Števila, predstavljiva kot vsota dveh kvadratov

Petra Janžekovič

Fakulteta za matematiko in fiziko
Oddelek za matematiko

13. marec 2009

Katera števila so predstavljiva?

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$$\begin{array}{rl} n = & x^2 + y^2 \\ \hline 1 = & \end{array}$$

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$
$8 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$
$8 =$	2^2	$+$	2^2

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$
$8 =$	2^2	$+$	2^2
$9 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$
$8 =$	2^2	$+$	2^2
$9 =$	3^2	$+$	0^2

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$
$8 =$	2^2	$+$	2^2
$9 =$	3^2	$+$	0^2
$10 =$			

Katera števila so predstavljiva?

Definicija

Število $n \in \mathbb{N}$ je predstavljivo, če je vsota dveh kvadratov, torej se da zapisati kot $n = x^2 + y^2$ za neka $x, y \in \mathbb{N}_0$.

Primeri

$n =$	x^2	$+$	y^2
$1 =$	1^2	$+$	0^2
$2 =$	1^2	$+$	1^2
$3 =$	$??$	$+$	$??$
$4 =$	2^2	$+$	0^2
$5 =$	2^2	$+$	1^2
$6 =$	$??$	$+$	$??$
$7 =$	$??$	$+$	$??$
$8 =$	2^2	$+$	2^2
$9 =$	3^2	$+$	0^2
$10 =$	3^2	$+$	1^2

Obseg praštevil

Če je p praštevilo, potem množica $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ skupaj z operacijama seštevanja in množenja po modulu p tvori končen obseg.

Obseg praštevil

Če je p praštevilo, potem množica $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ skupaj z operacijama seštevanja in množenja po modulu p tvori končen obseg.
Nekatere lastnosti obsega $\mathbb{Z}_p$:

Obseg praštevil

Če je p praštevilo, potem množica $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ skupaj z operacijama seštevanja in množenja po modulu p tvori končen obseg.
Nekatere lastnosti obsega $\mathbb{Z}_p$:

- za vsak $x \in \mathbb{Z}_p$, $x \neq 0$, obstaja aditivni inverz $p - x$ tako, da velja:

$$x + (p - x) = p \equiv 0 (mod\ p)$$

Obseg praštevil

Če je p praštevilo, potem množica $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ skupaj z operacijama seštevanja in množenja po modulu p tvori končen obseg.
Nekatere lastnosti obsega $\mathbb{Z}_p$:

- za vsak $x \in \mathbb{Z}_p$, $x \neq 0$, obstaja aditivni inverz $p - x$ tako, da velja:

$$x + (p - x) = p \equiv 0 (mod\ p)$$

- za vsak $x \in \mathbb{Z}_p \backslash \{0\}$ obstaja multiplikativni inverz $\bar{x}$ tako, da velja:

$$x\ \bar{x} \equiv 1 (mod\ p)$$

Obseg praštevil

Če je p praštevilo, potem množica $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ skupaj z operacijama seštevanja in množenja po modulu p tvori končen obseg.
Nekatere lastnosti obsega $\mathbb{Z}_p$:

- za vsak $x \in \mathbb{Z}_p$, $x \neq 0$, obstaja aditivni inverz $p - x$ tako, da velja:

$$x + (p - x) = p \equiv 0 (mod\ p)$$

- za vsak $x \in \mathbb{Z}_p \backslash \{0\}$ obstaja multiplikativni inverz $\bar{x}$ tako, da velja:

$$x\ \bar{x} \equiv 1 (mod\ p)$$

- kvadrati v $x \in \mathbb{Z}_p$: $0^2, 1^2, 2^2, \ldots, h^2$ za $h = \lfloor p/2 \rfloor$) določajo različne elemente iz $\mathbb{Z}_p$

Lemi

Lema

Za praštevila oblike $p = 4m + 1$ *ima enačba* $s^2 \equiv -1 (mod\ p)$ *dve rešitvi* $s \in \{1, 2, \ldots, p-1\}$, *za* $p = 2$ *ima eno rešitev, za praštevila oblike* $p = 4m + 3$ *pa nima rešitve.*

Lemi

Lema

Za praštevila oblike $p = 4m + 1$ ima enačba $s^2 \equiv -1 (mod\ p)$ dve rešitvi $s \in \{1, 2, \ldots, p-1\}$, za $p = 2$ ima eno rešitev, za praštevila oblike $p = 4m + 3$ pa nima rešitve.

Lema

Nobeno število oblike $p = 4m + 3$ ni vsota dveh kvadratov.

Predstavljiva števila

Trditev

Vsako praštevilo oblike $p = 4m + 1$ *je predstavljivo.*

Predstavljiva števila

Trditev

Vsako praštevilo oblike $p = 4m + 1$ je predstavljivo.

Definicija

Involucija je bijektivna preslikava, ki je sama sebi inverz.
Natančneje, $f : S \to S$ je involucija, če za vsak $x \in S$ velja

$$f(f(x)) = x.$$

Predstavljiva števila

Trditev

Vsako praštevilo oblike $p = 4m + 1$ je predstavljivo.

Definicija

Involucija je bijektivna preslikava, ki je sama sebi inverz.
Natančneje, $f : S \to S$ je involucija, če za vsak $x \in S$ velja

$$f(f(x)) = x.$$

Zgledi

- *komplement na množicah*

Predstavljiva števila

Trditev

Vsako praštevilo oblike $p = 4m + 1$ je predstavljivo.

Definicija

Involucija je bijektivna preslikava, ki je sama sebi inverz.
Natančneje, $f : S \to S$ je involucija, če za vsak $x \in S$ velja

$$f(f(x)) = x.$$

Zgledi

- *komplement na množicah*
- *zrcaljenje preko točke*

Predstavljiva števila

Trditev

Vsako praštevilo oblike $p = 4m + 1$ je predstavljivo.

Definicija

Involucija je bijektivna preslikava, ki je sama sebi inverz.
Natančneje, $f : S \to S$ je involucija, če za vsak $x \in S$ velja

$$f(f(x)) = x.$$

Zgledi

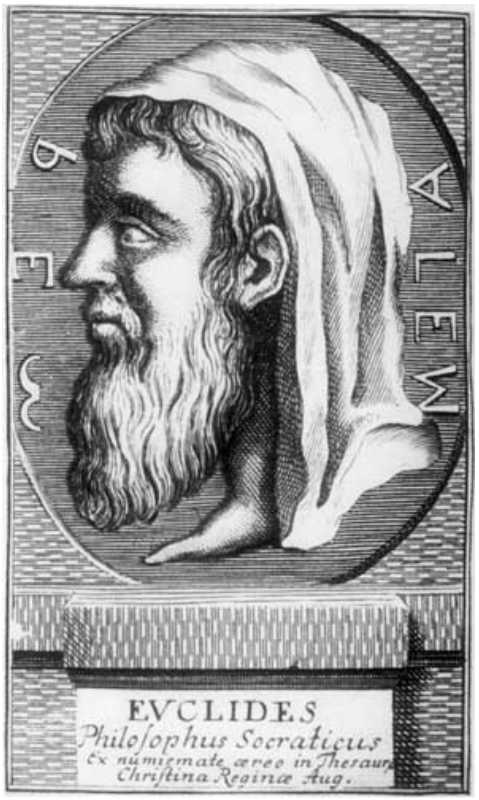
- *komplement na množicah*
- *zrcaljenje preko točke*
- *zrcaljenje preko premice*

Glavni izrek

Izrek

Naravno število n je predstavljivo natanko tedaj, ko se vsak praštevilski faktor oblike $p = 4m + 3$ pojavi s sodim eksponentom v praštevilski faktorizaciji števila n.

Katerim matematikom naj bomo hvaležni za odgovor na današnje vprašanje?



Euclid (cca. 325 - 265)



Pierre de Fermat (1601 - 1665)

Katerim matematikom naj bomo hvaležni za odgovor na današnje vprašanje?



Leonhard Euler (1707 - 1783)



Johann Peter Gustav Lejeune Dirichlet (1805 - 1859)

Katerim matematikom naj bomo hvaležni za odgovor na današnje vprašanje?



Axel Thue (1863 - 1922)



G. H. Hardy (1877 - 1947)

Katerim matematikom naj bomo hvaležni za odgovor na današnje vprašanje?



Don Zagier (1951)



Roger Heath - Brown