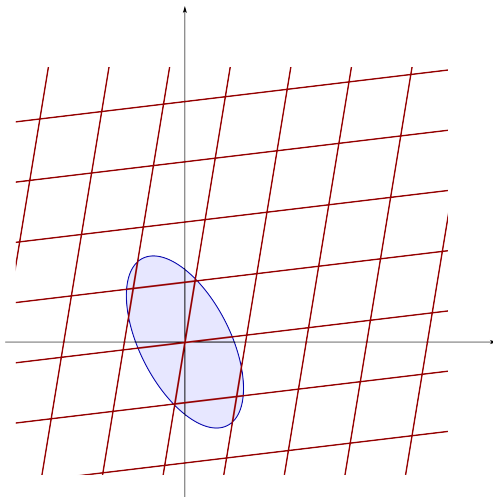


Két négyzetszám – öt bizonyítás

Minkowski tétele



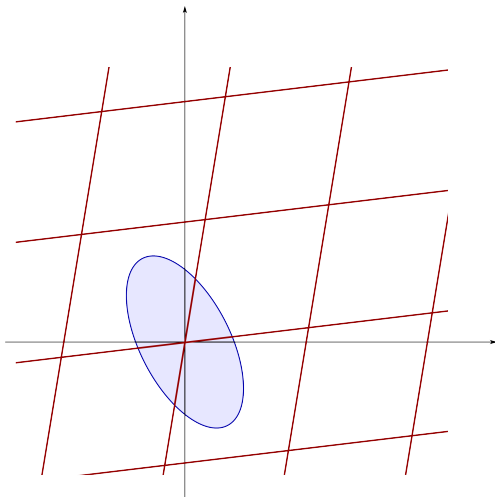
Legyen R egy paralelogrammarács a síkon; jelölje T a paralelogrammák területét.

Legyen K egy konvex, origóra szimmetrikus halmaz.

Tétel (Minkowski)

Ha K területe nagyobb, mint $4T$, akkor K tartalmaz az origón kívül még egy rácspontot.

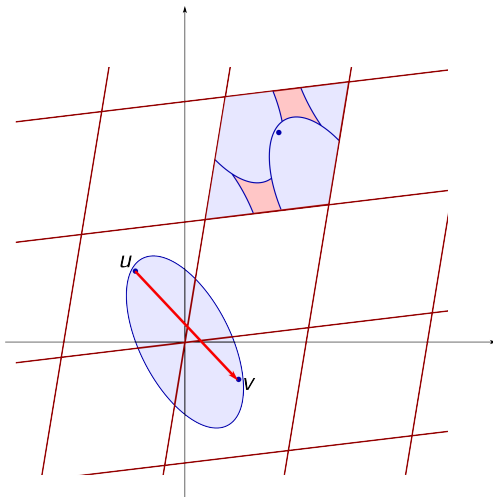
Minkowski tételének bizonyítása



$$R = \{k\mathbf{a} + l\mathbf{b} : k, l \in \mathbb{Z}\}$$

$$2R = \{2k\mathbf{a} + 2l\mathbf{b} : k, l \in \mathbb{Z}\}$$

Minkowski tételének bizonyítása



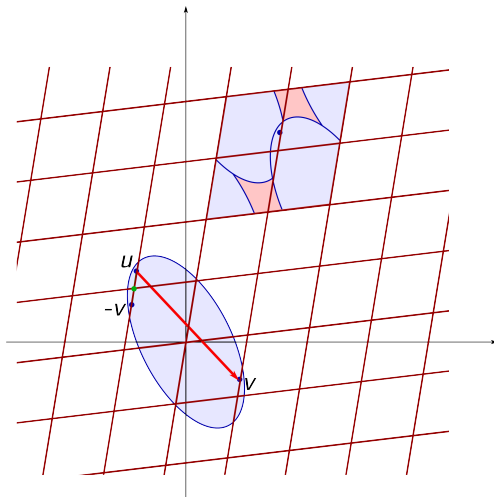
Jelöljük ki egy paralelogrammát (területe $4T$), és toljuk ide mindazokat a paralelogrammákat, amelyekbe K belemetsz.

Mivel K területe nagyobb, mint $4T$, van olyan pont, ami többszörösen le van fedve.

Jelölje egy ilyen pont két különböző „őset” \mathbf{u} és \mathbf{v} .

Ezek egymásból egy rácsvektorral való eltolással megkaphatók:
 $\mathbf{u} - \mathbf{v} \in 2R$.

Minkowski tételének bizonyítása



$$\mathbf{u}, \mathbf{v} \in K, \quad \mathbf{u} - \mathbf{v} \in 2R$$

$$K \text{ szimmetrikus} \implies -\mathbf{v} \in K$$

$$K \text{ konvex} \implies \frac{\mathbf{u} - \mathbf{v}}{2} \in K$$

$$\mathbf{u} - \mathbf{v} \in 2R \implies \frac{\mathbf{u} - \mathbf{v}}{2} \in R$$

$$\text{Tehát } \frac{\mathbf{u} - \mathbf{v}}{2} \in K \cap R.$$

□

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

Pontosan azok a természetes számok állnak elő két négyzetszám összegeként, amelyeknek prímszámhatványtényezős felbontásában a $4k + 3$ alakú prímszámok páros kitevővel szerepelnek.

A bizonyítás „lelke” az alábbi állítás.

Lemma

Minden $4k + 1$ alakú prímszám előáll két négyzetszám összegeként.

Biz.

$$p \equiv 1 \pmod{4} \implies \left(\frac{-1}{p}\right) = 1 \implies \exists c \in \mathbb{N} : c^2 \equiv -1 \pmod{p}$$

Tehát van p -nek olyan többszöröse, ami előáll két négyzetszám összegeként: $p \mid c^2 + 1$.

Innen többféleképpen lehet folytatni ...

Első bizonyítás: Minkowski tételével

Tekintsük az $\mathbf{a} = (p, 0)$ és $\mathbf{b} = (c, 1)$ vektorok által generált R rácsot. Az alaptartomány területe $T = p$.

Ha $\mathbf{u} = (u_1, u_2) \in R$, akkor $|\mathbf{u}|^2 = u_1^2 + u_2^2$ osztható p -vel. Valóban, ha $\mathbf{u} = k \cdot \mathbf{a} + \ell \cdot \mathbf{b} = (k \cdot p + \ell \cdot c, k \cdot 0 + \ell \cdot 1) = (kp + \ell c, \ell)$, akkor

$$|\mathbf{u}|^2 = (kp + \ell c)^2 + \ell^2 \equiv \ell^2 c^2 + \ell^2 = \ell^2 (c^2 + 1) \equiv 0 \pmod{p}.$$

Legyen K az origó középpontú, $\sqrt{2p}$ sugarú nyílt körlap:

$$K = \{(u_1, u_2) \in \mathbb{R}^2 : u_1^2 + u_2^2 < 2p\}.$$

Ennek területe $2p\pi > 4p$, tehát Minkowski tétele szerint $\exists \mathbf{u} \in K \cap R \setminus \{\mathbf{0}\}$.

$$\left. \begin{array}{l} \mathbf{u} \in R \implies p \mid u_1^2 + u_2^2 \\ \mathbf{0} \neq \mathbf{u} \in K \implies 0 < u_1^2 + u_2^2 < 2p \end{array} \right\} \implies u_1^2 + u_2^2 = p$$

□

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + bi$ ($a, b \in \mathbb{Z}$) alakú számok (Gauss-egészek) körében is fel lehet építeni a számelméletet. Itt is ekvivalens egymással a felbonthatatlanság és a prímtulajdonság. A $4k + 3$ alakú prímszámok ebben a gyűrűben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = (2 + 3i)(2 - 3i) = 2^2 - i^2 = 4 - (-9) = 13.$$

Legyen p egy $4k + 1$ alakú prímszám, ekkor $\exists c \in \mathbb{N} : p \mid c^2 + 1$.
Ha p prímtulajdonságú lenne a Gauss-egészek körében is, akkor

$$p \mid c^2 + 1 = (c + i)(c - i) \implies p \mid c + i \text{ vagy } p \mid c - i,$$

ami lehetetlen. Tehát p nem prím, ezért nem is felbonthatatlan.
Meg lehet mutatni, hogy p nemtriviális felbontása csak így festhet:

$$p = (a + bi)(a - bi).$$

Felbontva a zárójeleket, kapjuk, hogy $p = a^2 + b^2$.



Harmadik bizonyítás: végtelen leszállással (vázlat)

Létezik $x, y, k \in \mathbb{N}$, hogy $x^2 + y^2 = kp$ (pl. $x = c, y = 1$). Megmutatjuk, hogy $k > 1$ esetén van p -nek kp -nél kisebb többszöröse is, ami előáll két négyzetszám összegeként. Ez nem mehet végtelen sokáig...

AÁMNTFH. $|x|, |y| < \frac{p}{2}$; ebből következik, hogy $k < p$. Vegyük x és y legkisebb abszolút értékű maradékát modulo k :

$$x \equiv u \pmod{k}, \quad y \equiv v \pmod{k}, \quad |u|, |v| \leq \frac{k}{2}.$$

Az $1 < k < p$ egyenlőtlenségből következik, hogy $u, v \neq 0$ (miért?).

$$kp \cdot (u^2 + v^2) = (x^2 + y^2) \cdot (u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2. \quad (*)$$

A jobb oldalon mindkét tag osztható k^2 -tel, mert

$$xu + yv \equiv x^2 + y^2 = kp \equiv 0 \pmod{k};$$

$$xv - yu \equiv xy - yx = 0 \equiv 0 \pmod{k}.$$

Tehát a (*) egyenlőséget leoszthatjuk k^2 -tel:

$$\left(\frac{xu + yv}{k}\right)^2 + \left(\frac{xv - yu}{k}\right)^2 = kp \cdot \frac{u^2 + v^2}{k^2} \leq kp \cdot \left(\frac{1}{4} + \frac{1}{4}\right) < kp. \quad \square$$

Negyedik bizonyítás: skatulyaelvvel (vázlat)

Tekintsük az összes $x + cy$ alakú számokat, ahol $0 \leq x, y \leq \lfloor \sqrt{p} \rfloor$.

Ez összesen $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ szám, ezért van köztük kettő, amelyeknek ugyanaz a maradéka p -vel osztva:

$$\begin{aligned}x_1 + cy_1 &\equiv x_2 + cy_2 \pmod{p} \implies x_1 - x_2 \equiv c \cdot (y_2 - y_1) \\ &\implies (x_1 - x_2)^2 \equiv c^2 \cdot (y_1 - y_2)^2 \\ &\implies (x_1 - x_2)^2 \equiv (-1) \cdot (y_1 - y_2)^2 \\ &\implies (x_1 - x_2)^2 + (y_1 - y_2)^2 \equiv 0 \\ &\implies (x_1 - x_2)^2 + (y_1 - y_2)^2 \text{ osztható } p\text{-vel.}\end{aligned}$$

Node $|x_1 - x_2|, |y_1 - y_2| < \sqrt{p}$ miatt $0 < (x_1 - x_2)^2 + (y_1 - y_2)^2 < 2p$,
vagyis $(x_1 - x_2)^2 + (y_1 - y_2)^2 = p$. □

Ötödik bizonyítás: egy mondattal (vázlat)

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. \square

This proof is a simplification of one due to Heath-Brown [1] (inspired, in turn, by a proof given by Liouville). The verifications of the implicitly made assertions—that S is finite and that the map is well-defined and involutory (i.e., equal to its own inverse) and has exactly one fixed point—are immediate and have been left to the reader. Only the last requires that p be a prime of the form $4k + 1$, the fixed point then being $(1, 1, k)$.