3 négyzetszám-tétel?

Tétel $n \geq 0$ pontosan akkor áll elő 3 négyzetszám összegeként, ha

nem $4^a(8k-1)$ alakú.

(Másik: $\sum_{n=0}^{\infty} q^{n^2}$ + KFT.)

$x^2 + y^2$

$x^2 - 3y^2$

Biz.:

Tétel (Hasse–Minkowski) Egy egész együtthatós nemelfajuló kvadratikus alaknak pontosan akkor van nemtriviális egész számokból álló zérushelye, ha van nemtriviális valós gyöke és minden p prímre és $n \geq 1$-re van olyan gyöke mod p^n, hogy nem minden változó osztható p-vel.

ebből 3-négyzetszám-tétel

$\boxed{\Rightarrow}$ Tfh. $x^2+y^2+z^2 = 4^a(8k-1)$. Tfh. $a=0$

$$x^2 \equiv 0,1,4 \quad (8) \qquad \Rightarrow \quad 8k-1 \not\equiv x^2+y^2+z^2 \; (8).$$

Tfh. $a \geq 1 \Rightarrow 2 \mid x,y,z \Rightarrow \left(\frac{x}{2}\right)^2+\left(\frac{y}{2}\right)^2+\left(\frac{z}{2}\right)^2 = 4^{a-1}(8k-1)$

ind. a szerint.

$\boxed{\Leftarrow}$ Tfh. $n \neq 4^a(8k-1)$

$$f(x,y,z,w) = x^2+y^2+z^2-nw^2$$

H-M: $\mathbb{R}$ ✓

Lemma 1 Tfh. $a \equiv 1 \; (8) \Rightarrow x^2 \equiv a \; (2^k)$ $\forall k \geq 3$-ra megoldható.

Biz.: $x = 2y+1$

$$(2y+1)^2 \equiv a \quad (2^k)$$
$$4y^2+4y+1 \equiv a \quad (2^k)$$

$$\Longleftarrow \qquad y^2 + y \equiv \frac{a-1}{4} \qquad (2^{k-2})$$

$\frac{a-1}{4} \to$ ps.

$$y^2 + y \equiv 0 \quad (2) \qquad y \equiv 0, 1 \quad (2)$$

Hensel lemma (ált. prímhatványalapú kongruenciák visszavezetése prímalapúra)

$$\Longrightarrow \exists \text{ gyök } \bmod 2^{k-2}. \quad \square$$

[$a = 1 + 8t$

$$\sqrt{1+x} = \sum_{n=0}^{\infty} \binom{1/2}{n} x^n \qquad \binom{1/2}{n} = \frac{1/2\,(1/2-1)\cdots(1/2-n+1)}{n!}$$

$$\binom{\alpha}{n}$$

$$x = 8t$$]

Lemma 2 $k \geq 3$, $n \not\equiv 7 \ (8) \Longrightarrow \exists\, x, y, z \in \mathbb{Z}$

$$x^2 + y^2 + z^2 \equiv n \quad (2^k) \qquad (\Longrightarrow x^2 + y^2 + z^2 - nw^2 \equiv 0 \ \exists \text{ nemtriv. mo. } w > 1)$$

Biz.: mod 8 ✓ és tetszőleges $\equiv 1 \ (8)$ számmal végigszorozható. $\square$

Lemma 3 $p>2$ prím, $r \geq 1 \Rightarrow \forall$ szám előáll $x^2+y^2 p z^2$ alakban mod p^r.

Biz.:

mod p: $\quad c - y^2 \equiv x^2 \quad (p)$

$$\#\{c-y^2 \mid y \in \mathbb{F}_p\} = \frac{p+1}{2} = \#\{x^2 \mid x \in \mathbb{F}_p\}$$

nem lehet diszjunkt.

$$x_0^2 + y_0^2 \equiv c \quad (p)$$

$$x_0^2 \equiv a \quad (p)$$

(x^2-a)-nak csak $a \equiv 0$ (p) esetén van 2-szeres gyöke mod p, különben fel lehet emelni. $\square$

fKM $\Rightarrow$ $n = \left(\frac{x}{w}\right)^2 + \left(\frac{y}{w}\right)^2 - \left(\frac{z}{w}\right)^2$ error $z=1$ (egyébként $z=0$).

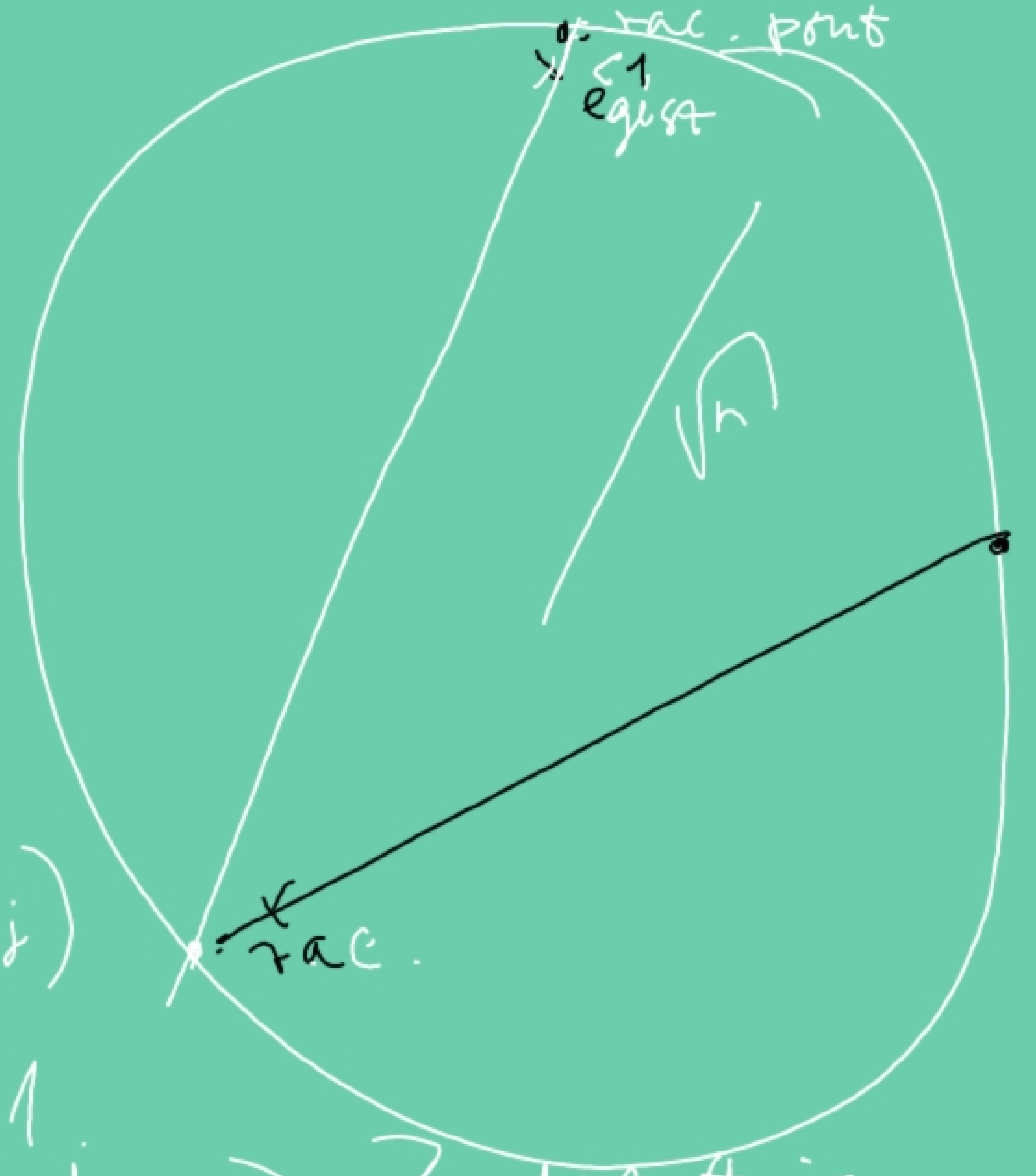
Lemma 4 (Davenport – Cassels)

$f(x) = \sum_{i,j=1}^{q} a_{ij} x_i x_j$ pozitív definit kvadratikus alak

$a_{ij} = a_{ji} \in \mathbb{Z}$. Tfh. $x = (x_1, \dots, x_q) \in \mathbb{Q}^q$

$\exists\; y \in \mathbb{Z}^q \qquad f(x-y) = \sum a_{ij}(x_i - y_i)(x_j - y_j) < 1$

$\Rightarrow$ Ha $n \in \mathbb{Z}$ előáll $\mathbb{Q}$ fölött f értékeként $\Rightarrow$ $\mathbb{Z}$ fölött is.



Biz.: $A = ((a_{ij})) \in \mathbb{Z}^{q \times q}$ $\quad f(x) = x^T A x$, $\quad \beta(x,y) = x^T A y$.

bilin. fv.

$\frac{x}{t}$: rac. pont $\left(\frac{x_1}{t}, \frac{x_2}{t}, \dots, \frac{x_q}{t}\right) \in \mathbb{Q}^q$ $\quad t$ közös nevező.

$x_j \in \mathbb{Z}$.

$$n = \beta\left(\frac{x}{t}, \frac{x}{t}\right) \Rightarrow t^2 n = \beta(x,x)$$

$$\exists\, y \in \mathbb{Z}^q \qquad \frac{x}{t} = y + z \qquad \beta(z,z) < 1. \qquad \beta(z,z) = 0 \ (\Rightarrow z = 0)$$

$$a := \beta(y,y) - n \in \mathbb{Z}$$

$$b := 2(nt - \beta(x,y))$$

$$t' = at + b \in \mathbb{Z}$$

$$x' = ax + by \in \mathbb{Z}^q$$

$\frac{x'}{t'} \in \mathbb{Q}^q$ a másik metszéspont.

$$\beta(x', x') = \beta(ax + by,\ ax + by) = a^2 \beta(x,x) + 2ab\, \beta(x,y)$$
$$+\ b^2 \beta(y,y) =$$

$$= n a^2 t^2 + b^2(\cancel{1} + n) + ab(2nt - \cancel{t})$$
$$= n(at + b)^2 = n(t')^2.$$

$$t t' = at^2 + bt = t^2 \beta(y,y) - nt^2 + 2nt^2 - 2t\, \beta(x,y) =$$
$$= t^2 \beta(y,y) + \beta(x,x) - 2t\, \beta(x,y) =$$
$$= \beta(x - ty,\ x - ty) = t^2 \beta(z,z) < t^2.$$
$$\Rightarrow t' < t. \qquad \square$$

<u>Követk.:</u> 4 négyzetszám tétel.

Waring problémakör

Legyen $g(k)$ legkisebb olyan r poz. egész, hogy $\forall$ poz. egész előáll $\leq r$ db pozitív k-adik hatvány összegeként.

$g(2)=4$, Waring (1770) azt állította, hogy

$g(2)\leq 4$, $g(3)\leq 9$, $g(4)\leq 19$, "stb."

__Tétel__ (Hilbert 1909) $g(k)<\infty$ $\forall k\geq 2$-re.

__Tétel__ $g(k)\geq 2^k+\left\lfloor\left(\frac{3}{2}\right)^k\right\rfloor-2$.

Biz.: $n = t2^k - 1$, t maximális úgy $n < 3^k$.

$\Rightarrow$ csak 2^k-ok és 1^k összege lehet, 2^k-ok száma $\le t-1$.

$$(t-1) + 2^k - 1 \le g(k)$$

$$t2^k - 1 < 3^k$$
$$\Updownarrow$$
$$t \le \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor \qquad \square$$

Mahler (1957) $\le$ véges sok olyan k van, amire $2^k\left\{\left(\tfrac{3}{2}\right)^k\right\} + \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor > 2^k$.

Tétel (Dickson, Pillai, Rubugunday, Niven, 1944)

$$g(k) = 2^k + \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor - 2 \quad \text{ha} \quad 2^k\left\{\left(\tfrac{3}{2}\right)^k\right\} + \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor \le 2^k.$$

(egyébként $g(k) = 2^k + \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\tfrac{4}{3}\right)^k \right\rfloor - 2$ vagy -3.)

$G(k)$: legkisebb olyan r, hogy $\forall$ elég nagy egész előáll $\leq r$ db pozitív k-adik hatvány összegeként.

$G(k) \leq g(k)$, $G(2) = g(2) = 4$.

Hardy–Littlewood / Vinogradov: $G(k) \leq k(3\log k + 11)$

Legjobb (~ 2000, Wooley, Vaughan) $G(k) \leq k\log k + k\log\log k + C\cdot k$

Sejtés: $G(k) = k+1$ "sok" k-ra.

Tétel $k+1 \leq G(k)$.

Biz.: Tfh. $G(q) \le q$ valamilyen q-ra. ≥ 2

$$f(M) := \left| \left\{ 0 \le n \le M \;\middle|\; \begin{array}{l} n = x_1^q + \dots + x_q^q \\ x_j \in \mathbb{Z}^{\ge 0} \end{array} \right\} \right| \geqq M - n_0$$

ha $\forall\, n \geqq n_0$ előáll.

$$0 \le x_i \le \sqrt[q]{n} \le \sqrt[q]{M}$$

$$M - n_0 \le f(M) \le \binom{\lfloor \sqrt[q]{M} \rfloor + 1 + q - 1}{q} \le \binom{\sqrt[q]{M} + q}{q} =$$

$$\underbrace{1 - \frac{n_0}{M}}_{\substack{M \to \infty \\ 1}} \le \frac{1}{q!} \underbrace{\left(1 + \frac{1}{\sqrt[q]{M}}\right) \cdots \left(1 + \frac{q}{\sqrt[q]{M}}\right)}_{\frac{1}{q!}} = \frac{1}{q!} \left(\frac{(\sqrt[q]{M} + 1)(\sqrt[q]{M} + 2) \cdots (\sqrt[q]{M} + q)}{\dots} \right.$$

$\lightning$

$\square$

Bináris kvadratikus alakok

$ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$ rögz.

Def.: primitív, ha $(a, b, c) = 1$.

Mely prímek tudják nemtriviálisan osztani? $(p \nmid x$ v. $p \nmid y)$.

$p \mid a \Rightarrow$ ✓ $x = 1$, $y = 0$. , $p \nmid a$. $p \neq 2$

$(p = 2: \mid x^2 + xy + y^2 \Leftrightarrow 2 \mid x$ és $2 \mid y)$

a, b, c ptlan $\Rightarrow$ nem tudja.

$p \mid ax^2 + bxy + cy^2 \Leftrightarrow p \mid 4a^2x^2 + 4abxy + 4acy^2$

$p \nmid a$

$$4a^2x^2 + 4abxy + 4acy^2 = (2ax + by)^2 + y^2(4ac - b^2)$$

$p \mid y \Rightarrow p \mid x$

$p \nmid y \Rightarrow \left(\frac{2ax + by}{y}\right)^2 \equiv b^2 - 4ac \quad (p).$

$$\Longleftrightarrow \quad \left(\frac{b^2-4ac}{p}\right) = 1 \text{ v. } 0.$$