SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DisKontNa Matematika 1

SEMINAR

Prosti brojevi

Izabela Gucunski

Petar Žuljević

Viktor Kolobarić

Vjeran Crnjak

Voditelj: *Prof. dr. sc. Neven Elezović*

Zagreb, lipanj, 2012

SADRŽAJ

UVOD

Djeljivost u skupu prirodnih brojeva

Za prirodni broj a kažemo da je djeljiv sa prirodnim brojem b (pišemo b|a) onda i samo onda ako postoji prirodni broj c takav da je a = bc. Broj b je mjera (divizor, djelitelj) broja a, koji je višekratnik (multiplum) broja b.

Primjer

Za 3|15 postoji broj 5 takav da je 15 = 5 x 3.

Prosti i složeni brojevi

Prirodni broj veći od 1 djeljiv jedino samim sobom i brojem 1 je prost broj. Prirodni brojevi veći od 1 koji nisu prosti su složeni.

Primjer

Prosti brojevi su 2, 3, 5, 7 ..., a složeni 4, 6, 8, 9, 10...

Iz navedenog se vidi da su prirodni brojevi podijeljeni u tri klase.

Broj 1

Prosti brojevi

Složeni brojevi

U skupu prirodnih brojeva broj 1 ima poseban položaj, zato je izdvojen u posebnu klasu.

Djeljivost u skupu N može se proširiti na skup N_0 i reći da je 0 djeljiva sa svakim prirodnim broj, jer je 0 = a x 0. Broj 0 nije ni prost ni složen broj.

Relativno prosti brojevi

Brojevi a i b su relativno prosti ako je najveći zajednički djelitelj brojeva a i b jednak 1, tj. brojevi a i b nemaju zajedničkih faktora ili nzd(a,b)=1.

Teoremi

Teoremi (1 – 7)

Teorem 1

Ako je prirodni broj a djeljiv sa brojem b onda je svaki višekratnik od a djeljiv sa b.

Dokaz: na = n(bc) = (nc)b

Teorem 2

Da bi suma (a + b) bila djeljiva sa c dovoljno je da svaki od brojeva a, b bude djeljiv sa c.

Dokaz:

Ako je a = cm i b = cn onda je (a + b) = cm + cn = c (m + n).

Teorem 3

Da bi suma (a + b), u kojoj je broj a djeljiv sa c, bila djeljiva sa c potrebno je da i drugi broj bude djeljiv sa c.

Dokaz: a = cm, i (a + b) = cn, imamo cm + b = cn => cn – cn = b => b =c(m – n) .

Teorem 4

Svaki prirodni broj djeljiv je sa bar jednim prostim brojem.

Dokaz:

Ako je n prost broj djeljiv je samim sobom, a ako je složen među njegovim djeljiteljima postoji najmanji. Označimo ga sa p. On mora biti prost broj, jer ako bi bio složen, postojao bi manji djelitelj kao faktor od p.

Svaki prost broj djeljiv je sam sa sobom.

Teorem 5

Svaki složen broj možemo napisati kao produkt prostih brojeva.

Dokaz:

Neka je p_1 najmanji prost broj, sa kojim je složen broj n djeljiv. Za $q_1 = n\ p_1$ imamo $n = p_1\ q_1$. Ako je q_1 složen, postoji najmanji prosti broj p_2 takav da $q_1 = p_1\ p_2\ q_2$. Ovaj postupak možemo nastaviti dok ne dođemo do oblika $n = p_1\ p_2 ...\ p_n$, a kako je $n > q_1 > q_2 >...$ jednom ćemo doći do q_n koji je prost broj.

Primjer:

3224 = 2 x 3 x 7 x 7 x 11

Teorem 6

Prostih brojeva ima beskonačno mnogo.

Dokaz: Pretpostavimo da ima konačno mnogo prostih brojeva, i to n njih. Posmatrajmo broj $2*3*5*7*...*p_n + 1$. On je veći od svakog prostog broja i kao takav ne može biti prost. Nije djeljiv ni sa jednim prostim brojem (pri dijeljenju uvijek ostane ostatak 1). Ovo znači da i taj broj mora biti prost, čime se dobiva kontradikcija.

Teorem 7

Postoji po volji beskonačno mnogo složenih brojeva.

Dokaz:

Za bilo koji prosti broj p, postoji složeni broj 2p. Budući da ima beskonačno mnogo prostih brojeva, onda ima i ovakvih složenih.

Osnovni teorem aritmetike

$\forall n \in N$, n>1 postoji jedinstven rastav na proste faktore: $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_1}$

Gdje su $p_1 < p_2 < \dots < p_k$ te su svi p_i prosti brojevi.

Faktorizacija svakog prirodnog broja n > 1 na proste faktore je jedinstvena do na poredak prostih faktora.

Euklidov teorem

Skup svih prostih brojeva je beskonačan, tj. ne postoji najveći prosti broj.

Teorem Prostih brojeva ima beskonačno mnogo.
Dokaz: Pretpostavimo suprotno tj. da ih ima konačno mnogo. Ako ih označimo sa p1,p2,...,pn tada definiramo P=∑ni=1pi+1. Tada P nije djeljiv sa niti jednim prostim brojem, a iz prvog teorema zaključujemo da je P ili prost ili ima prostog djelitelja koji je tada različit od svih pi. To je u kontradikciji sa pretpostavkom te smo dokazali tvrdnju.

Eratostenovo sito

Ovo je mehanički postupak pronalaženja prostih brojeva koji nisu veći od n. Ispišemo sve brojeve od 2 do n. Pođemo od broja 2 i precrtavamo svaki drugi broj, zatim pođemo od broja 3 i precrtavamo svaki treći s time da brojimo i precrtane brojeve, pa od prvog neprecrtanog broja itd. Ovaj postupak ponavljamo dok ne dođemo do broja p za koji je $p^2 > n$. Neprecrtani brojevi su prosti.

Primjer za n=20:

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

<u>2</u>, 3, **4**, 5, **6**, 7, **8**, 9, **10**, 11, **12**, 13, **14**, 15, **16**, 17, **18**, 19, **20**

2, <u>3</u>, **4**, 5, **6**, 7, **8**, **9**, **10**, 11, **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**

2, 3, **4**, 5, **6**, 7, **8**, **9**, **10**, 11, **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**

DISTRIBUCIJA PROSTIH BROJEVA

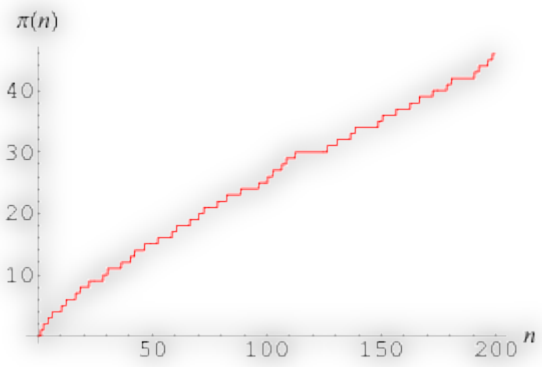
Skup prostih brojeva unutar skupa N

Još uvijek ne postoji egzaktna formula uz pomoć koje bi bilo moguće odrediti n-ti prosti broj, to predstavlja jedan od najvećih otvorenih matematičkih problema. Podjednako težak problem je i određivanje načina i gustoće raspodjele prostih brojeva u skupu N.

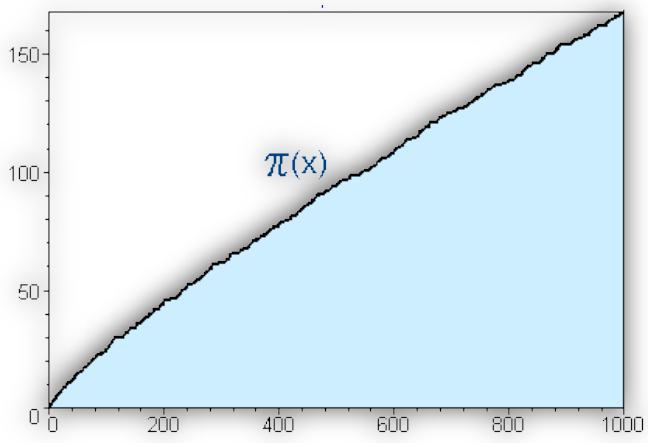
Postavlja se iduće pitanje:

„Koliki je udio prostih brojeva na nekom proizvoljno odabranom intervalu?“

Ukoliko bi postojala funkcija *π(n)* koja bi kao rezultat mogla dati broj prostih brojeva koji su manji ili jednaki zadanom broju „n“, tada bi njen graf izgledao kao na sl.1 i sl.2.



sl. 1



sl. 2

* http://oeis.org/A000720 *vrijednosti funkcije π(n) za uzastopne n = 0, 1, 2, 3...*

Definicija funkcije *π(x)*

Sa **π(x)** označavat ćemo broj prostih brojeva p takvih da je $p \leq x$, $x \in [\,2, +\infty >$

$$\pi(x) = \text{card}\ \{\, p \in P \mid p \leq x \,\}$$

Na taj način dobivamo funkciju $\pi : [\,2, +\infty > \longrightarrow N$

Jedan od prvih velikih problema matematike 19. stoljeća bio je razumjeti ponašanje te funkcije, odnosno dobiti informaciju o njenom asimptotskom ponašanju.

	x	pi(*x*)
1	10	4
2	100	25
3	1,000	168
4	10,000	1,229
5	100,000	9,592
6	1,000,000	78,498
7	10,000,000	664,579
8	100,000,000	5,761,455
9	1,000,000,000	50,847,534
10	10,000,000,000	455,052,511
11	100,000,000,000	4,118,054,813
12	1,000,000,000,000	37,607,912,018
13	10,000,000,000,000	346,065,536,839
14	100,000,000,000,000	3,204,941,750,802
15	1,000,000,000,000,000	29,844,570,422,669
16	10,000,000,000,000,000	279,238,341,033,925
17	100,000,000,000,000,000	2,623,557,157,654,233
18	1,000,000,000,000,000,000	24,739,954,287,740,860
19	10,000,000,000,000,000,000	234,057,667,276,344,607
20	100,000,000,000,000,000,000	2,220,819,602,560,918,840
21	1,000,000,000,000,000,000,000	21,127,269,486,018,731,928
22	10,000,000,000,000,000,000,000	201,467,286,689,315,906,290
23	100,000,000,000,000,000,000,000	1,925,320,391,606,803,968,923
24	1,000,000,000,000,000,000,000,000	18,435,599,767,349,200,867,866

Tablica 1, Vrijednosti funkcije *π (x)*

Gustoća raspodjele prostih brojeva

Zanimljiva je usporedba omjera gustoće prostih brojeva manjih od nekog broja „n“ i recipročne vrijednosti prirodnog logaritma tog broja. Kao što se vidi po tablici 2, gustoća prostih brojeva u skupu N opada kao i recipročna vrijednost prirodnog logaritma broja n, za velike vrijednosti n ($k/m \longrightarrow 1$).

n	**k = π(n) / n**	**m = 1 / ln(n)**	**k/m**
10^3	0,168	0,1448	1,16022
10^6	0,078498	0,0723824	1,08449
10^9	0,050847534	0,048254942	1,05372
10^{12}	0,037607912018	0,03619120682	1,03914
10^{24}	0,018435599767349	0,018095603412635	1,018788

Tablica 2, Raspodjela prostih brojeva, usporedba sa vrijednošću prirodnog logaritma

*Izračunata vrijednost za n = 10^{24} dobivena je pretpostavljajući Riemannovu hipotezu

Teorem (o prostim brojevima) – *engl. Prime Number Theorem (PNT)*

Tvrdnja teorema je da se funkcija može aproksimirati na sljedeći način

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

odnosno,

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$$

Prvu slutnju o tom problemu predstavili su, neovisno jedan o drugome, ***C.F.Gauss*** i ***A.M.Legendre*** na prijelazu iz 18. u 19. stoljeće.

- **Legendre** je 1798. formulirao aproksimaciju za $\pi(x)$ u obliku:

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

  Za uvedene konstante ustvrdio je da bi za najbolju aproksimaciju trebale biti

  $A = 1$, $B = -1.08366$. Legendre je radio sa tablicama prostih brojeva gdje je x bio manji od 400 000, te je zbog toga pogrešno odredio konstantu B. Na većim primjerima se pokaže da je aproksimacija bolja ukoliko je B = -1.

- **Gauss** je u svom poznatom pismu njemačkom astronomu Johann Franz Enckeu, poslanom na Badnjak 1849, napisao kako je on još kao šesnaestogodišnjak primjetio da gustoća prostih brojeva opada aproksimativno kao 1 / ln(x).

  Te je došao do pretpostavke da bi se funkcija $\pi(x)$ mogla prikazati pomoću logaritamskog integrala: $\pi(x) \approx Li(x) = \int_2^x \frac{dt}{\ln t}$

1896**. Jacques-Salomon Hadamard** i **Charles Jean de la Vallée-Poussin** dokazali su neovisno jedan o drugome PNT.

Švedski matematičar **Niels Fabian Helge von Koch** je pokazao, ukoliko je Riemannova hipoteza točna, da vrijedi: $\pi(x) = \mathrm{Li}(x) + O\left(\sqrt{x}\ \ln x\right)$

Najbolja aproksimacija od navedenih u tablici 2, za funkciju $\pi(x)$ je Gaussov Li(x), te se po L'Hospitalovom pravilu dobiva

$$\lim_{x \to \infty} \frac{Li(x)}{x/\ln x} = 1$$

x	pi(x)	Gauss' Li	Legendre	x/(log x - 1)
1000	168	178	172	169
10000	1229	1246	1231	1218
100000	9592	9630	9588	9512
1000000	78498	78628	78534	78030
10000000	664579	664918	665138	661459
100000000	5761455	5762209	5769341	5740304
1000000000	50847534	50849235	50917519	50701542
10000000000	455052511	455055614	455743004	454011971

Tablica 3, Usporedba raznih aproksimacija za π(x)

Procjena n-tog prostog broja

Neka je p(n) n-ti prost broj, tada kao posljedica PNT sljedi: p(n) ~ n*ln(n).

Pierre Dusart : $p(n) > n (\log n + \log\log n - 1)$

G. Robin: za n > 8601

$$n (\log n + \log\log n - 1.0073) < p(n) < n (\log n + \log\log n - 0.9385)$$

Milijunti prosti broj je prema toj procjeni između 15,434,000 i 15,502,000.

Točna vrijednost, $p(10^6)$ = 15,485,863.

Dirichletov teorem

Neka su d i a prirodni brojevi takvi da je njihova mjera (d, a) = 1, tj. oni su relativno prosti, tada postoji beskonačno mnogo prim brojeva oblika d n + a, n $\in N_0$, tj. postoji beskonačno mnogo prim brojeva u aritmetičkom nizu a, d + a, 2d + a, 3d + a...

Aritmetički niz	Prvih 10 prostih brojeva u nizu
1 + 2n	3, 5, 7, 11, 13, 17, 19, 23, 29, 31, …
1 + 4n	5, 13, 17, 29, 37, 41, 53, 61, 73, 89, …
3 + 4n	3, 7, 11, 19, 23, 31, 43, 47, 59, 67, …
1 + 6n	7, 13, 19, 31, 37, 43, 61, 67, 73, 79, …
5 + 6n	5, 11, 17, 23, 29, 41, 47, 53, 59, 71, …
1 + 8n	17, 41, 73, 89, 97, 113, 137, 193, 233, 241, …
3 + 8n	3, 11, 19, 43, 59, 67, 83, 107, 131, 139, …
5 + 8n	5, 13, 29, 37, 53, 61, 101, 109, 149, 157, …
7 + 8n	7, 23, 31, 47, 71, 79, 103, 127, 151, 167, …
1 + 10n	11, 31, 41, 61, 71, 101, 131, 151, 181, 191, …
3 + 10n	3, 13, 23, 43, 53, 73, 83, 103, 113, 163, …
7 + 10n	7, 17, 37, 47, 67, 97, 107, 127, 137, 157, …
9 + 10n	19, 29, 59, 79, 89, 109, 139, 149, 179, 199, …

Tablica 4, Prosti brojevi u aritmetičkim nizovima

Ovdje nećemo dokazati Dirichletov opći teorem već ćemo generalizirati Euklidov dokaz beskonačnosti skupa prostih brojeva te dokazati teorem za neke općenite aritmetičke nizove, primjerice za $4n + 3$.

Svaki prost broj veći od 2 je neparan, te je oblika $4n + 3$ ili $4n + 1$.
Umnožak dva broja oblika $4n + 1$ također je tog oblika:

$$(4a + 1) * (4b + 1) = 16ab + 4a + 4b + 1 = 4 * (b + a + 4ab) + 1$$

Pretpostavimo sada da postoji konačno mnogo prostih brojeva $p_1, p_2 \dots, p_n$ koji su oblika $\mathbf{4n + 3}$.

Neka je tada broj

$$N = 4 * p_1 * p_2 * \dots * p_n - 1 = 4 * (p_1 * p_2 * \dots * p_n - 1) + 3$$

Ili je N prost broj, ili se može rastaviti na produkt prostih brojeva, od kojih nijedan nije $p_1, \dots, p_n$ jer ostatak dijeljenja broja N sa nekim od brojeva p je -1.

Nadalje, svi prosti faktori broja N ne mogu biti oblika **4n+1**, jer N nije tog oblika. Kao što smo vidjeli, produkt brojeva oblika 4n+1 je također je broj tog oblika.

Prema tome, bar jedan prost faktor mora biti oblika 4n+3, što je nemoguće, jer taj faktor nije nijedan od brojeva p, za koje smo pretpostavili da su svi prosti brojevi oblika 4n+3.

Dakle, broj prostih brojeva takvog oblika je beskonačan.

Snažnija posljedica Dirichletovog teorema je tvrdnja da red recipročnih prostih brojeva navedenog oblika divergira.

$$\frac{1}{3} + \frac{1}{7} + \frac{1}{11} + \frac{1}{19} + \frac{1}{23} + \frac{1}{31} + \frac{1}{43} + \frac{1}{47} + \frac{1}{59} + \frac{1}{67} + \cdots$$

sl. 3, Red recipročnih prostih brojeva oblika 4n + 3

Red recipročnih prostih brojeva

Dokazati da za svaki realan broj y ≥ 2 vrijedi:

$$\sum_{p\leq y}\frac{1}{p} > \ln\ln y - 1$$

Odavde neposredno slijedi da red:

$$\sum_{p\ prost}^{\infty}\frac{1}{p}$$

divergira, što daje novi dokaz da prostih brojeva ima beskonačno mnogo.

Dokaz: S ℵ označimo skup svih prirodnih brojeva n koji su sastavljeni samo od prostih faktora p koji su ≤ y (uključujući i broj 1). Budući da imamo samo konačno mnogo prostih brojeva p koji su ≤ y, a u apsolutno konvergentnom redu možemo permutirati članove, imamo:

$$\prod_{p\leq y}\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\ \dots\right)=\sum_{n\in\aleph}\frac{1}{n}$$

Odnosno,

$$\prod_{p\leq y}\left(\frac{1}{1-\frac{1}{p}}\right)=\sum_{n\in\aleph}\frac{1}{n} \qquad (1)$$

Očito su svi prirodni brojevi koji su $\leq y$ elementi skupa ℵ.

Neka je $N = \lfloor y \rfloor$, najveći cijeli broj $\leq y$. Usporedbom (gornje Darbouxove) sume i integrala, dobivamo:

$$\sum_{n=1}^{N}\frac{1}{n}\geq\int_{1}^{N+1}\frac{dx}{x}=\ln(N+1)>\ln y$$

Prema tome, iz (1) dobivamo:

$$\prod_{p\leq y}\left(1-\frac{1}{p}\right)^{-1} > \ ln\ y \qquad (2)$$

Dokažimo sada da za sve realne brojeve v, takve da je $0 \leq v \leq \frac{1}{2}$, vrijedi:

$$e^{v+v^2} \geq (1-v)^{-1} \qquad (3)$$

Da bismo dokazali tvrdnju 3, definirat ćemo funkciju f.

Neka je $f(v) = (1-v)e^{v+v^2}$,

tada je $f'(v) = -e^{v+v^2} + (1-v)(1+2v)e^{v+v^2} = v(1-2v)e^{v+v^2}$

Budući da je $f'(v) \geq 0 \; za \; v \in \left[0, \frac{1}{2}\right]$, radi se o rastućoj funkciji

$$f(0) = 1, pa \; je \; f(v) \geq 1 \; za \; v \in \left[0, \frac{1}{2}\right]$$

Nakon uvrštavanja (3) u (2) dobivamo:

$$\prod_{p \leq y} e^{v+v^2} > \ln y$$

Logaritmirajući obje strane nejednakosti te nakon transformacije logaritma umnoška u zbroj logaritama, dobivamo:

$$\sum_{p \leq y} \frac{1}{p} + \sum_{p \leq y} \frac{1}{p^2} > \ln \ln y$$

Očito je da $\sum_{p \leq y} \frac{1}{p^2}$ konvergira jer je usporediv harnonijskim redom $\sum_{n=2}^{\infty} \frac{1}{n^2}$

$$\sum_{n=2}^{\infty} \frac{1}{n^2} < \int_1^{\infty} \frac{dx}{x^2} = 1$$

Odavde slijedi tvrdnja: $\sum_{p \leq y} \frac{1}{p} > \ln \ln y - 1$.

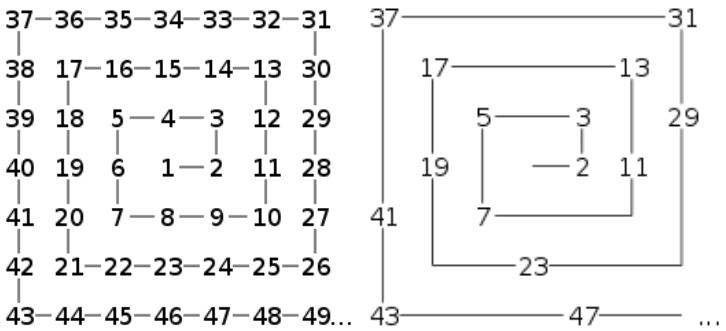
Kad $y \to \infty$, zaključujemo da red recipročnih prostih brojeva divergira.

Ulamova spirala

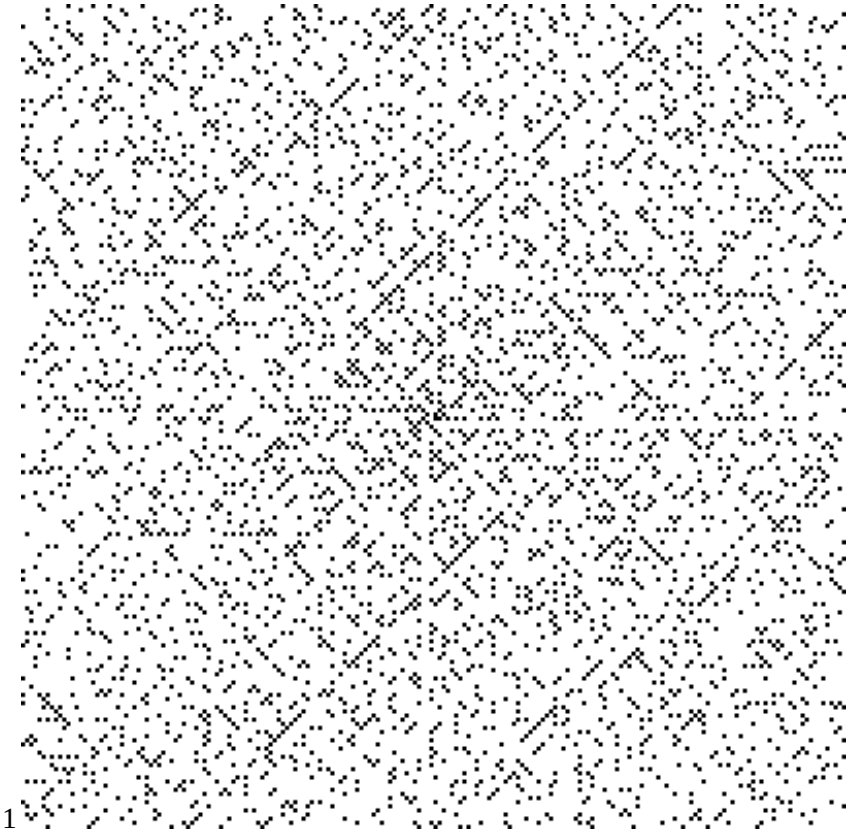
Ulamova spirala je jednostavan način vizualizacije prostih brojeva. Potrebno je napisati brojeve od 1 pa nadalje u obliku pravokutne spirale, te nakon toga pobrisati sve brojeve osim prostih, na taj način se dobiju zanimljivi oblici.

Otkrio ju je **Stanislaw Ulam** 1963. godine dok se dosađivao na sastanku crtkarajući po papiru, primjetivši da se prosti brojevi nalaze na dijagonalama.

Ubrzo nakon toga je sa suradnicima Myronom Steinom i Mark Wellsom koristeći MANIAC II (**M**athematical **A**nalyzer **N**umerical **I**ntegrator **a**nd **C**omputer Model **II)** u istraživačkom laboratoriju u Los Alamosu, generirao sliku spirale koja je obuhvaćala brojeve do 65,000.



sl. 4, Konstrukcija Ulam spirale



sl. 5, Ulamova spirala nakon većeg broja iteracija

TEOREMI I SLUTNJE

U potrazi za nekim zakonima i pravilnostima među prostim brojevima proizašli su mnogi teoremi i hipoteze. Neki od njih su :

Goldbachova hipoteza

Polovicom 18. stoljeća njemački (pruski) matematičar **Christian Goldbach** je napisao pismo **Leonhardu Euleru** u koje je izrekao sljedeću hipotezu :

„Svaki prirodni broj koji se može predstaviti kao suma 2 prosta također se može predstaviti kao suma prostih sve više i više prostih brojeva dok svi ne budu jedinice.“

Nakon toga je na margini pisma zapisao drugu hipotezu :

„Svaki parni prirodni broj veći od 2 se može zapisati kao suma 3 prosta.“

Goldbach je smatrao broj 1 prostim, što je kasnije defnicija prostih brojeva izostavila. Danas je poznato da su te 2 hipoteze ekvivalentne.

Euler mu je odgovorio i prepravio Goldbachovu hipoteza :

„Svaki prirodni broj veći od 2 se može zapisati kao suma 2 prosta.“

Još jedna Goldbachova hipoteza da se svaki neparni broj veći od 5 može prikazati kao suma 3 prosta slijedi implikacijom iz potonje.

Do danas je hipoteza provjerena za prirodne brojeve manje od 1.609×10^{18}.

Hipoteza još nije dokazana.

Chenov teorem

Chen Jingrun je bio kineski matematičar 20. stoljeća. Svojim teoremom je napravio veliki korak prema riješavanju Goldbachove hipoteze.

Teorem kaže da se svaki „dovoljno veliki prirodni broj može prikazati kao suma 2 prosta ili kao suma prostog i poluprostog (umnožak 2 prosta).

Green-Tao teorem

Teorem su dokazali **Ben Green** i **Terence Tao** 2004. godine. Govori o tome da niz prostih brojeva sadrži proizvoljno mnogo proizvoljno dugačkih aritmetičkih nizova.

Drugim riječima postoji niz prostih brojeva s n članova :

$P_k=P+k*d$ gdje je $k>0$ i $k<n+1$

Ovaj teorem samo govori da postoje i ne pokazuje kako se pronalaze. Prvi niz s 24 člana je pronašao Jaroslav Wroblewski :

468,395,662,504,823 + 205,619 · 223,092,870 · *n*, za *n* = 0 to 23.

Još nekoliko primjera :

6,171,054,912,832,631 + 366,384 · 223,092,870 · *n*, za *n* = 0 to 24.

43,142,746,595,714,191 + 23,681,770 · 223,092,870 · *n*, za *n* = 0 to 25.

Mali Fermatov teorem

Francuski matematičar **Pierre de Fermat** prvi iznio ovaj teorem koji daje nužan uvjet djeljivosti s prostim brojevima.

$$a^p \equiv a \pmod{p}$$

daje isti ostatak pri dijeljenju s p kao i a, gdje je a prirodni broj, a p prost

Kombinatorni dokaz :

Neka p predstavlja duljinu nekog niza koji se dobije koristeći (ponavljanje je dopušteno) „a“ različitih znakova.

Na primjer neka je p = 5 i a = 2 , znači da možemo koristiti 2 znaka
(neka to budu slova A i B) i ukupan broj nizova koje možemo napraviti duljine 5 je $2^5 = 32$.

AAAAA, AAAAB, AAABA, AAABB, AABAA, AABAB, AABBA, AABBB,

ABAAA, ABAAB, ABABA, ABABB, ABBAA, ABBAB, ABBBA, ABBBB,

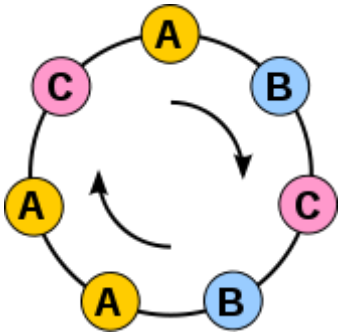
BAAAA, BAAAB, BAABA, BAABB, BABAA, BABAB, BABBA, BABBB,

BBAAA, BBAAB, BBABA, BBABB, BBBAA, BBBAB, BBBBA, BBBBB.

Promotrit ćemo slučaj kada uklonimo nizove koji se sastoji od samo jednogo simbola i pokazati da preostalih $a^p - a$ nizova mogu biti složeni u grupe od kojih svaka ima točno p nizova. Iz čega slijedi da je $a^p - a$ djeljivo s p.

Ogrlice i prijatelji

Neka svaki niz predstavlja ogrlicu kada mu se kraj spoji s početkom :



sl.6, Ogrlice i prijatelji

Ova ogrlica predstavlja 7 različiti nizova (ABCBAAC, BCBAACA, CBAACAB, BAACABC, AACABCB, ACABCBA, CABCBAA) ovisno o tome što smatramo početkom odnosno krajem.

Ako možemo dobiti 2 niza koristeći istu ogrlicu nazvati ćemo takve nizove prijateljima.

Na primjer u našem slučaju prijatelji su : AAAAB, AAABA, AABAA, ABAAA, BAAAA.

Ovdje svaki red predstavlja jednu ogrlicu za naš primjer :
AAABB, AABBA, ABBAA, BBAAA, BAAAB,
AABAB, ABABA, BABAA, ABAAB, BAABA,
AABBB, ABBBA, BBBAA, BBAAB, BAABB,
ABABB, BABBA, ABBAB, BBABA, BABAB,
ABBBB, BBBBA, BBBAB, BBABB, BABBB,
AAAAA,
BBBBB.

Neke ogrlice gore se sastoje od 5 nizova, a neke od jednog (1). Lako se vidi da je 32 - 5 djeljivo s 5.

Koliko ogrlica može imati prijatelja?

Dokle god se ogrlica nemože rastaviti na manje dijelove koji se ponavljaju rotacijom ogrlice se neće dobiti isti niz.

Na primjer niz ABBABBABBABB se sastoji od uzastopnih ABB nizova te se zato pomakom početka ogrlice za 3 mjesta opet dobiva isti niz.

Ako se nemože razbiti ogrlica na manje ponavljajuće dijelove koliko onda ima prijatelja?

Ima ih točno p jer se svakim pomakom početka u ogrlici dobiva novi niz.

No kako je duljina našeg niza prost broj on se sigurno nemože razbiti na dijelove koji se ponavljaju. Zato možemo sve od a^p nizova podijeliti u 2 skupine :

Oni nizovi koji se sastoji od samo jednog simbola, njih ima koliko i različitih slova, dakle ima ih p i ostali nizovi koje sve možemo prestaviti s n ogrlica od kojih svaka predstavlja p prijatelja.

Broj nizova (2) je djeljiv s p jer smo ih podijelili u grupe od kojih svaka ima pa članova.

$$a^p - a \equiv 0 \,(mod\, p) \qquad => \qquad a^p \equiv a \,(mod\, p)$$

Wilsonov teorem

Ovaj teorem je iskazao **John Wilson**, student engleskog matematičara Edwarda Waringa.

Objavio ga je 1770. godine, ali ga ni on ni profesor nisu dokazali. Slavni francuski matematičar Lagrange je 1771. godine prvi dokazao ovaj teorem. Ovaj teorem za razliku od od malog Fermatovog teorema koji daje samo nužan, daje i dovoljan uvjet da broj bude prost.

Dokaz:

Za p = 2 tvrdnja očigledno vrijedi. Ako je p prost broj veći od 2, tada je p neparan, pa se u produktu 1*2*3 . . . (p−1) pojavljuje paran broj faktora.

Neka je k ∈ {2, 3, . . . , p−2}. Brojevi k, 2k, 3k, . . . , (p−1)k, pk tvore potpuni sustav ostataka po modulu p, pa u nekom redoslijedu daju ostatke 0, 1, 2, . . .p−1 po modulu p. Obzirom da vrijedi k $\not\equiv$ 1 (mod p), (p−1)k $\not\equiv$ 1 (mod p) i pk $\not\equiv$ 1 (mod p), to je kl ≡ 1 (mod p) za jedan (i samo jedan) l ∈ {2, 3, . . . , p−2}.

Pretpostavimo li da je l = k, tada imamo k^2 ≡ 1 (mod p) odnosno (k −1)(k +1) ≡ 0 (mod p) što povlači k ≡ 1 (mod p) ili k ≡ −1 (mod p), suprotno tome da je k ∈ {2, 3, . . . , p−2}. Prema tome, skup *{2, 3, . . . , p−2}* možzemo podijeliti na dva jednaka dijela tako da za svaki *k* iz jednog dijela postoji jedinstven *l* iz drugog dijela sa svojstvom *kl* ≡ 1 (mod *p*).
Slijedi

2*3 . . . (p−2) ≡ $1^{(p-3)/2}$ (mod p)

odnosno

(*p* − 2)! ≡1 (mod p).

Za k = p − 1 je k ≡ −1 (mod p), pa je konačno

(p − 1)! ≡ −1 (modp) ili p | (p − 1)! + 1

Obrat

Pretpostavimo da p nije prost broj i da ima djelitelj d, d < p. Tada d | (p − 1)! odakle slijedi da d ne dijeli (p − 1)! + 1 što znači da p ne dijeli (p − 1)! + 1. Ovim smo došli u kontradikciju, pa p mora biti prost broj.

FERMATOVI I MERSENOVI BROJEVI

Fermatovi brojevi

Brojevi oblika,

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

gdje je n nenegativan cijeli broj.

Fermat je smatrao da su svi takvi brojevi prosti. Neki od njih jesu prosti.

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65537$$

Međutim, F_5nije prost.

$F_5 = 4294967297 = 641 * 6700417$

Povijesna crtica:

Dva imena ostaju zapamćena u povijesti teorije brojeva. **Pierre de Fermat** (1601 – 1665) i **Leonhard Euler** (1707 – 1783). Fermat, prozvan Velikim Amaterom, bio je, u svoje slobodno vrijeme, matematičar, Descartes-ov suvremenik i suparnik. Njegov „pravi posao“ bješe položaj suca u Toulouse-u, Francuska. U to vrijeme od sudaca se očekivalo da izbjegavaju društvo ljudi kojima će možda, u periodu svoga života, morati presuditi stoga je Fermat živio u izolaciji, daleko od ljudi Toulouse-a, imajući mnoštvo vremena za rad na svojoj matematici, uz suradnju s Marinom Mersenne-om.

Fermat je bio sličan i ostalim matematičarima sedamnaestog stoljeća. Samo je objavio svoja otkrića i uglavnom ostavio dokaze svojih tvrdnji kao izazov čitateljima, umjesto da ih je sam napisao. One koje je napisao, bili su u marginama njegovih knjiga. Te bilješke margina postale su poznate matematičkom svijetu kada je njegov sin, Samuel, objavio njegove bilješke i radove 1666., nakon Pierre-ove smrti. Tada je Fermat-ov Posljednji Teorem postao poznat ostatku matematičkog svijeta.

Matematičar osamnaestog stoljeća, **Leonhard Euler**, je tijekom svoje karijere dokazivao ili pobijao skoro sve Fermat-ove tvrdnje, uključujući i Fermat-ov Mali Teorem i Fermat-ov Posljednji Teorem(za n = 3 i n = 4).

Eulerov interes za teoriju brojeva je prvi put počeo upravo kada je naletio na Fermatovu slutnju da za sve brojeve n, broj oblika $F_n = 2^{2^n} + 1$ je prost.

Euler je na samom početku rekao da ne može uopće napredovati s problemom, ali 3 godine poslije, skoro 100 godina nakon samog nastanka slutnje, Euler je našao rješenje.

Više o rješenju u [1].

Do dan danas nije pronađen ni jedan Fermat-ov prosti broj za n > 4. Te su svi od sljedećih navedenih još uvijek otvoreni problemi:

Je li F_n složen za sve n > 4?

Postoji li beskonačno mnogo Fermat-ovih prostih brojeva?

Postoji li beskonačno mnogo složenih Fermat-ovih brojeva?

Do 2010. poznato je da je F_n složen za $5 \leq n \leq 32$, ali do veljače 2012. samo su brojevi od i F_0 do i F_{11}u potpunosti faktorizirani, a brojevi od i F_{20} do i F_{24} nemaju poznatih faktora.

Najveći Fermat-ov broj za koji se zna da je složen je i $F_{2543548}$, a njegov prosti faktor otkriven je pomoću PrimeGrid-ove Proth Prime potrage 22. lipnja 2011.

Zanimljivosti:

Rekurzivne relacije koje zadovoljavaju Fermat-ovi brojevi:

$$\begin{aligned} F_n &= (F_{n-1}-1)^2+1 \\ F_n &= F_{n-1}+2^{2n-1}F_0F_1\cdots F_{n-2} \\ F_n &= F_{n-1}^2-2(F_{n-2}-1)^2 \\ F_n &= F_0F_1\cdots F_{n-1}+2 \end{aligned}$$

Bilo bi zgodno za vježbu dokazati svaku.

Generalizirani Fermat-ovi brojevi

Brojevi oblika $a^{2^n}+b^{2^n}$ gdje je a > 1. (spominje se u Eulerovom dokazu [1]).

Mersenneovi brojevi:

Brojevi oblika,

$$M_n = 2^n - 1$$

gdje je n nenegativan cijeli broj.

Tvrdnja je da kada je god n prosti broj M_p je također prost. Dokazati možemo suprotno. Ako je n složen onda će i M_n biti složen.
Recimo da je n = ab.

Identitet

$$2^{ab}-1 = (2^a-1)\cdot\left(1+2^a+2^{2a}+2^{3a}+\cdots+2^{(b-1)a}\right) = (2^b-1)\cdot\left(1+2^b+2^{2b}+2^{3b}+\cdots+2^{(a-1)b}\right)$$

pokazuje da će M_p moći biti prost samo ako je i n = p prost, što uvelike olakšava potragu za Mersenne prostim brojevima.

Obrnuta tvrdnja koja je bila navedena na početku je kriva. M_p ne mora biti prost ako je p prost. Najmanji protuprimjer je $2^{11} - 1 = 2047 = 23 * 89$, složen broj.

Zanimljivosti:

Mersennovi brojevi povezani su s prostim brojevima. U četvrtom stoljeću prije nove ere Euklid je pokazao da kad god je $2^p - 1$ prosti broj, $2^{p-1}(2^p - 1)$ je paran savršeni broj. Savršeni brojevi su oni čiji je iznos jednak sumi svih njihovih pozitivnih djelitelja.

Euler je pokazao da svi savršeni brojevi imaju takvu formu.

Do dan danas nije dokazana slutnja da Mersennovih brojeva koji su prosti ima beskonačno mnogo, a trenutno ih je pronađeno samo 47.

Najveći prosti broj je Mersennov broj ($2^{43,112,609} - 1$), a da bi ga mogli vizualizirati trebalo bi 3461 stranica za prikaz svih znamenaka u bazi 10 koristeći 75 znamenaka po retku, 50 linija po stranici.

Catalan – Mersenne brojevi

Pisat ćemo M(p) umjesto M_p.

Rekurzivno zadan niz brojeva,
2, M(2), M(M(2)), M(M(M(2))), M(M(M(M(2)))), ...

zove se Catalan-Mersenne brojevi. Smatra se da je Catalan došao do ovog niza nakon otkrića Lucasa da je M(127) = M(M(M(M(2)))) prost. Catalanova slutnja je da su svi brojevi takvog oblika prosti.

Unatoč tome što su prvih 5 do M(127) prosti, ne postoje metode kojima se može provjeriti jesu li još koji prosti(u određenom vremenu) zato što su brojevi u pitanju ogromni. Ako se dokaže da M(M(127)) nije prost slutnja još uvijek stoji.

Nakon 1997. svi novopronađeni Mersenne prosti brojevi otkriveni su preko „Great Internet Mersenne Prime Search“(GIMPS), distribuirani računalni projekt na Internetu.

Zbog brzih algoritama (Lucas – Lehmer) za pronalaženje Mersenne prostih brojeva upravo su oni trenutno najveći prosti brojevi otkriveni.

ZAKLJUČAK

Potraga za prostim brojevima

Zašto tražimo proste brojeve?

- **Tradicija:**

Cataldi, Descartes, Fermat, Mersenne, Frenicle, Leibniz, Euler, Landry, Lucas, Catalan, Sylvester, Cunningham, Pepin, Putnam, Lehmer i mnogi drugi radili su s prostim brojevima, pronalazili najveće i tko se ne bi volio pridružiti toj družini.

- **Zbog napretka koji potraga donosi**

Kako potraga zahtjeva sve brže algoritme množenja dvaju brojeva razni matematičari otkrivaju nove metode kako to izvesti na računalu, a GIMPS trenutno koristi poboljšanu verziju Schonhage – Strassen algoritma.

Isto tako, ta distribuirana potraga je nešto s čime se učenici mogu susresti u osnovnoj školi gdje se može potaknuti njihovo zanimanje za znanost.

- **Ljudi skupljaju rijetke i lijepe predmete**

Mersenne prosti brojevi, najveći prosti brojevi, rijetki i lijepi. Od kad je Euklid započeo potragu i proučavanje Mersenne brojeva malo ih je pronađeno. Manje od pedeset u cijeloj ljudskoj povijesti.

- **Za slavu!**
- **Testiranje hardware-a**

Programi za pronalaženje prostih brojeva služe kao test za hardware. Software-ske rutine GIMPS-a korištene su od strane Intela za testiranje Pentium II čipova.

- **Da bi saznali više o njihovoj raspodjeli**
- **Novac**

Postoje oni koji traže proste brojeve za novčanu nagradu, trenutne nagrade za onoga koji pronađe prosti broj s više od sto milijuna znamenaka – 150000 USD, a onaj koji pronađe prosti broj s više od milijardu znamenaka – 250000 USD.

LITERATURA

[1] http://www.maa.org/editorial/euler/How%20Euler%20Did%20It%2041%20factoring%20F5.pdf

[2] http://primes.utm.edu/notes/faq/why.html

[3] http://en.wikipedia.org/wiki/Mersenne_prime

[4] http://www.math.ucla.edu/~tao/preprints/Slides/primes.pdf

[5] http://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf (1. poglavlje)

[6] http://marjan.fesb.hr/~borka/files/Diskretna-tb-05.pdf (poglavlje 3.4 - 3.6)

[7] http://www.kerrywong.com/2009/09/06/an-alternative-illustration-of-prime-number-distribution/

[8] http://www.ma.utexas.edu/users/kumchev/DistributionOfPrimesNotes.pdf

[9] http://demonstrations.wolfram.com/DistributionOfPrimes/

[10] http://www.math.uniri.hr/~ajurasic/drugo%20predavanje.pdf

[11] http://www.scribd.com/doc/68108948/4/Prosti-brojevi (stranica 10-15)

[12] http://www.math.uniri.hr/~ajurasic/Pseudoprosti%20brojevi-clanak.pdf

[13] http://www.fer.unizg.hr/_download/repository/diskretna1%5B1%5D.pdf

[14] http://primes.utm.edu/howmany.shtml#better