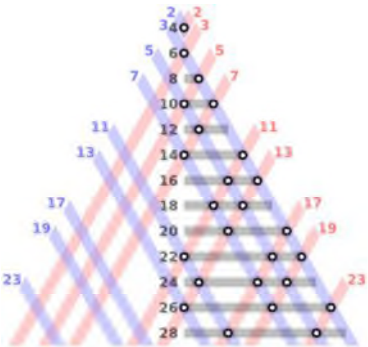
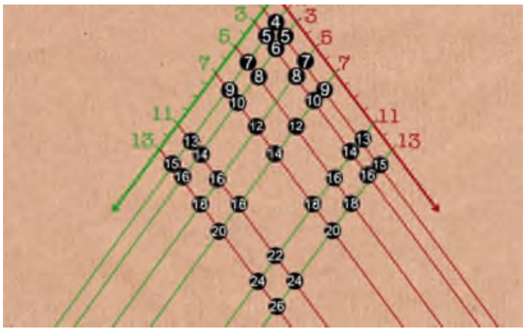



MAJ 2024- MESEC MATEMATIKE

Prosti brojevi

Definicija 1. Prirodan broj p > 1 je **prost broj** ako nema nijedan delilac d takav da je

$1 < d < p$ tj. ako ima samo trivijalne delioce.

Dakle, prost broj je onaj prirodni broj koji je veći od 1 i deljiv je samo sa brojem 1 i samim sobom.

Skup prostih brojeva je $\{2, 3, 5, 7, 11, 13,17 , \cdots\}$.

Definicija 2. Prirodan broj n > 1 koji nije prost naziva se **složen broj**.

Složen broj je onaj prirodni broj veći od jedan, a koji nije prost, tj. deljiv je, osim sa 1 i samim sobom, sa barem još jednim brojem.

Važno je istaći da broj 1 nije ni složen ni prost broj. Zato, skup prirodnih brojeva predstavlja uniju međusobno disjunktnih podskupova

$N = N_1 \cup N_2 \cup N_3,\ \ N_1 \cap N_2 \cap N_3 = \emptyset$, pri čemu

$N_1 = \{1\}, N_2 = \{2, 3, 5, 7, 11, 13,17 , \cdots\}, N_3 = \{4, 6, 8, 9, 10, 12,14 , \cdots\}$.

Teorema 1. Svaki prirodni broj n > 1 je ili prost broj ili ima prost delilac ne veći od $\sqrt{n}$.

Teorema 2. (Euklid) Prostih brojeva ima beskonačno mnogo.

Teorema 3. Svaki složen broj može se napisati kao proizvod prostih brojeva.

Eratostenovo sito (Eratosten, 276-194.pne, grčki matematičar) predstavlja jednostavan algoritam za dobijanje svih prostih brojeva manjih od proizvoljno izabranog broja:

Napišu se svi uzastopni brojevi počev od broja 2 do izabranog broja, pa se izbace svi činioci broja 2 odnosno precrtaju svi parni brojevi koji su deljivi sa 2; zatim se uzima drugi po redu prost broj 3, pa se izbace svi njegovi činioci odnosno precrtaju svi brojevi deljivi sa 3; isti postupak ponovimo sa brojem 5 i sa brojem 7 itd; svi brojevi koji su ostali su prosti brojevi. Postupak se ponavlja dok svi brojevi ne budu označeni (zaokruženi ili precrtani).

Na sledećoj slici je prikazan rezultat primene algoritma Eratostenovo sito na segmentu [1,100], odnosno svi prosti brojevi su zaokruženi, a ostali su precrtani:

Slika 1. Eratostenovo sito

Iz prethodnog primera se uočava da se zaista radi o ”prosejavanju” skupa prirodnih brojeva nakon čega u ”situ” ostaju samo prosti brojevi, zbog čega je ovaj postupak nazvan Eratostenovim sitom.

Distribucija prostih brojeva unutar skupa N:_Još uvek ne postoji egzaktna formula pomoću koje bi bilo moguće odrediti n-ti prosti broj, što predstavlja jedan od otvorenih matematičkih problema. Postavlja se sledeće pitanje: „Koliki je udeo prostih brojeva na nekom proizvoljno odabranom intervalu?“ Kako izgleda funkcija π(n) koja bi kao rezultat mogla dati broj prostih brojeva koji su manji ili jednaki zadatom broju „n“?

Definicija 3. Sa π(x) označimo broj prostih brojeva p takvih da je $p \leq x, x \in [2, \infty)$

π (x) = card { $p \in P \ | p \leq x$ }

Jedan od prvih velikih problema matematike 19. veka bio je opis ponašanja te funkcije, odnosno dobijanje informacija o njenom asimptotskom ponašanju.

Tablica 1. Neke vrednosti funkcije π (x)

x	$\pi(x)$
10^2	25
10^3	168
10^4	1229
10^5	9592
10^6	78498
10^7	664579
10^8	5761455
10^9	50847534

Gustina raspodele prostih brojeva: Zanimljivo je poređenje odnosa gustine prostih brojeva manjih od nekog broja „n“ i recipročne vrednosti prirodnog logaritma tog broja. Kao što se vidi u tablici, gustina prostih brojeva u skupu N opada kao i recipročna vrednost prirodnog logaritma broja n, za velike vrednosti n.

x	$\pi(x)$	$\frac{x}{\log x}$	$\pi(x)/(\frac{x}{\log x})$
10	4	4.34	0.92103
10^2	25	21.71	1.15129
10^3	168	144.76	1.16050
10^4	1229	1085.74	1.13195
10^5	9592	8685.89	1.10432
10^6	78498	72382.41	1.08449
10^7	664579	620420.69	1.07117
10^8	5761455	5428681.02	1.06130
10^9	50847534	48254942.43	1.05373

Tablica 2: Raspodela prostih brojeva, poređenje sa vrednošću prirodnog logaritma

Teorema o prostim brojevima (eng. Prime Number Theory):

Funkcija gustine raspodele prostih brojeva može se aproksimirati

$\pi(x) \sim x/ \ln x$ kada $x \to \infty$;

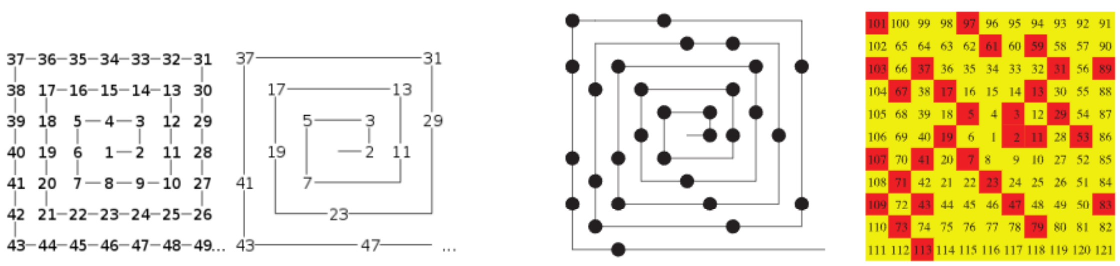
drugim rečima, $\lim\limits_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$.

Prema tome, verovatnoća da je slučajno izabran broj iz skupa $\{1, \ldots, N\}$ prost je (uz uniformnu raspodelu i dovoljno veliko N) približno jednaka $1/ \ln N$.

Prvu hipotezu o tom problemu predstavili su, nezavisno jedan od drugoga, C.F.Gauss i A.M.Legendre na prelazu iz 18. u 19. veka.

Ulamova spirala

Ulamova spirala predstavlja interesantan način vizualizacije prostih brojeva. Potrebno je napisati brojeve od 1 pa nadalje u obliku pravougle spirale, a nakon toga ukloniti sve brojeve osim prostih.



Slika 2. Konstrukcija Ulamove spirale

Goldbachova hipoteza

Goldbach je 1742. godine izneo sledeću pretpostavku:

"Svaki ceo broj veći od 2 može se napisati kao zbir tri prosta broja".

Ojler je, zainteresujući se za problem, odgovorio svojom verzijom pretpostavke:

"Svaki paran broj veći od 2 može se napisati kao zbir dva prosta broja".

Uprkos empirijskim dokazima i jednostavnosti izjave, Goldbahova hipoteza se odupire svim pokušajima dokazivanja već skoro tri veka, iako je testirana uz pomoć najmoćnijih kompjutera do 4×10^{18}.

Goldbah-Ojlerovaova hipoteza ("jaka" Goldbahova hipoteza): Svaki paran prirodan broj veći od 2 jednak je zbiru dva prosta broja.

Ako sa E označimo skup parnih brojeva većih od 2, a sa P skup prostih brojeva, Goldbahova hipoteza glasi: za svako $x \in E$ postoji $p \in P$ i postoji $q \in P$ tako da je $x = p + q$.

"Slaba" Goldbahova hipoteza: Svaki neparan broj veći od 5 može se zapisati kao zbir tri prosta broja.

Na primer 7 = 2 + 2 + 3, 9 = 3 + 3 + 3, 11 = 3 + 3 + 5, …

Iako je tačno da Goldbahova jaka pretpostavka implicira slabu, obrnuto nije tačno.
U stvari, slabu pretpostavku je dokazao peruanski matematičar Harald Andres Helfgot 2013. godine, ali, ipak, jaka pretpostavka nastavlja da se opire svim pokušajima da se dokaže.

U sledećoj tabeli prikazani su parni brojevi izraženi kao zbir prostih brojeva, pri čemu su jednaki brojevi istaknuti jednakim bojama:

+	2	3	5	7	11	13	17	19
2	4	5	7	9	13	15	19	21
3	5	6	8	10	14	16	20	22
5	7	8	10	12	16	18	22	24
7	9	10	12	14	18	20	24	26
11	13	14	16	18	22	24	28	30
13	15	16	18	20	24	26	30	32
17	19	20	22	24	28	30	34	36
19	21	22	24	26	30	32	36	38

Tablica 4. Goldbahova hipoteza

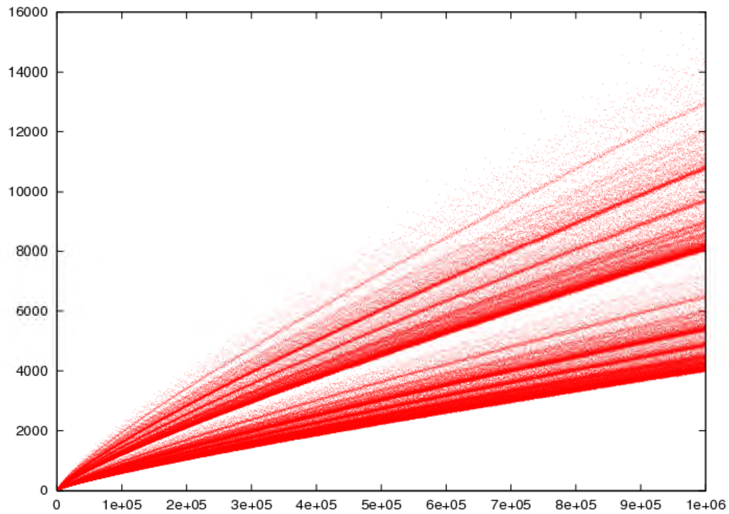
Na primer,

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 3 + 5 = 5 + 3,$$

$$10 = 3 + 7 = 5 + 5 = 7 + 3, \; 12 = 5 + 7 = 7 + 5, \; 14 = 3 + 11 = 11 + 3 = 7 + 7, \cdots$$

Empirijski dokazi u prilog te pretpostavke su ogromni: ne samo da izgleda da se svaki paran broj veći od 2 može izraziti kao zbir dva prosta broja, već vrlo često postoje različiti izrazi ove vrste za isti broj. Ovo se može videti čak i počev od najmanjih brojeva.

Koristeći on-line pregledač Goldbah parova, uočava se da broj različitih načina na koje se paran broj može izraziti kao zbir dva prosta broja ima tendenciju da raste kako se razmatrani broj povećava. Ovaj rast je prikazan na sledećem grafikonu, takozvana **Goldbahova kometa** (Broj različitih načina (y osa) na koje se paran broj (x- osa) može izraziti kao zbir dva prosta broja):



Slika 3. Goldbahova kometa

Dodatni aspekt koji treba uzeti u obzir pri rešavanju ovog i sličnih problema, jeste teškoća da se pođe od argumenata zasnovanih na intuiciji i da se oni transformišu u matematički argumentovane dokaze.

Autor,
dr Ljubica Diković, prof.str.st.

Literatura

[1] https://www.fer.unizg.hr/_download/repository/Seminar_Prosti_brojevi.pdf

[2] https://uu.diva-portal.org/smash/get/diva2:1471524/FULLTEXT02.pdf

[3] https://artofproblemsolving.com/wiki/index.php/Goldbach_Conjecture

[4] http://www.dimostriamogoldbach.it/en/goldbach-pairs-viewer

[5] https://demonstrations.wolfram.com/DistributionOfPrimes/

[6] https://mathworld.wolfram.com/PrimeNumberTheorem.html

[7] https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf

[8] https://www.math.ucla.edu/~tao/preprints/Slides/primes.pdf

[9]
https://petljamediastorage.blob.core.windows.net/root/Media/Default/Lecture/Matematicki%20Algoritmi%201/Matematicki%20algoritmi%20I%20-%20Eratostenovo%20sito.pdf

[10] https://mathworld.wolfram.com/PrimeSpiral.html

[11] https://math.uni.lu/eml/assets/reports/prime-distribution.pdf