Porazdelitev praštevil

Matevž Miščič

Fakulteta za matematiko in fiziko

21. 8. 2023

Praštevila

Definicija

Praštevilo *je naravno število, ki ima natanko dva delitelja.*
Naravno število, ki ima vsaj tri delitelje, imejujemo ***sestavljeno število****.*

Praštevila

Definicija

Praštevilo *je naravno število, ki ima natanko dva delitelja.*
Naravno število, ki ima vsaj tri delitelje, imejujemo ***sestavljeno število****.*

Zgled

Prvih nekaj praštevil je $2, 3, 5, 7, 11, 13, \ldots$.
Število 6 je sestavljeno število, ker ima štiri delitelje: $1, 2, 3, 6$.

Trditev

Vsako naravno število, večje od 1*, se da zapisati kot produkt števil.*

Trditev

Vsako naravno število, večje od 1*, se da zapisati kot produkt števil.*

Trditev

Praštevil je neskončno mnogo.

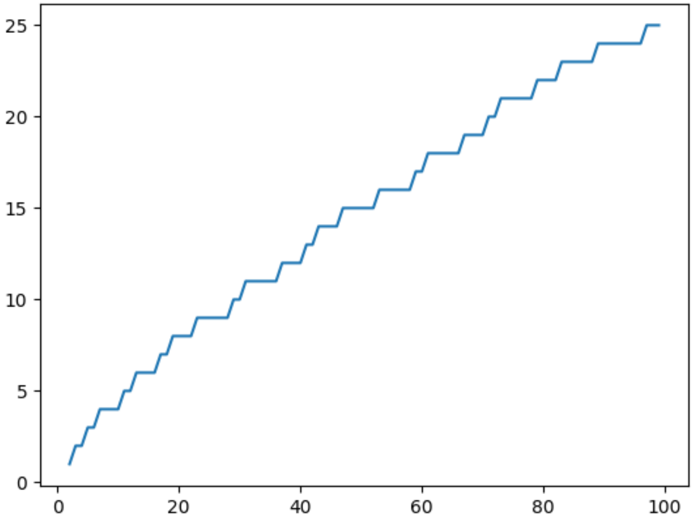
Praštevilski izrek

Med večjimi števili so praštevila bolj redka.

Definicija

Za naravno število $n \in \mathbb{N}$ s $\pi(n)$ označimo število praštevil manjših ali enakih n.

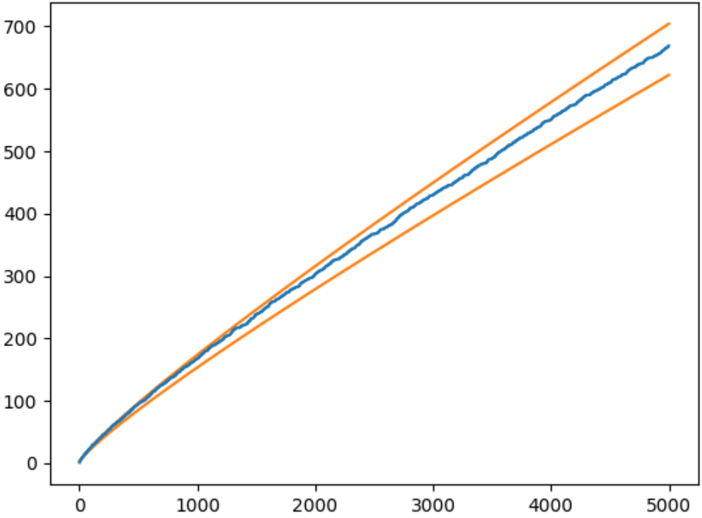
Zanima nas, kako raste funkcija π.


25
20
15
10
5
0
0
20
40
60
80
100

Izrek (Čebišov)

Obstajata pozitivni realni števili $A, B > 0$, da za vsak $n \in \mathbb{N}$ velja

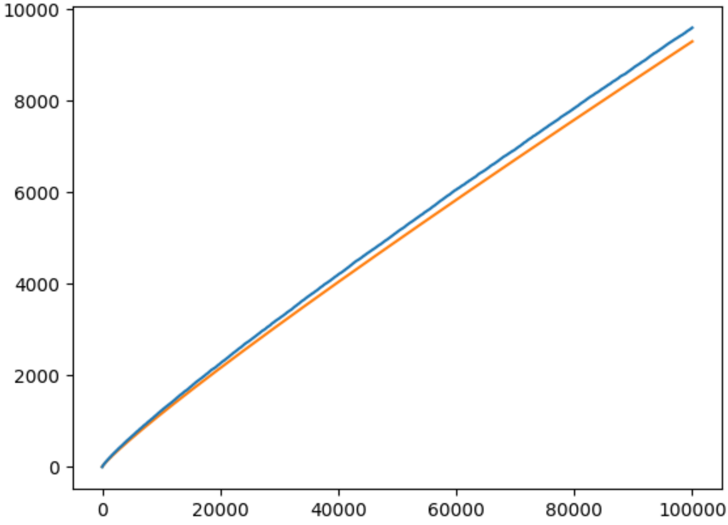
$$A\frac{n}{\log n} < \pi(n) < B\frac{n}{\log n}.$$


0
100
200
300
400
500
600
700
0
1000
2000
3000
4000
5000

Izrek (Praštevilski izrek)

Velja

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


10000
8000
6000
4000
2000
0
0
20000
40000
60000
80000
100000

Praštevila v aritmetičnih zaporedjih

Izrek (Dirichlet)

Naj bosta $a, b \in \mathbb{N}$ *tuji si števili. Potem je med členi zaporedja* $an + b, n \in \mathbb{N}$ *neskončno praštevil.*

Praštevila v aritmetičnih zaporedjih

Izrek (Dirichlet)

Naj bosta $a, b \in \mathbb{N}$ tuji si števili. Potem je med členi zaporedja $an + b, n \in \mathbb{N}$ neskončno praštevil.

Zgled

Če je $a = 3$ in $b = 6$, dobimo aritmetično zaporedje $9, 12, 15, 18, 21, 24, \ldots$. V tem zaporedju so vsi členi deljivi s 3, ki je največji skupni delitelj a in b. Če je $a = 8$ in $b = 3$, dobimo zaporedje

$11, 14, 17, 20, 23, 26, 29, \ldots$. Od tega so $11, 17, 23, 29$ praštevila. Po Dirichletovem izreku obstaja neskončno praštevilskih členov tega zaporedja.

Trditev

Med števili oblike $6n + 5$ je neskončno praštevil.

Razmaki med praštevili

Trditev

Obstajajo poljubno veliki bloki zaporednih naravnih števil, ki so vsa sestavljena števila.

Po praštevilskem izreku je povprečen razmak med preštevili manjšimi od n približno $\log n$. Razmaki torej postajajo vse večji.

Definicija

Praštevilski dvojček *je par praštevil* (p, q)*, za katerega velja* $q - p = 2$.

Definicija

Praštevilski dvojček *je par praštevil* (p, q)*, za katerega velja* $q - p = 2$.

Zgled

Primeri praštevilskih dvojčkov so $(3, 5), (5, 7), (9, 11), (11, 13)$.

Definicija

Praštevilski dvojček *je par praštevil* (p, q)*, za katerega velja* $q - p = 2$*.*

Zgled

Primeri praštevilskih dvojčkov so $(3, 5), (5, 7), (9, 11), (11, 13)$.

Domneva

Ali obstaja neskončno praštevilskih dvojčkov?

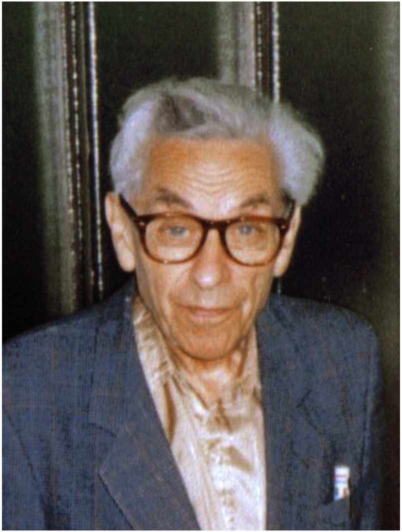
Bertrandov postulat

Izrek

Za vsako naravno število $n \in \mathbb{N}$ *obstaja praštevilo* p *za katero velja* $n \leq p \leq 2n$.

Izrek je prvi dokazal Pafnuti Čebišov leta 1850, mi pa si bomo ogledali enostavnejši dokaz, ki ga je podal Paul Erdős leta 1932.

Paul Erdős



Definicija

Centralni binomski koeficient *je število*

$$C_n = \binom{2n}{n} = \frac{(2n)!}{n!^2}.$$

Definicija

Centralni binomski koeficient *je število*

$$C_n = \binom{2n}{n} = \frac{(2n)!}{n!^2}.$$

Lema 1

Za vsako naravno število n velja $\frac{4^n}{2n} \leq C_n$.

Definicija

Centralni binomski koeficient *je število*

$$C_n = \binom{2n}{n} = \frac{(2n)!}{n!^2}.$$

Lema 1

Za vsako naravno število n *velja* $\frac{4^n}{2n} \leq C_n$.

Lema 2

Za vsako naravno število $n \in \mathbb{N}$ *za praštevilski razcep* $C_n = p_1^{a_1} \cdots p_r^{a_r}$ *velja* $p_i^{a_i} \leq 2n$ *za vsak* $i = 1, \ldots, r$.

Lema 3

Za vsako naravno število $n \in \mathbb{N}$ in praštevilo $p \neq 2$ z $\frac{2n}{3} < p < n$ velja, da p ne deli C_n.

Lema 3

Za vsako naravno število $n \in \mathbb{N}$ *in praštevilo* $p \neq 2$ *z* $\frac{2n}{3} < p < n$ *velja, da* p *ne deli* C_n.

Definicija

Za naravno število $n \in \mathbb{N}$ *definirajmo* n***-to primorielo*** *kot produkt vseh praštevil manjših ali enakih* n *in jo označimo z* $n\#$.

Lema 3

Za vsako naravno število $n \in \mathbb{N}$ *in praštevilo* $p \neq 2$ *z* $\frac{2n}{3} < p < n$ *velja, da* p *ne deli* C_n.

Definicija

Za naravno število $n \in \mathbb{N}$ *definirajmo* n***-to primorielo*** *kot produkt vseh praštevil manjših ali enakih* n *in jo označimo z* $n\#$.

Lema 4

Za vsako naravno število $n \in \mathbb{N}$ *velja* $n\# < 4^n$.