

# Nevezetes számelméleti problémák

---

Waldhauser Tamás  
SZTE Bolyai Intézet

Prímszámok

Számok felbontása hatványok összegére

## Tétel.

Végtelen sok prímszám van.

## Bizonyítás.

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

## Tétel.

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

## Bizonyítás.

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

## Tétel.

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

### Tétel (Dirichlet, 1837).

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

### Tétel (Csebisev, 1850).

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

### Tétel.

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

### Bizonyítás.

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

## Definíció.

**Ikerprímnek** nevezünk két prímszámot, ha különbségük 2.

## 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).

## Állítás.

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

## Tétel.

A prímszámok reciprokaiból alkotott sor divergens, azaz

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

## Megjegyzés.

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

## 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).

## Tétel.

Legyen  $p_1, p_2, \dots$  a prímszámok sorozata. Ekkor  $p_n \leq 2^{2^{n-1}}$ .

## Bizonyítás.

Euklidész gondolatmenete szerint az  $N = p_1 \cdot \dots \cdot p_n + 1$  számnak van olyan  $p$  prímosztója, amelyre  $p \notin \{p_1, \dots, p_n\}$ . Ekkor tehát  $p_{n+1} \leq p \leq p_1 \cdot \dots \cdot p_n + 1$ , azaz

$$p_{n+1} \leq p_1 \cdot \dots \cdot p_n + 1. \quad (\text{EU})$$

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

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

Indukciós lépés: Tegyük fel, hogy

$$p_1 \leq 2^{2^{1-1}}, p_2 \leq 2^{2^{2-1}}, \dots, p_n \leq 2^{2^{n-1}}. \quad (\text{IH})$$

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

$$\begin{aligned} p_{n+1} \leq p_1 \cdot \dots \cdot p_n + 1 &\leq 2^{2^{1-1}} \cdot 2^{2^{2-1}} \cdot \dots \cdot 2^{2^{n-1}} + 1 \\ &= 2^{1+2+\dots+2^{n-1}} + 1 \\ &= 2^{2^n - 1} + 1 < 2^{2^n - 1} + 2^{2^n - 1} = 2^{2^n}. \quad \square \end{aligned}$$

## 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:

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

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

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

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

## Következmény.

Az  $n$ -edik prímszám aszimptotikusan  $n \log n$ , azaz

$$\lim_{n \rightarrow \infty} \frac{p_n}{n \log n} = 1.$$

→ Szabó Lilla: A prímszámtétel bizonyításának története (szakdolgozat, SZTE, 2014).



Prímszámok

Számok felbontása hatványok összegére

## Definíció.

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

## Megjegyzés.

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

## Példa.

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

## Lemma.

Primitív pitagoraszi számhármásban a tagok páronként is relatív prímek.

## Bizonyítás.

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

$$\begin{aligned}d \mid x, y &\implies d^2 \mid x^2, y^2 \\ &\implies d^2 \mid x^2 + y^2 = z^2 \\ &\implies d \mid z \\ &\implies d \mid \text{Inko}(x, y, z) \\ &\implies d \sim 1 \\ &\implies x \perp y\end{aligned}$$

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



## Lemma.

Ha  $(x, y, z)$  primitív pitagoraszi számhármás, 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	⚡



## Lemma.

Ha  $UV$  négyzetszám és  $U \perp V$ , akkor  $U$  és  $V$  is négyzetszám.

## Bizonyítás.

Egy természetes szám akkor és csak akkor négyzetszám, ha prímszámhatványtényező felbontásában minden prímszám páros kitevővel szerepel.

Tegyük fel, hogy  $UV$  négyzetszám és  $U \perp V$ . Legyen  $p$  egy tetszőleges prímszám. Mivel  $UV$  négyzetszám,  $p$  kitevője  $UV$  prímszámhatványtényező felbontásában páros, mondjuk  $2k$ .

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

Ezzel beláttuk, hogy  $U$ -ban is és  $V$ -ben is minden prímszám páros kitevővel szerepel, így tehát  $U$  és  $V$  is négyzetszám. □

## Tétel.

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

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

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

## Példa.

Néhány kis  $u, v$  értékkel adódó primitív pitagoraszi számhármass:

$u$	$v$	$x$	$y$	$z$
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

## Tétel (Fermat, 1640).

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

## 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.

### Lemma.

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

### Bizonyítás.

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \quad \square$$

### Lemma.

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

### Tétel (Fermat, 1640; Girard, 1625).

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

### Példa.

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

$$2173 = 41 \cdot 53 = (4^2 + 5^2) \cdot (2^2 + 7^2) = 27^2 + 38^2 = 18^2 + 43^2$$



## Tétel (Lagrange, 1770).

Minden természetes szám előáll négy négyzetszám összegeként.

## Megjegyzés.

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

A természetes számok hatványösszegekként való előállításával 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.

## 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:

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

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).