Zakaj je praštevil neskončno mnogo

Jaka Gogala

Fakulteta za matematiko in fiziko
Oddelek za matematiko

6. marec 2009

Praštevila

Definicija

Število $p \in \mathbb{N}$ je praštevilo, če ima natanko dva delitelja.
Množico praštevil označimo s $\mathbb{P}$.

Praštevila

Definicija

Število $p \in \mathbb{N}$ je praštevilo, če ima natanko dva delitelja.
Množico praštevil označimo s $\mathbb{P}$.

Posledica

- *Število 1 ni praštevilo.*
- *Če je $p \in \mathbb{N}$ od 1 različno število, je praštevilo natanko tedaj, ko je deljivo le z 1 in samim sabo.*

Praštevila

Definicija

Število $p \in \mathbb{N}$ je praštevilo, če ima natanko dva delitelja.
Množico praštevil označimo s $\mathbb{P}$.

Posledica

- *Število 1 ni praštevilo.*
- *Če je $p \in \mathbb{N}$ od 1 različno število, je praštevilo natanko tedaj, ko je deljivo le z 1 in samim sabo.*

Izrek

Praštevil je neskončno mnogo.

Dokaz s pomočjo Fermatovih števil

Definicija

$F_n = 2^{2^n} + 1$ *je n-to Fermatovo število, kjer je* $n \in \mathbb{N} \cup \{0\}$

Dokaz s pomočjo Fermatovih števil

Definicija

$F_n = 2^{2^n} + 1$ *je n-to Fermatovo število, kjer je* $n \in \mathbb{N} \cup \{0\}$

Zgledi

$F_0 = 3$ $\quad F_3 = 257$

$F_1 = 5$ $\quad F_4 = 65.537$

$F_2 = 17$ $\quad F_5 = 4.294.967.297$

Dokaz s pomočjo Fermatovih števil

Definicija

$F_n = 2^{2^n} + 1$ *je n-to Fermatovo število, kjer je* $n \in \mathbb{N} \cup \{0\}$

Zgledi

$F_0 = 3$ $\quad F_3 = 257$

$F_1 = 5$ $\quad F_4 = 65.537$

$F_2 = 17$ $\quad F_5 = 4.294.967.297 = 641 \cdot 6.700.417$

Dokaz s pomočjo Fermatovih števil

Definicija

$F_n = 2^{2^n} + 1$ *je n-to Fermatovo število, kjer je* $n \in \mathbb{N} \cup \{0\}$

Zgledi

$F_0 = 3$ $\quad F_3 = 257$

$F_1 = 5$ $\quad F_4 = 65.537$

$F_2 = 17$ $\quad F_5 = 4.294.967.297 = 641 \cdot 6.700.417$

Lema

$$\forall n \geq 1 : \prod_{k=0}^{n-1} F_k = F_n - 2$$

Dokaz s pomočjo algebre

Definicija

$M_n = 2^n - 1$ *je n-to Mersennovo število, kjer je* $n \in \mathbb{N}$

Dokaz s pomočjo algebre

Definicija

$M_n = 2^n - 1$ je n-to Mersennovo število, kjer je $n \in \mathbb{N}$

Izrek

(Lagrangev izrek) Če je G končna grupa in U njena podgrupa velja:

$$|U| \mid |G|$$

Posledica

Red vsakega elementa poljubne končne grupe deli moč grupe.

Dokaz s pomočjo topologije

Trditev

Naj bo za poljubna $a, b \in \mathbb{Z} : N_{a,b} = \{a + nb; n \in \mathbb{Z}\}$. *In naj bo:*

$$\mathcal{O} = \{U \subset \mathbb{Z}; \forall a \in U \exists b \in \mathbb{N} : N_{a,b} \subset U\} \cup \{\emptyset\}$$

Tedaj je $\mathcal{O}$ *topologija na množici celih števil.*

Dokaz s pomočjo topologije

Trditev

Naj bo za poljubna $a, b \in \mathbb{Z} : N_{a,b} = \{a + nb; n \in \mathbb{Z}\}$. *In naj bo:*

$$\mathcal{O} = \{U \subset \mathbb{Z}; \forall a \in U \exists b \in \mathbb{N} : N_{a,b} \subset U\} \cup \{\emptyset\}$$

Tedaj je $\mathcal{O}$ *topologija na množici celih števil.*

Trditev

- *Vsaka neprazna odprta množica je neskončna.*

Dokaz s pomočjo topologije

Trditev

Naj bo za poljubna $a, b \in \mathbb{Z}$: $N_{a,b} = \{a + nb; n \in \mathbb{Z}\}$. *In naj bo:*

$$\mathcal{O} = \{U \subset \mathbb{Z}; \forall a \in U \exists b \in \mathbb{N} : N_{a,b} \subset U\} \cup \{\emptyset\}$$

Tedaj je $\mathcal{O}$ *topologija na množici celih števil.*

Trditev

- *Vsaka neprazna odprta množica je neskončna.*
- *Vsaka množica oblike* $N_{a,b}$ *je tudi zaprta.*

Erdősov dokaz

Izrek

Vsota

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

divergira.

Posledica

Praštevil je neskončno mnogo.