prím létezik. (Pl. ilyenek a híres Fermat-prímek: azaz a $2^{2^n}+1$ alakú prímszámok.)

Ezek közül talán leghíresebb Dirichlet tétele, mely a következőt mondja ki:

2.1 TÉTEL. *Amennyiben az a és b egész számok, és $(a,b)=1$, akkor az*

$$a, a+b, a+2b, \ldots$$

számtani sorozat végtelen sok prímet tartalmaz.

Dirichlet nem csak a fenti tételről nevezetes, hanem arról is, hogy alig húszévesen, ő volt az első, aki be tudta bizonyítani a Fermat-sejtést az $n=5$ kitevőre. Ez volt az első jelentős előrelépés, miután Fermat bizonyította az $n=4$ esetet és Euler az $n=3$-at.

Az eredmény azonnali hírnevet hozott Dirichlet-nek, aki addig gondokkal küszködött. No nem a a matematikával, hanem, hogy

az akkori kor elvárásaival ellentétben, képtelen volt megtanulni folyékonyan beszélni latinul.

De térjünk vissza a 2.1 Tételre. A bizonyítás nagyon mély, messze túl megy a jelen jegyzet keretein, viszont van néhány speciális eset, amelyeknek bizonyítása még elemileg is elérhető. Ezek közül a legegyszerűbb a következő:

2.2 Tétel. *∞ sok $4k-1$ alakú prímszám létezik.*

A tétel a következő nagyon egyszerű lemmán alapul.

2.3 Lemma. *Egy $n = 4k-1$ alakú természetes számnak mindig van $4\ell-1$ alakú prímosztója.*

(Pl. $n = 15$ szám $4k-1$ alakú, és ennek $3 \mid 15$ egy $4k-1$ alakú prímosztója.)

A 2.3 Lemma bizonyítása. A számelmélet alaptétele szerint n felírható prímszámok szorzataként:

$$n = 4k-1 = p_1 p_2 \dots p_r,$$

(ahol p_i-k közt lehetnek azonosak); itt $\forall\ p_i$ páratlan, tehát $4\ell-1$ vagy $4\ell+1$ alakú.

Elég: nem lehet mindegyik p_i prím $4\ell+1$ alakú.

Tudjuk $4\ell+1$ alakú számok szorzata is ilyen alakú, hiszen:

$$(4\ell+1)(4m+1) = 4(4\ell m + \ell + m) + 1 = 4t+1.$$

Vagyis, ha minden p_i prím $4\ell+1$ alakú, akkor a szorzatuk n is. Ezzel ellentmondásra jutottunk, és a lemmát beláttuk.

A 2.2 Tétel bizonyítása. Tegyük fel, hogy csak véges sok $4k-1$ alakú prím létezik, legyenek ezek $p_1 = 3$, $p_2 = 7, \dots, p_r$.

Tekintsük az

$$A \stackrel{\text{def}}{=} 4p_1p_2\dots p_r - 1$$

számot. A lemma szerint ennek létezik egy $q = 4\ell - 1$ alakú prímosztója:

$$q = 4\ell - 1 \mid A.$$

Ez a q különbözik $p_1, p_2, \dots, p_r$-től, hiszen a fenti prímek nem osztói A-nak: A ezekkel osztva -1 maradékot ad.

Így találtunk egy újabb, $p_1, \dots, p_r$-től különböző $4k - 1$ alakú prímet, pedig felsoroltuk az összeset. ↯ □

Mivel 2-t kivéve minden prím páratlan, és így vagy $4k - 1$, vagy $4k + 1$ alakú, azt várnánk, hogy mint ahogy végtelen sok $4k - 1$ alakú prím létezik, ugyanúgy végtelen sok van $4k + 1$ alakúakból is.

(Sőt belátható, hogy még a számuk is közel van).

Ez tényleg így van, de a bizonyítás kicsit nehezebb: az előbb olyan számot konstruáltunk, melynek létezik $4\ell - 1$ alakú prímosztója, most meg olyat kell, melynek létezik $4\ell + 1$ alakú prímosztója, és ez utóbbi nehezebb.

2.4 Tétel. *Végtelen sok $4k + 1$ alakú prím létezik.*

A 2.4 Tétel bizonyítása. Ezúttal a következő lemmát használjuk:

2.5 Lemma. *Ha $n \in \mathbb{N}$ és p pozitív prím, melyekre $p \mid 4n^2 + 1$, akkor p is $4\ell + 1$ alakú.*

A 2.5 Lemma bizonyítása. Mivel $4n^2 + 1$ páratlan és $p \mid 4n^2 + 1$ $\Rightarrow p \neq 2$.

A $p \mid 4n^2+1$ feltételt kongruencia alakban írva:

$$\begin{aligned} 4n^2+1 &\equiv 0 \qquad (p), \\ (2n)^2 &\equiv -1 \qquad (p). \end{aligned}$$

Tehát $x = 2n$ megoldása az

$$x^2 \equiv -1 \qquad (p)$$

kongruenciának, és így -1 kvadratikus maradék $\mod p$.

Ezért a $\left(\frac{-1}{p}\right)$ Legendre szimbólumra $\left(\frac{-1}{p}\right) = +1$, vagyis $p = 4\ell+1$ alakú prím. Ezzel a lemmát beláttuk.

A következőkben rátérünk a tétel bizonyítására.

Tegyük fel, hogy csak véges sok $4k+1$ alakú prím létezik, legyenek ezek $p_1 = 5$, $p_2 = 13, \ldots, p_r$.

Tekintsük az

$$A \stackrel{\text{def}}{=} 4(p_1 p_2 \ldots p_r)^2 + 1$$

számot.

A számelmélet alaptétele szerint felírható prímek szorzataként. Legyen A egy prímosztója q: $q \mid A$.

A lemma szerint q egy $4\ell+1$ alakú prím $q = 4\ell+1 \mid A$.

Ez a q különbözik $p_1, p_2, \ldots, p_r$-től, hiszen ezek nem osztói A-nak: A ezekkel osztva $+1$ maradékot ad.

Így találtunk egy újabb, $p_1, p_2, \ldots, p_r$-től különböző $4\ell+1$ alakú prímet (q-t), pedig az összeset felsoroltuk. ↯ □

Hasonlóan lehetne igazolni, hogy létezik végtelen sok $6k-1$, ill. végtelen sok $6k+1$ alakú prím. (HF)

Ezután egy kicsit még tovább megyünk, a következő általánosítással (ld. még [2],[3] és [4]):

2.6 TÉTEL. (Dirichlet speciális esete) *Legyen $a \in \mathbb{N}$. Ekkor végtelen sok $ak+1$ alakú pozitív prím létezik.*

A 2.6 Tétel bizonyítása. A bizonyításban körosztási polinomok szerepelnek, amelyeknek néhány alaptulajdonságát fogjuk használni, pl., hogy ezek mindig egész együtthatós polinomok.

Ezúttal a következő lemmára lesz szükségünk:

2.7 LEMMA. *Ha $m \in \mathbb{N}$, $x \in \mathbb{Z}$, p pozitív prím, amelyre $p \mid \Phi_m(x)$, ahol Φ_m az m-edik körosztási polinom, akkor*

$$p \equiv 1 \pmod{m},$$

vagy

$$p \mid m.$$

Mielőtt a lemmát bebizonyítanánk, lássuk, hogy következik a lemmából a tétel.

Egy a tétellel ekvivalens állítást igazolunk, nevezetesen minden m modulusra végtelen sok pozitív prím létezik, amely $\equiv 1 \pmod{m}$.

Indirekten bizonyítunk.

Tegyük fel, hogy véges sok ilyen prím van, ezek:

$$p_1, p_2, \ldots, p_n \equiv 1 \pmod{m}.$$

Tekintsük a

$$\Phi_m(mp_1p_2\ldots p_n)$$

egész számot és annak egy q prímosztóját

$$q \mid \Phi_m(mp_1p_2\dots p_n).$$

Az m-edik körosztási polinom konstans tagja ± 1, mivel

$$\Phi_m(x) = \prod_{\substack{\varepsilon \text{ primitív} \\ m\text{-edik egységgyök}}} (x-\varepsilon),$$

ahol a konstans tag az egységgyökök szorzata, vagyis abszolútértéke 1. Azt is tudjuk, hogy a konstans tag egész szám, így csak ± 1 lehet.

Tehát

$$\Phi_m(x) = a_s x^s + a_{s-1}x^{s-1} + \dots + a_1 x \pm 1.$$

Vagyis:

$$\Phi_m(mp_1\cdots p_n) = a_s(mp_1\cdots p_n)^s + \dots + a_1(mp_1\cdots p_n) \pm 1,$$

amiből adódóan $mp_1\cdots p_n$ és $\Phi_m(mp_1\cdots p_n)$ relatív prím, hisz a legnagyobb közös osztójuk, osztója

$$\Phi_m(mp_1\cdots p_n) - a_s(mp_1\cdots p_n)^s - \dots - a_1(mp_1\cdots p_n) = \pm 1\text{-nek.}$$

Azaz $(\Phi_m(mp_1\cdots p_n), mp_1\cdots p_n)$, de tudjuk, hogy $q \mid \Phi_m(mp_1\cdots p_n)$, vagyis $(q, mp_1\cdots p_n) = 1$.

Azaz q különbözik $p_1, p_2, \dots, p_n$ prímektől, és nem osztója m-nek sem.

Így a lemma szerint $q \equiv 1 \pmod m$, és új prím, nem egyezik az eddig felsoroltakkal. ϟ.

Tehát a tétel igazolásához már csak a lemmát kell belátni.

A 2.7 Lemma bizonyítása. Ismert, hogy $\Phi_m(x) \mid x^m - 1$, hiszen

$$\Phi_m(x) = \prod_{\substack{\varepsilon \text{ primitív} \\ m\text{-edik egységgyök}}} (x - \varepsilon) \;\Big|\; \prod_{\substack{\varepsilon \\ m\text{-edik egységgyök}}} (x - \varepsilon) = x^m - 1.$$

A lemma feltételei szerint $p \mid \Phi_m(x)$, azaz $p \mid x^m - 1$, vagyis

$$x^m \equiv 1 \quad (p). \tag{2.1}$$

Jelölje x rendjét r modulo p. A rendről tanultak alapján:

$$x^t \equiv 1 \quad (p) \Leftrightarrow r \mid t. \tag{2.2}$$

(Ez azért van így, mert az $1, x^2, x^3, \ldots \mod p$ sorozat periodikus, és a legkisebb periódusa r.)

Így (2.1) és (2.2) alapján:

$$r \mid m.$$

Most $x^m \equiv 1 \quad (p)$, tehát $(x, p) = 1$. Azaz a kis-Fermat tétel miatt:

$$x^{q-1} \equiv 1 \quad (q).$$

Vagyis (2.2) miatt $r \mid p - 1$.

Összefoglalva $r \mid m$ és $r \mid p - 1$.

Amennyiben $r = m$, akkor $m \mid p - 1$, azaz $p \equiv 1 \quad (m)$, és ezzel a lemma állítását ebben az esetben beláttuk.

A következőkben azt bizonyítjuk, hogy ha $r < m$, akkor $p \mid m$. Ha ez sikerül, akkor a lemma állítását teljes egészében igazoltuk.

Tegyük fel, hogy $r < m$. Tudjuk $r \mid m$. Ekkor $\dfrac{x^m - 1}{x^r - 1}$ egész együtthatós polinom, hiszen

$$\begin{aligned} x^m - 1 &= (x^r)^{m/r} - 1^{m/r} \\ &= (x^r - 1)\left((x^r)^{m/r-1} + (x^r)^{m/r-2} + \cdots + x^r + 1\right). \end{aligned}$$

Sőt,

$$\begin{aligned} \frac{x^m - 1}{x^r - 1} &= (x^r)^{m/r-1} + (x^r)^{m/r-2} + \ldots + x^r + 1 \\ &\equiv 1 + \quad 1 + \ldots + 1 + 1 \\ &= \frac{m}{r} \pmod{p}, \end{aligned}$$

hiszen x rendje r, azaz $x^r \equiv 1 \quad (p)$.

Másrészt

$$\Phi_m(x) \;\Big|\; \frac{x^m - 1}{x^r - 1}, \tag{2.3}$$

mert $r < m$ esetén

$$\prod_{\substack{\varepsilon \text{ primitív} \\ m \text{ egységgyök}}} (x - \varepsilon) \;\Big|\; \prod_{\substack{\varepsilon \ m\text{-edik egységgyök, de} \\ \text{nem } r\text{-edik egységgyök}}} (x - \varepsilon).$$

A tétel feltételei szerint $p \mid \Phi_m(x)$, így (2.3) miatt $p \mid \dfrac{x^m - 1}{x^r - 1}$. Azaz

$$0 \equiv \frac{x^m - 1}{x^r - 1} \equiv \frac{m}{r} \quad (p).$$

Amiből $p \mid \dfrac{m}{r} \Rightarrow p \mid m$.

Ezzel a lemma állítását teljes egészében igazoltuk.

A fejezet végén megemlítjük még a modern számelmélet egyik legfontosabb prímekkel kapcsolatos eredményét is (bizonyítás nélkül), mely Ben Greentől és Terence Taotól [1] származik:

2.8 TÉTEL. (Green - Tao) *A prímszámok között van tetszőlegesen hosszú számtani sorozat.*

Hivatkozások

[1] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics, 167 (2) (2008), 481–547, link.

[2] Keith Kearnes, Kiss Emil, Szendrei Ágnes, *Gauss-egészek és Dirichlet tétele I.*, KöMaL, 2010/március, 136-141, link.

[3] M. R. Murty,*Primes in certain arithmetic progressions*, J. Madras Univ. (1988), 161–169.

[4] I. Schur, *Über die existenz unendlich vieler primzahlen in einiger speziellen arithmetischen progressionen*, Sitzungber. Berliner Math. Ges. 11 (1912), 40—50.

[5] Kép, P. G. L. Dirichlet, link.

[6] Kép, B. Green, link.

[7] Kép, T. Tao, link.

3. Ikerprímek, prímdifferenciák

A számelmélet egyik leghíresebb sejtése Christian Goldbach-tól származik, aki egy Euler-hoz írt levelében a következőt fogalmazta meg:

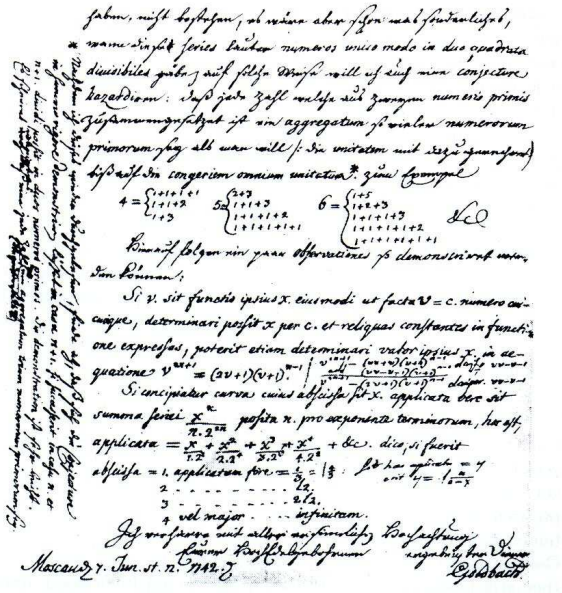
3.1 SEJTÉS. (Goldbach-sejtés) (I.) *Minden 2-nél nagyobb páros szám előáll két prímszám összegeként.*

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

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

Valóban, ha n páros, akkor az erős Goldbach sejtés azt állítja, hogy n két prím összege. Ha n páratlan, akkor $n-3$ páros szám, így $n-3$ két prím összege, és ekkor n három prím összege.

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. Goldbach-nak Eulerhez írt levele az alábbi is:



A Goldbach-sejtésről és kapcsolódó részeredményekről bővebben a kapcsolódó Wikipédia oldalon [13] is olvashatunk.

Most pusztán annyit említünk meg, hogy a gyenge sejtést Vinogradov [11] bizonyította elegendően nagy prímekre, és később Helfgott [4], [5] minden 4-nél nagyobb számra, de ez utóbbi eredmények még lektorálás alatt vannak.

Az erősebb Goldbach sejtés bizonyítása még mindig reménytelen. De vannak a sejtésnek kissé gyengített változatai, amelyeket azért sikerült igazolni. Pl. ha az egyik prím helyett megengedünk olyan összetett számokat is, amelyeknek legfeljebb r prímosztója van. Egy ilyen összetett számot jelöljünk P_r-rel. Pár idevonatkozó eredmény szerint minden páros szám:

Brun [1] (1920): $P_9 + P_9$ alakú,
Selberg [10] (1943): $P_2 + P_3$ alakú,
Rényi [9] (1948): ($\exists$ rögzített $K > 0$), hogy $P_1 + P_K$ alakú,
J. R. Chen [2] (1973): $P_1 + P_2$ alakú.

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 Daniel A. Goldstone, Pintz János és Cem Y. Yıldırım [6] 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 [12] 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 [7], [8] 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.

Egy egyszerű becslés a másik irányból:

3.2 Tétel. *Tetszőlegesen nagy $K \in \mathbb{N}$ számot megadva létezik olyan n szám, hogy*

$$d_n = p_{n+1} - p_n \geq K.$$

A 3.2 Tétel bizonyítása. Le lehetne vezetni a $\frac{\pi(x)}{x} \to \infty$ ($x \to \infty$ esetén)-ből is. Ehelyett egy egyszerű direkt bizonyítás:

Tekintsük a $K!+2, K!+3, \ldots, K!+K$ számokat. Ezek mindegyike összetett, hiszen $2 \leq i \leq K$ esetén $i \mid K!+i$ és i valódi osztó. Így n-et

$$p_n \leq K! + K \leq p_{n+1}$$

képlettel definiálva

$$p_{n+1} \geq K! + K + 1$$
$$p_n \leq K! + 1.$$

Azaz $d_n = p_{n+1} - p_n \geq K! + K + 1 - (K! + 1) = K$.

Persze ismert a fentinél élesebb becslés is, csak a bizonyítás jóval bonyolultabb. A legmodernebb eredmény Ford–Green–Konyagin–Maynard–Tao-tól [3] származik

$$d_n \gg \frac{\log n \log\log n \log\log\log\log n}{\log\log\log n}$$

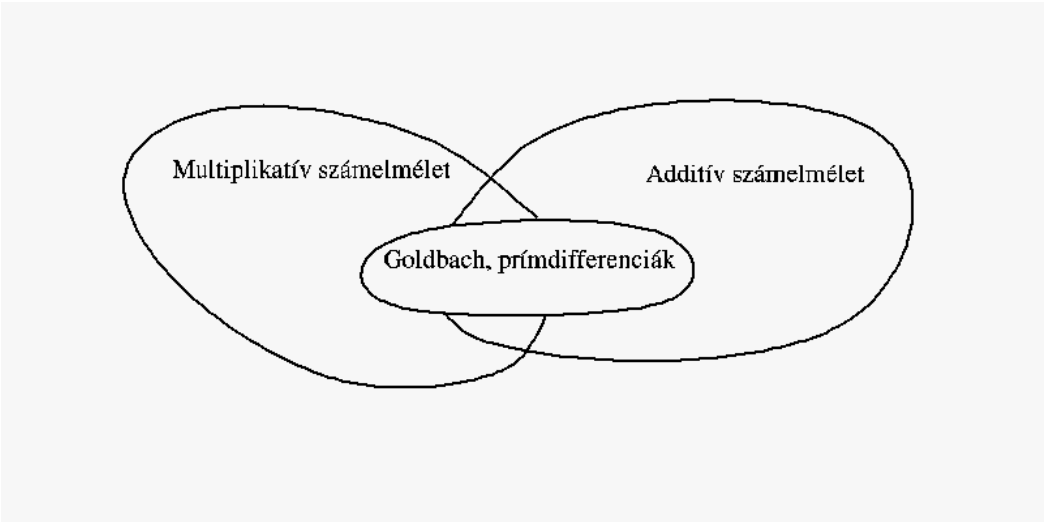
n végtelen sok értékére.

Tehát vannak a prímszámok között „nagy” hézagok. Ehhez kapcsolódó régi sejtés: a prímek között nem lehetnek nagyobb hézagok, mint a négyzetszámok között:

3.3 Sejtés. *n^2 és $(n+1)^2$ között mindig van prímszám.*

Reménytelen! (Még a Riemann-sejtésből is csak picivel gyengébb állítás következne.)

Témákat tekintve, eddig prímszámelméletet vettünk. Az 1. fejezetbeli ábrával szemléltetve:



De szó volt analitikus számelméletről is (1. fejezet). A 21 fejezetben visszatérünk még a prímszámelméletre kicsit. Többet azonban a fenti témákból nem veszünk; azok azonban egy-egy kurzus erejéig az egyetemi MSc matematikus programokban is szerepelnek.

Hivatkozások

[1] V. Brun, *Le crible d'Eratosthéne et le théorème de Goldbach* Videnselsk. Skr.1, Nr.3 (1920).

[2] J. R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica. 16 (1973), 157–176.

[3] K. Ford, B. Green, S. Konyagin, J. Maynard, T. Tao, *Long gaps between primes*, J. Amer. Math. Soc. 31 (1) (2018), 65–105.

[4] H. A. Helfgott, *Major arcs for Goldbach's theorem*. arXiv:1305.2897 [math.NT] (2013).

[5] H. A. Helfgott, *Minor arcs for Goldbach's problem*. arXiv:1205.5252 [math.NT] (2012).

[6] D. A. Goldstone, J. Pintz, C. Y. Yıldırım, *Primes in tuples. II*, Acta Math. 204 (1) (2010), 1–47.

[7] Polymath, D. H. J., *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. 1 (2014), Art. 12, 83 pp.

[8] 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.

[9] A. A. Rényi, *On the representation of an even number as the sum of a prime and an almost prime*, Izvestiya Akademii Nauk SSSR Seriya Matematicheskaya (in Russian) 12 (1948) 57–78.

[10] A. Selberg, *On the normal density of primes in small intervals and the difference between consecutive primes*, Arch. Math. Naturvid. 47, no. 6 (1943), 87–105.

[11] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, 1954, Translated, átdolgozta és jegyzetekkel ellátta K. F. Roth és Anne Davenport.

[12] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. (2) 179 (2014), 1121–1174.

[13] Wikipédia, Goldbach's conjecture, link

[14] Kép, Christian Goldbach, link.

[15] Kép, *Letter from Goldbach to Euler*, link.

4. Sidon sorozatok, kombinatorikus számelmélet

Még hallgatóként, Sidon Simon, 1932-ben egy kérdést tett fel Erdősnek. A kérdés Simon és Erdős témavezetőjének, Fejérnek (aki maga is rendkívül kreatív volt) egy végtelen sorozatok összegezésbeli vizsgálataihoz kapcsolódott.

Sidon bizonyos Fourier sorok L_p-beli normájának vizsgálatakor fogalmazta meg kérdését elemzésekor fogalmazta meg kérdését. A probléma modern megfogalmazása a következő:

A számelméletben Sidon sorozat (vagy Sidon halmaz) egy természetes számokból álló sorozat $\mathcal{A} = \{a_0, a_1, a_2, \dots\}$ sorozat, ha az összes $a_i + a_j$ összeg különböző, ahol $i \leq j$.

Feladat. Mutassunk példákat Sidon sorozatokra

Például a kettőhatványok.

4.1 Definíció. *Jelölje $S(N)$ azon Sidon halmazok maximális elemszámát, melynek elemei az $\{1, 2, 3, \dots, N\}$ halmazból valóak:*

$$S(N) = \max_{\substack{\mathcal{A} \subseteq \{1,2,\dots,N\} \\ \mathcal{A} \text{ Sidon}}} |\mathcal{A}| \tag{4.1}$$

Erdős azonnal észrevette, hogy a mohó algoritmussal bebizonyítható, hogy $S(N) > 2N^{1/3}$. Ezt az eredményt röviden bebizonyítjuk, de előbb lássunk néhány felső becslést.

A legegyszerűbb felső becslés a következő:

4.2 TÉTEL.

$$S(N) \leq 2\sqrt{N}.$$

A 4.2 Tétel bizonyítása. Tekintsünk egy

$$\mathcal{A} = \{a_1, a_2, \ldots, a_S\} \subseteq \{1, 2, \ldots, N\}.$$

Sidon sorozatot. Bebizonyítjuk, hogy

$$S = |\mathcal{A}| \leq 2\sqrt{N}.$$

Ehhez tekintsük a számegyenest, és rajta az $1, 2, \ldots, 2N$ számokat.

Tegyünk egy X-et azon egész számokra, amelyek felírhatóak $a + a'$ alakban, ahol $a, a' \in \mathcal{A}$. Ekkor az X-ek száma:

$$\binom{S}{2} + S \longleftarrow a_i = a_j,$$
$$\uparrow$$
$$(a_i, a_j) \quad a_i \neq a_j.$$

Tudjuk, hogy minden összeg különböző és

$$2 \leq a + a' \leq 2N.$$

Így

$$\binom{S}{2} + S \leq 2N,$$
$$\frac{S(S+1)}{2} \leq 2N,$$
$$S^2 < S(S+1) \leq 4N,$$

$$S < 2\sqrt{N},$$

ami bizonyítja a tételt.

Ez az eredmény kicsit javítható, ha összeg helyett különbségeket veszünk.

$$\begin{gathered} a_0 + {a_0}' = a_1 + {a_1}' \\ \Updownarrow \\ a_0 - a_1 = {a_1}' - {a_0}' \end{gathered}$$

Így az $\mathcal{A}$ halmaz akkor Sidon halmaz, ha minden $a - a'$ különbség (ahol $a, a' \in \mathcal{A}$, $a \neq a'$) különböző.

Tekintsük megint a számegyenest, és ezúttal rajta az $1, 2, \ldots, N-1$ egész számokat.

Tegyünk egy X-et azon egész számokra, amelyek felírhatóak $a - a'$ alakban, ahol $a, a' \in \mathcal{A}$ és $a - a'$ pozitív.

Ekkor az X-ek száma $\binom{S}{2}$.

Minden $a - a'$ különbség különböző és

$$1 \leq a - a' \leq N - 1,$$

így

$$\begin{aligned} \binom{S}{2} &\leq N - 1, \\ S(S-1) &\leq 2N - 2, \\ S^2 - S + \frac{1}{4} &\leq 2N - \frac{7}{4}, \end{aligned}$$

$$\left(S-\frac{1}{2}\right)^2 \leq 2N-\frac{7}{4},$$
$$S-\frac{1}{2} \leq \sqrt{2N-\frac{7}{4}} < \sqrt{2}\sqrt{N},$$
$$S < \sqrt{2}\cdot\sqrt{N}+\frac{1}{2}.$$

Még cselesebb ötletekkel a tételben szereplő $\sqrt{2}$ szorzótól is megszabadulhatunk. A következő trükkös bizonyítás Erdőstől és Turántól [5] származik.

4.3 TÉTEL.

$$S(N) < \sqrt{N}+\sqrt[4]{N}+1.$$

A következő bizonyítás Erdős és Surányi könyvéből, Válogatott Fejezetek a Számelméletből [4] való.

A 4.3 Tétel bizonyítása.

A t természetes szám értékét később rögzítjük.

A $[0,N]$ intervallumot részintervallumokra osztjuk. Tekintsük a következő $N+t$ darab intervallumot:

$$[-t+1,0],[-t+2,1],\ldots,[N,N+t-1].$$

Legyen $\mathcal{A}\subseteq\{1,2,\ldots,N\}$ egy Sidon halmaz. Az $\mathcal{A}$ halmaz elemei közül rendre

$$A_1, \quad A_2, \quad \ldots \quad A_{N+t}$$

darab esik a fenti intervallumokba.

Az intervallumok között átfedés is van, és könnyű látni, hogy $\mathcal{A}$ minden eleme t darab egymást követő intervallumban szerepel. Így

$$\sum_{i=1}^{N+t} A_i = ts.$$

A következőkben azt számoljuk ki, hogy egy (a_i, a_j) pár ($i > j$ esetén) összesen hány darab intervallumba esik bele.

Legyen ezek összesített száma D.

Egyrészről világos hogy

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \frac{1}{2} \sum_{i=1}^{n+t} A_i^2 - \frac{1}{2} \sum_{i=1}^{n+t} A_i.$$

Másrészt, ha egy számpár különbsége d, akkor az pont $t - d$ darab intervallumba esik bele.

Mivel minden különbség legfeljebb egyszer szerepel, minden d differenciához maximum egy számpár tartozik, amelyek különbsége d. Ez a számpár összesen $t - d$ intervallumba esik bele, így

$$D \leq \sum_{d=1}^{t-1} (t - d) = \frac{t(t-1)}{2}.$$

A D-re vonatkozó két becslést összevetve adódik, hogy

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \leq t(t-1).$$

Láttuk, hogy a második szumma összege éppen ts.

A számtani-négyzetes közép közti egyenlőtlenséget alkalmazva kapjuk, hogy:

$$\sum_{i=1}^{n+t} A_i^2 \geq \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{n+t} = \frac{t^2 s^2}{n+t}.$$

Ezeket a becsléseket az egyenlőtlenségbe írva, majd rendezve, és végül $(n+t)/t^2$-tel szorozva kapjuk, hogy

$$s^2 - s\left(\frac{n}{t} + 1\right) - \left(\frac{n}{t} + 1\right)(t-1) \leq 0.$$

A másodfokú egyenlőtlenséget s-re megoldva adódik, hogy

$$s \leq \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}}$$
$$= \frac{n}{2t} + \frac{1}{2} + \sqrt{n + t + \left(\frac{n}{2t} - \frac{1}{2}\right)^2 - 1}.$$

Ezután (hogy minél élesebb becslést kapjunk) rögzítsük $t = \left[\sqrt[4]{n^3}\right] + 1$-nek. Ekkor a becslésben az első tag nem nagyobb mint $\frac{1}{2}\sqrt[4]{n}$, míg az utolsó tag kisebb mint $\sqrt{n} + \frac{1}{2}\sqrt[4]{n} + \frac{1}{2}$.

Ezzel a kívánt egyenlőtlenséget bebizonyítottuk.

Balogh, Füredi és Roy [2] kicsit javított az eredményen, de csak 0.2%-kal:

$$S(N) \leq \sqrt{N} + 0.998N^{1/4}.$$

A következőkben alsó becsléseket adunk $S(N)$-re.

Először Erdős alsó becslését igazoljuk, mely a mohó algoritmusra épült.

4.4 Tétel. *Minden N-re létezik egy $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ Sidon halmaz, melyre $|\mathcal{A}| \geq [(2N)^{1/3}]$.*

A 4.4 Tétel bizonyítása. Elegendő a következőt megmutatni: ha

$$\{a_1, a_2, \ldots, a_t\} \subseteq \{1, 2, \ldots, N\}$$

egy Sidon halmaz, melynek elemszáma t, ahol $t \leq 2N^{1/3} - 1$, akkor létezik egy b egész szám, amelyre

$$1 \leq b \leq N \quad \text{és} \quad b \notin \{a_1, a_2, \ldots, a_t\}, \tag{4.2}$$

továbbá

$$\{a_1, a_2, \ldots, a_t\} \cup \{b\}$$

Sidon halmaz. Egy b számot „rossznak” hívunk, ha $\{a_1, a_2, \dots, a_t\} \cup \{b\}$ nem Sidon halmaz, és „jónak” hívunk, ha $\{a_1, a_2, \dots, a_t\} \cup \{b\}$ Sidon halmaz.

A bizonyítás befejezéséhez elegendő annyit belátni, hogy ha $t \leq N^{1/3} - 1$ fennáll, akkor létezik jó b elem, s amelyre (4.2) is teljesül.

Először számoljuk össze a rossz b-k darabszámát. Mivel $\{a_1, a_2, \dots, a_t\}$ Sidon halmaz, ha b rossz (azaz $\{a_1, a_2, \dots, a_t\} \cup \{b\}$ nem Sidon halmaz), akkor létezik a_i, a_j, a_k elemek, melyekre

$$a_i + a_j = a_k + b \tag{4.3}$$

vagy létezik a_u, a_v, melyekre

$$a_u + a_v = b + b. \tag{4.4}$$

Így azon rossz b-k száma, amelyekre (4.3) fennáll

$$\leq \left(\binom{t}{2} + t\right)(t-1) = \frac{t(t^2-1)}{2}.$$

Míg azon rossz b-k száma, amelyekre (4.4) fennáll

$$\leq \binom{t}{2} = \frac{t(t-1)}{2}.$$

Így a rossz b-k összesített száma $\leq \frac{t(t^2-1)}{2} + \frac{t(t-1)}{2} = \frac{t(t-1)(t+3)}{2}$. Végül azon b-k száma, melyre $b \in \{a_1, a_2, \dots, a_t\}$ teljesül t. Ha

$$\frac{t(t-1)(t+3)}{2} + t < N,$$

akkor létezik jó b, melyre (4.2) fennáll. Amennyiben $t \leq (2N)^{1/3} - 1$ ez nyilvánvalóan teljesül:

$$\frac{t(t-1)(t+3)}{2} + t < \frac{(t+1)^3}{2} \leq N,$$

amivel az állítást igazoltuk.

A következőkben mutatunk néhány trükkös konstrukciót Sidon sorozatokra.

Először Erdős és Turán [5] egy konstrukciójának kissé módosított változatát ismertetjük.

4.5 Tétel. *Létezik $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ Sidon halmaz, melyre*

$$|\mathcal{A}| \geq \frac{\sqrt{N}}{4}.$$

A 4.5 Tétel bizonyítása. Tegyük fel, hogy $N \geq 16$.

Csebisev tétele szerint minden $n \geq 2$ esetén létezik prímszám n és $2n$ között. (Erről a tételről bővebben olvashatunk a kapcsolódó Wikipédia oldalon: link. A tételre Erdős Pál is adott egy elemi bizonyítást, ld. pl. itt link.)

Csebisev tételét alkalmazva megkapjuk, hogy létezik p prímszám, amelyre

$$\frac{\sqrt{N}}{2} < p < \sqrt{N}.$$

Mivel $N \geq 16$, ez a prímszám páratlan. Jelölje $r_p(x)$ az x egész szám legkisebb nemnegatív maradékát modulo p. Azaz

$$x \equiv r_p(x) \pmod{p} \quad \text{és } 0 \leq r_p(x) \leq p-1.$$

Definiáljuk az $\mathcal{A}$ halmazt az

$$\mathcal{A} \stackrel{\text{def}}{=} \{a : \ a = x + p r_p(x^2),\ 0 \leq x \leq \frac{p-1}{2}\}$$

képlettel. Bebizonyítjuk, hogy ez a halmaz Sidon halmaz.

Világos, hogy $\mathcal{A}$ tartalmaz $\frac{p+1}{2}$ darab különböző elemet, mivel különböző x-ekre az $x + pr_p(x^2)$-nek más-más maradéka van modulo p.

Ezután bebizonyítjuk, hogy $\mathcal{A}$ Sidon halmaz. Tegyük fel, hogy

$$a_1 + a_2 = b_1 + b_2, \tag{4.5}$$

ahol $a_1, a_2, b_1, b_2 \in \mathcal{A}$. Ekkor létezik $0 \leq x_1, x_2, y_1, y_2 \leq \frac{p-1}{2}$ melyekre

$$\begin{aligned} a_1 &= x_1 + pr_p(x_1^2) \\ a_2 &= x_2 + pr_p(x_2^2) \\ b_1 &= y_1 + pr_p(y_1^2) \\ b_2 &= y_2 + pr_p(y_2^2). \end{aligned}$$

Ekkor (4.5) alapján

$$x_1 + x_2 + p\left(r_p(x_1^2) + r_p(x_2^2)\right) = y_1 + y_2 + p\left(r_p(y_1^2) + r_p(y_2^2)\right). \tag{4.6}$$

Így

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{p}.$$

Mivel $0 \leq x_1 + x_2, y_1 + y_2 \leq p - 1$, tudjuk, hogy

$$x_1 + x_2 = y_1 + y_2. \tag{4.7}$$

Ekkor (4.6) és (4.7) miatt

$$\begin{aligned} r_p(x_1^2) + r_p(x_2^2) &= r_p(y_1^2) + r_p(y_2^2) \\ x_1^2 + x_2^2 &\equiv y_1^2 + y_2^2 \pmod{p}. \end{aligned} \tag{4.8}$$

Ekkor (4.7)-t Négyzetreemlve, és abból (4.8)-t kivonva kapjuk, hogy

$$2x_1x_2 \equiv 2y_1y_2 \pmod{p}$$

$$x_1 x_2 \equiv y_1 y_2 \pmod{p} \tag{4.9}$$

A gyökök és együtthatók közötti összefüggés alapján, (4.7)-ből és (4.9)-ből adódóan kapjuk, hogy x_1, x_2 és y_1, y_2 ugyanannak a másodfokú egyenletnek a gyökei.

A fokszám tétel miatt minden másodfokú kongruenciának legfeljebb két gyöke van, így

$$\{x_1, x_2\} = \{y_1, y_2\},$$

azaz

$$\{a_1, a_2\} = \{b_1, b_2\}.$$

Tehát $\mathcal{A}$ olyan Sidon halmaz, melyre $|\mathcal{A}| \geq \frac{\sqrt{N}}{4}$, és ezzel a bizonyítást befejeztük.

A következő trükkös bizonyítás Ruzsától származik [3], aki eltüntette az $\frac{1}{4}$-es szorzót az előző tételben. Először a következőt igazoljuk:

4.6 Tétel. *Legyen p egy páratlan prímszám. Ekkor létezik $p-1$ darab a_i egész szám, amelyre az $a_i - a_j$ különbségek (ahol $i \neq j$) inkongruensek modulo $p^2 - p$.*

A 4.6 Tétel bizonyítása. Legyen g egy primitív gyök modulo p, és legyenek a_i-k a modulo $p^2 - p$ egyértelműen meghatározott megoldásai a

$$x \equiv i \pmod{p-1},$$
$$x \equiv g^i \pmod{p}.$$

szimultán kongruencia-rendszernek (a kínai maradéktétel miatt tudjuk, hogy ilyen megoldás létezik és egyértelmű). Azt kell megmutatnunk, hogy az

$$a_i - a_j \equiv a_r - a_s \pmod{p^2 - p},$$

kongruenciának, vagy evvel ekvivalensen az

$$a_i + a_s \equiv a_r + a_j \pmod{p^2 - p},$$

kongruenciának csak triviális megoldásai vannak. Más szóval minden c-re legfeljebb egy olyan i, j pár létezik, hogy

$$c \equiv a_i + a_j \pmod{p^2 - p}.$$

Az a_i-k definíciója alapján, ez ekvivalens a

$$c \equiv i + j \pmod{p - 1},$$
$$c \equiv g^i + g^j \pmod{p}.$$

szimultán kongruencia-rendszerrel Az első kongruencia ekvivalens a következővel:

$$g^c \equiv g^i g^j \pmod{p}.$$

Ekkor a gyökök és együtthatók közötti összefüggés szerint a g^i és g^j modulo p maradékosztályok egyértelműen meghatározottak, mivel mindketten megoldásai az

$$x^2 - cx + g^c \equiv 0 \pmod{p}.$$

másodfokú kongruenciának. A fokszám tétel miatt a másodfokú kongruenciának legfeljebb 2 gyöke van, így a gyökök valóban egyértelműen meghatározottak. Azaz i és j is egyértelműen meghatározott.

A fenti módon megkonstruált a_i-k valóban Sidon halmazt alkotnak $\mathbb{Z}_{p^2-p}$-ben. Ezzel a tétel állítását beláttuk.

Nyilvánvaló, hogy ha egy mod p^2-p Sidon halmaz elemeihez hozzárendeljük a vele kongruens legkisebb pozitív egészet, akkor Sidon halmazt kapunk $\{1,2,\dots,p^2-p\}$-ben.

Így ha történetesen N egy p^2-p alakú szám (ahol p prím), akkor

$$S(N) \geq p-1 = \frac{1}{2}(\sqrt{4N+1}+1)-1 > \sqrt{N}-1.$$

Tetszőleges N-re olyan p prímet választunk, amelyre p^2-p közel van N-hez.

Van egy híres sejtés, miszerint minden pozitív δ-ra n és $n+n^\delta$ közé esik prím, feltéve, hogy n elegendően nagy. A sejtés bizonyítása reménytelennek tűnik.

De ha az összes pozitív δ-ra nem is, de pár kicsi konkrét δ-ra azért sikerült igazolni a sejtést.

Azon δ-k értéke melyre igazolt a sejtés, egyre jobbak, egyre kisebbek. Jelenleg a legélesebb eredmény Bakertől, Harmantól és Pintztől [1] származik, nevezetesen $\delta = 0.525$.

Így tudunk p prímet választani $\sqrt{N}-N^{0.2625}$ és $\sqrt{N}$ között, és ekkor

$$S(N) \geq S(p^2-p) \geq p-1 \geq \sqrt{N}-O(N^{0.2625}).$$

Sidon sorozatokról Erdős számtalan sejtést fogalmazott meg, ezekről bővebben pl. itt olvashatunk: link. Sajnos, ma már (leg-

jobb tudomásom szerint) nem jár pénzjutalom a problémák megfejtésért...

Hivatkozások

[1] R. C. Baker, G. Harman, J. Pintz, *The difference between consecutive primes, II*, Proceedings of the London Mathematical Society. 83 (3) (2001), 532–562.

[2] J. Balogh, Z. Füredi, S. Roy, *An Upper Bound on the Size of Sidon Sets*, The American Mathematical Monthly, DOI: 10.1080/00029890.2023.2176667.

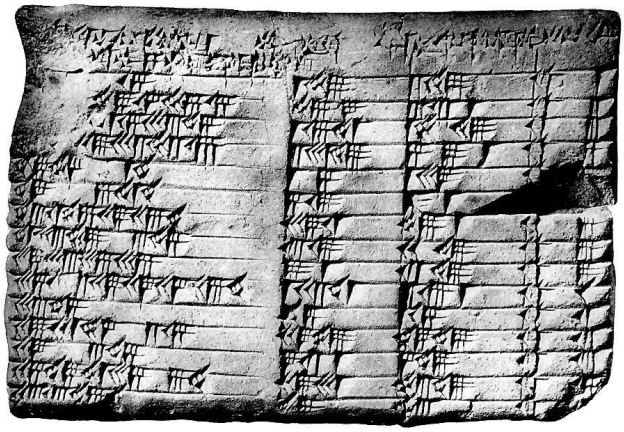
[3] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith.65 (1993), 259–282.

[4] P. Erdős, J. Surányi, *Válogatott Fejezetek a Számelméletből*, Polygon 2004, link.

[5] P. Erdős és P. Turán, *On a problem of Sidon in additive number theory and related problems*, Journ. London Math. Soc.16 (1941), 212—215.

5. Fermat sejtés

Pitagoraszi számhármasokat már az ókori bailóniaik is tanulmányoztak, erről a következő mezopotámiai kőtábla tanúskodik i.e. 1800-ból.



Mi történik akkor, ha a pitagoraszi számhármasokban, azaz az

$$x^2 + y^2 = z^2 \qquad x, y, z \in \mathbb{Z}^+$$

egyenletben a 2 kitevőt lecseréljük n-re?

Azaz a továbbiakban az ún. Fermat egyenletet

$$x^n + y^n = z^n \qquad 2 < n \in \mathbb{N}.$$

tanulmányozzuk.

Hosszú évszázadokig sejtés volt, hogy a fenti egyenletnek nincs pozitív egészekből álló megoldása.

Az alábbi ismertető és az azt követő érdekességek is a kapcsolódó Wikipédia [3] oldalról származnak.

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 eredeti 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.

Végül a Fermat sejtést Andrew Wilesnak sikerült bebizonyítania 1995-ben. A bizonyításon egyedül teljes titokban dolgozott 7 évig. Az elsőre tökéletes bizonyításban azonban volt egy hiba, pontosabban hiányosság, amit Wiles egy tanítványa, Richard Taylor segítségével korrigált.

A sejtést azóta nagy Fermat-tételnek nevezik.

A teljes bizonyítás 129 oldal hosszú, Galois-elméletet és elliptikus görbéket használ, tehát messze túlmegy az elemi számelmélet területén.

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. [2]).

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.

Tehát tekintsük az ún. Fermat-egyenlet az egészek körében:

$$x^n + y^n = z^n, \tag{5.1}$$

ahol $3 \leq n$ természetes szám.

Ekkor vannak bizonyos ún. triviális megoldások. Pl.:

$$x^n + 0^n = x^n \qquad (\Rightarrow (x, y, z) = (x, 0, x)),$$

vagy páratlan n-re

$$x^n + (-x)^n = 0^n \qquad (\Rightarrow (x, -x, 0)).$$

Közös jellemző: $xyz = 0$. Ennek megfelelően:

5.1 DEFINÍCIÓ. *Az* (5.1) *diofantikus egyenlet nem triviális megoldásainak az* $xyz \neq 0$ *tulajdonságú egész megoldásokat nevezzük.*

Faltings [1] 1983-ban igazolta, hogy a Fermat-egyenletnek csak véges sok nem triviális megoldása van. A Wiles [4] által igazolt nagy Fermat-tétel a következő alakban is kimondható:

5.2 TÉTEL. (nagy Fermat-tétel) *A Fermat-egyenletnek nincs nemtriviális megoldása.*

A nagy Fermat-tétel több okból is fontos:

1. Híressége; 2. Számelmélet fejlődésére gyakorolt hatása; 3. Aktualitása.

Egy egyszerű redukciós lépés:

Ha a Fermat-sejtés igaz $n = 4$-re és tetszőleges p páratlan prím-re, akkor $\forall\, n \in \mathbb{N}$, $n \geq 2$-re igaz.

Ez azért igaz, mert minden 2-nél nagyobb természetes számnak van egy páratlan prím osztója, vagy maga a szám egy kettőhatvány is így néggyel osztható.

Azaz amennyiben a Fermat egyenletben a kitevőnek, n-nek van egy p páratlan prím osztója, azaz $n = mp$, akkor, ha x_0, y_0, z_0 egy nem triviális megoldás, úgy:

$$x_0{}^{mp} + y_0{}^{mp} = z_0{}^{mp}$$
$$(x_0{}^m)^p + (y_0{}^m)^p = (z_0{}^m)^p$$

Tehát a Fermat-egyenletnek n helyén p-vel $x_0{}^m, y_0{}^m, z_0{}^m$ nem triviális megoldása.

Azaz amennyiben a Fermat egyenletben a kitevőnek, n egy 4-gyel osztható szám, azaz $n = 4m$, akkor, ha x_0, y_0, z_0 egy nem triviális megoldás, úgy:

$$x_0{}^{4m} + y_0{}^{4m} = z_0{}^{4m}$$
$$(x_0{}^m)^4 + (y_0{}^m)^4 = (z_0{}^m)^4$$

Tehát a Fermat-egyenletnek n helyén 4-gyel $x_0{}^m, y_0{}^m, z_0{}^m$ nem triviális megoldása.

A Fermat sejtés legegyszerűbb esete az $n = 4$ kitevő, amelyet még maga Fermat igazolt, az ún. descente infinitive (végtelen leszállás) módszerével. Fogjunk neki a Fermat-sejtés bizonyításának!

5.3 TÉTEL. (Fermat) $n = 4$ *esetén a Fermat-sejtés igaz.*

Fogjunk neki a Fermat-sejtés bizonyításának! Igazából kicsit többet igazolunk, nevezetesen:

5.4 TÉTEL. *Az* $x^4 + y^4 = z^2$ *diofantikus egyenletnek nem létezik nemtriviális* $(xyz \neq 0)$ *egészekből álló megoldása.*

A 5.4 Tétel bizonyítása. Tegyük fel, hogy $\exists\ x^4 + y^4 = z^2$ nem triviális egész megoldása.

Tekintsük az ilyen pozitív megoldások közül azt, ahol z minimális. Legyen ez (x_0, y_0, z_0).

Ebből ki fogjuk hozni, hogy létezik másik pozitív megoldás, ahol z kisebb z_0-nál, és ez ellentmondás.

Először csak a következőt igazoljuk:

$$(x_0, y_0) = (x_0, z_0) = (y_0, z_0) = 1.$$

Ezt indirekten: Tegyük fel, hogy például

$$(x_0, y_0) > 1$$

Ekkor $\exists\ p$ prím, melyre $p \mid (x_0, y_0)$. Mivel

$$x_0{}^4 + y_0{}^4 = z_0{}^2,$$

így $p \mid z_0^4$ is t, azaz $p \mid z_0$. p^4-nel osztva

$$x = \frac{x_0}{p} \qquad y = \frac{y_0}{p} \qquad z = \frac{z_0}{p^2},$$

olyan pozitív megoldást kaptunk, amelyben $z < z_0$, ellentmondás.

Hasonlóan $(x_0, z_0) > 1$-ből vagy $(y_0, z_0) > 1$-ból is ellentmondást kapunk, amivel (5)-t igazoltuk. Tehát:

$$({x_0}^2)^2 + ({y_0}^2)^2 = {z_0}^2,$$

ahol x_0, y_0, z_0 páronként relatív prímek, azaz x_0^2, y_0^2, z_0 egy primitív pitagoraszi számhármas.

Idézzük fel a primitív pitagoraszi számhármasokról tanultakat:

5.5 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 $\exists\, m, n \in \mathbb{Z}^+$, $m > n$, $(m, n) = 1$, $m \not\equiv n \pmod 2$, hogy

$$a = m^2 - n^2, \;\; b = 2mn, \;\; c = m^2 + n^2,$$

vagy fordítva

$$a = 2mn, \;\; b = m^2 - n^2, \;\; c = m^2 + n^2.$$

A tétel bizonyítása a legtöbb elemi számelmélettel foglalkozó könyvben megtalálható. Ez alapján: $\exists\, m, n \in \mathbb{N}$, hogy

$$(m, n) = 1, \; m \not\equiv n \pmod 2, m > n$$

és

$$\underbrace{{x_0}^2 = m^2 - n^2, \;\; y_0^2 = 2mn}_{\text{vagy megfordítva}}, \;\; z_0 = m^2 + n^2.$$

Szimmetrikus okokból feltehető, hogy

$${x_0}^2 = m^2 - n^2 m, \;\; y_0^2 = 2mn, \;\; z_0 = m^2 + n^2. \qquad (5.2)$$

Mivel $m \not\equiv n \pmod 2$, az egyik páros, a másik páratlan. Először tegyük fel, hogy m páros, n páratlan. Ekkor

$$x_0^2 \equiv 0 - 1 = -1 \quad (4),$$

ami ellentmondás. Tehát m páratlan és n páros.

Legyen $n = 2n_1$, ekkor:

$$(m, 2n_1) = 1 \;\Rightarrow\; (m, n_1) = 1.$$

Mivel $m > n$:

$$m > 2n_1.$$

Továbbá (5.2) miatt:

$$x_0{}^2 = m^2 - 4n_1{}^2, \quad y_0{}^2 = 4mn_1, \quad , z_0 = m^2 + 4n_1^2,$$

vagyis

$$\left(\frac{y_0}{2}\right)^2 = mn_1. \tag{5.3}$$

Mivel $(m, n_1) = 1$ mind m, mind n_1 négyzetszám; legyen

$$m = u^2, \quad n_1 = v^2,$$

ahol $u > v$. Ekkor (5.3) szerint

$$x_0^2 + 4n_1^2 = m^2$$
$$x_0{}^2 + 4v^4 = u^4$$
$$x_0{}^2 + (2v^2)^2 = (u^2)^2$$

Tehát x_0, $2v^2$, u^2 pitagoraszi számhármas, sőt mivel $(2v^2, u^2) = (n, m) = 1$, ez egy primitív pitagoraszi számhármas.

Megint az 5.5 Lemmát alkalmazva: $\exists\, r, s \in \mathbb{N}$

$$\underbrace{x_0 = r^2 - s^2,\ \ 2v^2 = 2rs}_{\text{vagy megfordítva}},\ \ u^2 = r^2 + s^2,$$

ahol $r > s$, $(r, s) = 1$ és $r \not\equiv s \pmod 2$. De itt igazából nem lehet megfordítva a két egyenlet, mert $r^2 - s^2$ páratlan, de $2v^2$ páros. Azaz

$$x_0 = r^2 - s^2,\ \ 2v^2 = 2rs,\ \ u^2 = r^2 + s^2,$$

amiből

$$v^2 = rs.$$

De itt $(r, s) = 1$, tehát $r = k^2$, $s = \ell^2$.

Így $u^2 = k^4 + \ell^4$ egy új megoldás, de vajon u kisebb-e, mint z?

Tudjuk, hogy: $z_0 = m^2 + 4{n_1}^2 = u^4 + 4v^4$. Azaz

$$u \leq u^4 < z_0,$$

és ez ellentmondás. Ezzel a tételt beláttuk.

Most nézzük a Fermat-sejtés $n = p$ páratlan prím speciális esetét először. A legegyszerűbb eset az $n = 3$, amelyet még Euler bizonyított. Ezt az esetet a 9 fejezetben fogjuk bővebben tanulmányozni.

Addig is azonban pár szó a bizonyításról. Ekkor

$$x^3 + y^3 = z^3.$$

A bal oldal szorzattá alakítható

$$(x + y)(x^2 - xy + y^2) = z^3.$$

Ez még nem elég, de alkalmas számkörben a baloldal tovább bontható:

$$x^2 - xy + y^2 = y^2\Bigg(\underbrace{\left(\frac{x}{y}\right)^2 - \frac{x}{y} + 1}_{f\left(\frac{x}{y}\right),\ \text{ahol } f(z)=z^2-z+1} \Bigg)$$

Itt $f(z)$ gyökei

$$z_{1,2} = \frac{1 \pm \sqrt{1-4}}{2} = \frac{1 \pm \sqrt{-3}}{2} = \frac{1 \pm i\sqrt{3}}{2}.$$

Emlékezzünk vissza, hogy a harmadik primitív egységgyökök:

$$\varepsilon = -\frac{1}{2} \pm \frac{\sqrt{3}i}{2} \qquad \frac{\sqrt{3}i}{2} = \xi + \frac{1}{2}.$$

Azaz:

$$\begin{aligned} f(z) = z^2 - z + 1 &= (z - z_1)(z - z_2) \\ &= (z - (1+\varepsilon))(z + \varepsilon). \end{aligned}$$

Vagyis

$$\begin{aligned} x^2 - xy + y^2 = y^2 f\left(\frac{x}{y}\right) &= y^2 \left(\frac{x}{y} - 1 - \varepsilon\right)\left(\frac{x}{y} + \varepsilon\right) \\ &= y^2((x-y) - y\varepsilon)(x + y\varepsilon). \end{aligned}$$

Tehát $n = 3$ esetén a Fermat-egyenlet baloldala 3 ún. Euler egész szorzatára bomlik. A Fermat-sejtés megoldását $n = 3$ esetén a 9 fejezetben tárgyaljuk részletesen.

Hasonlóan $n = 5$ esetén a bal oldal szorzattá alakítható $(a + b\varepsilon)$-ban, ahol ε primitív 5-ik egységgyök.

Nehézség $n = 3$-hoz képest, itt nem létezik egyértelmű prímfelbontás... Valószínű Fermat ezt nézte el. Az $n = 5$ esetet Dirichlet bizonyította először.

Hivatkozások

[1] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. math. 73 (1983), 349—366.

[2] Simon Singh, A nagy Fermat-sejtés (Park Könyvkiadó, Budapest, 1998, ISBN 9635304234; 2004, ISBN 9635306970)

[3] Wikipédia, Nagy-Fermat tétel, link.

[4] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443—551.

[5] Kép, Pierre de Fermat, Musée d'art et d'histoire de Narbonne, link.

6. Két négyzetszám-probléma

A fejezetben azt vizsgáljuk, mely egész számok írhatók fel két négyzetszám összegeként. Ez az ún. kétnégyzetszám-probléma. Az minden estre biztos, hogy ezek a számok nemnegatív egész számok...

A probléma eredete egészen az 1625-ös évig nyúlik vissza, amikor is Albert Girard publikálta prímekre vonatkozó eredményét [1].

De vajon miért kapnak ebben a problémában a prímek különleges szerepet? Az alábbi lemmából látszik az összefüggés:

6.1 LEMMA. *Ha két természetes szám felírható két négyzetszám összegeként, akkor a szorzatuk is.*

A 6.1 Lemma bizonyítása. Következik az

$$(x^2+y^2)(u^2+v^2) = (xu-yv)^2+(xv+yu)^2$$

azonosságból.

Így lényegében elég

$$x^2+y^2=p$$

egyenlet megoldására szorítkozni. Girard eredménye a következő volt:

6.2 TÉTEL. (Girard) *Valamely p prímre*

$$x^2+y^2=p \tag{6.1}$$

akkor és csak akkor oldható meg, ha $p=2$ vagy p egy $4k+1$ alakú prím.

Később, a probléma Fermat egy levelezésében is feltűnt, aki azt vizsgálta, hogy p^α hányféleképpen írható fel két négyzetszám összegeként.

A 6.2 Tétel bizonyítása. 1. Ha (6.1) megoldható, akkor $p = 2$ vagy $p = 4k+1$, vagyis ha $p = 4k+1 \Rightarrow x^2+y^2 = p$ megoldhatatlan.

Ez a bizonyítás könnyebb fele. Olyan módszerrel, mely igen gyakran használatos diofantikus egyenletek megoldhatatlanságának igazolására.

Kongruencia-módszer

Tegyük fel, hogy az

$$\underbrace{f(x_1, x_2, \ldots, x_n))}_{\in \mathbb{Z}[x_1, x_2, \ldots, x_n]} = 0 \tag{6.2}$$

diofantikus egyenlet egész megoldásait keressük.

Állítás. Ha létezik olyan $m \in \mathbb{N}$, hogy az

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{m} \tag{6.3}$$

(n változós) magasabb fokú kongruencia megoldhatatlan, akkor az (6.2) *diofantikus egyenlet is megoldhatatlan.*

Állítás bizonyítása. Ha ugyanis pl. $x_1', x_2', \ldots, x_n'$ megoldása lenne (6.2)-nek, azaz

$$\begin{gathered} f(x_1', x_2', \ldots, x_n') = 0 \\ \Downarrow \\ f(x_1', x_2', \ldots, x_n') \equiv 0 \pmod{m}, \end{gathered}$$

vagyis $x_1', x_2', \ldots, x_n'$ megoldása (6.2)-nek, ez ellentmondás, hiszen (6.3)-ról feltettük, hogy megoldhatatlan.

Ez csak elégséges feltétele a megoldhatatlanságnak!!!

Jelen esetben: azt kell igazolnunk, hogy ha $p = 4k - 1$ alakú prím, akkor $\Rightarrow x^2 + y^2 = p$ megoldhatatlan.

Tegyük fel ugyanis, hogy nem igaz az állítás, és p mégiscsak felírható két négyzetszám összegeként. Vagyis létezik x és y egész szám, melyre

$$x^2 + y^2 = p.$$

Ekkor

$$x^2 + y^2 \equiv p \pmod 4.$$

De mivel p egy $4k - 1$ alakú prím, ezért

$$x^2 + y^2 \equiv -1 \pmod 4.$$

Egy négyzetszám négyes maradéka csak 0 vagy 1 lehet. Azaz $x^2 + y^2$ négyes maradéka $0, 1$ vagy 2 lehet, de sohasem -1. Ezzel ellentmondásra jutottunk, és az állítást igazoltuk.

2. A 6.2 Tétel bizonyításának nehezebb fele, hogy ha $p = 2$ vagy $p = 4k + 1$, akkor $x^2 + y^2 = p$ megoldható.

Igazából, a $p = 2$ eset könnyű: $2 = 1^2 + 1^2$. Marad a következő lemmának a bizonyítása:

6.3 LEMMA. *Minden $4k + 1$ alakú p prím előáll két négyzetszám összegeként.*

Sokféleképpen.

A fejezet fő célja az algebrai azonosságok módszerének egy olyan továbbfejlesztése, mely elvezet az algebrai számelmélethez.

A 6.3 Lemma legismertebb és legkézenfekvőbb bizonyítása Gauss egészekkel történik, amely az első lépés az algebrai számelmélet megismeréséhez vezető úton.

De mielőtt rátérnénk a fenti módszer ismertetésére, lássunk egy elemi bizonyítást:

A 6.3 Lemma I. bizonyítása. Tehát p egy $4k+1$ alakú prím. Ekkor -1 kvadratikus maradék modulo p. Azaz az

$$x^2 \equiv -1 \pmod{p} \tag{6.4}$$

kongruencia megoldható. Jelöljön s a (6.4)-beli kongruencia egy megoldását. Ekkor

$$s^2 \equiv -1 \pmod{p}$$
$$p \mid s^2 + 1$$

Tekintsük az összes $a + bs$ alakú számot, ahol $a, b \in \mathbb{N}$ és

$$0 \leq a < \sqrt{p}, \quad 0 \leq b < \sqrt{p}.$$

Az ilyen számok száma $\left([\sqrt{p}+1]\right)^2 > p$, vagyis a skatulyaelv szerint létezik közöttük kettő, amelyek kongruensek modulo p:

$$a_1 + b_1 s \equiv a_2 + b_2 s \pmod{p}$$

Legyen $a = a_1 - a_2$ és $b = b_1 - b_2$. Ekkor:

$$a + bs \equiv 0 \pmod{p}$$

$$a \equiv -bs \pmod{p}$$
$$a^2 \equiv b^2 s^2 \pmod{p}$$
$$a^2 \equiv -b^2 \pmod{p}$$
$$p \mid a^2 + b^2.$$

Mivel $0 \leq a_1, a_2 < \sqrt{p}$ és $0 \leq b_1, b_2 < \sqrt{p}$ tudjuk, hogy $-\sqrt{p} < a < \sqrt{p}$ és $-\sqrt{p} < b < \sqrt{p}$. Vagyis

$$0 < a^2 + b^2 < 2p.$$

Mivel $p \mid a^2 + b^2$, ez csak úgy lehet, ha $a^2 + b^2 = p$.

Kétségtelen, ez a legegyszerűbb bizonyítása a 6.3 Lemmának, de talán a legcselesebb is, és nehéz lehet rájönni erre a bizonyításra.

Azonban van egy logikusabb út is, amely abból indul ki, hogy hasonlóan ahhoz, hogy

$$x^2 - y^2 = p$$

szorzattá bomlik egész számok esetén:

$$(x - y)(x + y) = p,$$

most:

$$x^2 + y^2 = p$$

is szorzattá bomlik, de a komplex egész számok körében:

$$(x + iy)(x - iy) = p \tag{6.5}$$

$a + bi$ $\quad a, b \in \mathbb{Z}$ alakú

6.4 DEFINÍCIÓ. *Az $a + bi$ (ahol $a, b \in \mathbb{Z}$) alakú számokat Gauss-egészeknek (komplex egészeknek) nevezzük, ezek halmazát G-vel jelöljük.*

Annak céljából, hogy (6.5)-ből továbbmenjünk, a számelméletet ki kell építeni a Gauss-egészek körében. Ehhez először oszthatóság:

6.5 DEFINÍCIÓ. *Ha $\alpha \in \mathcal{G}$, $\beta \in \mathcal{G}$ és $\exists\, \gamma \in \mathcal{G}$ hogy $\alpha = \beta\gamma$, akkor azt mondjuk, hogy α osztható β-val: $\beta \mid \alpha$.*

Az alábbi tétel bizonyítását az olvasóra bízzuk:

6.6 TÉTEL. *Az oszthatóság $\mathcal{G}$-ben is reflexív, tranzitív, és rendelkezik a lineáris kombináció tulajdonsággal.*

Ahogy általában a komplex számoknak, úgy a Gauss-egészeknek is van konjugáltja és normája:

6.7 DEFINÍCIÓ. *$\alpha = a + bi \in \mathcal{G}$ esetén az $|\alpha|^2 = \alpha\overline{\alpha} = a^2 + b^2$ számot az α Gauss-egész normájának nevezzük, és $N(\alpha)$-val jelöljük.*

Megjegyzés. $\alpha \in \mathcal{G} \Rightarrow N(\alpha) \in \{0\} \cup \mathbb{N}$ és $N(\alpha) = 0 \Leftrightarrow \alpha = 0$.

A norma multiplikatív:

6.8 TÉTEL. $\alpha, \beta \in \mathcal{G} \Rightarrow N(\alpha\beta) = N(\alpha)N(\beta)$.

A 6.8 Tétel bizonyítása. Valóban, $|\alpha\beta|^2 = |\alpha|^2 \cdot |\beta|^2$. igaz, mert az abszolútérték multiplikatív.

Ebből pedig:

6.9 TÉTEL. *Ha $\alpha, \beta \in \mathcal{G}$, akkor*

$$\underbrace{\alpha \mid \beta}_{\mathcal{G}\text{-ben}} \Rightarrow \underbrace{N(\alpha) \mid N(\beta)}_{\mathbb{Z}\text{-ben}}.$$

A 6.9 Tétel bizonyítása.

$$\alpha \mid \beta \Rightarrow \exists\, \gamma\ \mathcal{G}\text{-ben} \quad \beta = \alpha\gamma$$

$$N(\beta) = N(\alpha)N(\gamma),$$
$$N(\alpha) \mid N(\beta).$$

6.10 DEFINÍCIÓ. *Ha $\varepsilon \in \mathcal{G}$ és $\varepsilon \mid \alpha\ \forall\ \alpha \in \mathcal{G}$-re, akkor ε-t egységnek nevezzük.*

Emlékeztetőül felidézzük, hogy egy S számkörben, ahol $1 \in S$, az $\varepsilon \in S$ szám pontosan akkor egység, ha $\varepsilon \mid 1$. Ez alapján:

6.11 TÉTEL. *$\mathcal{G}$-ben az összes egységek: $\pm 1, \pm i$.*

A 6.11 Tétel bizonyítása. $\varepsilon = a + bi$ egység $\Rightarrow\ \varepsilon \mid 1\ \Rightarrow\ N(\varepsilon) \mid N(1) \Rightarrow a^2 + b^2 = 1$. Ebből már következik, hogy csak ± 1 és $\pm i$ lehet egység. Ezek meg valóban azok.

6.12 DEFINÍCIÓ. *Ha $\alpha, \beta \in \mathcal{G}$ és $\alpha \mid \beta$, $\beta \mid \alpha$, akkor α-t és β-t asszociáltnak mondjuk.*

Ekkor nyilván:

6.13 TÉTEL. *$\alpha, \beta \in \mathcal{G}$ asszociáltak $\Rightarrow \beta = \varepsilon\alpha$, ahol ε egység.*

Algebrából szerepelt az eukleidészi gyűrű definíciója.

6.14 DEFINÍCIÓ. *Euklideszi gyűrű: olyan E integritási tartomány (kommutatív, 0-osztómentes gyűrű), melynek $\forall\ a \neq 0$ eleméhez*

hozzá van rendelve egy $\varphi(\alpha)$ nemnegatív egész a következő tulajdonságokkal:
1. $a, b \in E$, $b \neq 0$ esetén $\exists\, q, r$ hogy

$$a = bq + r \quad \text{és vagy } r = 0, \text{ vagy } \varphi(r) < \varphi(b);$$

2. $a, b \in E$, $a \neq 0$, $b \neq 0$ esetén

$$\varphi(ab) \geq \varphi(a).$$

Az eukleidészi gyűrűkben létezik legnagyobb közös osztó (hiszen az eukleidészi algoritmus ugyanúgy működik mint $\mathbb{Z}$-ben, van maradékos osztás, amely most φ-t használja). Sőt, a legnagyobb közös osztó felírható lineáris kombinációként, amiből adódóan az eukleidészi gyűrűkben a prímek és felbonthatatlanok azonosak.

6.15 TÉTEL. *$\mathcal{G}$ a $\varphi(\alpha) = N(\alpha)$ választással euklideszi gyűrűt alkot.*

A 6.15 Tétel bizonyítása. Annak bizonyítása, hogy $\mathcal{G}$ integritási tartomány házifeladat. A tétel nehezebb része, hogy létezik maradékos osztás, azaz:

Bizonyítandó, hogy adott $\alpha, \beta\ (\neq 0)$ Gauss-egészhez γ, δ létezése, amelyekre

$$\alpha = \beta\gamma + \delta \quad \text{ahol } \delta = 0 \text{ vagy } N(\delta) < N(\beta).$$

Most $\delta = 0$-ra $N(\delta) = 0$ vagyis ekkor is teljesül $N(\delta) < N(\beta)$.

$\beta \neq 0$ miatt $\alpha = \beta\gamma + \delta$ ekvivalens

$$\frac{\alpha}{\beta} - \gamma = \frac{\delta}{\beta}$$

egyenlettel. Azaz $N(\delta) < N(\beta)$ akkor és csak akkor teljesül, ha

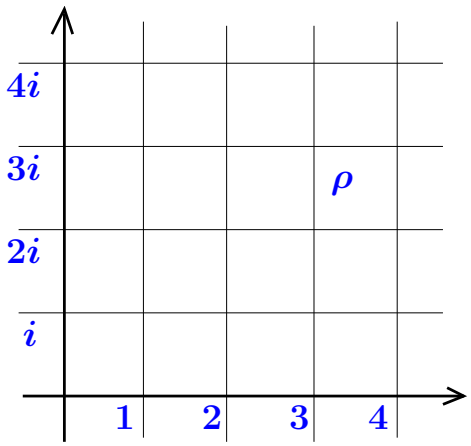
$$\left|\frac{\alpha}{\beta} - \gamma\right| = \frac{|\delta|}{|\beta|} < 1.$$

Tehát adott $\varrho \stackrel{\text{def}}{=} \frac{\alpha}{\beta}$-hoz létezik-e γ Gauss-egész, hogy

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1$$

teljesül?

Ehhez tekintsük a komplex számsíkot, és rajta az egységnégyzetekből álló rácsot:



Ebben a rácsban tekintsük a $\varrho = \frac{\alpha}{\beta}$-t tartalmazó egységnégyzetet és legyen ennek ϱ-hoz legközelebbi csúcsa γ. Ekkor:

$$|\varrho - \gamma| \leq \text{ „egységnégyzet átlójának fele”}$$
$$= \frac{\sqrt{2}}{2} < 1$$

Ha γ már adott, akkor δ értéke adódik az $\alpha = \beta\gamma + \delta$ összefüggésből.

Eukleidészi gyűrűknél még fontos a tételbeli 2. tulajdonság is. Ezt bizonyítjuk most. Legyen $\alpha \neq 0$ és $\beta \neq 0$. Ekkor

$$\varphi(\alpha\beta) = N(\alpha\beta) \geq \varphi(\alpha) = N(\alpha),$$

hiszen $N(\beta) \geq 1$.

Fontos kérdés, hogy vajon, hogyan karakterizálhatóak a Gauss-egészek körében a prímek (amelyek most azonosak a felbonthatatlanokkal)?

Kérdés. Legyen $p = 4k + 1$ alakú prím $\mathbb{Z}$-ben. Prímszám-e ez a Gauss-egészek körében? Azaz ún. Gauss-prím-e?

6.16 Lemma. *A $p = 4k + 1$ prím nem Gauss-prím.*

A 6.16 Lemma bizonyítása. Indirekt: Tegyük fel, hogy p Gauss-prím.

Mivel p most $4k+1$ alakú, ezért -1 kvadratikus maradék modulo p.

Azaz $z^2 \equiv -1 \pmod{p}$ megoldható: $\exists\, z_0 \in \mathbb{Z}$, hogy

$$z_0^2 \equiv -1 \pmod{p}$$
$$p \mid {z_0}^2 + 1 = (z_0 + i)(z_0 - i).$$

Indirekt feltevésünk szerint p Gauss-prím, azaz

$$p \mid z_0 + i \qquad \text{vagy} \qquad p \mid z_0 - i.$$

Amennyiben $p \mid z_0 + i$, akkor

$$z + i = (a + bi)p = ap + bp\, i,$$

amelynek képzetes részét tekintve

$$1 = bp \;\Rightarrow\; p \mid 1,$$

tehát $p = 4k + 1$ nem Gauss-prím. Ezzel a lemmát beláttuk.

A következő fejezetben részletesen fogunk foglalkozni a Gauss-prímekkel. Előbb azonban lássunk egy második bizonyítást a 6.3 Lemmára.

A 6.3 Lemma II. bizonyítása. A 6.16 Lemma miatt $p = 4k + 1$ nem Gauss-prím. Tehát $\exists$ nem triviális felbontása.

Azaz $\exists \alpha, \beta \in \mathcal{G}$, hogy $p = \alpha\beta$, és ahol α, β nem egység.

A Gauss-egészek körében az egységek normája 1.

A norma multiplikativitása miatt következik:

$$p^2 = N(p) = N(\alpha)N(\beta),$$

ahol $N(\alpha), N(\beta) \in \mathbb{N}$ és 1-től különbözőek. Tehát

$$N(\alpha) = p, \ N(\beta) = p.$$

Legyen végül $\alpha = a + bi$, ekkor

$$N(\alpha) = a^2 + b^2 = p,$$

és ezzel a 6.3 Lemma állítását beláttuk.

Ezzel Girard prímekre vonatkozó eredményét megbeszéltük. De vajon egy tetszőleges összetett természetes szám, mikor áll ellő két négyzetszám összegeként?

Láttuk: 2 előáll két négyzetszám összegeként

$$2 = 1^2 + 1^2,$$

és ha p egy $4k+1$ alakú prím, akkor ő is előáll két négyzetszám összegeként. Továbbá, q^2 is (ahol most q egy $4k+3$ alakú prím):

$$q^2 = 0^2 + q^2.$$

A 6.1 Lemma alapján, ha α, β előáll két négyzetszám összegeként, akkor $\alpha\beta$ is. Tehát:

Ha n prímtényezős felbontása

$$n = 2^{\alpha} {p_1}^{\alpha_1} \dots {p_r}^{\alpha_r} {q_1}^{\beta_1} \dots {q_s}^{\beta},$$

ahol p_i-k a $4k+1$, q_j a $4k+3$ alakú prímek, akkor ha $\forall\ \beta_i$ páros, akkor n előáll két négyzetszám összegeként.

Fordítva is igaz ez. Azaz ha β_i-k között akad páratlan, akkor n nem áll elő két négyzetszám összegeként.

Ugyanis: Tegyük fel, hogy β_i páratlan és

$$n = a^2 + b^2 = 2^{\alpha} {p_1}^{\alpha_1} \dots {p_r}^{\alpha_r} {q_1}^{\beta_1} \dots {q_s}^{\beta_s}.$$

Ekkor $q_i \mid a^2 + b^2$. Bebizonyítjuk, hogy $q_i \mid a \Leftrightarrow q_i \mid b$.

Először tegyük fel, hogy $(q_i, a) = (q_i, b) = 1$. Ekkor

$$\begin{aligned} a^2 + b^2 &\equiv 0 \qquad (q_i) \\ a^2 &\equiv -b^2 \quad (q_i). \end{aligned}$$

A Legendre-szimbólumra

$$\begin{aligned} \left(\frac{a^2}{q_i}\right) = \left(\frac{-b^2}{q_i}\right) &= \left(\frac{-1}{q_i}\right)\left(\frac{b^2}{q_i}\right) \\ 1 &= \left(\frac{-1}{q_i}\right). \end{aligned}$$

De most q_i egy $4k+3$ alakú prím, tehát $\left(\frac{-1}{q_i}\right) = -1$, amivel ellentmondásra jutottunk.

Tehát $q_i \mid a$ vagy $q_i \mid b$. Azonban $q_i \mid a^2+b^2$ miatt a kettő egyszerre teljesül mindig. Tehát most:

$$n = a^2 + b^2 = 2^{\alpha} {p_1}^{\alpha_1} \dots {p_r}^{\alpha_r} {q_1}^{\beta_1} \dots {q_s}^{\beta_s},$$

ahol $q_i \mid a$ és $q_i \mid b$. Osszunk le ${q_i}^2$-tel

$$\left(\frac{a}{q_i}\right)^2 + \left(\frac{b}{q_i}\right)^2 = 2^{\alpha} {p_1}^{\alpha_1} \dots {p_r}^{\alpha_r} {q_1}^{\beta_1} \dots {q_i}^{\beta_i - 2} \dots {q_s}^{\beta}.$$

A jobb oldalon q_i kitevője továbbra is páratlan, az eljárást folytathatjuk, megint leoszthatunk ${q_i}^2$-tel, majd megint. Végtelen sokszor leoszthatjuk a-t és b-t ${q_i}^2$-tel, ami nyilván nem lehetséges, és itt az ellentmondás.

Ezzel a következőt igazoltuk:

6.17 TÉTEL. *Egy $n \geq 2$ természetes szám pontosan akkor írható fel két négyzetszám összegeként, ha prímtényezős felbontása nem tartalmaz olyan p^k prímhatvány szorzót, ahol $p \equiv 3 \pmod 4$ és k páratlan.*

Hivatkozások

[1] L. E. Dickson, *History of the Theory of Numbers, II. kötet, VI fejezet: „Sum of two squares"*, Washington, D.C.: Carnegie Institution of Washington 1920, 227–228.

7. Gauss-prímek

A fejezetben megpróbáljuk teljesen karakterizálni a Gauss-prímeket.

Azért, hogy világos legyen mikor melyik számkörben vagyunk, $\mathbb{Z}$ elemeit racionális egészeknek, $\mathcal{G}$ elemeit Gauss-egészeknek hívjuk.

Hasonlóan, a $\mathbb{Z}$-beli prímek a racionális prímek, és a $\mathbb{G}$-beli prímek a Gauss-prímek.

Először azt vizsgáljuk, hogy egy $n \in \mathbb{Z}$ egész szám mikor lehet Gauss-prím.

Triviális, hogy ha n összetett $\mathbb{Z}$-ben, akkor a Gauss-egészek körében is összetett. Következőleg azt vizsgáljuk, hogy egy $p \in \mathbb{N}$ racionális prímszám mikor Gauss-prím.

Könnyen ellenőrizhető, hogy a 2 a következőképp írható fel Gauss-egészek szorzataként:

$$2 = (1+i)(1-i),$$

az $1+i$ és $1-i$ nem bontható tovább (egységtől különböző elemek) szorzatává, azaz $1+i$ és $1-i$ Gauss prímek. Ezek azonban egymás asszociáltjai:

$$1 - i = -i(1+i),$$

azaz 2 prímtényezős felbontása a Gauss -egészek körében

$$2 = -i(1+i)^2. \tag{7.1}$$

Ezután tekintsük a páratlan prímek esetét:

7.1 Tétel. *Legyen $p \in \mathbb{N}$ racionális páratlan prímszám. Ekkor:*

1. $p = 4k - 1$ *alakú racionális prímek egyszersmind Gauss-prímek.*

2. $p = 4k + 1$ *alakú racionális prímek felbonthatóak két (különböző) Gauss-prím szorzatára, melyek egymás konjugáltjai:*

$$p = \pi\overline{\pi}.$$

Megjegyezzük még, hogy itt $N(\pi) = N(\overline{\pi}) = p$.

A 7.1 Tétel bizonyítása. Először 1.-t látjuk be. Tegyük fel, hogy $p = 4k - 1$ Gauss-összetett szám:

$$p = \alpha\beta,$$

ahol α, β nem egység. Ekkor

$$N(p) = N(\alpha)N(\beta)$$
$$p^2 = N(\alpha)N(\beta),$$

ahol $N(\alpha), N(\beta) > 1$, így $N(\alpha) = N(\beta) = p$.

Ha $\alpha = a + bi$, akkor $N(\alpha) = a^2 + b^2 = p$, amiből

$$a^2 + b^2 = p \equiv -1 \pmod 4,$$

és ez ellentmondás, mert két négyzetszám összege $0, 1$ vagy 2-vel kongruens modulo 4.

Ezután térjünk rá 2. bizonyítására. Tekintsük a $p = 4k+1$ alakú racionális prímet, és írjuk fel p prímtényezős felbontását a Gauss-egészek körében:

$$p = \varepsilon\pi_1\pi_2 \cdots \pi_r,$$

ahol ε egység, π_i-k Gauss-prímek. Ekkor:

$$p^2 = N(p) = N(\pi_1)N(\pi_2) \cdots N(\pi_r),$$

ahol $N(\pi_i) > 1$, és ez csak úgy lehet, ha

$$p = \varepsilon\pi_1 \tag{7.2}$$

vagy

$$p = \varepsilon\pi_1\pi_2.$$

A 6.16 Lemma állítása szerint p nem Gauss-prím, így (7.2) nem lehet. Vagyis

$$p = \varepsilon\pi_1\pi_2, \tag{7.3}$$

amiből $N(\pi_1) = N(\pi_2) = p$.

(7.3)-ből világos, hogy $\pi_1 \mid p$, de ekkor $\overline{\pi_1} \mid \overline{p}$ is teljesül, azaz $\overline{\pi_1} \mid p$. Itt π_1 Gauss-prím, így $\overline{\pi_1}$ is Gauss-prím.

Sőt, π_1 nem $\overline{\pi_1}$ egységszerese, hiszen ha $\pi = a + bi$, akkor

$$\frac{\pi_1}{\overline{\pi_1}} = \frac{a+bi}{a-bi} = \frac{(a+bi)^2}{a^2+b^2} = \frac{a^2-b^2}{a^2+b^2} + \frac{2ab}{a^2+b^2}i.$$

Mivel most $N(\pi_1) = p = a^2 + b^2$:

$$\frac{\pi_1}{\overline{\pi_1}} = \frac{a^2-b^2}{p} + \frac{2ab}{p}i,$$

ami akkor lehet egység ha

$$a^2 - b^2 = \pm p, \quad 2ab = 0$$

vagy

$$a^2 - b^2 = 0, \quad 2ab = \pm p.$$

Az első esetben a vagy b nulla, a másik szám pedig $\pm\sqrt{p}$, ami nem egész, és ez ellentmondás. A második esetben $p = \pm 2ab$ páros szám, ami megint csak ellentmondás.

Ott tartottunk, hogy

$$p = \varepsilon\pi_1\pi_2,$$

de $\overline{\pi_1} \mid p$ szintén teljesül, ahol $\overline{\pi_1}$ nem π_1 asszociáltja. Ez csak úgy lehet, ha

$$p = \varepsilon' \pi_1 \overline{\pi_1},$$

ahol ε' egység.

Világos, hogy $\pi_1 \overline{\pi_1} = N(\pi_1)$ pozitív racionális egész, p is pozitív racionális egész, azaz ε' egység csak $+1$ lehet. Tehát:

$$p = \pi_1 \overline{\pi_1},$$

és ezzel a tétel állítását beláttuk.

Eddig bebizonyítottuk, hogy ha p prím, akkor

$$\begin{aligned} x^2 + y^2 = p \quad \text{megoldható} \quad &\Leftrightarrow \quad p = 2 \text{ vagy } \ 4k+1 \text{alakú prím} \\ &\Rightarrow \quad \text{könnyű} \\ &\Leftarrow \quad \text{pl. Gauss-egészekkel.} \end{aligned}$$

Azt is láttuk, hogy $x^2 + y^2 = n$ megoldhatósága visszavezethető $x^2 + y^2 = p$ egyenletek vizsgálatára, ahol p prím.

A következő célunk az $x^2 + x^2 = n$ egyenlet megoldásszámának vizsgálata. Ekkor a Gauss-prímek további karakterizációja szükséges.

7.2 TÉTEL.

a) *különböző p-khez tartozó π, $\overline{\pi}$-k különbözők, sőt egyik sem asszociáltja a másiknak.*

b) *Ugyanahhoz a p-hez tartozó π, $\overline{\pi}$ is különbözőek; vagyis hogy nem asszociáltak.*

A 7.2 Tétel bizonyítása. A tétel b) részét már a 7.1 Tétel bizonyításában beláttuk.

Csak az a) rész igazolása maradt hátra. Ha $p_1 = \pi_1\overline{\pi_1}$ és $p_2 = \pi_2\overline{\pi_2}$, ahol $p_1 \neq p_2$, akkor

$$N(\pi_1) = {p_1}^2 \neq {p_2}^2 = N(\pi_2).$$

Vagyis π_1 és π_2 nem lehetnek asszociáltak, hiszen akkor normájuk megegyezne.

A 7.1 Tételben és előtte a (7.1)-nél a következőt bizonyítottuk:

1. $1 + i$ Gauss-prím.
2. Ha $p = 4k + 3$ alakú racionális prím, akkor egyúttal Gauss-prím is.
3. Ha $p = 4k + 1$ alakú racionális prím, akkor $p = \pi\overline{\pi}$ alakú, ahol π és $\overline{\pi}$ Gauss prímek, amelyek nem asszociáltak.

7.3 TÉTEL. *Az összes $\mathcal{G}$ prímek az 1, 2 és 3 alattiak.*

A 7.3 Tétel bizonyítása. Tegyük fel, hogy π Gauss-prím. Ekkor

$$\pi \mid \pi\overline{\pi} = \underbrace{N(\pi)}_{\text{rac. poz. egész}} = {p_1}^{\alpha_1} \dots {p_r}^{\alpha_r}.$$

De π Gauss-prím, így $\exists\, i$, hogy

$$\pi \mid p_i.$$

Azaz az összes Gauss-prímek racionális prímek osztói, melyek prímtényezős felbontását a 7.1 Tételben és (7.1) képletben már láttunk. Ebből adódik a tétel állítása.

7.4 TÉTEL. *Legyen $n \in \mathbb{N}$ prímtényezős felbontása $\mathbb{N}$-ben:*

$$n = 2^{\alpha} {p_1}^{\beta_1} \dots {p_r}^{\beta_r} {q_1}^{\gamma_1} \dots {q_s}^{\gamma_s},$$

ahol $p_1, \dots, p_r$ a $4k-1$; $q_1, q_2, \dots, q_s$ a $4k+1$ alakú prímosztók (lehetséges, hogy a 3 féle prímtényező közül valamelyek hiányoznak). Ekkor az

$$x^2 + y^2 = n$$

diofantikus egyenlet (egész) megoldásainak száma

a) 0, ha $\exists$ páratlan β_j;

b) $4(\gamma_1 + 1) \dots (\gamma_s + 1)$, ha $\forall\, \beta_j$ páros.

A 7.4 Tétel bizonyítása. A tétel a) részét már a 6.17 Tételben beláttuk.

Tegyük fel tehát, hogy $\forall\, \beta_j$ páros. $\forall\, q_j$ racionális ($4k+1$ alakú) prím $q_j = \pi_j \overline{\pi_j}$ alakba írható. Így n prímtényezős felbontása a Gauss-egészek körében:

$$\begin{aligned} n &= \left(-i(1+i)^2\right)^{\alpha} {p_1}^{\beta_1} \cdots {p_r}^{\beta_r} (\pi_1\overline{\pi_1})^{\gamma_1} \dots (\pi_s\overline{\pi_s})^{\gamma_s} \\ &= \underbrace{(-i)^{\alpha}}_{\varepsilon_1 \text{ egység}} (1+i)^{2\alpha} {p_1}^{\beta_1} \dots {p_r}^{\beta_r} (\pi_1\overline{\pi_1})^{\gamma_1} \dots (\pi_s\overline{\pi_s})^{\gamma_s}. \end{aligned} \tag{7.4}$$

Itt minden tényező (ε_1-et kivéve) $\mathcal{G}$ prím $\Rightarrow$ ez lesz n-nek a $\mathcal{G}$ kanonikus alakja. Másrészt, ha x, y-re $x^2 + y^2 = n$, akkor

$$\begin{aligned} (x+iy)(x-iy) &= n \\ x+iy \;\underset{\mathcal{G}}{|}\; n. & \end{aligned}$$

Tekintsük $x+iy$ kanonikus alakját $\mathcal{G}$-ben:

$$x + iy = \varepsilon_2 (1+i)^{\delta}\; {p_1}^{\varphi_1} \cdots p_r^{\varphi_r} \pi_1^{\nu_1} \overline{\pi_1}^{\,\mu_1} \cdots \pi_r^{\nu_r} \overline{\pi_r}^{\,\mu_r}$$

alakú. Konjugáltat véve:

$$x+iy=\overline{\varepsilon_2}\underbrace{(1-i)^{\delta}}_{(-i(1+i))^{\delta}}\ {p_1}^{\varphi_1}\cdots p_r^{\varphi_r}\overline{\pi_1}^{\ \mu_1}\pi_1^{\nu_1}\cdots\overline{\pi_r}^{\ mnu_r}\pi_r^{\nu_r}$$
$$\varepsilon_3(1+i)^{\delta}\ {p_1}^{\varphi_1}\cdots p_r^{\varphi_r}\overline{\pi_1}^{\ \mu_1}\pi_1^{\nu_1}\cdots\overline{\pi_r}^{\ \mu_r}\pi_r^{\nu_r}.$$

Összeszorozva:

$$x^2+y^2=\varepsilon_2\varepsilon_3(1+i)^{2\delta}\ {p_1}^{2\varphi_1}\cdots p_r^{2\varphi_r}\pi_1^{\nu_1+\mu_1}\overline{\pi_1}^{\ \nu_1+\mu_1}\cdots\pi_r^{\nu_r+\mu_r}\overline{\pi_r}^{\ \nu_r+\mu_r}$$

Ezt (7.4)-mal egybevetve, kanonikus alak egyértelműsége miatt

$$\begin{aligned}\alpha&=\delta\\ \beta_j&=2\varphi_j\qquad(j=1,2\ldots,r)\\ \mu_j+\nu_j&=\gamma_j\qquad(j=1,2,\ldots,s)\end{aligned}$$

Így $x+iy$-ban δ és φ_j-k értéke egyértelmű; ν_j értéke γ_j+1 féle lehet: $0,1,2,\ldots,\gamma_j$.

Ha ν_j adott, akkor már μ_j éréke egyértelmű. Végül ε_2 egység négyféle lehet: $\pm1,\ \pm i$.

Ezek alapján $x+iy$ értéke valóban $4(\gamma_1+1)\cdots(\gamma_s+1)$ féle lehet, és $x+y$ valós illetve képzetes részét véve megkapjuk x-et és y-t. Ezzel a tétel állítását beláttuk.

8. Algebrai Számelmélet

A diofantikus egyenletek elméletében domináló módszer az algebrai számelmélet alkalmazása.

Alapgondolat: adott egy

$$\underbrace{f(x_1, x_2, \ldots, x_n)}_{\in \mathbb{Z}[x_1, x_2, \ldots, x_n]} = 0$$

diofantikus egyenlet.

Itt minden egész együtthatós, és az egész megoldásokat keressük. Sokszor előnyösebb, ha áttérünk egy bővebb számkörre, és ott keresünk megoldásokat. Ez a bővebb számkör tipikusan a következő típusú:

Legyen α algebrai szám, azaz α gyöke egy egész együtthatós polinomnak.

Az algebrai számok testet alkotnak, azaz ha α és β algebrai szám $\alpha + \beta$, $\alpha\beta$ és $\frac{1}{\alpha}$ is (ennek bizonyítása elemi, de kissé komplikált, nem térünk ki rá).

A racionális számtest $\mathbb{Q}$, α-val való (egyszerű) algebrai bővítése:

$$\mathbb{Q}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in \mathbb{Z}[x]\ g(\alpha) \neq 0 \right\}.$$

$\mathbb{Q}[\alpha]$ gyűrűt alkot.

Egy β számot algebrai egésznek hívunk, ha gyöke egy 1 főegyütthatós (azaz normált), egész együtthatós polinomnak.

A $K = \mathbb{Q}(\alpha)$-beli algebrai egészek gyűrűt alkotnak, jelölése $\mathcal{O}_K(\alpha)$.

Tehát $\mathbb{Z}$ helyett egy ilyen $\mathcal{O}_K$-ban vizsgálódunk.

Most egyszerűsítünk kicsit az elméleten, és $\mathcal{O}_K$ helyett egyszerűen $\mathbb{Z}(\alpha) = \{f(\alpha) : \ f(x) \in \mathbb{Z}[x]\}$-ban vizsgálódunk.

De hogyan választjuk α-t?

Sokszor azon az alapon választjuk α-t, hogy a kérdéses diofantikus egyenletben szereplő többváltozós polinom $\mathbb{Z}$ felett nem alakítható szorzattá (algebrai azonosságok módszere), de alkalmas α-val, $\mathbb{Z}(\alpha) = \{f(\alpha) : \ f(x) \in \mathbb{Z}[x]\}$ felett már igen.

Például:

Két-négyzetszám-probléma:

$$x^2 + y^2 = n$$

irreducibilis $\mathbb{Z}$ felett, de $\mathbb{Z}(i)$ felett már nem:

$$\underbrace{(x+iy)}_{\text{Gauss egész}}\ \underbrace{(x-iy)}_{\text{Gauss egész}} = n$$

Menjünk tovább, és nézzük az $x^2 + ay^2 = n$ egyenletet, ahol most $a \in \mathbb{N}$ és a „kicsi”.

$a = 2$:

$$n = x^2 + 2y^2$$
$$n = \underbrace{(x+\sqrt{2}iy)}_{\in\mathbb{Z}(\sqrt{2}i)}\underbrace{(x-\sqrt{2}iy)}_{\in\mathbb{Z}(\sqrt{2}i)}.$$

Itt $\mathbb{Z}(\sqrt{2}i) = \{f(\sqrt{2}) : \ f(x) \in \mathbb{Z}[x]\} = \{a + b\sqrt{2}i,\ a, b \in \mathbb{Z}\}$.

$a = 3$:

$$n = x^2 + 3y^2$$

$$n = \underbrace{(x + \sqrt{3}iy)}_{\in \mathbb{Z}(\sqrt{3}i)} \underbrace{(x - \sqrt{3}iy)}_{\in \mathbb{Z}(\sqrt{3}i)}.$$

Itt $\mathbb{Z}(\sqrt{3}i) = \{f(\sqrt{3}i) : \ f(x) \in \mathbb{Z}[x]\} = \{a + b\sqrt{3}i, \ a, b \in \mathbb{Z}\}$.

$a = 4$

$n = x^2 + 4y^2$

$n = x^2 + (2y)^2$

$n = x^2 + z^2$ (ahol z páros szám)

$\Rightarrow$ a két-négyzetszám-problémára redukálható.

$a = 5$:

$$n = x^2 + 5y^2$$

$$n = \underbrace{(x + \sqrt{5}iy)}_{\in \mathbb{Z}(\sqrt{5}i)} \underbrace{(x - \sqrt{5}iy)}_{\in \mathbb{Z}(\sqrt{5}i)}.$$

Itt $\mathbb{Z}[\sqrt{5}] = \{f(\sqrt{5}) : \ f(x) \in \mathbb{Z}[x]\} = \{a + b\sqrt{5}i, \ a, b \in \mathbb{Z}\}$.

Tehát találunk olyan α algebrai egészet, hogy $\mathbb{Z}[\alpha]$-ban vizsgálódunk.

1. $\mathbb{Z}(\alpha)$-ban $\exists$ egyértelmű prímfelbontás (ehhez elég (de nem szükséges): létezik maradékos osztás $\Rightarrow \mathbb{Z}(\alpha)$ euklideszi gyűrű $\Rightarrow \exists$ Számelmélet Alaptétele). Ekkor $\mathbb{Z}(\alpha)$-ban kiépíthető számelmélet, mehetünk tovább mint a Gauss-egészeknél).

2. $\mathbb{Z}(\alpha)$-ban nem létezik egyértelmű prímfelbontás. (nem létezik hagyományos értelemben számelmélet – nehezebb, visszatérünk.)

Visszatérve $x^2 + 2y^2 = n$-re, egyszerűség kedvéért szorítkozzunk $n = p$ prím esetre:

$$x^2 + 2y^2 = p.$$

Meg fogjuk állapítani, hogy ez mely p prímekre oldható meg.

Mint ahogy $x^2+y^2 = p$, $z^2 \equiv -1 \pmod{p}$ megoldhatóságával kapcsolatos, ez $z^2 \equiv -2 \pmod{p}$-vel.

Valóban, ha $x^2 + y^2 = p$, akkor $x^2 \equiv -y^2 \pmod{p}$, azaz -1 kvadratikus maradék modulo p. Hasonlóan, ha $x^2 + 2y^2 = p$, akkor $x^2 \equiv -2y^2 \pmod{p}$, azaz -2 kvadratikus maradék modulo p.

Tehát most az $x^2+2y^2 = p$ egyenletet akarjuk megoldani, ahol p prím, és $\mathbb{Z}(\sqrt{2}i)$-ben vizsgálódunk. Kérdés: alaptételes-e? Ehhez elég lenne euklideszi, azaz felidézzük a 6.14 Definíciót:

8.1 Definíció. *Az E integritási tartományt (= kommutatív, nullosztó mentes gyűrű) euklideszi gyűrűnek mondjuk, ha $\exists$ olyan $\varphi : (E \setminus \{0\}) \to \mathbb{N}$ leképezés, amely rendelkezik a következő tulajdonságokkal:*

1. *$a, b \in E$, $b \neq 0$ esetén $\exists\, q, r$ hogy*

$$a = bq + r \quad \text{és vagy } r = 0, \text{ vagy } \varphi(r) < \varphi(b);$$

2. *$a, b \in E$, $a \neq 0$, $b \neq 0$ esetén*

$$\varphi(ab) \geq \varphi(a).$$

Pl. $\mathbb{Z}$-ben ilyen norma $\varphi(n) = |n|$, a Gauss-egészek körében pedig $\varphi(\alpha) = \varphi(a + bi) = a^2 + b^2 = |\alpha|^2$. Ha $E = T[x]$ polinomgyűrű, akkor $\varphi(f(x)) = \deg f(x)$.

Most

$$E = \mathbb{Z}(\sqrt{2}i) = \{a + bi\sqrt{2} : \ a, b \in \mathbb{Z}\}.$$

Kérdés tehát: ez euklideszi-e? Ehhez egy 8.1 definícióbeli φ norma kell.

Akárcsak Gauss-egészeknél, most is

$$\varphi(\alpha) = |\alpha|^2$$

-t veszünk, tehát

$$\varphi(\alpha) = \varphi(a + b\sqrt{2}i) = |\alpha|^2 = |a + bi\sqrt{2}|^2 = a^2 + 2b^2,$$

és ezt most is $N(\alpha)$-val fogjuk jelölni, tehát

$$N(\alpha) = N(a + b\sqrt{2}i) = |\alpha|^2 = a^2 + 2b^2.$$

Jó-e ez a φ?

$$\varphi : \ \mathbb{E} \setminus \{0\} \to \mathbb{N}$$

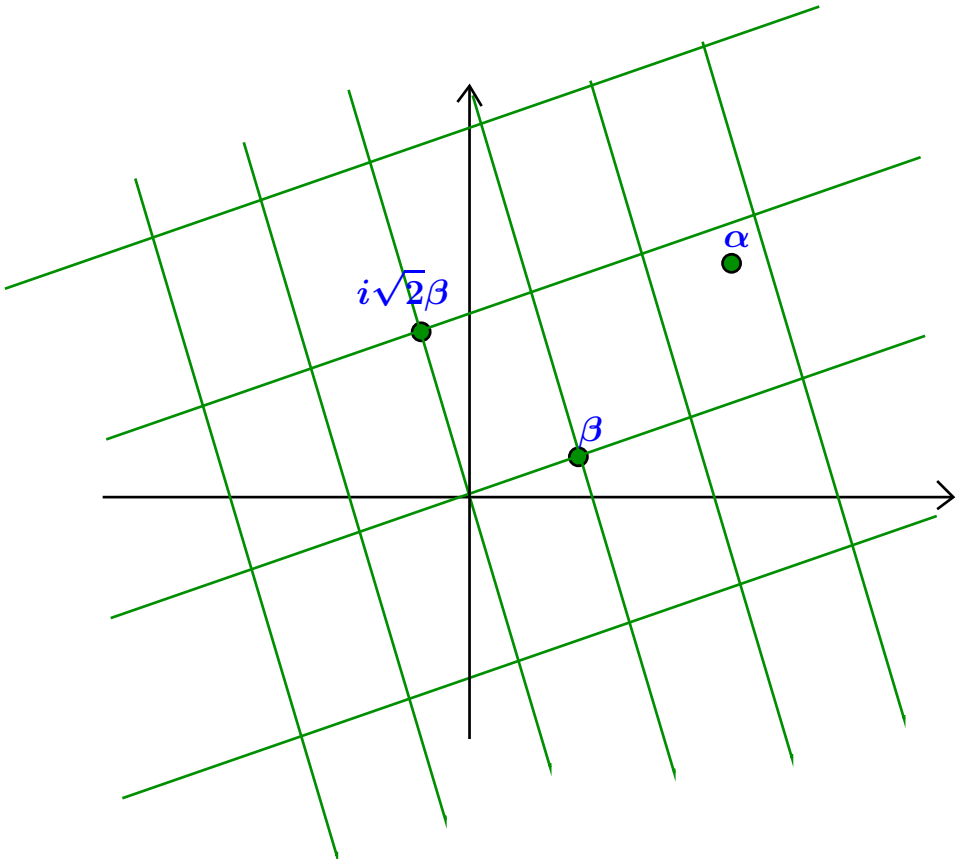
nyilvánvaló, és $\varphi(\alpha\beta) > \varphi(\alpha)$ is.

Marad: $\alpha, \beta \in \mathbb{Z}(\sqrt{2}i)$, $\beta \neq 0$-hoz létezik-e γ, δ, hogy

$$\alpha = \beta\gamma + \delta \quad \text{és} \quad \varphi(\delta) < \varphi(\beta),$$

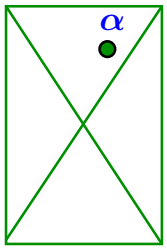
azaz létezik-e maradékos osztás, és így eukleidészi algoritmus is?

Ehhez ábrázoljuk β-nak a $\beta\gamma$ alakú többszöröseit (ahol $\gamma \in \mathbb{Z}[\sqrt{2}i]$) a komplex számsíkon:



1. ábra.

A fenti rácsban α beleesik valamelyik kis téglalapba. Az alábbiakban elforgatva látjuk a fenti téglalapot:



Vegyük $\beta\gamma$-nak a fenti téglalap α-hoz legközelebbi csúcsát (ha több ilyen is van, akkor az egyik csúcsot jelöljük ki). Legyen δ pedig az $\alpha - \beta\gamma$.

Ez a γ és δ megfelel a maradékos osztás feltételeinek, hiszen

$|\delta| \leq$ mint a téglalap átlója hosszának a fele, ami a Pitagorasz-tétel szerint $\frac{1}{2}\sqrt{|\beta|^2 + |\sqrt{2}\beta|^2} = \frac{\sqrt{3}}{2}|\beta|$.

Így $N(\delta) = \frac{3}{4}|\beta|^2 < |\beta|^2 = N(\beta)$.

Tehát létezik maradékos osztás, így létezik eukleidészi algoritmus. Van legnagyobb közös osztó. Azaz prímek és felbonthatatlanok azonosak.

Ezt felhasználva igazoljuk, hogy:

8.2 Tétel. *Legyen p prím, ekkor*

$$x^2 + 2y^2 = p \tag{8.1}$$

akkor és csak akkor oldható meg, ha $p = 2$, $8k + 1$ vagy $8k + 3$.

A 8.2 Tétel bizonyítása (vázlat). Azt már láttuk, hogy ha (8.1) megoldható, akkor $p = 2$ vagy $x^2 \equiv -2y^2 \pmod{p}$ miatt -2 kvadratikus maradék, azaz $p = 8k + 1$ vagy $8k + 3$ alakú.

Ha $p = 2$, akkor (8.1) megoldható: $x = 0$, $y = 1$.

Marad annak a bizonyítása, hogy ha p egy $8k + 1$ vagy $8k + 3$ alakú prím, akkor is megoldható (8.1).

A következőkben felsorolunk pár lemmát, amelyek bizonyítása házifeladat.

8.3 Lemma. *A norma multiplikatív. Továbbá, ha $\alpha, \beta \in \mathbb{Z}(\sqrt{2}i)$ esetén $\alpha \mid \beta$ teljesül $\mathbb{Z}[\sqrt{2}i]$-ben, akkor $N(\alpha) \mid N(\beta)$ $\mathbb{Z}$-ben (de fordítva nem feltétlen).*

8.4 Lemma. *$\varepsilon \in \mathbb{Z}(i\sqrt{2})$ egység $\Leftrightarrow$ $N(\varepsilon) = 1 \Leftrightarrow$ $\varepsilon = \pm 1$.*

8.5 LEMMA. *Ha* $p = 8k + 1$ *vagy* $8k + 3$, *akkor* $\exists\, z \in \mathbb{Z}$, *hogy*

$$z^2 + 2 \equiv 0 \pmod{p}.$$

Az első nehezebb lemma a következő:

8.6 LEMMA. *Ha* $p = 8k+1$ *vagy* $8k+3$ *alakú racionális prím, akkor* p *nem prím* $\mathbb{Z}(\sqrt{2}i)$*-ben.*

A 8.6 Lemma bizonyítása. Indirekt úton, tegyük fel, hogy létezik ilyen racionális p prím, amely prím $\mathbb{Z}[\sqrt{2}i]$-ben is.

Mivel p prím $8k + 1$ vagy $8k + 3$ alakú, a 8.5 Lemma alapján létezik z racionális egész amelyre

$$p \mid z^2 + 2 = (z + \sqrt{2}i)(z - \sqrt{2}i).$$

Mivel p prím $\mathbb{Z}[\sqrt{2}i]$-ben, feltehetjük, hogy $p \mid z + \sqrt{2}i$ vagy $p \mid z - \sqrt{2}i$. Jelöljük ezt úgy most, hogy $p \mid z \pm \sqrt{2}i$.

Ekkor $\exists\, u + vi\sqrt{2} \in \mathbb{Z}(\sqrt{2}i)$, azaz $u, v \in \mathbb{Z}$, amelyre:

$$p(u + v\sqrt{2}i) = z \pm \sqrt{2}i$$
$$pv = \pm 1$$
$$p \mid 1,$$

ami ellentmond p racionális prím voltának.

A tétel bizonyításához az utolsó lemma:

8.7 LEMMA. *Ha* $p = 8k + 1$ *vagy* $8k + 3$, *akkor* p *felbontható* $\mathbb{Z}(\sqrt{2}i)$*-ben, mint*

$$p = \alpha\beta,$$

ahol

$$N(\alpha) = N(\beta) = p.$$

A 8.7 Lemma bizonyítása. A 8.6 Lemma miatt p nem prím $\mathbb{Z}[\sqrt{2}i]$-ben, azaz $\exists$ nem triviális felbontása: $p = \alpha\beta$, ahol $\alpha,\ \beta$ nem egység. Ekkor

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Mivel $\alpha,\ \beta$ nem egység $N(\alpha),\ N(\beta) > 1$, amiből adódik a lemma állítása.

A 8.2 Tétel bizonyításának befejezése. A 8.7 Lemma miatt $\exists\ \alpha, \beta \in \mathbb{Z}[\sqrt{2}i]$, hogy

$$\alpha\beta = p,$$

és $N(\alpha) = N(\beta) = p$. Legyen $\alpha = u + v\sqrt{2}i$. Ekkor $p = N(\alpha) = u^2 + 2v^2$. Ezzel igazoltuk, hogy (8.1) megoldható.

Ezzel most az $x^2 + 2x^2 = p$ egyenlet megoldhatóságának vizsgálatát befejeztük. De vajon általánosítható-e ez az elmélet tovább, pl. $x^2 + 3y^2 = p$-re?

A következő tételt nem bizonyítjuk precízen, csak nagyjából megnézzük, hogy működik-e a $\mathbb{Z}[\sqrt{2}i]$ esetében tanult módszer. (Természetesen a tétel igaz.)

8.8 TÉTEL. *Legyen p prím, ekkor az*

$$x^2 + 3y^2 = p \tag{8.2}$$

akkor és csak akkor oldható meg, ha

$$z^2 + 3 \equiv 0 \pmod{p}$$

megoldható, azaz $p = 3$, p egy $12k + 1$ vagy $12k + 7$ alakú prím.

A 8.8 Tétel bizonyítása (vázlat). A tétel egyik iránya triviális. Valóban, ha (8.2) megoldható, és x_0, y_0 jelöl egy megoldást, akkor

$0 < x_i, y_0 < p$, így $(x_0, p) = (y_0, p) = 1$. Jelölje y_0 inverzét mod p y_0^*. Ekkor

$$\begin{aligned} x_0^2 + 3y_0^2 &= p \\ x_0^2 + 3y_0^2 &\equiv 0 \pmod{p} \\ (x_0 y_0^*)^2 + 3(y_0 x_0^*)^2 &\equiv 0 \pmod{p} \\ (x_0 y_0^*)^2 + 3 &\equiv 0 \pmod{p}, \end{aligned}$$

azaz $z^2 + 3 \equiv 0 \pmod{p}$ megoldható, hiszen $z = x_0 y_0^*$ megoldás.

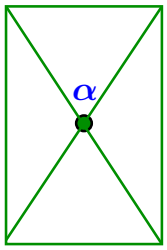
A tétel másik iránya nehezebb. Vajon működik-e ott is a $\mathbb{Z}[\sqrt{2}i]$ esetén tanult módszer?

Legyen most is $N(\alpha) = \alpha\overline{\alpha}$, azaz $\alpha = a + b\sqrt{3}i$ esetén $N(\alpha) = a^2 + 3b^2$.

A főkérdés, hogy $\mathbb{Z}[\sqrt{3}i]$ esetén létezik-e maradékos osztás, azaz $\mathbb{Z}[\sqrt{3}i]$ gyűrű eukleidészi-e?

A 1. Ábrához hasonlóan most is készíthetünk egy rácsot β többszöröseivel, és α ugyanúgy beleesik valamelyik kis téglalapba mint az előbb.

Csakhogy most a kis téglalap oldal hosszai $|\beta|$ és $\sqrt{3}|\beta|$, ezért (Pitagorasz-tétel szerint) az átló hosszának a fele pont $|\beta|$ lesz.



Vagyis, ha α pont az átlók metszetébe esik, akkor ezzel a normával nincs maradékos osztás, nincs eukleidészi algoritmus.

Vajon a helyzet megmenthető? Szerencsére igen, legyen ρ a primitív harmadik egységgyökök valamelyike, pl.

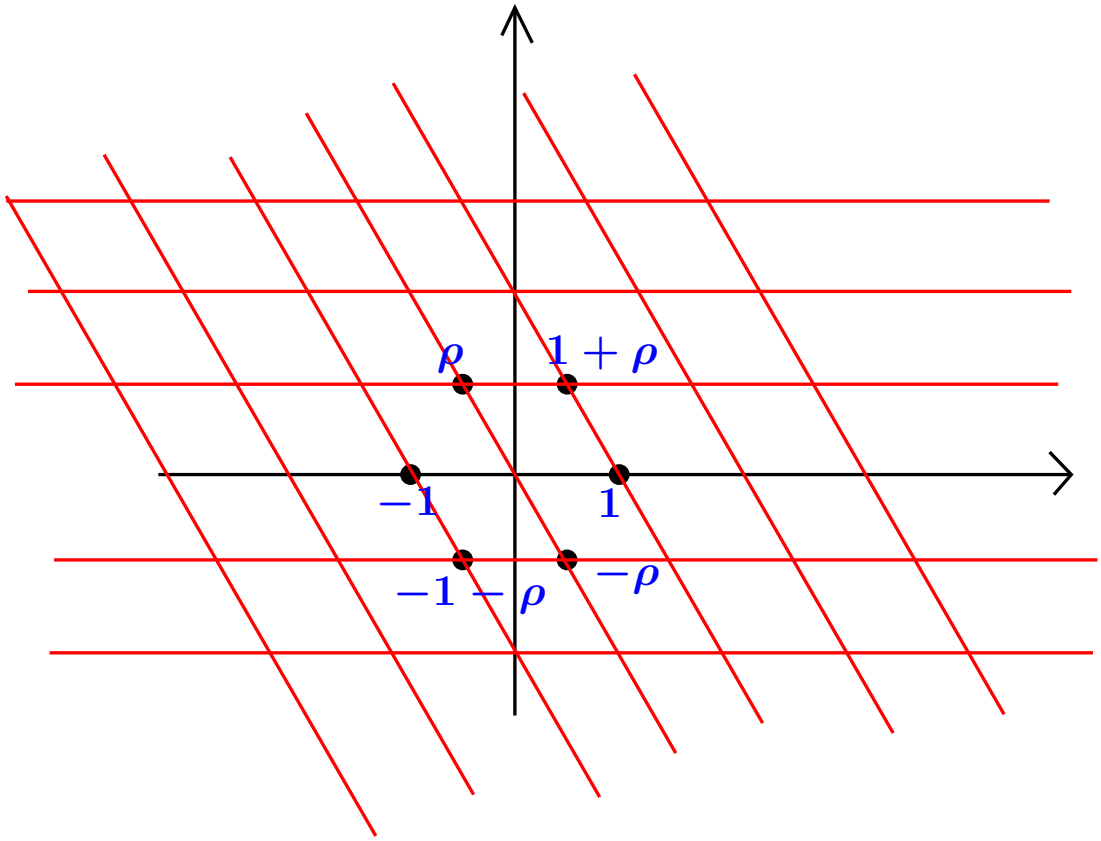
$$\rho = -\frac{1}{2} + \frac{\sqrt{3}i}{2} = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i.$$

Ekkor $\mathbb{Z}(\sqrt{3}i)$ helyett $\mathbb{Z}(\rho)$-t tanulmányozzuk.

Könnyen látható, hogy $\mathbb{Z}(\rho)$ gyűrű, amelyre:

$$\mathbb{Z}(\rho) = \{x + y\rho : \ x, y \in \mathbb{Z}\}$$
$$\mathbb{Z}(\rho) = \{\frac{a}{2} + \frac{b}{2}\sqrt{3}i, \ a \equiv b \pmod 2\}$$

$\mathbb{Z}(\rho)$ elemeit a következő ráccsal szemléltethetjük:



$\mathbb{Z}(\rho)$ elemeit Euler-egészeknek hívjuk. Itt is definiálhatunk egy normát a következővel:

8.9 DEFINÍCIÓ. *Legyen $\alpha = a + b\rho$ egy Euler-egész. Ekkor*

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 - ab.$$

Hasonlóan a Gauss-egészekhez, $\mathbb{Z}(\rho)$-ban azok az ε elemek az egységek, amelyekre $N(\varepsilon) = 1$. Ez az egységkör és az előbbi rács elemeinek metszete: 1, -1, ρ, $-\rho$, $1+\rho$, $-1-\rho$. Másképpen a hatodik egységgyökök.

Könnyen látható, hogy $\mathbb{Z}(\rho)$ elemeit a következőképpen is felírhatjuk:

$$\mathbb{Z}(\rho) = \{\varepsilon(a + b\sqrt{3}i) : \ a, b \in \mathbb{Z}, \ \varepsilon \text{ Euler egység } \}. \qquad (8.3)$$

Valóban, ha $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{3}i$ alakú szám, ahol a és b páros, az állítás triviális.

Ha a, b páratlan, akkor pedig $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{3}i$ számra

$$\alpha = (1+\rho)\left(\frac{a+3b}{4} + \frac{b-a}{4}\sqrt{3}i\right) = \rho\left(\frac{3b-a}{4} - \frac{a+b}{4}\sqrt{3}i\right),$$

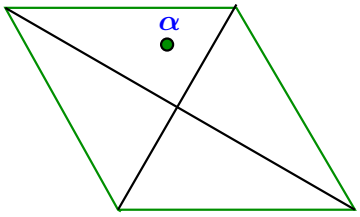
és valamelyik felírásban az együtthatók egészek.

A $\mathbb{Z}(\rho)$ gyűrű eukleidészi, hiszen van maradékos osztás. A bizonyítás nagyon hasonló $\mathbb{Z}(\sqrt{2}i)$-hez, itt csak vázoljuk. Adott $\alpha, \beta \neq 0 \in \mathbb{Z}(\rho)$-hoz kell $\gamma, \delta \in \mathbb{Z}(\rho)$, hogy

$$\alpha = \beta\gamma + \delta, \quad N(\delta) < N(\beta).$$

Valóban egy β elem többszöröseit ábrázolva egy rombusz rácsot kapunk (hasonlóan a $\mathbb{Z}(\sqrt{2}i)$-ben ábrázoltakhoz, csak a kis téglalapokat kis rombuszok helyettesítik), ahol a kis rombuszok szögei $60°$ és $120°$.

Az egyik kis rombuszba beleesik α. Ezt elforgatva ábrázoljuk:



Ebbe a rombuszba esik bele α, és α távolsága a legközelebbi csúcstól (amely csúcs lesz $\beta\gamma$) $\leq$ mint a hosszabbik átló fele, ami kisebb mint a rombusz oldala: $|\beta|$. Ebből pedig már adódik az állítás.

Vagyis $\mathbb{Z}[\sqrt{3}i]$-ben van maradékos osztás, így létezik euklideszi algoritmus, prímek és felbonthatatlanok egybeesnek. Így itt is igaz a számelmélet alaptétele:

8.10 TÉTEL. *Az egységtől és 0-tól különböző Euler-egész az egységfaktoroktól és sorrendtől eltekintve egyértelműen felírható Euler-prímek szorzataként.*

Az Euler-prímek karakterizációjának bizonyítása megtalálható pl. a Freud-Gyarmati [1] és Gyarmati-Turán [2] könyvekben, mi csak bizonyítás nélkül említjük az ideavonatkozó tételeket. (De a bizonyítás nagyon hasonló a Gauss-egészeknél tanultakhoz.)

8.11 TÉTEL. *A $3k+2$ racionális prímek egyben Euler prímek is. A $3k+1$ alakú racionális prímek*

$$\pi\overline{\pi}$$

alakúak, ahol a π, $\overline{\pi}$ Euler prímek egymás konjugáltjai, de nem asszociáltak. Végül a 3 felbontása

$$3 = -\rho^2(1-\rho),$$

ahol $1-\rho$ Euler prím.

Azaz most már be tudjuk bizonyítani a 8.8 Tétel nehezebbik felét is, miszerint, ha $p = 12k + 1$ vagy $12k + 7$ alakú prím, akkor

$$x^2 + 3y^2 = p$$

megoldható. Valóban a p racionális prím prímtényezős felbontása Euler-egészek körében $p = \pi\overline{\pi}$. A (8.3) alakból látható, hogy π felírható $\pi = \varepsilon\left(x + i\sqrt{3}\right)y$ alakban, ahol ε Euler-egység, viszont $x, y \in \mathbb{Z}$. Ekkor:

$$\begin{aligned} p = \pi\overline{\pi} &= \varepsilon(x + \sqrt{3}iy)\overline{\varepsilon}(x - \sqrt{3}iy) \\ &= \varepsilon\overline{\varepsilon}(x + \sqrt{3}iy)(x - \sqrt{3}iy) = x^2 + 3y^2, \end{aligned}$$

és ezzel az állítást igazoltuk.

Az Euler-egészeknek van egy nagyon nevezetes alkalmazása, mégpedig az alábbi lemma segítségével igazolható a Fermat-sejtés $n = 3$ speciális esete.

Magát a sejtést, csak a következő fejezetben igazoljuk, azonban a szükséges lemma bizonyítása már most időszerű:

8.12 LEMMA. *Ha s páratlan és*

$$s^3 = u^2 + 3v^2$$

alakú, ahol $u, v \in \mathbb{Z}$ és $(u, v) = 1$, akkor s, u, v felírható

$$\begin{aligned} s &= e^2 + 3f^2 \\ u &= e(e^2 - 9f^2) \\ v &= 3f(e^2 - f^2) \end{aligned}$$

alakban, ahol $e, f \in \mathbb{Z}$, sőt $(e, f) = 1$.

Ha meggondoljuk a fenti tétel kissé hasonlít a primitív pitagoraszi számhármasok paraméteres alakjára, csak azzal a különbséggel, hogy a szorzattá bontás most nem $\mathbb{Z}$-ben, hanem $\mathbb{Z}(\sqrt{3}i)$-ben történik. Lássuk a precíz bizonyítást.

A 8.12 Lemma bizonyítása. Írjuk fel s^3-öt

$$s^3 = (u + \sqrt{3}iv)(u - \sqrt{3}iv)$$

alakban. Ez egy szorzattá bontás $\mathbb{Z}[\rho]$-ban, és a fenti számkörben $u+\sqrt{3}iv$ és $u-\sqrt{3}iv$ relatív prímek. Jelölje ugyanis d az $u+\sqrt{3}iv$ és $u - \sqrt{3}iv$ számok legnagyobb közös osztóját $\mathbb{Z}(\rho)$-ban. Ekkor

$$d \mid (u + \sqrt{3}iv) + (u - \sqrt{3}iv) = 2u$$
$$d \mid (u + \sqrt{3}iv) - (u - \sqrt{3}iv) = 2\sqrt{3}iv.$$

De 2 Euler-prím ($3k + 2$ alakú), $2 \nmid d$ (hiszen, ha $2 \mid d$, akkor $2 \mid u + \sqrt{3}iv \;\Rightarrow\; 2 \mid u^2 + 3v^2 = s^3 \;\Rightarrow\; s$ nem lehet páratlan szám), azaz 2 és d relatív prímek. Vagyis

$$d \mid u, \sqrt{3}iv \tag{8.4}$$

Kicsit hasonlóan látható, hogy $(d, \sqrt{3}i) = 1$, hiszen $\sqrt{3}i$ Euler prím, és ha $\sqrt{3}i \mid d$, akkor

$$\sqrt{3}i \mid u + \sqrt{3}iv,\; u - \sqrt{3}iv,$$
$$3 \mid u^2 + 3v^2 \quad \text{az Euler egészek körében}$$
$$3 \mid s^3 \quad \text{az Euler egészek körében}$$
$$3 \mid s^3 \quad \mathbb{Z}\text{-ben}$$
$$9 \mid s^3 \quad \mathbb{Z}\text{-ben}$$
$$9 \mid u^2 + 3v^2 \quad \mathbb{Z}\text{-ben}$$

$3 \mid u \quad \mathbb{Z}$-ben

$9 \mid u^2 \quad \mathbb{Z}$-ben

$9 \mid 3v^2 \quad \mathbb{Z}$-ben

$3 \mid v \quad \mathbb{Z}$-ben

$3 \mid (u, v) \quad \mathbb{Z}$-ben,

ami ellentmondás. Vagyis $(d, \sqrt{3}i) = 1$ és (8.4) miatt $d \mid v \Rightarrow d \mid (u, v) = 1$. Tehát $d = 1$ és ez azt jelenti, hogy $u + \sqrt{3}iv$ és $u - \sqrt{3}iv$ relatív prímek.

Írjuk fel

$$s^3 = (u + \sqrt{3}iv)(u - \sqrt{3}iv)$$

számot mint Euler prímek szorzatát. Az nem lehet, hogy egy Euler prím mindkét szorzótényezőt osztja, ezért mindkét szorzótényezőben minden prímtényező 3-mal osztható kitevőn szerepel. Vagyis $u + \sqrt{3}iv$ és $u - \sqrt{3}iv$ is egy-egy Euler egész köbének egységszerese.

Mivel $\mathbb{Z}(\rho)$ elemei felírhatóak (8.3) alakban, ezért az eddigiek alapján

$$u + \sqrt{3}iv = \varepsilon(e + \sqrt{3}if)^3 \tag{8.5}$$

alakú, ahol ε Euler egység és $e, f \in \mathbb{Z}$. Mennyi lehet ε értéke? (8.5) alapján

$$\overline{\varepsilon}(u + \sqrt{3}iv) = (e + \sqrt{3}if)^3 = g + \sqrt{3}ih, \tag{8.6}$$

ahol $g, h \in \mathbb{Z}$. Ha ε Euler egység $\varepsilon = \pm\frac{1}{2} \pm \frac{\sqrt{3}i}{2}$ alakú, akkor

$$\overline{\varepsilon}(u + \sqrt{3}iv) = (\pm\frac{1}{2} \pm \frac{\sqrt{3}i}{2})(u + \sqrt{3}iv) = \frac{\pm u \pm 3v}{2} + \frac{\pm u \pm v}{2}$$

alakú. De most u és v paritása különböző, hiszen $s^3 = u^2 + 3v^2$ páratlan szám. Azaz $\frac{\pm u \pm 3v}{2}$, $\frac{\pm u \pm v}{2}$ nem egészek, és ez ellentmond (8.6) felírásnak.

Vagyis $\overline{\varepsilon}$ egység csak ± 1 lehet, és így $\varepsilon = \pm 1$. Az e és f számok előjelének megfelelő választásával elérhető, hogy

$$u + \sqrt{3}iv = (e + \sqrt{3}if)^3, \tag{8.7}$$

ahonnan

$$u = e^3 - 9ef^2 = e(e^2 - 9f^2)$$
$$v = 3fe^2 - 3f^3 = 3f(e^2 - f^2),$$

és ezzel a paraméteres alakot a lemma állításában igazoltuk. $(u, v) = 1$-ből pedig azonnal következik $(e, f) = 1$.

Térjünk vissza $s = x^2 + ay^2 = n$ egyenlet vizsgálatára.

Ha $a = 4$, akkor

$$\underbrace{x^2 + (2y)^2}_{\text{két négyzetszám összege}} = n,$$

így az $x^2 + y^2 = n$ egyenletre redukálható.

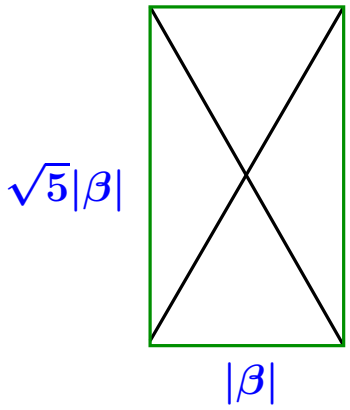
Következik $x^2 + 5y^2 = n$ egyenlet.

Most is, az első kérdés vajon létezik-e maradékos osztás? Az első természetesen adódó norma amivel próbálkozunk:

$$N(\alpha) = \alpha\overline{\alpha} = a^2 + 5b^2,$$

ha $\alpha = a + \sqrt{5}ib$, ahol a, b egész számok.

A szokásos kis téglalap most:



Látható ebben az átló fele nagyobb mint a kisebbik oldal, így az eddig jól működő stratégiánk most nem vált be...

Nem lehet ezen valahogy segíteni? Pl. más normával? Sajnos nincs ilyen...

Amennyiben $\mathbb{Z}(\sqrt{5})$-ben nem létezik egyértelmű felbontás felbonthatatlanokra, más normával sincs maradékos osztás (hiszen ha van eukleidészi algoritmus, akkor van számelmélet alaptétele is).

Más szóval a következőt szeretnénk: $\exists\, \mathbb{Z}(\sqrt{5}i)$-beli szám, mely legalább kétféleképpen bontható fel felbonthatatlanokra.

(Ez még nem teljesen elég; elvben lehetne, hogy egy bővebb gyűrűben mint $\mathbb{Z}(\sqrt{5}i)$-ben (hasonlóan az Euler-egészek) ezek tovább bomlanak ugyanarra a felbontásra; nem így van, de nem megyünk bele. Most csak azt látjuk be, hogy $\mathbb{Z}(\sqrt{5}i)$-ben nincs egyértelmű felbontás.)

8.13 TÉTEL. *A 6 számnak a $6 = 2\cdot 3$ és a $6 = (1+\sqrt{5}i)(1-i\sqrt{5})$ két lényegesen különböző felbontása $\mathbb{Z}(\sqrt{5}i)$-beli felbonthatatlanokra.*

A 8.13 Tétel bizonyítása. Most is legyen $N(\alpha) = N(a+b\sqrt{5}i) = |\alpha|^2 = a^2 + 5b^2$. (Bár most nem fog működni a maradékos osztás a fenti definícióval, de ez a norma enélkül is fontos.)

A norma nemnegatív egész, és multiplikatív: $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$.

Ekkor $\alpha \mid \beta$ esetén $N(\alpha) \mid N(\beta)$.

ε most is pont akkor egység, ha $N(\varepsilon) = 1$, azaz $\varepsilon = \pm 1$.

Ebből adódóan a két felbontás lényegesen különböző (nemcsak sorrendben és egységszorzókban térnek el).

Marad $2, 3, 1 + \sqrt{5}i$, $1 - \sqrt{5}i$ mind felbonthatatlanok.

Ezek közül most csak azt igazoljuk, hogy a 2 felbonthatatlan. A bizonyítás ugyanúgy működik a többi tényezőre is.

Tegyük fel, hogy

$$2 = \alpha\beta \qquad \text{ahol } \alpha, \beta \text{ nem egység}$$
$$N(\alpha), N(\beta) \mid N(2) = 4$$

Itt α, β nem egység, tehát $N(\alpha), N(\beta) \neq 1$. Azaz

$$N(\alpha) = N(\beta) = 2$$

Ha $\alpha = x + \sqrt{5}iy$ alakú $x, y \in \mathbb{Z}$, akkor ebből azt kapjuk, hogy

$$x^2 + 5y^2 = 2,$$

aminek nincs racionális egészekből álló megoldása.

Tehát $\mathbb{Z}(\sqrt{5}i)$-ben nem létezik legnagyobb közös osztó. Mit lehet helyette csinálni, mivel lehetne helyettesíteni? Erre a kérdésre adott választ Dedekind.

A Dedekind-féle ideálelmélet a mélyebb algebrai számelmélet alapja.

Alapötlet: Ha valamely E gyűrű euklideszi, azaz létezik benne maradékos osztás $\Rightarrow$ $\exists$ legnagyobb közös osztó, és az felírható a két elem lineáris kombinációjaként.

$$(\alpha, \beta) = \gamma\alpha + \delta\beta \qquad \text{, ahol } \gamma, \delta \in E.$$

Tetszőleges $\Psi \in E$-re szorozva Ψ-vel

$$\Psi(\alpha, \beta) = \Psi\gamma\alpha + \Psi\delta\beta$$

Azaz (α, β) minden többese felírható α, β (E-beli együtthatós) lineáris kombinációjaként.

Másrészt, ha vesszük α, β bármely lineáris kombinációját, akkor

$$(\alpha, \beta) \mid \lambda\alpha + \mu\beta.$$

Így

$$\underbrace{\{\Psi(\alpha, \beta) : \Psi \in E\}}_{\substack{\text{Ha } E\text{-ben } \nexists \text{ lnko} \\ \text{erről nem beszélhetünk}}} = \underbrace{\{\lambda\alpha + \mu\beta : \lambda, \mu \in E\}}_{\text{de erről akkor is!}}$$

A legnagyobb közös osztó helyettesíthető ilyenek, ún. ideálok vizsgálatával (pontosabban: az ún. α, β által generált ideálok vizsgálatával).

Ideálok körében lehet számelméletet kiépíteni $\Rightarrow$ Dedekind-féle ideálelmélet $\Rightarrow$ algebrai számelmélet.

Hivatkozások

[1] Freud Róbert, Gyarmati Edit, *Számelmélet*, link.

[2] Gyarmati Edit, Turán Pál, *Számelmélet*, link.

[3] Kép, Julius Wilhelm Richard Dedekind, .

9. Fermat tétel $n = 3$ esetén

1753-ban Euler küldött egy levelet Goldbach-nak, amelyben azt állította, hogy megoldotta a Fermat-sejtést az $n = 3$ esetben. Ezt az eredményt Euler 1770-ben publikálta.

Azóta sokan adtak további bizonyításokat az $n = 3$ estre, így pl. Kausler, Legendre, Calzolari, Lamé, Tait, Günther, Gambioli, Krey, Rychlik, Stockhaus, Carmichael, van der Corput, Thue és Duarte.

A kapcsolódó referenciákat az olvasók a következő Wikipédia oldalon találhatják: [3], ahonnan is, mi is ismertetni fogjuk Euler bizonyításának egy mai változatát. (Ha a neten rákeresünk sok helyen olvashatjuk, hogy Euler eredeti bizonyítása kissé hiányos volt, ennek a hírnek az eldöntését az olvasóra bízzuk.)

Szerencsére, az alábbi bizonyítás, a 8.12 Lemmától eltekintve, teljesen elemi.

A végtelen leszállás módszerét alkalmazzuk. Tegyük fel, hogy az $x^3+y^3+z^3 = 0$ egyenletnek létezik megoldása a nullától különböző egészek körében.

Vegyünk a megoldások közül egy olyat, amire $\max\{|x|, |y|, |z|\}$ minimális. Találni fogunk egy olyan k, ℓ, m megoldást, amelyre

$k^3 + l^3 + m^3 = 0$ és $\max\{|k|, |\ell|, |m|\} < \max\{|x|, |y|, |z|\}$, és ez ellentmondás.

Az világos, hogy a legkisebb megoldás esetén $(x, y) = (x, z) = (y, z) = 1$. Tudjuk azt is, hogy x, y, z között két páratlan van és egy páros. Szimmetrikus okokból feltehetjük, hogy a páros szám z, x, y pedig páratlan. Definiáljuk u-t és v egész számokat:

$$u = \frac{x+y}{2}$$
$$v = \frac{x-y}{2}$$

képlettel. Ekkor $(u, v) = 1$ mivel $(x, y) = 1$ és

$$x = u + v$$
$$y = u - v.$$

Mivel x páratlan, u és v paritása különböző. Továbbá:

$$\begin{aligned} -z^3 &= x^3 + y^3 \\ &= (u+v)^3 + (u-v)^3 \\ &= 2u(u^2 + 3v^2). \end{aligned} \tag{9.1}$$

Az u és v paritása különböző: $u^2 + 3v^2$ páratlan szám. Sőt, z páros volta miatt $8 \mid -z^3 = 2u(u^2 + 3v^2)$, amiből adódóan u a páros, és v a páratlan.

Tehát $(2u, u^2 + 3v^2)$ csak 1 vagy 3 lehet $(u, v) = 1$ miatt. A továbbiakban két esetet különböztetünk meg aszerint, hogy $(2u, u^2 + 3v^2)$ értéke 1 vagy 3.

I. eset: $(2u, u^2+3v^2) = 1$. Ekkor $-z^3 = 2u(u^2+3v^2)$-ből adódóan

$$2u = r^3$$

$$u^2 + 3v^2 = s^3$$

alakú, ahol $r, s \in \mathbb{Z}$. Ez azonban a 8.12 Lemma miatt csak úgy lehet, ha

$$s = e^2 + 3f^2$$
$$u = e(e^2 - 9f^2)$$
$$v = 3f(e^2 - f^2)$$

alakú, ahol $e, f \in \mathbb{Z}$. Mivel $(u, v) = 1$ ezért $(e, f) = 1$. Mivel u páros, v páratlan, ezért e páros és f páratlan. Így

$$r^3 = 2u = 2e(e - 3f)(e + 3f).$$

A $2e, e-3f, e+3f$ számok páronként relatív prímek, mert $(e, f) = 1$, $2 \nmid e - 3f$ és $3 \nmid e$ (ha $3 \mid e$ teljesülne, akkor $3 \mid u$, így $3 \mid u, v$, ami ellentmond $(u, v) = 1$-nek). Azaz:

$$-2e = k^3,$$
$$e - 3f = \ell^3$$
$$e + 3f = m^3.$$

Ekkor $k^3 + \ell^3 + m^3 = 0$ tehát találtunk egy kisebb megoldását a Fermat egyenletnek. Valóban $|e| \geq 3, |f| \geq 1$ (különben nem adnak köbszámot egyszerre $2e$, $e - 3f$ és $e + 3f$), így

$$\max\{|k|, |\ell|, |m|\} \leq \max\{2|e|, |e| + 3|f|\} < e^2 + 3f^2 = s$$
$$= (u^2 + 3v^2)^{1/3} \leq |z| \leq \max\{|x|, |y|, |z|\}.$$

Ezzel ellentmondásra jutottunk; találtunk az eredetinél egy kisebb megoldást.

II. eset: $(2u, u^2 + 3v^2) = 3$. Ekkor $3 \mid u$, legyen tehát $u = 3w$, ahol $w \in \mathbb{Z}$. Mivel u páros, w is. $(u, v) = 1$, tehát $3 \nmid v$. Azaz

$$(6, v) = 1.$$

Az u helyébe $3w$-t írva a (9.1) képletből

$$-z^3 = 18w(3w^2 + v^2)$$

adódik. Mivel $1 = (u, v) = (u, 3w)$, ezért $(u, w) = 1$. $3w^2 + v^2$ nem osztható 3-mal és páratlan, tehát $(18w, 3w^2 + v^2) = 1$. Vagyis

$$\begin{aligned} 18w &= r^3, \\ 3w^2 + v^2 &= s^3. \end{aligned} \tag{9.2}$$

A 9.2 egyenletnek a 8.13 Lemma szerint van egy paraméteres felírása, mégpedig

$$\begin{aligned} s &= e^2 + 3f^2 \\ v &= e(e^2 - f^2) \\ w &= 3f(e^2 - f^2). \end{aligned}$$

Ekkor

$$r^3 = 18w = 3^3 \cdot 2f(e - f)(e + f).$$

Azaz $2f(e - f)(e + f)$ is köbszám. Mivel $(e, f) = 1$ ezért $2f$, $e + f$ és $e - f$ páronként relatív prímek. Így létezik k, ℓ, m egész számok, melyekre

$$\begin{aligned} -2f &= k^3 \\ e + f &= \ell^3 \\ f - e &= m^3, \end{aligned}$$

amelyekre $k^3 + \ell^3 + m^3 = 0$ tehát találtunk egy kisebb megoldását a Fermat egyenletnek. Valóban $|e| \geq 2, |f| \geq 1$ (különben nem adnak köbszámot egyszerre $2f$, $e + f$ és $e - f$), így

$$\max\{|k|, |\ell|, |m|\} \leq \max\{2|f|, |e| + |f|\} < e^2 + 3f^2 = s$$

$$= (3w^2 + v^2)^{1/3} \leq |z| \leq \max\{|x|, |y|, |z|\}.$$

Ezzel ellentmondásra jutottunk; találtunk az eredetinél egy kisebb megoldást.

Természetesen sok más egyszerűen követhető további bizonyítás létezik a Fermat sejtésre, pl. [1] és [2]-ben olyan bizonyítást találunk, amely bevezeti az Euler-egészek körében is a kongruenciát. Ez mindenképpen érdekes olvasmány, amely segítségével nagyobb jártasságra tehetünk szert diofantikus egyenletek megoldása során.

A diofantikus egyenletek kapcsán érdemes megemlíteni a debreceni diofantikus iskolát, ahol sok érdekes megoldási módszert tanítanak egyenletek egész megoldásainak megkeresésére.

Hivatkozások

[1] Freud Róbert, Gyarmati Edit, *Számelmélet*, link.

[2] Gyarmati Edit, Turán Pál, *Számelmélet*, link.

[3] Wikipédia, *Proof of Fermat's Last Theorem for specific exponents*, link.

10. Három négyzetszám-probléma

Térjünk vissza a két-négyzetszám-problémára:

$$x^2 + y^2 = n.$$

Ebből továbbmentünk egy irányban: $y^2 \to 2y^2, 3y^2$. Lehet más irányban is: a tagok (négyzetszámok) számát növelni 3 négyzetszámot véve:

$$x^2 + y^2 + z^2 = n.$$

Ennek megoldhatóságára vonatkozik a következő Legendre-tól származó tétel. A problémát később Gauss is vizsgálta.

10.1 TÉTEL. (3 négyzetszám, Legendre) *Egy $n \in \mathbb{N}$ szám akkor és csak akkor írható fel 3 négyzetszám összegeként, ha n nem $4^\alpha(8k+7)$ alakú (ahol α, k egészek).*

Legendre nevét a számelméletben a Legendre szimbólum örökíti meg, és talán kevésbé ismert, hogy a kvadratikus reciprocitási tételt is ő fogalmazta meg sejtésként (mielőtt Gauss bebizonyította), akárcsak a prímszámtételt (amelyet közel száz évvel később bizonyított Hadamard és de la Valée Poussin.)

A tétel kicsit más jellegű, és bizony az akkor és csak akkor állítás egyik iránya nagyon nehéz. A másik irány viszont egyszerű, modulo 8 vizsgálatokra vezetődik vissza. Ezt a könnyebb irányt mi is bebizonyítjuk most.

A 10.1 Tétel bizonyítása. a) $n = 4^\alpha(8k+7)$ nem írható fel: α-ra vonatkozó teljes indukcióval.

1. $\alpha = 0$-ra bizonyítandó:

$$x^2 + y^2 + z^2 \neq 8k + 7.$$

Nézzük a bal oldalt $\mod 8$:

$$x^2 + y^2 + z^2 = \left\{\begin{matrix}0\\1\\4\end{matrix}\right\} + \left\{\begin{matrix}0\\1\\4\end{matrix}\right\} + \left\{\begin{matrix}0\\1\\4\end{matrix}\right\} \not\equiv 7 \qquad (8),$$

vagyis $x^2 + y^2 + z^2$ lehet $0, 1, 2, \ldots, 6$, de 7 nem modulo 8. Ezzel az állítást (kongruenciamódszerrel) bebizonyítottuk.

2. Tegyük fel, hogy $\alpha \in \mathbb{N}$ és α helyen $0, 1, 2, \ldots, \beta - 1$-gyel igaz az állítás. Tegyük fel indirekten, hogy

$$x^2 + y^2 + z^2 = 4^\beta(8k+7)$$

Ekkor $4 \mid x^2 + y^2 + z^2$, de ez csak úgy lehet, ha x, y, z páros:

$$x = 2x_1, \quad y = 2y_1, \quad z = 2z_1.$$

Vagyis:

$$(2x_1)^2 + (2y_1)^2 + (2z_1)^2 = 4^\beta(8k+7)$$
$$x_1{}^2 + y_1{}^2 + z_1{}^2 = 4^{\beta-1}(8k+7)$$

Az indukciós feltevés miatt ez nem lehet, így ellentmondásra jutottunk.

b) $n \neq 4^\alpha(8k+7)$ felírható: nehéz, nem bizonyítjuk:

Hivatkozások

[1] Kép, Adrien-Marie Legendre, link.

11. Négy négyzetszám-probléma

A négy négyzetszám-probléma már Diophantosz műveiben is feltűnt, melyben példákat találunk egy-egy pozitív egész négy négyzetszám összegeként való felírására... Magát a sejtést azonban Bachet fogalmazta meg először miközben Diophantosz, Arithmetica című művét fordította latinra.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
AVCTORE CLAVDIO GASPARE, BACHETO
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via
Iacobea, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

A sejtést 150 évvel később Lagrange bizonyította be.

Lagrange 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.”

11.1 TÉTEL. (Négy négyzetszám-tétel, Lagrange) $\forall\, n \in \mathbb{N}$ *felírható* 4 *négyzetszám összegeként.*

A 11.1 Tétel bizonyítása. Gyakorlatilag minden bizonyítás három részből áll; az első kettő mindig ugyanaz, a harmadik, a legnehezebb sokféleképpen oldható meg.

A 11.2 Lemma még Eulertől származik:

11.2 LEMMA. *Ha két természetes szám felírható* 4 *négyzetszám összegeként, akkor a szorzatuk is.*

Ebből azonnal adódik a következő:

11.3 KÖVETKEZMÉNY. *Elég a* 4 *négyzetszám tételt* $n = p$ *prím esetben bebizonyítani.*

A 11.2 Lemma bizonyítása. Következik a következő azonosságból: Ha

$$r = a^2 + b^2 + c^2 + d^2,$$
$$s = x^2 + y^2 + z^2 + u^2,$$

akkor

$$t_1 = ax + by + cz + du,$$
$$t_2 = -ay + bx - cu + dz,$$
$$t_3 = az - bu - cx + dy,$$
$$t_4 = au + bz - cy - dx$$

-et írva

$$rs = {t_1}^2 + {t_2}^2 + {t_3}^2 + {t_4}^2.$$

Ennek bizonyítása HF. (Arról van szó, hogy egy $\alpha = a+bi+cj+dk$ kvaternió normáját $N(\alpha) = \alpha\overline{\alpha} = (a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2$-nel definiálva $N(\alpha\beta) = N(\alpha)N(\beta)$.)

A következőkben bebizonyítjuk, hogy minden p páratlan prímnek van olyan np többszöröse, amely előáll 4 négyzetszám összegeként, sőt igaz a következő:

11.4 LEMMA. *Legyen p prím, ekkor $\exists\, a, b \in \mathbb{Z}_p$, melyre*

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

A 11.4 Lemma bizonyítása. Tekintsük az

$$\mathcal{A} = \left\{ 1 + a^2 : 0 \le a \le \frac{p-1}{2} \right\} \quad \text{és}$$
$$\mathcal{B} = \left\{ -b^2 : 0 \le b \le \frac{p-1}{2} \right\}$$

halmazokat. Mindkét halmaz elemszáma $\frac{p+1}{2}$.

A skatulyaelv miatt $\exists\, a \in A$ és $b \in B$, hogy

$$a \equiv b \qquad (p).$$

Azaz $\exists\, 0 \le a \le \frac{p-1}{2}$ és $0 \le b \le \frac{p-1}{2}$, melyekre

$$1 + a^2 \equiv -b^2 \qquad (p).$$

Vagyis

$$p \mid 1 + a^2 + b^2.$$

Legyen $1 + a^2 + b^2 = np$. Ekkor $n > 0 \;\Rightarrow\; n \ge 1$. Továbbá:

$$np = 1 + a^2 + b^2 < 1 + 2 \cdot \left(\frac{p-1}{2} \right)^2 < p^2 \quad \Rightarrow \quad n < p.$$

Ezzel állításunkat beláttuk.

Az, hogy $p = 2$ és 3 előáll négy négyzetszám összegeként triviális, könnyű dolgunk van:

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$
$$3 = 1^2 + 1^2 + 1^2 + 0^2.$$

A bizonyítás legnehezebb része, hogy minden $p > 3$ prím előáll négy négyzetszám összegeként. Ezt sokféleképpen lehet, pl. geometriailag is (Minkowski tétel). Egy elemi megoldás található Erdős-Surányi [1] könyvben is, amely végtelen leszállást használ.

Mi most egy másik elemi bizonyítást ismertetünk, amely az ún. Thue-lemmára [2] épül (ennek a megközelítésnek azaz előnye, hogy ez is elemi és nem kell hosszú előkészítés).

11.5 Lemma. (Thue-lemma) *Legyen* $n, m \in \mathbb{N}$, $m \geq 2$, $u_1, \dots, u_n, v_1, \dots, v_n \in \mathbb{N}$, $u_1, \dots, u_n, v_1, \dots, v_n < m$ *és*

$$u_1 \cdots u_n v_1 \cdots v_n > m^n.$$

Legyen $(a_{i,j})$ *egy* $m \times n$ *egész elemekből álló mátrix. Ekkor* $\exists$ $x_1, \dots, x_n, y_1, \dots, y_n \in \mathbb{Z}$, *hogy*

$$\left.\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,n}x_n &\equiv y_1 \qquad (p) \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,n}x_n &\equiv y_n \qquad (p) \end{aligned}\right\} \tag{11.1}$$

és $|x_i| < u_i$, $|y_i| < v_i$ $(i = 1, 2, \dots, n)$, *valamint* $\exists\, x_i$, *hogy* $x_i \neq 0$ *(azaz létezik nem triviális „kicsi” megoldása* (11.1)*-nek).*

A 11.5 Lemma bizonyítása. Legyen

$$z_i \overset{\text{def}}{=} s_i - (a_{i,1}r_1 + \cdots + a_{i,n}r_n), \qquad i = 1, 2, \dots, n\text{-re},$$

ahol futtassuk s_i, r_j-ket úgy, hogy

$$r_i \in \{1, 2, \dots, u_i\}, \;\; s_j \in \{1, 2, \dots, v_j\}, \qquad i, j \in \{1, 2, \dots, n\}.$$

Így kapunk $(z_1, \dots, z_n) \in \mathbb{Z}^n$ n-eseket (ezeknek a száma, ahányféleképpen választhatjuk $(r_1, \dots, r_n, s_1, \dots, s_n)$-t, azaz $u_1 \cdots u_n v_1 \cdots v_n$). Itt a lemma feltétele miatt

$$u_1 \cdots u_n v_1 \cdots v_n > m^n,$$

de mod m legfeljebb m^n darab különböző szám n-es van, azaz a skatulyaelv miatt létezik két különböző $(z_1, \dots, z_n)$-es, amelyek mod m azonosak.

Ha ezek közül az első az $r'_1, \dots, r'_n, s'_1, \dots, s'_n$ számokból adódik, a második pedig az $r''_1, \dots, r''_n, s''_1, \dots, s''_n$ számokból, akkor $\forall$ i-re $z'_i \equiv z''_i \pmod m$ miatt:

$$s'_i - (a_{i,1} r'_1 + \cdots + a_{i,n} r'_n) \equiv s'_i - (a_{i,1} r'_1 + \cdots + a_{i,n} r'_n) \pmod m,$$

amiből

$$a_{i,1} \underbrace{(r'_1 - r''_1)}_{= x_1} + \cdots + a_{i,n} \underbrace{(r'_n - r''_n)}_{= x_n} \equiv \underbrace{s'_i - s''_i}_{= y_i} \pmod m$$
$$(i = 1, 2, \dots, n)$$

Erre az $x_1, \dots, x_n$-re teljesül a lemma állítása. Valóban (11.1) igaz. Továbbá

$$0 < r'_i, r''_i \le u_i \;\; \Rightarrow \;\; |r'_i - r''_i| < u_i$$
$$0 < s'_i, s''_i \le u_i \;\; \Rightarrow \;\; |s'_i - s''_i| < v_i.$$

Végül $(r'_1, \dots, r'_n, s'_1, \dots, s'_n) \neq (r''_1, \dots, r''_n, s''_1, \dots, s''_n)$, hiszen $\exists$ $x_i = r'_i - r'_i \neq 0$ (ugyanis, ha $\forall$ $x_i = 0$, akkor $\forall$ y_i is 0, és a két

szám n-es $(z_1', \ldots, z_n')$ és $(z_1'', \ldots, z_n'')$ ugyanaz. Ezzel a lemmát igazoltuk.

Térjünk vissza a négy négyzetszám-tétel bizonyítására. Már csak az utolsó lépés hiányzik, hogy az $x^2 + y^2 + z^2 + u^2 = p$ egyenlet megoldható, ha p prím.

Ez $p = 2, 3$ esetén triviális. Feltehető $p \geq 3$.

Legyen a,b a 11.4 Lemma szerinti ($a^2 + b^2 + 1 \equiv 0 \pmod{p}$), és alkalmazzuk a Thue lemmát $n = 2$, $m = p$, $u_1 = u_2 = v_1 = v_2 = [\sqrt{p}] + 1$-gyel és $(a_{i,j}) = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}$ mátrixszal.

A lemma valóban alkalmazható, hiszen

$$u_1 u_2 v_1 v_2 = ([\sqrt{p}] + 1)^4 > \sqrt{p}^4 = p^2.$$

Vagyis a 11.5 Lemma miatt $\exists\, x_1, x_2, y_1, y_2 < [\sqrt{p}] + 1$, hogy x_1 és x_2 nem mindkettő 0, továbbá:

$$\begin{aligned} ax_1 + bx_2 &\equiv y_1 \\ bx_1 - ax_2 &\equiv y_2 \pmod{p}. \end{aligned}$$

Tekintsük ekkor

$$w \stackrel{\text{def}}{=} x_2^2 + x_2^2 + y_1^2 + y_2^2$$

kifejezést. Mekkora z és mivel kongruens mod p?

Ekkor $0 < w$, hiszen $\exists\, x_i \neq 0$. Továbbá:

$$w \leq 4[\sqrt{p}]^2 < 4p.$$

Végül mivel kongruens mod p?

$$x_1^2+x_2^2+y_1^2+y_2^2 \equiv x_1^2+x_2^2+(ax_1+bx_2)^2+(bx_1-ax_2)^2$$
$$\equiv x_1^2+x_2^2+a^2x_1^2+2abx_1x_2+b^2x_2^2+b^2x_1^2-2abx_1x_2+a^2x_2^2$$
$$\equiv x_1^2+x_2^2+a^2x_1^2+b^2x_2^2+b^2x_1^2+a^2x_2^2$$
$$= (x_1^2+x_2^2)\underbrace{(1+a^2+b^2)}_{\equiv 0 \ (p)}$$
$$\equiv 0 \pmod{p}$$

Így

$$x_1^2+x_2^2+y_1^2+y_2^2 = \begin{cases} p \\ 2p \\ 3p. \end{cases}$$

Ha ez az érték p készen vagyunk. Marad annak a bizonyítása, hogyha $2p$ vagy $3p$ előáll két négyzetszám összegeként, akkor p is.

Először nézzük az $x_1^2+x_2^2+y_1^2+y_2^2 = 2p$ esetet. Ekkor x_1, x_2, y_1, y_2 között páros sok páratlan van. Azaz a négy szám két csoportba osztható úgy, hogy az azonos csoportokba esők paritása megegyezik. Szimmetrikus okokból feltehető $x_1 \equiv x_2 \pmod 2$ és $y_1 \equiv y_2 \pmod 2$. Ekkor:

$$\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{y_1-y_2}{2}\right)^2+\left(\frac{y_1+y_2}{2}\right)^2$$
$$= \frac{x_1^2+x_2^2+y_1^2+y_2^2}{2} = p.$$

Végül nézzük az $x_1^2+x_2^2+y_1^2+y_2^2 = 3p$ esetet. Milyen maradékot adhat négy négyzetszám összege modulo 3? Tudjuk, hogy egy négyzetszám hármas maradéka 0 vagy 1.

$$x_1^2+x_2^2+y_1^2+y_2^2 = 3p$$

$$\left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\} + \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\} + \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\} + \left\{ \begin{matrix} 0 \\ 1 \end{matrix} \right\} \equiv 0 \pmod 3.$$

Vagyis a fenti négy négyzetszám összege csak akkor osztható 3-mal, ha vagy mind a négy osztható 3-mal, vagy van köztük 3 darab, amely $\equiv 1 \ \ (0)$ és 1 darab, amely $\equiv 0 \ \ (0)$.

Az első esetben $3 \mid x_1, x_2, y_1, y_2$, így $9 \mid x_1^2+x_2^2+y_1^2+y_2^2 = 3p$, amiből $3 \mid p$. De p egy 3-nál nagyobb prím, és ez ellentmondás.

A második esetben szimmetrikus okokból feltehető:

$$x_1^2 \equiv x_2^2 \equiv y_1^2 \equiv 1 \quad (3), y_2 \equiv 0 \qquad (3).$$

Definiáljuk $r_1, r_2, r_3 \in \{-1, +1\}$-et

$$\begin{aligned} x_1 &\equiv r_1 \pmod 3 \\ x_2 &\equiv r_2 \pmod 3 \\ x_3 &\equiv r_3 \pmod 3 \end{aligned}$$

képletekkel. Ekkor kiszámolható, hogy

$$\begin{aligned} &\left(\frac{r_1x_1 + r_2x_2 + r_3y_1}{3}\right)^2 + \left(\frac{r_1x_1 - r_2x_2 + y_2}{3}\right)^2 \\ &+ \left(\frac{r_2x_2 - r_3y_1 + y_2}{3}\right)^2 + \left(\frac{r_3y_1 - r_1x_1 + y_2}{3}\right)^2 \\ &= \frac{r_1^2x_1^2 + r_2^2x_2^2 + r_3^2y_1^2 + y_2^2}{3} \\ &= p. \end{aligned}$$

Az $r_1x_1 \equiv r_1^2 \equiv 1 \quad (3)$, $r_2x_2 \equiv r_2^2 \equiv 1 \quad (3)$, $r_3y_1 \equiv r_3^2 \equiv 1 \quad (3)$ és $y_2 \equiv 0 \quad (3)$ összefüggéseket használva az is könnyen látszik, hogy a fenti felírásban minden tag egy egész szám négyzete, azaz négyzetszám. Ezzel a tétel állítását beláttuk.

Hivatkozások

[1] P. Erdős, J. Surányi, *Válogatott Fejezetek a Számelméletből*, Polygon 2004, link.

[2] A. Thue, *Et par antydninger til en taltheoretisk metode*, Kra. Vidensk. Selsk. Forh. 7 (1902), 57–75.

[3] Kép, Claude-Gaspard Bachet de Meziriac, link.

[4] Kép, Fedőlapja Bachetnek, Diophantosz, Arithmetica művének 1621-es latin fordításának, link.

[5] Kép, Giuseppe Luigi Lagrangia, link.

12. A Waring-probléma

Lagrange 1770-ben oldotta meg a négy négyzetszám problémát, és még abban az évben Waring kérdezte a következőt:

Mi történik, ha négyzetszámok helyett köböket, negyedik hatványokat, általában k-adik hatványokat veszünk?

Waring matematikai kutatásai mellett orvosként is praktizált. Azonban orvosi pályája nem volt túl sikeres, hiszen súlyosan rövidlátó és eléggé félénk ember volt.

A következő az ún. Waring-probléma: Létezik-e $\forall\, k \in \mathbb{N}$-hez olyan g szám, hogy $\forall\, n \in \mathbb{N}$ felírható

$$x_1{}^k + x_2{}^k + \ldots + x_g{}^k = n, \qquad x_i \in \{0, 1, \ldots\}\ \forall\, i$$

alakban? Ha igen, a legkisebb ilyen g-t $g(k)$-val jelöljük.

Hilbert 1909-ben bebizonyította a következőt:

12.1 TÉTEL. (Hilbert, 1909) $g(k)$ *létezik.*

Nem bizonyítjuk. Elég komplikált, de elemi. Sőt, Hilbert bizonyítása becslést is adott $g(k)$-ra, de nagyon gyengét. Ma már $g(k)$ $k \leq 471\,600\,000$-ig pontosan ismert, további részleteket a kapcsolódó Wikipédia oldalon olvashatunk: link.

Egy triviális alsó becslés $g(k)$-ra:

12.2 TÉTEL.

$$g(k) \geq 2^k - 1.$$

A 12.2 Tétel bizonyítása.

$$x_1{}^k + \ldots + x_g{}^k = 2^k - 1$$

esetén $\forall\ x_i = 0$ vagy 1; hogy $2^k - 1$ kiadja, $2^k - 1$ darab egyes kell.

A 12.2 Tétel javítható, hiszen

$$x_1{}^k + \ldots + x_g{}^k = 2^k \cdot \left[\left(\frac{3}{2}\right)^k\right] - 1$$

előállításához $\left[\frac{3}{2}\right]^k - 1$ db 2^k és $2^k - 1$ db egyes kell. Így:

$$g(k) \geq 2^k + \left[\frac{3}{2}\right]^k - 2.$$

Ez a konstrukció már sejteti, hogy $g(k)$ értéke döntően függ attól, hogy a kis számok előállításához hány k-adik hatvány kell.

Ezért fontosabb és mélyebb kérdés annak vizsgálata, hogy „nagy” számok előállításához hány k-adik hatvány kell. Pontosabban:

12.3 DEFINÍCIÓ. *$\mathcal{G}(k)$-val jelöljük a legkisebb olyan $\mathcal{G}$ természetes számot, melyhez található olyan $n_0 = n_0(k)$ szám, hogy $n \in \mathbb{N}$, $n > n_0$ esetén n felírható legfeljebb $\mathcal{G}$ darab nem negatív egész k-adik hatvány összegeként.*

Megjegyzések:

1. $\mathcal{G}(k)$ $\exists$. Következik Hilbert tételéből, hiszen nyilván

$$G(k) \leq g(k).$$

2. $g(2) \leq 4$ (négy négyzetszám tétel)
   $4 \leq G(2)$ (három négyzetszám tétel)

Így:

$$4 \leq G(2) \leq g(2) \leq 4,$$
$$G(2) = g(2) = 4.$$

Mekkora $G(k)$? Először megint egy triviális alsó becslés:

12.4 TÉTEL. *$\forall\, k \in \mathbb{N}$-re, $k \geq 2$-re*

$$G(k) \geq k.$$

A 12.4 Tétel bizonyítása. Indirekt. Tegyük fel, hogy

$$G(k) \leq k - 1.$$

Azaz $\exists$ olyan L természetes szám, hogy $\forall\, n \in \mathbb{N}$, $n > L$ felírható $k - 1$ darab k-adik hatvány összegeként:

$$x_1{}^k + \ldots + x_{k-1}{}^k = n \qquad (n \geq L) \tag{12.1}$$

Tekintsünk egy „nagy” $x \in \mathbb{N}$-et, ekkor $\forall\, L \leq n \leq x$-re (12.1) megoldható. Nyilván (12.1)-ben ekkor $\forall\, i = 1, \ldots, k = 1$-re

$$x_i{}^k \leq x \;\Rightarrow\; 0 \leq x_i \leq x^{1/k}.$$

Így $\forall\, x_i$ legfeljebb $[x^{1/k}] + 1$ értéket vehet fel, azaz $(x_1, \ldots, x_{k-1})$ $k-1$-es legfeljebb

$$\left(\left[x^{1/k}\right] + 1\right)^{k-1}$$

különböző értéket vehet fel.

Minthogy ezek az $L+1, \ldots, X$ számok mindegyikét előállítják, ezért számuk legalább akkora, mint e számok száma, azaz $X - L$.

$$\begin{aligned} X - L &\leq \left(\left[x^{1/k}\right] + 1\right)^{k-1} \leq (2x^{1/k})^{k-1} \\ &= 2^{k-1} x^{\frac{k-1}{k}} \qquad / : x \\ 1 - \frac{L}{X} &< 2^{k-1} \frac{1}{x^k}. \end{aligned}$$

Azaz $x \to \infty$ esetén

$$1 - \frac{L}{X} \to 1 < 2^{k-1} \frac{1}{x^k} \to 0. \qquad \lightning$$

Ezzel ellentmondásra jutottunk a tételt bebizonyítottuk. (Sőt, kis fáradsággal $G(k) \geq k+1$ is kijön.)

Persze az igazi probléma a felső becslés. Hilbert bizonyítása csak igen gyenge felső becslést ad.

Aztán Hardy és Littlewood (egy Hardytól és Ramanujantól származó partíciók vizsgálatára kidolgozott módszert továbbfejlesztve) 1920 és 1928 között kidolgoztak egy analitikus módszert általában additív problémák tárgyalására: ez az ún. Hardy–Littlewood-körmódszer.

Bebizonyították

$$G(k) \leq k \cdot 2^{k-2} \qquad (k \geq k_0)$$

(Goldbach is belátta).

Azután Vinogradov továbbfejlesztette: 1928-34-ben lényegesen javította, majd

$$\limsup_{k\to+\infty} \frac{G(k)}{k \log k} \leq \begin{cases} 6 & '34 \\ 3 & '47 \\ 2 & '59 \end{cases}$$

Végül Wooley '92

$$\limsup_{k\to\infty} \frac{G(k)}{k \log k} \leq 1.$$

12.5 SEJTÉS. (Hardy–Littlewood)

$$G(k) \leq \begin{cases} 2k+1, & \text{ha } k \neq 2^\alpha,\ \alpha \geq 2, \\ 4k, & \text{ha } k = 2^\alpha,\ \alpha \geq 2. \end{cases}$$

(A sejtést csak $k = 2$ és 4 esetén igazolt.)

A fenti eredmények és hozzájuk referenciák megtalálhatóak pl. [2] cikkben.

$G(4)$ becsléséhez magyar irodalmat is találunk ld. Turán-Gyarmati [1].

Hivatkozások

[1] Gyarmati Edit, Turán Pál, *Számelmélet*, link.

[2] R. C. Vaughan, T. Wooley, *Waring's Problem: A Survey*, megtalálható: M. A. Bennet, B. C. Berndt, N. Boston, H. G. Diamond, A. J. Hildebrand, W. Philipp (szerkesztők), Number Theory for the Millennium. Vol. III. Natick, MA: A. K. Peters, 301–340.

[3] Vaughan, R. C. (1997). The Hardy–Littlewood method. Cambridge Tracts in Mathematics. Vol. 125 (2nd ed.). Cambridge: Cambridge University Press. ISBN 0-521-57347-5. Zbl 0868.11046.

[4] Kép, Edward Waring, megtalálható a Wikipedián, link.

13. Pell-egyenletek

Visszatérünk az

$$x^2 + ay^2 = n$$

egyenletre. Innen tovább lehet menni más irányba is. Írjunk $-$ jelet az a elé.

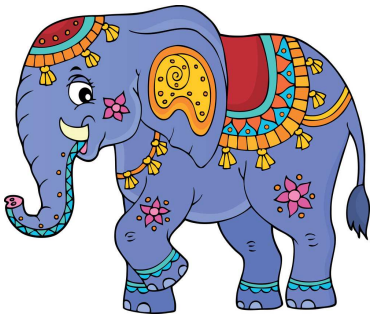
Ez részben visszavezethető az $n = 1$ speciális esetre. Ez az ún. Pell-egyenlet:

13.1 Definíció. *Egy $x^2 - Dy^2 = 1$ egyenletet, ahol $D \in \mathbb{N}$, és D nem négyzetszám, Pell-egyenletnek nevezünk.*

A legegyszerűbb Pell-egyenleteket már i.e. 400-ban Indiában és Görögországban is tanulmányozták. Később a VII. században Brahmagupta felfedezte az

$$(x_1^2 - ay_1^2)(x_2^2 - ay_2^2) = (x_1x_2 + ay_1y_2)^2 - a(x_1y_2 + x_2y_1)^2$$

összefüggést, amely tulajdonképpen egy első lépés lehet a Pell-egyenletek megoldása során.



A terület később egyidőre feledésbe merült, majd John Pell matematikus újra divatba hozta Angliában.

13.2 Tétel. *Az $x^2 - Dy^2 = 1$, $D \in \mathbb{N}$ egyenletnek*

a) ha D négyzetszám, csak $x = \pm 1$, $y = 0$ megoldása.

b) ha D nem négyzetszám (tehát $\forall$ Pell-egyenletnek) ∞ sok egész megoldása van.

A 13.2 Tétel bizonyítása. a) Tegyük fel, hogy $D = k^2$, $k \in \mathbb{N}$, és x, y megoldás. Ekkor:

$$x^2 - Dy^2 = x^2 - k^2y^2 = (x - ky)(x + ky) = 1$$

Így:

$$\left.\begin{aligned} x - ky &= 1 \\ x + ky &= 1, \end{aligned}\right\} \Leftrightarrow \; x = 1, \; y = 0$$

vagy

$$\left.\begin{aligned} x - ky &= -1 \\ x + ky &= -1, \end{aligned}\right\} \Leftrightarrow \; x = -1, \; y = 0$$

és ezek valóban megoldások.

b) Szorítkozhatunk pozitív egész megoldások keresésére (hiszen ezekből előjelek változtatásával minden további megoldás megkapható).

Először kicsit gondolkozzunk: ∞ sok x_n, y_n megoldást szeretnénk.

Ha x_n, y_n pozitív megoldás, nyilván x_n, y_n egyértelműen meghatározza egymást. Ezért ha ∞ sok megoldás $\exists$, akkor ha az egyik $\to \infty$, a másik is.

Tehát a megoldások nagyság szerint sorba rendezhetők úgy, hogy ha az n-edik pozitív egész megoldást x_n, y_n jelöli, akkor végtelen sok megoldás esetében feltehető, hogy $x_n \to \infty$ és $y_n \to \infty$.

Ekkor

$$x_n{}^2 - D y_n{}^2 = 1$$
$$\left(\frac{x_n}{y_n}\right)^2 - D = \frac{1}{y_n{}^2}.$$

Amennyiben végtelen sok megoldás van, nézzük mi történik, ha $n \to \infty$:

$$\left(\frac{x_n}{y_n}\right)^2 - \underbrace{D}_{\downarrow D} = \underbrace{\frac{1}{y_n{}^2}}_{\downarrow 0}.$$

Így:

$$\left(\frac{x_n}{y_n}\right)^2 \to D \;\Rightarrow\; \frac{x_n}{y_n} \to \sqrt{D}, \text{ azaz } \sqrt{D} \sim \frac{x_n}{y_n},$$

vagyis $\left|\sqrt{D} - \frac{x_n}{y_n}\right|$ „kicsi”.

Ezt úgy fejezhetjük ki, hogy az $\frac{x_n}{y_n}$ racionális szám jól közelíti, „approximálja” a $\sqrt{D}$ számot.

Tehát a megoldások létezése összefügg a $\sqrt{D}$ (irracionális) szám racionális számokkal való approximálhatóságával.

Ezek után nem meglepő, hogy egy ilyen típusú tételből indulunk ki:

13.3 Tétel. (Dirichlet approximációs tétele) *$\forall$ α irracionális számhoz $\exists$ ∞ sok q_n természetes szám, hogy alkalmas p_n egész számmal*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n{}^2}.$$

A tételt a következő fejezetben bizonyítjuk (ld. 14.2 Tétel).

Először e tételt használva befejezzük a 13.2 Tétel bizonyításának b) részét.

13.4 Lemma. *$\exists\, t \in \mathbb{Z}$, hogy $0 < t < 2\sqrt{D} + 1$ és $x^2 - Dy^2 = t$-nek ∞ sok megoldása létezik.*

A 13.4 Lemma bizonyítása. Alkalmazzuk a Dirichlet-tételt $\alpha = \sqrt{D}$-vel: ez irracionális; mert D nem négyzetszám (a számelmélet alaptételéből következik, hogy ilyenkor $\sqrt{D}$ irracionális: HF.)

Azaz a 13.3 Tételből következik, hogy $\exists\, \infty$ sok $q_n \in \mathbb{N}$, $p_n \in \mathbb{Z}$, melyekre

$$\left|\sqrt{D} - \frac{p_n}{q_n}\right| < \frac{1}{{q_n}^2},.$$

Ekkor $q_n > 0$ különben

$$\left|\sqrt{D} - \frac{p_n}{q_n}\right| = \sqrt{D} + \frac{(-p_n)}{q_n} \geq \sqrt{D} > 1 \geq \frac{1}{{q_n}^2}. \;\lightning$$

Tekintsük

$$\begin{aligned}
\left|{p_n}^2 - D{q_n}^2\right| &= \left|p_n - \sqrt{D}q_n\right| \cdot \left|p_n + \sqrt{D}q_n\right| \\
&= {q_n}^2 \underbrace{\left|\frac{p_n}{q_n} - \sqrt{D}\right|}_{< \frac{1}{{q_n}^2}} \cdot \underbrace{\left|\frac{p_n}{q_n} + \sqrt{D}\right|}_{< \left|\frac{p_n}{q_n} - \sqrt{D} + 2\sqrt{D}\right|} \\
&< \left|\frac{p_n}{q_n} - \sqrt{D}\right| + 2\sqrt{D} \\
&< \frac{1}{{q_n}^2} + 2\sqrt{D}
\end{aligned}$$

Így:

$$\left|{p_n}^2 - D{q_n}^2\right| < {q_n}^2 \cdot \frac{1}{{q_n}^2}\left(\frac{1}{{q_n}^2} + 2\sqrt{D}\right)$$

$$= \frac{1}{{q_n}^2} + 2\sqrt{D} \leq 1 + 2\sqrt{D}.$$

Azaz ∞ sok $q_n \in \mathbb{N}$ és ehhez $p_n \in \mathbb{Z}$ $\exists$, hogy

$$-(1 + 2\sqrt{D}) \leq \underbrace{{p_n}^2 - D{q_n}^2}_{\text{és persze ez } \neq 0, \text{ hiszen } D \text{ nem négyzetszám.}} \leq 1 + 2\sqrt{D}$$

Ebben az intervallumban csak véges sok (kevesebb mint $< 2(1 + 2\sqrt{D}$ darab) nem nulla egész esik, azaz skatulyaelv miatt $\exists$ olyan $t \neq 0$ egész, amelyre $|t| < 1 + 2\sqrt{D}$, és amely ∞ sokszor fordul elő:

$${p_n}^2 - D{q_n}^2 = t \qquad \infty \text{ sok } n\text{-re.}$$

Ezzel a tétel bizonyítását befejeztük.

Tehát

$$x^2 - Dy^2 = t \tag{13.1}$$

egyenletnek ∞ sok pozitív megoldása létezik.

Most ebből megkonstruáljuk

$$x^2 - Dy^2 = 1$$

-nek egy pozitív egész megoldását.

Tekintsük (13.1)-nek az (x, y) pozitív megoldásait modulo $|t|$.

Mod $|t|$ csak $|t|^2$ db maradékpár $\exists$, azaz a skatulyaelv miatt $\exists$ olyan maradékpár, amely ∞ sokszor fordul elő.

Vegyük (13.1)-nek két különböző pozitív megoldását, $(x_1, y_1), (x_2, y_2)$-t, melyekre

$$y_1 \neq y_2$$

$$x_1 \equiv x_2 \pmod{|t|}$$
$$y_1 \equiv y_2 \pmod{|t|}$$
$$x_1{}^2 - Dy_1{}^2 = x_2{}^2 - Dy_2{}^2 = t$$

Legyen

$$u \overset{\text{def}}{=} \frac{x_1x_2 - Dy_1y_2}{|t|},$$
$$v \overset{\text{def}}{=} \frac{x_1x_2 - x_2y_1}{|t|}.$$

13.5 LEMMA. *Ezek az u, v számok*

a) egészek;

b) kielégítik az $x^2 - Dy^2 = 1$ Pell-egyenletet;

c) nem triviális megoldások ($\neq (\pm 1, 0)$).

A 13.5 Lemma bizonyítása. a) Mivel a két megoldás kongruens mod $|t|$:

$$x_1x_2 - Dy_1y_2 \equiv x_1{}^2 - Dy_1{}^2 = t \equiv 0 \pmod{|t|}$$
$$\Rightarrow \ u \text{ egész},$$
$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 = 0 \pmod{|t|}$$
$$\Rightarrow \ v \text{ egész}.$$

b)

$$u^2 - Dv^2 =$$
$$= \left(\frac{x_1x_2 - Dy_1y_2}{|t|}\right)^2 - D\left(\frac{x_1y_2 - x_2y_1}{|t|}\right)^2$$
$$= \frac{x_1{}^2x_2{}^2 - 2Dx_1x_2y_1y_2 + D^2y_1{}^2y_2{}^2 - Dx_1{}^2y_2{}^2 + 2Dx_1x_2y_1y_2 + Dx_2^2y_1^2}{|t|^2}$$

$$= \frac{x_1{}^2(x_2{}^2 - Dy_2{}^2) - Dy_1{}^2(x_2{}^2 - Dy_2{}^2)}{|t|^2}$$
$$= \frac{(x_1{}^2 - Dy_1{}^2)(x_2{}^2 - Dy_2{}^2)}{t^2} = \frac{t \cdot t}{t^2} = 1.$$

c) Bár egyszerűnek tűnik, ez sem egészen triviális. Indirekt. Tegyük fel, hogy $v = 0$.

$$x_1 y_2 - x_2 y_1 = 0.$$

Legyen $x_2 = \lambda x_1$, ahol $\lambda > 0$. Ekkor $y_2 = \lambda y_1$. Így

$$1 = x_2{}^2 - Dy_2{}^2 = (\lambda x_1)^2 - D(\lambda y_1)^2$$
$$= \lambda^2(x_1{}^2 - Dy_1{}^2) = \lambda^2.$$

Azaz $\lambda^2 = 1$ és $\lambda > 0$ miatt $\lambda = 1$. Vagyis

$$(x_1 y_1) = (x_2, y_2),$$

és ezzel ellentmondásra jutottunk, és a lemma bizonyítását befejeztük.

Tehát beláttuk $\exists$ tehát egy pozitív egész megoldás. Marad: $\exists\ \infty$ sok is. Ehhez:

13.6 Lemma. *Legyenek $(x_1, y_1), (x_2, y_2)$ pozitív megoldások. Ekkor az egész u, v-t*

$$u + \sqrt{D}v = \left(x_1 + \sqrt{D}y_1\right)\left(x_2 + \sqrt{D}y_2\right)$$

-vel definiálva, azaz

$$u + \sqrt{D}v = (\underbrace{x_1x_2 + Dy_1y_2}_{u}) + \sqrt{D}(\underbrace{x_1y_2 + x_2y_1}_{v}),$$

azt kapjuk, hogy u, v is pozitív megoldás.

Megjegyzés: $u + \sqrt{D}v$ egyértelműen van definiálva, hiszen ha $u + \sqrt{D}\, v = r + \sqrt{D}s$ (ahol $u, v, r, s \in \mathbb{Z}$), akkor $u = r,\ v = s$.

A 13.6 Lemma bizonyítása.

$$\begin{aligned} u^2 - Dv^2 &= (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2 \\ &= ({x_1}^2 - D{y_1}^2)({x_2}^2 - D{y_2}^2) = 1, \end{aligned}$$

és u, v nyilván pozitív.

Térjünk vissza a 13.2 Tétel bizonyításához. Csak annak bizonyítása maradt hátra, hogy $\exists\ \infty$ sok megoldás.

A 13.5 Lemma miatt $\exists\ x_1, y_1$ pozitív megoldás.

Legyen x_n, y_n definíciója:

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n.$$

A 13.6 Lemma miatt x_n, y_n pozitív megoldás.

Ekkor az (x_i, y_i) és (x_j, y_j) megoldások különbözőek, ha $i < j$:

$$\begin{aligned} x_j + y_j\sqrt{D} = (x_1 + y_1\sqrt{D})^j &= (x_1 + y_1\sqrt{D})^i \underbrace{(x_1 + y_1\sqrt{D})}_{>\,1} \\ &> (x_1 + y_1\sqrt{D})^i = x_i + y_i\sqrt{D}. \end{aligned}$$

Azaz $(x_j, y_j) \neq (x_i, y_i)$. Ezzel a tétel bizonyítását befejeztük.

A következőkben csak pár szóban ismertetünk még néhány elméleti eredményt a Pell-egyenletek kapcsán.

13.7 DEFINÍCIÓ. *Tekintsük az $x^2 - Dy^2 = 1$ Pell-egyenlet pozitív megoldásai közül azt az $x = \alpha$, $y = \beta$ megoldást, melyre $x + y\sqrt{D}$ minimális ($\exists$ minimum). Ezt az egyenlet alapmegoldásának nevezzük.*

13.8 TÉTEL. *Az $x^2 - Dy^2 = 1$ Pell-egyenlet összes u, v megoldásai*

$$u + v\sqrt{D} = \pm(\alpha + \beta\sqrt{D})^n,$$

ahol $n \in \mathbb{Z}$. Az n kitevő lehet negatív is.

A tétel bizonyítása megtalálható pl. Gyarmati-Turán [2] könyvben. A negatív n kitevőkhöz egy apró megjegyzés:

$$(\alpha + \beta\sqrt{D})^{-1} = \frac{1}{\alpha + \beta\sqrt{D}} = \frac{\alpha - \beta\sqrt{D}}{\alpha^2 - \beta^2 D} = \alpha - \beta\sqrt{D}.$$

A Pell-egyenlek elmélete erősen kapcsolódik a lánctörtek elméletéhez is. Erről bővebben [1]-ben vagy magyarul [3], [4]-ben is olvashatunk.

Hivatkozások

[1] B. Lynn, *Continued Fractions*, link.

[2] Gyarmati Edit, Turán Pál, *Számelmélet*, link.

[3] Gyarmati Katalin, *Számelméleti 5letek*, link.

[4] Sárközy András, *Számelmélet*, link.

[5] Kép, elefánt, link.

14. Diofantikus approximációelmélet

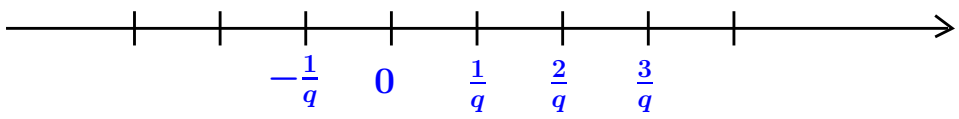
Az előző fejezetben láttunk milyen fontos lehet az, hogy egy irracionális szám mennyire jól közelíthető racionálisokkal (ld. 13.3 Tétel).

Ezt a területet hívjuk Diofantikus approximációelméletnek.

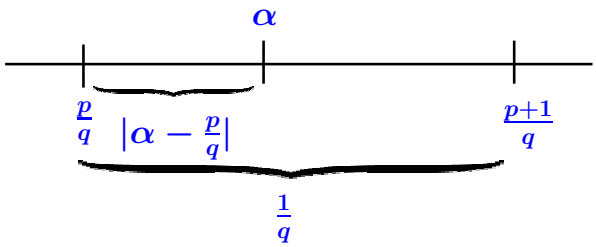
Alapprobléma: Ha α adott irracionális szám, akkor alkalmas $p \in \mathbb{Z}$, $q \in \mathbb{N}$-nel $\left|\alpha - \frac{p}{q}\right|$ milyen „kicsivé” tehető, azaz egy irracionális szám milyen jól közelíthető, approximálható egy racionális számmal?

A fejezet fő célja Dirichlet tételének (13.3 Tétel) bizonyítása, de előtte egy kis előkészítés:

$\left|\alpha - \frac{p}{q}\right|$ „kicsiségét” q-nak függvényében szoktuk jellemezni. Mi az ami triviális? Rögzítsük q-t, futassuk p-t:



α beleesik egy ilyen $\frac{1}{q}$ hosszú kis intervallumba:



Legyen $\frac{p}{q}$ az intervallum két végpontja közül a közelebbi α-hoz. Nyilván:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q}.$$

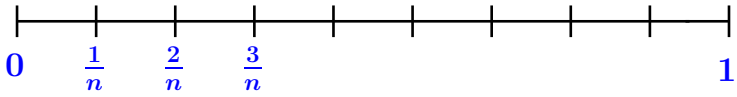
Ez tehát elérhető minden fix q-ra, de ha q-t is változtatjuk, akkor a hiba már $\frac{1}{q}$-ban négyzetesen kicsire csökkenthető.

A bizonyítás a következő lemmán múlik:

14.1 Lemma. *Legyen α irracionális, ekkor $\forall\, n \in \mathbb{N}$ esetén $\exists\, p, q \in \mathbb{Z}$, hogy $1 \leq q \leq n$ és*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}.$$

A 14.1 Lemma bizonyítása. Tekintsük az $\{\alpha\}, \{2\alpha\}, \{3\alpha\}, \ldots, \{(n+1)\alpha\} \in (0,1)$ számokat. A $(0,1)$ intervallumot pedig osszuk n darab $\frac{1}{n}$ hosszú részintervallumra:



A skatulyaelv miatt létezik két elem: $\{r_1\alpha\}$ és $\{r_2\alpha\}$, amelyek ugyanabba a kis intervallumba esnek (ahol feltehető, hogy $1 \leq r_1 < r_2 \leq n+1$).

Azaz $\exists\, k$, melyre $\{r_1\alpha\}, \{r_2\alpha\} \in \left(\frac{k}{n}, \frac{k+1}{n}\right)$.

Legyen

$$\{r_1\alpha\} = r_1\alpha - p_1, \text{ ahol } p_1 \in \mathbb{Z}$$
$$\{r_2\alpha\} = r_2\alpha - p_2, \text{ ahol } p_2 \in \mathbb{Z}.$$

Ekkor

$$\begin{aligned} \big|\{r_2\alpha\} - \{r_1\alpha\}\big| &< \frac{1}{n} \\ \big|r_2\alpha - p_2 - (r_1\alpha - p_1)\big| &< \frac{1}{n} \\ \big|\underbrace{(r_2 - r_1)}_{\stackrel{\text{def}}{=} q}\alpha - \underbrace{(p_2 - p_1)}_{\stackrel{\text{def}}{=} p}\big| &< \frac{1}{n} \\ |q\alpha - p| &< \frac{1}{n}. \end{aligned}$$

Mivel $1 \le r_1 < r_2 \le n+1$, ezért $1 \le q = r_2 - r_1 \le n$ is teljesül, és ezzel a lemma állítását igazoltuk.

14.2 Tétel. (Dirichlet approximációs tétele) *$\forall \quad \alpha$ irracionális számhoz $\exists\, \infty$ sok $\frac{p_n}{q_n}$ racionális szám, hogy*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{{q_n}^2}.$$

A 14.2 Tétel bizonyítása. Az előző lemmát alkalmazzuk rendre $n = 1, 2, 3, \ldots$ választással.

Legyen $\frac{p_n}{q_n}$ olyan racionális szám, amelyre $1 \le q_n \le n$ és

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{nq_n}.$$

Mivel $1 \le q_n \le n$, ezért

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{nq_n} \le \frac{1}{q_n^2}$$

is teljesül.

Nyilván $\frac{p_n}{q_n} \to \alpha$, hiszen $\frac{1}{nq_n} < \frac{1}{n} \to 0$.

Hiányzik még annak bizonyítása, hogy $\frac{p_n}{q_n}$ törtek között ∞ sok különböző van.

Valóban, $\frac{p_i}{q_i} \to \alpha$ miatt, ha véges sok különböző lenne a $\frac{p_i}{q_i}$ racionális számok között, akkor nem tarthatna a sorozat egy irracionális számhoz.

Vajon mennyire éles a 14.2 Tétel? A következő példában egy ellenkező irányú becslést adunk meg egy nevezetes irracionális szám esetében.

14.3 Tétel. $\forall \frac{p}{q}$ *racionális számra* $\left|\sqrt{2} - \frac{p}{q}\right| \geq \frac{1}{4q^2}$.

Vagyis a 14.2 Tételben maximum a konstansszorzó javítható meg.

A 14.3 Tétel Bizonyítása. Indirekten bizonyítunk. Tegyük fel, hogy egy $\frac{p}{q}$ racionális számra:

$$\left|\sqrt{2} - \frac{p}{q}\right| < \frac{1}{4q^2}.$$

Ekkor:

$$\left|\sqrt{2} - \frac{p}{q}\right| < \frac{1}{4q^2} < \frac{1}{4}$$
$$\sqrt{2} - \frac{1}{4} < \frac{p}{q} < \sqrt{2} + \frac{1}{4}$$

Tehát:

$$\left|2 - \frac{p^2}{q^2}\right| = \frac{\overbrace{|2q^2 - p^2|}^{\neq 0 \Rightarrow \geq 1}}{q^2} \geq \frac{1}{q^2}$$
$$\left|\sqrt{2} - \frac{p}{q}\right| \cdot \left|\sqrt{2} + \frac{p}{q}\right| \geq \frac{1}{q^2}$$

A háromszög egyenlőtlenség szerint $\left|\sqrt{2}+\frac{p}{q}\right| \leq |\sqrt{2}| + \left|\frac{p}{q}\right| \leq 2\sqrt{2}+\frac{1}{4} < 4$, így:

$$4\left|\sqrt{2}-\frac{p}{q}\right| > \frac{1}{q^2}.$$

Azaz

$$4\left|\sqrt{2}-\frac{p}{q}\right| > \frac{1}{4q^2},$$

amivel ellentmondásra jutottunk és a tétel állítását igazoltuk

Tehát a 14.2 Tétel szerint irracionális α-hoz $\exists\ \infty$ sok $\frac{p}{q}$, hogy $\left|\alpha-\frac{p}{q}\right| < \frac{1}{q^2}$.

Viszont a 14.3 Tétel szerint van olyan α, hogy minden $\frac{p}{q}$ racionális számra $\left|\alpha-\frac{p}{q}\right| > \frac{1}{4q^2}$.

Vajon hol az igazság? A 14.2 Tételben mi a legjobb konstans? Hurwitz [1] cikke óta (1891) a következőt tudjuk:

14.4 TÉTEL. *Ha α irracionális, akkor $\exists\ \infty$ sok $\frac{p}{q}$ tört úgy, hogy* $\left|\alpha-\frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$.

A tétel legismertebb bizonyítása lánctörtekre épül. Émile Borel [2, 2. fejezet, 15. Tétel] megmutatta, hogy minden irracionális α lánctört alakjának három egymást követő közelítő törtje közül az egyik eleget tesz a fenti tételnek.

Ebben az általános tételben a $\sqrt{5}$ éles, azonban ha nem minden irracionális számot szeretnénk jól approximálni, hanem csak bizonyos feltételeknek eleget tevőeket, akkor a konstans szorzó még tovább csökkenthető.

Hivatkozások

[1] A. Hurwitz, *Üeber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche*, Mathematische Annalen 39 (2) (1891), 279–284.

[2] O. Perron, *Die Lehre von den Kettenbrüchen*, Leipzig: B. G. Teubner.

15. Algebrai számok nem approximálhatóak túl jól

Az előző fejezetben láttuk, hogy az irracionális számok jól approximálhatóak. Ebben a fejezetben megmutatjuk, hogy Dirichlet tétele (14.2 Tétel), konstans szorzótól eltekintve nem élesíthető tovább algebrai számok esetében.

Eredményünk alkalmas lesz transzcendens számok konstrukciójára is.

15.1 Definíció. *Az α komplex számot algebrai számnak nevezzük, ha van olyan (nem azonosan nulla) egész együtthatós polinom, amelynek α gyöke.*

15.2 Definíció. *Az α algebrai szám minimálpolinomja olyan (nem azonosan nulla) egész együtthatós $m(x)$ polinom, amelynek α gyöke, és emellett a fokszáma a lehető legkisebb. Ekkor α foka a minimálpolinom fokszáma.*

Először a következőt bizonyítjuk be:

15.3 Tétel. *Ha α egy n-edfokú algebrai szám, és gyöke az $f(x),\ g(x) \in \mathbb{Z}[x]$ n-edfokú polinomoknak, akkor f és g (racionális) konstansszorosai.*

A 15.3 Tétel bizonyítása. Tegyük fel, hogy $f(x), g(x) \in \mathbb{Z}[x]$, $\deg f(x) = \deg g(x) = n$, $f(\alpha) = g(\alpha) = 0$. Legyen

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0.$$

Ekkor $h(x) \stackrel{\text{def}}{=} b_n f(x) - a_n g(x) \in \mathbb{Z}[x]$ legfeljebb $n-1$-edfokú polinom, amelynek α gyöke. Mivel α foka n nincs olyan n-nél kisebb nem nulla polinom, amelynek ő gyöke, tehát $h(x) \equiv 0$, amiből adódóan

$$b_n f(x) \equiv a_n g(x)$$
$$f(x) \equiv \frac{a_n}{b_n} g(x),$$

azaz a két polinom egymás konstansszorosa.

Vagyis a minimálpolinom konstansszorzótól eltekintve egyértelmű. A továbbiakban azt is kikötjük a minimálpolinomról, hogy az együtthatók legnagyobb közös osztója 1.

15.4 Tétel. *Egy α algebrai szám $m(\alpha)$ minimálpolinomja mindig irreducibilis polinom $\mathbb{Q}$ felett.*

A 15.4 Tétel bizonyítása. Indirekten bizonyítunk. Tegyük fel, hogy m nem irreducibilis. Ekkor $m = fg$ alakú, ahol $f, g \in \mathbb{Q}[x]$ és $\deg f, \deg g < \deg m$.

Mivel $m(\alpha) = f(\alpha)g(\alpha) = 0$, ezért $f(\alpha)$ vagy $g(\alpha)$ értéke 0. Feltehető $g(\alpha) = 0$.

Ha g együtthatóit közös nevezőre hozzuk, és ez a közös nevező c, akkor cg egész együtthatós polinom és fokszáma kisebb az m minimálpolinom fokánál, amivel ellentmondásra jutottunk. Tehát m irreducibilis.

15.5 Definíció. *Az α algebrai számot algebrai egésznek nevezzük, ha gyöke egy 1 főegyütthatós, egész együtthatós polinomnak.*

Az algebrai számokról pár szót ejtettünk már a 8. fejezetben is, ahol is -többek közt- megemlítettük, hogy az algebrai számok testet, az algebrai egészek gyűrűt alkotnak.

Most egy kicsit más irányban indulunk tovább, és bebizonyítjuk, hogy az algebrai számok nem approximálhatóak túl jól.

A következő tétel megalkotója Liouville, akiről azt is érdemes tudni, hogy szintén ő volt, aki felfedezte Galois addig publikálatlan munkájának (pl. az általános ötödfokú egyenletnek nincs megoldóképlete) fontosságát, és amely elméletet újságjában meg is jelentett 1846-ban.

15.6 TÉTEL. (Liouville [1], 1844) *Legyen α algebrai szám, melynek foka $n \geq 2$. Ekkor létezik olyan csak α-tól függő $c(\alpha)$ pozitív konstans, hogy minden $\frac{p}{q}$ racionális számra (ahol $q > 0$):*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}.$$

A 15.6 Tétel bizonyítása. Az α algebrai egész minimálpolinomja $m(x)$, ahol

$$\deg m = n \geq 2.$$

Mivel m irreducibilis polinom, így nincs racionális gyöke,

$$m\left(\frac{p}{q}\right) \neq 0.$$

Legyen

$$m(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

Ekkor

$$m\left(\frac{p}{q}\right) = \frac{a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 p q^{n-1} + a_0 q^n}{q^n}.$$

Itt a számláló nem nulla, így a számláló abszolút értéke ≥ 1, azaz

$$\left|m\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}.$$

De $m(\alpha) = 0$, vagyis

$$\left|m(\alpha) - m\left(\frac{p}{q}\right)\right| = \left|m\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}.$$

Tehát

$$\left|\sum_{i=0}^{n} a_i \underbrace{\left(\alpha^i - \left(\frac{p}{q}\right)^i\right)}\right| \geq \frac{1}{q^n}$$
$$\left(\alpha - \frac{p}{q}\right) \cdot \left(\alpha^{i-1} + \alpha^{i-2}\frac{p}{q} + \ldots + \left(\frac{p}{q}\right)^{i-1}\right). \quad (15.1)$$

Ha $\left|\alpha - \frac{p}{q}\right| > \frac{|\alpha/2|}{q^n}$, akkor a tétel fennáll minden $c(\alpha) < |\alpha/2|$ konstansra, és készen is vagyunk a bizonyítással. Ha

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{|\alpha/2|}{q^n},$$

akkor a háromszög egyenlőtlenség miatt

$$\left|\frac{p}{q}\right| - |\alpha| \leq \left|\frac{p}{q} - \alpha\right| \leq \frac{|\alpha/2|}{q^n}$$

$$\left|\frac{p}{q}\right| < |\alpha| + \frac{|\alpha/2|}{q^n} \leq \frac{3}{2}|\alpha|.$$

Szintén a háromszög-egyenlőtlenség és a fenti egyenlőtlenség miatt

$$\left|\alpha^{i-1} + \alpha^{i-2}\frac{p}{q} + \ldots + \left(\frac{p}{q}\right)^{i-1}\right| \leq |\alpha|^{i-1}\left(1 + \frac{3}{2} + \ldots + \left(\frac{3}{2}\right)^{i-1}\right)$$
$$< |\alpha|^{i-1} \cdot 2\left(\frac{3}{2}\right)^{i}$$

Visszatérve (15.1)-hez:

$$\left|\sum_{i=0}^{n} a_i\left(\alpha^i - \left(\frac{p}{q}\right)^i\right)\right| \geq \frac{1}{q^n},$$

így

$$\left|\alpha - \frac{p}{q}\right| \cdot \Bigg| \underbrace{\sum_{i=1}^{n-1} a_i\left(\alpha^{i-1} + \alpha^{i-2}\frac{p}{q} + \ldots + \left(\frac{p}{q}\right)^{i-1}\right)}_{\leq \sum_{i=1}^{n-1} |a_i| \cdot |\alpha|^{i-1} \cdot 2\left(\frac{3}{2}\right)^{i}} \Bigg| \geq \frac{1}{q^n}.$$

Ez csak egy csak α-tól függő $c_1(\alpha)$ konstans

Ekkor

$$\left|\alpha - \frac{p}{q}\right| \cdot c_1(\alpha) \geq \frac{1}{q^n}$$
$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{c_1(\alpha)} \cdot \frac{1}{q^n}.$$

Ezzel a tételt igazoltuk (mégpedig $c(\alpha) = \min\left\{|\alpha/2|, \frac{1}{c_1(\alpha)}\right\}$ konstanssal).

Liouville tételét Thue [3] a következőképp javította:

15.7 TÉTEL. (Thue, 1909) *Ha α algebrai szám, amelynek foka $n \geq 3$, akkor adott ε-hoz, $\varepsilon > 0$ létezik olyan $c(\alpha, \varepsilon)$ csak α-tól és ε-tól függő pozitív konstans, hogy $\forall \frac{p}{q}$ racionális számra, ahol $q > 0$ fennáll:*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \varepsilon)}{q^{n/2+1+\varepsilon}}$$

Nem bizonyítjuk.

A következő években a becslésben q kitevőjét folyamatosan javítgatták. Végül 1955-ben Roth bizonyította a tétel legélesebb változatát, amelyért 1958-ban Fields-érmet kapott.

15.8 TÉTEL. (Roth [2], 1955) *Ha α irracionális algebrai szám, akkor minden adott $\varepsilon > 0$-hoz létezik olyan $c(\alpha, \varepsilon)$ csak α-tól és ε-tól függő pozitív konstans, hogy $\forall \frac{p}{q}$ racionális számra, ahol $q > 0$, fennáll:*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \varepsilon)}{q^{2+\varepsilon}}.$$

Liouville tételére visszatérve, már ez a tétel is remekül alkalmas transzcendens számok konstruálására. Vegyük például az ún. Liouville állandót:

15.9 TÉTEL. *Az*

$$\alpha \stackrel{\text{def}}{=} \sum_{n=1}^{+\infty} \frac{1}{2^{n!}}$$

transzcendens.

A 15.9 Tétel bizonyítása. Legyen

$$\frac{p_k}{q_k} \stackrel{\text{def}}{=} \sum_{n=1}^{k} \frac{1}{2^{n!}}.$$

Ekkor a $\frac{p_k}{q_k}$ törtek különbözőek, hiszen szigorúan monoton növekvő sorozatot alkotnak. Az is világos, hogy ha a fenti szummában közös nevezőre hozunk, akkor $q_k = 2^{(k+1)!}$

Másrészt

$$\begin{aligned}\left|\alpha - \frac{p_k}{q_k}\right| &= \frac{1}{2^{(k+1)!}} + \frac{1}{2^{(k+2)!}} + \frac{1}{2^{(k+3)!}} + \dots \\ &\le \frac{1}{2^{(k+1)!}} + \frac{1}{2^{(k+1)!+1}} + \frac{1}{2^{(k+1)!+2}} + \dots \\ &= \frac{2}{2^{(k+1)!}} \\ &= 2\left(\frac{1}{2^{k!}}\right)^{k+1} \\ &= \frac{2}{q_k^{k+1}}.\end{aligned}$$

Ha α n-edfokú algebrai szám lenne, akkor Liouville tételének értelmében minden p/q racionális számra

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n},$$

azaz a p_k/q_k racionális számokra

$$\frac{2}{q_k^{k+1}} \ge \left|\alpha - \frac{p_k}{q_k}\right| > \frac{c(\alpha)}{q_k^n},$$

vagyis

$$\frac{2}{q_k^{k-n+1}} \ge c(\alpha)$$

ami ellentmondás, ha $k \to \infty$.

A transzcendenciára még visszatérünk a jegyzet utolsó fejezetében.

Hivatkozások

[1] J. Liouville, *Sur les classes très étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationelles algébriques*, Comptes rendus de l'Académie des Sciences de Paris. 18. 883–885, 910–911 (1844); Journal Math. Pures et Appl. 16, 133–142.

[2] K. F. Roth, *Rational approximations to algebraic numbers*. Mathematika. 2 (1): 1–20 and "Corrigendum", p. 168.

[3] A. Thue, *Über Annäherungswerte algebraischer Zahlen*. J. Reine Angew. Math. 1909 (135), 284–305.

[4] Kép, *Joseph Liouville*, megtalálható a Wikipédián: link.

16. Thue egyenletek

Thue által megjavított diofantikus approximációs tételnek (15.7 Tétel) nem csak elméleti érdekessége van, hanem használható diofantikus egyenletek megoldására is.

Thue apja tengerész volt, és Thue-t gyerekkorában a fizika érdekelte. A matematika iránti érdeklődése egy könyvkölcsönzéssel kezdődött, meglátta egy hirdetésben a „On pendulum's meaning of geometry" című könyvet (Az inga-féle geometria) és kivette a könyvtárból. De amikor megérkezett könyv kiderült, hogy az igazi címe: „On Poncelet's meaning of geometry" (a Poncelot-féle geometria). Thue amikor rájött tévedésére, azt hitte sose fogja elolvasni a könyvet, de nem így történt (ld. [2]).

16.1 TÉTEL. (Thue [1]) *Ha $F(x,y) \in \mathbb{Z}[x,y]$ egy homogén, legalább harmadfokú kétváltozós irreducibilis polinom, $m \in \mathbb{Z}$, akkor az*

$$F(x,y) = m$$

egyenletnek csak véges sok egész megoldása van.

A 16.1 Tétel bizonyítása. Legyen

$$F(x,y) = a_r x^r + a_{r-1} x^{r-1} y + \ldots + a_1 x y^{r-1} + a_0 y^r$$

(Mivel $F(x,y)$ homogén, minden tagjának ugyanannyi a foka $= r$)
Most

$$F(x,y) = m,$$

azaz

$$\sum_{i=0}^{r} a_i x^i y^{r-i} = m \qquad / : y^r$$
$$\sum_{i=0}^{r} a_i \left(\frac{x}{y}\right)^i = \frac{m}{y^r}.$$

Tekintsük az egyváltozós

$$f(z) = a_r z^r + a_{r-1} z^{r-1} + \ldots + a_1 z + a_0$$

polinomot. Mivel $F(x,y) = y^r f\left(\frac{x}{y}\right)$ irreducibilis, ezért $f(z)$ is irreducibilis. Ekkor

$$f\left(\frac{x}{y}\right) = \frac{m}{y^r}. \tag{16.1}$$

Tegyük fel, hogy $F(x,y) = m$-nek végtelen sok megoldása van. Ezek $(x_1, y_1), (x_2, y_2), \ldots$. Feltehető $|y_i| \to \infty$. Jelölje az

$$f(z) = a_r z^r + a_{r-1} z^{r-1} + \ldots + a_1 z + a_0$$

irreducibilis polinom gyökeit

$$\alpha_1, \alpha_2, \ldots, \alpha_r.$$

Ekkor

$$f(z) = a_r (z - \alpha_1) \ldots (z - \alpha_r).$$

Azaz (16.1) alapján:

$$a_r \left(\frac{x}{y} - \alpha_1\right) \ldots \left(\frac{x}{y} - \alpha_r\right) = \frac{m}{y^r}.$$

Feltettük, hogy $i \to \infty$ esetén $|y_i| \to \infty$, ezért $\dfrac{m}{{y_i}^r} \to 0$. Így

$$a_r \left(\frac{x_i}{y_i} - \alpha_1\right) \dots \left(\frac{x_i}{y_i} - \alpha_r\right) \to 0 \qquad i \to \infty \text{ esetén}$$

$$a_r \min_{j \in \{1,\dots,r\}} \left|\frac{x_i}{y_i} - \alpha_j\right| \to 0 \qquad i \to \infty \text{ esetén.} \tag{16.2}$$

A skatulyaelv szerint $\exists$ f-nek olyan α_ℓ gyöke, hogy az (x_i, y_i) megoldások közül végtelen sokra teljesül, hogy:

$$\min_{j \in \{1,\dots,r\}} \left|\frac{x_i}{y_i} - \alpha_j\right| = \left|\frac{x_i}{y_i} - \alpha_\ell\right|. \tag{16.3}$$

Rögzítsük ezt az α_ℓ gyököt, és jelölje $(x_{i_1}, y_{i_1}), (x_{i_2}, y_{i_2}), (x_{i_3}, y_{i_3}), \dots$ azt a végtelen sok (x_i, y_i) megoldást, amelyre (16.3) fennáll.

Ekkor (16.2) alapján

$$\left|\frac{x_{i_k}}{y_{i_k}} - \alpha_\ell\right| \to 0 \qquad k \to \infty \text{ esetén,}$$

$$\frac{x_{i_k}}{y_{i_k}} \to \alpha_\ell \qquad k \to \infty \text{ esetén.}$$

Tekintsük a

$$a_r \left(\frac{x_{i_k}}{y_{i_k}} - \alpha_i\right) \dots \left(\frac{x_{i_k}}{y_{i_k}} - \alpha_r\right) = \frac{m}{{y_{i_k}}^r}.$$

egyenletet. Ebben a szorzatban

$$\left|\frac{x_{i_k}}{y_{i_k}} - \alpha_\ell\right|$$

-t becsüljük a Thue-tétellel (15.7 Tétel):

$$\left|\frac{x_{i_k}}{y_{i_k}} - \alpha_\ell\right| > \frac{c(\alpha, \varepsilon)}{|y_{i_k}|^{r/2+1+\varepsilon}}$$

Az egyszerűség kedvéért legyen most $\varepsilon = \frac{1}{4}$ és $c(\alpha, 1/4) = c(\alpha)$. Ekkor:

$$\left|\frac{x_{i_k}}{y_{i_k}} - \alpha_\ell\right| > \frac{c(\alpha)}{|y_{i_k}|^{r/2+5/4}}.$$

Így:

$$\frac{c(\alpha)}{|y_{i_k}|^{r/2+5/4}}\left|a_r \prod_{\substack{t=1 \\ t\neq\ell}}^{r}\left(\frac{x_{i_k}}{y_{i_k}} - \alpha_t\right)\right| \leq \frac{|m|}{|y_{i_k}|^r}$$

$$c(\alpha)\left|a_r \prod_{\substack{t=1 \\ t\neq\ell}}^{r}\left(\frac{x_{i_k}}{y_{i_k}} - \alpha_t\right)\right| \leq \frac{|m|}{|y_{i_k}|^{r/2-5/4}}.$$

Mivel $k \to \infty$ esetén $\frac{x_{i_k}}{y_{i_k}} \to \alpha_\ell$-hez, ezért a bal oldal véges pozitív nem nulla értékhez tart, mégpedig

$$c(\alpha) \cdot |a_r| \prod_{\substack{t=1 \\ t\neq\ell}}^{r} |\alpha_\ell - \alpha_\ell|$$

-hez. (Ez azért nem 0, mert f irreducibilis, így f-nek nincs többszörös gyöke.) A jobb oldal 0-hoz tart, és ez ellentmondás.

Hivatkozások

[1] A. Thue, *Über Annäherungswerte algebraischer Zahlen*. J. Reine Angew. Math. 1909 (135), 284–305.

[2] MaCTutor, *Axel Thue*, link.

[3] Kép, *Axel Thue*, megtalálható a Wikipédián: link.

17. Geometriai számelmélet

Gausstól származik a következő probléma:

Ha $N \in \mathbb{N}$, hány (x, y) egész számpár létezik, melyre

$$x^2 + y^2 \leq N?$$

Ez az ún. körprobléma.

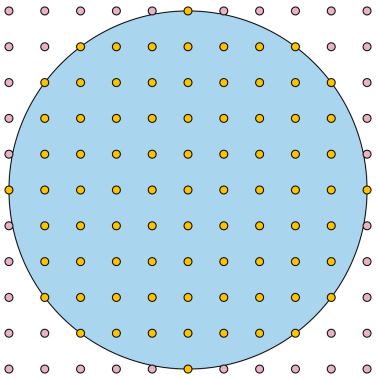
Ugyanis gyököt vonva:

$$\sqrt{x^2 + y^2} \leq \sqrt{N},$$

ahol $\sqrt{x^2 + y^2}$ az (x, y) pont távolsága az origótól.

Másképpen megfogalmazva: Körprobléma:

Az $\{(x, y) : x, y \in \mathbb{Z}\}$ négyzetrácsnak hány rácspontja van a $\sqrt{N}$ sugarú körben?



Jelöljük az ilyen rácspontok számát $F(N)$-nel.

Valószínűleg, Gausst az is motiválta, hogy egy adott szám két négyzetszám összegeként való felírására már ismert formula (ld. 7.4 Tétel), és így érdekes kérdéssé vált az aszimptotikus viselkedés is.

17.1 TÉTEL. (Gauss) *$\forall\, N \in \mathbb{N}$-re*

$$|F(N) - \pi N| < 20\sqrt{N}.$$

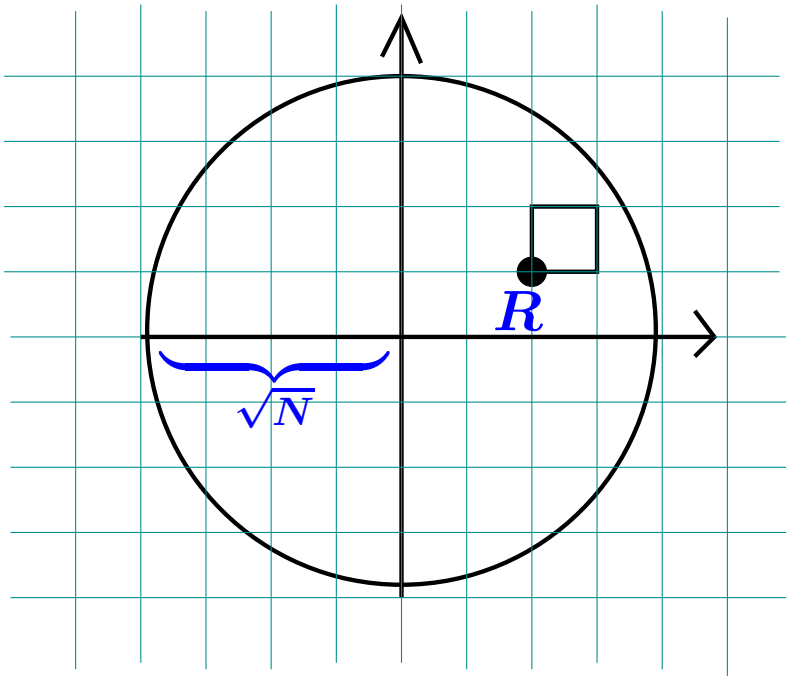
A 17.1 Tétel bizonyítása: Jelölések: Legyen egy területtel rendelkező S halmaz területe $T(S)$. Legyen

$$H = \{(x, y) : x^2 + y^2 \leq N,\ x, y \in \mathbb{Z}\}$$

Ekkor

$$F(N) = |H|$$

$\forall$ H-beli (x, y) rácsponthoz rendeljük azt az egységnégyzetet, amelynek ő a bal alsó csúcsa.



Jelöljük a H-beli R rácsponthoz rendelt négyzetek egyesítését Q-val:

$$Q = \bigcup_{R \in H} \square.$$

Nyilván

$$F(N) = |H| = T(Q).$$

Jelöljük az origó középpontú r sugarú zárt körlemezt

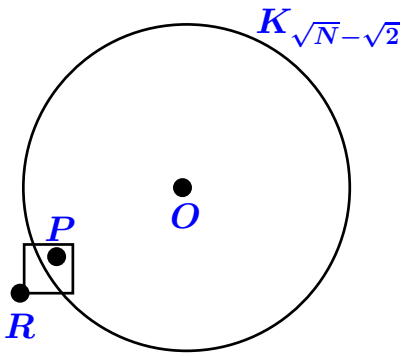
$$\{(x, y) : x^2 + y^2 \leq r^2\} \qquad K_r\text{-rel.}$$

17.2 LEMMA.

$$K_{\sqrt{N}-\sqrt{2}} \underset{\boxed{I.}}{\subset} Q \underset{\boxed{II.}}{\subset} K_{\sqrt{N}+\sqrt{2}}.$$

A 17.2 Lemma bizonyítása. $\boxed{I.}$ Azaz $K_{\sqrt{N}-\sqrt{2}}$-nek $\forall\, P$ pontja benne van egy Q-beli négyzetben.

Tekintsük a négyzetrács P-t tartalmazó négyzetét; ennek bal alsó csúcsa legyen R.



Ekkor

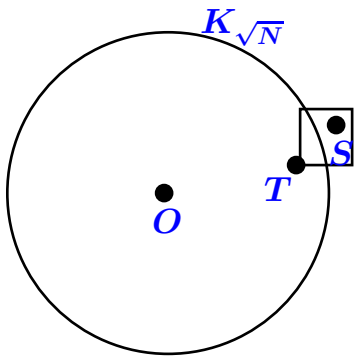
$$\overline{OR} \leq \overline{OP} + \overline{PR} \leq \sqrt{N} - \sqrt{2} + \sqrt{2} = \sqrt{N}.$$

Azaz

$$R \in K_{\sqrt{N}}$$
$$R \in H$$
$$R \in Q$$

Ezzel I.-t igazoltuk.

II. Legyen S egy Q-beli pont. Az S-et tartalmazó négyzet bal alsó csúcsa T. Ekkor $T \in H$.



Nyilván

$$\overline{OS} \leq \overline{OT} + \overline{TS} \leq \sqrt{N} + \sqrt{2}. \text{ Kész.}$$

A lemmából adódóan:

$$T\left(K_{\sqrt{N}-\sqrt{2}}\right) \leq T(Q) = F(N) \leq T\left(K_{\sqrt{N}+\sqrt{2}}\right)$$
$$\left(\sqrt{N}-\sqrt{2}\right)^2 \pi \leq F(N) \leq \left(\sqrt{N}+\sqrt{2}\right)^2 \pi$$
$$N\pi - 2\sqrt{2}\pi\sqrt{N} \leq F(N) \leq \left(N + \underbrace{2\sqrt{2}\sqrt{N}+2}_{\leq 6\sqrt{N}}\right)\pi$$

Azaz:

$$|F(N) - N\pi| \leq 6\pi\sqrt{N},$$
$$|F(N) - N\pi| < 20\sqrt{N}.$$

Vajon a körprobléma mennyire javítható?

Alulról: Már a század elején

$$\neq o\left(N^{1/4}(\log N)^{1/4}\right) \qquad \text{(Hardy [2] 1915)}$$

ma is csak

$$\neq o\big(N^{1/4}(\log N)^{1/4}(\log\log N)^{c}\big) \qquad \text{Erdős és Fuchs [1].}$$

Felülről

$$= O(N^{1/3+\varepsilon}) \qquad \text{Voronoi [4], 1903,}$$
$$= O\left(N^{131/516+\varepsilon}\right) \qquad \text{Huxley [3], 2003.}$$

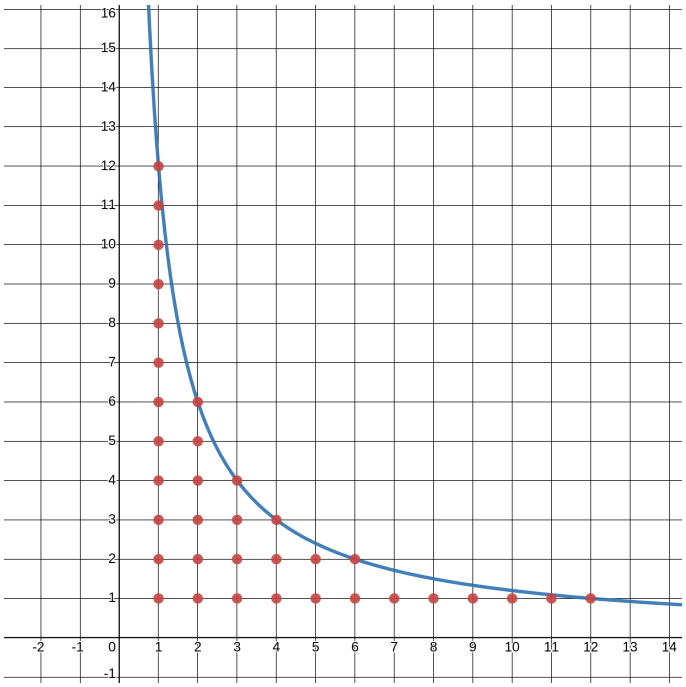
Rokon a Dirichlet-féle osztóproblémával, amely

$$D(N) = \sum_{n=1}^{N} d(n).$$

becsléséből áll. Technikailag is rokon, de utóbbi geometriai nyelven is megfogalmazható, ugyanis

$$D(N) = \sum_{n=1}^{N} d(n) = \sum_{n=1}^{N} \sum_{d|n} 1 = \sum_{d=1}^{N} \sum_{\substack{n\le N \\ d|n}} 1 = \sum_{d=1}^{N} \left[\frac{N}{d}\right],$$

ahol az utóbbi összeg az $y = \dfrac{N}{x}$ hiperbola alatti pozitív rácspontok száma:



Tehát $D(N)$ az $y = \dfrac{N}{x}$ hiperbola alatti első nyílt síknegyedbeli rácspontok száma.

A következő tételben egy pontos becslést adunk $D(N)$-re.

17.3 TÉTEL.

$$D(N) = N \log N + (2\gamma - 1)N + O(\sqrt{N}),$$

ahol γ az ún. Euler–Mascheroni konstans:

$$\gamma \stackrel{\text{def}}{=} \lim_{x \to +\infty} \left(\sum_{n \le x} \frac{1}{n} - \log x \right) \approx 0.5772\ldots.$$

A 17.3 Tétel bizonyítása. $D(N) = \sum_{n=1}^{N} d(n)$ első felírása során a $d(n) = \sum_{d|n} 1$ képletet használtuk.

Jobban járunk, ha $d(n)$-et osztópárok száma szerint számoljuk ki. (a, b) osztópár, ha mindketten n osztói és $n = ab$. Ha az osztópárban $a \le b$, akkor $a \le \sqrt{n}$. Így

$$d(n) = 2 \sum_{d \le \sqrt{n},\ d|n} 1 - \delta_n,$$

ahol

$$d(n) \begin{cases} 1, & \text{ha } n = k^2, \\ 0, & \text{ha } n \neq k^2. \end{cases}$$

Ekkor

$$\begin{aligned} D(n) &= \sum_{n=1}^{N} \left(2 \sum_{d \le \sqrt{n},\ d|n} 1 - \delta_n \right) \\ &= 2 \sum_{n=1}^{N} \sum_{d \le \sqrt{n},\ d|n} 1 - \sum_{n=1}^{N} \delta_n \end{aligned}$$

$$= 2 \sum_{d \le \sqrt{N}} \sum_{\substack{d^2 \le n \le N \\ d \mid n}} 1 - \underbrace{\sum_{n=1}^{N} \delta_n}_{|\{n:\ n \le N,\ n = k^2\}}$$

$$= 2 \sum_{d \le \sqrt{N}} \sum_{\substack{d^2 \le n \le N \\ d \mid n}} 1 - [\sqrt{N}]$$

$$= 2 \sum_{d \le \sqrt{N}} \left(\underbrace{\sum_{\substack{n \le N \\ d \mid n}} 1}_{= \left[\frac{N}{d}\right]} - \underbrace{\sum_{\substack{n < d^2 \\ d \mid n}} 1}_{= d-1} \right) + O(\sqrt{N})$$

$$= 2 \sum_{d \le \sqrt{N}} \frac{N}{d} - \sum_{d \le \sqrt{N}} 2(d-1) + O(\sqrt{N})$$

$$= 2N \sum_{d \le \sqrt{N}} \frac{1}{d} - 2\frac{\left([\sqrt{N}] - 1\right)[\sqrt{N}]}{2} + O(\sqrt{N}).$$

Ismert, hogy az Euler-Mascheroni konstansra fennáll

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right),$$

így

$$\sum_{d \le \sqrt{N}} \frac{1}{d} = \log \sqrt{N} + \gamma + O\left(\frac{1}{\sqrt{N}}\right).$$

Azaz

$$D(N) = 2N \left(\log \sqrt{N} + \gamma + O\left(\frac{1}{\sqrt{N}}\right)\right) - N + O(\sqrt{N})$$
$$= N \log N + (2\gamma - 1)N + O(\sqrt{N}),$$

és ezzel igazoltuk a tételt.

Ezek utána Dirichlet-féle osztóprobléma igazából:

$$A(N) = D(N) - N \log N - (2\gamma - 1)N$$

különbség becslése. Erről ugyanaz mondható el mint a körprobléma hibatagjáról.

Igazán eredményesen mindkét probléma exponenciális összegekkel tárgyalható.

Hivatkozások

[1] P. Erdős, W. H. J. Fuchs, *On a problem of additive number theory*, J. London Math. Soc. 31 (1956), 67–73.

[2] G. H. Hardy, *On the expression of a number as the sum of two squares*, Quarterly Journal of Mathematics. 46 (1915), 263–283.

[3] M. N. Huxley, M. N. *Exponential Sums and Lattice Points III.*, Proc. London Math. Soc. 87, 5910-609, 2003.

[4] G. Voronoi, *Sur un problème du calcul des fonctions asymptotiques*, Journal für die reine und angewandte Mathematik 126 (1903), 241–282.

[5] Kép, Gauss körproblémája, megtalálható a Wikipedián: link.

18. Exponenciális összegek

Mi is az, hogy exponenciális összeg?

Komplex szám exponenciális alakjából indulunk ki:

$$z = r(\cos\varphi + i\sin\varphi) = re^{i\varphi}.$$

Exponenciális összegben tipikusan 1 abszolútértékű, azaz $e^{i\varphi}$ alakú számok összege áll.

Volt szó arról, hogy multiplikatív számelméletben (pl. prímszámelméletben) milyen fontos szerepet játszanak a komplex függvénytani eszközök. Ha ilyen eszközöket használunk, akkor analitikus számelméletről beszélünk.

Vannak azonban a számelméletnek olyan területei is (additív számelmélet, „egyenletes eloszlás”), ahol tipikusan komplex számokkal dolgozunk ugyan, de nincs szükség a komplex függvénytan eszközeire („fél-analitikus” számelmélet).

Mondjuk egy számelméleti probléma kapcsán bizonyos komplex számok összegét kell becsülnünk

$$S = \sum_k z_k.$$

Írjuk a z_k-t exponenciális alakban

$$z = re^{i\varphi} = r(\cos\varphi + i\sin\varphi),$$

ahol $0 \le r$ az abszolútérték, φ az argumentum, ami mod 2π egyértelmű. Azaz

$$S = \sum_k re^{i\varphi_k}.$$

Nagyon sok alkalmazásban r_k fix

$$r_1 = r_2 = \cdots = r_n \ (= 1 \text{ sokszor}).$$

Ilyenkor

$$S = \sum_{k=1}^{n} r e^{i\varphi_k} = r \underbrace{\sum_{k=1}^{n} e^{i\varphi_k}}_{\text{exponenciális összeg}} .$$

Itt az $e^{i\varphi}$ kifejezést úgy írjuk és olvassuk mintha hatvány lenne. ás pedig a természetes logaritmus alapszámának a hatványa. Ezt alátámasztja az a tény, hogy 2 ilyen számot úgy szorozhatunk, illetve 1 ilyet úgy hatványozhatunk, mint általában a hatványokat:

(1) $e^{i\varphi_1} e^{i\varphi_2} = e^{i(\varphi_1+\varphi_2)}$ (Moivre tétele szerint).

(2) $\left(e^{i\varphi}\right)^n = e^{in\varphi}$.

Aztán a komplex függvénytanban derül ki igazán, hogy a valós e^x függvény értelmezése kiterjeszthető a komplex számsíkra, és $e^{i\varphi}$ tekinthető az így nyert

$$e^z : \mathbb{C} \to \mathbb{C}$$

függvény $z = i\varphi$ helyen felvett értékének. Most elég annyit tudni, hogy ilyen $e^{i\varphi}$-kel (1) és (2) szerint számolhatunk.

Miért olyan fontos az $e^{i\varphi}$ kifejezés mint φ függvénye?

Mert periodikus 2π periódussal, hiszen

$$\operatorname{Re} e^{i\varphi} = \cos\varphi, \quad \operatorname{Im} e^{i\varphi} = \sin\varphi$$

is periodikus 2π periódussal

Ebből következik, hogy az $e^{2\pi i\varphi}$ kifejezés mint φ függvénye periodikus 1 periódussal, azaz $e^{2\pi i\varphi}$ értéke csak $\{\varphi\}$-től függ.

Azaz $e^{2\pi i\frac{p}{q}}$ értéke csak p modulo q maradékától függ. Tipikusan ezt a tényt hasznosítjuk az exponenciális összegek alkalmazásaiban. (Másrészt sok problémában elég

$$F(t) = f(e^{i\varphi}) : \mathbb{R} \to \mathbb{C}$$

típusú komplex függvényekre szorítkoznunk.)

Egy illusztráció (régi tétel, új bizonyítással):

18.1 TÉTEL. *Ha $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, akkor az*

$$ax \equiv b \ (m) \ \textit{megoldható}$$
$$\Updownarrow$$
$$(a,m) \mid b, \quad \textit{és ekkor a megoldások száma} (a,m).$$

A 18.1 Tétel bizonyítása. Legyen $x \in \mathbb{Z}$ esetén

$$S_x = \sum_{k=0}^{m-1} \left(e^{2\pi i\frac{ax-b}{m}} \right)^h .$$

Ez mértani sor, melynek kvóciense: $e^{2\pi i\frac{ax-b}{m}}$.

Szeretnénk a mértani sor összegképletét alkalmazni, de ezt csak akkor lehet, ha a kvóciens nem 1. Tehát:

Ha $m \nmid ax - b$, akkor a mértani sor összegképlete alapján

$$S_x = \frac{1 - \left(e^{2\pi i\frac{ax-b}{m}} \right)^m}{1 - e^{2\pi i\frac{ax-b}{m}}} = \frac{0}{\text{valami}} = 0.$$

Vagyis

$$S_x = \begin{cases} m, & \text{ha } x \text{ megoldása } ax \equiv b \quad (m)\text{-nek,} \\ 0, & \text{ha } x \text{ nem megoldása } ax \equiv b \quad (m)\text{-nek.} \end{cases}$$

Így az $ax \equiv b \quad (m)$ megoldásszáma

$$\begin{aligned} S &= \frac{1}{m} \sum_{x=0}^{m-1} S_x \\ &= \frac{1}{m} \sum_{x=0}^{m-1} \sum_{n=0}^{m-1} e^{2\pi i \frac{ax-b}{m} h} \\ &= \frac{1}{m} \sum_{x=0}^{m-1} \sum_{n=0}^{m-1} e^{2\pi i \frac{ax-b}{m} h} \\ &= \frac{1}{m} \sum_{n=0}^{m-1} e^{-2\pi i \frac{b}{m} h} \underbrace{\sum_{x=0}^{m-1} e^{2\pi i \frac{axh}{m}}} \\ &\qquad = \begin{cases} m, & \text{ha } m \mid ah \\ 0 & \text{különben} \end{cases} \\ &\qquad = \begin{cases} m, & \text{ha } \frac{m}{(a,m)} \mid h \\ 0 & \text{különben} \end{cases} \end{aligned}$$

$$\frac{m}{(a,m)} \mid h \Leftrightarrow h = \frac{m}{(a,m)} k, \text{ ahol } k = 0, 1, \ldots, (a,m) - 1,$$

$$\begin{aligned} S &= \frac{1}{m} \sum_{k=0}^{(a,m)-1} e^{-2\pi i \frac{b}{(a,m)} k} \cdot m \\ &= \underbrace{\sum_{k=0}^{(a,m)-1} e^{-2\pi i \frac{b}{(a,m)} k}} \end{aligned}$$

$$= \begin{cases} (a,m), & \text{ha } (a,m) \mid b, \\ 0 & \text{különben.} \end{cases}$$

Ebből a tétel adódik.

Az ELTE matematikus MSc képzésén egy egy féléves tárgy bővebben foglalkozik a területtel, ld. Exponenciális és Karakterösszgek jegyzetünk [1].

Hivatkozások

[1] Gyarmati K., Sárközy A.,*Exponenciális és Karakterösszegek*, link.

19. Generátorfüggvény-módszer

Az analitikus számelméletnek, sőt, az egész számelméletben kulcsszerepet játszik az un. generátorfüggvény elv (Euler). Itt a következőről van szó:

Egy $\{a_1, a_2, \dots\}$ sorozat bizonyos számelméleti tulajdonságait akarjuk vizsgálni. Ezt úgy, hogy

$\{a_1, a_2, \dots\}$-hez egy $f(t)$ függvényt rendelünk. Ezt a (valós, komplex vagy harmonikus) analízis eszközeivel vizsgáljuk, majd az $f(t)$-ről így gyűjtött információból visszakövetkeztetünk az $\{a_1, a_2, \dots\}$ sorozat számelméleti tulajdonságaira. Tehát

$$\{a_1, a_2, \dots\} \to f(t) \text{ ez lehet pl. } \begin{cases} \sum_k e^{a_k i t} & \text{trigonometrikus polinomok, exponenciális összegek} \\ \sum_k \dfrac{a_k}{k^t} & \text{Dirichlet sor,} \\ \sum_k a_k t^k \text{ vagy } \sum t^{a_k} & \text{polinom vagy hatvány sor.} \end{cases}$$

Az első kettőről volt szó. Most a harmadikra egy példa.

19.1 Tétel. (Binet-formula) *Az $F_0 = F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$ $(n = 0, 1, 2, \dots)$ rekurzióval definiált ún. Fibonacci sorozat elemeinek explicit alakja:*

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{\sqrt{5}+1}{2} \right)^{n+1} + (-1)^n \left(\frac{\sqrt{5}-1}{2} \right)^{n+1} \right).$$

Fibonacci az „Az abakusz könyve” című művében vezette be a Fibonacci számokat. Fiatalon bejárta a Mediterráneumot, és hazatérve megismertette Európát az arab-hindi számokkal és a helyiértékes írásmóddal: „Van tíz hindu jel: 9, 8, 7, 6, 5, 4, 3, 2, 1, 0.

Ezen jelek segítségével bármilyen számot fel lehet írni, amit csak akarunk.”

A 19.1 Tételt csak jóval később (500 évvel) bizonyította be de Moivre és Binet.

A 19.1 Tétel bizonyítása. Egy analízisbeli tételre épül.

Ha véges sorozatról van szó: A generátorfüggvény polinom ilyenkor. Ha két $\leq n$-edfokú polinom értéke $n+1$ helyen megegyezik, akkor az együtthatók is megegyeznek.

A végtelen esetben (mint itt):

19.2 LEMMA. (Együtthatók összehasonlításának elve) *Ha két hatványsor konvergens egy intervallumban, és ott $\forall\, x$-re megegyezik az összegfüggvény, akkor az együtthatók is megegyeznek:*

$$\sum_n a_n x^n = \sum_n b_n x^n \quad |x| < r \;\Rightarrow a_n = b_n.$$

A fejezetben szereplő lemmákat nem bizonyítjuk.

Lássuk tehát a tétel bizonyítását. Jelöljük a Fibonacci sorozat generátorfüggvényét $F(x)$-szel. Ekkor

$$F(x) = \sum_{n=0}^{\infty} F_n x^n = F_0 + F_1 x + F_2 x^2 + \cdots + F_n x^n + \dots$$

Teljes indukcióval könnyen igazolható:

$$F_n < 2^n.$$

Így $F(x)$ abszolút konvergens $|x| < 1/2$-re. Tudjuk:

$$\begin{aligned} F(x) &= F_0 + F_1 x + F_2 x^2 + \cdots + F_n x^n + \dots \\ xF(x) &= F_0 x + F_1 x^2 + F_2 x^3 + \cdots + F_n x^{n+1} + \dots \\ x^2F(x) &= F_0 x^2 + F_1 x^3 + F_2 x^4 + \cdots + F_n x^{n+2} + \dots . \end{aligned}$$

Tekintsük az

$$F(x) - xF(x) - x^2F(x) = \underbrace{a_0}_{=1} + \underbrace{(a_1 - a_0)}_{=0} x + \underbrace{(a_2 - a_1 - a_0)}_{=0} x^2 + \dots + \underbrace{(a_n - a_{n-1} - a_{n-2})}_{=0} x^n + \dots$$

egyenletet. Ekkor

$$F(x)(1 - x - x^2) = 1,$$

így minden $1 - x - x^2 \neq 0$ esetén

$$F(x) = \sum_{n=0}^{\infty} a_n x^n = \frac{1}{1 - x - x^2} \quad \text{ha } |x| < 1/2.$$

Tehát, ha $\dfrac{1}{1 - x - x^2}$-et hatványsorba fejtjük: $\dfrac{1}{1 - x - x^2} = \sum_n b_n x^n$, akkor az együtthatók összehasonlításának elve alapján $F_n = b_n$.

Marad

$$\frac{1}{1-x-x^2}$$

hatványsorba fejtése. Ez parciális törtekre bontással.

19.3 Lemma. *Ha $f(x), g(x) \in \mathbb{C}[x]$ és $g(x)$ gyöktényezős alakja*

$$g(x) = a_0(x-x_1)(x-x_2)\cdots(x-x_k),$$

ahol $1 \le i < j \le k$ esetén $i \neq j$ (tehát minden gyök egyszeres), továbbá

$$\deg g(x) > \deg f(x),$$

akkor $\exists$ egyértelmű $A_1, A_2, \ldots, A_k \in \mathbb{C}$, hogy

$$\frac{f(x)}{g(x)} = \frac{A_1}{x-a_1} + \frac{A_2}{x-a_2} + \cdots + \frac{A_k}{x-a_k}.$$

Ezt a lemmát alkalmazva $\frac{1}{1-x-x^2}$-re:

$$x^2 + x - 1 = (x-x_1)(x-x_2),$$

ahol $x_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$.

Így most:

$$\underbrace{\frac{1}{1-x-x^2}}_{-(x-x_1)(x-x_2)} = \frac{A_1}{x - \frac{-1-\sqrt{5}}{2}} + \frac{A_1}{x + \frac{-1-\sqrt{5}}{2}} \qquad / \cdot (x-x_1)$$

$$-\frac{1}{x-x_2} = A_1 + A_2\frac{x-x_1}{x-x_2}$$

teljesül $\forall\, x \neq x_2$-re, így $x = x_1$-re is

$$-\frac{1}{x_1-x_2} = A_1,$$

azaz $A_1 = \frac{1}{\sqrt{5}}$. Ugyanígy $x - x_2$-vel szorozva és aztán $x = x_2$-t helyettesítve $A_2 = -\frac{1}{\sqrt{5}}$.

Tehát:

$$F(x) = \frac{1}{1-x-x^2} = \underbrace{\frac{1}{\sqrt{5}\left(x - \frac{-1-\sqrt{5}}{2}\right)}}_{\text{Bővítjük: } \frac{\sqrt{5}-1}{2}\text{-vel}} - \underbrace{\frac{1}{\sqrt{5}\left(x - \frac{-1+\sqrt{5}}{2}\right)}}_{\text{Bővítjük: } -\frac{\sqrt{5}+1}{2}\text{-vel}}$$

$$= \frac{\sqrt{5}-1}{2\sqrt{5}\left(\frac{\sqrt{5}-1}{2}x + 1\right)} - \frac{\sqrt{5}+1}{2\sqrt{5}\left(-\frac{\sqrt{5}+1}{2}x + 1\right)}$$

A végtelen mértani sor összegképlete:

$$\frac{1}{1-y} = \sum y^n \qquad (|y| < 1).$$

Így:

$$F(x) = \frac{\sqrt{5}-1}{2\sqrt{5}} \sum_{n=0}^{\infty} (-1)^n \left(\frac{\sqrt{5}-1}{2}\right)^n x^n + \frac{\sqrt{5}+1}{2} \sum_{n=0}^{\infty} \left(\frac{\sqrt{5}+1}{2}\right)^n x^n$$

$$= \sum_{n=0}^{\infty} \underbrace{\frac{1}{\sqrt{5}} \left(\left(\frac{\sqrt{5}+1}{2}\right)^{n+1} + (-1)^n \left(\frac{\sqrt{5}-1}{2}\right)^{n+1} \right)}_{F_n} x^n.$$

Hivatkozások

[1] Kép, *Leonardo Fibonacci*, megtalálható a Wikipedián: link.

20. Lefedőrendszerek

A generátorfüggvény-módszerre most egy szép példát látunk Erdős Páltól [1].

Egy

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

kongruencia-rendszert lefedőrendszernek nevezünk, ha

(1) Az $m_1, m_2, \ldots, m_k$ modulusok különbözőek és 1-nél nagyobbak.

(2) Minden természetes szám eleget tesz valamelyik kongruenciának.

Példa.

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 1 \pmod{6} \\ x &\equiv 11 \pmod{12} \end{aligned}$$

Erdős Pál vetette fel a következő, több mint 60 évig megoldatlan problémát: Igaz-e, hogy tetszőleges nagy N számhoz létezik olyan lefedőrendszer, amelynek legkisebb modulusa nagyobb, mint N?

A sejtést végül 2015-ben Hough [3] igazolta, bebizonyítva, hogy lefedőrendszerek legkisebb modulusa kisebb mint 10^{16}.

Erdős Pál és John Selfridge sejtése: Nincs olyan lefedőrendszer, amelynek minden modulusa páratlan.

Szintén megoldatlan sejtés:

Létezik-e négyzetmentes számokból álló lefedőrendszer?

Egy lefedőrendszer egzakt, ha minden természetes szám pontosan egy kongruenciának tesz eleget. Erdős 1950-ben a következőt sejtette: Nem létezik egzakt lefedőrendszer.

A sejtést Mirsky, Newman igazolták, de eredményüket sosem publikálták. Szerencsére, tőlük függetlenül Davenport és Rado [2] megtalálta ugyanazt a bizonyítást.

Most egy generátorfüggvényes bizonyítást ismertetünk, amelyet a kapcsolódó Wikipédia [4] oldalon találtunk.

A bizonyítás indirekt. Tegyük fel, hogy létezik egzakt lefedőrendszer

$$\begin{aligned} x &\equiv a_1 \ \ (m_1) \\ x &\equiv a_2 \ \ (m_2) \\ &\vdots \\ x &\equiv a_k \ \ (m_k) \end{aligned}$$

Feltehető $\forall\, i$-re $0 \leq a_i < m_i - 1$.

Tekintsük a

$$t^{a_1} + t^{a_1+m_1} + t^{a_1+2m_1} + \ldots = \frac{t^{a_1}}{1 - t^{m_1}}$$

$$t^{a_2} + t^{a_2+m_2} + t^{a_2+2m_2} + \ldots = \frac{t^{a_2}}{1-t^{m_2}}$$
$$\vdots$$
$$t^{a_k} + t^{a_k+m_k} + t^{a_k+2m_k} + \ldots = \frac{t^{a_k}}{1-t^{m_k}}$$

hatványsorokat.

Mivel a lefedőrendszer egzakt, ezért mindegyik természetes szám pontosan egy t hatvány kitevőjében szerepel. Vagyis

$$\frac{t^{a_1}}{1-t^{m_1}} + \frac{t^{a_2}}{1-t^{m_2}} + \ldots + \frac{t^{a_k}}{1-t^{m_k}} = \\ = t^0 + t^1 + t^2 + \ldots = \frac{1}{1-t}.$$

Feltehető, hogy a modulusok közül m_k a legnagyobb. Vegyünk egy m_k-adik primitív egységgyököt, ε-t. Tudjuk:

$$\frac{t^{a_1}}{1-t^{m_1}} + \ldots + \frac{t^{a_k}}{1-t^{m_k}} = \frac{1}{1-t}$$

teljesül, ha $|t| < 1$.

Nézzük, mi történik, ha $t \to \varepsilon$-hoz.

$$\frac{t^{a_1}}{1-t^{m_1}} \to \frac{\varepsilon^{a_1}}{1-\varepsilon^{m_1}} \quad \text{(véges)},$$
$$\frac{t^{a_2}}{1-t^{m_2}} \to \frac{\varepsilon^{a_2}}{1-\varepsilon^{m_2}} \quad \text{(véges)},$$
$$\vdots$$
$$\frac{t^{a_{k-1}}}{1-t^{m_{k-1}}} \to \frac{\varepsilon^{a_{k-1}}}{1-\varepsilon^{m_{k-1}}} \quad \text{(véges)}.$$

De $\frac{t^{a_k}}{1-t^{m_k}} \to \infty$. Vagyis

$$\frac{t^{a_1}}{1-t^{m_1}} + \ldots + \frac{t^{a_k}}{1-t^{m_k}} \to \infty.$$

Viszont

$$\frac{1}{1-t} \to \frac{1}{1-\varepsilon} \qquad \text{ez véges,}$$

és így ellentmondásra jutottunk.

Hivatkozások

[1] P. Erdős, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. 2 (1950), 113–123.

[2] P. Erdős, *On a problem concerning congruence systems*, Math. Lapok 3 (1952) 122-128.

[3] R. Hough, *Solution of the minimum modulus problem for covering systems*, Ann. Math. 181 (2015), 361–382.

[4] *Lefedőrendszer (számelmélet)* megtalálható a Wikipedián: link.

21. Prímszámelmélet

1885-ben Stieltjes egy Hermitnek szóló levélben a következő sejtést fogalmazta meg: legyen

$$M(n) = \sum_{k=1}^{n} \mu(k),$$

ahol μ a Möbius függvényt jelöli. Ekkor:

$$|M(n)| < \sqrt{n}.$$

Mertens 1897-ben szintén megfogalmazta a sejtést (immár nyomtatott formában), és azóta Mertens-sejtésként nevezzük.

A Mertens-sejtésnek azaz érdekessége, hogy következne belőle a Riemann-sejtés, ezért sokáig úgy tekintettek rá, hogy biztosan igaz. Mígnem Odlyzko és Riele [7] 1985-ben a Lenstra-Lenstra-Lovász algoritmust használva megcáfolta a sejtést, bebizonyítva, hogy:

$$\liminf \frac{M(n)}{\sqrt{n}} < -1.009 \quad \text{és} \quad \limsup \frac{M(n)}{\sqrt{n}} > 1.06.$$

Két évvel később Pintz János [8] bebizonyította, hogy az első ellenpélda kisebb mint $\approx 10^{1.39 \times 10^{64}}$, amely felső becslést $e^{1.59 \times 10^{40}}$-re javított Kontnik és te Riele [4] 2006-ban. Ma már azt is tudjuk, hogy a sejtésre a legkisebb ellenpélda nagyobb mint 10^{16} ([2]).

A következőkben rátérünk Mertens lengyel matematikus néhány prímszámelméleti eredményének ismertetésére. Mertens [3] az alábbi tételeket 22 évvel a prímszám tétel bizonyítása előtt ismertette (1874), és tulajdonképpen fontos lépések voltak a prímszámtétel teljes bizonyításához.

A továbbiakban minden p-n futó szummát úgy értelmezünk, hogy a szumma a p prímeken fut.

21.1 TÉTEL. (Mertens I. tétele)

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$$

A 21.1 Tétel bizonyítása.

A következő Legendre-tól származó lemmát használjuk.

21.2 LEMMA. *$n \in \mathbb{N}$ esetén $n!$ kvadratikus alakja*

$$n! = \prod_{p \le n} p^{\alpha_p},$$

ahol

$$\alpha_p = \sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right].$$

A 21.2 Lemma bizonyítása. Az, hogy a $\prod$ csak $p \leq n$ prímeken fut triviális Csak

$$\alpha_p = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right]$$

szorul bizonyításra.

Milyen tényezők járulnak hozzá p kitevőjéhez a kanonikus alakban? Csak a p többszörösei.

$$n! = 1 \cdot 2 \cdot \dots \cdot p \cdot \dots \cdot 2p \cdot \dots \qquad \left[\frac{n}{p}\right] p \qquad \dots \cdot n.$$

(p legnagyobb többese)

$\left[\frac{n}{p}\right]$ ilyen van, mind hozzájárul legalább egy p-faktorral. De van olyan többszörös, ami 2-vel járul hozzá a kitevőhöz, t.i. p^2 többszörösei.

$$n! = 1 \cdot 2 \cdot \dots \cdot p^2 \cdot \dots \cdot p^4 \cdot \dots \left[\frac{n}{p^2}\right] p^2 \cdot \dots \cdot n.$$

még egy p-vel; $\left[\frac{n}{p^2}\right]$ ilyen van

Azután p^3 többesei még egy p-vel: $\left[\frac{n}{p^3}\right]$ ilyen van. Összesen p kitevője:

$$\alpha_p = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots.$$

Az alábbi a Stirling-formula következménye:

21.3 Lemma.

$$\sum_{k=1}^{n} \log k = n \log n - n + O(\log n).$$

A 21.3 Lemma bizonyítása. A Stirling formula alapján:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n = \theta_n\sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

ahol $\theta_n \to 1$.

Logaritmust véve:

$$\sum_{k=1}^{n} \log k = \log\theta_n + \log\sqrt{2\pi} + \frac{1}{2}\log n + n\log n - n.$$

Ezek után a tétel bizonyítása: A 21.2 Lemma alapján:

$$\prod_{p\le n} p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]} = n!.$$

Logaritmust véve:

$$\sum_{p\le n}\log\left(p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]}\right) = \sum_{k=1}^{n}\log k \underset{\text{21.3 Lemma}}{=} n\log n - n + O(\log n). \tag{21.1}$$

A baloldal:

$$\sum_{p\le n}\left(\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]\right)\log p = \sum_{p\le n}\left(\frac{n}{p} + \left(\left[\frac{n}{p}\right] - \frac{n}{p}\right) + \sum_{k=2}^{\infty}\left[\frac{n}{p^k}\right]\right)\log p$$
$$= n\sum_{p\le n}\frac{\log p}{p} + \underbrace{\sum_{p\le n}\left(\left[\frac{n}{p}\right] - \frac{n}{p}\right)\log p}_{R_1} + \underbrace{\sum_{p\le n}\sum_{k=2}^{\infty}\left[\frac{n}{p^k}\right]\log p}_{R_2} \tag{21.2}$$

Ezután R_1-t és R_2-t becsüljük:

$$|R_1| \le \sum_{p\le n}\left|\left[\frac{n}{p}\right] - \frac{n}{p}\right|\log n$$

$$\leq \log n \sum_{p \leq n} 1 = \log n \cdot \pi(n) = \log n \cdot O\left(\frac{n}{\log n}\right)$$
$$= O(n). \tag{21.3}$$

$$|R_2| \leq \sum_{p \leq n} n \log p \sum_{k=2}^{\infty} \frac{1}{p^k} = \sum_{p \leq n} \frac{n \log p}{p^2} \underbrace{\sum_{i=0}^{\infty} \frac{1}{p^i}}_{\frac{1}{1-\frac{1}{p_i}} \leq \frac{1}{1-\frac{1}{2}} = 2}$$
$$\leq 2n \sum_{p} \frac{\log p}{p^2}$$
$$< 2n \sum_{k=1}^{\infty} \frac{\log k}{k^2} = O(n) \tag{21.4}$$

Összefoglalva: (21.1), (21.2), (21.3) és (21.4) alapján:

$$n \sum_{p \leq n} \frac{\log p}{p} + O(n) = n \log n - n + O(\log n)$$
$$n \sum_{p \leq n} \frac{\log p}{p} = n \log n + O(n)$$
$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

Ezzel $x = n \in \mathbb{N}$ esetén készen is vagyunk.

Végül:

$$\sum_{p \leq x} \frac{\log p}{p} = \sum_{p \leq [x]} \frac{\log p}{p} = \log[x] + O(1) = \log x + O(1).$$

Ebből levezethető, hogy $\sum \frac{1}{p}$ divergens (Euler), sőt,

21.4 TÉTEL. (Mertens II. tétele) *$x \to \infty$ esetén*

$$\sum_{p \le x} \frac{1}{p} = \log\log x + M + O\left(\frac{1}{\log x}\right),$$

ahol M az ún. Meissel–Mertens konstans, $M \approx 0.261497212847642783755426838608695859051 6\ldots$.

A 21.4 Tétel bizonyítása. Mi kicsit kevesebbet bizonyítunk, csak

$$\sum_{p \le x} \frac{1}{p} = \log\log x + O(1).$$

A bizonyítás parciális összegzésen vagy más néven Ábel átrendezésen múlik.

21.5 LEMMA. *Ha $n \in \mathbb{N}$, $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{C}$, akkor*

$$A_k \overset{\text{def}}{=} \begin{cases} 0 & \text{ha } k = 0 \\ \sum_{i=1}^{k} a_i & \text{ha } k = 1, 2, \ldots, n \end{cases}$$

-et írva

$$\begin{aligned} \sum_{i=1}^{n} a_i b_i &= \sum_{i=1}^{n} (A_i - A_{i-1}) b_i \\ &= \sum_{i=1}^{n} A_i (b_i - b_{i+1}) + A_n b_n \end{aligned} \tag{21.5}$$

Megjegyzés. Tipikusan akkor alkalmazzuk, ha

(i) $a_1, a_2 \ldots, b_1, b_2, \cdots \in \mathbb{R}$

(ii) A_k-kra jó aszimptotika van

(iii) $b_1, b_2, \ldots$ monoton és $b_i - b_{i+1}$-re jó formula van.

Nézzük tehát 21.4 Tétel bizonyítását. Az előző lemmát alkalmazuk

$$a_i = \begin{cases} \dfrac{\log i}{i} & \text{ha } i = p \text{ prím} \\ 0 & \text{ha } i \neq p \text{ nem prím,} \end{cases}$$

$$b_i = \begin{cases} \dfrac{1}{\log i} & \text{ha } i > 1 \\ 1 & \text{ha } i = 1 \end{cases}$$

választással.

Ekkor (21.5) baloldala:

$$\begin{aligned} S_n &= \sum_{i=1}^{n} a_i b_i \\ &= \sum_{p \leq n} \frac{\log p}{p} \cdot \frac{1}{\log p} \end{aligned}$$

Most:

$$A_i = \begin{cases} a_1 = 0 \text{ ha } i = 1 \\ \sum\limits_{j \leq i} a_j = \sum\limits_{p \leq i} \dfrac{\log p}{p} & \text{ha i>1.} \end{cases}$$

Vagyis (21.5) jobboldala:

$$\sum_{i=1}^{n-1} A_i (b_i - b_{i+1}) + A_n b_n =$$

mivel $A_1 = 0$:

$$= \sum_{i=2}^{n-1} \left(\frac{\log p}{p} \right) \left(\frac{1}{\log i} - \frac{1}{\log (i+1)} \right) + \sum_{p \leq n} \frac{\log p}{p} \cdot \frac{1}{\log n}$$

legyen $\delta_i \stackrel{\text{def}}{=} \sum_{p\le i} \frac{\log p}{p} - \log i \; (= O(1),$ Mertens I. tétele)

$$= \sum_{i=2}^{n-1} (\log i + \delta_i) \left(\frac{1}{\log i} - \frac{1}{\log(i+1)} \right) + (\log n + O(1)) \frac{1}{\log n}$$

$$= \underbrace{\sum_{i=2}^{n} \log i \left(\frac{1}{\log i} - \frac{1}{\log(i+1)} \right)}_{\sum_1} + \underbrace{\sum_{i=2}^{n} \delta_i \left(\frac{1}{\log i} - \frac{1}{\log(i+1)} \right)}_{\sum_2} + O(n)$$

Itt

$$\sum\nolimits_1 = \sum_{i=2}^{n-1} \log i \left(\frac{1}{\log i} - \frac{1}{\log(i+1)} \right)$$

visszarendezve

$$\sum\nolimits_1 = \sum_{i=2}^{n} \frac{1}{\log i} (\log i - \log(i-1)) - \frac{\log n}{\log n}.$$

Következőkben megjegyezzük, hogy

$$\log i - \log(i-1) = -\log \frac{i-1}{i} = -\log \left(1 - \frac{1}{i} \right)$$

-re használhatjuk a

$$\log(1-x) = -x - \frac{x^2}{2} - \frac{x^3}{3} - \cdots = -x + O(x^2)$$

összefüggést, azaz

$$\log i - \log(i-1) = \frac{1}{i} + O\left(\frac{1}{i^2} \right).$$

Így

$$\sum\nolimits_1 = \sum_{i=2}^{n} \frac{1}{\log i} (\log i - \log(i-1)) - \frac{\log n}{\log n}$$

$$= \sum_{i=2}^{n} \frac{1}{\log i} \left(\frac{1}{i} + O\left(\frac{1}{i^2} \right) \right) - 1$$
$$= \sum_{i=2}^{n} \frac{1}{i \log i} + O\left(\sum_{i=2}^{n} \frac{1}{i^2 \log i} \right) - 1$$
$$= \sum_{i=2}^{n} \frac{1}{i \log i} + O(1).$$

Itt

$$\sum_{i=2}^{n} \frac{1}{i \log i} = \int_2^x \frac{dx}{x \log x} + O(1)$$
$$= [\log \log x]_2^n + O(1)$$
$$= \log \log n + O(1).$$

Azaz

$$\sum_1 = \log \log n + O(1).$$

Következik $\sum_1$ becslése. Emlékeztetünk δ_i definíciójára:

$$\sum_{p \le i} \frac{\log p}{p} - \log i \ = O(1).$$

Ekkor:

$$\left| \sum\nolimits_2 \right| = \sum_{i=2}^{n-1} |\delta_i| \cdot \left| \frac{1}{\log i} - \frac{1}{\log(i+1)} \right|$$
$$= \sum_{i=2}^{n-1} O(1) \left(\frac{1}{\log i} - \frac{1}{\log(i+1)} \right)$$
$$= O\left(\sum_{i=2}^{n-1} \frac{1}{\log i} - \frac{1}{\log(i+1)} \right)$$
$$= O\left(\frac{1}{\log 2} \right)$$
$$= O(1).$$

Vagyis

$$S_n = \sum_{p \le n} \frac{1}{p} = \log\log n + O(1).$$

Ezzel a tételt, ha x egész be is bizonyítottuk.

Tetszőleges x-re felírjuk a már bizonyított összefüggés x helyén $[x]$-szel, és használjuk, hogy $\log\log x - \log\log[x] = o(1)$.

21.6 TÉTEL. (Mertens III. tétele)

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) \sim \frac{c}{\log x},$$

ahol $c = e^{-\gamma} \approx 0.561459483566885\ldots$ *(itt* γ *az ún. Euler–Mascheroni konstans).*

A Tétel Mertens II. tételéből következik.

(Megjegyezzük, hogy Mertens II. tételének általunk bizonyított gyengébb verzióból csak

$$\frac{c_1}{\log x} < \prod_{p \le x} \left(1 - \frac{1}{p}\right) < \frac{c_2}{\log x}$$

következne...)

A 21.6 Tétel bizonyítása. A bizonyításban nem határozzuk meg a c konstans értéket. Legyen

$$\rho(p) \stackrel{\text{def}}{=} \log\left(1 - \frac{1}{p}\right) + \frac{1}{p}.$$

Ekkor

$$\log(1 - x) = -x + O(x^2)$$

miatt

$$\rho(p) = O\left(\frac{1}{p^2}\right).$$

Itt $\sum_p \rho(p)$ abszolút konvergens.

Ekkor

$$\begin{aligned}\sum_{p\le x}\left(1-\frac{1}{p}\right) &= e^{\log\prod_{p\le x}\left(1-\frac{1}{p}\right)}\\ &= e^{\sum_{p\le x}\log\left(1-\frac{1}{p}\right)}\\ &= e^{\sum_{p\le x}\left(-\frac{1}{p}+\rho(p)\right)}\\ &= e^{-\sum_{p\le x}\frac{1}{p}+\sum_p\rho(p)-\sum_{p>x}\rho(p)}\\ &= e^{-(\log\log x+c_1+o(1))+c_2+o(1)}\\ &= e^{-\log\log x+c_3}\cdot e^{o(1)}\\ &= \frac{e^{c_3}}{\log x}(1+o(1)),\end{aligned}$$

ezzel a bizonyítást befejeztük.

A $\pi(x)$ elemi becslése a legtöbb elsőéves kurzuson szerepel. Emlékeztetőül: bebizonyítottuk, hogy $\exists c_1, c_2 > 0$ konstans, hogy

$$c_1\frac{x}{\log x} < \pi(x) < c_2\frac{x}{\log x} \qquad x \ge 2. \tag{21.6}$$

Továbbá kimondtuk a prímszámtételt:

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

Ez az élesebb változat most még túl nehéz lenne. De visszatérve (21.6)-re, egy (az első évben megadottól különböző) elegáns és tanulságos bizonyítást adunk az alsó becslésre.

21.7 TÉTEL. *Ha $n \in \mathbb{N}$, $n \ge 7$, akkor*

$$\log 2\frac{n}{\log n} < \pi(n).$$

A 21.7 Tétel bizonyítása. A bizonyítás Gelfond és Schnirelmann ötletét használja (ld. Gelfond szerkesztői megjegyzéseit [1]-ben), melyet később Nair [5], [6] újra felfedezett.

21.8 LEMMA. *$n \geq 7$ esetén $[1, 2, \ldots, n] > 2^n$.*

Ez elég ugyanis

$$2^n < [1, 2, \ldots, n] = \prod_{p \leq n} p^{\alpha_p} \leq \prod_{p \leq n} n = n^{\pi(n)}.$$

$$\uparrow$$

$$\text{ahol } \; p^{\alpha_p} \leq n < p^{\alpha_p + 1}$$

A logaritmus függvény szigorúan monoton:

$$n \log 2 < \pi(n) \log n$$

$$\log 2 \frac{n}{\log n} < \pi(n).$$

A 21.8 Lemma bizonyítása. Tegyük fel, hogy k, ℓ természetes számok, $1 \leq k \leq \ell$; tekintsük

$$\begin{aligned} I(k, \ell) &\overset{\text{def}}{=} \int_0^1 \underbrace{x^{k-1}(1-x)^{\ell-k}}_{\substack{\text{egész együtthatós} \\ \ell-1\text{-ed fokú polinom}}} dx \\ &= \int_0^1 \left(a_{\ell-1} x^{\ell-1} + a_{\ell-2} x^{\ell-2} + \cdots + a_1 x + a_0 \right) dx \\ &= a_{\ell-1} \int_0^1 x^{\ell-1} dx + a_{\ell-2} \int_0^1 x^{\ell-2} dx + \cdots + a_1 \int_0^1 x dx + a_0 \\ &= \frac{a_{\ell-1}}{\ell} + \frac{a_{\ell-2}}{\ell - 1} + \cdots + a_1 \frac{1}{2} + a_0 \\ &= \frac{u}{v}, \end{aligned}$$

ahol u, v egész, $(u, v) = 1$, $v >$, $v \mid [1, 2, \ldots, \ell]$.

De $I(k, \ell)$, azaz v közvetlenül kiszámolható.

Tekintsük tetszőleges y-ra

$$\sum_{k=1}^{\ell}\binom{\ell-1}{k}y^{k-1}I(k,\ell)=\sum_{k=1}^{\ell}\binom{\ell-1}{k}y^{k-1}\int_0^1 x^{k-1}(1-x)^{\ell-k}dx$$
$$=\int_0^1\sum_{k=1}^{\ell}\binom{\ell-1}{k}(xy)^{k-1}(1-x)^{\ell-k}dx$$

a binomiális tétel szerint

$$=\int_0^1 (xy+(1-x))^{\ell-1}\,dx$$
$$=\int_0^1 (1+x(y-1))^{\ell-1}\,dx$$
$$\left[\frac{(1+x(y-1))^{\ell}}{\ell(y-1)}\right]_0^1$$
$$=\frac{y^{\ell}}{\ell(y-1)}-\frac{1}{\ell(y-1)}$$
$$=\frac{1}{\ell}\cdot\frac{y^{\ell}-1}{y-1}$$
$$=\frac{1}{\ell}\sum_{k=1}^{\ell}y^{k-1}.$$

Tehát

$$\sum_{k=1}^{\ell}\binom{\ell-1}{k}y^{k-1}I(k,\ell)=\frac{1}{\ell}\sum_{k=1}^{\ell}y^{k-1}.$$

Itt a jobb és baloldalon y-nak két polinomja áll, amelyekre a helyettesítési értékek minden y-ra megegyeznek. Azaz a megfelelő együtthatóik is megegyeznek, vagyis

$$\binom{\ell-1}{k-1}I(k,\ell)=\frac{1}{\ell}.$$

Tehát

$$I(k,\ell)=\frac{1}{\ell\binom{\ell-1}{k-1}}=\frac{1}{k\binom{\ell}{k}}.$$

Itt a jobboldalon eredetileg $\frac{u}{v}$ volt, ahol $(u,v)=1$, azaz most $u=1$, $v=k\binom{\ell}{k}$. Vagyis $v=k\binom{\ell}{k} \mid [1,2,\dots,\ell]$.

Speciálisan $k=m$, $\ell=2m$-et véve

$$m\binom{2m}{m}\Big| [1,2,\dots,2m] \mid [1,2,\dots,2m+1].$$

Hasonlóan, $k=m$, $\ell=2m+1$-et véve

$$\underbrace{m\binom{2m+1}{m}}_{(2m+1)\binom{2m}{m}} \mid [1,2,\dots,2m+1].$$

Az előbbi két oszthatóságot összefoglalva:

$$\left[m\binom{2m}{m},\ m\binom{2m+1}{m}\right] \mid [1,2,\dots,2m+1].$$

Vagyis

$$m(2m+1)\binom{2m+1}{m}] \mid [1,2,\dots,2m+1].$$

Azaz

$$\begin{aligned}[1,2,\dots,2m+1] &\geq m(2m+1)\binom{2m}{m}\\ &> m\left(\binom{2m}{0}+\binom{2m}{1}+\binom{2m}{2}+\dots+\binom{2m}{2m}\right)\\ &= m2^{2m}.\end{aligned}$$

Így, ha $m\geq 2$ ($\Rightarrow\ 2m+1\geq 5$), akkor

$$[1,2,\dots,2m+1] > 2\cdot 2^{2m} = 2^{2m+1}.$$

Továbbá, $m\geq 4$ ($\Rightarrow\ 2m+2\geq 10$), akkor

$$[1,2,\dots,2m+2] > [1,2,\dots,2m+1] > m\cdot 2^{2m} \geq 4\cdot 2^{2m} = 2^{2m+2}.$$

Összefoglalva:

$$[1, 2, \ldots, n] > 2^n, \qquad \text{ha } n \geq 9.$$

Végül $n = 7$-re, 8-ra kiszámolható:

$$[1, 2, \ldots, 7] = 420 > 128 = 2^7$$
$$[1, 2, \ldots, 8] = 840 > 256 = 2^8.$$

Ezzel a lemmát igazoltuk.

Hivatkozások

[1] P.L. Chebyshev, *Collected Works*, Vol. 1, Theory of Numbers, Akad. Nauk SSSR (Moscow, 1944).

[2] G. Hurst, *Computations of the Mertens function and improved bounds on the Mertens conjecture*, Mathematics of Computation 87 (310) (2018), 1013-1028.

[3] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. Reine Angew. Math. 78 (1874), 46–62.

[4] T. Kotnik, H. te Riele, *The Mertens Conjecture Revisited* Lecture Notes in Computer Science 4076, 2006, 156-167.

[5] M. Nair, *On Chebyshev's-type inequalities for primes*, Amer. Math. Montly 89 (1982), 126–129.

[6] M. Nair, *A new method in elementary prime number theory*, J. London Math. Soc. 25 (2) (1982), 385–391.

[7] A. M. Odlyzko, H. J. J. te Riele *Disproof of the Mertens conjecture*, Journal für die reine und angewandte Mathematik (357) (1985), 138–160.

[8] J. Pintz, *An effective disproof of the Mertens conjecture*, Astérisque. 147–148 (1987), 325–333.

[9] Kép, Franz Mertens, megtalálható: link.

22. Transzcendens számok.

Hermite 1873-ban igazolta, hogy az e transzcendens. Módszerét általánosítva 9 évvel később Lindemann bebizonyította, hogy a π is transzcendens.

C. Hermite

C. L. F. von Lindemann

Ma már sok bizonyítás ismert ennek a két tételnek az igazolására, vannak köztük viszonylag elemiek is, pl. elemi bizonyítást találunk a következő oldalon is: link.

Mi most nem térünk rá a fenti elemi bizonyítások ismertetésére, hanem inkább megnézzük, hogy vajon milyen általánosabb tételek léteznek transzcendencia bizonyítására. A legismertebb ezek közül a következő:

22.1 TÉTEL. (Lindemann-Weierstrass) *Ha $\alpha_1, \alpha_2, \ldots, \alpha_n$ algebrai számok lineárisan függetlenek $\mathbb{Q}$ felett, akkor $e^{\alpha_1}, \ldots, e^{\alpha_n}$ algebrailag független $\mathbb{Q}$ felett, azaz nincs olyan konstans nullától különböző többváltozós racionális együtthatós polinom, amelynek $e^{\alpha_1}, \ldots, e^{\alpha_n}$ gyöke.*

Baker 1990-ben [1, 1. fejezet, 1.4. Tétel] újrafogalmazta ezt a tételt a következő állítás formájában:

22.2 TÉTEL. *Ha $a_1, a_2, \ldots, a_n$ algebrai számok és $\alpha_1, \alpha_2, \ldots, \alpha_n$ különböző algebrai számok, akkor*

$$a_1 e^{\alpha_1} + a_2 e^{\alpha_2} + \cdots + a_n e^{\alpha_n} = 0$$

egyenletnek csak akkor teljesülhet, ha $a_1 = a_2 = \cdots = a_n = 0$.

Ha meggondoljuk, ebből a tételből azonnal következik, hogy az e transzcendens.

Ha ugyanis e gyöke az $a_n x^n + \cdots + a_1 x + a_0$ racionális együtthatós nem nulla polinomnak, akkor a 22.2 Tételt alkalmazva az $\alpha_0 = 0, \alpha_1 = 1, \ldots, \alpha_n = n$ számokra, azt kapjuk, hogy $a_0 e^{\alpha_0} + a_1 e^{\alpha_1} + \cdots + a_n e^{\alpha_n} = 0$-ból adódóan $a_0, a_1, \ldots, a_n$ számokra $a_0 = a_1 = \cdots = a_n = 0$ teljesül, és ez ellentmondás.

A π transzcendenciája is következik a tételből, ugyanis, ha π algebrai szám, akkor $i\pi$ is (mivel ekkor i és π algebrai szám, ezért $i\pi$ is. Ugyanerre elemi bizonyítás:

ha π gyöke az $f(x)$ egész együtthatós polinomnak, akkor $i\pi$ gyöke az $f(ix)f(-ix)$ polinomnak. De $f(ix)f(-ix)$ egész együtthatós, hiszen $f(ix) = g(x) + ih(x)$ alakú, ahol $g(x), h(x)$ egész együtthatós polinom. Ekkor $f(-ix) = \overline{f(ix)} = g(x) - ih(x)$ és $f(ix)f(-ix) = g^2(x) + h^2(x)$.)

Ha $i\pi$ algebrai szám, akkor a Lindemann-Weierstrass tételből következik, hogy

$$a_1 e^0 + a_2 e^{i\pi} = 0$$

csak akkor teljesülhet, ha $a_1 = a_2 = 0$. Azonban az Euler-azonosság miatt $e^{i\pi} = -1$, azaz $1 + e^{i\pi} = 0$ mégis teljesül, és ez ellentmondás.

A Lindemann-Weierstrass tétel bizonyítása túl megy jelen jegyzetünk keretein.

Fontos azonban megemlíteni, hogy Baker továbbfejlesztette a fenti módszert, megalkotva a híres Baker-módszert.

A Baker módszerről egy nagyon jó kis magyar nyelvű összefoglalót olvashatunk Pink István [2] tollából, amely az alábbi helyen érhető el: link.

A cikk utolsó részében példát is láthatunk a Baker-módszer alkalmazására, nevezetesen a $3^n - 2^m = 1$ (speciális Catalan egyenletnek) nincs más megoldása az egészek körében mint $(n, m) = (2, 3)$.

Visszatérve a transzcendenciára, bizonyítás nélkül megemlítjük még a híres Gelfond-Schneider tételt is:

22.3 TÉTEL. (Gelfond-Schneider) *Ha a és b algebrai számok, melyekre $a \notin \{0, 1\}$ és b irracionális szám, akkor a^b transzcendens.*

Ebből a tételből például könnyen következik, hogy $\sqrt{2}^{\sqrt{2}}$ transzcendens, hiszen, ha $a = \sqrt{2}^{\sqrt{2}} \notin \{0, 1\}$ algebrai lenne, akkor mivel

$b = \sqrt{2}$ is algebrai szám, a tétel értelmében a^b transzcendens, de

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2.$$

A következő oldalon jó pár példát láthatunk transzcendens számokra, és olyan számokra is, amelyekről ma még csak sejtés, hogy transzcendensek: link.

Hivatkozások

[1] A. Baker, *Transcendental number theory*, Cambridge Mathematical Library (2nd ed.), Cambridge University Press 1990.

[2] Pink I., *A Baker-módszer és egy alkalmazása*, Érintő 23 (2022), link.

[3] Kép, *Alan Baker*, megtalálható: link.

[4] Kép, *Charles Hermite*, megtalálható a Wikipédián: link.

[5] Kép, *Carl Louis Ferdinand von Lindemann*, megtalálható a Wikipédián: link.