Algebra és számelmélet 3 előadás
Nevezetes számelméleti problémák

Waldhauser Tamás
2014 őszi félév

Tartalom

Tartalom

Pitagoraszi számhármasok

1. Definíció.

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

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).

3. Lemma.

Primitív pitagoraszi számhármasban a tagok páronként is relatív prímek. Fordítva, ha egy pitagoraszi számhármasban valamelyik két tag relatív prím, akkor a számhármas primitív.

Házi feladat.

A bizonyítás befejezése.

4. Lemma.

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

Pitagoraszi számhármasok

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.*

6. Tétel.

Az $x^4 + y^4 = z^2$ *egyenletnek nincs pozitív egészekből álló megoldása.*

7. Következmény.

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

8. Tétel (nagy Fermat-tétel).

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

Két négyzetszám összege

9. Lemma.

Ha a és b előáll két négyzetszám összegeként, akkor ab is előáll.

10. Lemma.

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

11. 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.

Állítsuk elő két négyzetszám összegeként: 153, 12^2+3^2 1170, 33^2+9^2 390.nem lehet

Házi feladat.

Állítsuk elő két négyzetszám összegeként: 377, 610, 2014.

Waring-problémakör

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

Minden természetes szám előáll négy négyzetszám összegeként.

13. 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.

13. 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.

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

Tartalom

Végtelen sok prím

14. Tétel.

Végtelen sok prímszám van.

15. Tétel.

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

16. Tétel.

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

17. Tétel (Dirichlet tétele).

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

Hézagok a prímek között

18. Tétel (Csebisev tétele).

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

19. Tétel.

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

20. Definíció.

Ikerprímnek nevezünk két prímszámot, ha különbségük 2.

Ikerprímsejtés.

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 jóval lejjebb vitték).

A prímharmonikus sor

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.

22. Tétel.

A prímszámok reciprokaiból alkotott sor divergens, azaz

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

23. Megjegyzés.

Ez a tétel durván fogalmazva azt állítja, hogy „sok" prímszám van (négyzetszámból viszont a 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).

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).

A prímszámtétel

25. Tétel.

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

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:

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

27. Tétel (prímszámtétel).

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

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

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

29. Definíció.

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

30. Definíció.

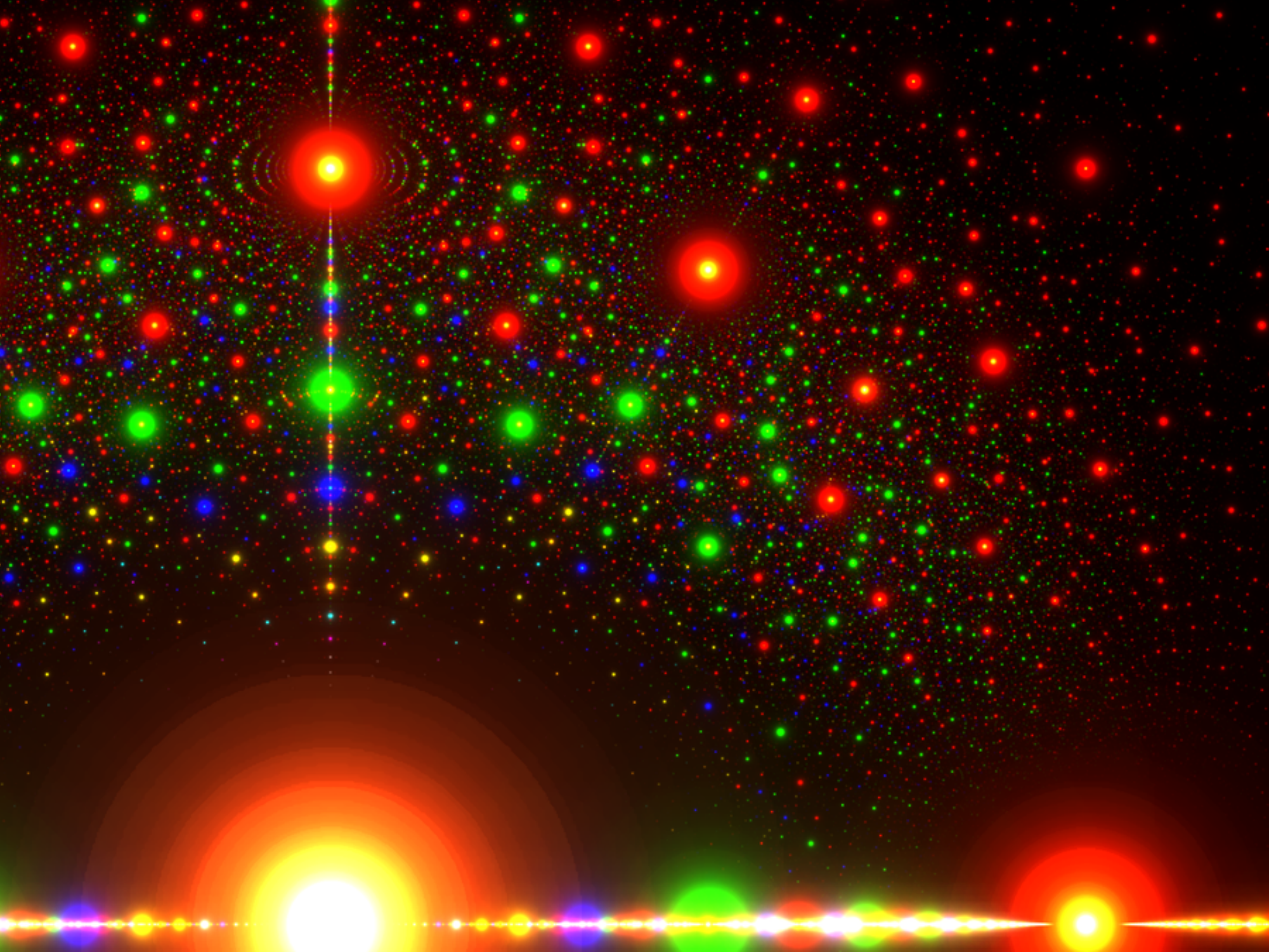
Ha $f \in \mathbb{Q}[x]$ minimális fokszámú mindazon nemzéró racionális együtthatós főpolinomok között, melyeknek α gyöke, akkor f-et az α algebrai szám **minimálpolinom**jának nevezzük.

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.

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

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.

33. Tétel (Dirichlet approximációs tétele).

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

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

34. Következmény.

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

35. Állítás.

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

Diofantoszi approximáció

36. 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.

37. 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

38. Tétel.

Az algebrai számok résztestet alkotnak a komplex számok testében.

39. Tétel.

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

40. Definíció.

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

41. 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

42. 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.

43. 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.