Gaussova praštevila in magični kvadrat kvadratov

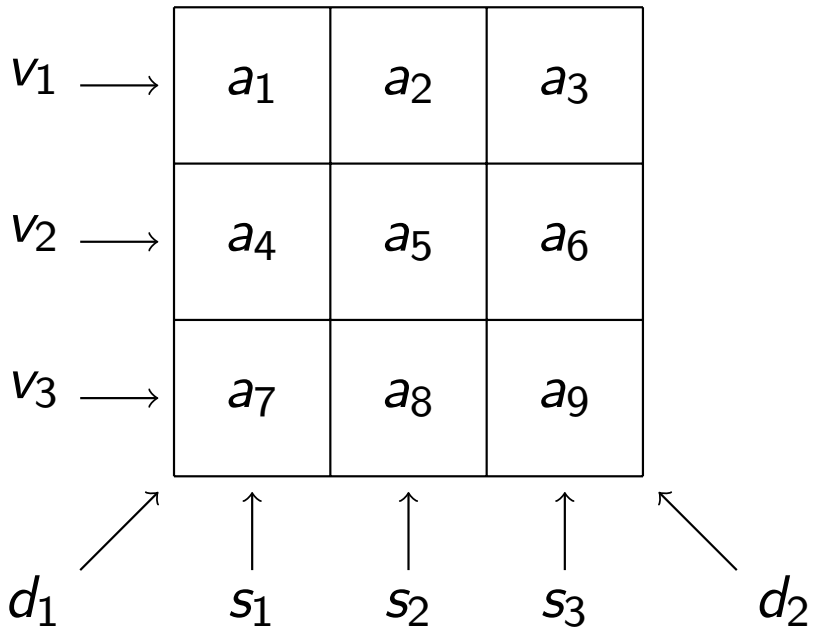
Aleš Vavpetič

7. junij 2021

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

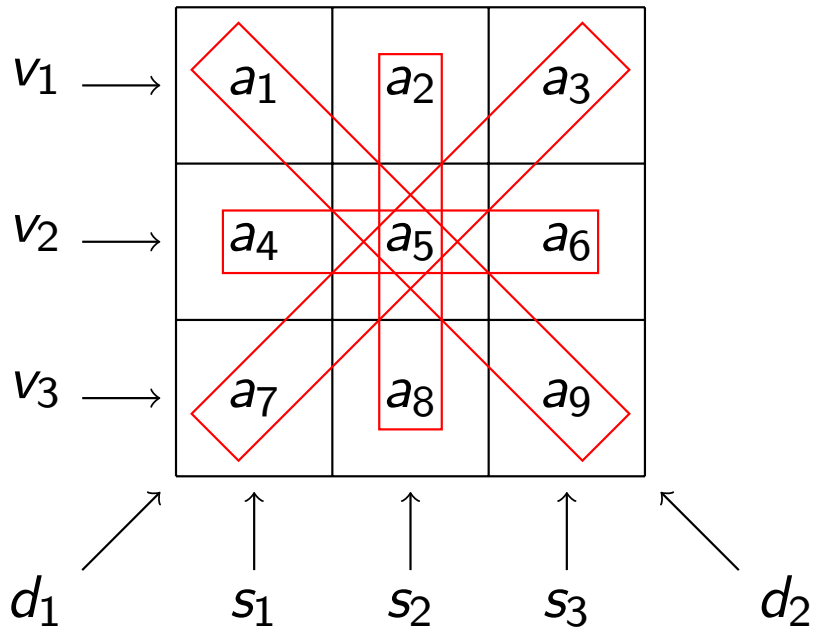
a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$



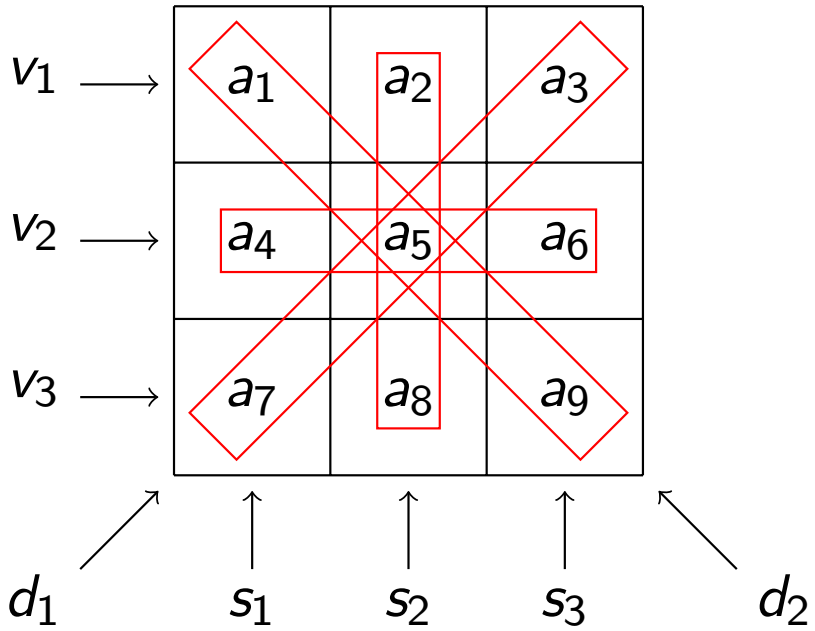
- Vsota S v vsaki vrtici, stolpcu in diagonali je $\frac{1}{3}(a_1 + \ldots + a_9) = 15$.

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$



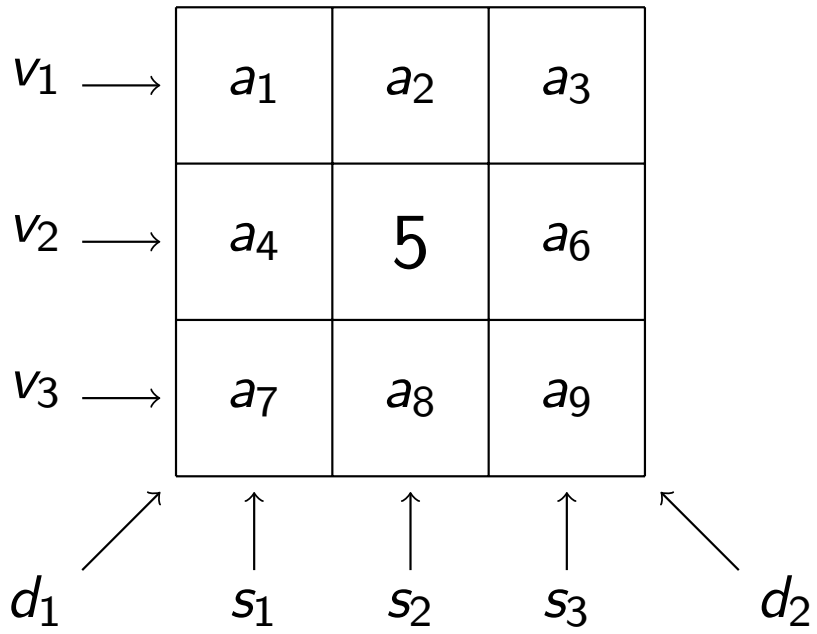
- Vsota S v vsaki vrtici, stolpcu in diagonali je $\frac{1}{3}(a_1 + \ldots + a_9) = 15$.
- $4S = v_2 + s_2 + d_1 + d_2$

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$



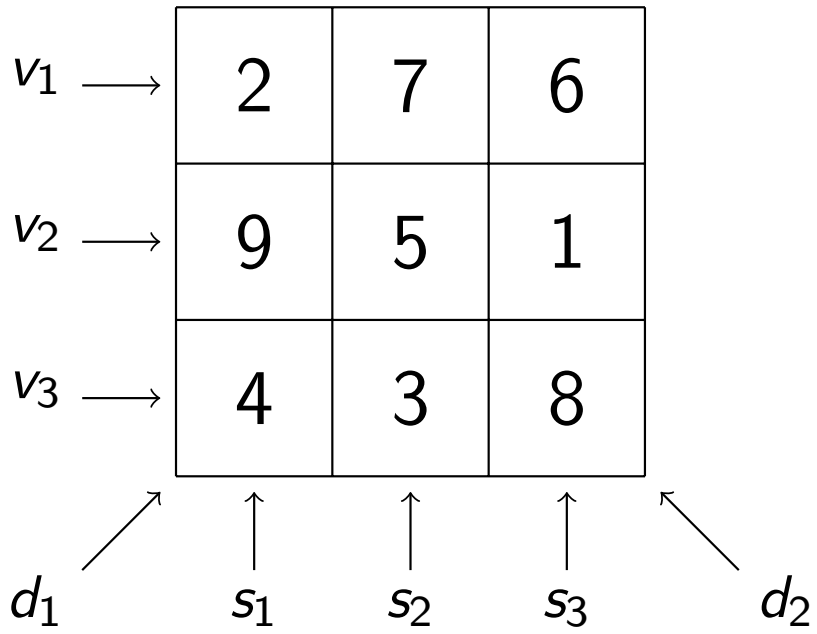
- Vsota S v vsaki vrtici, stolpcu in diagonali je $\frac{1}{3}(a_1 + \ldots + a_9) = 15$.
- $4S = v_2 + s_2 + d_1 + d_2 = 3S + 3a_5$

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$



- Vsota S v vsaki vrtici, stolpcu in diagonali je $\frac{1}{3}(a_1 + \ldots + a_9) = 15$.
- $4S = v_2 + s_2 + d_1 + d_2 = 3S + 3a_5 \Rightarrow a_5 = \frac{1}{3}S = 5$.

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$



- Vsota S v vsaki vrtici, stolpcu in diagonali je $\frac{1}{3}(a_1 + \ldots + a_9) = 15$.
- $4S = v_2 + s_2 + d_1 + d_2 = 3S + 3a_5 \Rightarrow a_5 = \frac{1}{3}S = 5$.
- Do simetrije kvadrata obstaja le en magični kvadrat.

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N}$$

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N}$$

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

Koliko je kvadratov z *magično vsoto* S?

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N}$$

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

Koliko je kvadratov z *magično vsoto* S?

- Za $S = 15$ je do simetrije le 1 (sicer 8).

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N}$$

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

Koliko je kvadratov z *magično vsoto* S?

- Za $S = 15$ je do simetrije le 1 (sicer 8).
- Za $S \not\equiv 0 \pmod 3$ ne obstaja.

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N}$$

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

Koliko je kvadratov z *magično vsoto* S?

- Za $S = 15$ je do simetrije le 1 (sicer 8).
- Za $S \not\equiv 0 \pmod 3$ ne obstaja.
- Za $S = 18$ so do simetrije le 3 (sicer 24).

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N}$$

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

Koliko je kvadratov z *magično vsoto* S?

- Za $S = 15$ je do simetrije le 1 (sicer 8).
- Za $S \not\equiv 0 \pmod 3$ ne obstaja.
- Za $S = 18$ so do simetrije le 3 (sicer 24).
- Za $S \equiv 0 \pmod{12}$ je do simetrije $\frac{S}{12}(4S - 3)$ kvadratov.

Ali obstaja magični kvadrat k-tih potenc za kak $k \in \mathbb{N}$:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N},$$

a_1^k	a_2^k	a_3^k
a_4^k	a_5^k	a_6^k
a_7^k	a_8^k	a_9^k

- Spomnimo se: $a_j^k + a_5^k + a_{10-j}^k = S = 3a_5^k \Rightarrow a_j^k + a_{10-j}^k = 2a_5^k$.

Ali obstaja magični kvadrat k-tih potenc za kak $k \in \mathbb{N}$:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N},$$

a_1^k	a_2^k	a_3^k
a_4^k	a_5^k	a_6^k
a_7^k	a_8^k	a_9^k

- Spomnimo se: $a_j^k + a_5^k + a_{10-j}^k = S = 3a_5^k \Rightarrow a_j^k + a_{10-j}^k = 2a_5^k$.
- Euler: Diofantska enačba $x^3 + y^3 = 2z^3$ nima rešitve v množici $\mathbb{N}$.

Ali obstaja magični kvadrat k-tih potenc za kak $k \in \mathbb{N}$:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N},$$

a_1^k	a_2^k	a_3^k
a_4^k	a_5^k	a_6^k
a_7^k	a_8^k	a_9^k

- Spomnimo se: $a_j^k + a_5^k + a_{10-j}^k = S = 3a_5^k \Rightarrow a_j^k + a_{10-j}^k = 2a_5^k$.
- Euler: Diofantska enačba $x^3 + y^3 = 2z^3$ nima rešitve v množici $\mathbb{N}$.
- Legendre: Diofantska enačba $x^4 + y^4 = 2z^4$ nima rešitve v množici $\mathbb{N}$.

Ali obstaja magični kvadrat k-tih potenc za kak $k \in \mathbb{N}$:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N},$$

a_1^k	a_2^k	a_3^k
a_4^k	a_5^k	a_6^k
a_7^k	a_8^k	a_9^k

- Spomnimo se: $a_j^k + a_5^k + a_{10-j}^k = S = 3a_5^k \Rightarrow a_j^k + a_{10-j}^k = 2a_5^k$.
- Euler: Diofantska enačba $x^3 + y^3 = 2z^3$ nima rešitve v množici $\mathbb{N}$.
- Legendre: Diofantska enačba $x^4 + y^4 = 2z^4$ nima rešitve v množici $\mathbb{N}$.
- Noam Elkies: Za vsak $n \geq 3$ diofantska enačba $x^n + y^n = 2z^n$ nima rešitve v množici $\mathbb{N}$.

Ali obstaja magični kvadrat k-tih potenc za kak $k \in \mathbb{N}$:

$$\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9\} \subset \mathbb{N},$$

a_1^k	a_2^k	a_3^k
a_4^k	a_5^k	a_6^k
a_7^k	a_8^k	a_9^k

- Spomnimo se: $a_j^k + a_5^k + a_{10-j}^k = S = 3a_5^k \Rightarrow a_j^k + a_{10-j}^k = 2a_5^k$.
- Euler: Diofantska enačba $x^3 + y^3 = 2z^3$ nima rešitve v množici $\mathbb{N}$.
- Legendre: Diofantska enačba $x^4 + y^4 = 2z^4$ nima rešitve v množici $\mathbb{N}$.
- Noam Elkies: Za vsak $n \geq 3$ diofantska enačba $x^n + y^n = 2z^n$ nima rešitve v množici $\mathbb{N}$.
- Ali obstaja magični kvadrat kvadratov?

Če je $\begin{array}{|c|c|c|}\hline a_1^2 & a_2^2 & a_3^2 \\ \hline a_4^2 & a_5^2 & a_6^2 \\ \hline a_7^2 & a_8^2 & a_9^2 \\ \hline \end{array}$ magični kvadrat kvadratov, je tak tudi $\begin{array}{|c|c|c|}\hline d^2a_1^2 & d^2a_2^2 & d^2a_3^2 \\ \hline d^2a_4^2 & d^2a_5^2 & d^2a_6^2 \\ \hline d^2a_7^2 & d^2a_8^2 & d^2a_9^2 \\ \hline \end{array}$.

Če je $\begin{array}{|c|c|c|}\hline a_1^2 & a_2^2 & a_3^2 \\ \hline a_4^2 & a_5^2 & a_6^2 \\ \hline a_7^2 & a_8^2 & a_9^2 \\ \hline \end{array}$ magični kvadrat kvadratov, je tak tudi $\begin{array}{|c|c|c|}\hline d^2a_1^2 & d^2a_2^2 & d^2a_3^2 \\ \hline d^2a_4^2 & d^2a_5^2 & d^2a_6^2 \\ \hline d^2a_7^2 & d^2a_8^2 & d^2a_9^2 \\ \hline \end{array}$.

Če je $\begin{array}{|c|c|c|}\hline a_1^2 & a_2^2 & a_3^2 \\ \hline a_4^2 & a_5^2 & a_6^2 \\ \hline a_7^2 & a_8^2 & a_9^2 \\ \hline \end{array}$ magični kvadrat kvadratov, je tak tudi $\begin{array}{|c|c|c|}\hline \frac{a_1^2}{d^2} & \frac{a_2^2}{d^2} & \frac{a_3^2}{d^2} \\ \hline \frac{a_4^2}{d^2} & \frac{a_5^2}{d^2} & \frac{a_6^2}{d^2} \\ \hline \frac{a_7^2}{d^2} & \frac{a_8^2}{d^2} & \frac{a_9^2}{d^2} \\ \hline \end{array}$, kjer je d (največji) skupni delitelj števil $a_1, \ldots, a_9$.

Če je $\begin{array}{|c|c|c|}\hline a_1^2 & a_2^2 & a_3^2 \\ \hline a_4^2 & a_5^2 & a_6^2 \\ \hline a_7^2 & a_8^2 & a_9^2 \\ \hline \end{array}$ magični kvadrat kvadratov, je tak tudi $\begin{array}{|c|c|c|}\hline d^2a_1^2 & d^2a_2^2 & d^2a_3^2 \\ \hline d^2a_4^2 & d^2a_5^2 & d^2a_6^2 \\ \hline d^2a_7^2 & d^2a_8^2 & d^2a_9^2 \\ \hline \end{array}$.

Če je $\begin{array}{|c|c|c|}\hline a_1^2 & a_2^2 & a_3^2 \\ \hline a_4^2 & a_5^2 & a_6^2 \\ \hline a_7^2 & a_8^2 & a_9^2 \\ \hline \end{array}$ magični kvadrat kvadratov, je tak tudi $\begin{array}{|c|c|c|}\hline \frac{a_1^2}{d^2} & \frac{a_2^2}{d^2} & \frac{a_3^2}{d^2} \\ \hline \frac{a_4^2}{d^2} & \frac{a_5^2}{d^2} & \frac{a_6^2}{d^2} \\ \hline \frac{a_7^2}{d^2} & \frac{a_8^2}{d^2} & \frac{a_9^2}{d^2} \\ \hline \end{array}$, kjer je d (največji) skupni delitelj števil $a_1, \ldots, a_9$.

Definicija

Magični kvadrat kvadratov je *primitiven*, če je največji skupni delitelj števil $a_1, \ldots, a_9$ enak 1.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2$$

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2$$

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'}).$$

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'}).$$

- Če $3 \mid a_5$, potem $3 \mid a_j + ia_{j'}$ ali $3 \mid a_j - ia_{j'}$.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'}).$$

- Če $3 \mid a_5$, potem $3 \mid a_j + ia_{j'}$ ali $3 \mid a_j - ia_{j'}$.
- Če $3 \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = 3x$

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'}).$$

- Če $3 \mid a_5$, potem $3 \mid a_j + ia_{j'}$ ali $3 \mid a_j - ia_{j'}$.
- Če $3 \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = 3x$ in zato $a_j - ia_{j'} = 3\bar{x}$.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'}).$$

- Če $3 \mid a_5$, potem $3 \mid a_j + ia_{j'}$ ali $3 \mid a_j - ia_{j'}$.
- Če $3 \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = 3x$ in zato $a_j - ia_{j'} = 3\bar{x}$.
- Torej je $2a_j = 3(x + \bar{x})$ in $2ia_{j'} = 3(x - \bar{x})$.

Trditev

V primitivnem magičnem kvadratu kvadratov so vsa števila liha.

Za vsak j je vsota $a_j^2 + a_{j'}^2 = 2a_5^2$ sodo število.

- Če je a_5 sodo, $8 \mid 2a_5^2$, torej $2 \mid a_j$ in $2 \mid a_{j'}$.
- Če je a_j sodo, je tudi $a_{j'}$ sodo, zato $4 \mid a_j^2 + a_{j'}^2$, sledi $2 \mid a_5$.

Trditev

V primitivnem magičnem kvadratu kvadratov število a_5 ni deljivo s 3.

Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'}).$$

- Če $3 \mid a_5$, potem $3 \mid a_j + ia_{j'}$ ali $3 \mid a_j - ia_{j'}$.
- Če $3 \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = 3x$ in zato $a_j - ia_{j'} = 3\bar{x}$.
- Torej je $2a_j = 3(x + \bar{x})$ in $2ia_{j'} = 3(x - \bar{x})$.
- Zato $3 \mid a_j$ in $3 \mid a_{j'}$.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

in $n^2 + m^2 = 1$ le za $(n, m) = (\pm 1, 0), (0, \pm 1)$.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

in $n^2 + m^2 = 1$ le za $(n, m) = (\pm 1, 0), (0, \pm 1)$.
V kolobarju $\mathbb{Z}[\mathrm{i}]$ so obrnljivi le elementi ± 1 in $\pm \mathrm{i}$.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

in $n^2 + m^2 = 1$ le za $(n, m) = (\pm 1, 0), (0, \pm 1)$.
V kolobarju $\mathbb{Z}[\mathrm{i}]$ so obrnljivi le elementi ± 1 in $\pm\mathrm{i}$.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *Gaussovo praštevilo*, če iz $p = z \cdot w$ $(z, w \in \mathbb{Z}[\mathrm{i}])$, sledi, da je natanko eno izmed števil z in w obrnljivo.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

in $n^2 + m^2 = 1$ le za $(n, m) = (\pm 1, 0), (0, \pm 1)$.
V kolobarju $\mathbb{Z}[\mathrm{i}]$ so obrnljivi le elementi ± 1 in $\pm\mathrm{i}$.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *Gaussovo praštevilo*, če iz $p = z \cdot w$ $(z, w \in \mathbb{Z}[\mathrm{i}])$, sledi, da je natanko eno izmed števil z in w obrnljivo.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *Gaussovo praštevilo*, če za poljubni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ za kateri velja, da če $p \mid z \cdot w$, potem $p \mid z$ ali $p \mid w$

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

in $n^2 + m^2 = 1$ le za $(n, m) = (\pm 1, 0), (0, \pm 1)$.
V kolobarju $\mathbb{Z}[\mathrm{i}]$ so obrnljivi le elementi ± 1 in $\pm\mathrm{i}$.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *Gaussovo praštevilo*, če iz $p = z \cdot w$ $(z, w \in \mathbb{Z}[\mathrm{i}])$, sledi, da je natanko eno izmed števil z in w obrnljivo.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *Gaussovo praštevilo*, če za poljubni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ za kateri velja, da če $p \mid z \cdot w$, potem $p \mid z$ ali $p \mid w$ in p ni obrnljiv element.

$\mathbb{Z}[\mathrm{i}] = \{(n + m\mathrm{i}) \in \mathbb{C}; n, m \in \mathbb{Z}\}$ je množica *Gaussovih celih števil*.
$\mathbb{Z}[\mathrm{i}]$ je (komutativen) kolobar z operacijama $+$ in $\cdot$.
Kateri elementi kolobarja $\mathbb{Z}[\mathrm{i}]$ so obrnljivi?
Velja

$$1 = \frac{(n + m\mathrm{i})(n - m\mathrm{i})}{n^2 + m^2} = (n + m\mathrm{i})\frac{(n - m\mathrm{i})}{n^2 + m^2}$$

in $n^2 + m^2 = 1$ le za $(n, m) = (\pm 1, 0), (0, \pm 1)$.
V kolobarju $\mathbb{Z}[\mathrm{i}]$ so obrnljivi le elementi ± 1 in $\pm\mathrm{i}$.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *nerazcepno število*, če iz $p = z \cdot w$ $(z, w \in \mathbb{Z}[\mathrm{i}])$, sledi, da je natanko eno izmed števil z in w obrnljivo.

Definicija

$p \in \mathbb{Z}[\mathrm{i}]$ je *Gaussovo praštevilo*, če za poljubni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ za kateri velja, da če $p \mid z \cdot w$, potem $p \mid z$ ali $p \mid w$ in p ni obrnljiv element.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n + m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n + m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.
- $N(z \cdot w) = N(z) \cdot N(w)$.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.
- $N(z \cdot w) = N(z) \cdot N(w)$.
  Velja $N(z) = z \cdot \bar{z}$

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.
- $N(z \cdot w) = N(z) \cdot N(w)$.
  Velja $N(z) = z \cdot \bar{z}$ in zato $N(z \cdot w) = z \cdot w \cdot \overline{z \cdot w} = N(z) \cdot N(w)$.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.
- $N(z \cdot w) = N(z) \cdot N(w)$.
  Velja $N(z) = z \cdot \bar{z}$ in zato $N(z \cdot w) = z \cdot w \cdot \overline{z \cdot w} = N(z) \cdot N(w)$.
- Če $z|w$, je $N(z) \leq N(w)$.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.
- $N(z \cdot w) = N(z) \cdot N(w)$.
  Velja $N(z) = z \cdot \bar{z}$ in zato $N(z \cdot w) = z \cdot w \cdot \overline{z \cdot w} = N(z) \cdot N(w)$.
- Če $z|w$, je $N(z) \leq N(w)$.
  Če je z pravi delitelj števila w, je $N(z) < N(w)$.

Definicija

Funkcijo $N\colon \mathbb{Z}[\mathrm{i}] \to \mathbb{N}_0$ podano s predpisom $N(n+m\mathrm{i}) = n^2 + m^2$ imenujemo *norma*.

Za normo velja:

- $N(z) = 0$ natanko tedaj, ko je $z = 0$.
- $N(z) = 1$ natanko tedaj, ko je z obrnljiv element.
- $N(z \cdot w) = N(z) \cdot N(w)$.
  Velja $N(z) = z \cdot \bar{z}$ in zato $N(z \cdot w) = z \cdot w \cdot \overline{z \cdot w} = N(z) \cdot N(w)$.
- Če $z|w$, je $N(z) \leq N(w)$.
  Če je z pravi delitelj števila w, je $N(z) < N(w)$.

Definicija

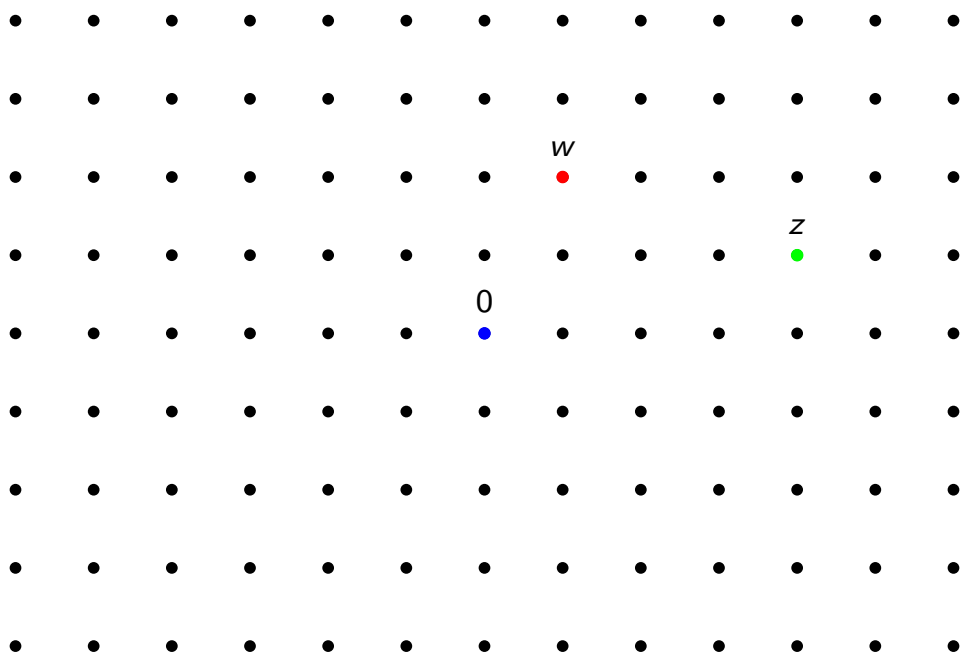
Največji skupni delitelj števil z in w je delitelj obeh števil z največjo normo.

Trditev

Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.

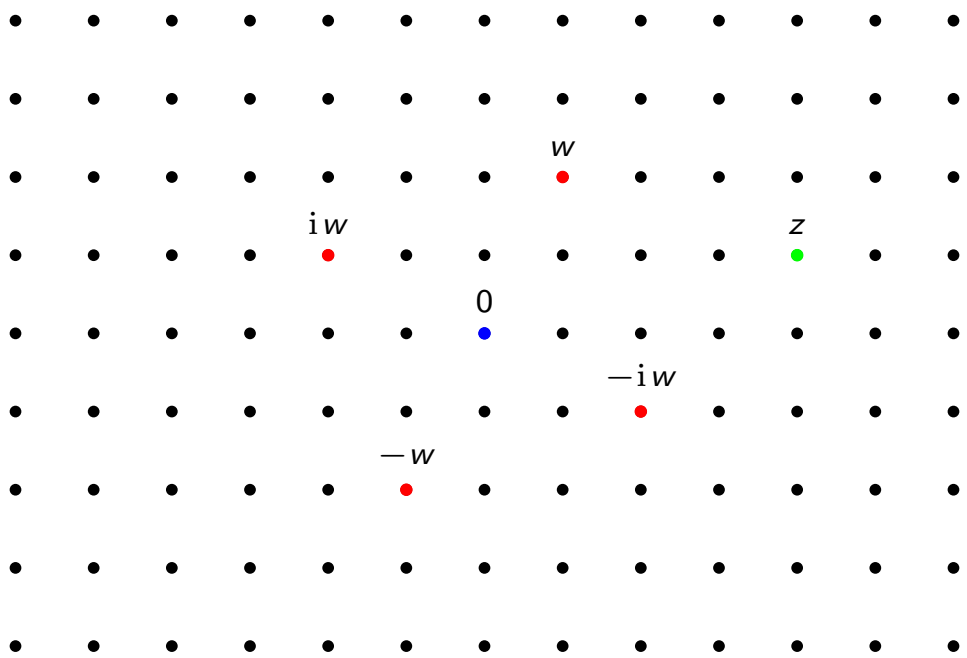
Trditev

Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



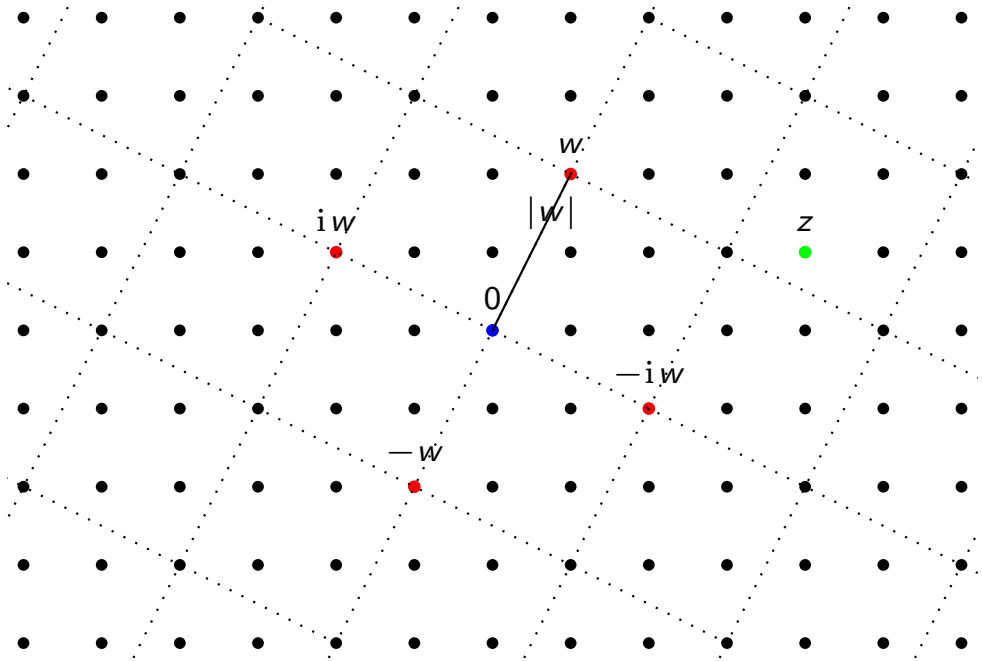
Trditev

Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



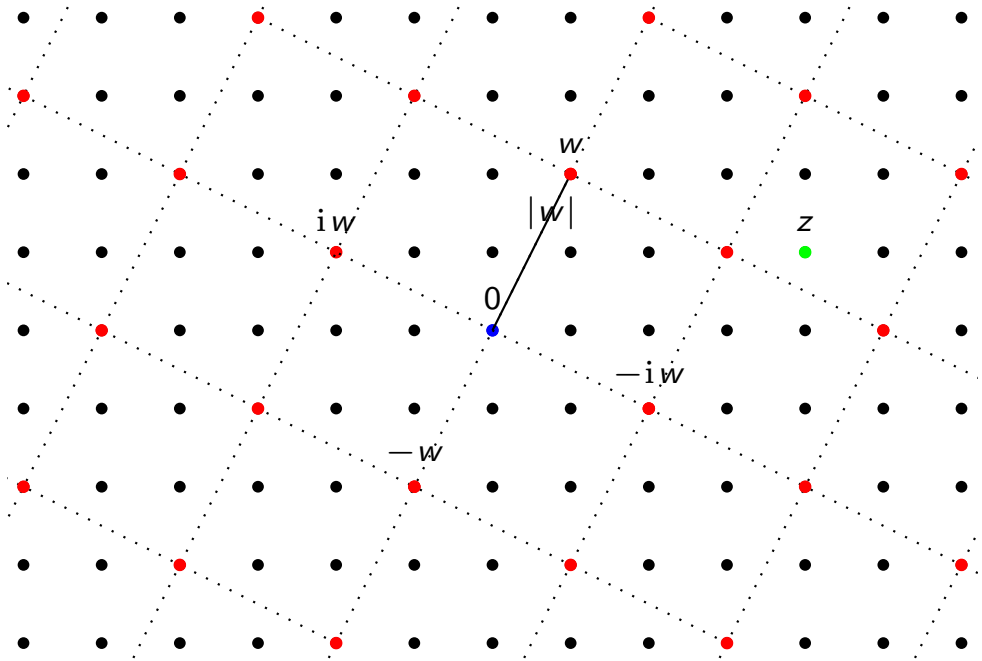
Trditev

Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



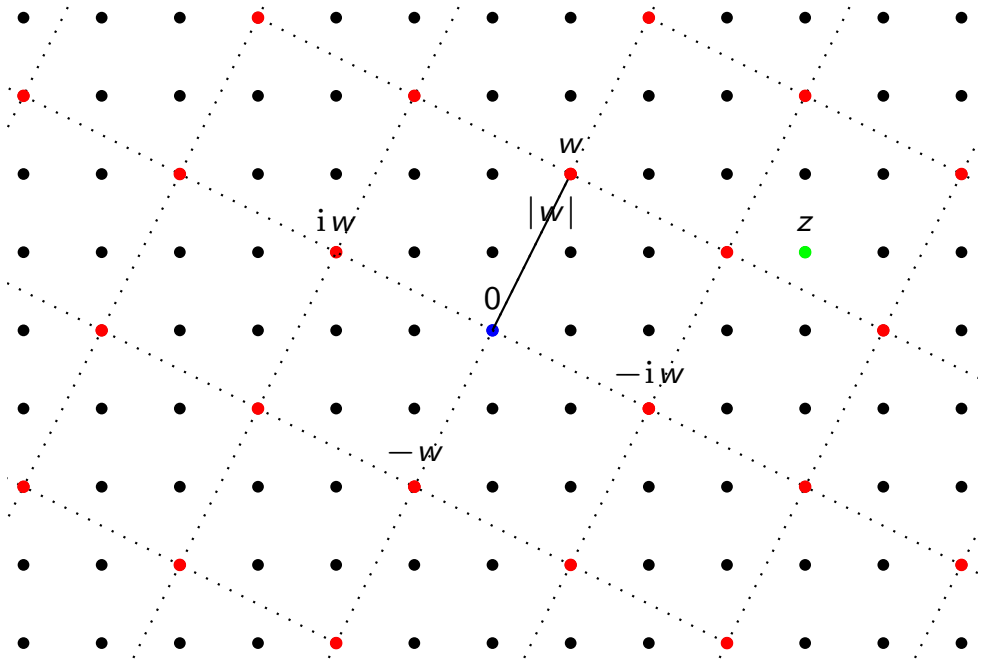
Trditev

Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



Trditev

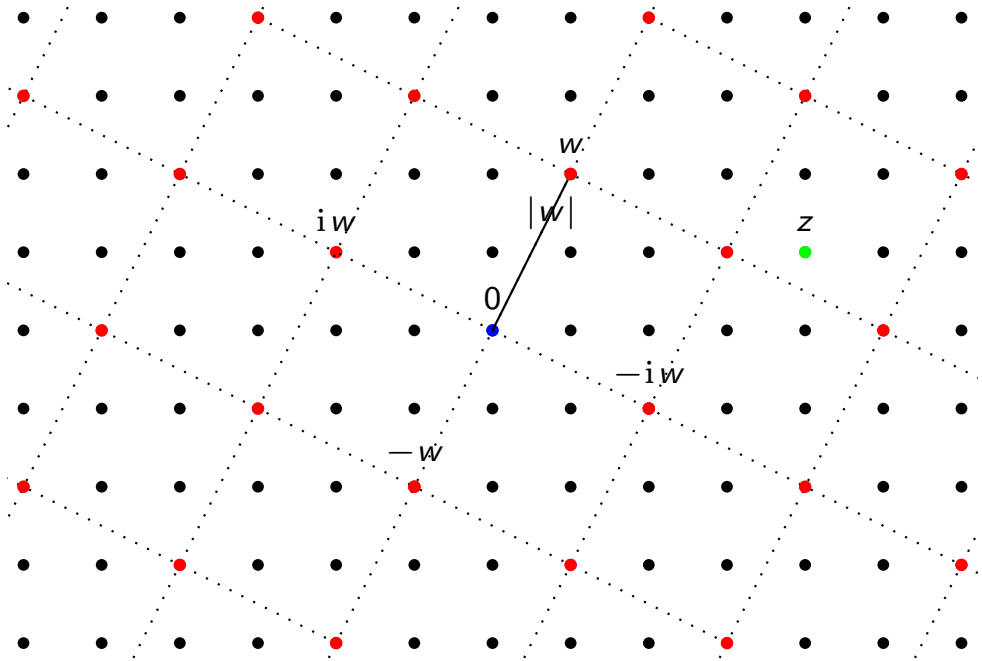
Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



Število z se nahaja v vsaj enem kvadratu.

Trditev

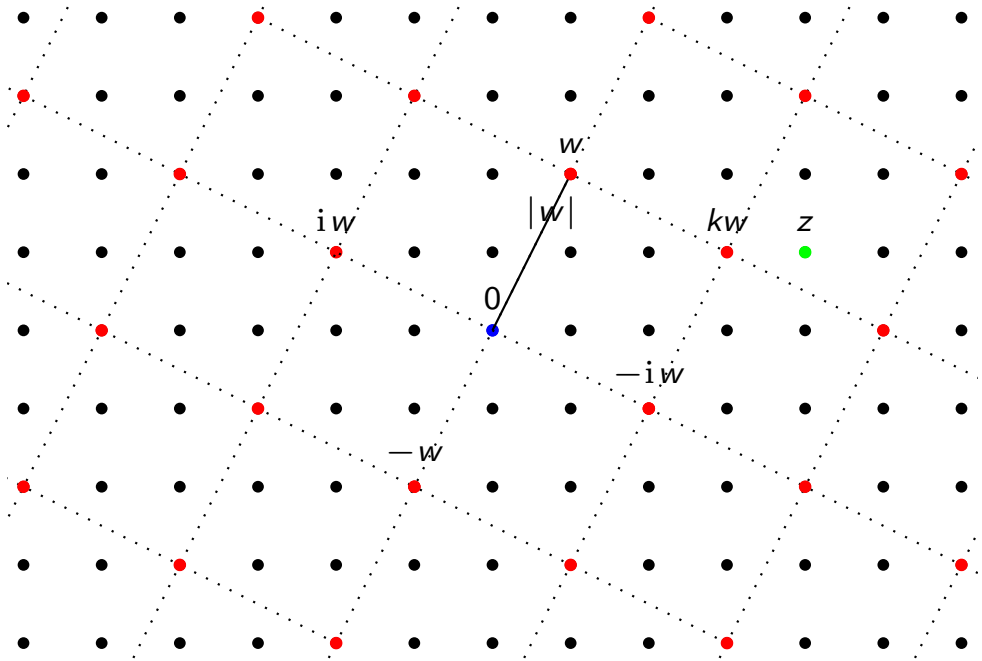
Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



Število z se nahaja v vsaj enem kvadratu. Izberemo eno od oglišč kvadrata, ki je najbližje z

Trditev

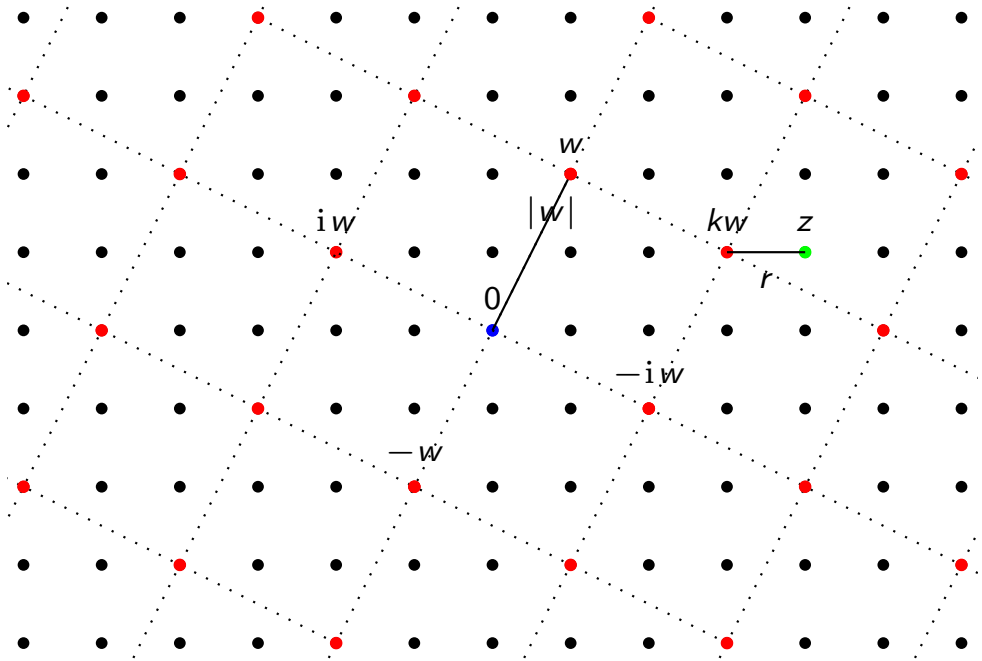
Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



Število z se nahaja v vsaj enem kvadratu. Izberemo eno od oglišč kvadrata, ki je najbližje z in ga označimo z kw.

Trditev

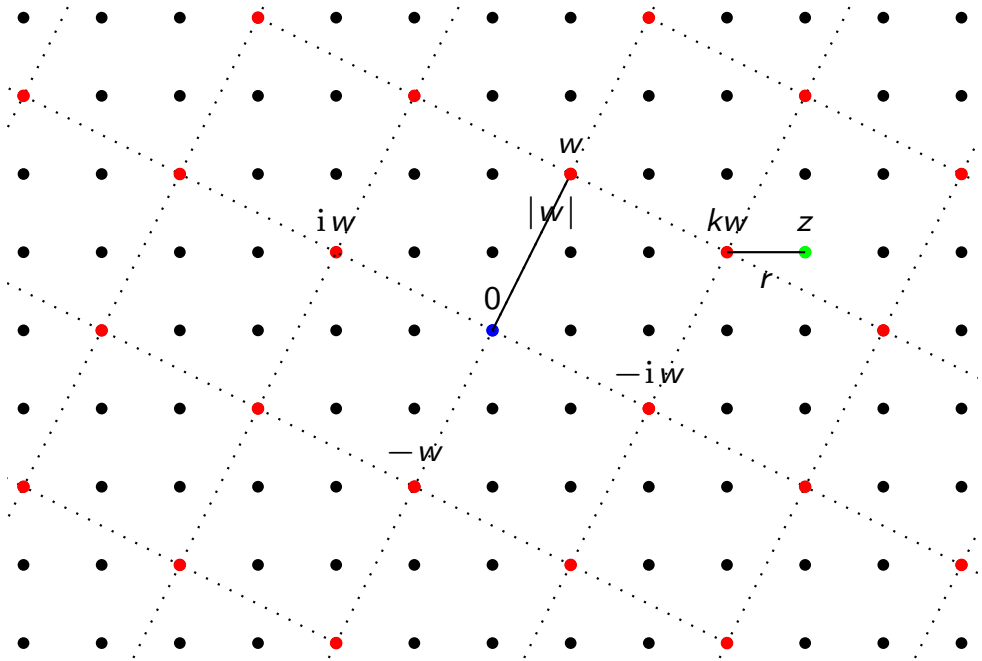
Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



Število z se nahaja v vsaj enem kvadratu. Izberemo eno od oglišč kvadrata, ki je najbližje z in ga označimo z kw. Razlika $z - kw$ je r,

Trditev

Za poljubni neničelni števili $z, w \in \mathbb{Z}[\mathrm{i}]$ obstajata $k, r \in \mathbb{Z}[\mathrm{i}]$, da je $z = kw + r$ in $N(r) < N(w)$.



Število z se nahaja v vsaj enem kvadratu. Izberemo eno od oglišč kvadrata, ki je najbližje z in ga označimo z kw. Razlika $z - kw$ je r, zato je $N(r) = |r|^2 \leq (\frac{\sqrt{2}}{2}|w|)^2 < N(w)$.

Kako poiščemo (kak) največji skupni delitelj števil z in w:

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Število r_n deli števili z in w.

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Število r_n deli števili z in w.
Vsak delitelj d števil z in w deli vsa števila r_i.

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Število r_n deli števili z in w.
Vsak delitelj d števil z in w deli vsa števila r_i.
Zato $N(d) \leq N(r_n)$ in je tako je r_n največji delitelj števil z in w.

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Število r_n deli števili z in w.
Vsak delitelj d števil z in w deli vsa števila r_i.
Zato $N(d) \leq N(r_n)$ in je tako je r_n največji delitelj števil z in w.
Za vsak drugi največji delitelj d velja $d = kr_n$ in

$$N(d) = N(kr_n) = N(k)N(r_n) = N(r_n).$$

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Število r_n deli števili z in w.
Vsak delitelj d števil z in w deli vsa števila r_i.
Zato $N(d) \leq N(r_n)$ in je tako je r_n največji delitelj števil z in w.
Za vsak drugi največji delitelj d velja $d = kr_n$ in

$$N(d) = N(kr_n) = N(k)N(r_n) = N(r_n).$$

Vsak največji delitelj $\mathrm{D}(z, w)$ je oblike kr_n, kjer je k obrnljiv element.

Kako poiščemo (kak) največji skupni delitelj števil z in w:

$$\begin{aligned} z &= k_1 w + r_1, \\ w &= k_2 r_1 + r_2, \\ r_1 &= k_3 r_2 + r_3, \\ &\dots \\ r_{n-2} &= k_n r_{n-1} + r_n, \\ r_{n-1} &= k_{n+1} r_n. \end{aligned}$$

Število r_n deli števili z in w.
Vsak delitelj d števil z in w deli vsa števila r_i.
Zato $N(d) \leq N(r_n)$ in je tako je r_n največji delitelj števil z in w.
Za vsak drugi največji delitelj d velja $d = kr_n$ in

$$N(d) = N(kr_n) = N(k)N(r_n) = N(r_n).$$

Vsak največji delitelj $\mathrm{D}(z, w)$ je oblike kr_n, kjer je k obrnljiv element.
Vedno lahko zapišemo $\mathrm{D}(z, w) = az + bw$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$)

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$,

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$, potem je $p = kd$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$, potem je $p = kd$.

1. Če je k obrnljiv, $k^{-1}p = d \mid z$ in zato tudi $p \mid z$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$, potem je $p = kd$.

1. Če je k obrnljiv, $k^{-1}p = d \mid z$ in zato tudi $p \mid z$.
2. Če je d obrnljiv,

$$\begin{aligned} d &= ap + bz, \\ dw &= apw + bzw, \\ w &= d^{-1}apw + d^{-1}bzw. \end{aligned}$$

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$, potem je $p = kd$.

1. Če je k obrnljiv, $k^{-1}p = d \mid z$ in zato tudi $p \mid z$.
2. Če je d obrnljiv,

$$\begin{aligned} d &= ap + bz, \\ dw &= apw + bzw, \\ w &= d^{-1}apw + d^{-1}bzw. \end{aligned}$$

Torej $p \mid w$.

Trditev

Število $p \in \mathbb{Z}[i]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$, potem je $p = kd$.

1. Če je k obrnljiv, $k^{-1}p = d \mid z$ in zato tudi $p \mid z$.
2. Če je d obrnljiv,

$$\begin{aligned} d &= ap + bz, \\ dw &= apw + bzw, \\ w &= d^{-1}apw + d^{-1}bzw. \end{aligned}$$

Torej $p \mid w$.

(Proti)primer: Število $3 \in \mathbb{Z}[i\sqrt{5}]$ je nerazcepno,

Trditev

Število $p \in \mathbb{Z}[\mathrm{i}]$ je Gaussovo praštevilo natanko tedaj, ko je nerazcepno.

($\Rightarrow$) Naj bo p Gaussovo praštevilo in $p = zw$.
Torej $p \mid z$ (ali $p \mid w$) in zato $z = kp$.
Dobili: $p = zw = kpw$, torej $kw = 1$ in zato je w obrnljivo.
($\Leftarrow$) Naj bo p nerazcepno in $p \mid zw$.
Naj bo $d = \mathrm{D}(p, z)$, potem je $p = kd$.

1. Če je k obrnljiv, $k^{-1}p = d \mid z$ in zato tudi $p \mid z$.
2. Če je d obrnljiv,

$$\begin{aligned} d &= ap + bz, \\ dw &= apw + bzw, \\ w &= d^{-1}apw + d^{-1}bzw. \end{aligned}$$

Torej $p \mid w$.

(Proti)primer: Število $3 \in \mathbb{Z}[\mathrm{i}\sqrt{5}]$ je nerazcepno,
ni pa praštevilo, saj $3 \mid 9 = (2 + \mathrm{i}\sqrt{5})(2 - \mathrm{i}\sqrt{5})$.

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1 + \mathrm{i})(1 - \mathrm{i})$,

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1 + \mathrm{i})(1 - \mathrm{i})$,
- $5 = (2 + \mathrm{i})(2 - \mathrm{i})$,

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1 + \mathrm{i})(1 - \mathrm{i})$,
- $5 = (2 + \mathrm{i})(2 - \mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1 + \mathrm{i})(1 - \mathrm{i})$,
- $5 = (2 + \mathrm{i})(2 - \mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Trditev

Če je $p \equiv 3 \pmod 4$ in je p praštevilo, je p Gaussovo praštevilo.

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1 + \mathrm{i})(1 - \mathrm{i})$,
- $5 = (2 + \mathrm{i})(2 - \mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Trditev

Če je $p \equiv 3 \pmod 4$ in je p praštevilo, je p Gaussovo praštevilo.

Denimo, da je $p = (a + b\mathrm{i})(c + d\mathrm{i})$.

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1+\mathrm{i})(1-\mathrm{i})$,
- $5 = (2+\mathrm{i})(2-\mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Trditev

Če je $p \equiv 3 \pmod 4$ in je p praštevilo, je p Gaussovo praštevilo.

Denimo, da je $p = (a+b\mathrm{i})(c+d\mathrm{i})$. Potem je

$$p^2 = N(p) = N(a+b\mathrm{i})N(c+d\mathrm{i}) = (a^2+b^2)(c^2+d^2).$$

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1+\mathrm{i})(1-\mathrm{i})$,
- $5 = (2+\mathrm{i})(2-\mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Trditev

Če je $p \equiv 3 \pmod 4$ in je p praštevilo, je p Gaussovo praštevilo.

Denimo, da je $p = (a+b\mathrm{i})(c+d\mathrm{i})$. Potem je

$$p^2 = N(p) = N(a+b\mathrm{i})N(c+d\mathrm{i}) = (a^2+b^2)(c^2+d^2).$$

Torej je $a^2 + b^2 = p = c^2 + d^2$.

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1+\mathrm{i})(1-\mathrm{i})$,
- $5 = (2+\mathrm{i})(2-\mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Trditev

Če je $p \equiv 3 \pmod 4$ in je p praštevilo, je p Gaussovo praštevilo.

Denimo, da je $p = (a+b\mathrm{i})(c+d\mathrm{i})$. Potem je

$$p^2 = N(p) = N(a+b\mathrm{i})N(c+d\mathrm{i}) = (a^2+b^2)(c^2+d^2).$$

Torej je $a^2+b^2 = p = c^2+d^2$.
Ker je $n^2 \equiv 0$ ali $1 \pmod 4$

Primeri (in neprimeri) Gaussovih praštevil:

- $2 = (1+\mathrm{i})(1-\mathrm{i})$,
- $5 = (2+\mathrm{i})(2-\mathrm{i})$,
- 3 je Gaussovo praštevilo, saj je $N(z) \neq 3$ za vse $z \in \mathbb{Z}[\mathrm{i}]$.

Trditev

Če je $p \equiv 3 \pmod 4$ in je p praštevilo, je p Gaussovo praštevilo.

Denimo, da je $p = (a+b\mathrm{i})(c+d\mathrm{i})$. Potem je

$$p^2 = N(p) = N(a+b\mathrm{i})N(c+d\mathrm{i}) = (a^2+b^2)(c^2+d^2).$$

Torej je $a^2+b^2 = p = c^2+d^2$.
Ker je $n^2 \equiv 0$ ali $1 \pmod 4$, je $a^2+b^2 \equiv 0, 1$ ali $2 \pmod 4$.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y)

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Vsaka točka, ki ni negibna, ima preko predpisa f svoj par.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Vsaka točka, ki ni negibna, ima preko predpisa f svoj par.
Če je n_f število negibnih točk za f,

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Vsaka točka, ki ni negibna, ima preko predpisa f svoj par.
Če je n_f število negibnih točk za f, je

$$|S| = n_f + 2k.$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Vsaka točka, ki ni negibna, ima preko predpisa f svoj par.
Če je n_f število negibnih točk za f, je

$$|S| = n_f + 2k.$$

Če pokažemo, da ima S liho mnogo elementov,

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Vsaka točka, ki ni negibna, ima preko predpisa f svoj par.
Če je n_f število negibnih točk za f, je

$$|S| = n_f + 2k.$$

Če pokažemo, da ima S liho mnogo elementov, ima f vsaj eno negibno točko

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Dovolj je pokazati, da p lahko zapišemo kot vsoto dveh kvadratov:

$$p = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i}).$$

(Zagier) Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ (S je končna).
Predpis $f : S \to S$, $f(x, y, z) = (x, z, y)$ je idempotent.
Vsaka negibna točka za f je oblike (x, y, y) in nam poda zapis

$$x^2 + 4y^2 = x^2 + (2y)^2 = p.$$

Vsaka točka, ki ni negibna, ima preko predpisa f svoj par.
Če je n_f število negibnih točk za f, je

$$|S| = n_f + 2k.$$

Če pokažemo, da ima S liho mnogo elementov, ima f vsaj eno negibno točko in tako p na vsaj en način zapišemo kot vsoto dveh kvadratov.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Trojica $(y - z, y, z)$ ni v S,

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Trojica $(y - z, y, z)$ ni v S, saj število

$$(y - z)^2 + 4yz = y^2 - 2yz + z^2 + 4yz = y^2 + 2yz + z^2 = (y + z)^2$$

ni praštevilo.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Trojica $(y - z, y, z)$ ni v S, saj število

$$(y - z)^2 + 4yz = y^2 - 2yz + z^2 + 4yz = y^2 + 2yz + z^2 = (y + z)^2$$

ni praštevilo.
Tudi trojica $(2y, y, z)$ ni v S,

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Trojica $(y - z, y, z)$ ni v S, saj število

$$(y - z)^2 + 4yz = y^2 - 2yz + z^2 + 4yz = y^2 + 2yz + z^2 = (y + z)^2$$

ni praštevilo.
Tudi trojica $(2y, y, z)$ ni v S, saj število

$$(2y)^2 + 4yz = 4y^2 + 4yz = 4y(y + z)$$

ni praštevilo.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
$x < y - z$:

- $(x')^2 + 4y'z' = x^2 + 4xz + 4z^2 + 4yz - 4xz - 4z^2 = x^2 + 4yz = p$,

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
$x < y - z$:

- $(x')^2 + 4y'z' = x^2 + 4xz + 4z^2 + 4yz - 4xz - 4z^2 = x^2 + 4yz = p$,
- $x' = x + 2z > 2z = 2y'$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
$x < y - z$:

- $(x')^2 + 4y'z' = x^2 + 4xz + 4z^2 + 4yz - 4xz - 4z^2 = x^2 + 4yz = p$,
- $x' = x + 2z > 2z = 2y'$, zato

$$g^2(x, y, z) = (x' - 2y', x' - y' + z', y') = (x, y, z).$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
$y - z < x < 2y$:

- $(x')^2 + 4y'z' = 4y^2 - 4xy + x^2 + 4xy - 4y^2 + 4yz = x^2 + 4yz = p$,
- $y' - z' = 2y - x - z < x' = 2y - x < 2y = 2y'$, zato

$$g^2(x, y, z) = (2y' - x', y', x' - y' + z') = (x, y, z).$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
$2y < x$:

- $(x')^2 + 4y'z' = x^2 - 4xy + 4y^2 + 4xy - 4y^2 + 4yz = x^2 + 4yz = p$,
- $y' - z' = x - 2y + z > x'$, zato

$$g^2(x, y, z) = (x' + 2z', z', y' - x' - z') = (x, y, z).$$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
Negibno točko lahko dobimo le za $y - z < x < 2y$.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
Negibno točko lahko dobimo le za $y - z < x < 2y$.
Dobimo $x = y$

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
Negibno točko lahko dobimo le za $y - z < x < 2y$.
Dobimo $x = y$ in tako $x^2 + 4xz = x(x + 4z) = p$.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

Pišimo $g(x, y, z) = (x', y', z')$.
Negibno točko lahko dobimo le za $y - z < x < 2y$.
Dobimo $x = y$ in tako $x^2 + 4xz = x(x + 4z) = p$.
g ima le eno negibno točko $(1, 1, \frac{1}{4}(p - 1))$.

Trditev

Če je $p \equiv 1 \pmod 4$ in je p praštevilo, p ni Gaussovo praštevilo.

Naj bo $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$.
Definirajmo $g \colon S \to S$,

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x. \end{cases}$$

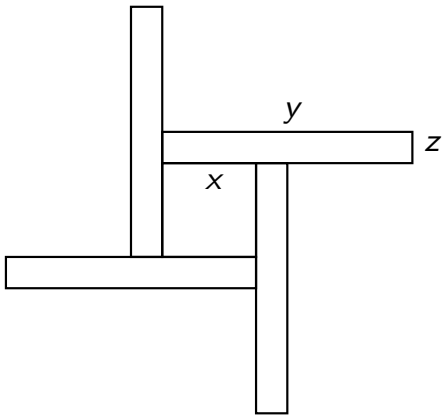
Pišimo $g(x, y, z) = (x', y', z')$.
Negibno točko lahko dobimo le za $y - z < x < 2y$.
Dobimo $x = y$ in tako $x^2 + 4xz = x(x + 4z) = p$.
g ima le eno negibno točko $(1, 1, \frac{1}{4}(p - 1))$.
Množica S ima liho mnogo elementov, zato je $n_f > 0$.

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$

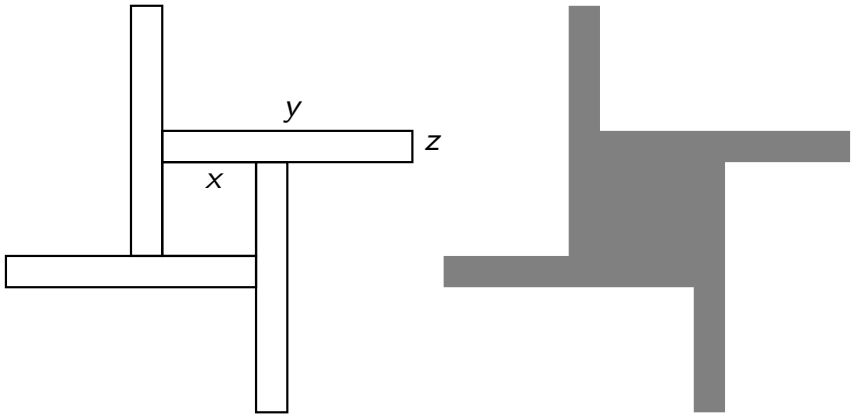
Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



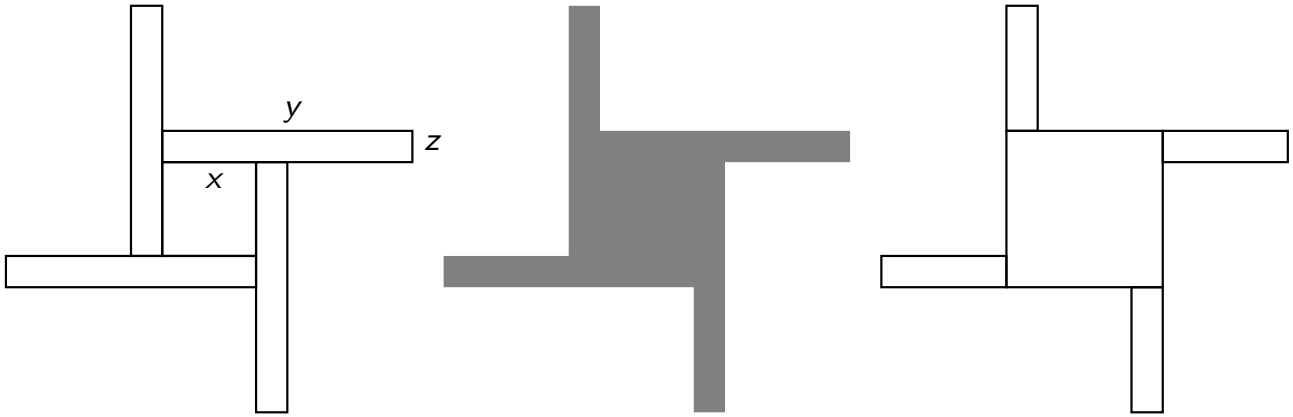
Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



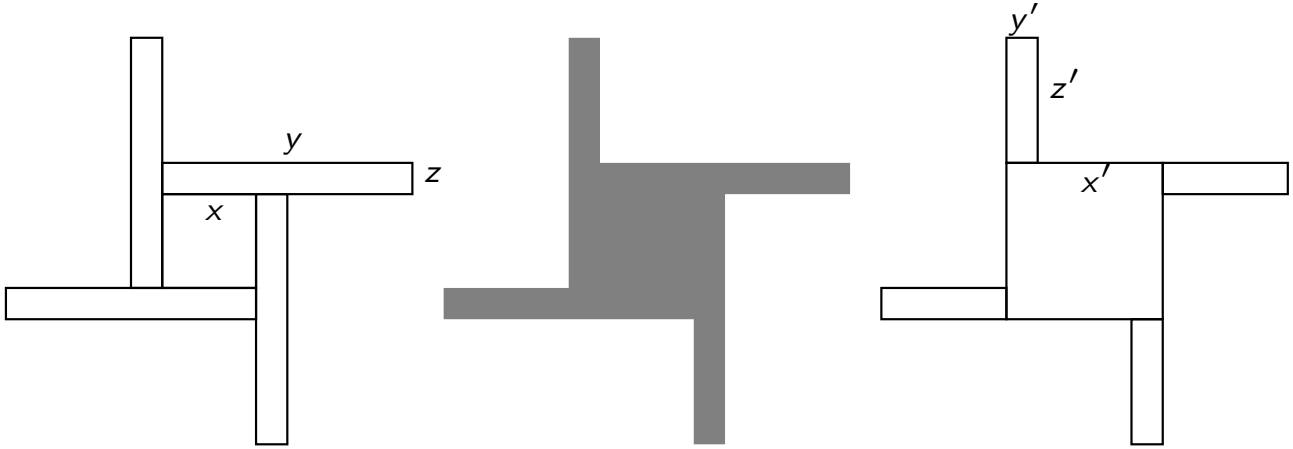
Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



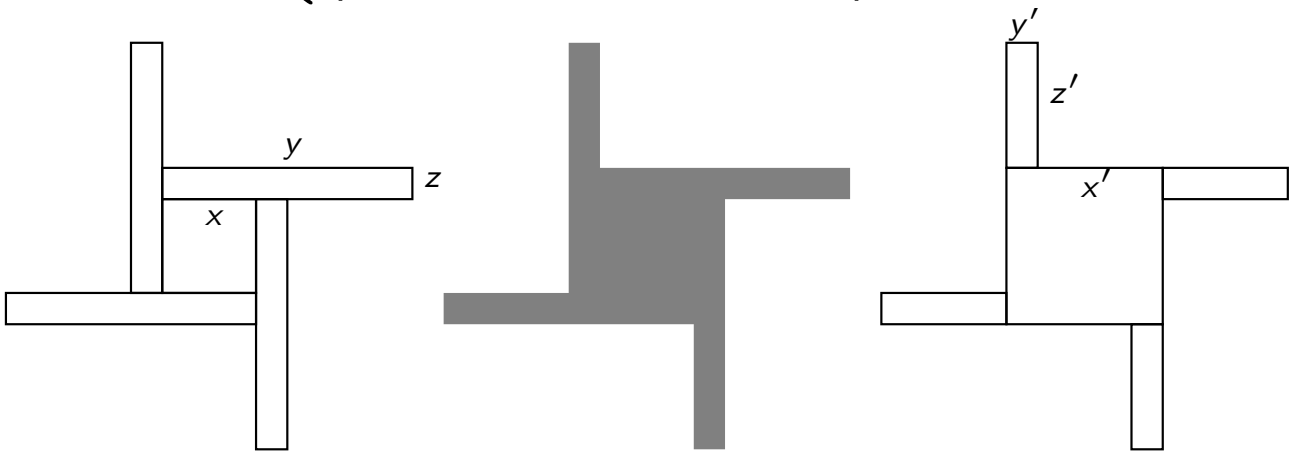
Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x,y,z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

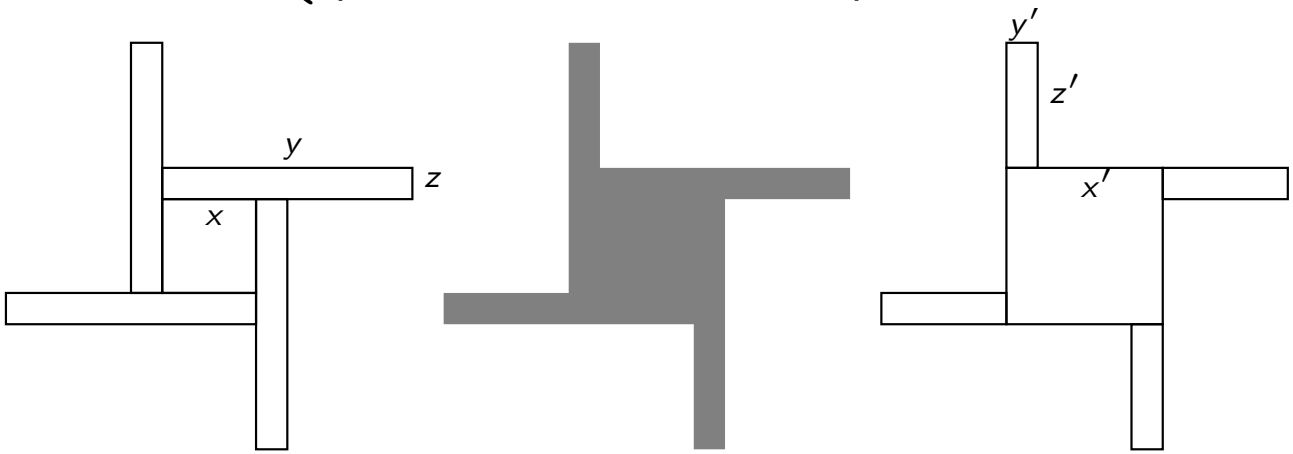
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $x < y - z$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

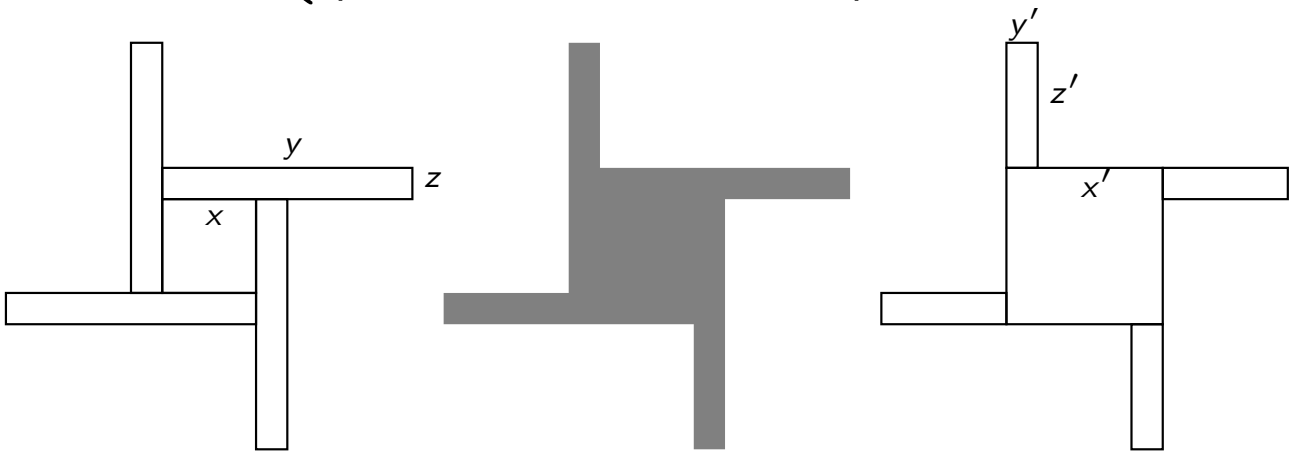
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $x < y - z$ in $x' = x + 2z$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

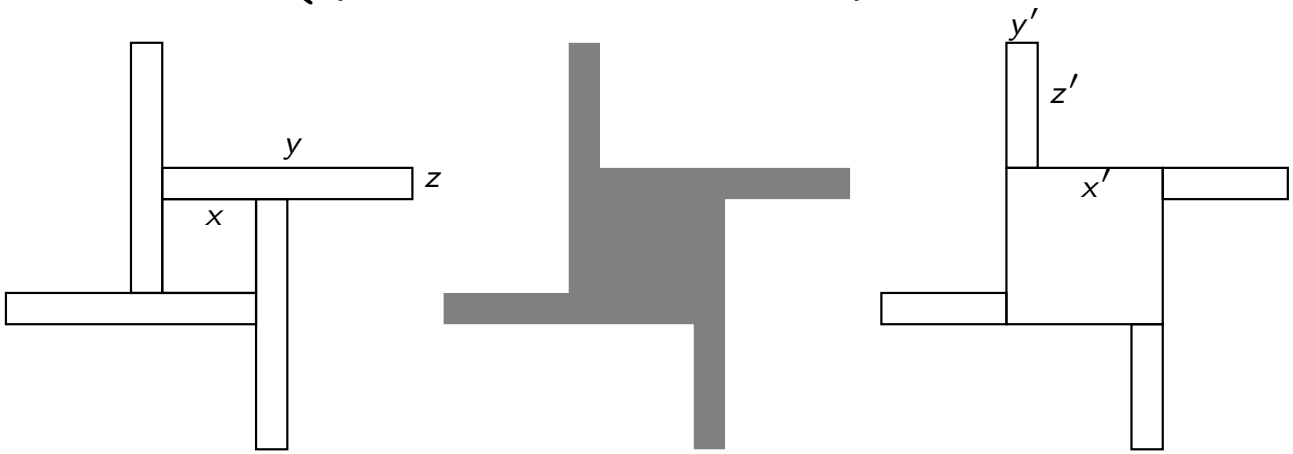
$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & x < y-z, \\ (2y-x, y, x-y+z), & y-z < x < 2y, \\ (x-2y, x-y+z, y), & 2y < x? \end{cases}$$



Velja $x < y - z$ in $x' = x + 2z$, $y' = z$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

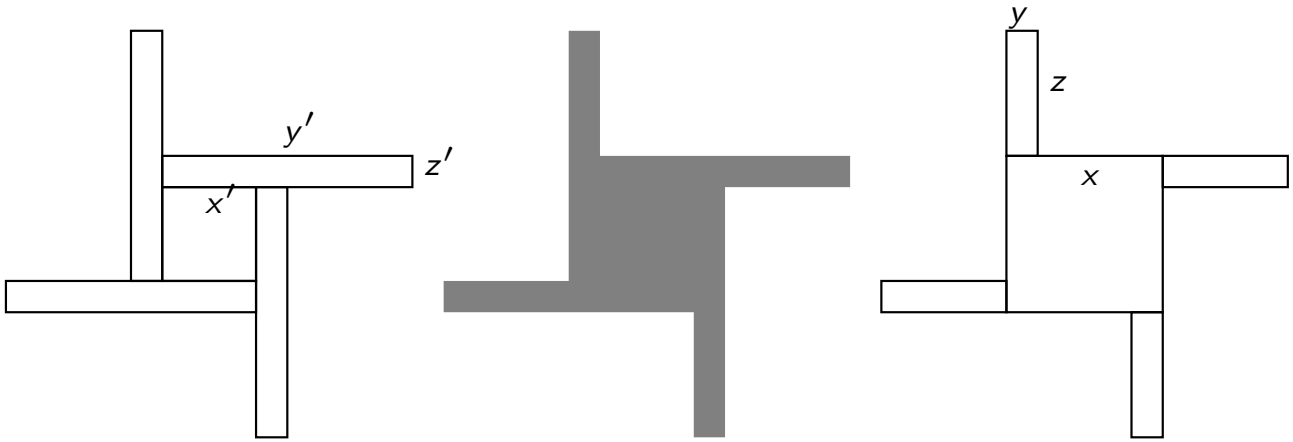
$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & x < y-z, \\ (2y-x, y, x-y+z), & y-z < x < 2y, \\ (x-2y, x-y+z, y), & 2y < x? \end{cases}$$



Velja $x < y - z$ in $x' = x + 2z$, $y' = z$ in $z' = y - x - z$.

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

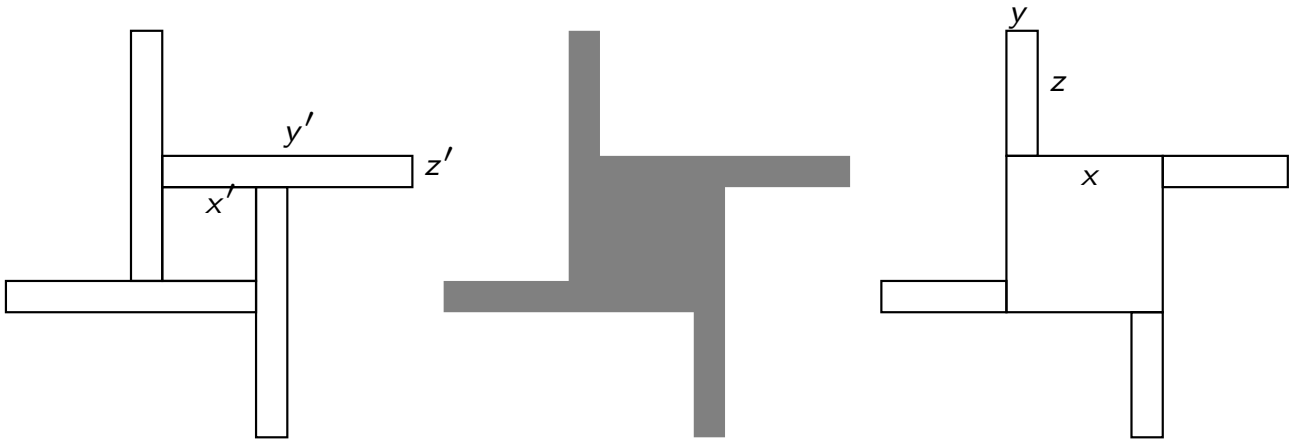
$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & x < y-z, \\ (2y-x, y, x-y+z), & y-z < x < 2y, \\ (x-2y, x-y+z, y), & 2y < x? \end{cases}$$



Velja $x < y - z$ in $x' = x + 2z$, $y' = z$ in $z' = y - x - z$.
V drugo smer:

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

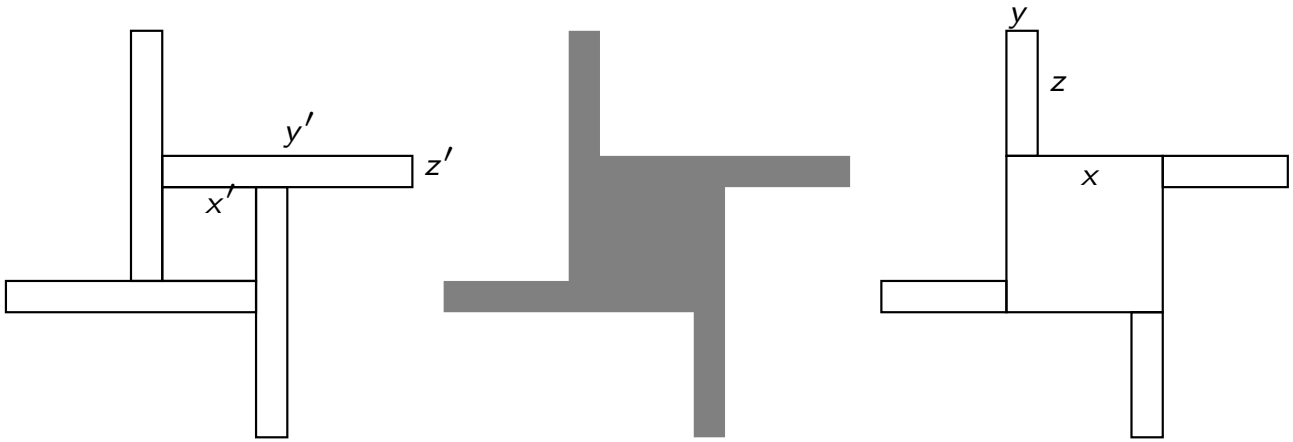
$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & x < y-z, \\ (2y-x, y, x-y+z), & y-z < x < 2y, \\ (x-2y, x-y+z, y), & 2y < x? \end{cases}$$



Velja $x < y - z$ in $x' = x + 2z$, $y' = z$ in $z' = y - x - z$.
V drugo smer:
Velja: $2y < x$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & x < y-z, \\ (2y-x, y, x-y+z), & y-z < x < 2y, \\ (x-2y, x-y+z, y), & 2y < x? \end{cases}$$



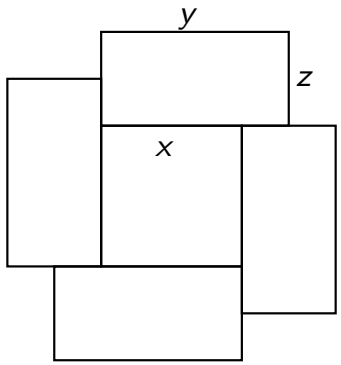
Velja $x < y - z$ in $x' = x + 2z$, $y' = z$ in $z' = y - x - z$.
V drugo smer:
Velja: $2y < x$ in $x' = x - 2y$, $y' = x + z - y$ in $z' = y$.

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$

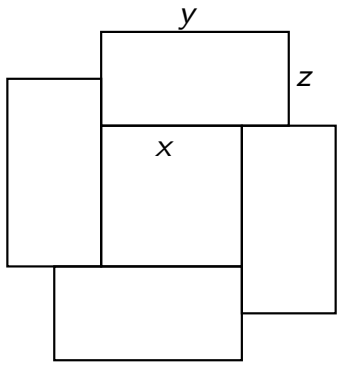
Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



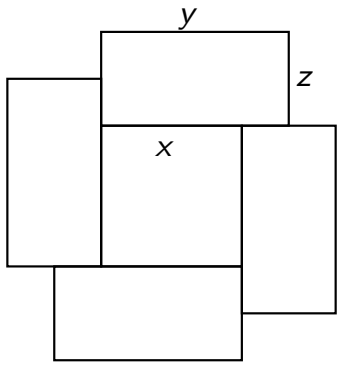
Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

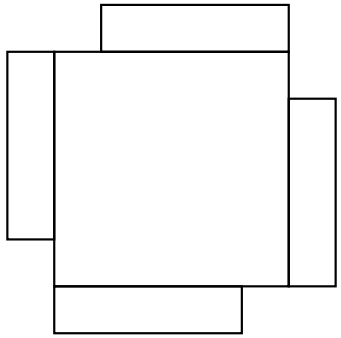
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

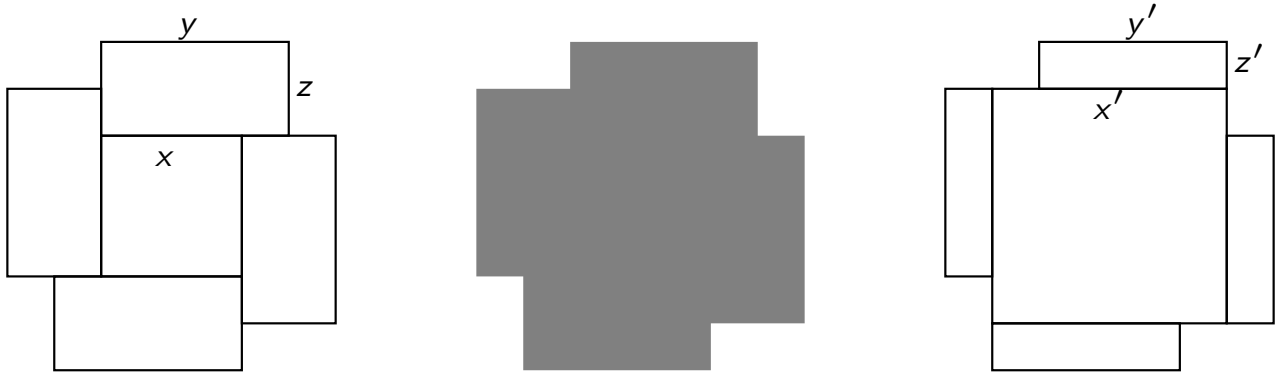
$$g(x,y,z) = \begin{cases} (x+2z, z, y-x-z), & x < y-z, \\ (2y-x, y, x-y+z), & y-z < x < 2y, \\ (x-2y, x-y+z, y), & 2y < x? \end{cases}$$





Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

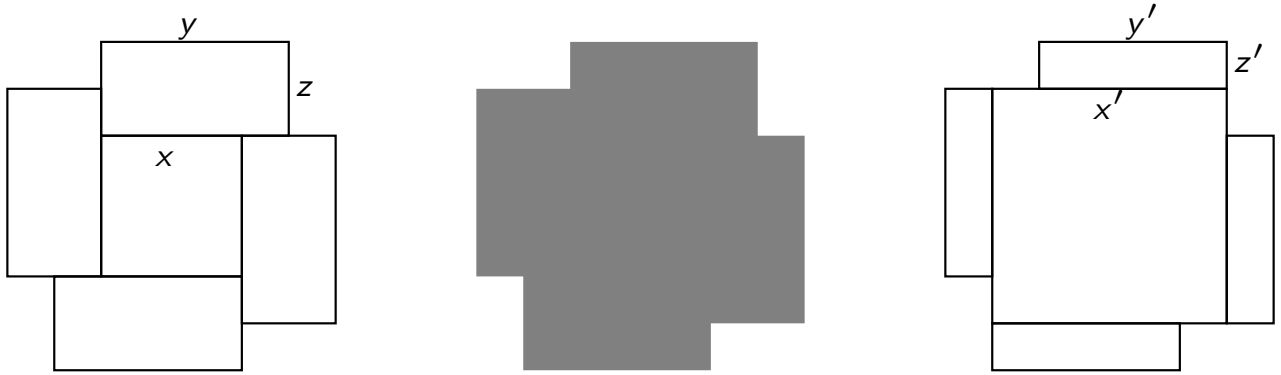
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $y - z < x < 2y$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

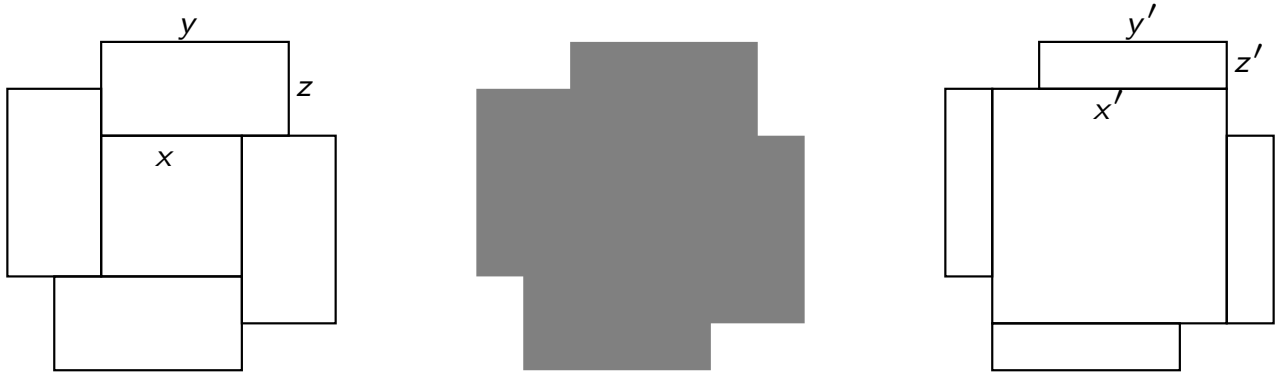
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $y - z < x < 2y$ in $x' = x + 2(y - x) = 2y - x$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

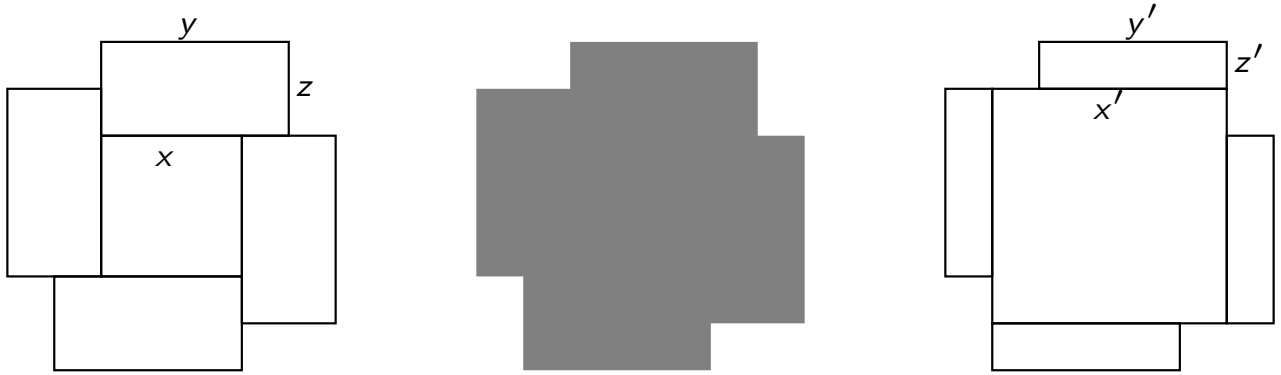
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $y - z < x < 2y$ in $x' = x + 2(y - x) = 2y - x$, $y' = y$

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

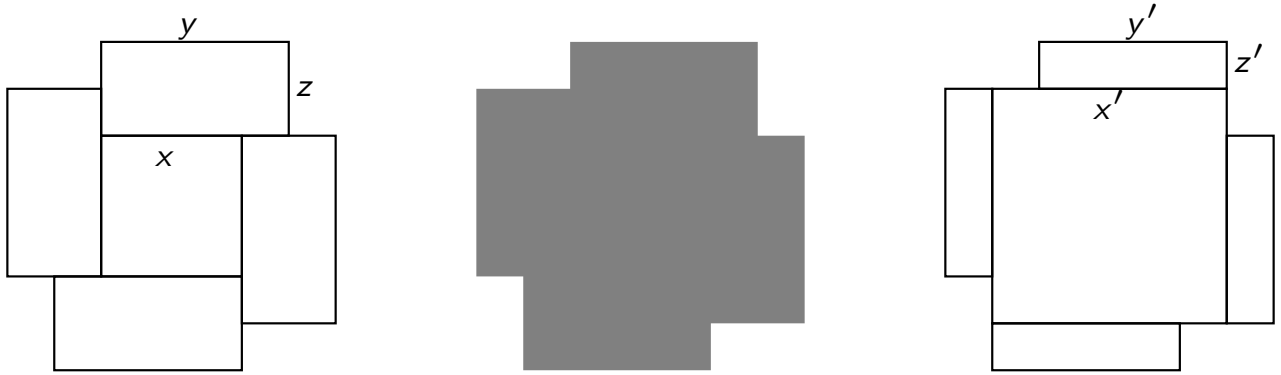
$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $y - z < x < 2y$ in $x' = x + 2(y - x) = 2y - x$, $y' = y$ in $z' = z - y + x$.

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$



Velja $y - z < x < 2y$ in $x' = x + 2(y - x) = 2y - x$, $y' = y$ in $z' = z - y + x$.

V drugo smer

Ali obstaja geometrična interpretacija preslikave $g\colon S \to S$ ($S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$), dane kot

$$g(x, y, z) = \begin{cases} (x + 2z, z, y - x - z), & x < y - z, \\ (2y - x, y, x - y + z), & y - z < x < 2y, \\ (x - 2y, x - y + z, y), & 2y < x? \end{cases}$$

Velja $y - z < x < 2y$ in $x' = x + 2(y - x) = 2y - x$, $y' = y$ in $z' = z - y + x$.
V drugo smer velja enako kot zgoraj.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.
Če $p = q\overline{q} = r\overline{r}$

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.
Če $p = q\overline{q} = r\overline{r}$, je $N(q) = N(r) = p$, zato sta q in r Gaussovi praštevili.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.
Če $p = q\overline{q} = r\overline{r}$, je $N(q) = N(r) = p$, zato sta q in r Gaussovi praštevili.
Ker $q \mid p = r\overline{r}$

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.
Če $p = q\overline{q} = r\overline{r}$, je $N(q) = N(r) = p$, zato sta q in r Gaussovi praštevili.
Ker $q \mid p = r\overline{r}$, velja $q \mid r$ ali $q \mid \overline{r}$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.
Če $p = q\overline{q} = r\overline{r}$, je $N(q) = N(r) = p$, zato sta q in r Gaussovi praštevili.
Ker $q \mid p = r\overline{r}$, velja $q \mid r$ ali $q \mid \overline{r}$.
Torej $q = kr$ ali $q = k\overline{r}$, za nek obrnljiv element k.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Naj bo $p \equiv 1 \pmod 4$ in p praštevilo.
Če $p = q\overline{q} = r\overline{r}$, je $N(q) = N(r) = p$, zato sta q in r Gaussovi praštevili.
Ker $q \mid p = r\overline{r}$, velja $q \mid r$ ali $q \mid \overline{r}$.
Torej $q = kr$ ali $q = k\overline{r}$, za nek obrnljiv element k.

Trditev

Praštevilo $p \equiv 1 \pmod 4$ lahko zapišemo kot vsoto dveh kvadratov le na en način.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Če z ni z zgornjega seznama, $N(z)$ ni niti praštevilo niti kvadrat praštevila $p \equiv 3 \pmod 4$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Če z ni z zgornjega seznama, $N(z)$ ni niti praštevilo niti kvadrat praštevila $p \equiv 3 \pmod 4$. Naj $p \mid N(z)$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Če z ni z zgornjega seznama, $N(z)$ ni niti praštevilo niti kvadrat praštevila $p \equiv 3 \pmod 4$. Naj $p \mid N(z)$.

1. $p \equiv 3 \pmod 4$, potem Gaussovo praštevilo $p \mid z\overline{z}$ in zato $p \mid z$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Če z ni z zgornjega seznama, $N(z)$ ni niti praštevilo niti kvadrat praštevila $p \equiv 3 \pmod 4$. Naj $p \mid N(z)$.

1. $p \equiv 3 \pmod 4$, potem Gaussovo praštevilo $p \mid z\overline{z}$ in zato $p \mid z$.
2. $q\overline{q} = p \equiv 1 \pmod 4$, potem Gaussovo praštevilo $q \mid z\overline{z}$ in zato $q \mid z$ ali $q \mid \overline{z}$ (oz. $\overline{q} \mid z$).

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Če z ni z zgornjega seznama, $N(z)$ ni niti praštevilo niti kvadrat praštevila $p \equiv 3 \pmod 4$. Naj $p \mid N(z)$.

1. $p \equiv 3 \pmod 4$, potem Gaussovo praštevilo $p \mid z\overline{z}$ in zato $p \mid z$.
2. $q\overline{q} = p \equiv 1 \pmod 4$, potem Gaussovo praštevilo $q \mid z\overline{z}$ in zato $q \mid z$ ali $q \mid \overline{z}$ (oz. $\overline{q} \mid z$).

Torej z ni Gaussovo praštevilo.

Izrek

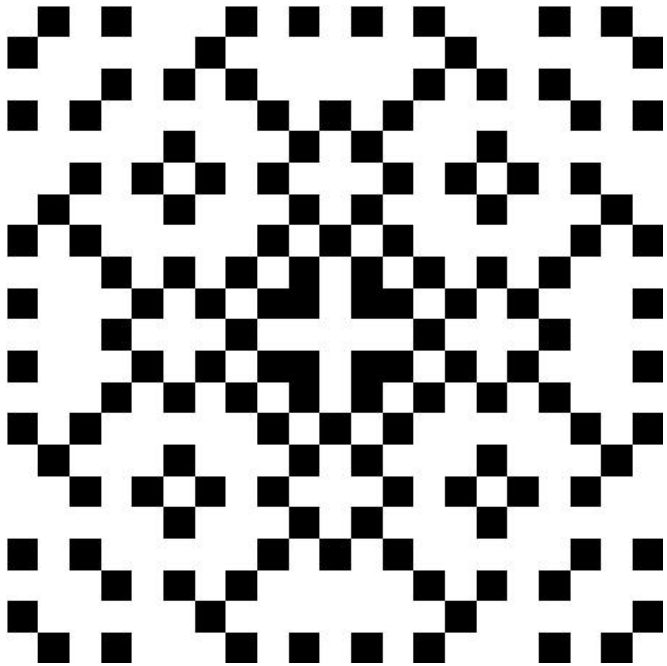
Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.

Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

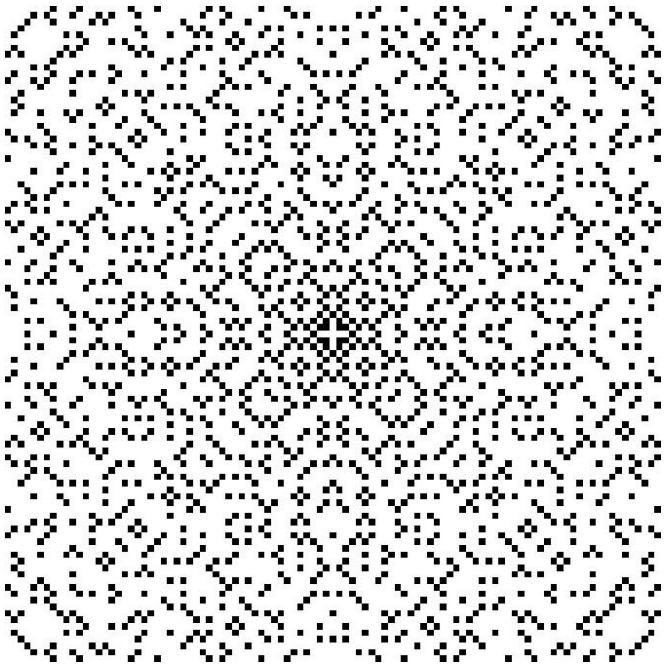
- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.



Izrek

Do množenja z obrnljivim elementom, so Gaussova praštevila:

- $1 + \mathrm{i}$,
- če $p \equiv 3 \pmod 4$ praštevilo, je p Gaussovo praštevilo,
- če $p \equiv 1 \pmod 4$ praštevilo, obstajata dve Gaussovi praštevili q in $\overline{q}$, kjer je $q\overline{q} = p$.



Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2$$

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2$$

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'})$$

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'})$$

- Če $p \mid a_5$, potem $p \mid a_j + ia_{j'}$ ali $p \mid a_j - ia_{j'}$.

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'})$$

- Če $p \mid a_5$, potem $p \mid a_j + ia_{j'}$ ali $p \mid a_j - ia_{j'}$.
- Če $p \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = pz$

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'})$$

- Če $p \mid a_5$, potem $p \mid a_j + ia_{j'}$ ali $p \mid a_j - ia_{j'}$.
- Če $p \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = pz$ in zato $a_j - ia_{j'} = p\bar{z}$.

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'})$$

- Če $p \mid a_5$, potem $p \mid a_j + ia_{j'}$ ali $p \mid a_j - ia_{j'}$.
- Če $p \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = pz$ in zato $a_j - ia_{j'} = p\bar{z}$.
- Torej je $2a_j = p(z + \bar{z})$ in $2ia_{j'} = p(z - \bar{z})$.

Trditev

V primitivnem magičnem kvadratu kvadratov število $a_5 = \frac{1}{3}S$ ni deljivo s praštevilom $p \equiv 3 \pmod 4$.

Dokaz:

- Za vsak j velja

$$2a_5^2 = a_j^2 + a_{j'}^2 = a_j^2 - i^2 a_{j'}^2 = (a_j + ia_{j'})(a_j - ia_{j'})$$

- Če $p \mid a_5$, potem $p \mid a_j + ia_{j'}$ ali $p \mid a_j - ia_{j'}$.
- Če $p \mid a_j + ia_{j'}$, je $a_j + ia_{j'} = pz$ in zato $a_j - ia_{j'} = p\bar{z}$.
- Torej je $2a_j = p(z + \bar{z})$ in $2ia_{j'} = p(z - \bar{z})$.
- Zato $p \mid a_j$ in $p \mid a_{j'}$.

http://www.multimagie.com/

Christian Boyer za magični kvadrat kvadratov ponuja 1000€ in šampanjec.