

Hatványösszegekre bontás.

Pithagoraszai számhármások, a Fermat problémakör.

Klukovits Lajos

TTIK Bolyai Intézet

2016. április 7.

Definíciók.

$(a, b, c) \in \mathbb{N}^3$ **Pithagoraszai számhármás**, ha

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

Az

$$x^2 + y^2 = z^2$$

egyenletet szokás **Pithagoraszai egyenletnek** nevezni.

A folyamamenti kultúrák.

- Mindegyikben ismerték a (3, 4, 5) hármast
- Az Óbabiloni Birodalom korából származó Plimpton 622-es agyagtáblán 15 olyan (racionális számokból álló) hármast van, amelyek megoldásai a Pithagoraszai egyenletnek.
- Indiában számos ilyen hármast szerepel az a. i. e. I. évezredben keletkezett írásokban, ún. szútrákban — ezek zömmel tanító írások —, többnyire oltár-konstrukciós problémák kapcsán.
- Például (5, 12, 13), (12, 35, 37), (15, 36, 39), összesen 6 hármast ismertek.
- Ugyancsak a. i. e. I. évezredben Kínában is ismertek több Pithagoraszai számhármast.

Görögök.

- Ha m páratlan szám, akkor

•

$$\left(m, \frac{m^2 - 1}{2}, \frac{m^2 + 1}{2}\right)$$

ún. Pithagoraszai számhármast, azaz az ilyen oldalhosszúságú háromszögek derékszögűek.

- Ez vélhetően a tarrentumi Archytasz eredménye.

A pisai Leonardo: Liber quadratorum.

Az 1. könyv bevezető állítása.

Az első n páralan szám összege n^2 .

A könyv fő problémája.

- Keressünk olyan négyzetszámokat, amelyek előállnak két négyzetszám összegeként.
- Másképpen fogalmazva: Keressük a Pithagoraszai egyenlet megoldásait.

Megjegyzés.

A kor szokásainak megfelelően Leonardo speciális eseteket vizsgált, mindig konkrét számokkal dolgozott. Módszere azonban tartalmazta az általánosítás csíráját.

A pisai Leonardo: Liber quadratorum.

Az első eset: páratlan négyzetszám.

- Legyen a páratlan négyzetszám a 9.
- $1 + 3 + 5 + 7 = 16 = 4^2$,
- $1 + 3 + 5 + 7 + 9 = 25 = 5^2$,
- kaptuk, hogy $5^2 = 3^2 + 4^2$.

Általános.

Legyen $y^2 = d$ páratlan. Ekkor

$$x^2 = 1 + 3 + \dots + (d-2) = \left(\frac{d-1}{2}\right)^2$$

$$z^2 = x^2 + y^2 = 1 + 3 + \dots + (d-2) + d = \left(\frac{d+1}{2}\right)^2.$$

A pisai Leonardo: Liber quadratorum.

Egy további eset: páros négyzetszám.

- Megjegyzi, hogy a páros négyzetszámok oszthatók 4-gyel, továbbá
- két egymást követő páratlan szám összegére bomlanak.
- Legyen a páros négyzetszám a 36, $36 = 17 + 19$.
- $1 + 3 + \dots + 15 = 8^2$,
- azaz összegezte a 17-nél kisebb páratlan számokat.
- $(1 + 3 + \dots + 15) + (17 + 19) = 10^2$,
- amiből a $10^2 = 8^2 + 6^2$ fölbontás adódik.

Megjegyzés.

E hármast megkapható az előbbi (3, 4, 5) hármastól, de Leonardo igyekezett minden egyes általa vizsgált hármast minél többféleképp előállítani.

A pisai Leonardo: Liber quadratorum.

A páros négyzetszám esete általános.

- Legyen a páros négyzetszám $4k = (2k-1) + (2k+1)$, majd Leonardo eljárását követve
- $= 1 + 3 + \dots + (2k-3) = \left(\frac{2k-3+1}{2}\right)^2 = (k-1)^2$
- $(1 + 3 + \dots + (2k-3)) + ((2k-1) + (2k+1)) = \left(\frac{2k+1+1}{2}\right)^2$,
- $= (k+1)^2$,
- amelyekből $(k-1)^2 + 4k = (k+1)^2$.

Megjegyzés.

Az eljárással

$$(a^2 - 1, 2a, a^2 + 1), \quad a > 1$$

alakú hármásokat kap.

Leonardo: Liber quadratorum.

3. eset: a 3-mal osztható páratlan négyzetszámok.

- Csak számokkal adjuk meg.
- Az alap: $y^2 = 9k = 3(3k) = (3k - 2) + 3k + (3k + 2)$.
- Leonardo példája:

$$y^2 = 81 = 3 \cdot 27 = 25 + 27 + 29 = 9^2,$$

$$x^2 = 1 + \dots + 23 = 144 = 12^2,$$

$$z^2 = 1 + \dots + 23 + (25 + 27 + 29) = 144 + 81 = 225 = 15^2.$$

Leonardo: Liber quadratorum.

4. eset: a 6-tal osztható négyzetszámok.

- A legkisebb ilyen a 36, de a 144-et választja.
- A számpélda

$$y^2 = 144 = 6 \cdot 24 = (19 + 21) + (23 + 25) + (27 + 29)$$

$$x^2 = 1 + 3 + \dots + 17 = 81 = 9^2$$

$$z^2 = (1 + 3 + \dots + 17) + (19 + 21 + \dots + 29) \\ = 81 + 144 = 225 = 15^2.$$

Leonardo: Liber quadratorum.

4. eset: a 6-tal osztható négyzetszámok.

- Általánosan a probléma:
-

$$y^2 = 36k = (6k - 5) + \dots + (6k + 5)$$

$$x^2 = 1 + \dots + (6k - 7) = (3k - 3)^2$$

$$x^2 + y^2 = 1 + \dots + (6k - 7) + (6k - 5) + \dots + (6k + 5) \\ = 36k + (3k - 3)^2 = (3k + 3)^2$$

Mit mondhatunk ma.

Definíció.

Az olyan (a, b, c) Pithagoraszai számhármast, amelyre $\text{In. k. o.}(a, b, c) = 1$, **primitív Pithagoraszai számhármast** nevezzük.

Egy tétel.

Legyenek $m > n > 0$ egészek, különböző paritásúak és $\text{In. k. o.}(m, n) = 1$. Az

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

hármast primitív Pithagoraszai számhármast, és az összes primitív Pithagoraszai számhármast előáll ilyen alakban.

Következmény.

Végtelen sok primitív Pithagoraszai számhármast létezik.

Fermat problémakör

A kiindulópont.

- 1637-ben **Pierre Fermat** Diophantosz Aritmetikájában az ún. Pithagorasz számhármakokról olvasott.
- Fölismerete, hogy bizonyos négyzetszámok két négyzetszám összegére bonthatók, pl. $25 = 9 + 16$, azaz $5^2 = 3^2 + 4^2$.

A legendás lapszéli mondat.

„...csodálatos bizonyítást találtam arra, hogy sem egyetlen köbszám, negyedik és magasabb hatvány nem bontható két köbszám, két negyedik hatvány, és így tovább, összegére, azaz az

$$x^n + y^n = z^n \quad n \geq 3$$

egyenletnek nincs megoldása a pozitív egészekben, de túl kicsi e margó arra, hogy ezt ide leírjam...”

Fermat problémakör

- E rövid bejegyzés — amelyet kezdetben úgy emlegettek, mint „A Nagy Fermat Tétel”, vagy „Fermat utolsó tétele” —, egy kiterjedt kutatást indított el.
- A kezdeti általános vélekedés szerint a bizonyítás létezett, csak „újra meg kell találni”.
- A XIX. század közepétől — az általános sikertelenség miatt — kezdék az állítást „Fermat-sejtésként” említeni.
- A sejtést a XX. század utolsó évtizedében sikerült igazolni.

Az $n = 2$ eset.

- Legyen (a, b, c) primitív Pithagorasz számhármak.
- Világos, hogy $\ln. k. o. (a, b) = \ln. k. o. (a, c) = \ln. k. o. (b, c) = 1$.
- Nyilvánvaló, hogy a, b, c nem lehet mind páratlan, ezért közülük kettő páratlan, egy páros. c nem lehet páros.

Az $n = 2$ eset.

- Ha az a páros, akkor $a^2 = c^2 - b^2 = (c + b)(c - b)$, amiből

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

- A jobb oldali két tényező is relatív prím, így a számelmélet alaptételéből adódóan

$$\frac{c+b}{2} = m^2, \quad \frac{c-b}{2} = n^2,$$

azaz mindkettő négyzetszám.

- $m > n$, $\ln. k. o. (m, n) = 1$, és m, n ellenkező paritású.
- Kaptuk: $a = 2mn$, $b = m^2 - n^2$, $c = m^2 + n^2$.
- Világos, hogy minden primitív hármak ilyen alakú, és az összes ilyen hármak Pithagorasz.

Az $n = 4$ eset.

- Ezzel az esettel részletesen foglalkozott Fermat.
- Megmutatta, hogy ha (a, b, c) megoldása az $x^4 + y^4 = z^2$ egyenletnek, akkor van olyan (a', b', c') megoldása is, hogy $c' < c$.
- Az alkalmazott módszer az ún. **végtelen leszállás**.
- Ebből már következik, hogy az $x^4 + y^4 = z^4$ egyenletnek nincs nemtriviális egész megoldása.
- Vélhető, hogy — hasonló módszerrel — az $n = 3$ esettel is boldogult.
- **Bizonyításaiban alapvető volt, hogy alkalmazhatta a számelmélet alaptételét.** (Azaz, hogy létezik egyértelmű prímfaktorizáció.)

Euler megoldása az $n = 3$ esetre.

Az ún. Euler egészek gyűjűje.

- Euler az $x^3 + y^3 + z^3 = 0$ egyenletet vizsgálta.
- Igazolta, hogy nincs nemtriviális megoldása az

$$\{a + b\alpha : a, b \in \mathbb{Z}, \alpha \neq 1, \alpha^3 = 1\} \subset \mathbb{C}$$

alakú komplex számok (az ún. Euler egészek) gyűjűjében.

- Mivel e gyűrű tartalmazza az egészeket, eredményéből következik, hogy az $x^3 + y^3 = z^3$ egyenletnek nincs nemtriviális (racionális) egész megoldása.
- Euler bizonyításában is alapvető volt, hogy az Euler egészek körében **érvényes a számelmélet alaptételének egy általánosítása.**

Fermat problémakör: a továbblépés egy lehetősége.

Egy egyszerű észrevétel.

- Nyilvánvaló, hogy az $x^n + y^n = z^n$ $n > 2$ egyenlet megoldhatatlanságát elegendő az $n = 4$ esetre igazolni, valamint arra, ha n páratlan prím.
- Ugyanis, ha $n \geq 5$, akkor $4 \mid n$, vagy n -nek van páratlan prímosztója, és
- ha megoldható $\mathbb{Z}$ fölött az $x^n + y^n = z^n$ $n > 2$ egyenlet, és $k \mid n$ akkor megoldható az $x^k + y^k = z^k$ egyenlet is.
- Kínálkozik, hogy Euler gondolatmenetét általánosítsuk $p > 3$ prímekre.

Fermat problémakör: a továbblépés egy lehetősége.

Euler eljárásának általánosítása.

- Legyen $p \geq 3$ prím, és $\alpha \in \mathbb{C}$ egy p -edik primitív egységgyök ($\alpha^p = 1$ de α egyetlen p -nél kisebb pozitív kitevős hatványa sem 1).
- Megvizsgáljuk az $x^p + y^p = z^p$ egyenletet.
- 1847-ben Lamé úgy találta, hogy tetszőleges $a, b \in \mathbb{Z}$ egészekre

$$a^p + b^p = (a + b)(a + \alpha b)(a + \alpha^2 b) \dots (a + \alpha^{p-1} b) \quad (1)$$

ahol α p -edik primitív egységgyök.

- Ez egy

$$\mathbb{Z}[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{p-2}\alpha^{p-2} : a_i \in \mathbb{Z}\} \quad (2)$$

gyűrű fölötti fölbontás.

- E gyűrűk integritástartományok.

Fermat problémakör: a továbblépés egy lehetősége.

Euler eljárásának általánosítása: Lamé eljárása

- Ha valamely $a, b \in \mathbb{Z}$ -re $a^p + b^p = c^p$ alkalmas c egészre, akkor
- az (1) egyenlőség jobb oldalán valamennyi tényező teljes p -edik hatvány, és alkalmazhatjuk Euler módszert.
- Ehhez az kell, hogy a (2)-ben definiált integritástartományban érvényes legyen a számelmélet alaptétele.
- Kezdetben Lamé úgy vélte ez igaz, de később rájött, hogy nem. Ugyanis
- ez minden $p \leq 19$ -re igaz, de már $p = 23$ -ra nem.
- Erre néhány év múlva ő maga is rájött.
- Kérdés: vannak-e olyan 23-nál nagyobb prímek, amelyekre van fölbontási tétel.**

Fermat problémakör: a továbblépés egy lehetősége.

Fermat megjegyzéséről.

- Vélhető, hogy Fermat képes volt Euler (későbbi) gondolatmenetének alkalmazására, azaz ezen az úton is elintézni az $n = 3$ esetet.
- Az is föltételezhető, hogy képes volt áttekinteni az $n = 5$, sőt talán még az $n = 7$ eseteket is, amelyek már igen nagymértékű számolást igényelnek.
- Mindezek alapján úgy vélhette, hogy ez az eljárás működik az összes páratlan prímre, azaz
- mindegyik $\mathbb{Z}[\alpha]$ gyűrűben érvényes a számelmélet alaptételének megfelelő általánosítása.
- Sajnos ez nem bizonyult igaznak. **a kívánt típusú fölbontások a $p < 23$ prímekekre biztosan léteznek, de nagyobbakra? $p = 23$ -ra nem..**
- A „nagy elme” is elbőbiskol olykor.

Fermat problémakör: a továbblépés egy lehetősége.

Euler eljárásának általánosítása, Kummer 1840-től.

Definíció. A p páratlan prím *reguláris*, ha nem osztója a $B_2, B_4, \dots, B_{p-3}$ ún. Bernoulli számok számlálóinak.

Definíció. A Bernoulli számok a $\frac{t}{e^t - 1}$ függvény hatványsorának együtthatóiban szerepelők:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n.$$

- Ezen B_n számok a „nem túl nagy” indexekre viszonylag könnyen kiszámolhatók.
- A $p < 100$ -ra csak a 37, 59, 67 nem reguláris pl.:

$$B_{32} = \frac{37 \cdot 683 \cdot 305065927}{510},$$

Fermat problémakör: a XIX. század fejleményei.

Kummer eredményei az 1840-es évekből.

Kummer tétele. *A Fermat sejtés igaz a reguláris prímekekre.*

- Kummer azt sejtette, hogy végtelen sok reguláris prím van, de
- ez a mai napig sem bizonyított.

Fermat problémakör: a XX. század.

- 1993. június 23-án Cambridge-ben Andrew Wiles bejelentette egy konferencián, hogy igazolta a sejtést.
- Miután leírta az igen hosszú bizonyítást rájött, hogy az nem teljes, egy jelentős „hézag” van benne.
- **1995-re Richard Taylорral közösen megadott egy korrekt bizonyítást, amely kb. 200 oldalas.**
- **Az alkalmazott módszer alapján világos, hogy korábban lehetetlen volt korrekt bizonyítást adni a sejtésre.**

Négyzetösszegekre bontás.

Indító kérdések.

- Pithagoraszai számhármások: bizonyos négyzetszámok fölbonthatók két négyzetszám összegére.
- Általában megmondható-e, hogy mely természetes számok bonthatók két négyzetszám összegére?
- Melyek azok, amelyek csak kettőnél több négyzetszám összegére bonthatók? (Ha vannak ilyenek.)
- Van-e olyan korlát, hogy legfőljebb annyi négyzetszám összegére már mindegyik természetes szám fölbontható.
- Mi a helyzet a magasabb hatványokkal?
- Tudjuk (Fermat sejtése, Wiles tétele), hogy $n > 2$ -re egyetlen n -edik hatvány sem bontható két n -edik hatvány összegére. De fölbontható-e kettőnél többre?

Négyzetösszegekre bontás.

Két négyzetszám összege.

- A pisai Leonardo eredménye: Ha $m, n \in \mathbb{N}$ két négyzetszám összegére bontható, akkor szorzatuk is.
- Pontosabban, ha $m = a^2 + b^2$, $n = c^2 + d^2$, akkor $mn = (ac - bd)^2 + (ad + bc)^2$.
- Következésképp elegendő a prímszámok fölbonthatóságával foglalkozni.
- Euler: Ha $p = 4k + 1$ prím, akkor előáll két négyzetszám összegeként.
- Egy $n > 1$ egész pontosan akkor áll elő két négyzetszám összegeként, ha prímtényezős fölbonthatásában a $4k + 3$ alakú prímek csak páros kitevővel fordulnak elő.
- **Megjegyzés.** Itt és a továbbiakban a fölbonthatóságban a 0 is szerepelhet.

Négyzetösszegekre bontás.

Három négyzetszám összege.

Gauss: Valamely $n > 1$ pontosan akkor **nem** áll elő 3 négyzetszám összegeként, ha

$$n = 4^m(8k + 7), \quad m, k \in \mathbb{N}_0.$$

Négy négyzetszám összege.

- Lagrange: Ha $m, n \in \mathbb{N}$ négy négyzetszám összegére bontható, akkor szorzatuk is.
- Így most is elég prímszámokkal foglalkozni.
- Lagrange: Minden prímszám előáll 4 négyzetszám összegeként.
- **Következmény.** (Lagrange) Minden természetes szám előáll négy négyzetszám összegeként.

Magasabb kitevős hatványok.

Waring 1770.

- Bizonyítás nélkül a következőket jelentette be:
- Minden (természetes) szám előáll 4 négyzetszám, 9 köbszám, 19 negyedik hatvány, stb. összegeként.
- **Megjegyzés.** A „stb” erős túlzás, mert implicite azt tartalmazza, hogy minden $k > 1$ egészhez van olyan $w(k) \in \mathbb{N}$, hogy minden természetes szám előáll $w(k)$ számú k -adik hatvány összegeként.

Hilbert 1909.

- A Waring bejelentés szerinti $w(k)$ szám minden $k > 1$ egészre létezik.
- DE Hilbert tételének a bizonyítása egy ún. **tiszta egzisztencia bizonyítás**, azaz semmit sem mond a $w(k)$ függvény értékeiről.
- Waring $w(4) = 19$ állítását csak 1986-ban igazolták.

Magasabb kitevős hatványok.

Becslések.

- Ha $g(k)$, $k > 1$ jelöli a $w(k)$ lehető legkisebb értékét, akkor

$$g(k) \geq 2^k \left[\left(\frac{3}{2} \right)^2 \right] - 2,$$

ahol $[.]$ az egészrész (pontosabban az ún. alsó-egészrész) függvényt jelöli.

- Ha $G(k)$ jelöli a $w(k)$ értékét „elég nagy” n -ekre, akkor

$$G(k) < 6k \log k.$$

Magasabb kitevős hatványok.

$g(k)$ és a $G(k)$ értékek

k	2	3	4	5	6	7	8
$g(k)$	4	9	19	37	73	143	279
$G(k)$	4	4 – 7	16	6 – 18	9 – 28	8 – 45	32 – 57

Megjegyzés.

Sajnos még kis k -ra is nagy a bizonytalanság a $G(k)$ értékekre. Pl. A $G(3)$ -nál a 4-7 jelölés azt mutatja, hogy csak az bizonyított (jelenleg), hogy

$$4 \leq G(k) \leq 7.$$