Nevezetes számelméleti problémák

Tartalom

6.1. Definíció.

Az $(x, y, z) \in \mathbb{N}^3$ számhármast **pitagoraszi számhármasnak** nevezzük, ha $x^2 + y^2 = z^2$. Az (x, y, z) pitagoraszi számhármas **primitív**, ha $\text{lnko}(x, y, z) = 1$.

6.2. Megjegyzés.

Tetszőleges (x, y, z) pitagoraszi számhármas esetén $(x/d, y/d, z/d)$ primitív pitagoraszi számhármas, ahol $d = \text{lnko}(x, y, z)$. Tehát elegendő a primitív pitagoraszi számhármasokat meghatározni, mert ezekből minden pitagoraszi számhármas megkapható (egy konstanssal való szorzással).

Példa.

- $(3, 4, 5)$
- $(5, 12, 13)$
- $(8, 15, 17)$
- $(7, 24, 25)$
- $\ldots$

Titkos lemma.

Ha ab négyzetszám és $a \perp b$, akkor a és b is négyzetszám.

Bizonyítás.

Egy természetes szám akkor és csak akkor négyzetszám, ha prímhatványtényezős felbontásában minden prím páros kitevővel szerepel.

Tegyük fel, hogy ab négyzetszám és $a \perp b$. Legyen p egy tetszőleges prímszám. Mivel ab négyzetszám, p kitevője ab prímfelbontásában páros; legyen mondjuk $2k$.

Az a és b számok közül csak az egyik lehet p-vel osztható, mert $a \perp b$. Tehát p kitevője a és b prímfelbontásában $2k$, illetve 0 (vagy fordítva).

Ezzel beláttuk, hogy a-ban is és b-ben is minden prím páros kitevővel szerepel, így tehát a és b is négyzetszám. □

6.3. Lemma.

Primitív pitagoraszi számhármasban a tagok páronként is relatív prímek.

Bizonyítás.

Legyen (x, y, z) primitív pitagoraszi számhármas, $d := \text{lnko}\,(x, y)$.

$$
\begin{aligned}
d \mid x, y \quad &\Longrightarrow \quad d^2 \mid x^2, y^2 \\
&\Longrightarrow \quad d^2 \mid x^2 + y^2 = z^2 \\
&\Longrightarrow \quad d \mid z \\
&\Longrightarrow \quad d \mid \text{lnko}\,(x, y, z) \\
&\Longrightarrow \quad d = 1 \\
&\Longrightarrow \quad x \perp y
\end{aligned}
$$

Hasonlóan igazolható, hogy $x \perp z$ és $y \perp z$. □

6.4. Lemma.

Ha (x, y, z) primitív pitagoraszi számhármas, akkor x és y paritása különböző, z pedig páratlan.

Bizonyítás.

Páros szám négyzete nullát, páratlan szám négyzete pedig egyet ad maradékul 4-gyel osztva. Ezt felhasználva . . .

$x \bmod 2$	$y \bmod 2$	$x^2 + y^2 = z^2 \bmod 4$	
0	0	0	↯
0	1	1	✓
1	0	1	✓
1	1	2	↯

□

6.5. Tétel.

Legyen (x, y, z) primitív pitagoraszi számhármas, és tegyük fel, hogy x páros. Ekkor léteznek olyan u, v természetes számok, melyekre

$$u > v,\ u \not\equiv v \pmod 2,\ \text{lnko}(u, v) = 1, \text{ és } x = 2uv,\ y = u^2 - v^2,\ z = u^2 + v^2.$$

Fordítva, a fenti *formulákkal definiált (x, y, z) számhármas mindig primitív pitagoraszi számhármas.*

Bizonyítás.

Először azt mutatjuk meg, hogy minden primitív pitagoraszi számhármal előáll a fenti módon. Tfh. (x, y, z) primitív pitagoraszi számhármas, és x páros.

$$x^2 + y^2 = z^2 \implies x^2 = z^2 - y^2 = (z + y)(z - y) \implies \left(\frac{x}{2}\right)^2 = \underbrace{\frac{z + y}{2}}_{U} \cdot \underbrace{\frac{z - y}{2}}_{V}.$$

Mivel $U \perp V$ (lásd a következő oldalon) és szorzatuk négyzetszám, ezért U és V is négyzetszám: $U = u^2$ és $V = v^2$.

$$u^2 + v^2 = z \checkmark \qquad u^2 - v^2 = y \checkmark \qquad 2uv = x \checkmark$$

Bizonyítás (folyt.)

Ha $k \mid U, V$, akkor $k \mid U + V = z$ és $k \mid U - V = y$. Mivel $z \perp y$ (miért?), ez csak $k \sim 1$ esetén lehetséges. Tehát U és V relatív prímek.

Ebből következik, hogy u és v is relatív prímek, hiszen $U = u^2$ és $V = v^2$ (miért?).

Tudjuk, hogy $u^2 - v^2 = y$, és ez egy pozitív páratlan szám. Így $u > v$ és $u \not\equiv v \pmod 2$. ◊

A másik irány igazolásához tegyük fel, hogy

$$u > v,\ u \not\equiv v \pmod 2,\ \text{lnko}\,(u, v) = 1, \text{ és } x = 2uv,\ y = u^2 - v^2,\ z = u^2 + v^2.$$

Az $x^2 + y^2 = z^2$ egyenlőséget egyszerű számolás mutatja.

A számhármas primitívségéhez elegendő azt belátni, hogy $y \perp z$.
Ha $k \mid y, z$, akkor $k \mid y + z = 2u^2$ és $k \mid z - y = 2v^2$. Mivel $u \perp v$, ez csak $k \sim 1, 2$ esetén lehetséges. Node $2 \nmid y$, hiszen y páratlan. Tehát $k \sim 1$, azaz $y \perp z$. □

Példa.

Néhány kis u, v értékkel adódó primitív pitagoraszi számhármas:

u	v	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	4	40	9	41
5	2	20	21	29

6.6. Tétel (Fermat, 1640).

Az $x^4 + y^4 = z^4$ egyenletnek nincs pozitív egészekből álló megoldása.

6.7. Tétel (nagy Fermat-tétel, Wiles és Taylor, 1993-95).

Ha $n \geq 3$, akkor az $x^n + y^n = z^n$ egyenletnek nincs pozitív egészekből álló megoldása.

6.8. Lemma.

Ha m és n előáll két négyzetszám összegeként, akkor mn is előáll.

Bizonyítás.

$$mn = \left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2$$ □

6.9. Lemma.

A $4k + 1$ alakú prímszámok előállnak két négyzetszám összegeként, a $4k + 3$ alakú prímek viszont nem.

6.10. Tétel (Fermat-féle két négyzetszám tétel).

Pontosan azok a számok állnak elő két négyzetszám összegeként, amelyek prímfelbontásában a $4k + 3$ alakú prímek páros kitevővel szerepelnek.

Példa.

$$153 = 3^2 \cdot 17 = 3^2 \cdot \left(4^2 + 1^2\right) = (3 \cdot 4)^2 + (3 \cdot 1)^2 = 12^2 + 3^2$$

$$2173 = 41 \cdot 53 = \left(4^2 + 5^2\right) \cdot \left(2^2 + 7^2\right) = 27^2 + 38^2$$

$$13949 = 13 \cdot 29 \cdot 37 = \left(2^2 + 3^2\right) \cdot \left(2^2 + 5^2\right) \cdot \left(1^2 + 6^2\right) = \left(11^2 + 16^2\right) \cdot \left(1^2 + 6^2\right)$$

$$= 85^2 + 82^2$$

6.11. Tétel (Lagrange-féle négy négyzetszám tétel).

Minden természetes szám előáll négy négyzetszám összegeként.

6.12. Megjegyzés.

Lagrange tétele éles abban az értelemben, hogy három négyzetszám összegeként nem lehet minden természetes számot előállítani (keressünk ellenpéldát!).

A természetes számok hatványösszegekként való előállításaival kapcsolatos problémákat összefoglaló néven Waring-problémakörnek szokás nevezni. Edward Waring XVIII. századi angol matematikus Meditationes Algebraicae című művében azt állította (bizonyítás nélkül), hogy minden szám előállítható kilenc köbszám összegeként, illetve tizenkilenc negyedik hatvány összegeként. Ezek az állítások helyesnek bizonyultak, de csak a huszadik században találtak rájuk bizonyítást.

6.12. Megjegyzés (folyt.).

Általában $g(k)$ jelöli azt a legkisebb számot, amelyre igaz az, hogy minden természetes szám előállítható $g(k)$ darab k-adik hatvány összegeként.

Az előzőek alapján tehát $g(2) = 4, g(3) \leq 9, g(4) \leq 19$, és példák mutatják, hogy 8 köb, illetve 18 negyedik hatvány nem mindig elég, tehát $g(3) = 9$ és $g(4) = 19$.

A $g(k)$ számok meghatározása igen nehéz probléma, még az sem világos, hogy egyáltalán léteznek[§] minden k-ra, bár ezt már Waring is sejtette. Hilbert igazolta Waring sejtését, és van egy feltételezett képlet is a $g(k)$ számokra:

$$g(k) = 2^k + \left[\frac{3^k}{2^k}\right] - 2.$$

Bizonyított tény, hogy ez a képlet legfeljebb véges sok k-ra nem helyes, és általánosan elfogadott az a sejtés, hogy valójában minden k-ra érvényes.

→ Fazekas Róbert: A Waring-sejtés bizonyítása (szakdolg., SZTE, 2015).

[§]Mit jelentene az, hogy $g(k)$ nem létezik?

Tartalom

6.13. Tétel.

Végtelen sok prímszám van.

Bizonyítás.

Tfh. $p_1, \ldots, p_n$ az összes prím, és legyen $N = p_1 \cdot \ldots \cdot p_n + 1$. Mivel $N > 1$, van prímosztója. Node N nem osztható a $p_1, \ldots, p_n$ számok egyikével sem! $\lightning$ □

6.14. Tétel.

Végtelen sok $4k - 1$ alakú prímszám van.

Bizonyítás.

Tfh. $p_1, \ldots, p_n$ az összes $4k - 1$ alakú prím, és legyen $N = 4 \cdot p_1 \cdot \ldots \cdot p_n - 1$. Mivel $N > 1$, van prímosztója. Node N nem osztható a $p_1, \ldots, p_n$ számok egyikével sem, tehát minden prímosztója $4k + 1$ alakú. Eszerint N előáll $4k + 1$ alakú számok szorzataként, és így maga is $4k + 1$ alakú. $\lightning$ □

6.15. Tétel.

Végtelen sok $4k + 1$ alakú prímszám van.

6.16. Tétel (Dirichlet, 1837).

Ha egy nemkonstans számtani sorozat kezdőtagja és differenciája egymáshoz relatív prím, akkor a számtani sorozatban végtelen sok prímszám található.

6.17. Tétel (Csebisev, 1850).

Bármely szám és a kétszerese között van prímszám. Pontosabban:
minden n természetes számhoz létezik olyan p prímszám, amelyre $n < p \leq 2n$.

$\rightarrow$ Szabó Lilla: A prímszámtétel bizonyításának története (szakdolg., SZTE, 2014).

6.18. Tétel.

A szomszédos prímek között tetszőlegesen nagy hézagok találhatók.
(*Azaz minden $N \in \mathbb{N}$ esetén lehet találni N egymást követő összetett számot.*)

Bizonyítás.

Ha $n \geq 2$, akkor az $n! + 2,\ n! + 3, \ldots, n! + n$ számok mind összetettek (miért?).
Ez $n - 1$ egymást követő összetett szám. □

6.19. Definíció.

Ikerprímnek nevezünk két prímszámot, ha különbségük 2.

6.20. Megjegyzés.

Azt sejtik, hogy végtelen sok ikerprím van. Yitang Zhang 2013 áprilisában bebizonyította, hogy létezik olyan K korlát, amelyre végtelen sok olyan prímpár létezik, ahol a két tag különbsége legfeljebb K ($K = 70\,000\,000$ értékre, de ezt azóta levitték 246-ra).

6.21. Lemma.

A $\sum_{n=1}^{\infty} \frac{1}{n}$ harmonikus sor divergens, míg a $\sum_{n=1}^{\infty} \frac{1}{n^2}$ sor konvergens.

6.22. Tétel.

A prímszámok reciprokaiból alkotott sor divergens, azaz

$$\sum_{p} \frac{1}{p} = \infty.$$

6.23. Megjegyzés.

Ez a tétel durván fogalmazva azt állítja, hogy „sok" prímszám van (négyzetszámból viszont a 6.21. Lemma szerint „kevés" van).
Ismert tény, hogy „kevés" páratlan tökéletes szám, illetve „kevés" ikerprím van (ebből persze még nem derül ki, hogy végtelen sok van-e belőlük).

6.24. Megjegyzés.

A harmonikus sor lassan divergál, a prímszámok reciprokaiból alkotott sor még lassabban. Például $\sum_{p<10^{18}} \frac{1}{p} < 4$ (ez kb. a sor első huszonnégybilliárd tagja).

6.25. Tétel.

Az n-edik prímszám nem nagyobb, mint $2^{2^{n-1}}$.

Bizonyítás.

Legyen $p_1, p_2, \ldots$ a prímek sorozata (növekvő sorrendben). Euklidész gondolatmenete szerint az $N = p_1 \cdot \ldots \cdot p_n + 1$ számnak van olyan p prímosztója, amelyre $p \notin \{p_1, \ldots, p_n\}$. Ekkor tehát $p_{n+1} \leq p \leq p_1 \cdot \ldots \cdot p_n + 1$, azaz

$$p_{n+1} \leq p_1 \cdot \ldots \cdot p_n + 1. \tag{EU}$$

Ezt az egyenlőtlenséget használva teljes indukcióval bizonyítjuk, hogy $p_n \leq 2^{2^{n-1}}$.

Kezdőlépés: $n = 1$ esetén $p_1 = 2 \leq 2^{2^{1-1}} = 2^{2^0} = 2^1$ ✓.

Indukciós lépés: Tegyük fel, hogy

$$p_1 \leq 2^{2^{1-1}},\ p_2 \leq 2^{2^{2-1}}, \ldots, p_n \leq 2^{2^{n-1}}. \tag{IH}$$

Becsüljük p_{n+1}-et az (EU) és (IH) egyenlőtlenségek segítségével:

$$\begin{aligned} p_{n+1} \leq p_1 \cdot \ldots \cdot p_n + 1 &\leq 2^{2^{1-1}} \cdot 2^{2^{2-1}} \cdot \ldots \cdot 2^{2^{n-1}} + 1 \\ &= 2^{1+2+\cdots+2^{n-1}} + 1 \\ &= 2^{2^n-1} + 1 \qquad < 2^{2^n-1} + 2^{2^n-1} = 2^{2^n} \end{aligned}$$

□

6.26. Definíció.

A prímszámok eloszlásának pontosabb vizsgálatánál hasznos a $\pi(x)$ függvény, az úgynevezett **prímszámláló függvény**, amely megadja az x pozitív valós számnál nem nagyobb prímek számát:

$$\pi(x) = \sum_{p \leq x} 1.$$

6.27. Tétel (prímszámtétel, Hadamard és de la Vallée-Poussin, 1896).

A $\pi(x)$ prímszámláló függvény aszimptotikusan ekvivalens az $\frac{x}{\log x}$ függvénnyel, azaz

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

$\rightarrow$ Szabó Lilla: A prímszámtétel bizonyításának története (szakdolg., SZTE, 2014).

6.28. Következmény.

Az n-edik prímszám aszimptotikusan $n \log n$, azaz $\lim_{n \to \infty} \frac{p_n}{n \log n} = 1$.

Tartalom

Algebrai és transzcendens számok

6.29. Definíció.

Az α komplex számot **algebrai számnak** nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak. A nem algebrai számokat **transzcendens számoknak** nevezzük.

6.30. Definíció.

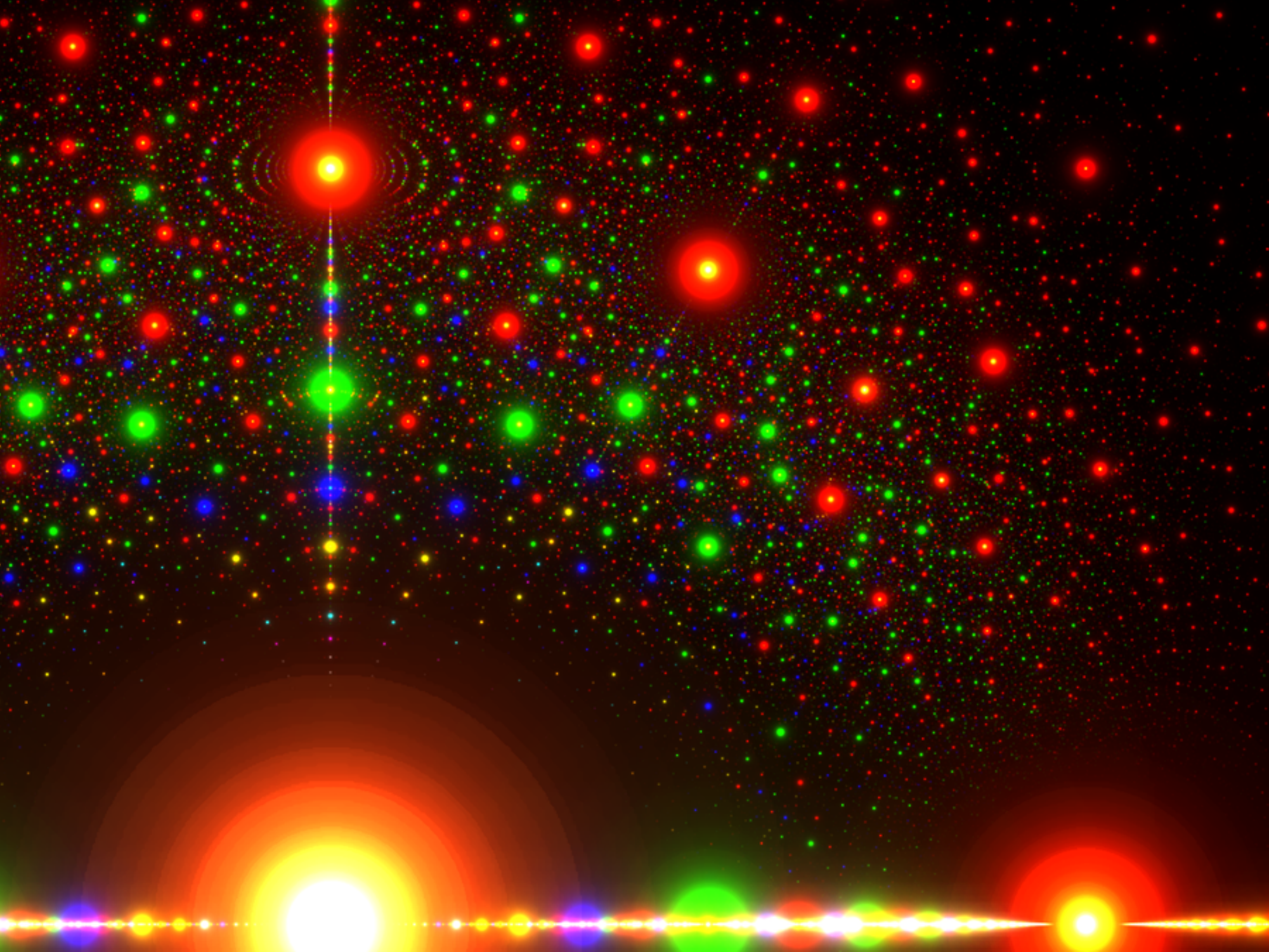
Ha $f \in \mathbb{Q}[x]$ minimális fokszámú mindazon nemzéró racionális együtthatós főpolinomok között, melyeknek α gyöke, akkor f-et az α algebrai szám **minimálpolinomjának** nevezzük.

6.31. Tétel.

Algebrai szám minimálpolinomja mindig egyértelműen meghatározott, és irreducibilis a racionális számtest felett. Továbbá, ha $f \in \mathbb{Q}[x]$ olyan irreducibilis főpolinom melynek az α algebrai szám gyöke, akkor f megegyezik α minimálpolinomjával.

6.32. Tétel.

Létezik transzcendens szám.



Algebrai és transzcendens számok

Példa.

- $\sqrt{2}$ algebrai szám, minimálpolinomja: $x^2 - 2$ (miért irreducibilis?).
- $\sqrt[n]{2}$ algebrai szám, minimálpolinomja: $x^n - 2$ (miért irreducibilis?).
- i algebrai szám, minimálpolinomja: $x^2 + 1$ (miért irreducibilis?).
- π és e transzcendens számok.
- A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- Gelfond–Schneider-tétel: Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám.

  Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $i^i = e^{-\pi/2}$ transzcendens számok.

Diofantoszi approximáció

6.33. Megjegyzés.

A 6.32. Tétel (egyik) bizonyítása azon múlik, hogy algebrai számokat nem lehet nagyon jól közelíteni racionális számokkal (lásd a 6.38. Tételt). Ez a *diofantoszi approximáció* témaköre: adott α valós számhoz szeretnénk olyan $\frac{p}{q}$ közelítő törtet találni ($p, q \in \mathbb{Z}, q > 0, p \perp q$), amelyre $\left|\alpha - \frac{p}{q}\right|$ kicsi, és q nem túl nagy.

6.34. Tétel (Dirichlet approximációs tétele).

Minden α valós szám és minden N természetes szám esetén van α-nak olyan $\frac{p}{q}$ közelítése, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq} \quad \text{és} \quad q \leq N.$$

6.35. Következmény.

Ha $\alpha \notin \mathbb{Q}$, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

6.36. Állítás.

Ha $\alpha \in \mathbb{Q}$, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Diofantoszi approximáció

6.37. Tétel (Hurwitz tétele).

Ha α irracionális szám, akkor végtelen sok olyan $\frac{p}{q}$ közelítése van, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Ha $\alpha = \frac{1+\sqrt{5}}{2}$, akkor az állítás nem javítható: nem írhatunk a nevezőbe semmilyen $\sqrt{5}$-nél nagyobb számot.

6.38. Tétel (Liouville, Thue, Siegel, Roth).

Ha α irracionális algebrai szám és $\varepsilon > 0$, akkor csak véges sok olyan $\frac{p}{q}$ közelítése van, amelyre

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}.$$

Algebrai számok és gyökmennyiségek

6.39. Tétel.

Az algebrai számok résztestet alkotnak a komplex számok testében.

6.40. Tétel.

Ha α algebrai szám és $n \geq 2$, akkor $\sqrt[n]{\alpha}$ is algebrai szám (a gyöknek mind az n értékére).

6.41. Definíció.

Az α komplex számot **gyökmennyiségnek** nevezzük, ha megkapható racionális számokból kiindulva a négy alapművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával.

6.42. Következmény.

A gyökmennyiségek algebrai számok.

Példa.

Ez a szám algebrai:

$$\frac{\sqrt[3]{3-\sqrt{\sqrt[4]{2}+\sqrt[5]{\frac{3}{17}}}}+\sqrt[17]{323-\sqrt{2014}}}{\sqrt{2}+\sqrt[3]{3}+\sqrt[5]{5}}$$

Algebrai számok és gyökmennyiségek

6.43. Tétel.

Van olyan algebrai szám, ami nem gyökmennyiség.

A fenti ártatlannak látszó tételből következik, hogy nem minden egyenlet oldható meg gyökjelek segítségével. Az ötödfokú egyenletnek már nincs általános megoldóképlete, sőt, például az $x^5 - 4x + 2 = 0$ egyenletnek még „ad hoc" megoldóképlete sincs, mert gyökei nem gyökmennyiségek.

6.44. Tétel.

Az algebrai számok teste algebrailag zárt, azaz ha $\alpha \in \mathbb{C}$ gyöke a legalább elsőfokú $f = a_n x^n + \cdots + a_1 x + a_0$ polinomnak, ahol $a_0, \ldots, a_n$ algebrai számok, akkor α maga is algebrai szám.