Praštevila in njihove lastnosti

Sara Bizjak

Fakulteta za matematiko in fiziko
Oddelek za matematiko

April 2018

- Odprta vprašanja
- Velika praštevila
- Eratostenovo rešeto

Definicija

Praštevilo je naravno število $n > 1$, če število n delita le števili 1 in n.

Izrek (Osnovni izrek aritmetike)

Vsako naravno število lahko na natanko en način zapišemo kot produkt samih praštevil. Takemu zapisu pravimo tudi razcep števila na prafaktorje.

Definicija

Naj bo $gcd(a, b)$ *največji skupni delitelj števil* a *in* b, *torej*

$$gcd(a, b) = max\{d \in \mathbb{N} : d|a \text{ in } d|b\},$$

razen če sta a *in* b *oba 0–tedaj velja* $gcd(0, 0) = 0$.

Zgled

- $gcd(1, 2) = 1$
- $gcd(5, 15) = 5$
- $gcd(6, 27) = 3$

Zgled

S pomočjo faktorizacije izračunajmo $gcd(2261, 1275)$.

Motivacija: Naj bosta $a, b \in \mathbb{Z}$, tako da $0 \leq r < |b|$ in $a = bq + r$.
To nas pripelje do Evklidovega algoritma.

Zgled

Izračunajmo $gcd(2261, 1275)$ *še s pomočjo Evklidovega algoritma.*

Lema

Za $a, b, n \in \mathbb{Z}$ *velja:*

$$gcd(an, bn) = gcd(a, b) \cdot |n|$$

Lema

Naj bodo $a, b, n \in \mathbb{Z}$ *in naj* $n|a$ *in* $n|b$. *Tedaj* $n|gcd(a, b)$.

Izrek

Naj bo $p \in \mathbb{P}$ in $a, b \in \mathbb{N}$. Če $p|ab$, potem $p|a$ ali $p|b$.

- Ključ pri dokazu osnovnega izreka aritmetike.

DOKAZ OSNOVNEGA IZREKA ARITMETIKE

Motivacija:

$$3 = 2 + 1$$

$$7 = 2 \cdot 3 + 1$$

$$31 = 2 \cdot 3 \cdot 5 + 1$$

$$211 = 2 \cdot 3 \cdot 5 \cdot 7 + 1$$

$$2311 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$$

Trditev

Obstaja neskončno mnogo praštevil.

Dokazi: Evklidov, Euler, Polyajev, Kummer,...

- Smiselno vprašanje o največjih praštevilih.
- Največje poznano praštevilo je $2^{74207281} - 1$ in ima več kot 22 milijonov mest.

Praštevila oblike $ax + b$

- Zapišimo prvih nekaj števil oblike $4x - 1$.

Izrek

Obstaja neskončno praštevil oblike $4x - 1$.

Izrek

Naj bosta a *in* b *taki celi števili, da* $\gcd(a, b) = 1$. *Tedaj obstaja neskončno mnogo praštevil oblike* $ax + b$.

- Gostota praštevil v naravnih številih
- $\pi(x) = \#\{p \in \mathbb{N} : p \leq x, \ \textit{kjer } p \in \mathbb{P}\}$

Izrek

Funkcija $\pi(x)$ *je asimptotična funkciji* $\frac{x}{\log(x)}$, *tako da*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} = 1.$$

x	$\pi(x)$	$\frac{x}{\log(x)-1}$ (aproksimacija)
1000	168	169,269029060440816578625 6278
2000	303	302,988873454546387802980 0994
3000	430	428,181931797523704374738 5740
4000	550	548,392209727825326413340 0985
5000	669	665,141878448650217236945 5815
6000	783	779,269888585477862686367 7374
7000	900	891,303565722333997435256 7759
8000	1007	1001,602962794770080754784281
9000	1117	1110,428422963188172310675011
10000	1229	1217,976301461550279200775705

Tabela: Primerjava $\pi(x)$ in $\frac{x}{\log(x)-1}$

- Največja znana praštevila nekoč in danes
- Praštevilski dvojčki
- Kriptografija