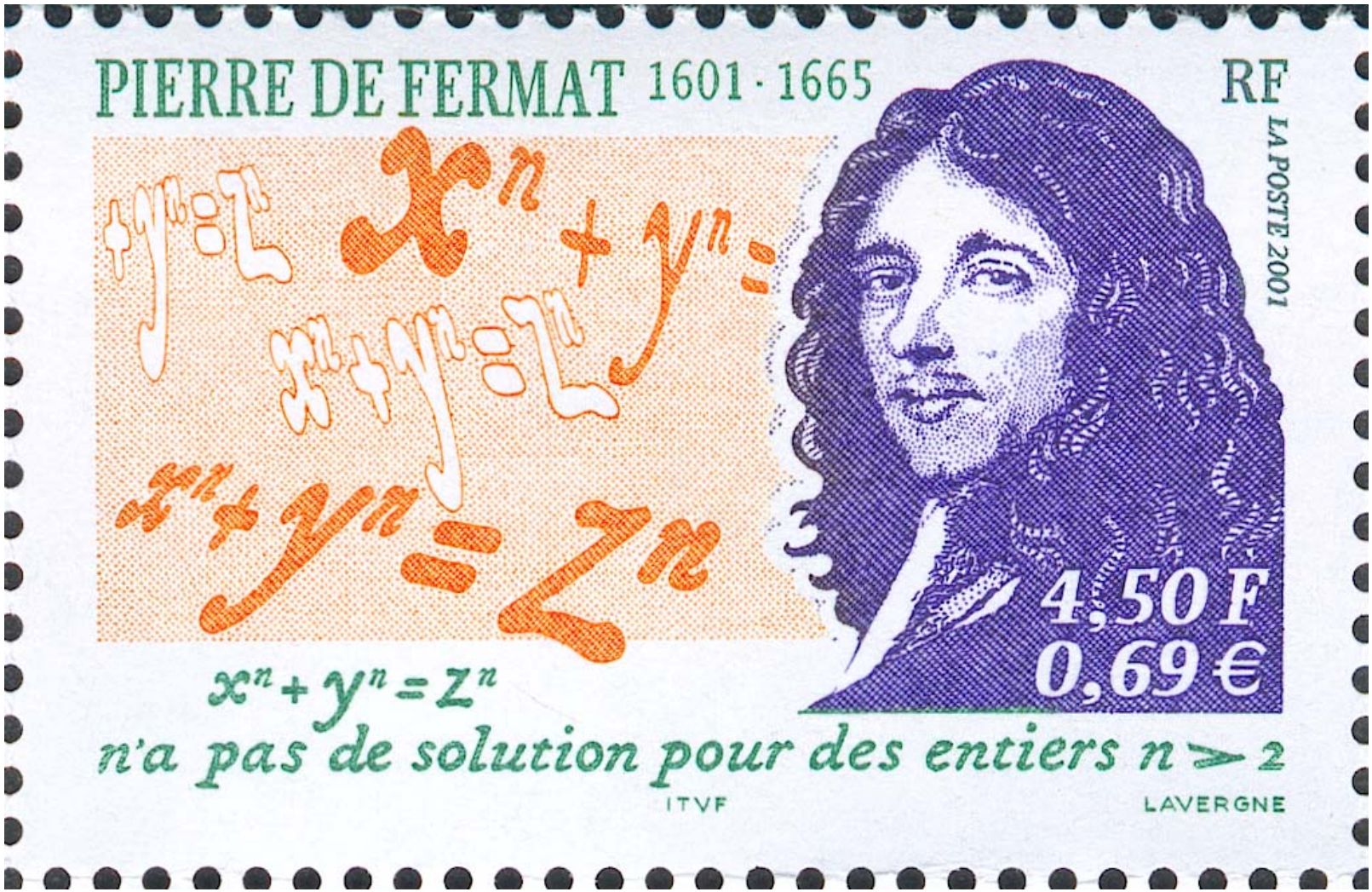
Fermat karácsonyi tétele

Rónyai Lajos, BME és MTA SZTAKI

Budapest, 2015. december 17.


PIERRE DE FERMAT 1601 · 1665
RF
LA POSTE 2001
4,50 F
0,69 €
$x^n + y^n = z^n$
n'a pas de solution pour des entiers $n > 2$
ITVF
LAVERGNE

A karácsonyi tétel

Tétel.

Minden $4k+1$ alakú p prímszámhoz léteznek a, b egészek, amelyekkel

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

Az állítás nem igaz egyetlen $4k+3$ alakú prímre sem.

Fermat 1640. december 25-én M. Mersenne-nek írt levelében állítja, hogy a tételt be tudja bizonyítani.

Az Aritmetikához fűzött margójegyzetei között is szerepel (Obs. VII.).

Nem maradt fenn bizonyítás Fermat-tól, de hihető, hogy volt neki (Hardy-Wright, Weil, Grosswald).

Képzelt karácsonyi kapcsolat

Már Diofantosznál...

Ismerte az

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2$$

azonosságot (*Aritmetika*, III. 19).

Mohamed Ben Alhocain (X. század) táblázatot közöl két négyzet összegeként megkapható számokról.

Albert Girard (1632) mondta ki először a tételt.

A tétel 1920 előtti története 34 sűrű oldal L. E. Dickson könyvében.

Több, mint 50 bizonyítás ismert, legalább 10 lényegesen különböző.

Két idézet

„Másik híres és gyönyörű tétel Fermat két négyzetszám tétele... Az első osztályba eső prímek kifejezhetők két egész szám négyzetének az összegeként...Ez Fermat tétele, amelyet igen jogosan sorolnak a számelmélet legnagyszerűbb tételei közé. Sajnos nincs olyan bizonyítása, amelyet a meglehetősen szakértő matematikuson kívül más is megértene." G. H. Hardy

„Ez az eredmény figyelemre méltó abban az értelemben, hogy a prímeket - olyan objektumokat, amelyek definíciójában csak szorzás és osztás szerepel - összeköti az egészek *additív* struktúrájával." D. R. Heath-Brown

Az első fennmaradt bizonyítások

A legelső L. Eulertől származik 1746-ból. Hosszú és bonyolult.

a Lemma

Tegyük fel, hogy az n két relatív prím egész négyzetének az összege. Ekkor n minden pozitív egész osztója is felírható két négyzet összegeként.

Euler végtelen leszállással bizonyítja.

A. M. Legendre (1771) egyszerűbb bizonyítás és az alapvető állítás:

Legyen p $4k+1$ alakú prím. Van olyan c egész, amelyre c^2+1 osztható p-vel.

Legyen $m > 0$, a, b tetszőleges egészek.

$$a \equiv b \pmod{m},$$

ha az m osztja az $a - b$ különbséget.

A $\equiv$ örökli az $=$ több hasznos tulajdonságát.
Pl. ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor

$$a \pm c \equiv b \pm d \pmod{m},$$

$$ac \equiv bd \pmod{m}.$$

A $c^2 \equiv -1 \pmod{p}$ megoldhatósága

Legyen p prím, és

$$T = \{1, 2, \ldots, p-1\}.$$

Legyen $i \in T$. Ekkor az

$$i, 2i, \ldots, (p-1)i$$

számok p-vel való osztási maradékai mind különbözők.

Ellenkező esetben volnának $1 \leq j_1 < j_2 \leq p-1$ egészek, melyekre p osztja az $i(j_2 - j_1)$ számot, ami nem lehet.

Tehát minden $i \in T$-hez van (pontosan egy) $i^* \in T$, hogy ii^* p-vel osztva 1-et ad maradékul – röviden $ii^* \equiv 1 \pmod{p}$.

Példa: $p = 13$.

i	1	2	3	4	5	6	7	8	9	10	11	12
i^*	1	7	9	10	8	11	2	5	3	4	6	12

A $c^2 \equiv -1 \pmod{p}$ megoldhatósága II.

Legyen p egy $4k+1$ alakú prímszám és

$$S = \left\{2, 3, \ldots, \frac{p-1}{2}\right\}.$$

Tekintsük az alábbi $\gamma : S \to S$ leképezést:
legyen $\gamma(i) = i^*$, ha $i^* \in S$, és legyen $\gamma(i) = p - i^*$, ha $i^* \notin S$.

A γ involúció: $\gamma(\gamma(i)) = i$ minden $i \in S$-re.

Ugyanis $(p - i^*)^* = p - i$, mert

$$(p - i^*)(p - i) \equiv (-i^*)(-i) \equiv 1 \pmod{p}.$$

Az $|S|$ páratlan: van $c \in S$, melyre $\gamma(c) = c$.

A $c^2 \equiv -1 \pmod{p}$ megoldhatósága III.

Példa: $p = 13$.

i	2	3	4	5	6
$\gamma(i)$	6	4	3	5	2

Ekkor $c = c^*$ nem lehet: különben p osztja $c^2 - 1 = (c+1)(c-1)$-et, vagyis a T elemei közül c csak 1 vagy $p-1$ lehet, de ezek nincsenek S-ben.

Beláttuk, hogy $c = p - c^*$.

Ezt szorozzuk meg c-vel, és használjuk, hogy $cc^* = dp + 1$: $c^2 = cp - dp - 1$, azaz

$$c^2 + 1 = (c - d)p,$$

p osztja a $c^2 + 1$ egészet.

Más megoldások

- $c \equiv \left(\frac{p-1}{2}\right)!$ (Wilson-tétel).
- $c \equiv h^{\frac{p-1}{4}}$, ahol h egy véletlen eleme T-nek. Ez $\frac{1}{2}$ valószínűséggel ad megoldást.
- $c \equiv ab^*$, ahol $a^2 + b^2 = p$.

Példa: $p = 13$.

h	1	2	3	4	5	6	7	8	9	10	11	12
$c \equiv h^3$	1	8	1	12	8	8	5	5	1	12	5	12
c^2	1	12	1	1	12	12	12	12	1	1	12	1

A. Thue bizonyítása, avagy a legegyszerűbb

Legyen $c \in \mathbb{Z}$ melyre $c^2 \equiv -1 \pmod{p}$.

Tekintsük az (x, y) egész párokat, ahol $0 \leq x, y \leq \sqrt{p}$. A számuk $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$.
Van közöttük két különböző (x_1, y_1) és (x_2, y_2) pár, melyekre

$$cx_1 - y_1 \equiv cx_2 - y_2 \pmod{p},$$

$$c(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}.$$

Legyen $x = x_1 - x_2$ és $y = y_1 - y_2$. Ekkor

$$cx \equiv y \pmod{p},$$

$$-x^2 \equiv y^2 \pmod{p},$$

$0 \equiv y^2 + x^2 \pmod{p}$, és $0 < y^2 + x^2 < 2p$, ahonnan $y^2 + x^2 = p$.

Ugyanaz a rács máshogy nézve: J. H. Grace (1927)

Legyen $\mathcal{L}$ azon $(x, y) \in \mathbb{Z}^2$ rácspontok halmaza, amelyekre

$$cx \equiv y \pmod{p}.$$

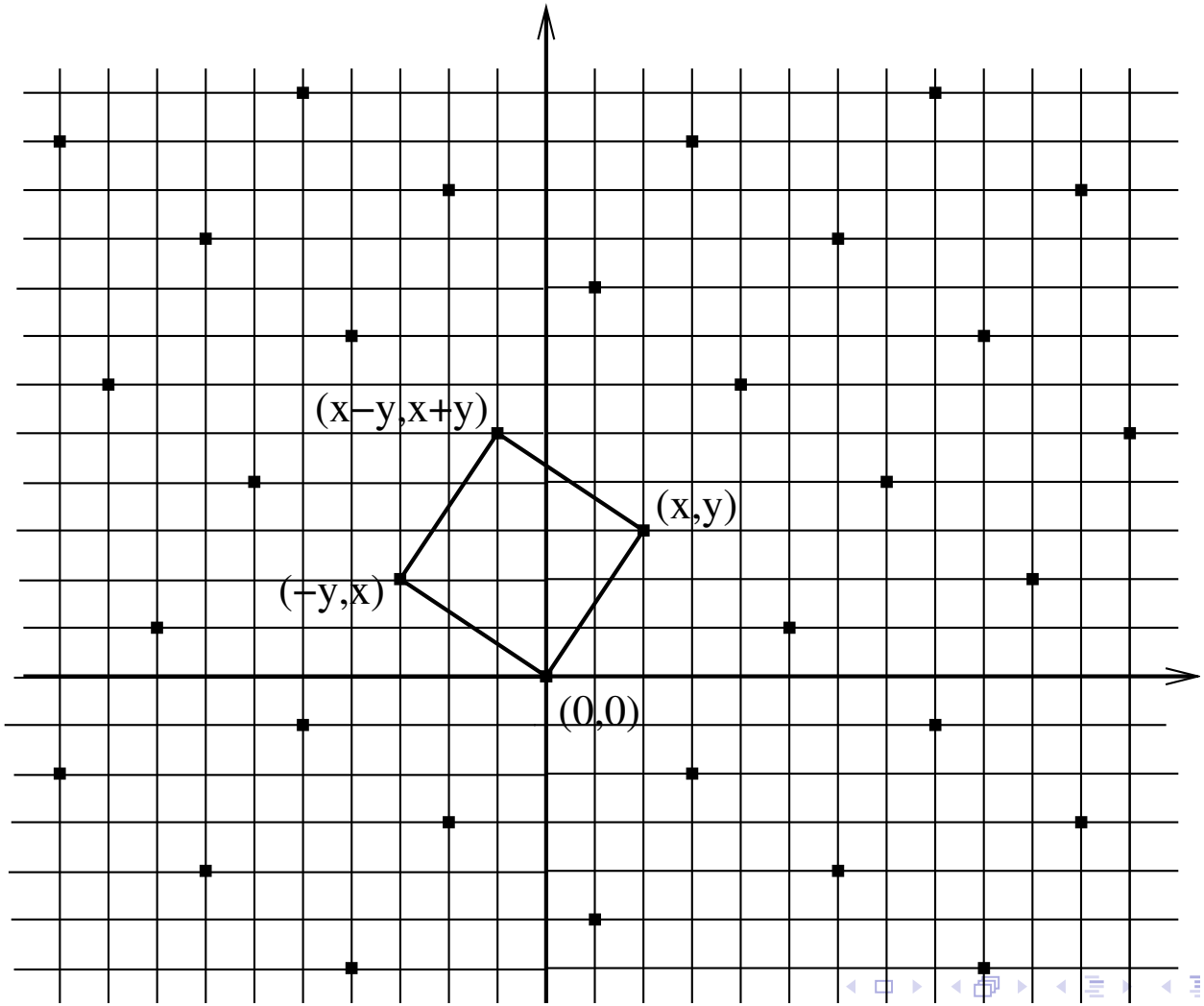
Ha $(x, y), (x', y') \in \mathcal{L}$, akkor $(x \pm x', y \pm y') \in \mathcal{L}$, és $(-y, x) \in \mathcal{L}$.

Legyen $(x, y) \in \mathcal{L}$ minimális hoszúságú nem nulla vektor.

Ekkor $(0, 0)$, (x, y), $(-y, x)$, $(x - y, x + y)$ mind $\mathcal{L}$-beli pontok, és egy üres négyzet csúcsai.
Mekkora a négyzet t területe?

Példa

$p = 13,\ c = 5,\ (x, y) = (2, 3).$



t kiszámolása

Legyen K egy nagy kör $(0,0)$ középponttal. Legyen a K-beli rácspontok száma R, az $\mathcal{L}$ halmaz K-ba eső pontjainak a száma r. Ekkor

$$R + * = tr + *,$$

$$R = pr + *.$$

Innen $(p-t)r = *$, ahonnan $p = t$.

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

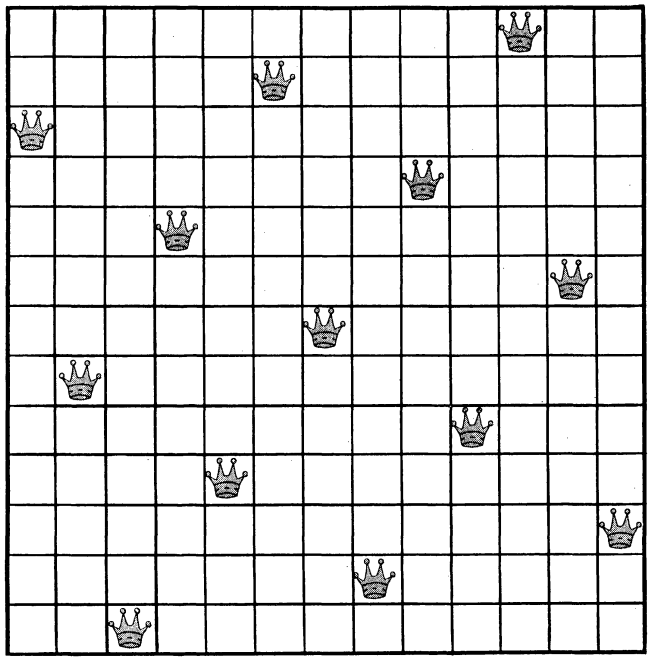
$\mathcal{L}$ ismét másként: Pólya Gy. (1918) nyomán

Szabályos vezérelrendezés a $p \times p$-es sakktáblán: a középső mezőről indulva pl. $(2, 3)$-at lépegetünk.

p egymás nem ütő vezér, 90° forgásszimmetria.

Elemi bizonyítás a Karácsonyi tételre.

(Forrás: L. C. Larson, Math. Magazine, 50(1977), 70. old.)



Bizonyítás a c/p nagyon jó racionális közelítésével

Léteznek a, b egészek, $0 < b < \sqrt{p}$, amelyekkel

$$\left| -\frac{c}{p} - \frac{a}{b} \right| < \frac{1}{b\sqrt{p}}.$$

Legyen

$$d = cb + pa.$$

Ekkor a tört

$$\left| \frac{-d}{pb} \right| < \frac{1}{b\sqrt{p}}.$$

Innen $|d| \leq \sqrt{p}$ és

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

Mivel $d \equiv cb \pmod{p}$,

$$b^2 + d^2 \equiv b^2 + c^2 b^2 \equiv b^2(1 + c^2) \equiv 0 \pmod{p},$$

tehát

$$b^2 + d^2 = p.$$

Bizonyítás leszállással (G. H. Hardy és E.M. Wright nyomán)

Talán Fermat maga is ilyesmire gondolt...

Vannak olyan x, y, m egészek, $0 < m < p$, melyekkel

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

Például $x = c$ és $y = 1$ jó, ahol $c^2 + 1 \equiv 0 \pmod{p}$ és $|c| < p$.

Ha $m > 1$, akkor létezik $x_1, y_1 \in \mathbb{Z}$, amelyekre

$$x_1^2 + y_1^2 = m_1 p, \text{ és } 0 < m_1 < m.$$

Legyen x_0 az x, y_0 pedig az y min. abszolút értékű osztási maradéka m-mel osztva. Ekkor $|x_0|, |y_0| \leq \frac{m}{2}$ és

$$x_0^2 + y_0^2 = m_0 m.$$

Itt $m_0 > 0$, mert nem lehet $x_0 = y_0 = 0$.

$$0 < x_0^2 + y_0^2 \leq 2(m^2/4) = \frac{m}{2} m,$$

tehát $0 < m_0 \leq \frac{m}{2}$.

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

$$x_0^2 + y_0^2 = m_0 m, \qquad 0 < m_0 \leq \frac{m}{2}.$$

Szorozzuk össze őket:

$$m_0 m^2 p = (x^2+y^2)(x_0^2+y_0^2) = (xx_0+yy_0)^2+(xy_0-yx_0)^2 = X^2+Y^2.$$

Itt az X és Y egész is osztható m-mel, amiből

$$m_0 p = \left(\frac{X}{m}\right)^2 + \left(\frac{Y}{m}\right)^2.$$

□

A kezdőlépés után hatékony (polinom idejű) algoritmust kapunk.

Jacobi-azonosság

$$\left(1+2\sum_{k=1}^{\infty} z^{k^2}\right)^2 = 1+4\sum_{n=0}^{\infty}\frac{(-1)^n z^{2n+1}}{1-z^{2n+1}}.$$

Jelölje $r_2(n)$ az $x^2+y^2=n$ egész x,y megoldásainak számát.

$$\sum_{n=0}^{\infty} r_2(n) z^n = \sum_{k=-\infty}^{\infty}\sum_{m=-\infty}^{\infty} z^{k^2+m^2} =$$

$$= \left(\sum_{k=-\infty}^{\infty} z^{k^2}\right)^2 = \left(1+2\sum_{k=1}^{\infty} z^{k^2}\right)^2.$$

$$\sum_{n=1}^{\infty} r_2(n) z^n = 4 \sum_{k=0}^{\infty} \frac{(-1)^k z^{2k+1}}{1 - z^{2k+1}} = 4 \sum_{k=0}^{\infty} (-1)^k z^{2k+1} \sum_{m=0}^{\infty} z^{m(2k+1)} =$$

$$= 4 \sum_{k=0}^{\infty} (-1)^k \sum_{m=1}^{\infty} z^{m(2k+1)} = 4 \sum_{n=1}^{\infty} z^n \sum_{2k+1 \mid n} (-1)^k.$$

$$r_2(n) = 4 \sum_{2k+1 \mid n} (-1)^k$$

Ha p $4l+1$ alakú prím, akkor $r_2(p) = 8$.
Ha p $4l+3$ alakú prím, akkor $r_2(p) = 0$.

Bizonyítás Gauss-egészekkel, R. Dedekind,...

$$\mathbb{G} = \{a + bi : \ a, b \in \mathbb{Z}\}.$$

- $$(a + bi) \pm (c + di) = a \pm c + (b \pm d)i$$
- $$(a + bi)(c + di) = ac - bd + (ad + bc)i$$
- értelmezhető az oszthatóság $\mathbb{G}$-ben: legyen $\alpha, \beta \in \mathbb{G}$, α osztója β-nak, ha van $\gamma \in \mathbb{G}$, hogy $\alpha\gamma = \beta$
- $\pm 1, \pm i$ az egységek $\mathbb{G}$-ben
- érvényes a számelmélet alaptétele
- van egészértékű norma:

$$N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

- a norma multiplikatív: $\alpha, \beta \in \mathbb{G}$ esetén

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

Legyen p egy $4k+1$ alakú prím, $c \in \mathbb{Z}$ melyre p osztója c^2+1-nek.

A p osztja a $(c+i)(c-i)$ szorzatot, és nem osztja egyik tényezőt sem, ezért nem lehet prím $\mathbb{G}$-ben.

A p felbomlik $r \geq 2$ prím szorzatára $\mathbb{G}$-ben:

$$\pi_1 \pi_2 \cdots \pi_r = p.$$

Normát véve mindkét oldalon:

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

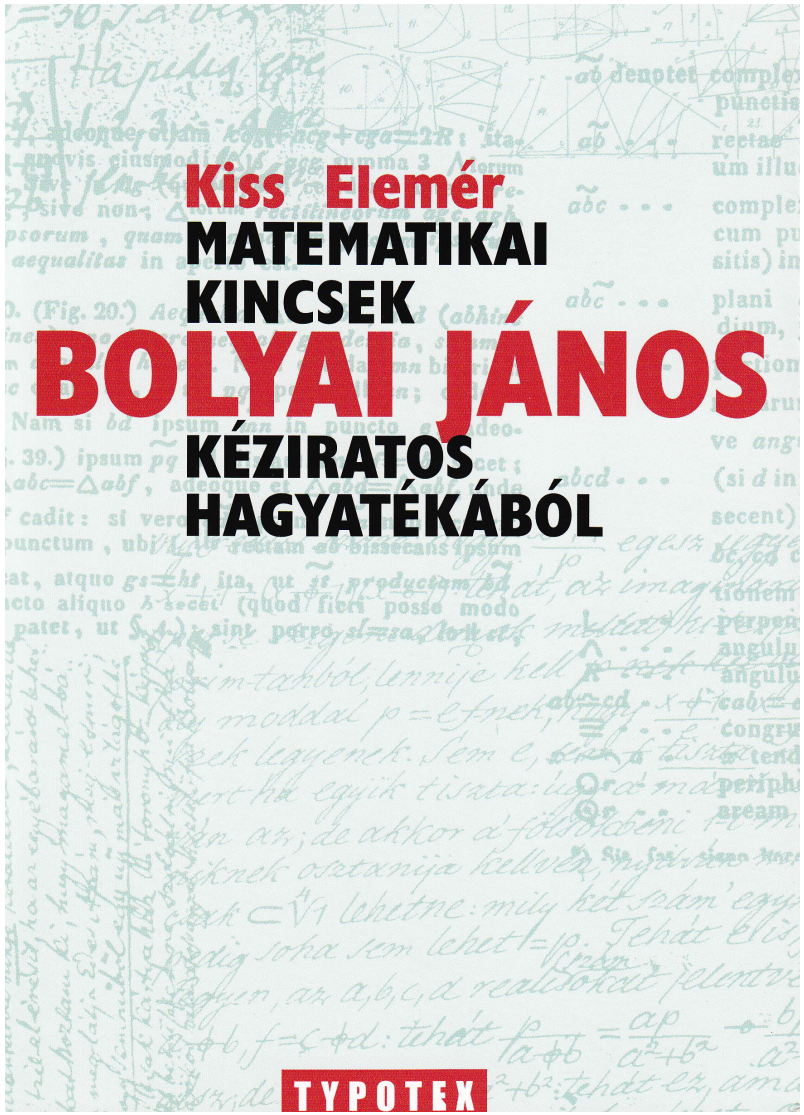
ahonnan $r = 2$ és $N(\pi_1) = p$.

Legyen $\pi = a + bi$. Ekkor

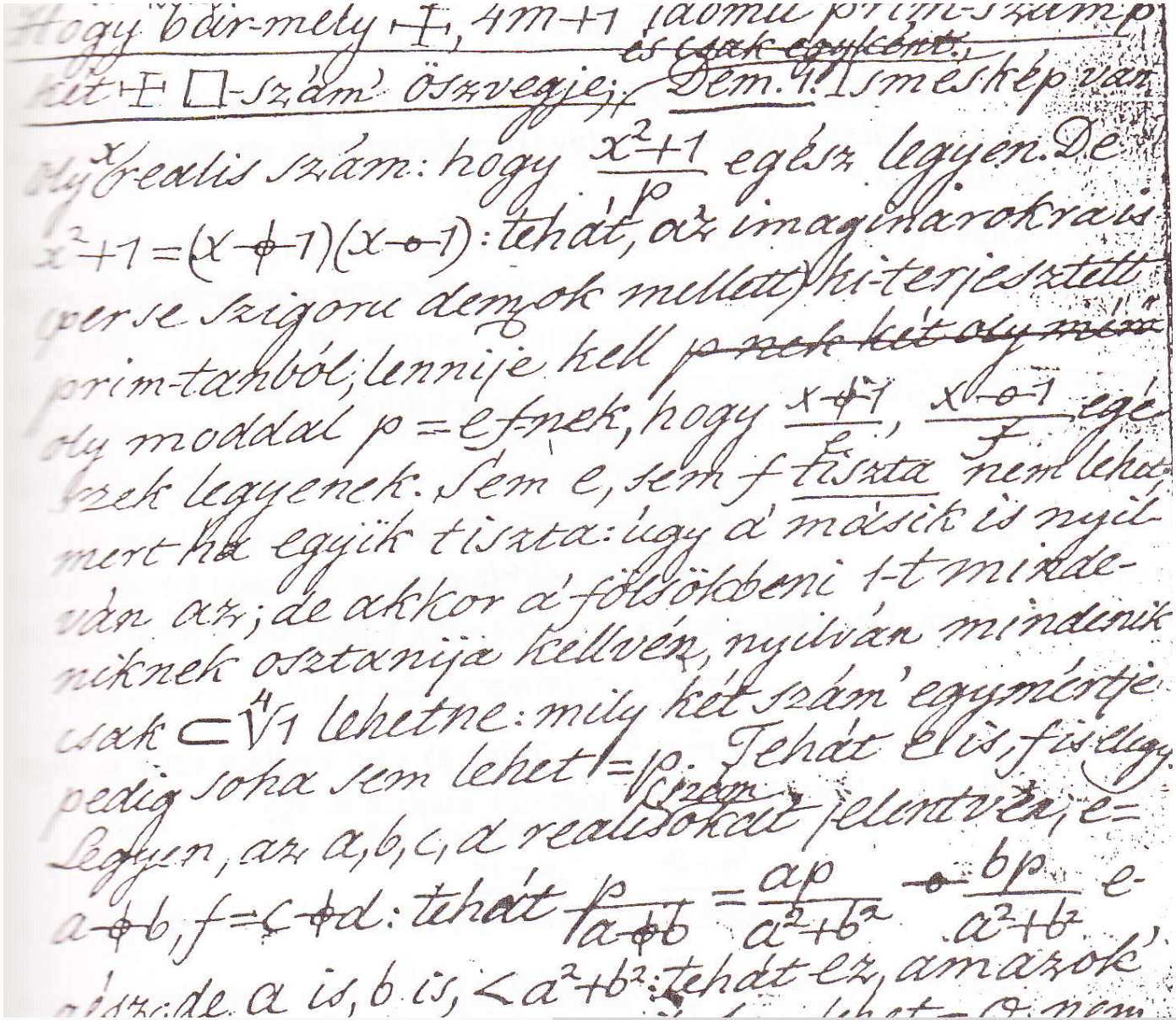
$$p = N(\pi_1) = a^2 + b^2.$$

Bolyai-bélyeg

Egy érdekes könyv



Bolyai János egy (1855-ös?) levele (forrás: az előző kötet)



A levél átirata (forrás: az előző kötet)

Hogy bármely, $4m+1$ idomu prím-szám p két $\square$-szám öszvegje; és csak egyként. {Bármely pozitív $4m+1$ alakú prímszám egyértelműen felírható két egész szám négyzetének összegeként.}

Dem.1! Isméskép {ismeretes} *van oly x reális* {egész} *szám: hogy* $\frac{x^2+1}{p}$ *egész legyen. De* $x^2+1=(x+1)(x-1)$*: tehát, az imagináriusokra is (per se szigorú dem-ok mellett) kiterjesztett prímtanból, lennie kell oly móddal $p=ef$-nek, hogy* $\frac{x+1}{e}, \frac{x-1}{f}$ *egészek legyenek: Sem e, sem f tiszta nem lehet, mert ha egyik tiszta: úgy a másik is nyílván az; de akkor a fölsőkbeni $1-t$ mindeniknek osztania kellvén, nyilván mindenik csak* $\subset \sqrt[4]{1}\{\pm 1, \pm i\}$ *lehetne: míly két szám egymértje* {szorzata} *pedig soha sem lehet $=p$. Tehát e is, f is elegy. Legyen az a, b, c, d reális számokat jelentvén, $e=a+b$, $f=c+d$: tehát*

$$\frac{p}{a+b}=\frac{ap}{a^2+b^2}-\frac{bp}{a^2+b^2}$$

egész, de a is, b is, $<a^2+b^2$: tehát ez, amazok egyikét is, mivel egyik sem lehet $=0$, nem oszthatja; lennie kell tehát az a^2+b^2-nak valamely az 1-nél $>$ mérőjének {tényezőjének}*, mely a p-t ossza, vagyis p-nek az a^2+b^2-tal valamely 1-nél $>$ köz-osztójának. De p prím lévén, más számmal, saját többösin (multipla) kívül, ily osztóval nem bír. Vagy, rövidebben: az említett mérője az a^2+b^2-nek p-t osztván, az, mivel p prím, szükségképp $=p$ magához. Osztja tehát p az a^2+b^2-t, és ha $a^2+b^2=cp$: úgy*

$$\frac{ap}{a^2+b^2}, \quad \frac{bp}{a^2+b^2}$$

Két kérdés

Volt-e Bolyai Jánosénál korábbi, a Gauss-egészek számelméletét használó bizonyítás?

Meghatározható-e pontosa(bba)n a Bolyai János levelének a keletkezési ideje?

A legrövidebb (Amer. Math. Monthly, 97(1990), 144. old.)

A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares

D. ZAGIER
Department of Mathematics, University of Maryland, College Park, MD 20742

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

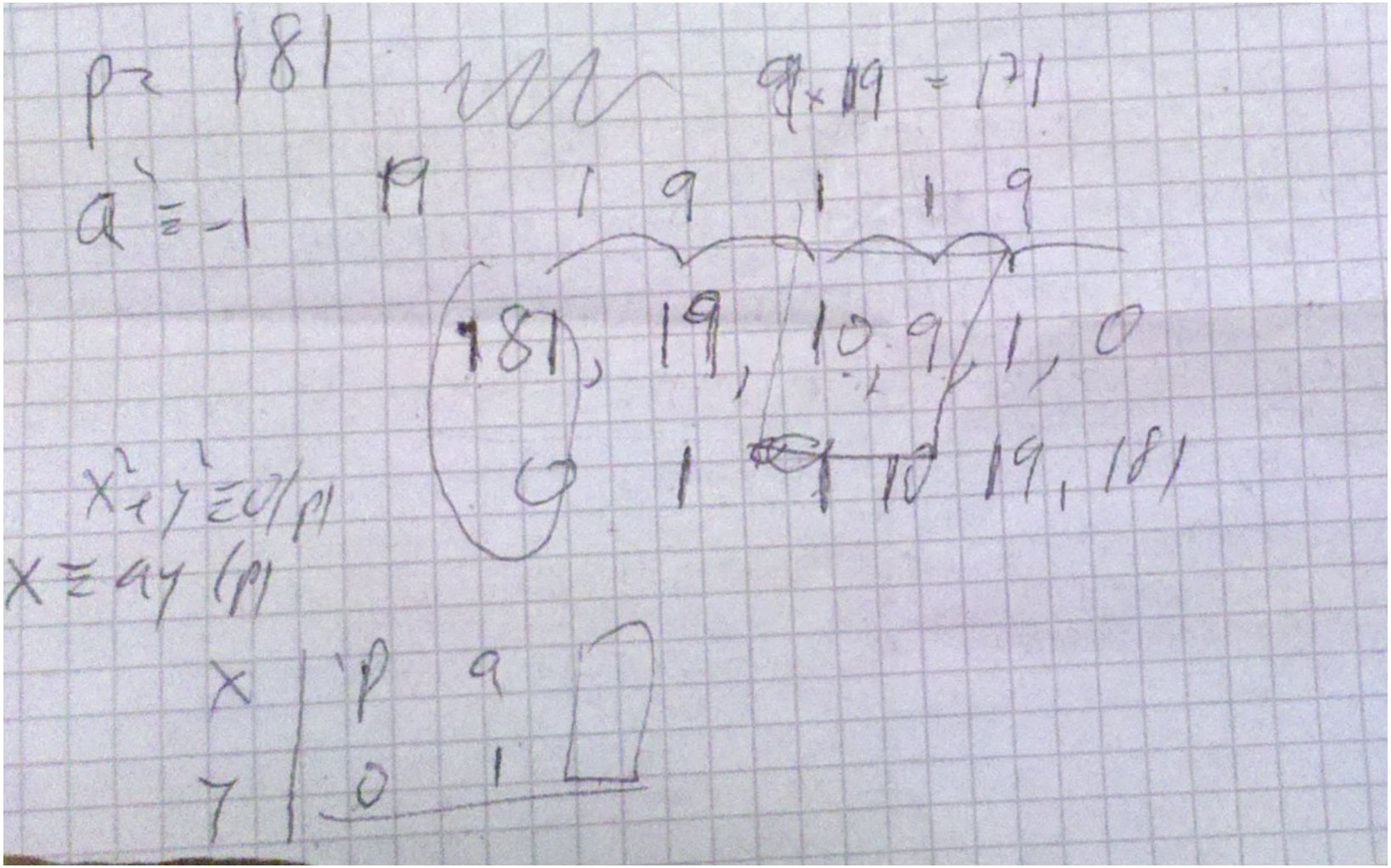
$$(x,y,z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & \text{if } x < y - z \\ (2y - x,\ y,\ x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point. □

$(1, 1, \frac{p-1}{4})$ az egy szem fixpont.

$$(x-2y)^2+4(x-y+z)y = x^2-4xy+4y^2+4xy-4y^2+4yz = x^2+4yz = p.$$

Don Zagier számai (Budapest, 2010. december)



A híres-nevezetes rokon

J. L. Lagrange tétele (1770)

Minden természetes szám előáll négy négyzetszám összegeként.

Végtelen leszállás, nagyjából ugyanaz a gondolatmenet, mint a karácsonyi tételnél.

Legyen p tetszőleges prímszám. Vannak a, b egészek, hogy p osztja az $1 + a^2 + b^2$ számot.

M. O. Rabin, J. Shallit (1986): egy előállítás megkapható polinom időben - véletlent használva.

Irodalom+

- M. Aigner, G. Ziegler, Bizonyítások a Könyvből, Typotex, 2009.
- J. H. Conway, D. A. Smith, On quaternions and octonions: their geometry, arithmetic, and symmetry, A. K. Peters, 2003.
- L. E. Dickson, History of the theory of numbers II., Carnegie Institution of Washington, 1920.
- C. Elsholtz, A combinatorial approach to sums of two squares and related problems, In: Additive number theory, Festschrift in honor of the sixtieth birthday of Melvyn B. Nathanson. Springer, 2010, pp. 115–140.
- Freud R., Gyarmati E., Számelmélet, Nemzeti Tankönyvkiadó, 2006.
- E. Grosswald, Representations of integers as sums of squares, Springer, 1985.

- G. H. Hardy, E. M. Wright, An introduction to the theory of numbers, 3rd ed., Oxford Univ. Press, 1956.
- K. F. Ireland, M. I. Rosen, A classical introduction to modern number theory, 2nd ed., Springer, 1990.
- K. Kato, N. Kurokawa, T. Saito, Number Theory I: Fermat's dream, American Math. Soc., 2000
- I. Niven, H. S. Zuckerman, Bevezetés a számelméletbe, Műszaki Könyvkiadó, 1978.
- L. C. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, 2003.
- A. Weil, Number theory: an approach through history from Hammurapi to Legendre, Birkhäuser, 2007.