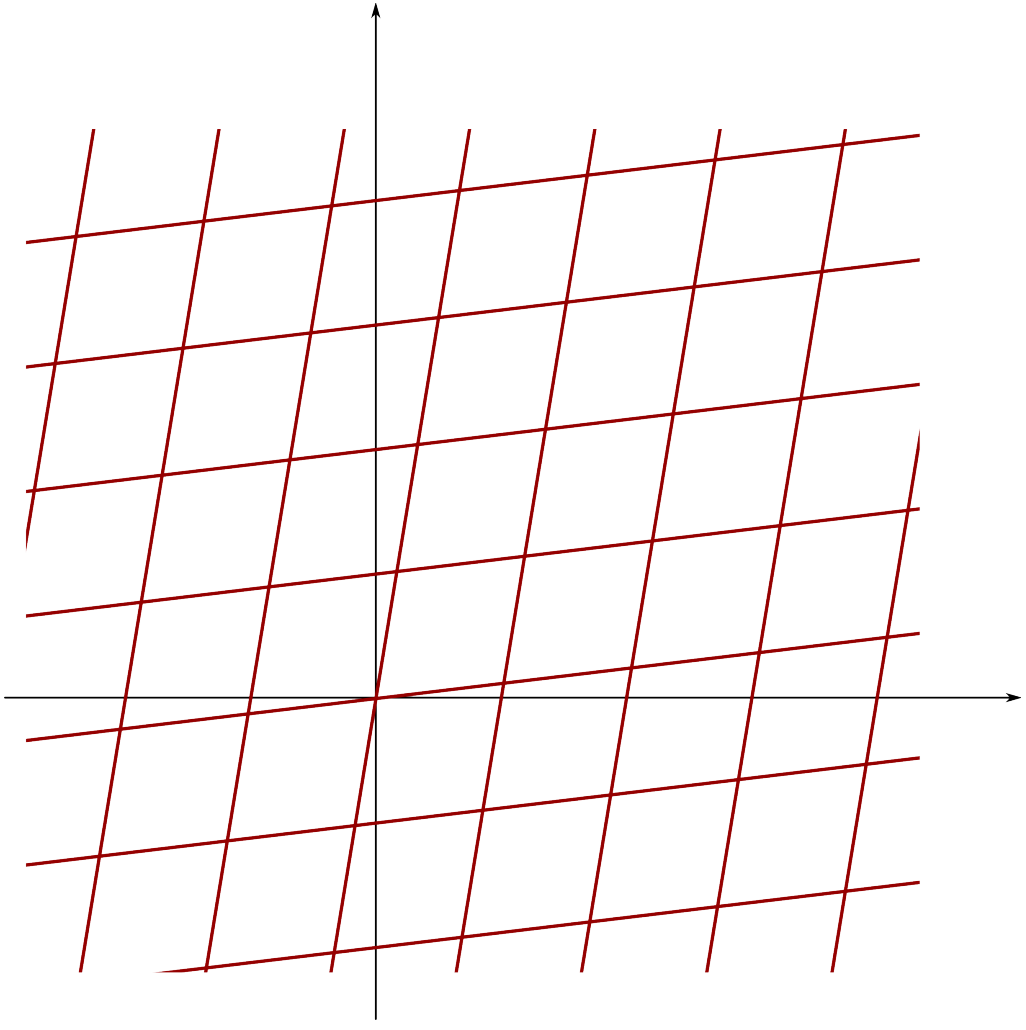
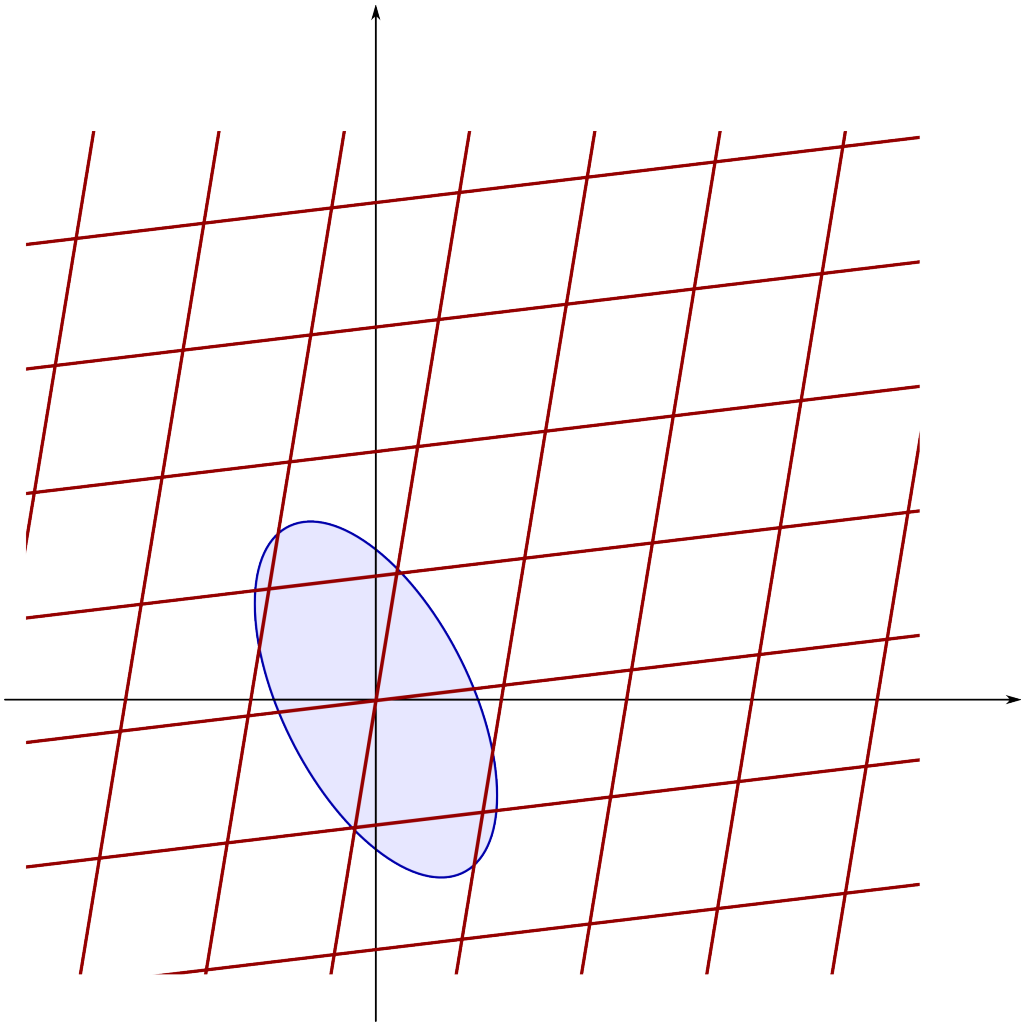
Két négyzetszám — három bizonyítás

Minkowski tétele



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

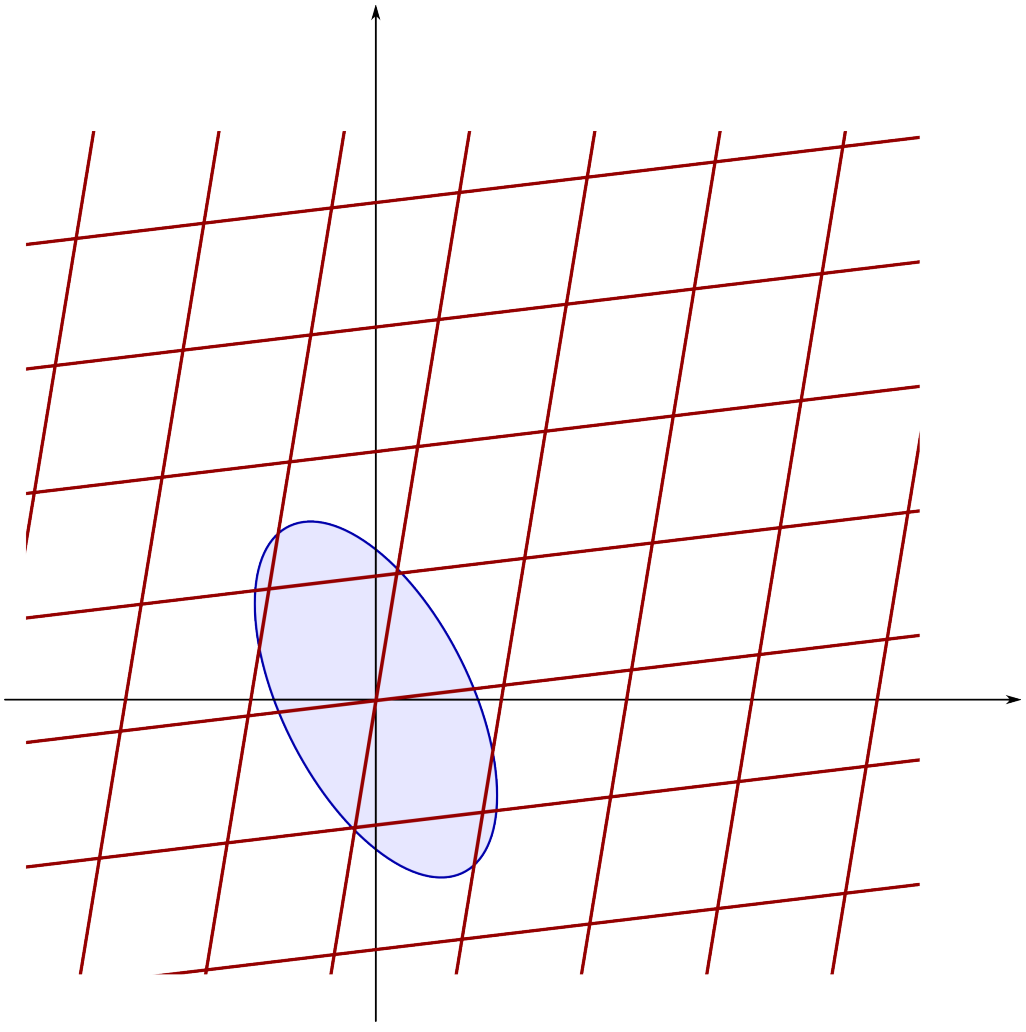
Minkowski tétele



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

Legyen K egy konvex, origóra szimmetrikus halmaz.

Minkowski tétele

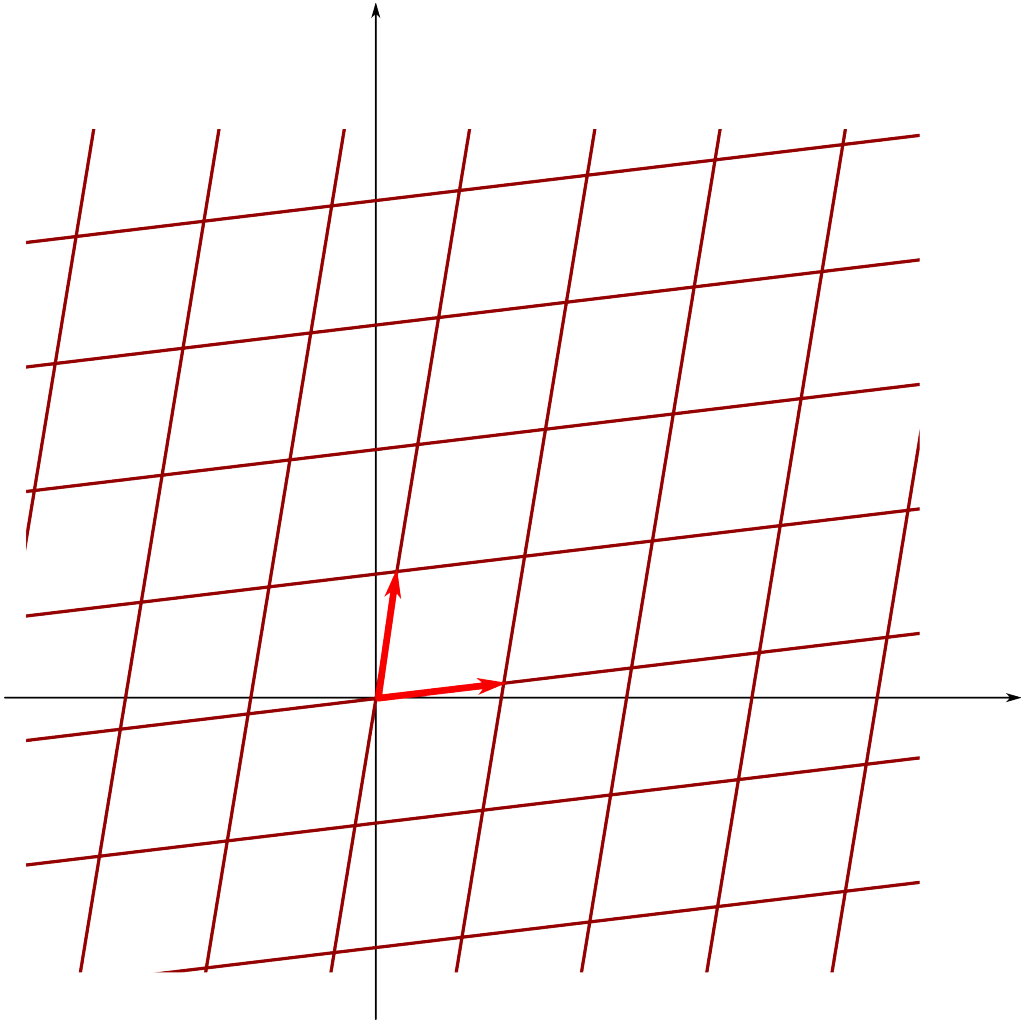


Legyen R egy paralelogrammarács a síkon; jelölje T a paralelogrammák területét.

Legyen K egy konvex, origóra szimmetrikus halmaz.

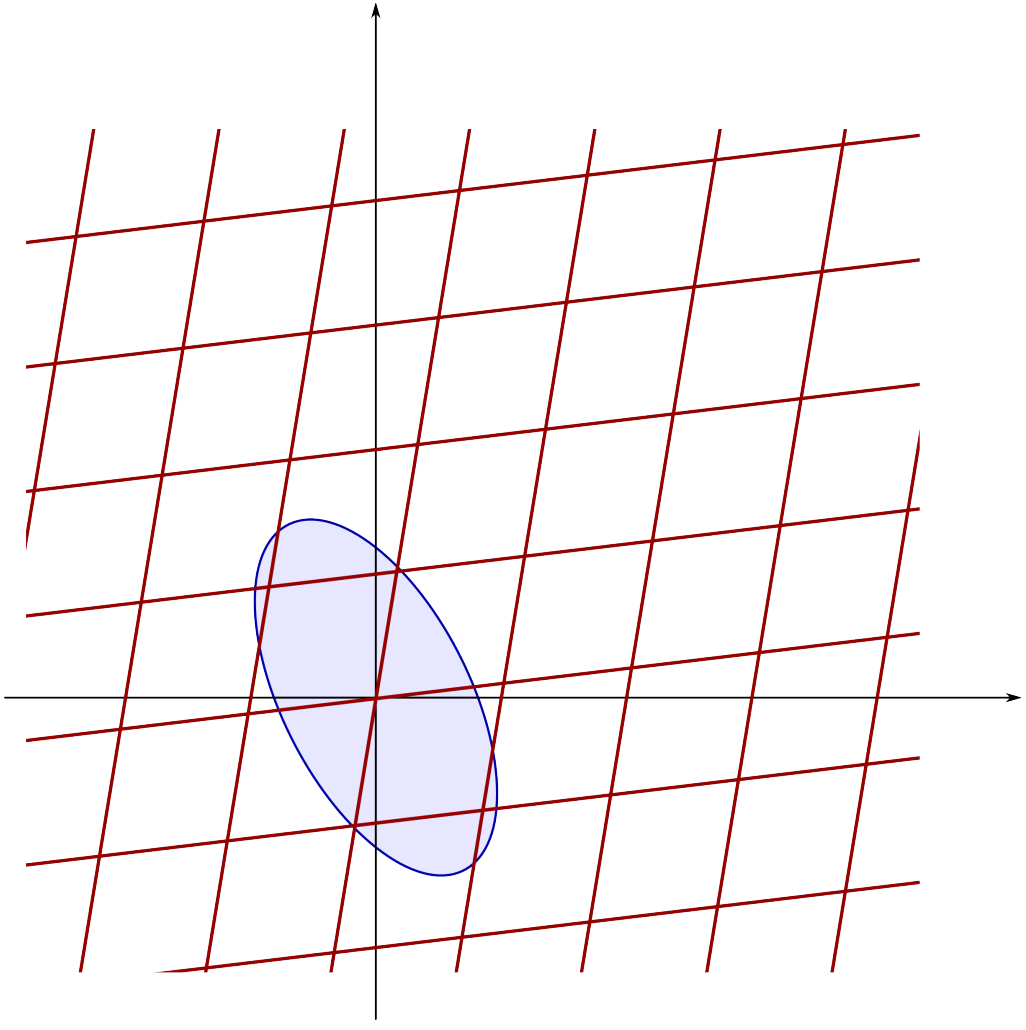
Ha K területe nagyobb, mint $4T$, akkor K tartalmaz az origón kívül még egy rácspontot.

Minkowski tételének bizonyítása



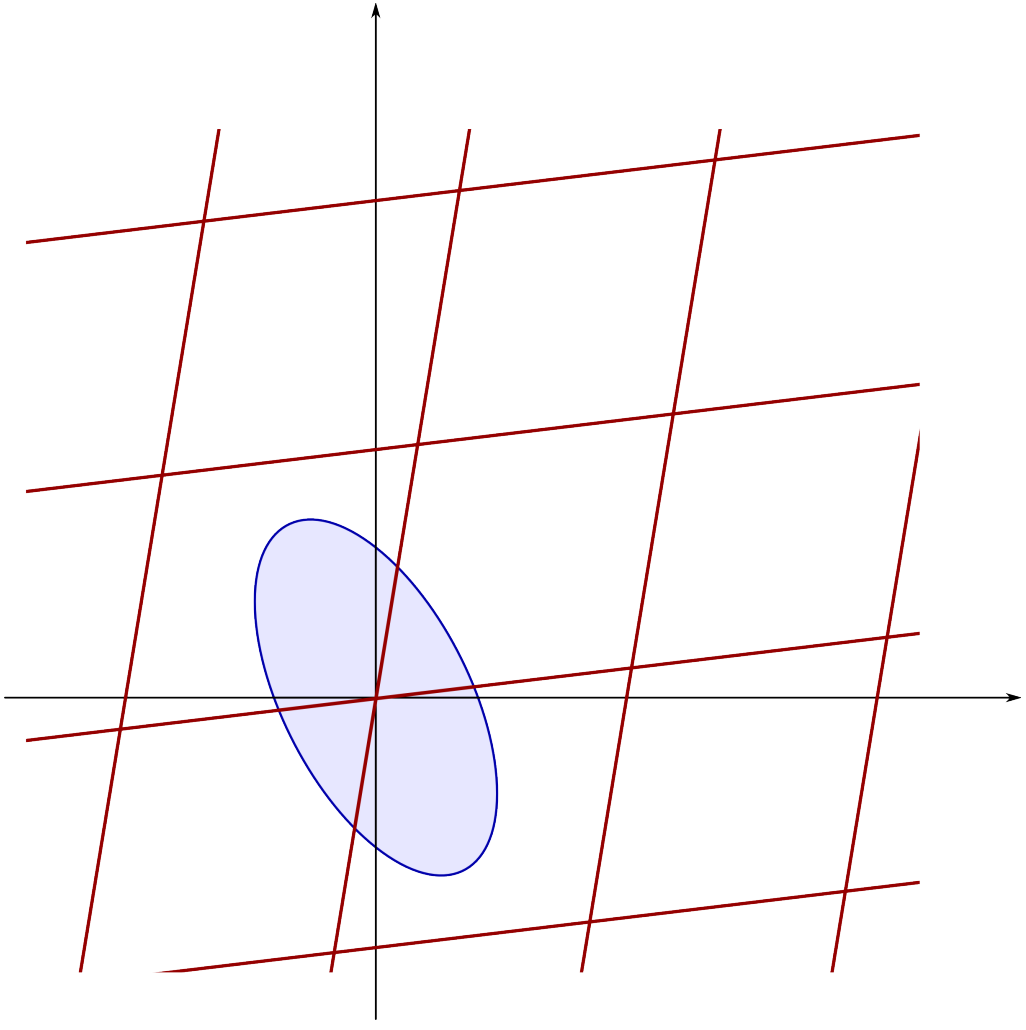
$$R = \{k\mathbf{a} + \ell\mathbf{b} \colon k, \ell \in \mathbb{Z}\}$$

Minkowski tételének bizonyítása



$$R = \{k\mathbf{a} + \ell\mathbf{b} \colon k, \ell \in \mathbb{Z}\}$$

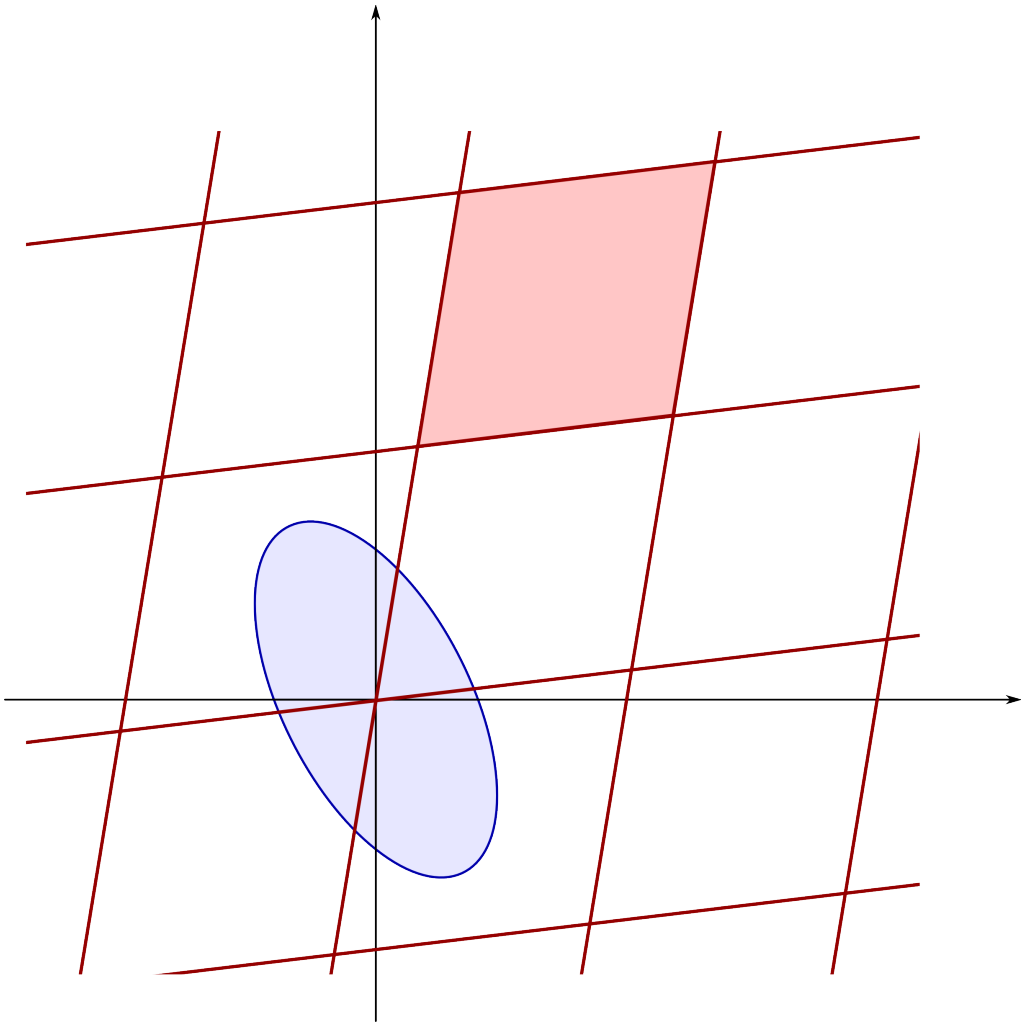
Minkowski tételének bizonyítása



$$R = \{k\mathbf{a} + \ell\mathbf{b} \colon k, \ell \in \mathbb{Z}\}$$

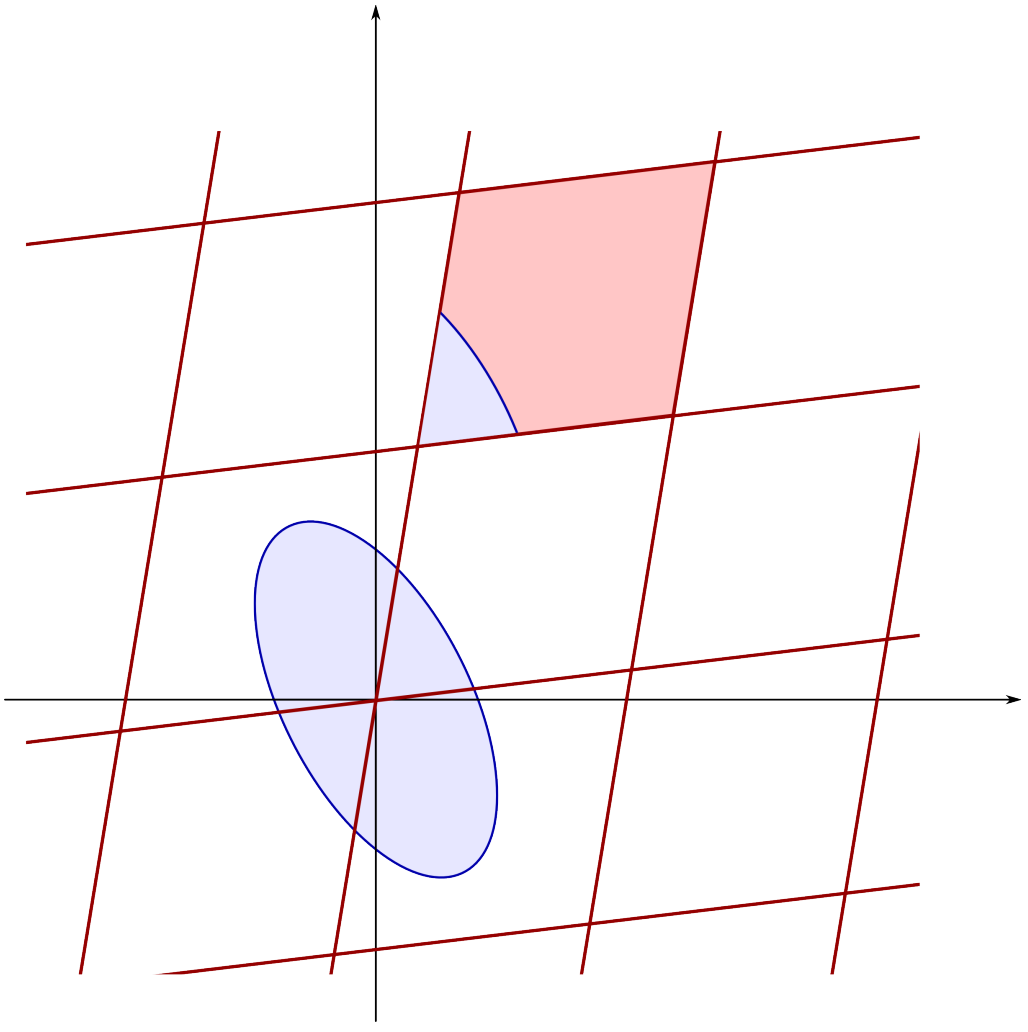
$$2R = \{2k\mathbf{a} + 2\ell\mathbf{b} \colon k, \ell \in \mathbb{Z}\}$$

Minkowski tételének bizonyítása



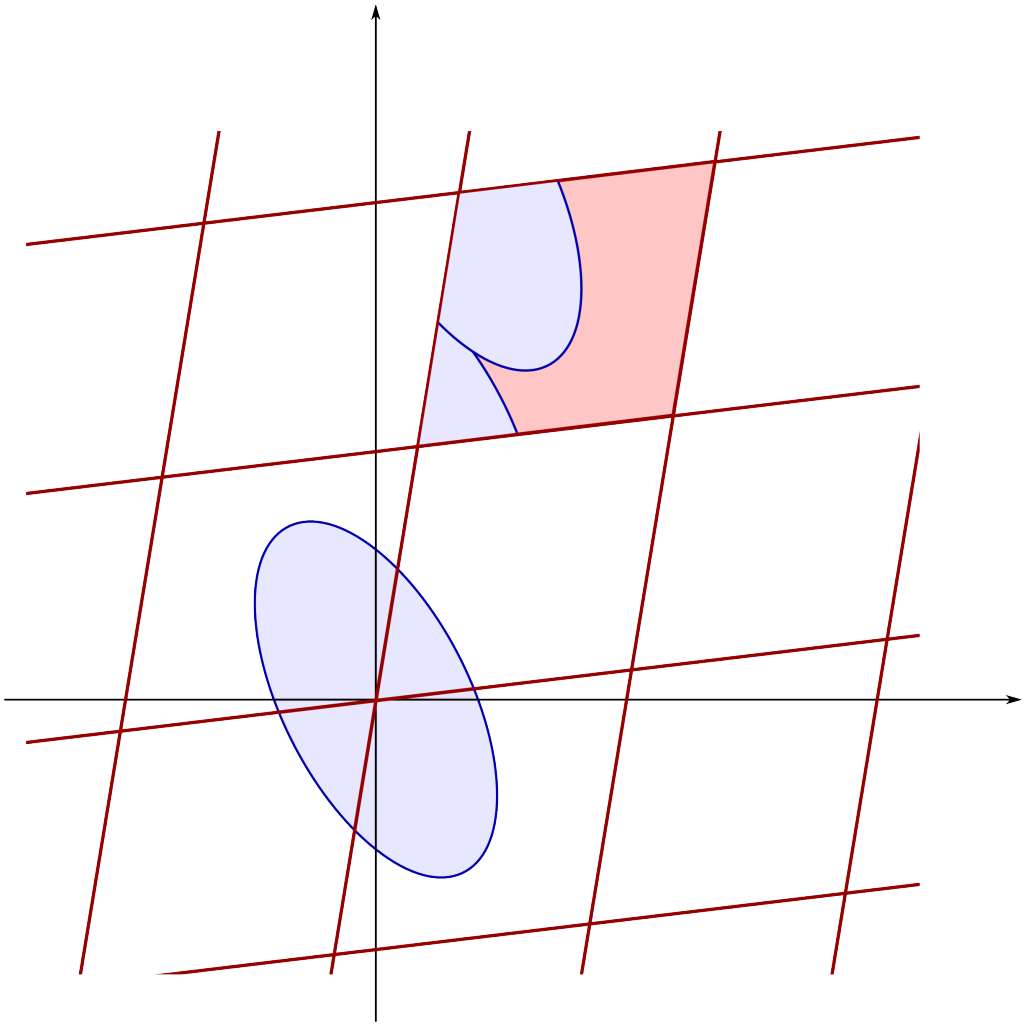
Jelöljünk ki egy paralelogrammát (területe $4T$)

Minkowski tételének bizonyítása



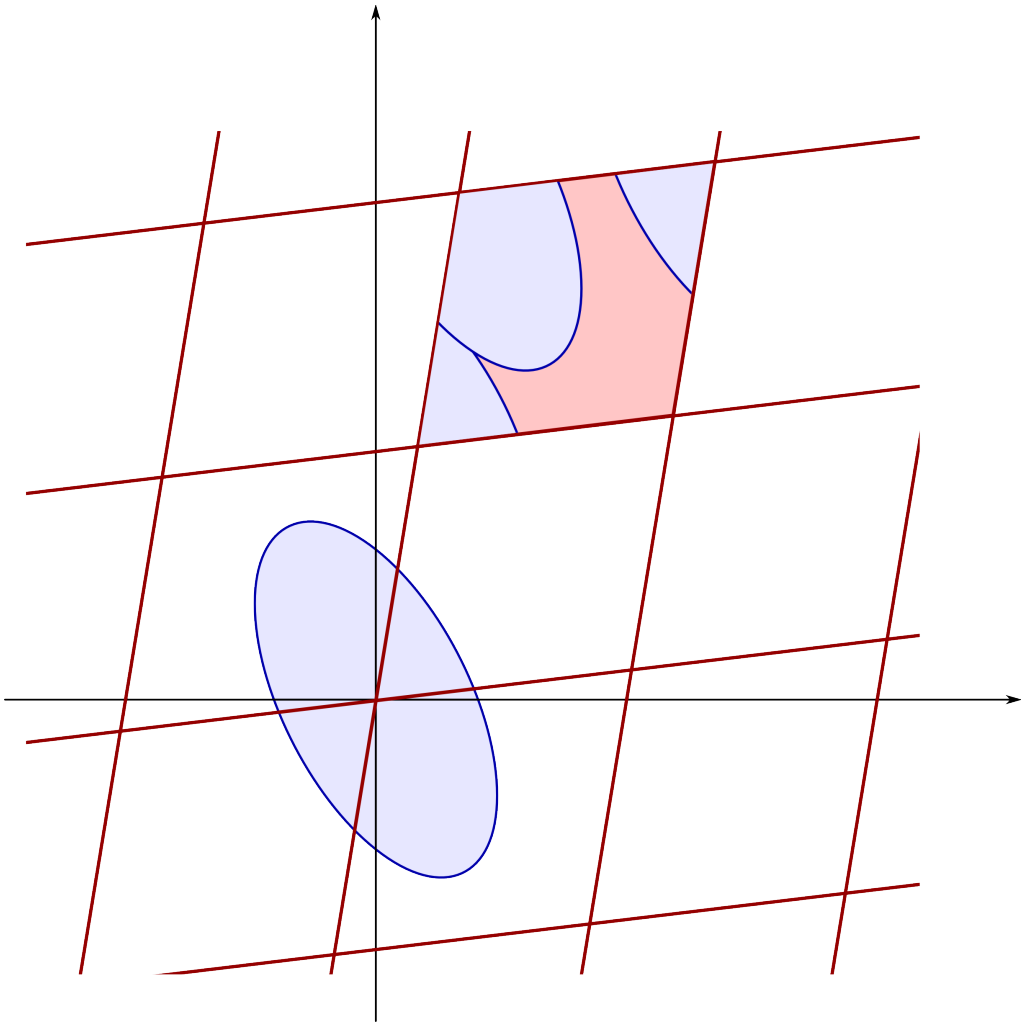
Jelöljünk ki egy paralelogrammát (területe $4T$), és toljuk ide mindazokat a paralelogrammákat, amelyekbe K belemetsz.

Minkowski tételének bizonyítása



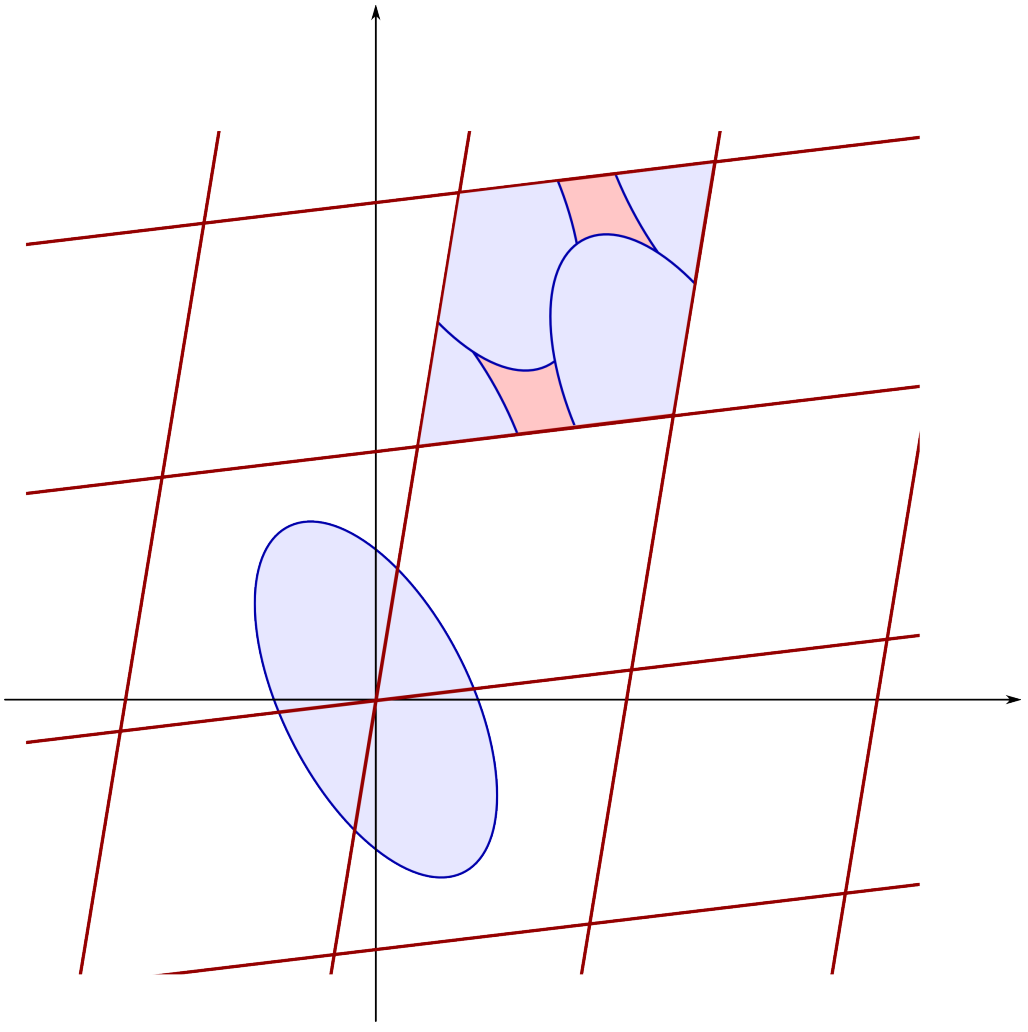
Jelöljünk ki egy paralelogrammát (területe $4T$), és toljuk ide mindazokat a paralelogrammákat, amelyekbe K belemetsz.

Minkowski tételének bizonyítása



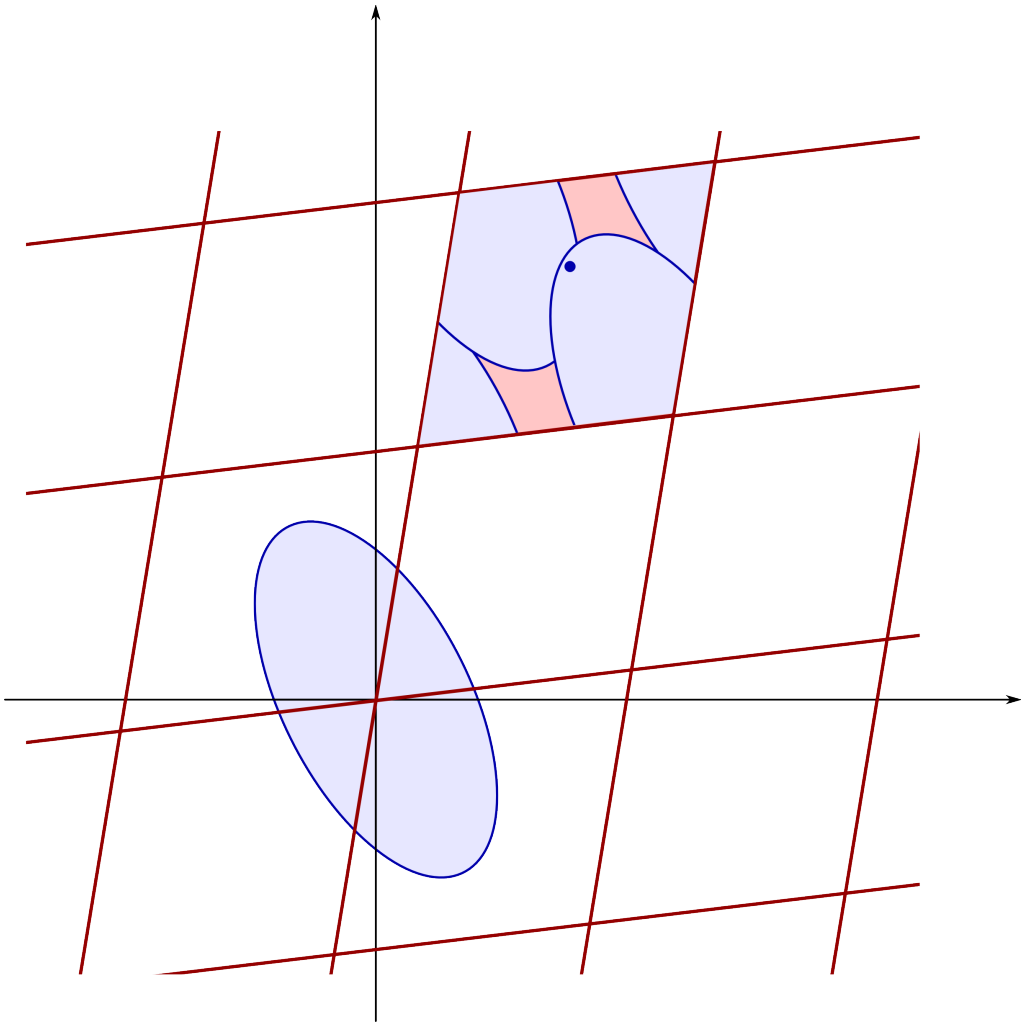
Jelöljünk ki egy paralelogrammát (területe $4T$), és toljuk ide mindazokat a paralelogrammákat, amelyekbe K belemetsz.

Minkowski tételének bizonyítása



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

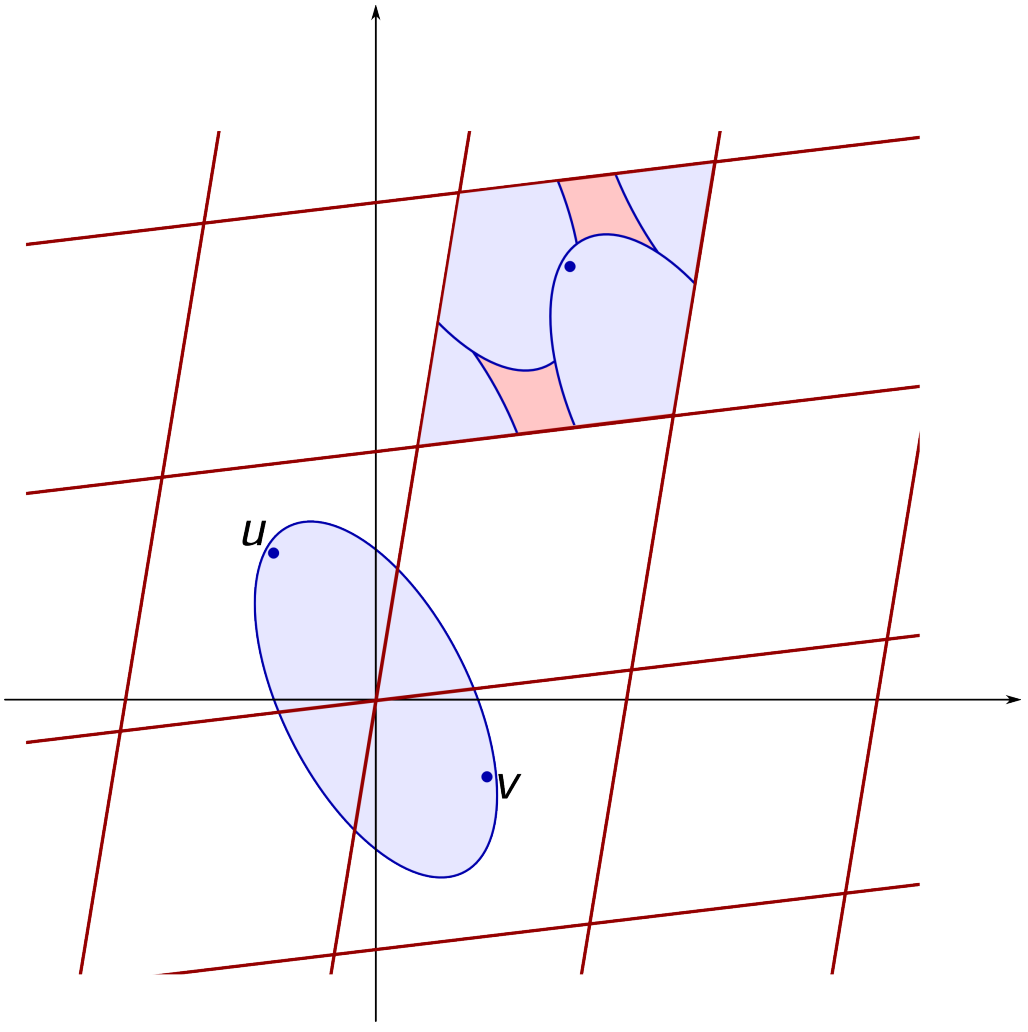
Minkowski tételének bizonyítása



Jelöljünk 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.

Minkowski tételének bizonyítása

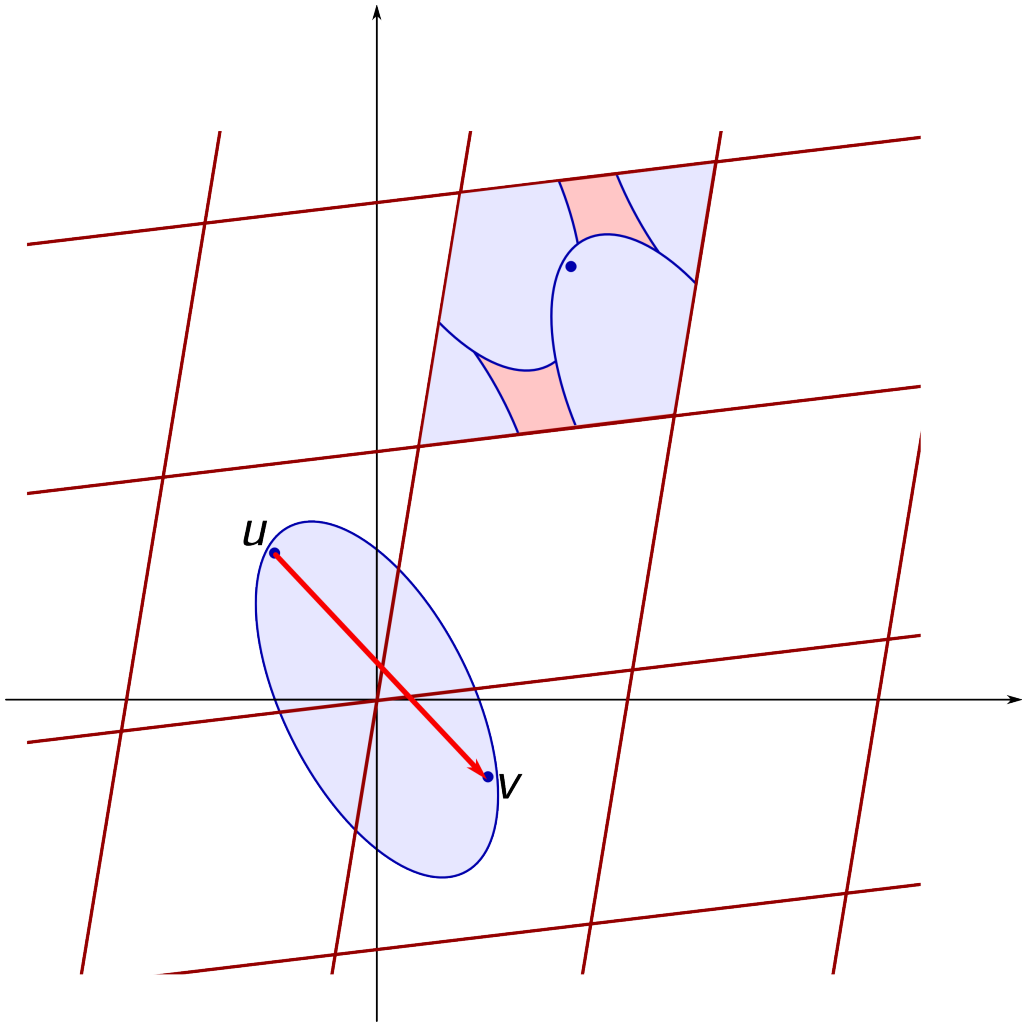


Jelöljünk ki egy paralelogrammát (területe $4T$), és toljuk ide mindazokat a paralelogrammákat, amelyekbe K belemetsz.

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

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

Minkowski tételének bizonyítása



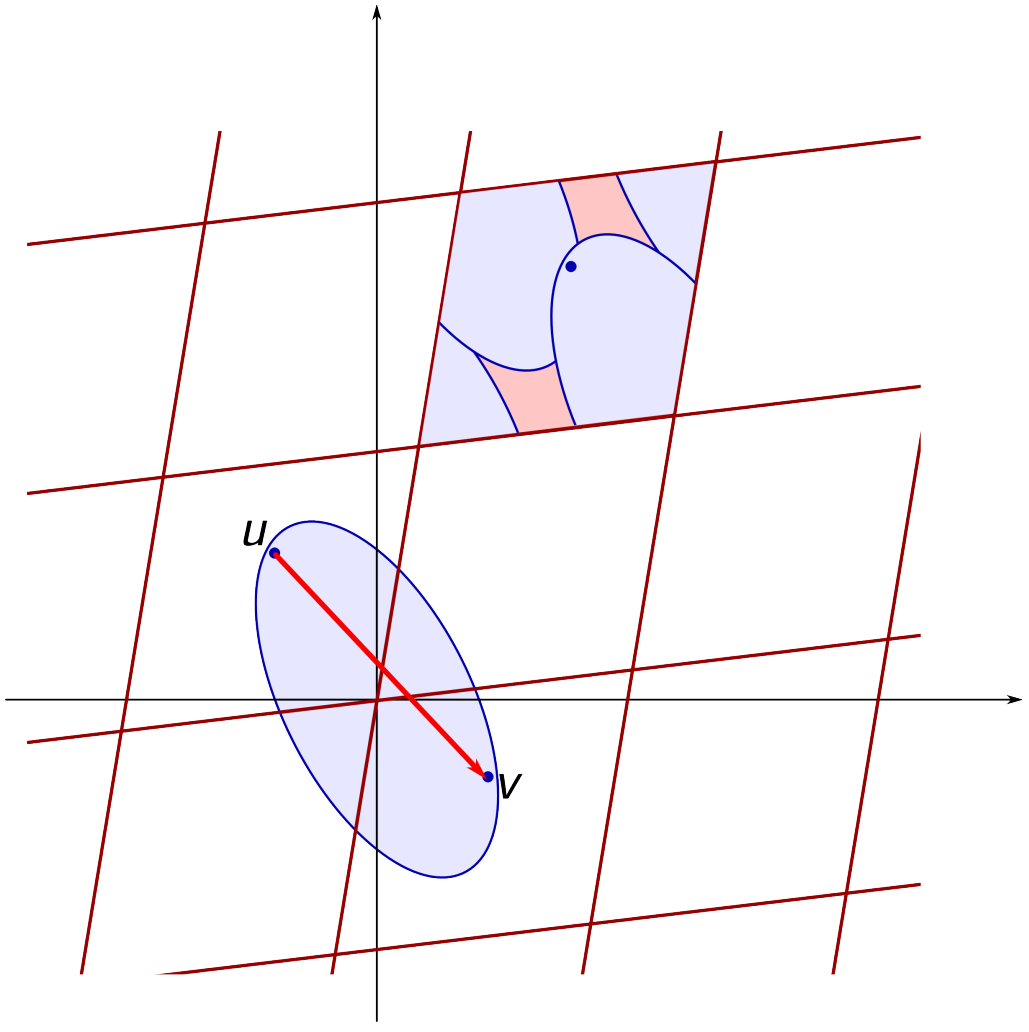
Jelöljünk ki egy paralelogrammát (területe $4T$), és toljuk ide mindazokat a paralelogrammákat, amelyekbe K belemetsz.

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

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

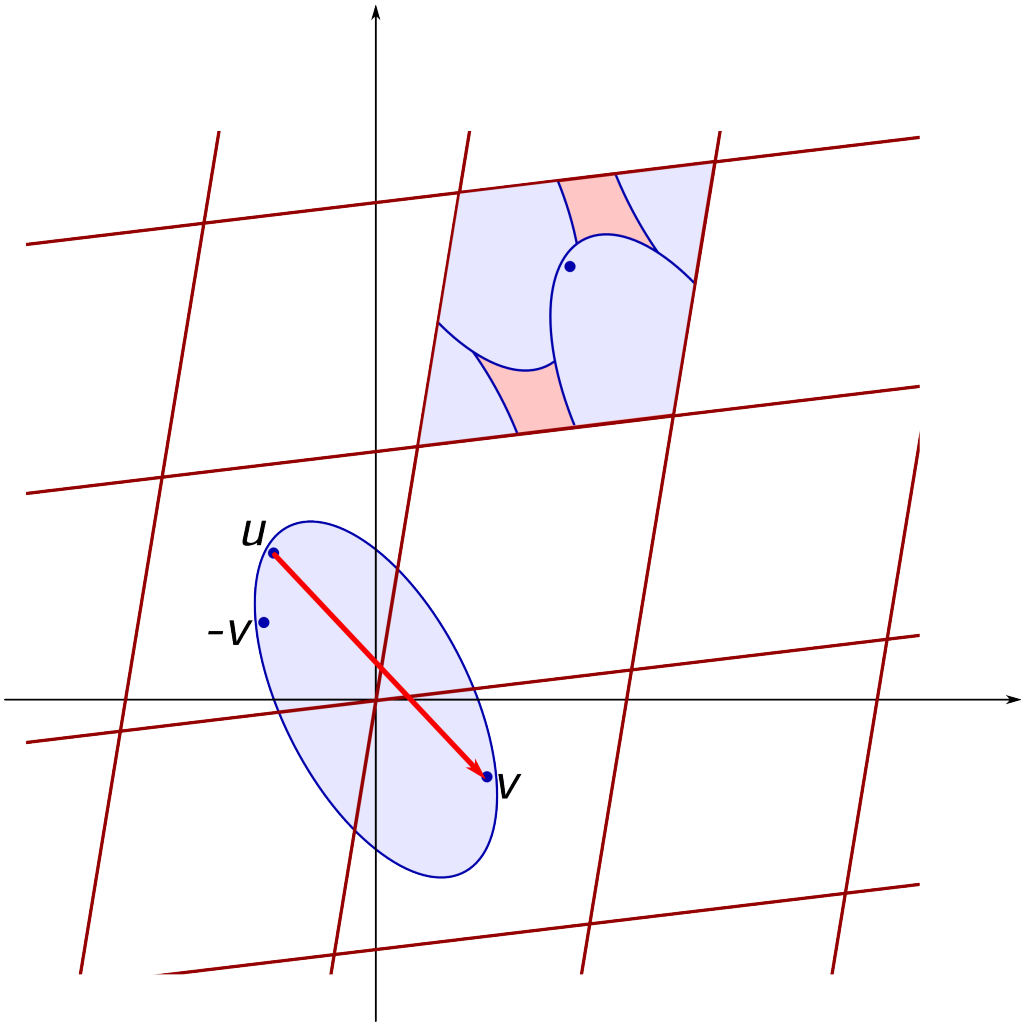
Ezek egymásból egy rácsvektorral való eltolással megkaphatók: $\mathbf{u} - \mathbf{v} \in 2R$.

Minkowski tételének bizonyítása



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

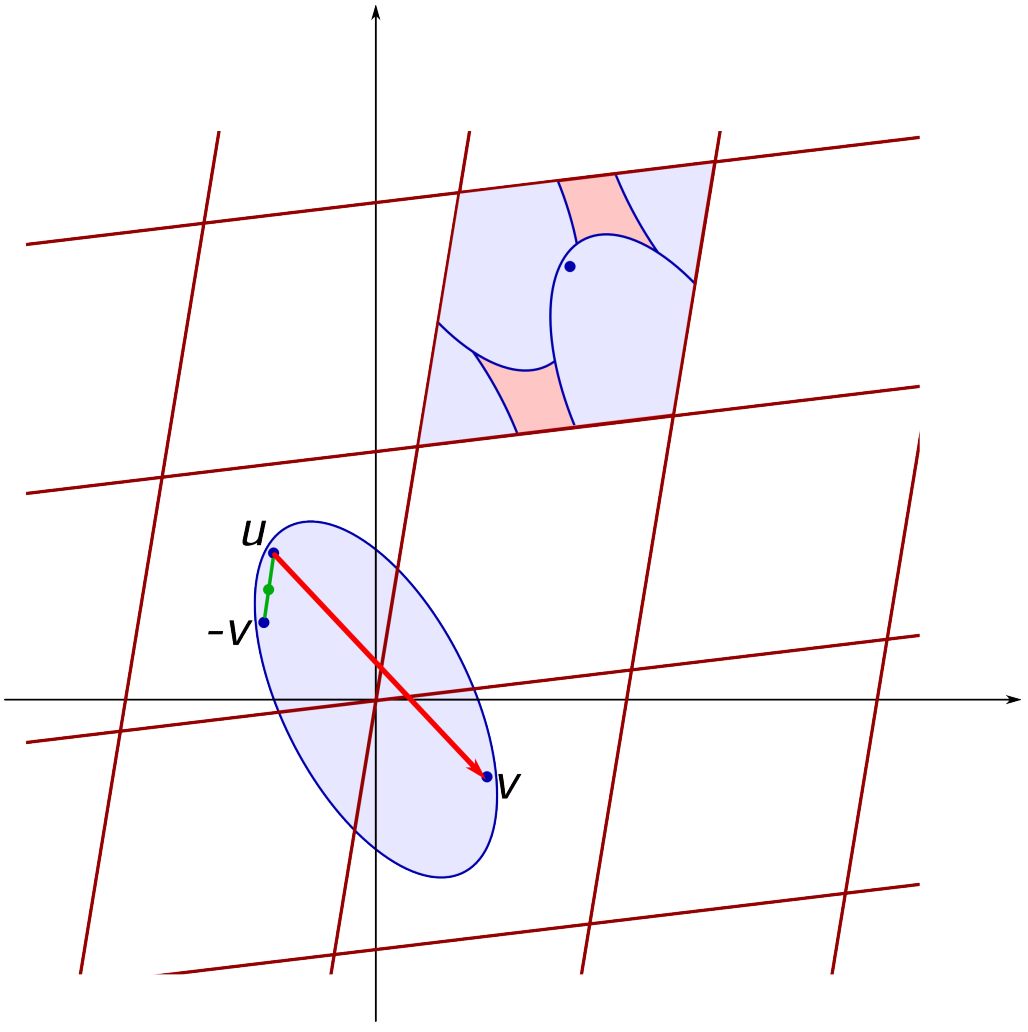
Minkowski tételének bizonyítása



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

K szimmetrikus $\Longrightarrow$ $-\mathbf{v} \in K$

Minkowski tételének bizonyítása

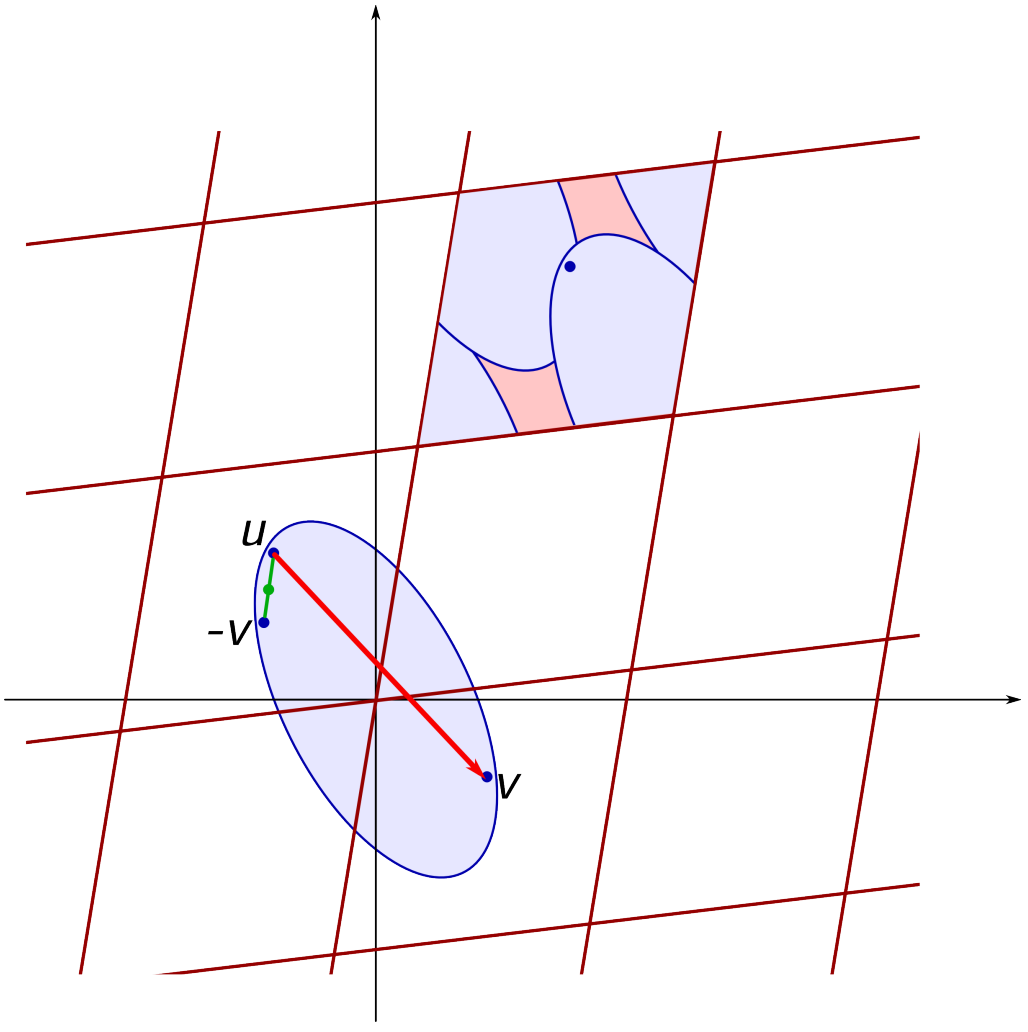


$\mathbf{u}, \mathbf{v} \in K, \quad \mathbf{u} - \mathbf{v} \in 2R$

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

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

Minkowski tételének bizonyítása



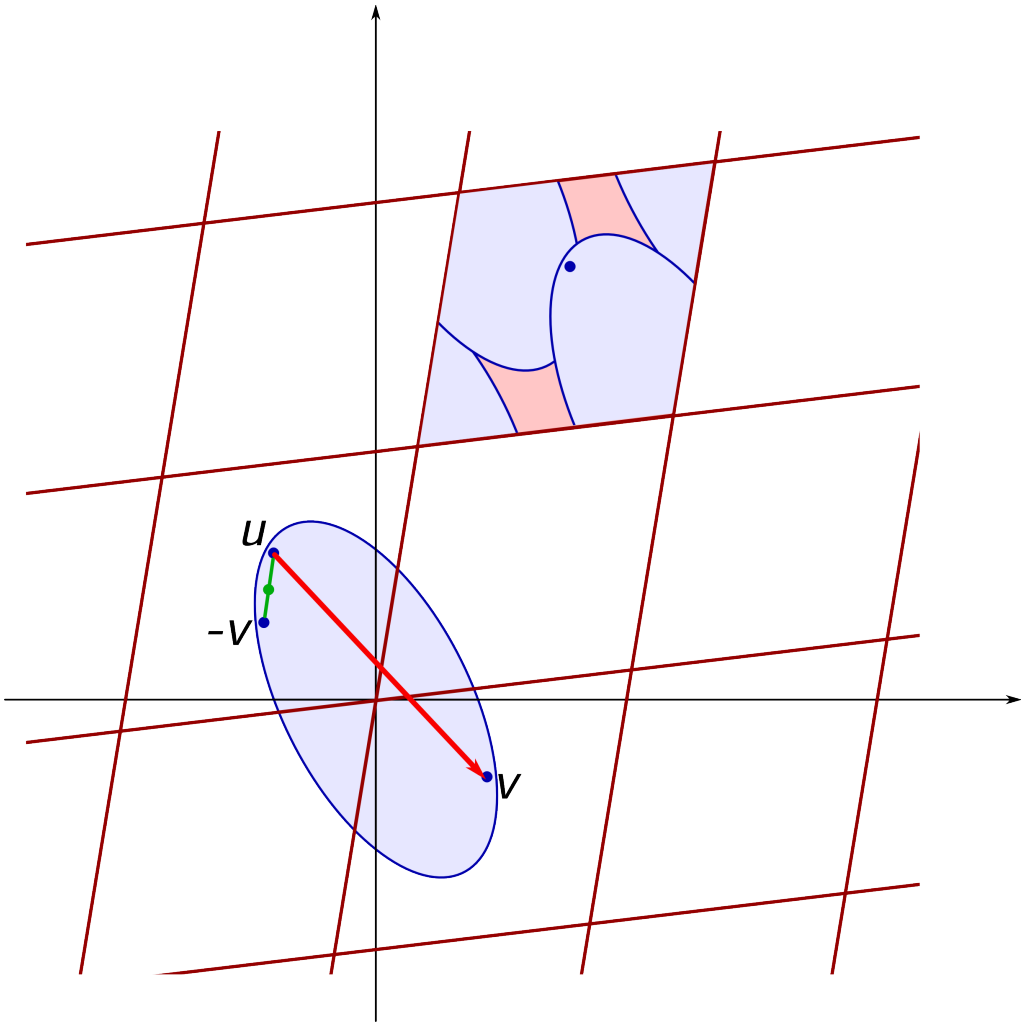
$\mathbf{u}, \mathbf{v} \in K, \quad \mathbf{u} - \mathbf{v} \in 2R$

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

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

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

Minkowski tételének bizonyítása



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

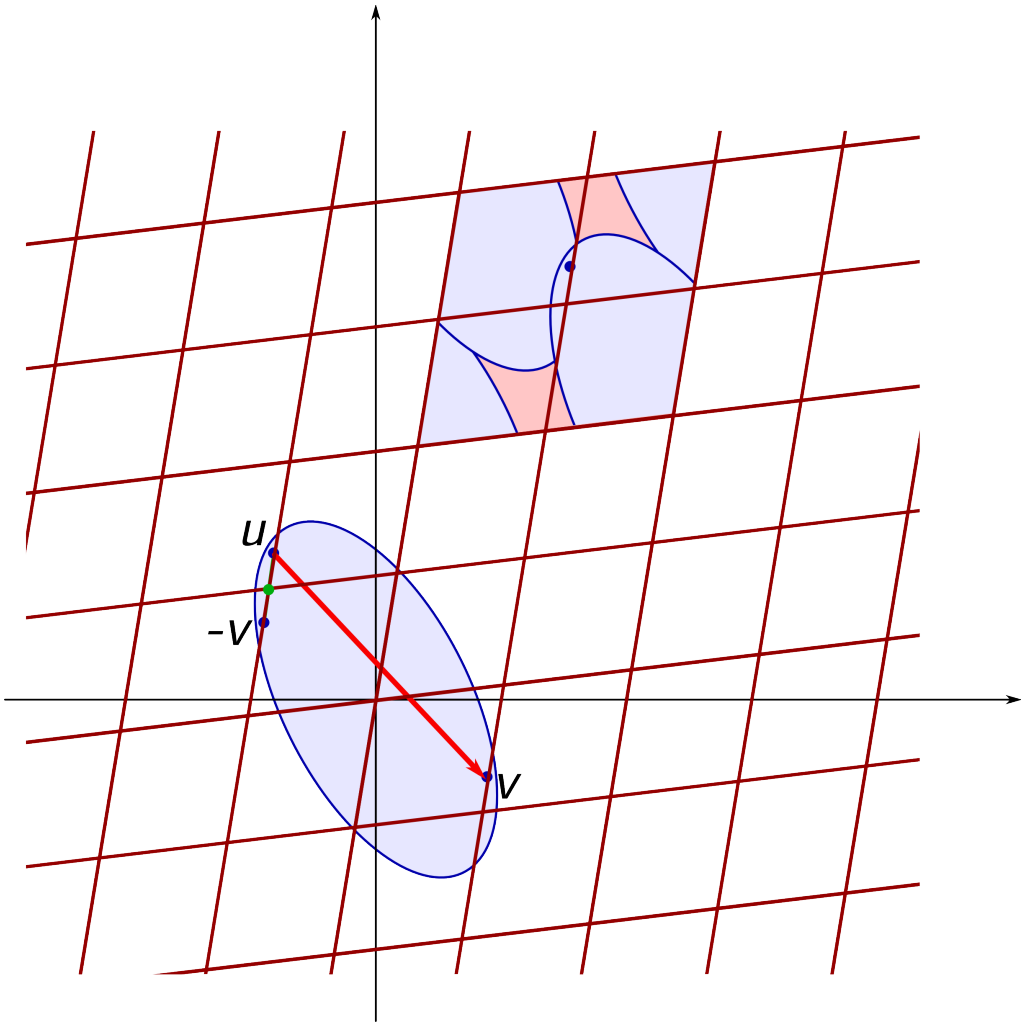
K szimmetrikus $\implies -\mathbf{v} \in K$

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

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

Tehát $\dfrac{\mathbf{u} - \mathbf{v}}{2} \in K \cap R.$ $\square$

Minkowski tételének bizonyítása



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

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

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

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

Tehát $\dfrac{\mathbf{u} - \mathbf{v}}{2} \in K \cap R.$ $\square$

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

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

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

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

A bizonyítás „lelke” az alábbi állítás.

Lemma

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

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

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

A bizonyítás „lelke” az alábbi állítás.

Lemma

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

Biz.

$p \equiv 1 \pmod 4$

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

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

A bizonyítás „lelke” az alábbi állítás.

Lemma

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

Biz.

$$p \equiv 1 \pmod 4 \implies \left(\frac{-1}{p}\right) = 1$$

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

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

A bizonyítás „lelke” az alábbi állítás.

Lemma

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

Biz.

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

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

Pontosan azok a természetes számok állnak elő két négyzetszám összegeként, amelyeknek prímhatványtényezős felbontásában a $4k+3$ alakú prímek 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:

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

Pontosan azok a természetes számok állnak elő két négyzetszám összegeként, amelyeknek prímhatványtényezős felbontásában a $4k+3$ alakú prímek 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: $p \mid c^2+1$.

Fermat-féle két négyzetszám tétel

Tétel (Fermat)

Pontosan azok a természetes számok állnak elő két négyzetszám összegeként, amelyeknek prímhatványtényezős felbontásában a $4k+3$ alakú prímek 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.

Első bizonyítás: Minkowski tételével

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

Első bizonyítás: Minkowski tételével

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

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.

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 $\mathbf{u} = k \cdot \mathbf{a} + \ell \cdot \mathbf{b}$

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 $\mathbf{u} = k \cdot \mathbf{a} + \ell \cdot \mathbf{b} = (k \cdot p + \ell \cdot c,\ k \cdot 0 + \ell \cdot 1) = (kp + \ell c,\ \ell)$

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

$$|\mathbf{u}|^2 = (kp + \ell c)^2 + \ell^2$$

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

$$|\mathbf{u}|^2 = (kp + \ell c)^2 + \ell^2 \equiv \ell^2 c^2 + \ell^2$$

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

$$|\mathbf{u}|^2 = (kp + \ell c)^2 + \ell^2 \equiv \ell^2 c^2 + \ell^2 = \ell^2 \left(c^2 + 1\right)$$

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

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

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

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

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

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

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

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

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

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

Ennek területe

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

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

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

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

Ennek területe $2p\pi > 4p$

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

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

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

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

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

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

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

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

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

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

$\mathbf{u} \in R$

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

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

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

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

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

$$\mathbf{u} \in R \implies p \mid u_1^2 + u_2^2$$

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

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

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

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

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

$$\mathbf{u} \in R \implies p \mid u_1^2 + u_2^2$$

$$\mathbf{0} \neq \mathbf{u} \in K$$

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

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

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

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

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

$$\begin{aligned} \mathbf{u} \in R &\implies p \mid u_1^2 + u_2^2 \\ \mathbf{0} \neq \mathbf{u} \in K &\implies 0 < u_1^2 + u_2^2 < 2p \end{aligned}$$

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

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

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

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

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

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

□

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) alakú számok (Gauss-egészek) körében is fel lehet építeni a számelméletet.

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) alakú számok (Gauss-egészek) körében is fel lehet építeni a számelméletet. Itt is ekvivalens egymással a felbonthatatlanság és a prímtulajdonság.

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = \left(2 + 3\sqrt{-1}\right)\left(2 - 3\sqrt{-1}\right) = 2^2 - \left(3\sqrt{-1}\right)^2 = 4 - (-9) = 13.$$

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = \left(2 + 3\sqrt{-1}\right)\left(2 - 3\sqrt{-1}\right) = 2^2 - \left(3\sqrt{-1}\right)^2 = 4 - (-9) = 13.$$

Legyen p egy $4k + 1$ alakú prímszám, ekkor $\exists c \in \mathbb{N} : p \mid c^2 + 1$.

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ $(a, b \in \mathbb{Z})$ 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = \left(2 + 3\sqrt{-1}\right)\left(2 - 3\sqrt{-1}\right) = 2^2 - \left(3\sqrt{-1}\right)^2 = 4 - (-9) = 13.$$

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

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

ami lehetetlen.

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ $(a, b \in \mathbb{Z})$ 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = \left(2 + 3\sqrt{-1}\right)\left(2 - 3\sqrt{-1}\right) = 2^2 - \left(3\sqrt{-1}\right)^2 = 4 - (-9) = 13.$$

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

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

ami lehetetlen. Tehát p nem prím, ezért nem is felbonthatatlan.

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ $(a, b \in \mathbb{Z})$ 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = \left(2 + 3\sqrt{-1}\right)\left(2 - 3\sqrt{-1}\right) = 2^2 - \left(3\sqrt{-1}\right)^2 = 4 - (-9) = 13.$$

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

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

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

$$p = \left(a + b\sqrt{-1}\right)\left(a - b\sqrt{-1}\right).$$

Második bizonyítás: Gauss-egészekkel (vázlat)

Az $a + b\sqrt{-1}$ ($a, b \in \mathbb{Z}$) 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 számkörben is felbonthatatlanok, de a 2 és a $4k + 1$ alakú prímek nem, pl.:

$$13 = \left(2 + 3\sqrt{-1}\right)\left(2 - 3\sqrt{-1}\right) = 2^2 - \left(3\sqrt{-1}\right)^2 = 4 - (-9) = 13.$$

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

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

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

$$p = \left(a + b\sqrt{-1}\right)\left(a - b\sqrt{-1}\right).$$

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

Harmadik 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. □

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 $(1,1,k)$.