Vzorci praštevil

Primož Moravec

Moderni izzivi poučevanja matematike

Ljubljana, 30. januar 2015

Praštevila

Naravno število $n > 1$ je **praštevilo**, če je deljivo le z 1 in n.

Množica praštevil:

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, \ldots\}.$$

Elementom množice

$$\mathbb{N} \setminus (\mathbb{P} \cup \{1\}) = \{4, 6, 8, 9, 10, 12, 14, 15 \ldots\}$$

pravimo **sestavljena števila**.

Izrek (Izrek o enolični faktorizaciji)

Vsako sestavljeno število n je produkt praštevil. Pri tem so praštevila, ki nastopajo v razcepu števila n, do vrstnega reda enolično določena.

Recimo, da je množica $\mathbb{P}$ končna, torej

$$\mathbb{P} = \{p_1, p_2, \dots, p_k\}.$$

Oglejmo si število

$$n = p_1 \cdot p_2 \cdots p_k + 1.$$

Po predpostavki je $n \neq p_i$ za vsak $i = 1, 2, \dots, k$, zato je n sestavljeno število.

Torej je število n deljivo z nekim praštevilom p_j, kar pa ni res.

Prišlo smo v protislovje s predpostavko, da je množica $\mathbb{P}$ končna.

Nekaj vprašanj

1. Posebni tipi praštevil?
2. Kako preverimo, ali je dano naravno število praštevilo?
3. Naj bo $x \in \mathbb{N}$. Koliko je praštevil v množici $\{1, 2, \ldots, x\}$?
4. Kaj lahko povemo o razlikah med sosednjimi praštevili?

Posebni tipi praštevil

Mersennova praštevila
Marin Mersenne, 1588 – 1648

Definicija

Praštevilom oblike

$$M_n = 2^n - 1$$

pravimo **Mersennova praštevila**.

n	M_n
1	1
2	3
3	7
4	15
5	31
6	63
7	127

Trditev

Če je n sestavljeno število, je tudi M_n sestavljeno število.

Dokaz.

$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$. $\square$

Obratna trditev ne velja, saj je

$$M_{11} = 2047 = 23 \cdot 89.$$

Domneva (Lenstra-Pomerance-Wagstaffova domneva)

Mersennovih praštevil neskončno mnogo.

Prvih deset največjih znanih praštevil je Mersennovih; največje do sedaj znano praštevilo je $M_{57.885.161}$. Ima 17.425.170 števk.

Fermatova praštevila

Pierre de Fermat, 1601 – 1665

Definicija

Praštevilom oblike

$$F_n = 2^{2^n} + 1$$

pravimo **Fermatova praštevila**.

n	F_n
0	3
1	5
2	17
3	257
4	65537

- Fermat je domneval, da so vsa števila F_n praštevila.
- Euler je pokazal, da je $F_5 = 4294967297 = 641 \cdot 6700417$.

Fermatova praštevila

Domneva (Eisenstein, 1844)

Fermatovih praštevil je neskončno mnogo.

- F_0, F_1, F_2, F_3 in F_4 so do sedaj edina znana Fermatova praštevila.
- Do sedaj je znano, da so $F_5, F_6, \ldots, F_{32}$ sestavljena števila.

Praštevilski testi

Preverjanje praštevilskosti

Trditev

Naj bo $n > 1$ naravno število. Če n ni deljiv z nobenim naravnim številom k, za katerega velja $1 < k \leq \sqrt{n}$, potem je n praštevilo.

Dokaz.

Recimo, da je n sestavljeno število. Potem je

$$n = xy,$$

kjer sta $x, y \in \mathbb{N}$, $x > 1$, $y > 1$. Po predpostavki velja $x > \sqrt{n}$ in $y > \sqrt{n}$. Toda potem dobimo

$$n = xy > \sqrt{n} \cdot \sqrt{n} = n,$$

kar je v protislovju s predpostavko. $\square$

Eratostenovo rešeto

Eratosten, 276 – 195/194 pr. n. št.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Praštevila med 1 in 100 so: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Nekaj praštevilskih testov

Izrek (Wilson)

Naravno število p je praštevilo natanko tedaj, ko velja

$$(p-1)! \equiv -1 \mod p.$$

Ta test je neučinkovit za velika števila.

Bolj uporaben je naslednji šibkejši rezultat:

Izrek (Mali Fermatov izrek)

Naj bo a naravno število in p praštevilo. Potem je

$$a^p \equiv a \mod p.$$

Če sta a in p tuji števili, velja $a^{p-1} \equiv 1 \mod p$.

Obrat ne velja; 341 je sestavljeno število $(341 = 11 \cdot 31)$ in $2^{340} \equiv 1 \mod 341$.

Fermatov praštevilski test

- **Vhod:** Število n, za katerega preverjamo, ali je praštevilo, in število korakov k.
- **Izhod:** `sestavljeno število`, če se izkaže, da za n to velja, sicer pa `verjetno praštevilo`.

Algoritem

Naslednja koraka ponovimo k-krat:

1. Naključno izberemo $a \in \{1, 2 \dots, n-1\}$;
2. Če $a^{n-1} \not\equiv 1 \mod n$, vrnemo `sestavljeno število` in končamo postopek.

Če po k korakih ne končamo, vrnemo `verjetno praštevilo`.

V praksi se Fermatov test uporablja v kombinaciji z drugimi praštevilskimi testi, da lahko z dovolj veliko verjetnostjo ugotovimo, ali je dano število praštevilo.

AKS praštevilski test

Leta 2002 so Agrawal, Kayal in Saxena iznašli determinističen algoritem, ki v **polinomskem času** ugotovi, ali je dano število praštevilo ali sestavljeno število. Algoritem temelji na naslednjem rezultatu, ki je posplošitev malega Fermatovega izreka:

Izrek

Naravno število $n \geq 2$ je praštevilo natanko tedaj, ko so vsi koeficienti polinoma

$$(x-1)^n - (x^n - 1)$$

deljivi z n.

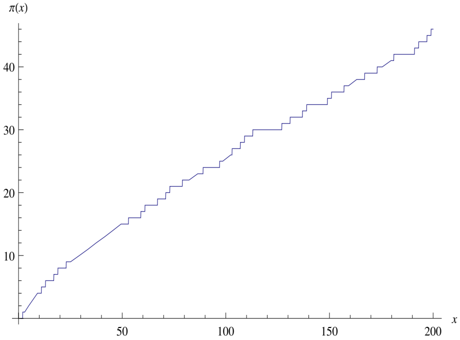
Primer: $n = 7$ in $n = 6$

- $(x-1)^7 - (x^7 - 1) = -7x^6 + 21x^5 - 35x^4 + 35x^3 - 21x^2 + 7x$,
- $(x-1)^6 - (x^6 - 1) = -6x^5 + 15x^4 - 20x^3 + 15x^2 - 6x + 2$.

Koliko je praštevil?

Število praštevil v množici $\{1, 2, \ldots, x\}$

Za realno število x naj bo $\pi(x)$ število praštevil, ki so manjša ali kvečjemu enaka x.



Bertrandov postulat

Bertrandov postulat (Bertrand, 1845)

Za vsako naravno število x obstaja vsaj eno praštevilo med številoma x in $2x$.

Veljavnost Bertrandovega postulata je dokazal Čebišev leta 1852.

Bertrandov rezultat implicira

$$\pi(2x) - \pi(x) \geq 1.$$

Asimptotsko obnašanje $\pi(x)$

Za realni funkciji f in g pišemo $f(x) \sim g(x)$, kadar je $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Na osnovi **Vegovih tabel** Je Legendre leta 1797 domneval, da je

$$\pi(x) \sim \frac{x}{A\ln x + B}$$

za primerni konstanti A in B.

Izrek (Izrek o praštevilih)

$$\pi(x) \sim \frac{x}{\ln x}.$$

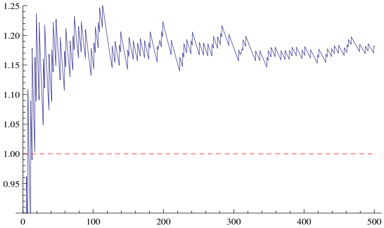
Izrek je dokazal Hadamard leta 1896 s pomočjo analitičnih orodij, ki jih bomo opisali kasneje.

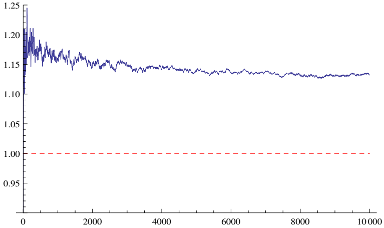
Grafični prikaz asimptotike

Kvocient

$$\frac{\pi(x)}{\frac{x}{\ln x}}$$

se razmeroma počasi bliža proti 1:





Nekaj posledic izreka o praštevilih

Verjetnost, da med prvimi x naravnimi števili naključno izberemo praštevilo, je

$$\frac{\pi(x)}{x}.$$

Posledica

Po izreku o praštevilih je

$$\frac{\pi(x)}{x} \sim \frac{1}{\ln x}.$$

Posledica

Če je p_n n-to praštevilo, je

$$p_n \sim n \ln n.$$

Goldbachova domneva in izrek o praštevilih

Christian Goldbach, 1690 – 1764

Domneva (Goldbachova domneva)

Vsako sodo število, večje kot 2, je vsota dveh praštevil.

- $100 = 3+97 = 11+89 = 17+83 = 29+71 = 41+59 = 47+53$
- Do sedaj preverjena za števila $\leq 4 \cdot 10^{18}$.

Izrek (Helfgott, 2013)

Vsako liho število, večje od 5, je vsota treh praštevil.

Površen argument, zakaj bi morala domneva veljati

Naj bo n veliko sodo število.
Naj bo m naravno število med 3 in $n/2$. Verjetnost, da je m praštevilo, je po **izreku o praštevilih** približno enaka

$$\frac{1}{\ln m}.$$

$n = m + (n - m)$; verjetnost, da sta m in $n - m$ hkrati praštevili, je približno (napačen sklep!)

$$\frac{1}{\ln m \cdot \ln(n-m)}.$$

Okvirno število načinov, kako lahko n zapišemo kot vsoto dveh praštevil, je

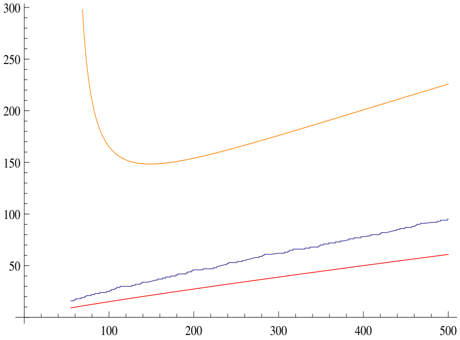
$$\sum_{m=3}^{n/2} \frac{1}{\ln m \cdot \ln(n-m)} \approx \frac{n}{2\ln^2 n} \xrightarrow[n\to\infty]{} \infty.$$

Zgornja in spodnja meja za $\pi(x)$

Izrek (Dussart, 1998)

Za $x \geq 55$ velja ocena

$$\frac{x}{\ln x + 2} \leq \pi(x) \leq \frac{x}{\ln x - 4}.$$

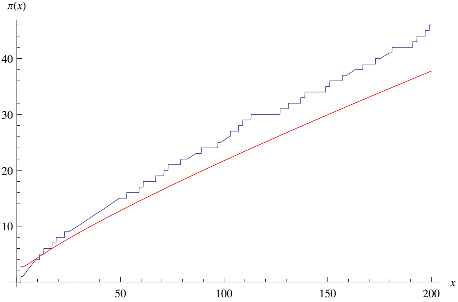


Dejanska odstopanja $\pi(x)$ od $\frac{x}{\ln x}$

Absolutna napaka

$$|\pi(x) - x/\ln x|$$

se z x veča:



Ali ima kakšna druga funkcija, ki opisuje porazdelitev praštevil, boljše asimptotsko obnašanje?

Izkaže se, da je vprašanje tesno povezano z **Riemannovo zeta funkcijo**.

Definicija

Riemannova zeta funkcija *je funkcija* $\zeta : \mathbb{C} \to \mathbb{C}$, *definirana s predpisom*

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n=1}^{\infty} n^{-s}.$$

Pri tem so potence s kompleksnim eksponentom $s = x + yi$ definirane preko

$$\begin{aligned} n^{-s} &= e^{s \ln n^{-1}} \\ &= e^{x \ln n^{-1}} \cdot e^{iy \ln n^{-1}} \\ &= n^{-x} \cdot (\cos(y \ln n^{-1}) + i \sin(y \ln n^{-1})). \end{aligned}$$

Konvergenca Riemannove zeta funkcije

Trditev

Vrsta $\zeta(s)$ *konvergira za* $\operatorname{Re} s > 1$.

Dokaz.

Naj bo $s = x + yi$. Oglejmo si

$$\sum_{n=1}^{\infty} |n^{-s}| = \sum_{n=1}^{\infty} n^{-x} |\cos(y \ln n^{-1}) + i \sin(y \ln n^{-1})| = \sum_{n=1}^{\infty} n^{-x}.$$

Ta vrsta konvergira za $x > 1$, torej vrsta $\zeta(s)$ absolutno konvergira in zato konvergira za $x > 1$. $\square$

Vrsta $\zeta(1) = 1 + 1/2 + 1/3 + \cdots$ divergira, zato je rezultat najboljši možen.

Analitično nadaljevanje funkcije ζ

Vemo že, da vrsta $\zeta(s)$ konvergira, če je $\operatorname{Re} s > 1$.

Izkaže se, da obstaja analitična funkcija, definirana na $\mathbb{C} \setminus \{1\}$, ki se za $\operatorname{Re} s > 1$ ujema z $\zeta(s)$. Razširjeno funkcijo označimo zopet s $\zeta(s)$.

Ta funkcija zadošča funkcionalni enačbi

$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2) \Gamma(1-s) \zeta(1-s),$$

kjer je $\Gamma(s)$ kompleksna gama funkcija, ki ima enostavne pole pri $s = -n$, $n \in \mathbb{N} \cup \{0\}$.

$\zeta(s)$ ima analitično nadaljevanje na $\mathbb{C} \setminus \{1\}$; v $s = 1$ je pol prve stopnje.

Izrek (Euler)

Naj bo $\operatorname{Re} s > 1$. *Potem je*

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Ideja dokaza je podobna kot pri Eratostenovemu rešetu.

Dokaz Eulerjevega izreka

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} \cdots$$

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} \cdots$$

Odštejemo obe enačbi:

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \cdots .$$

Pomnožimo rezultat s 3^{-s}:

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \cdots .$$

Odštejemo to od prejšnje vrste:

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \cdots .$$

Nadaljevanje dokaza Eulerjevega izreka

„Eratostenovo rešeto" za zeta funkcijo

- $\left(1-\frac{1}{2^s}\right)\zeta(s)$ v vrsti za $\zeta(s)$ eliminira vse $1/n^s$, kjer so n večkratniki števila 2.
- $\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)$ v vrsti za $\left(1-\frac{1}{2^s}\right)\zeta(s)$ eliminira vse $1/n^s$, kjer so n preostali večkratniki števila 3.
- $\dots$

Dobimo

$$\cdots\left(1-\frac{1}{11^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s)=1.$$

Od tod hitro sledi Eulerjev izrek:

$$\zeta(s)=\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1}.$$

Eulerjev izrek

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Izračunajmo desno limito na obeh straneh, ko $s \to 1+$:

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right)^{-1} = \infty,$$

od tod pa sledi, da mora biti praštevil neskončno mnogo.

Izrek o praštevilih in funkcija ζ

Izrek o praštevilih: $\pi(x) \sim x/\ln x$.

Večina klasičnih dokazov Izreka o praštevilih si pomaga s tem, da oceni, kje ima Riemannova funkcija ζ ničle.

Vprašanje za milijon dolarjev

Kje so ničle Riemannove zeta funkcije?

Položaj ničel funkcije ζ

$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2) \Gamma(1-s) \zeta(1-s)$$

Zaradi te zveze ničle iščemo v polravnini $\operatorname{Re} s \leq 1$.

Recimo, da je $\operatorname{Re} s < 0$. Kdaj je desna stran enaka 0?

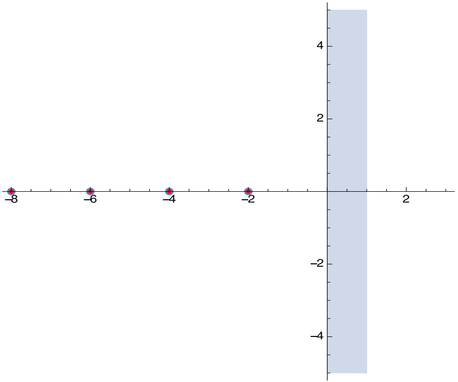
1. $\sin(\pi s/2) = 0$ za $s = -2, -4, -6, \ldots$.
2. $\Gamma(1-s)$ ni nikoli 0.
3. Ker $\ln \zeta(1-s)$ konvergira, $\zeta(1-s) \neq 0$.

Sklep

Za ničle funkcije $\zeta(s)$ velja ena od možnosti:

- $s \in \{-2, -4, -6, \ldots\}$ (**trivialne ničle**),
- $0 \leq \operatorname{Re} s \leq 1$ (**kritični pas**).

Ničle funkcije ζ

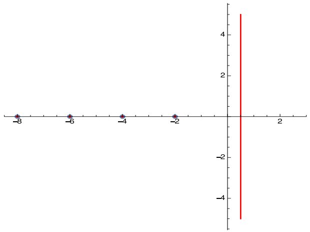


V Hadamardovem dokazu izreka o praštevilih je ključni korak dokaz dejstva, da je $\zeta(s) \neq 0$ za $\operatorname{Re} s = 1$.

Domneva (Riemannova hipoteza; Riemann, 1859)

Za **netrivialne ničle** *funkcije* $\zeta(s)$ *velja*

$$\operatorname{Re} s = \frac{1}{2}.$$



Za netrivialne ničle je znano, da:

- jih je neskončno mnogo;
- nastopajo simetrično glede na realno os;
- nastopajo simetrično glede na premico $\operatorname{Re} s = 1/2$.

Funkcija ψ

Ideja

Funkcijo $\pi(x)$ si lahko predstavljamo na naslednji način:

- Vsako praštevilo $p \leq x$ da „signal" 1;
- $\pi(x)$ je vsota teh signalov.

Izkaže se, da je bolje signale „utežiti" glede na velikost praštevil.

Funkcija ψ

- Za realno število x poiščemo vse praštevilske potence p^n, ki so kvečjemu x;
- Vsaka od teh potenc naj da „signal" velikosti $\ln p$;
- Zanima nas vsota vseh takšnih signalov.

$$\psi(x) = \sum_{p^n \leq x} \ln p.$$

Primer

Primer: $\psi(24)$

Praštevilske potence, ki so kvečjemu 24, so:

$$2, 2^2, 2^3, 2^4, 3, 3^2, 5, 7, 11, 13, 17, 19, 23.$$

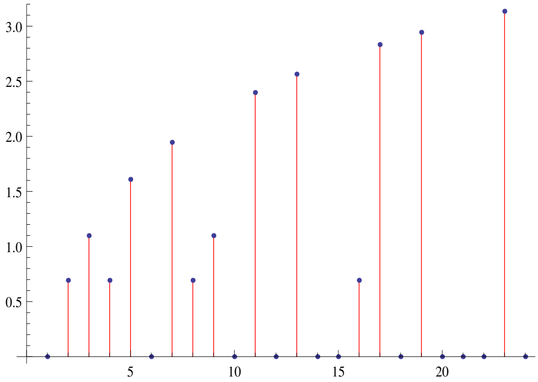
Zato je

$$\begin{aligned}
\psi(24) &= 4\ln 2 + 2\ln 3 + \ln 5 + \ln 7 + \ln 11 + \ln 13 + \ln 17 + \\
&\quad + \ln 19 + \ln 23 \\
&= \ln 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \\
&= \ln v(1, 2, 3, \ldots, 24) \\
&\approx 22,4012.
\end{aligned}$$

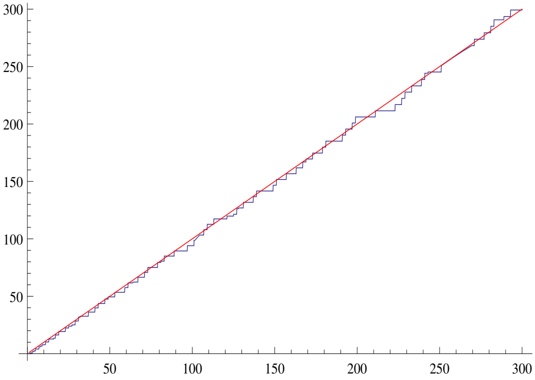
V splošnem za $x \in \mathbb{N}$ velja

$$\psi(x) = \ln v(1, 2, \ldots, x).$$

Signali, ki definirajo $\psi(24)$



Graf funkcije ψ



Posledica izreka o praštevilih je

$$\psi(x) \sim x.$$

Kako dobra je ta aproksimacija?

Funkcija ψ in ničle Riemannove funkcije ζ

Definirajmo

$$\psi_0(x) = \begin{cases} \psi(x) & : \quad \psi \text{ zvezna v } x \\ \frac{\psi(x^-)+\psi(x^+)}{2} & : \quad \text{sicer} \end{cases}$$

Potem velja

$$\psi_0(x) = x - \ln(2\pi) - \frac{1}{2}\ln\left(1 - \frac{1}{x^2}\right) + \sum_{\rho} \frac{x^{\rho}}{\rho},$$

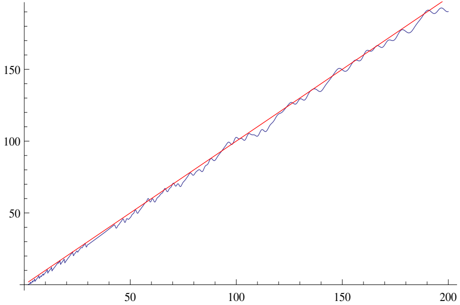
kjer ρ preteče množico netrivialnih ničel funkcije ζ.

Izkaže se:

Če Riemannova hipoteza velja, potem:

- je funkcija $\psi(x)$ zelo blizu $f(x) = x$.
- dobimo boljšo asimptotsko oceno $\pi(x)$.

Aproksimacija, pri kateri vzamemo prvih 100 ničel funkcije ζ s pozitivnim imaginarnim delom in njihove konjugiranke:



Razlike med sosednjimi praštevili

Praštevilski dvojčki

Definicija

Par praštevil oblike $(p, p+2)$ *imenujemo* **praštevilski dvojček**.

2, 3, 5, 7,11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971,...

Domneva in vprašanja

Domneva (Hardy – Littlewoodova domneva)

Praštevilskih dvojčkov je neskončno mnogo.

Izrek (Clement, 1919)

Par $(n, n+2)$ *je praštevilski dvojček natanko tedaj, ko je*

$$4((n-1)!+1) \equiv -n \mod n(n+2).$$

Nekaj vprašanj

- Kako je s praštevilskimi pari oblike $(p, p+d)$?
- Par $(p, p+d)$ lahko gledamo kot prva dva člena aritmetičnega zaporedja
$$p + nd,$$
kjer $n = 0, 1, 2, \ldots$. Kako je s praštevili, ki nastopajo v aritmetičnih zaporedjih?

Izrek (Dirichletov izrek)

Naj bosta a in d tuji števili. Potem v aritmetičnem zaporedju

$$a + nd,\ n = 0, 1, 2, \ldots$$

nastopa neskončno mnogo praštevil.

Izrek se dokaže s pomočjo analitičnih orodij.

Seveda lahko v takšnem zaporedju nastopajo tudi sestavljena števila.

Ali obstajajo poljubno dolga aritmetična zaporedja, sestavljena iz samih praštevil?

Green – Taov izrek

Izrek (Green, Tao, 2004)

Množica praštevil, urejena po velikosti, vsebuje poljubno dolga aritmetična zaporedja.

Numeričen rezultat; Perichon, 2010

Prvih 26 členov zaporedja

$$43.142.746.595.714.191 + 23.681.770 \cdot 223.092.870n$$

so praštevila.

Green in Tao sta pokazala, da obstaja k-členo aritmetično zaporedje samih različnih praštevil, kjer so vsi členi kvečjemu

$$2^{2^{2^{2^{2^{2^{2^{100k}}}}}}}.$$

Definicija

Magični kvadrat *je* $n \times n$ *tabela različnih števil, v kateri je vsota poljubne vrstice, stolpca in diagonale enaka neki konstanti.*

17	89	71
113	59	5
47	29	101

- Za vsak $n \geq 3$ obstaja magični kvadrat velikosti $n \times n$.
- Če je $M = [m_{ij}]$ magični kvadrat, je tudi $\bar{M} = [a + m_{ij}b]$ magični kvadrat.

Praštevila in magični kvadrati

Posledica Green–Taovega izreka je

Naj bo $M = [m_{ij}]$ poljuben magični kvadrat velikosti $n \times n$. Obstaja neskončno parov naravnih števil a in b, za katere so vsa števila

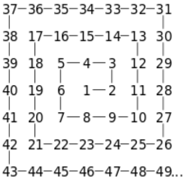
$$a + bd\ , \ \min m_{ij} \leq d \leq \max m_{ij}$$

praštevila. Obstaja torej neskončno mnogo $n \times n$ magičnih kvadratov, v katerih nastopajo sama praštevila.

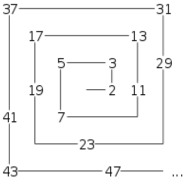
37	83	97	41
53	61	71	73
89	67	59	43
79	47	31	101

Ulamova spirala

Naravna števila napišemo v obliki spirale:



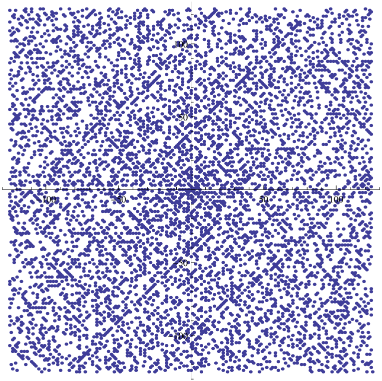
Ven izberemo le praštevila:



Ulam (1963) je opazil, da se veliko praštevil razvrsti po diagonalah.

Slika Ulamove spirale

Tudi za večji vzorec števil se pojavi podobna slika:



Ulamova spirala in Hardy-Littlewoodova domneva F

Izkaže se, da je Ulamova spirala v zvezi z naslednjim vprašanjem:

Naj bodo $a, b, c \in \mathbb{N}$. Koliko je praštevil oblike $F(n) = an^2 + bn + c$, ko n teče po množici naravnih števil?

- Če je $D = b^2 - 4ac$ popoln kvadrat, se izraz $F(n)$ da razstaviti in je zato skoraj vedno sestavljeno število.
- Če sta števili $a + b$ in c obe sodi, potem je $F(n)$ vedno sodo število:
  - Če je n sodo število, je $F(n)$ očitno sodo.
  - Če je $n = 2k + 1$, je $F(n) = n(2ak + a + b) + c$ sodo.

Domneva (Hardy–Littlewoodova domneva F)

Če izključimo zgornja dva primera, je med števili oblike $F(n) = an^2 + bn + c$ neskončno mnogo praštevil.

Pozitivna rešitev te domneve bi razložila diagonalne vzorce v Ulamovi spirali.

Skoki med praštevili

Zanimajo nas pari praštevil, katerih razlika je konstantna. Kako pogosto se pojavljajo?

Izrek (Zhang, 2013)

Obstaja $d \leq 70.000.000$*, da je praštevilskih parov oblike* $(p, p + d)$ *neskončno mnogo.*

Izboljšave

- Maynard (2013) je pokazal, da zgornja trditev velja za nek $d \leq 600$;
- Projekt Polymath 8 (2014) je uspel zgornjo mejo 600 znižati na 246.