Funkcije povezane s distribucijom prostih brojeva

Leoni, Danijel

Sveučilište u Rijeci - Fakultet za matematiku
Diplomski studij Diskretna matematika i primjene

Danijel Leoni

Funkcije povezane s distribucijom prostih brojeva

Diplomski rad
Rijeka, rujan 2022.

Sveučilište u Rijeci - Fakultet za matematiku
Diplomski studij Diskretna matematika i primjene

Danijel Leoni

Funkcije povezane s distribucijom prostih brojeva

Mentor: dr. sc. Ana Jurasić

Diplomski rad
Rijeka, rujan 2022.

Sadržaj

1 Uvod

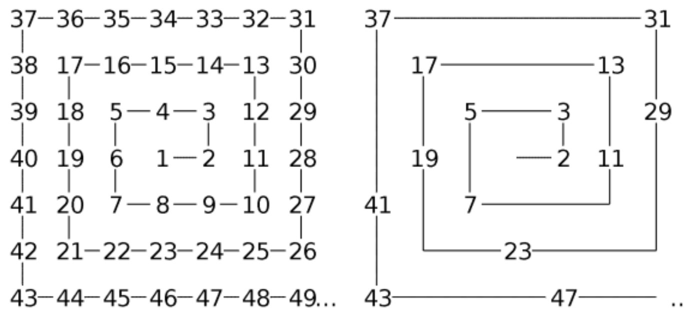
Teorija brojeva je grana matematike koja se prvenstveno bavi proučavanjem svojstava prirodnih brojeva. Važnost ove grane matematičari su shvaćali još od doba prije Krista. Poznata je izreka "Matematika je kraljica znanosti, a aritmetika je kraljica matematike". Izjavio ju je jedan od najvećih matematičara svih vremena Carl Friedrich Gauss, koji je teoriju brojeva nazivao aritmetikom. Osim Gaussa, bitan doprinos ovoj grani matematike dali su i drugi veliki matematičari kao što su Euklid, Euler i mnogi drugi. Teorija brojeva je jedna od najvažnijih grana koja se koristi u kriptografiji i sigurnoj razmjeni informacija, te u prirodnima znanostima koje istražuju strukture DNA kodova.

Važno područje kojim se bavi teorija brojeva su prosti brojevi, odnosno prirodni brojevi veći od 1 koji su djeljivi samo s brojem 1 i sa samim sobom. Skup svih prostih brojeva označavamo s $\mathbb{P}$. Glavno je pitanje vezano uz distribuciju prostih brojeva koliko ima prostih brojeva manjih od nekog prirodnog broja n. Zanimljiva je činjenica da ne znamo napisati po volji veliki prosti broj, a pitanje je hoćemo li ikada i znati.

U ovom radu će se detaljnije opisati, kao što i sam naslov kaže, funkcije povezane s distribucijom prostih brojeva. Konkretno, to su Čebiševljeve funkcije i Riemannova zeta-funkcija, koje su veliki značaj imale u takozvanom Teoremu o prostim brojevima te Dirichletova L-funkcija pomoću koje je dokazan Dirichletov teorem o prostim brojevima u aritmetičkom nizu. Osim toga, spomenut će se i razvoj teorije brojeva kroz povijest te na kraju navesti neke nedokazane tvrdnje vezane uz proste brojeve.

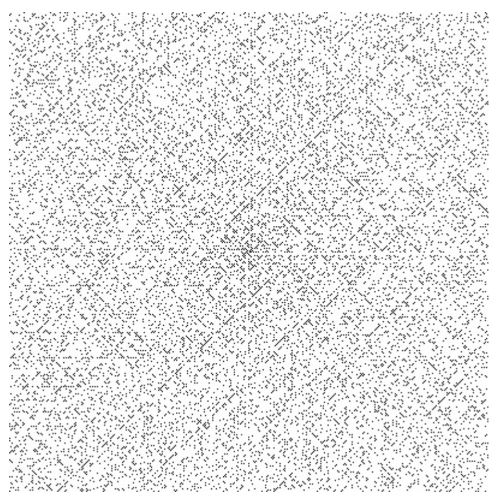
Pod distribucijom prostih brojeva zapravo smatramo njihov udio i raspored u skupu prirodnih brojeva. Jedan od glavnih teorema vezan uz to pitanje je prethodno spomenuti Teorem o prostim brojevima, kojeg ćemo u radu detaljnije opisati. On nam daje generalni pogled na to kako su prosti brojevi smješteni u skupu prirodnih brojeva. Također, kaže da se prosti brojevi u tom skupu pojavljuju sve rjeđe kako oni postaju sve veći. Funkcije koje će se opisivati u ovom radu uvedene su upravo u svrhu otkrivanja distribucije prostih brojeva i dokazivanja prethodno navedenog teorema.

Iako nam Teorem o prostim brojevima daje dobar pogled na njihovu distribuciju, prosti se brojevi mogu vizualizirati i na druge različite načine, bez korištenja prethodno spomenutih funkcija. Jedan od načina njihove vizualizacije je takozvana Ulamova spirala. Ova je konstrukcija prvi puta napravljena od strane poljskog matematičara Stanislawa Ulama 1963. godine. Spirala se dobije tako da se ispišu svi prirodni brojevi u obliku pravokutne spirale, te se nakon toga izbrišu svi oni koji nisu prosti. Primjer jedne ulamove spirale prikazan je na slici 1.



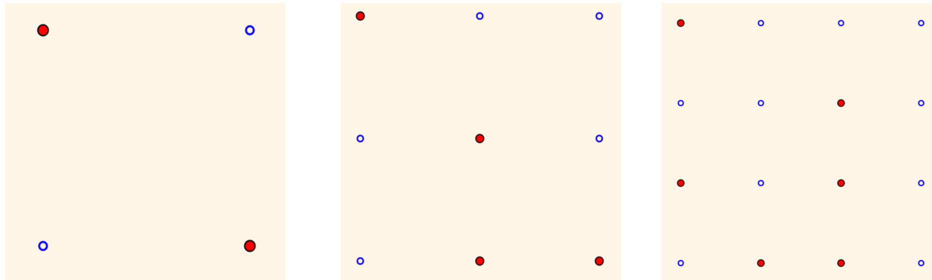
Slika 1: Postupak dobivanja Ulamove spirale

Pomoću ovog načina mogu se vidjeti i pretpostavljati neka svojstva distribucije prostih brojeva koristeći dijagonalne linije. Naravno, kako se povećava broj prostih brojeva tako i Ulamova spirala postaje teža za razumijevanje. Zbog toga se ovaj način vizualizacije ne koristi često, već se biraju neke preglednije metode.



Slika 2: Ulamova spirala veličine 399 x 399

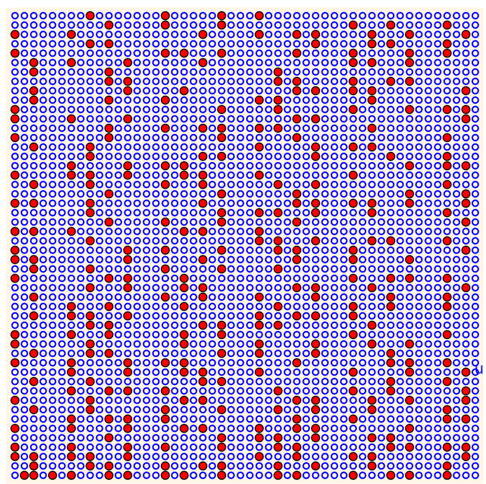
Drukčiji pristup vizualizaciji distribucije prostih brojeva osmislio je John Golden postavljajući prirodne brojeve u obliku kvadrata, pri čemu se prosti brojevi označavaju crvenom, a ostali plavom bojom. Ovaj nam način daje jasniju vizualizaciju same distribucije prostih brojeva u odnosu na Ulamovu spiralu. Primjer jedne takve konstrukcije prikazan je na slici 3. Uočimo da


(a) $n = 2$ (b) $n = 3$ (c) $n = 4$

Slika 3: Postupak Goldenove konstrukcije za prvih 16 prostih brojeva

n predstavlja broj točaka koje se nalaze na jednoj stranici kvadrata, te da u svakom trenutku imamo n x n točaka koje predstavljaju prirodne brojeve.

Na ovaj način možemo vizualizirati i više prostih brojeva. Tako, na primjer, za $n = 50$ dobivamo vizualizaciju za prvih 2500 prostih brojeva, što je prikazano na slici 4.



Slika 4: Goldenova vizualizacija prvih 2500 prostih brojeva

2 Osnovna teorija potrebna za razmatranje prostih brojeva

U ovom ćemo poglavlju navesti osnovne tvrdnje i definicije koje će se koristiti u daljnjim razmatranjima. Dokaze navedenih tvrdnji nećemo navoditi, a oni se mogu pronaći u [3, Poglavlje 2].

Definicija 2.1. *Za prirodan broj $p > 1$ kažemo da je prost ako p nema nijednog djelitelja d takvog da je $1 < d < p$.*

Teorem 2.1. *Svaki se prirodan broj $n > 1$ može prikazati kao umnožak prostih brojeva (s jednim ili više faktora).*

Sljedeći je teorem prvi dokazao Euler, matematičar o kojem ćemo više reći u sljedećem poglavlju.

Teorem 2.2 (**Osnovni teorem aritmetike**). *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

U daljnjim razmatranjima s $nzd(a, b)$ označavat ćemo najveći zajednički djelitelj prirodnih brojeva a i b, a $\varphi(m)$ označavat će broj brojeva u nizu $1, 2, \ldots, m$ koji su relativno prosti s m. Funkciju φ nazivamo Eulerova funkcija. Za navedenu funkciju vrijedi sljedeći bitan rezulat.

Teorem 2.3 (**Eulerov teorem**). *Ako je $nzd(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Također, Eulerova funkcija je multiplikativna, odnosno može se pokazati da ima sljedeća svojstva.

Definicija 2.2. *Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako vrijedi:*

(i) $f(1) = 1$,

(ii) $f(mn) = f(m)f(n)$, *za sve prirodne brojeve m i n, takve da je $nzd(m, n) = 1$.*

Navedimo još definiciju Mersennovih brojeva koje ćemo koristiti u sljedećem poglavlju.

Definicija 2.3. *Mersennovi brojevi su prirodni brojevi oblika*

$$M_p = 2^p - 1,$$

gdje je p prost broj.

Neki su Mersennovi brojevi prosti, a neki složeni. Na primjer, $M_7 = 127$ je prost, dok je $M_{11} = 2047$ složen broj. Do danas nije dokazana slutnja da postoji beskonačno mnogo prostih Mersennovih brojeva. Često se novi najveći poznati prosti brojevi traže upravo među Mersennovim brojevima, o čemu ćemo više reći nešto kasnije.

Osim pojmova iz teorije brojeva, za potrebe rada navodimo i neke potrebne osnovne definicije iz kompleksne analize. U razmatranju nultočaka Riemannove zeta-funkcije, od posebne će važnosti biti pojam pola funkcije u točki. Za početak uvodimo pojam reda i osnovne definicije vezane uz konvergenciju reda.

Definicija 2.4. *Neka je* (a_n) *niz realnih brojeva. Red realnih brojeva, u oznaci* $\sum a_n$, *je uređeni par* $((a_n), (s_n))$, *gdje je* (s_n) *niz oblika*

$$s_1 = a_1, s_2 = a_1 + a_2, \ldots, s_n = a_1 + \cdots + a_n, \ldots$$

Za a_n *kažemo da je opći član reda, a* s_n *parcijalna suma reda.*

Definicija 2.5. *Za red realnih brojeva* $\sum a_n$ *kažemo da je konvergentan ako je njegov niz* (s_n) *parcijalnih suma konvergentan. Ako red konvergira, onda se*

$$s = \lim_{n\to\infty} s_n$$

naziva suma reda i označava se s $s = \sum_{n=1}^{\infty} a_n$. *Red* $\sum a_n$ *je divergentan ukoliko je niz* (s_n) *divergentan.*

Definicija 2.6. *Za red* $\sum a_n$ *kažemo da apsolutno konvergira ukoliko red* $\sum |a_n|$ *konvergira.*

Sljedeće što uvodimo je pojam otvorenog kruga i otvorenog skupa, koji se koriste pri definiranju derivacije funkcije u točki.

Definicija 2.7. *Neka je* $z_0 \in \mathbb{C}$ *i* $r > 0$. *Tada je*

$$K(z_0, r) = \{z \in \mathbb{C} : |z - z_0| < r\}$$

otvoreni krug sa središtem u z_0 *radijusa* r.

Definicija 2.8. *Za neprazan skup* $\Omega \subseteq \mathbb{C}$ *kažemo da je otvoren ako za svaku točku* $z_0 \in \Omega$ *postoji* $r > 0$ *takav da je* $K(z_0, r) \subseteq \Omega$.

Definicija 2.9. *Neka je* $\Omega \subseteq \mathbb{C}$ *otvoren skup i neka je* $f : \Omega \to \mathbb{C}$ *funkcija. Kažemo da je* f *derivabilna u točki* $z_0 \in \Omega$ *ako postoji limes*

$$\lim_{z\to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

U tom slučaju taj limes se označava s $f'(z_0)$ *i naziva se derivacija funkcije* f *u točki* z_0. *Dakle,*

$$f'(z_0) = \lim_{z\to z_0} \frac{f(z) - f(z_0)}{z - z_0}.$$

Također ćemo često u radu korisiti pojam holomorfne funkcije, zbog čega ju ovdje definiramo.

Definicija 2.10. *Ako je funkcija f derivabilna u svakoj točki $z_0 \in \Omega$, onda kažemo da je funkcija f derivabilna na Ω. Ako je f još i neprekidna na Ω, onda kažemo da je f holomorfna ili analitička funkcija na Ω.*

Konačno, možemo definirati pojam pola funkcije u točki.

Definicija 2.11. *Neka je $f : \Omega \subseteq \mathbb{C} \to \mathbb{C}$ funkcija. Kažemo da je točka z_0 singularitet funkcije f ako f u z_0 nije derivabilna ili uopće nije definirana u toj točki.*

Definicija 2.12. *Za singularitet z_0 funkcije f kažemo da je izoliran ako je f holomorfna na $K(z_0, r)\backslash\{z_0\}$, za neki $r > 0$.*

Izolirani se singulariteti mogu podijeliti na uklonjive singularitete, polove i bitne singularitete. Vrsta singulariteta određuje se promatrajući Laurentov red funkcije u okolini točke z_0

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z - z_0)^n.$$

Pri tome, za red $\sum_{n=0}^{\infty} a_n (z - z_0)^n$ kažemo da je pravilni dio, a za red $\sum_{n=-\infty}^{-1} a_n (z - z_0)^n$ glavni dio Laurentovog reda. Ako je $n = -1$, onda se koeficijent a_{-1} uz $\frac{1}{z-z_0}$ tog reda zove reziduum funkcije f u točki z_0 (Oznaka $res(f, z_0)$).

Definicija 2.13. *Za izolirani singularitet kažemo da je uklonjiv ako je u razvoju funkcije u Laurientov red $a_n = 0$, za svaki $n \in \mathbb{N}, n \leq -1$ (ako ne postoji glavni dio Laurentovog reda).*

Definicija 2.14. *Za izolirani singularitet kažemo da je pol ako postoji $m \in \mathbb{N}$ takav da je $a_{-m} \neq 0$ i $a_{-k} = 0$, za svaki $k > m$ (glavni dio Laurentovog reda je konačan). Tada se m naziva red pola.*

Definicija 2.15. *Za izolirani singularitet kažemo da je bitan ako postoji beskonačni niz prirodnih brojeva $n_1 < n_2 < \cdots < n_k < \ldots$ takav da je $a_{-n_k} \neq 0$, za svaki $k \in \mathbb{N}$ (glavni dio Laurentovog reda je beskonačan).*

Za kraj ovog poglavlja navedimo još definiciju meromorfne funkcije, koju ćemo korisiti u opisivanju Dirichletovih L-funkcija.

Definicija 2.16. *Meromorfna funkcija na Ω je holomorfna funkcija f na skupu $\Omega\backslash P$, gdje je $P \subseteq \Omega$ bez gomilišta u skupu Ω, takva da je svaka točka $a \in P$ ili uklonjiv singularitet ili pol funkcije f.*

3 Povijest prostih brojeva

Prirodne, a među njima i proste brojeve, među prvima su počeli proučavati matematičari Pitagorejske škole (500. - 300. g. pr. Kr.). Posebno su ih zanimali savršeni brojevi, to jest prirodni brojevi koji su jednaki zbroju svojih pravih djelitelja (npr. $6 = 1 + 2 + 3$).

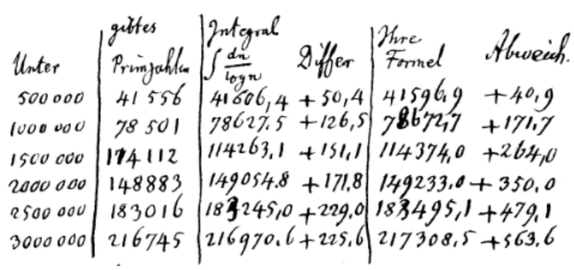
Oko 300. g. pr. Kr. bitan doprinos u istraživanju prostih brojeva daje Euklid. On je u svojoj knjizi *Elementi* dokazao da postoji beskonačno mnogo prostih brojeva. To je ujedno i jedan od prvih dokaza koji koristi metodu kontradikcije kako bi se pokazala navedena tvrdnja. Euklid je također dokazao Osnovni teorem aritmetike, kojeg smo iskazali u prethodnom poglavlju.

Eratosten (oko 200. g. pr. Kr.) razvija algoritam za pronalaženje prostih brojeva. Taj je algoritam poznat kao "Eratostenovo sito". Nakon Eratostena slijedi dugi period u kojem nije bilo većih otkrića vezanih uz istraživanje svojstava prostih brojeva. Taj je period još poznat kao Mračno doba. Na sljedeće novo otkriće vezano za proste brojeve čekalo se sve do 17-og stoljeća. Fermat uspjeva dokazati slutnju Alberta Girarda da se svaki prost broj oblika $4n + 1$ može na jedinstven način zapisati kao suma dva kvadrata. Također, Fermat uspjeva dokazati da za prost broj p takav da $p \nmid a$ vrijedi $a^{p-1} \equiv a \pmod{p}$. Ta je tvrdnja još poznata kao Mali Fermatov teorem.

Istraživanje prostih brojeva nastavlja Gauss. Radio je tablice o tome kako se prosti brojevi distribuiraju u intervalima dužine 1000. Prva tablica koju je stvorio sadržavala je proste brojeve od 1 do 50 000. Promatrajući dobivene tablice, Gauss je uočio da bi broj prostih brojeva u intervalu $[a, b\rangle$ trebao biti otprilike jednak

$$\int_a^b \frac{dx}{\log x}.$$

Kasnije se matematičari počinju baviti funkcijom $\pi(x)$ te Teoremom o prostim brojevima, o čemu će se govoriti u nastavku rada.



Unter	gibtes Primzahlen	Integral $\int \frac{dn}{\log n}$	Differ	Ihre Formel	Abweich.
500 000	41 556	41606,4	+50,4	41596,9	+40,9
1000 000	78 501	78627,5	+126,5	78672,7	+171,7
1500 000	114 112	114263,1	+151,1	114374,0	+264,0
2000 000	148883	149054,8	+171,8	149233,0	+350,0
2500 000	183016	183245,0	+229,0	183495,1	+479,1
3000 000	216745	216970,6	+225,6	217308,5	+563,6

Slika 5: Primjer Gaussove tablice

3.1 Najveći prost broj kroz povijest

Mersennovi brojevi bili su glavni fokus u traženju najvećeg prostog broja. Kroz povijest je bilo mnogo krivih zaključaka o prostosti nekih brojeva. Čak su i veliki matematičari poput Leibniza i Eulera davali krive rezultate, uglavnom zbog vjerovanja da su svi Mersennovi brojevi prosti.

Do 1588. godine Pietro Cataldi je uspio dokazati da su $2^{17}-1$ i $2^{19}-1$ prosti brojevi (sačinjeni od 6 znamenki). Također je tvrdio da je 2^n-1 prost za $n=23$ i $n=29$, što se kasnije ispostavilo netočnim.

Euler je 1772. godine dokazao da pravi djelitelji broja $2^{31}-1$ moraju imati oblik $248n+1$ ili $248n+63$, gdje je prirodni broj $n \geq 0$. Djeljenjem sa svim prostim brojevima tog oblika manjim od 46339 potvrdio je svoju pretpostavku da je $2^{31}-1$ prost broj (sačinjen od 10 znamenki). Pri tome se koristio sljedećom modifikacijom Fermatovog teorema.

Teorem 3.1. *Neka su p i q neparni prosti brojevi. Ako p dijeli M_q, onda je $p \equiv 1 \pmod{q}$ i $p \equiv \pm 1 \pmod{8}$.*

Do 1867. godine Landry je, koristeći se istom metodom, našao veći prosti broj $(2^{59}-1)/179951$. Iako su ovi pronalasci bili velika otkrića u istraživanju prostih brojeva, najveći pomak dogodio se 1876. godine kada Lucas razvija test za određivanje je li Mersennov broj prost. Kasnije Lehmer pojednostavljuje Lucasovu metodu čime je dobiven Lucas-Lehmer test, koji se koristi i danas u istraživanju prostih brojeva. Taj test glasi:

Za neparan prost broj p, Mersennov broj 2^p-1 je prost ako i samo ako 2^p-1 dijeli $S(p-1)$, gdje je $S(n+1)=S(n)^2-2$ i $S(1)=4$.

Pomoću te metode Lucas je dokazao kako je broj $2^{127}-1$ prost broj (s 39 znamenki). Ovo je ujedno i posljednji pronađeni prost broj bez upotrebe računala.

1951. Miller i Wheeler započinju s primjenom računala pronalazeći proste brojeve oblika

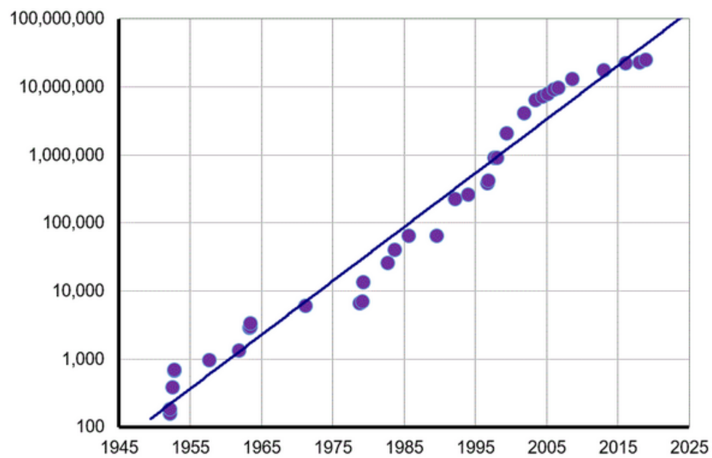
$$kM_{127}+1, \text{ za } k = 114, 124, 388, 408, 498, 696, 738, 774, 780 \text{ i } 978,$$

koji su imali 79 znamenki. Upotreba računala uvelike je ubrzala proces traženja najvećeg prostog broja, što se može vidjeti i u tablici 1. Napomenimo da ovdje nisu detaljno navedena sva otkrića, već je okvirno navedeno kretanje broja znamenki kroz godine. Kako se razvijala tehnologija i brzina računala, tako se povećavala efikasnost u brzini traženja najvećeg prostog broja. Danas najveći poznati prost broj je $M_{82589933}$. Otkriven je 2018. godine i ima 24862048 znamenki.

Mersennov prost broj	Br. znamenki	Godina
M_{521}	157	1952.
M_{4423}	1332	1961.
M_{19937}	6002	1971.
M_{86243}	25962	1982.
M_{756839}	227832	1992.
$M_{13466917}$	4053946	2001.
$M_{57885161}$	17425170	2013.
$M_{74207281}$	22338618	2016.
$M_{82589933}$	24862048	2018.

Tablica 1: Prosti brojevi pronađeni korištenjem računala

Osim tablično, proces traženja najvećeg prostog broja možemo prikazati i grafički. Vrijednosti na x-osi predstavljaju godine, dok vrijednosti na y-osi predstavljaju broj znamenki pronađenog prostog broja. Navedeni graf je prikazan na slici 6.

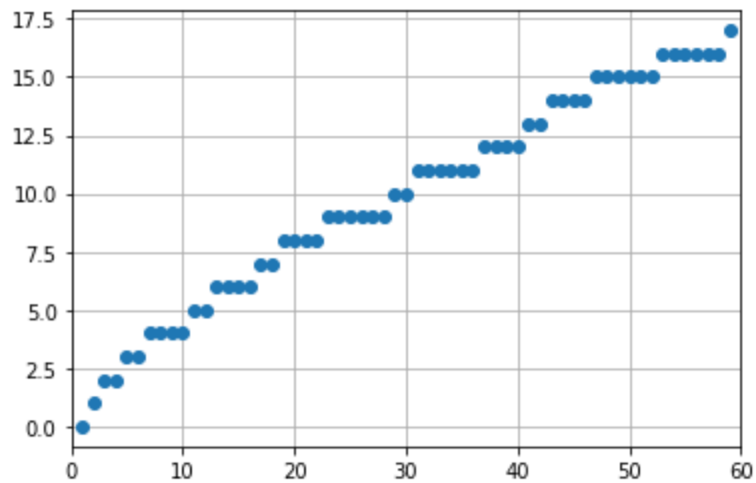


Slika 6: Znamenke najvećeg poznatog prostog broja po godinama

4 Distribucija prostih brojeva

Mnogi su se matematičari kroz povijest bavili distribucijom prostih brojeva, odnosno zanimalo ih je kako što točnije odrediti koliko ima prostih brojeva u određenom intervalu. U tu je svrhu definirana sljedeća funkcija.

Definicija 4.1. *Za realni broj $x > 0$, s $\pi(x)$ označavamo broj prostih brojeva p takvih da je $p \leq x$.*



Slika 7: Graf funkcije π na segmentu [0,60]

Dakle, problem distribucije prostih brojeva zapravo se svodi na pitanje kako što preciznije ocijeniti funkciju $\pi(x)$. Jedan od najbitnijih rezultata vezanih uz distribuciju prostih brojeva je sljedeći teorem.

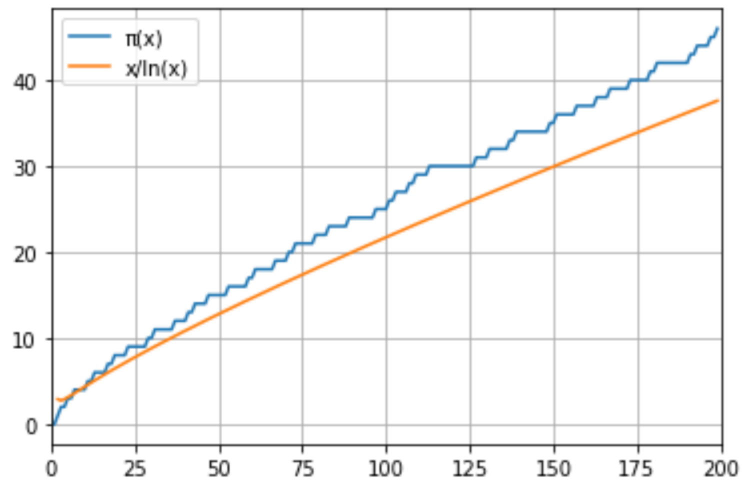
Teorem 4.1 (Teorem o prostim brojevima). *Vrijedi*[1]

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

Pomoću grafa prikazanog na slici 8 vidimo da funkcija $\frac{x}{\ln x}$ dobro aproksimira funkciju $\pi(x)$.

---

[1] Oznaka $f(x) \sim g(x)$ označava $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$ i čita se "$f(x)$ je asimptotski jednako $g(x)$".



Slika 8: Usporedba funkcija $\pi(x)$ i $\frac{x}{\ln x}$

Precizniji podaci dani su u sljedećoj tablici koja prikazuje točnu razliku između vrijednosti prethodno navedenih funkcija za pojedine vrijednosti argumenta.

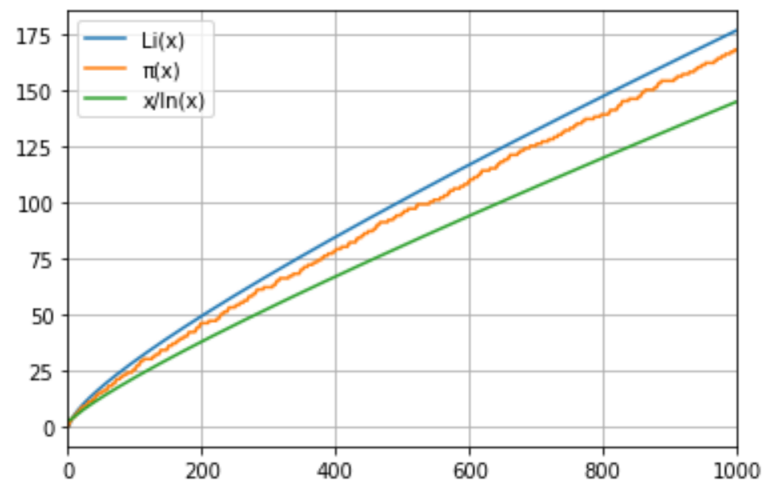
x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{x}{\ln x} - \pi(x)$	relativna greška(%)
10^2	25	21	4	16.00
10^3	168	144	24	14.29
10^4	1229	1085	144	11.72
10^5	9592	8685	907	9.46
10^6	78498	72382	6116	7.79
10^7	664579	620420	44159	6.64

Tablica 2: Relativna greška između vrijednosti funkcija $\frac{x}{\ln x}$ i $\pi(x)$

Kasnije je Gauss dao znatno bolju aproksimaciju funkcije π, koristeći takozvanu *logaritamsko-integralnu* funkciju:

$$Li(x) = \int_2^x \frac{1}{\ln t} dt.$$

Prikažemo li graf ove funkcije u istom koordinatnom sustavu u kojem su prikazani grafovi funkcija $\frac{x}{\ln x}$ i $\pi(x)$, odmah je očito kako je $Li(x)$ bolja aproksimacija funkcije $\pi(x)$.



Slika 9: Usporedba grafova funkcija $Li(x), \pi(x)$ i $\frac{x}{\ln x}$

Koliko je zaista funkcija $Li(x)$ bolja aproksimacija funkcije $\pi(x)$ nego što je to funkcija $\frac{x}{\ln x}$, možemo vidjeti u sljedećoj tablici napravljenoj za velike vrijednosti od x.

x	$\pi(x)$	$\frac{x}{\ln x} - \pi(x)$	$Li(x) - \pi(x)$
10^8	5761455	-332774	754
10^9	50847534	-2592592	1701
10^{10}	455052511	-20758030	3104
10^{11}	4,118054313	-169923160	11588
10^{12}	37607912018	-1416706193	38263
10^{13}	346065536839	-11992858452	108971
10^{14}	3,204941750802	-102838308636	314890

Tablica 3: Razlika između vrijednosti funkcija $Li(x), \pi(x)$ i $\frac{x}{\ln x}$

U ostatku rada bavit ćemo se Teoremom o prostim brojevima, točnije kako je on nastao i koje su funkcije bile nužne u njegovom dokazu.

4.1 Razvoj tvrdnje teorema o prostim brojevima

Prva objavljena tvrdnja slična teoremu o prostim brojevima pripisuje se Legendreu i datira iz 1798. godine. On je utvrdio da funkcija $\pi(x)$ ima oblik

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

za realne konstante A, B. Kasnije je tvrdnju poboljšao dobivajući da je

$$\pi(x) = \frac{x}{\log x + A(x)},$$

gdje je $\lim_{x\to\infty} A(x) = 1.08366$.

Prvu skicu dokaza Teorema o prostim brojevima dao je B. Riemann. U njegovoj je skici dokaza veliki doprinos imala zeta-funkcija, koja će se detaljnije objasniti u nastavku rada. Kasnije su, neovisno jedan o drugom, Jacques Hadamard i Charles Jean de la Vallée Poussin dali potpuni dokaz teorema.

Veliki doprinos u razmatranju distribucije prostih brojeva dao je ruski matematičar Pafnuti Lvovič Čebišev. On je dokazao tvrdnju da postoje pozitivni realni brojevi a i b takvi da je

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}, \tag{4.1}$$

za dovoljno velike realne brojeve $x \geq 2$. Tvrdnju ćemo najprije pokazati za $a = \frac{1}{8}, b = 6$, a kasnije ćemo te konstante "poboljšati" uz pomoć Čebiševljevih funkcija. U dokazu prethodno navedene tvrdnje potrebna nam je sljedeća lema, čiji se dokaz može naći u [3, Lema 7.1].

Lema 4.1. *Neka je $n \in \mathbb{N}$. Tada vrijedi:*

(i) $2^n \leq \binom{2n}{n} < 2^{2n}$,

(ii) $\prod\limits_{p\in S} p$ *dijeli* $\binom{2n}{n}$, *gdje je* $S = \{p \in \mathbb{P} | n < p \leq 2n\}$.

(iii) $\binom{2n}{n}$ *dijeli* $\prod\limits_{p\leq 2n} p^{\lfloor \log_p 2n \rfloor}$, *gdje je* $\lfloor x \rfloor$ *oznaka za najveći cijeli broj* $\leq x$.

(iv) Ako je $n > 2$ *i* $\frac{2n}{3} < p \leq n$, *onda* p *ne dijeli* $\binom{2n}{n}$.

(v) Vrijedi $\prod\limits_{p\leq n} p < 4^n$, *gdje je* $n \in \mathbb{N}$.

Sada možemo dokazati relaciju (4.1) za $a = \frac{1}{8}$ i $b = 6$.

Teorem 4.2. *Za* $n \geq 2$ *vrijedi*

$$\frac{n}{8\ln n} < \pi(n) < \frac{6n}{\ln n}.$$

Dokaz. Koristeći relacije (*ii*) i (*iii*) iz Leme 4.1, uočimo da vrijedi

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{p\leq 2n} p^{\lfloor \log_p 2n \rfloor} \leq (2n)^{\pi(2n)}.$$

Nadalje, ponovno koristeći Lemu 4.1 (*i*), slijedi

$$n^{\pi(2n)-\pi(n)} < 2^{2n} \text{ i } 2^n \leq (2n)^{\pi(2n)}. \tag{4.2}$$

Stavimo da je $n = 2^k$ u prethodnoj jednakosti pa dobivamo

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1} \text{ i } 2^k \leq (k+1)\pi(2^{k+1}).$$

Kako je $\pi(2^{k+1}) \leq 2^k$, slijedi

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < \pi(2^{k+1}) + 2^{k+1} \leq 3 \cdot 2^k. \tag{4.3}$$

Zbrojimo relacije (4.3) za $k = m, m-1, \ldots, 1, 0$ te nakon kraćenja dobivamo

$$(m+1)\pi(2^{m+1}) \leq 3(2^m + 2^{m-1} + \cdots + 2^1 + 2^0) < 3 \cdot 2^{m+1}.$$

Iz prethodne nejednakosti i relacije (4.2), možemo zaključiti da vrijedi

$$\frac{2^m}{m+1} \leq \pi(2^{m+1}) < \frac{3 \cdot 2^{m+1}}{m+1}. \tag{4.4}$$

Stavimo da je $m = \lfloor \log_2 n \rfloor - 1$, za $n \in \mathbb{N}, n \geq 2$. Tada je $2^{m+1} \leq n < 2^{m+2}$. Nadalje, uočimo da za svaki $x > 0$ vrijedi

$$\ln 2^x = x \ln 2 < x \text{ i } \ln 2^x > \frac{x}{2}.$$

Konačno, iz (4.4) dobivamo

$$\pi(n) \leq \pi(2^{m+2}) < \frac{3 \cdot 2^{m+2}}{m+2} < \frac{6 \cdot 2^{m+1}}{\ln(2^{m+2})} < \frac{6n}{\ln n} \text{ i}$$

$$\pi(n) \geq \pi(2^{m+1}) > \frac{2^m}{m+1} = \frac{2^{m+2}}{8 \cdot \frac{m+1}{2}} > \frac{2^{m+2}}{8 \ln(2^{m+1})} > \frac{n}{8 \ln n}.$$

□

U sljedećem poglavlju pokazat ćemo kako se pomoću Čebiševljevih funkcija može doći do boljih konstanti nego što su one u prethodnom teoremu.

4.2 Čebiševljeve funkcije

Važnu ulogu u distribuciji prostih brojeva imaju Čebiševljeve funkcije. Te je funkcije prvi definirao ruski matematičar Pafnuty Lvovich Čebišev. Pomoću njih dolazimo do boljih konstanti a i b od onih u Teoremu 4.2. Najprije navodimo definiciju Von Manoldtove funkcije koju ćemo koristiti u definiranju Čebiševljevih funkcija.

Definicija 4.2. *Von Mangoldtova funkcija, u oznaci* $\Lambda(n), n \in \mathbb{N}$, *definirana je s:*

$$\Lambda(n) = \begin{cases} \ln p\,, & \text{ako je } n = p^k, p \in \mathbb{P}, \\ 0 & , \text{inače.} \end{cases}$$

Definicija 4.3. *Čebiševljeve funkcije* ψ *i* ϑ *definiraju se s:*

$$\psi(x) = \sum_{n \leq x} \Lambda(n), \qquad \vartheta(x) = \sum_{p \leq x} \ln p,$$

pri čemu je x *realan broj.*

Kako bi dokazali relaciju (4.1) s boljim konstantama a i b, koristiti ćemo sljedeći rezultat. Dokaz ovog teorema može se naći u [3, Teorem 7.6].

Teorem 4.3. *Neka je* $a_0 = \frac{1}{3}\ln 2 + \frac{1}{2}\ln 3 \approx 0.7804$ *i* $b_0 = \frac{3}{2}a_0 \approx 1.1705$. *Ako je* $a < a_0$ *i* $b > b_0$, *onda postoji realan broj* x_0 *koji ovisi o* a *i* b, *takav da vrijedi*

$$ax < \psi(x) < bx,$$

za sve $x > x_0$.

Uvedimo sada sljedeću oznaku (veliko O):

$f(x) = O(g(x))$ ako postoji realna konstanta C takva da je $|f(x)| \leq Cg(x)$,

za dovoljno velike realne brojeve x. Ova se oznaka često koristi u teoriji brojeva, a uvodi se zato što je često potrebno ispitati asimptotsko ponašanje neke funkcije. Također se koristi i za usporedbu dviju funkcija kada argument teži u beskonačno na sljedeći način:
Ako postoje realne konstante B, C takve da je $|f(x) - h(x)| \leq C \cdot g(x)$, za sve $x \geq B$, onda pišemo $f(x) = h(x) + O(g(x))$. Slično, uvodimo i oznaku (malo o):

$$f(x) = o(g(x)) \text{ ako je } \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Oznaku veliko O koristimo u sljedećoj tvrdnji.

Teorem 4.4. *Za realni broj* $x \geq 1$ *vrijedi*

$$\vartheta(x) = \psi(x) + O(\sqrt{x}).$$

Dokaz. Iz Definicije 4.3 očito vrijedi $\vartheta(x) \leq \psi(x)$, za sve realne brojeve x. Preostaje još pronaći gornju ogradu za $\psi(x) - \vartheta(x)$. Vrijedi

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p^k \leq x} \ln p = \sum_{k} \sum_{p \leq \sqrt[k]{x}} \ln p = \sum_{k} \vartheta(\sqrt[k]{x}).$$

Stavimo da je $K = \lfloor \frac{\ln x}{\ln 2} \rfloor$. Za $k > K$ vrijedi $\sqrt[k]{x} < 2$, pa je $\vartheta(\sqrt[k]{x}) = 0$. Primjenimo li to na Teorem 4.3, dobivamo

$$\psi(x) - \vartheta(x) = \sum_{2 \leq k \leq K} \vartheta(\sqrt[k]{x}) \leq \sum_{2 \leq k \leq K} \psi(\sqrt[k]{x}) = \sum_{2 \leq k \leq K} O(\sqrt[k]{x}).$$

Nadalje, uočimo da konstanta vezana uz O ne ovisi o k te da članovi u sumi opadaju. Zbog toga je

$$\psi(x) - \vartheta(x) = O(\sqrt{x} + K\sqrt[3]{x}) = O\big(\sqrt{x} + \sqrt[3]{x}\ln x\big) = O(\sqrt{x}).$$

□

Ponovimo sada važan rezultat iz matematičke analize.

Teorem 4.5 (**Abelova formula parcijalne sumacije**). *Neka je $a_1, a_2, \ldots$ niz realnih brojeva te $s(x) = \sum_{n \leq x} a_n$. Nadalje, neka su x i y realni brojevi takvi da je $0 \leq y < x$ te f(u) realna funkcija s neprekidnom derivacijom f'(u) na intervalu [y, x]. Tada vrijedi*

$$\sum_{y < n \leq x} a_n f(n) = s(x)f(x) - s(y)f(y) - \int_y^x s(u)f'(u)du. \tag{4.5}$$

Koristeći se do sada navedenim tvrdnjama, prije dokaza relacije (4.1) preostaje nam pokazati sljedeći rezultat.

Teorem 4.6. *Za realan broj $x \geq 2$ vrijedi*

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big).$$

Dokaz. Pokažimo najprije da za $x \geq 2$ vrijedi

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + \int_2^x \frac{\vartheta(u)}{u \ln^2 u} du. \tag{4.6}$$

Uočimo da vrijedi

$$\pi(x) - \frac{\vartheta(x)}{\ln x} = \sum_{p \leq x} \ln p \Big(\frac{1}{\ln p} - \frac{1}{\ln x}\Big).$$

Primjenimo formulu (4.5) iz prethodnog teorema, uz $f(u) = \frac{1}{\ln u} - \frac{1}{\ln x}$ te $a_n = \ln p$ ako je $n = p$ prost, a $a_n = 0$ inače. Tada dobivamo

$$\pi(x) - \frac{\vartheta(x)}{\ln x} = \vartheta(x)\Big(\frac{1}{\ln x} - \frac{1}{\ln x}\Big) - \int_2^x \vartheta(u)\Big(\frac{1}{\ln u} - \frac{1}{\ln x}\Big)' du = \int_2^x \frac{\vartheta(u)}{u \ln^2 u} du,$$

tj. pokazali smo da (4.6) vrijedi.
Kako je $0 \leq \vartheta(x) \leq \psi(x)$, iz Teorema 4.3 slijedi da je $\vartheta(x) = O(x)$. Zbog toga možemo zaključiti da je integral u (4.6) jednak $O(\int_2^x \ln^{-2} u du)$. Rastavimo sada područje integracije na dva dijela:

$$2 \leq u \leq \sqrt{x} \text{ i } \sqrt{x} \leq u \leq x.$$

Uočimo da je na prvom dijelu podintegralna funkcija omeđena, pa je doprinos tog dijela jednak $O(\sqrt{x})$. Na drugom je dijelu podintegralna funkcija manja ili jednaka $\frac{4}{\ln^2 x}$ pa je doprinos tog dijela $O(\frac{x}{\ln^2 x})$. □

Konačno, možemo dokazati relaciju (4.1) uz bolje konstante a i b nego što su bile one u prethodnom poglavlju, odnosno možemo pokazati sljedeći teorem.

Teorem 4.7. *Neka je $a_0 = \frac{1}{3}\ln 2 + \frac{1}{2}\ln 3 \approx 0.7804$ i $b_0 = \frac{3}{2}a_0 \approx 1.1705$. Ako je $a < a_0$ i $b > b_0$, onda za sve dovoljno velike x vrijedi*

$$a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}. \tag{4.7}$$

Dokaz. Uočimo da vrijedi

$$\pi(x) = \frac{\vartheta(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big) = \frac{\psi(x)}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big) \leq \frac{b_0 + b}{2} \cdot \frac{x}{\ln x} + O\Big(\frac{x}{\ln^2 x}\Big),$$

pri čemu smo koristili Teoreme 4.6, 4.4 i 4.3. Time dobivamo gornju ogradu u (4.7) za dovoljno velike x. Slično se za dovoljno velike x dobije

$$\pi(x) \geq \tfrac{a_0+a}{2} \cdot \tfrac{x}{\ln x} + O(\tfrac{x}{\ln^2 x}).$$

□

Napomena 4.1. *Pomoću teorema 4.6 i 4.4 slijedi da je Teorem o prostim brojevima ekvivalentan s*

$$\vartheta(x) \sim x \text{ i } \psi(x) \sim x.$$

Osim Teorema o prostim brojevima, vrlo bitan rezultat vezan uz distribuciju prostih brojeva je takozvani Bertrandov postulat. Ova se tvrdnja u mnogim izvorima zove i Bertrand-Čebiševljev teorem, upravo iz razloga što ga je prvi dokazao Čebišev 1852. godine. Taj teorem glasi:

Teorem 4.8. *Za svaki prirodan broj n postoji prosti broj p takav da je $n < p \leq 2n$.*

Sada nam je cilj dati vrlo sažetu skicu dokaza prehodno navedenog teorema u svrhu ilustracije važnosti Čebiševljevih funkcija. Napomenimo da je 1932. godine Edős dao alternativni dokaz koji se može naći u [3, Teorem 7.3]. Dokaz Bertrandovog postulata zasniva se na sljedeće dvije leme.

Lema 4.2. *Za $x > 750$ vrijedi*

$$\psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) > \frac{2}{3}x.$$

Dokaz. Slijedi direktno iz sljedeće dvije tvrdnje, čiji se dokazi mogu naći u [2, Poglavlje 4.6].

Tvrdnja 1. *Za pozitivan realan broj x vrijedi*

$$\psi(x) - \psi\left(\frac{x}{2}\right) \leq \ln(x)! - 2\ln(x/2)! \leq \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right).$$

Tvrdnja 2. *Za realan broj $x > 750$ vrijedi*

$$\ln(x)! - 2\ln(x/2)! > \frac{2}{3}x.$$

□

Lema 4.3. *Za svaki pozitivan realan broj x vrijedi*

$$\psi(x)-\psi\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right) \leq \vartheta(x)+2\psi(\sqrt{x})-\vartheta\left(\frac{x}{2}\right)+\psi\left(\frac{x}{3}\right) < \vartheta(x)-\vartheta\left(\frac{x}{2}\right)+\frac{x}{2}+3\sqrt{x}.$$

Kao i u prethodnoj lemi, koristiti ćemo dvije tvrdnje koje nećemo dokazivati, a čiji se dokazi mogu naći u [2, Poglavlje 4.6].

Tvrdnja 3. *Za pozitivan realan broj x vrijedi*

$$\psi(x) - 2\psi(\sqrt{x}) \leq \vartheta(x) \leq \psi(x).$$

Tvrdnja 4. *Za svaki realan broj $x > 0$ vrijedi*

$$\psi(x) < \frac{3}{2}x.$$

Dokažimo sada Lemu 4.3

Dokaz Leme 4.3. Prema tvrdnji 3 vrijedi

$$\psi(x) - 2\psi(\sqrt{x}) \leq \vartheta(x),$$

to jest

$$\psi(x) \leq \vartheta(x) + 2\psi(\sqrt{x}).$$

Nadalje, ponovno prema tvrdnji 3 vrijedi

$$\vartheta\Big(\frac{x}{2}\Big) \leq \psi\Big(\frac{x}{2}\Big).$$

Koristeći prethodne nejednakosti, dobivamo

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) + \psi\Big(\frac{x}{3}\Big) \leq \vartheta(x) + 2\psi(\sqrt{x}) - \vartheta\Big(\frac{x}{2}\Big) + \psi\Big(\frac{x}{3}\Big).$$

Za drugu nejednakost iz tvrdnje leme, koristimo tvrdnju 4 kako bi zaključili da vrijedi

$$2\psi(\sqrt{x}) + \psi\Big(\frac{x}{3}\Big) \leq 3\sqrt{x} + \frac{x}{3}.$$

□

Sada smo spremni dokazati Bertrandov postulat.

Dokaz Teorema 4.8. Prema lemi 4.2. vrijedi

$$\psi(x) - \psi\Big(\frac{x}{2}\Big) + \psi\Big(\frac{x}{3}\Big) \geq \frac{2}{3}x,$$

za $x > 750$. Nadalje, iz leme 4.3. možemo zaključiti da vrijedi

$$\vartheta(x) - \vartheta\Big(\frac{x}{2}\Big) \geq 2\frac{x}{3} - \frac{x}{2} - 3\sqrt{x},$$

što znači da postoji prost broj između x i $2x$ za $x > 750$. Tvrdnja teorema za $n \leq 750$ slijedi iz činjenice da je sljedećem nizu prostih brojeva

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

svaki član manji od dvostrukog prethodnog člana. □

4.3 Riemannova zeta-funkcija

Zeta funkcija jedna je od najvažnijih funkcija u matematici. Iako ju Riemann nije prvi definirao, nazvana je po njemu jer je on prvi dokazao vezu između nultočaka te funkcije i distribucije prostih brojeva. Njegovi su rezultati i ideje bili krucijalni za dokaz teorema o prostim brojevima. Za početak navedimo definiciju zeta-funkcije.

Definicija 4.4. *Riemannova zeta-funkcija definirana je s*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

gdje je $s \in \mathbb{C}$ *takav da je* $Re(s) > 1$.

Uvjet $Re(s) > 1$ u prethodnoj definiciji osigurava da red $\sum_{n=1}^{\infty} \frac{1}{n^s}$ apsolutno konvergira. Naime, vrijedi

$$\begin{aligned} |\zeta(s)| &= \Big|\sum_{n=1}^{\infty} \frac{1}{n^s}\Big| \leq \sum_{n=1}^{\infty} \Big|\frac{1}{n^s}\Big| = \sum_{n=1}^{\infty} \frac{1}{|n^s|} = \sum_{n=1}^{\infty} \frac{1}{|n^{\sigma+it}|} = \sum_{n=1}^{\infty} \frac{1}{|n^{\sigma}||n^{it}|} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}|e^{it\log(n)}|} = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}}. \end{aligned}$$

Hiperharmonijski red[2] $\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}}$ konvergira za $\sigma > 1$, čime je pokazana gornja tvrdnja.

Važnost Riemannove zeta-funkcije u distribuciji prostih brojeva veže se uz računanje nultočaka te funkcije. Sljedeći teorem daje osnovnu vezu između Riemannove zeta-funkcije i prostih brojeva. Navedena jednakost naziva se Eulerova produktna formula.

Teorem 4.9. *Vrijedi*

$$\zeta(s) = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}. \tag{4.8}$$

Dokaz. Neka su $M, N \in \mathbb{N}$ takvi da je $M > N$. Prema Osnovnom teoremu aritmetike (Teorem 2.2), svaki se pozitivan prirodni broj n takav da je $n \leq N$ može na jedinstveni način zapisati kao umnožak prostih brojeva. Također, znamo da svaki prosti broj u tom umnošku mora biti manji ili jednak N (inače bi vrijedilo $n > N$, što bi bila kontradikcija) te da se svaki od njih u tom umnošku javlja manje od M puta. Dakle, vrijedi

$$\begin{aligned} \sum_{n=1}^{N} \frac{1}{n^s} &\leq \prod_{p\leq N} \Big(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}}\Big) \\ &= \prod_{p\leq N} \Big(\frac{1}{1-p^{-s}} - \sum_{n=Ms+1}^{\infty} \frac{1}{p^{ns}}\Big) \\ &\leq \prod_{p\leq N} \Big(\frac{1}{1-p^{-s}}\Big) \\ &\leq \prod_{p\in\mathbb{P}} \Big(\frac{1}{1-p^{-s}}\Big). \end{aligned}$$

[2]Hiperharmonijski red je red $\sum_{n=1}^{\infty} a_n$ s članovima oblika $a_n = \frac{1}{n^{\alpha}}$, gdje je $\alpha \in \mathbb{R}$.

Pustimo li da N teži u beskonačnost, dobivamo

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \prod_{p \in \mathbb{P}} \Big(\frac{1}{1-p^{-s}} \Big).$$

Obratno, ponovno koristeći Osnovni teorem aritmetike, vrijedi

$$\prod_{p \leq N} \Big(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots + \frac{1}{p^{Ms}} \Big) \leq \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Pustimo da M teži u beskonačnost i dobivamo

$$\prod_{p \leq N} \Big(\frac{1}{1-p^{-s}} \Big) \leq \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Stoga je

$$\prod_{p \in \mathbb{P}} \Big(\frac{1}{1-p^{-s}} \Big) \leq \sum_{n=1}^{\infty} \frac{1}{n^s},$$

čime je tvrdnja teorema dokazana. $\square$

4.3.1 Nultočke zeta-funkcije

Kao što smo i prehodno naveli, veza između Riemannove zeta-funkcije i distribucije prostih brojeva vezana je uz nultočke te funkcije. U ovom ćemo dijelu rada njih detaljnije opisati. Prije nego što krenemo na tvrdnje vezane za nultočke zeta-funkcije, moramo definirati i dokazati osnovna svojstva sljedeće funkcije.

Definicija 4.5. *Gama funkcija je definirana s*

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt,$$

gdje je $s \in \mathbb{C}, Re(s) > 0$.

Gama funkcija zbog svojih svojstava zasigurno spada u najvažnije funkcije u matematici. Svrha uvođenja ove funkcije je njezina veza s Riemannovom zeta-funkcijom. Gama funkcija ima sljedeće vrlo bitno svojstvo.

Lema 4.4. *Ako je* $Re(s) > 0$, *onda vrijedi*

$$\Gamma(s+1) = s\Gamma(s). \tag{4.9}$$

Nadalje, za $n = 0, 1, 2, \ldots$ *vrijedi* $\Gamma(n+1) = n!$.

Dokaz. Parcijalnom integracijom dobivamo

$$\int_{\epsilon}^{1/\epsilon} \frac{d}{dt}(e^{-t}t^s)dt = -\int_{\epsilon}^{1/\epsilon} e^{-t}t^s dt + s\int_{\epsilon}^{1/\epsilon} e^{-t}t^{s-1}dt.$$

Pustimo li da ϵ teži u 0, lijeva strana jednakosti nestaje jer $e^{-t}t^s \to 0$, za $t \to 0$ ili $t \to \infty$. Time je jednakost (4.9) dokazana.
Pokažimo sada da je $\Gamma(n+1) = n!$, za $n = 0, 1, 2, \ldots$ Uočimo da vrijedi

$$\Gamma(1) = \int_0^\infty e^{-t}dt = [-e^{-t}]_0^\infty = 1.$$

Tražena tvrdnja slijedi iz relacije (4.9). □

Sada navedimo još nekoliko bitnih svojstava Gama funkcije.

Teorem 4.10. *Za sve $s \in \mathbb{C}$ vrijedi*

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}.$$

Za dokazati prethodni teorem, potreban je sljedeći "trik" dan u sljedećoj lemi. Dokaz leme može se naći u [18, Lema 1.5].

Lema 4.5. *Za $0 < a < 1$ vrijedi*

$$\int_0^\infty \frac{v^{a-1}}{1+v}dv = \frac{\pi}{\sin \pi a}.$$

Dokaz Teorema 4.10. Za $0 < s < 1$ vrijedi

$$\Gamma(1-s) = \int_0^\infty e^{-u}u^{-s}du = t\int_0^\infty e^{-vt}(vt)^{-s}dv,$$

gdje smo za $t > 0$ primjenili supstituciju varijabli $vt = u$. Koristeći prethodnu jednakost i Lemu 4.5, dobivamo

$$\begin{aligned}
\Gamma(1-s)\Gamma(s) &= \int_0^\infty e^{-t}t^{s-1}\Gamma(1-s)dt \\
&= \int_0^\infty e^{-t}t^{s-1}\Big(t\int_0^\infty e^{-vt}(vt)^{-s}dv\Big)dt \\
&= \int_0^\infty \int_0^\infty e^{-t(1+v)}v^{-s}dvdt \\
&= \int_0^\infty \frac{v^{-s}}{1+v}dv \\
&= \frac{\pi}{\sin \pi(1-s)} \\
&= \frac{\pi}{\sin \pi s},
\end{aligned}$$

čime je tvrdnja teorema dokazana. □

Sada nam je cilj dokazati da Gama funkcija nema nultočaka u $\mathbb{C}$. Da bismo to učinili, potrebna su nam neka svojstva njoj recipročne funkcije $\frac{1}{\Gamma}$. Dokaz sljedećeg teorema nećemo navoditi, a on se može naći u [18, Teorem 1.6].

Teorem 4.11. *Funkcija $\frac{1}{\Gamma(s)}$ je holomorfna funkcija čija je domena cijela kompleksna ravnina te ima jednostruke nultočke $s = 0, -1, -2, \ldots$.*

Sljedeći teorem daje bitan zapis funkcije $\frac{1}{\Gamma}$. Dokaz ovog teorema može se naći u [18, Teorem 1.7].

Teorem 4.12. *Za sve $s \in \mathbb{C}$ vrijedi*

$$\frac{1}{\Gamma(s)} = e^{\gamma s} s \prod_{n=1}^{\infty} \Big(1 + \frac{s}{n}\Big) e^{-s/n},$$

gdje je realan broj γ, koji se još zove i Eulerova konstanta, definiran s

$$\gamma = \lim_{N \to \infty} \sum_{n=1}^{N} \frac{1}{n} - \log N.$$

Napomena 4.2. *Iz prethodnog zapisa funkcije $\frac{1}{\Gamma(s)}$ vidimo da je ona definirana za sve $s \in \mathbb{C}$, odnosno da nema polova. Prema tome, funkcija $\Gamma(s)$ nema nultočaka, jer kada bi imala, one bi bile polovi od $\frac{1}{\Gamma(s)}$.*

Osim Gama funkcije, za određivanje nultočaka zeta-funkcije potrebna nam je i sljedeća modifikacija te funkcije.

Definicija 4.6. *Za $Re(s) > 1$ definiramo funkciju xi s*

$$\xi(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s).$$

Za funkciju ξ vrijedi sljedeće svojstvo koje je poznato i kao Fundamentalna jednakost. Dokaz ovog teorema može se naći u [18, Teorem 2.3].

Teorem 4.13. *Vrijedi $\xi(s) = \xi(1 - s)$, za sve $s \in \mathbb{C}$.*

Pri ispitivanju nultočaka Riemannove zeta funkcije, područje $0 \leq Re(s) \leq 1$, za $s \in \mathbb{C}$, ćemo nazivati kritično područje, a nultočke koje se nalaze izvan tog područja trivijalne nultočke. Sljedeća lema potrebna nam je za opisati trivijalne nultočke zeta-funkcije. Njezin se dokaz može naći u [18, Propozicija 3.1].

Lema 4.6. *Neka je $\{a_n\}$ red kompleksnih brojeva. Ako je $\displaystyle\sum_{n=1}^{\infty} |a_n| < \infty$, onda umnožak $\displaystyle\prod_{n=1}^{\infty} (1 + a_n)$ konvergira. Nadalje, umnožak teži k 0 ako i samo ako je jedan od njegovih faktora jednak 0.*

Teorem 4.14. *Jedine nultočke funkcije* ζ *izvan kritičnog područja* $0 \leq Re(s) \leq 1$ *su negativni parni cijeli brojevi* $-2, -4, -6, \ldots$.

Dokaz. U Teoremu 4.9 pokazali smo da vrijedi

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

za $s \in \mathbb{C}$. Sada koristeći Lemu 4.6, zaključujemo da funkcija ζ nema nultočaka kada je $Re(s) > 1$. Dakle, preostaje još ispitati nultočke u području $Re(s) < 0$.
Fundamentalnu jednakost $\xi(s) = \xi(1-s)$ možemo zapisati u obliku

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

odnosno

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

Uočimo da za $Re(s) < 0$ vrijede sljedeće tvrdnje:

(i) $\zeta(1-s)$ nema nultočaka jer je $Re(1-s) > 1$.

(ii) $\Gamma((1-s)/2)$ nema nultočaka.

(iii) $\frac{1}{\Gamma(s/2)}$ ima nultočke u $s = -2, -4, -6, \ldots$

Dakle, iz toga zaključujemo da su jedine nultočke funkcije ζ u području $Re(s) < 0$ negativni parni brojevi $-2, -4, -6, \ldots$. □

Ostaje još proučiti nultočke zeta funkcije u kritičnom području. Ključna tvrdnja u dokazu Teorema o prostim brojevima je da ζ nema nultočaka na pravcu $Re(s) = 1$. Kao jednostavna posljedica te tvrdnje slijedi da zeta funkcija nema nultočaka na pravcu $Re(s) = 0$. Dakle, cilj nam je pokazati sljedeći teorem.

Teorem 4.15. *Zeta funkcija nema nultočaka na pravcu* $Re(s) = 1$.

Ključna tvrdnja u dokazu prethog teorema je sljedeća lema.

Lema 4.7. *Neka je* $\sigma > 1$ *i* t *realan broj. Tada vrijedi*

$$\log|\zeta^3(\sigma)\zeta^4(\sigma + it)\zeta(\sigma + 2it)| \geq 0.$$

U dokazu ove leme, potrebna nam je još jedna lema, čiji se dokaz može naći u [18, Korolar 1.5].

Lema 4.8. *Ako je $Re(s) > 1$, vrijedi*

$$\log\zeta(s) = \sum_{p,m} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} c_n n^{-s},$$

za neki $c_n \geq 0$.

Dokaz leme 4.7. Neka je $s = \sigma + it$, gdje su $\sigma, t \in \mathbb{R}$. Tada vrijedi

$$Re(n^{-s}) = Re(e^{-(\sigma+it)\log n}) = e^{-\sigma \log n}\cos(t\log n) = n^{-\sigma}\cos(t\log n).$$

Nadalje, vrijedi

$$\begin{aligned}
& \log(\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)) = \\
= \;& 3\log(\zeta(\sigma)) + 4\log(\zeta(\sigma+it)) + \log(\zeta(\sigma+2it)) \\
= \;& 3Re[\log(\zeta(\sigma))] + 4Re[\log\zeta(\sigma+it)] + Re[\log\zeta(\sigma+2it)] \\
= \;& \sum c_n n^{-\sigma}(3 + 4\cos\theta_n + \cos 2\theta_n),
\end{aligned}$$

gdje je $\theta_n = t\log n$. Uočimo da vrijedi

$$3 + 4\cos\theta + \cos 2\theta = 2(1+\cos\theta) \geq 0,$$

za $\theta \in \mathbb{R}$, te kako je $c_n \geq 0$ (Lema 4.8.), zaključujemo da je

$$\log(\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)) \geq 0,$$

što je trebalo i pokazati. □

Sada možemo dokazati Teorem 4.15.

Dokaz Teorema 4.15. Pretpostavimo suprotno, tj. pretpostavimo da je $\zeta(1+it_0) = 0$, za neki $t_0 \neq 0$ realni broj. Kako je ζ holomorfna, mora imati barem jednu nultočku reda 1 u $1 + it_0$. Dakle,

$$|\zeta(\sigma + it_0)|^4 \leq C(\sigma - 1)^4 \quad za \quad \sigma \to 1,$$

za neku realnu konstantu $C > 0$. Također, kako funkcija $\zeta(s)$ ima pol u $s = 1$, vrijedi

$$|\zeta(\sigma)|^3 \leq C'(\sigma - 1)^{-3} \quad za \quad \sigma \to 1,$$

za neku realnu konstantu $C' > 0$. Konačno, kako je ζ holomorfna, u točkama $\sigma + 2it_0$ izraz $|\zeta(\sigma + 2it_0)|$ ostaje omeđen kada $\sigma \to 1$. Kombinirajući prethodne tvrdnje, slijedi

$$|\zeta^3(\sigma)\zeta^4(\sigma+it)\zeta(\sigma+2it)| \to 0 \quad za \quad \sigma \to 1,$$

što je kontradikcija s lemom 4.8, jer je logaritam realnog broja između 0 i 1 uvijek negativan. Time je pokazano da ζ nema nultočaka na realnom pravcu $Re(s) = 1$. □

Proučavajući nultočke zeta-funkcije, Riemann je uočio da bi moglo vrijediti:

Nultočke funkcije $\zeta(s)$ u kritičnom području leže na pravcu $Re(s) = 1/2$.

Ova je tvrdnja poznata kao *Riemannova hipoteza* i smatra se jednom od najpoznatijih nedokazanih matematičkih slutnji današnjice. Istinitost Riemannove hipoteze značila bi da bi mnogi teoremi bili automatski dokazani.

Postoji mnogo razloga za vjerovati da je Riemannova hipoteza istinita. Do sada je provedena provjera te tvrdnje do vrlo visokih vrijednosti, što sugerira njezinu istinitost. Zapravo, brojčane provjere za ovu hipotezu dovoljno su jaki da se mogu smatrati eksperimentalno potvrđenima u drugim područjima kao što su fizika i kemija. Međutim, kroz povijest matematike bilo je više takvih tvrdnji koje su se brojčano provjerile za vrlo visoke vrijednosti, ali su se ipak pokazale netotčnima. Jedan od takvih rezultata je poznata priča o Skewesovom broju, vrlo velikom broju pomoću kojeg se dokazala netočnost jedne od Gaussovih pretpostavki da je logaritamski integral $Li(x)$ uvijek veći od funkcije $\pi(x)$. Ova je pretpostavka bila provjerena za vrlo velike vrijednosti, zbog čega se smatrala istinitom. Na kraju je Littlewood dokazao da ova tvrdnja vrijedi za sve realne brojeve x koji su manji od Skewesovog broja, odnosno da ova pretpostavka nije istinita.

To bi također mogao biti slučaj s Riemannovom hipotezom, koja je do sada potvrđena za 10^{12} netrivijalnih nultočaka.

4.4 Skica dokaza teorema o prostim brojevima

Kao što smo i prethodno naveli, prvi dokaz teorema o prostim brojevima dali su Hadamard i Poussin. U ovom ćemo poglavlju dati skicu dokaza kojeg su osmislili matematičari Paul Erdős i Atle Selberg. Ovaj se dokaz smatra prvim elementarnim dokazom teorema o prostim brojevima jer se u njemu ne koriste tvrdnje iz kompleksne analize, već samo neka osnovna svojstva logaritamske funkcije.

Za početak, prisjetimo se definicije Čebiševljeve funkcije:

$$\vartheta(x) = \sum_{p \leq x} \ln p,$$

gdje je $p \in \mathbb{P}$, a x realan broj. Ovaj dokaz je još jedna ilustracija važnosti Čebiševljevih funkcija u istraživanju distribucije prostih brojeva. Iz definicije prethodne funkcije jasno je da vrijedi

$$\pi(x) \sim \frac{x}{\log x} \iff \vartheta(x) \sim x.$$

Dakle, dokazat ćemo tvrdnju ekvivalentnu tvrdnji Teorema o prostim brojevima:

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

Glavni "alat" u dokazivanju teorema o prostim brojevima je takozvana Selbergova fundamentalna formula

$$\vartheta(x)\log x + \sum_{p\le x} \log p\,\vartheta\Big(\frac{x}{p}\Big) = 2x\log x + O(x).$$

Dokaz ove formule može se naći u [14, Poglavlje 2].

Definirajmo sada

$$a = \liminf_{x\to\infty} \frac{\vartheta(x)}{x} \text{ i } A = \limsup_{x\to\infty} \frac{\vartheta(x)}{x}. \tag{4.10}$$

Sylvesterova procjena garantira da je

$$0.956 \le a \le A \le 1.045.$$

Za dokaz Teorema o prostim brojevima ključna je sljedeća lema.

Lema 4.9. *Vrijedi:*

$$a + A = 2,$$

gdje su a i A definirani kao u (4.10).

Dokaz. Uzmimo dovoljno velik realan broj x takav da vrijedi

$$\vartheta(x) = ax + o(x).$$

Kako je $\vartheta(x) \le Ax + o(x)$, iz Selbergove fundamentalne formule slijedi

$$ax\log x + \sum_{p\le x} A\frac{x}{p}\log p \ge 2x\log x + o(x\log x).$$

Koristeći Čebiševljev rezultat da je

$$\sum_{p\le x} \frac{\log p}{p} \sim \log x,$$

direktno slijedi da je $a + A \ge 2$. S druge strane, možemo odabrati dovoljno velik realan broj x takav da vrijedi

$$\vartheta(x) = Ax + o(x).$$

Kako je $\vartheta(x) \geq ax + o(x)$, iz Selbergove fundamentalne formule slijedi

$$Ax \log x + \sum_{p \leq x} a \frac{x}{p} \log p \leq 2x \log x + o(x \log x),$$

iz čega dobijemo $a + A \leq 2$. Dakle, vrijedi

$$a + A = 2.$$

□

Preostaje još pokazati da je $a = A = 1$. Iz toga će slijediti

$$\liminf_{x \to \infty} \frac{\vartheta(x)}{x} = \limsup_{x \to \infty} \frac{\vartheta(x)}{x} = \lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1.$$

Uzmimo dovoljno velik realan broj x takav da je

$$\vartheta(x) = ax + o(x).$$

Uvrstimo li prethodnu jednakost u Selbergovu fundamentalnu formulu dobivamo

$$(\vartheta(x) - ax) \log x + \sum_{p \leq x} \log p \left(\vartheta\left(\frac{x}{p}\right) - A \frac{x}{p} \right) = O(x).$$

Iz toga možemo zaključiti da za fiksan pozitivan realan broj δ vrijedi

$$\vartheta\left(\frac{x}{p}\right) > (A - \delta) \frac{x}{p}, \tag{4.11}$$

za sve osim za specijalan skup (označimo taj skup s P_1) prostih brojeva koji su manji ili jednaki x i takvi da vrijedi

$$\sum \frac{\log p}{p} = o(\log x).$$

Obratno, može se pokazati da postoji realan broj x' takav da je $\sqrt{x} < x' < x$ i

$$\vartheta(x') = Ax' + o(x').$$

Ponovimo li sličan postupak kao ranije, uz zamjenu a s A te x s x', dobivamo

$$\vartheta\left(\frac{x'}{p}\right) < (a + \delta) \frac{x'}{p}, \tag{4.12}$$

za sve osim za specijalan skup (označimo taj skup s P_2) prostih brojeva koji su manji ili jednaki x' i takvi da vrijedi

$$\sum \frac{\log p}{p} = o(\log x).$$

Erdos je pokazao da je moguće pronaći proste brojeve $p \in P_1$ i $p' \in P_2$ takve da je
$$\frac{x}{p} < \frac{x'}{p'} < (1+\delta)\frac{x}{p}.$$
Sada iz (4.11) i (4.12) dobivamo
$$(A-\delta)\frac{x}{p} < \vartheta\Big(\frac{x}{p}\Big) \le \vartheta\Big(\frac{x'}{p'}\Big) < (a+\delta)\frac{x'}{p'} < (a+\delta)(1+\delta)\frac{x}{p},$$
odnosno
$$A-\delta < (a+\delta)(1+\delta).$$
Pustimo li da δ ide u 0 dobivamo
$$A \le a.$$
Također, znamo da je $A \ge a$ i kako smo pokazali da je $a + A = 2$, slijedi $a = A = 1$. Time je dovršen dokaz teorema o prostim brojevima.

4.5 Dirichletova L-funkcija

Poznati njemački matematičar Peter Gustav Lejeune Dirichlet također se bavio distribucijom prostih brojeva. On je poopćio Riemannovu zeta-funkciju te je formirao novu koja je po njemu dobila i ime. Glavni razlog zbog kojeg uvodimo ovu funkciju je sljedeći rezultat poznat i kao *Dirichletov teorem o prostim brojevima u aritmeičkom nizu.*

Teorem 4.16. *Neka su k, l relativno prosti*[3] *prirodni brojevi. Tada postoji beskonačno mnogo prostih brojeva oblika $l + kn, n \in \mathbb{N}$.*

Cilj ovog poglavlja je definirati i navesti osnovna svojstva Dirichletove L-funkcije te dokazati prethodno navedeni teorem. Za početak uvodimo Dirichletov karakter modulo k.

Definicija 4.7. *Neka je $k \in \mathbb{N}$. Dirichletov karakter modulo k je funkcija $\chi : \mathbb{N} \to \mathbb{C}$ takva da vrijedi:*

(i) $\chi(mn) = \chi(m)\chi(n)$, *za sve* $m, n \in \mathbb{N}$,

(ii) *ako je* $nzd(n,k) > 1$, *onda je* $\chi(n) = 0$, *dok je* $\chi(1) \neq 0$,

(iii) *ako je* $n \equiv m \pmod k$, *onda je* $\chi(m) = \chi(n)$.

[3]Relativno prosti brojevi su prirodni brojevi koji nemaju zajedničkog djelitelja osim 1.

Primjer 4.1. *Definirajmo funkciju* $\chi_0 : \mathbb{N} \to \mathbb{C}$ *s*

$$\chi_0(n) = \begin{cases} 1\,, & \textit{ako je } nzd(k,n) = 1, \\ 0\,, & \textit{inače.} \end{cases}$$

Lako se pokaže da tako definirana funkcija zadovoljava svojstva iz Definicije 4.7. Ovako definiranu funkciju nazivamo glavni karakter modulo k.

Primjer 4.2. *Funkcija definirana s*

$$\chi_1(n) = \begin{cases} 1 & , \textit{ ako je } n \equiv 1 \pmod 4, \\ -1 & , \textit{ ako je } n \equiv 3 \pmod 4, \\ 0 & , \textit{ inače,} \end{cases}$$

je jedan Dirichletov karakter modulo 4.

Sljedeća lema daje neka korisna svojstva Dirichletovih karaktera koja će se koristiti u daljnjim razmatranjima.

Lema 4.10. *Neka je* $\chi : \mathbb{N} \to \mathbb{C}$ *Dirichletov karakter. Tada vrijedi:*

a) Ako je $nzd(k,n) = 1$*, onda je* $(\chi(n))^{\varphi(k)} = 1$*. Drugim riječima, ako je* $\chi(n) \neq 0$*, onda je* $\chi(n)\varphi(k)$*-ti korijen iz 1 i vrijedi* $|\chi(n)| = 1$.

b) Postoji samo konačno mnogo Dirichletovih karaktera modulo k.

c) Ako su χ_1 *i* χ_2 *Dirichletovi karakteri, onda je i* $\chi_1\chi_2$ *Dirichletov karakter.*

Dokaz.

a) Stavimo da je $m = n = 1$. Tada, koristeći (i) i (ii) iz Definicije 4.7, slijedi da je $\chi(1) = 1$. Nadalje, pretpostavimo da je $nzd(n,k) = 1$. Tada, prema Eulerovom teoremu (Teorem 2.3), vrijedi $n^{\varphi(k)} \equiv 1 \pmod k$. Prema tome, koristeći (i) i (ii) iz definicije 4.7, dobivamo

$$(\chi(n))^{\varphi(k)} = \chi(n^{\varphi(k)}) = \chi(1) = 1.$$

b) Uočimo da je χ zadan vrijednostima $\chi(j)$, za $j = 1, \ldots, k$, takvim da je $nzd(k,j) = 1$ (Prema (i) i (ii) iz definicije 4.7.). Takvih j-ova ima najviše $\varphi(k)$. Prema a), $\chi(j)$ može poprimiti jednu od $\varphi(k)$ vrijednosti jer toliko ima $\varphi(k)$-tih korijena iz 1. Prema tome, postoji najviše $\varphi(k)^{\varphi(k)}$ Dirichletovih karaktera modulo k.

c) Očito je da $\chi_1\chi_2$ zadovoljava svojstva $(i) - (iii)$ iz Definicije 4.7.

□

Koristeći se Lemom 4.10, može se pokazati sljedeći bitan rezultat. Njegov se dokaz može naći u [2, Teorem 7.3].

Teorem 4.17. *Postoji točno $\varphi(k)$ Dirichletovih karaktera modulo k.*

Napomena 4.3. *Funkcije definirane u primjerima 4.1 i 4.2 su prema prethodnom teoremu jedini Dirichletovi karakteri modulo 4.*

Oznaka $\overline{\chi}$ u daljnjim će razmatranjima predstavljati inverz od χ, odnosno Dirichletov karakter za koji je $\chi \cdot \overline{\chi} = \chi_0$. Lako se pokaže da je $\overline{\chi}$ također Dirichletov karakter.
Sljedeći teorem daje bitna svojstva Dirichletovih karaktera. Dokaz teorema može se naći u [2, Teorem 7.4].

Teorem 4.18.

a) Neka su χ_1, χ_2 Dirichletovi karakteri modulo k. Tada je

$$\sum_{a=1}^{k} \chi_1(a)\overline{\chi_2}(a) = \begin{cases} \varphi(k)\,, & \text{ako je } \chi_1 = \chi_2, \\ 0 & , \text{inače.} \end{cases}$$

b) Neka su a_1, a_2 prirodni brojevi takvi da je $nzd(a_1, k) = nzd(a_2, k) = 1$. Tada vrijedi

$$\sum_{\chi \bmod k} \chi(a_1)\overline{\chi}(a_2) = \begin{cases} \varphi(k)\,, & \text{ako je } a_1 \equiv a_2 \pmod{k}, \\ 0 & , \text{inače.} \end{cases}$$

Dirichletovi karakteri modulo k te njihova svojstva bili su nam nužni za definirati sljedeću funkciju. Ona se koristi u dokazu teorema 4.16.

Definicija 4.8. *Neka je χ Dirichletov karakter modulo k. Dirichletovu L-funkciju definiramo s*

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}, \tag{4.13}$$

gdje je $s = \sigma + it \in \mathbb{C}, Re(s) > 1$.

Kako je $|\chi(n)| \leq 1$, red u (4.13) konvergira za $\sigma > 1$. Za $k = 1$ jedini Dirichletov karakter modulo 1 je glavni karakter χ_0. U tom je slučaju $L(\chi_0, s) = \zeta(s)$, iz čega vidimo da je Dirichletova L-funkcija poopćenje Riemannove zeta-funkcije.

Sada želimo pokazati još nekoliko bitnih svojstava Dirichletove $L-$ funkcije. Pokazat ćemo da se ona uz neke uvjete može analitički produljiti[4] na poluravninu $\sigma > 0$. Za to će nam biti potreban sljedeći rezultat iz matematičke analize, čiji se dokaz može naći u [2, Teorem 5.4].

[4]Analitički produljiti zapravo znači proširiti domenu funkcije na kojoj je ona definirana.

Teorem 4.19. *Neka je $f : \mathbb{N} \to \mathbb{C}$ multiplikativna funkcija takva da red*

$$\sum_{n=1}^{\infty} f(n)$$

apsolutno konvergira. Tada vrijedi

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} (1 + f(p) + f(p^2) + \dots),$$

gdje je beskonačni umnožak na desnoj strani jednakosti apsolutno konvergentan.

Sada možemo dokazati sljedeći bitan rezultat.

Teorem 4.20.

a) Ako je $\chi = \chi_0$, onda se $L(s, \chi)$ može analitički produljiti na poluravninu $\sigma > 0$, s izuzetkom u točki $s = 1$ u kojoj funkcija ima pol prvog reda s reziduumom $\varphi(k)/k$.

b) Ako je $\chi \neq \chi_0$, onda se $L(s, \chi)$ može analitički produljiti na poluravninu $\sigma > 0$.

Dokaz.

a) Za $\sigma > 1$, prema prethodnom teoremu vrijedi

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

Nadalje, vrijedi

$$L(s, \chi_0) = \prod_{p \nmid k} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \mid k} \left(1 - \frac{1}{p^s}\right) = \zeta(s) \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right).$$

Prethodna relacija daje analitičko produljenje od $L(s, \chi_0)$ na cijelu kompleksnu ravninu. Nadalje, kako je $\zeta(s)$ meromorfna funkcija s jednim polom prvom reda u $s = 1$ i reziduumom 1, slijedi da je i $L(s, \chi_0)$ meromorfna s jednim polom u $s = 1$ prvog reda, te da je reziduum jednak $\prod_{p|k} \left(1 - \frac{1}{p}\right) = \varphi(k)/k$.

b) Ako je $\chi \neq \chi_0$, onda je

$$\sum_{n=1}^{k} \chi(n) = 0.$$

Stoga za $x \geq 1$ vrijedi
$$\Big|\sum_{n\leq x}\chi(n)\Big| \leq k.$$
Nadalje, za svaki $\epsilon > 0$,
$$\Big|\sum_{y\leq n\leq x}\frac{\chi(n)}{n^s}\Big| \leq \frac{1}{|y^s|}\Big|\sum_{y\leq n\leq x}\chi(n)\Big| < \frac{k}{|y|^\sigma} < \epsilon,$$
kad god je
$$|y| > \left(\frac{k}{\epsilon}\right)^{1/\sigma}.$$
Ovo povlači da red iz definicije Dirichletove L-funkcije konvergira za svaki $\sigma > 0$

□

Kako bi dokazali teorem 4.16, potreban nam je još sljedeći teorem. On nam daje ključno svojstvo koje se koristi u dokazu. Napomenimo kako se u mnogim izvorima ovaj teorem dokazuje kao korak u dokazu Dirichletovog teorema, ali smo ga ovdje zbog njegove kompleksnosti odlučili zasebno istaknuti.

Teorem 4.21. *Ako je $\chi \neq \chi_0$, onda je $L(1,\chi) \neq 0$.*

Dokaz. Najprije pokazujemo tvrdnju u slučaju kada je χ kompleksni Dirichletov karakter modulo k. Dakle, taj karakter ne poprima samo realne vrijednosti, već može poprimiti i kompleksne. Promotrimo funkciju
$$P(s) = \prod_{\chi \bmod k} L(s,\chi),$$
gdje umnožak ide po svim Dirichletovim karakterima modulo k. Za $\sigma > 1$ vrijedi
$$\begin{aligned}
\ln P(\sigma) &= \sum_{\chi \bmod k} \ln L(\sigma,\chi)\\
&= \sum_{\chi \bmod k}\sum_{p\in\mathbb{P}}\sum_{m\geq 1}\frac{\chi(p^m)}{mp^{m\sigma}}\\
&= \sum_{p\in\mathbb{P}}\sum_{m\geq 1}\frac{1}{mp^{m\sigma}}\sum_{\chi \bmod k}\chi(p^m)\\
&= \sum_{p\in\mathbb{P}}\sum_{\substack{m\geq 1\\ p^m\equiv 1 \pmod k}}\frac{\varphi(k)}{mp^{m\sigma}} \geq 0.
\end{aligned}$$

Dakle, pokazali smo da za $\sigma > 1$ vrijedi

$$P(\sigma) \geq 1. \tag{4.14}$$

Sada, pretpostavimo suprotno, tj. pretpostavimo postoji neki kompleksni χ takav da je $L(1, \chi) = 0$. Kao što smo i prije naveli, inverz $\overline{\chi}$ od χ je također Dirichletov karakter modulo k, te kako je χ kompleksan vrijedi $\overline{\chi} \neq \chi$. Stoga $P(s)$ ma dvije nultočke u $s = 1$, ali $L(s, \chi_0)$ ima u $s = 1$ pol prvog reda, pa se samo jedna od nultočaka "pokrati". Iz toga dobivamo da je $P(1) = 0$, što je u kontradikciji s (4.14).
Pretpostavimo sada da je $\chi \neq \chi_0$ realni karakter. Promotrimo funkcije $f(n) = \sum_{d|n} \chi(d)$ i $F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$. Lako se pokaže da je f multiplikativna. Nadalje, vrijedi

$$\sum_{l=0}^{m} \chi(p^l) = \begin{cases} 1 & \text{, ako } p|k, \\ \geq 1 & \text{, ako } p \nmid k \text{ i } m \text{ je paran,} \\ \geq 0 & \text{, ako } p \nmid k \text{ i } m \text{ je neparan.} \end{cases}$$

Stoga je $f(n) \geq 0$, za svaki n, te $f(n) \geq 1$, ako je n potpun kvadrat. Iz toga dobivamo da vrijedi

$$F(\sigma) = \sum_{n\geq 1} \frac{f(n)}{n^\sigma} \geq \sum_{n\geq 1} \frac{1}{n^{2\sigma}} = \zeta(2\sigma).$$

Iz prethodne nejednakosti možemo zaključiti da $F(\sigma)$ divergira u $\sigma = \frac{1}{2}$, pa $F(s)$ mora imati singularitet u $s = \sigma_c \geq \frac{1}{2}$, gdje je $\sigma_c \in \mathbb{R}$ takav da $F(s)$ konvergira za $Re(s) > \sigma_c$ i divergira za $Re(s) > \sigma_c$.
S druge strane, za $\sigma > 1$ vrijedi da je

$$F(s) = L(s, \chi)\zeta(s),$$

jer je

$$\Big(\sum_{n\geq 1} \frac{\chi(n)}{n^s}\Big)\Big(\sum_{n\geq 1} \frac{1}{n^s}\Big) = \sum_{n\geq 1} \frac{1}{n^s} \sum_{d|n} \chi(d) = \sum_{n\geq 1} \frac{f(n)}{n^s}.$$

Kada bi vrijedilo $L(1, \chi) = 0$, onda bi F bila analitička za $\sigma > 0$. To bi dalje značilo da je $\sigma = \sigma_c$, čime bi dobili kontradikciju. Dakle, vrijedi $L(1, \chi) \neq 0$. $\square$

4.5.1 Dokaz Dirichletovog teorema

Dokaz Dirichletovog teorema o prostim brojevima u aritmetičkom nizu provest ćemo kroz 3 koraka.

Korak 1

Tvrdimo da je za dokazati teorem dovoljno pokazati da ako je $x \geq 3$ i $\sigma = 1 + \frac{1}{\ln x}$, onda vrijedi

$$\sum_{p \equiv l \pmod{k}} \frac{1}{p^\sigma} = \frac{1}{\varphi(k)} \ln\Big(\frac{1}{\sigma - 1}\Big) + O(1).$$

Uvedimo oznake

$$\Sigma_1 = \sum_{p \equiv l \pmod{k}} \frac{1}{p^\sigma} \text{ i } \Sigma_2 = \sum_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \frac{1}{p}.$$

Tada je

$$|\Sigma_1 - \Sigma_2| \leq \sum_{p \leq x} \Big(\frac{1}{p} - \frac{1}{p^\sigma}\Big) + \sum_{p > x} \frac{1}{p^\sigma}.$$

Nadalje, vrijedi

$$\sum_{p \leq x} \Big(\frac{1}{p} - \frac{1}{p^\sigma}\Big) = \sum_{p \leq x} \frac{1 - e^{-(\sigma-1)\ln p}}{p} \leq \sum_{p \leq x} \frac{(\sigma - 1)\ln p}{p} = \frac{1}{\ln x} \sum_{p \leq x} \frac{\ln p}{p} = O(1),$$

pri čemu zadnja jednakost slijedi iz formule

$$\sum_{p \leq x} \frac{\ln p}{p} = \ln x + O(1),$$

čiji se dokaz može naći u [3, poglavlje 7.2].
Nadalje, koristeći Abelovu formulu parcijalne sumacije (teorem 4.5) i teorem 4.7 slijedi,

$$\begin{aligned}
\sum_{p > x} \frac{1}{p^\sigma} &= \lim_{y \to \infty} \sum_{x \leq p \leq y} \frac{1}{p^\sigma} \\
&= \lim_{y \to \infty} \Big(\frac{1}{y^\sigma} \sum_{p \leq y} 1 - \frac{1}{x^\sigma} \sum_{p \leq x} 1 - \int_x^y \Big(\sum_{p \leq t} 1\Big)\Big(-\frac{\sigma}{t^\sigma + 1}\Big) dt\Big) \\
&= O(1) + \int_x^\infty O\Big(\frac{t}{\ln t}\Big) \frac{dt}{t^{\sigma+1}} \\
&= O(1) + O\Big(\int_x^\infty \frac{dt}{t^\sigma \ln t}\Big) \\
&= O(1) + O\Big(\frac{1}{\ln x} \int_x^\infty \frac{dt}{t^\sigma}\Big) = O(1).
\end{aligned}$$

Dakle, pokazali smo da je

$$|\Sigma_1 - \Sigma_2| \leq O(1),$$

to jest da je taj izraz ograničen neovisno o x, čime smo pokazali tvrdnju iz koraka 1.

Korak 2

Uočimo da za $\sigma > 1$ prema teoremu 4.18. d) vrijedi

$$\sum_{\substack{p \\ p\equiv l (\text{mod } k)}} \frac{1}{p^\sigma} = \sum_{p\in\mathbb{P}} \frac{1}{p^\sigma}\Big(\frac{1}{\varphi(k)} \sum_{\chi (\text{mod } k)} \overline{\chi(l)}\chi(p)\Big) = \frac{1}{\varphi(k)} \sum_{\chi (\text{mod } k)} \overline{\chi(l)} S(\sigma,\chi),$$

gdje je

$$S(\sigma,\chi) = \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^\sigma}.$$

Sada je

$$\sum_{p\in\mathbb{P}}\sum_{m\geq 1} \frac{1}{mp^{m\sigma}} - \sum_{p\in\mathbb{P}} \frac{1}{p^\sigma} = -\ln{(1-\frac{1}{p^\sigma})} - \sum_{p\in\mathbb{P}} \frac{1}{p^\sigma} = O(1),$$

jer je

$$\sum_{p\in\mathbb{P}}\sum_{m\geq 2} \frac{1}{mp^{m\sigma}} \leq \frac{1}{2}\sum_{p\in\mathbb{P}}\sum_{m\geq 2} \frac{1}{p^{m\sigma}} = \frac{1}{2}\sum_{p} \frac{1}{p^\sigma(p^\sigma - 1)} = O(1).$$

Stoga je

$$\begin{aligned}
S(\sigma,\chi_0) &= \sum_{p}\sum_{m\geq 1} \frac{1}{mp^{m\sigma}} - \sum_{p|k}\sum_{m\geq 1} \frac{1}{mp^{m\sigma}} \\
&= -\sum_{p} \ln\Big(1-\frac{1}{p^\sigma}\Big) + O(1) \\
&= \ln\prod_{p\in\mathbb{P}}\Big(1-\frac{1}{p^\sigma}\Big)^{-1} + O(1) \\
&= \ln\zeta(\sigma) + O(1) \\
&= \ln\Big(\frac{1}{\sigma - 1}\Big) + O(1).
\end{aligned}$$

Zadnja jednakost slijedi iz Eulerove produktne formule i činjenice da za σ u okolini 1 imamo

$$\zeta(\sigma) = \frac{1}{\sigma - 1} + g(\sigma),$$

gdje je $g(\sigma)$ funkcija koja je analitička u 1.
Učimo da smo ovime za χ_0 dobili glavni član u ocjeni, što znači da preostaje pokazati da je

$$S(\sigma, \chi) = O(1),$$

za $\sigma > 1$ i sve Dirichletove karaktere različite od glavnog.

Korak 3

Koristeći se sličim postupkom kao u prethodnom koraku, imamo

$$\begin{aligned} S(\sigma, \chi) &= \sum_p \frac{\chi(p)}{p^\sigma} = \sum_p \sum_{m \geq 1} \frac{\chi(p)^m}{mp^{m\sigma}} + O(1) \\ &= -\sum_p \left(\ln 1 - \frac{\chi(p)}{p^\sigma} \right)^{-1} + O(1) \\ &= \ln L(\sigma, \chi) + O(1). \end{aligned}$$

Za $\chi \neq \chi_0$ funkcija $L(s, \chi)$ je analitička u $\sigma > 0$. Stoga je $L(\sigma, \chi)$ neprekidna u $\sigma > 1$ i vrijedi

$$\lim_{\sigma \to 1} L(\sigma, \chi) = L(1, \chi).$$

Kako je prema teoremu 4.21.

$$L(1, \chi) \neq 0,$$

slijedi da je

$$S(\sigma, \chi) = O(1),$$

što je i trebalo pokazati. Time je pokazana tvrdnja teorema 4.16.

5 Neke nedokazane tvrdnje vezane uz proste brojeve

U teoriji brojeva postoji još mnogo nedokazanih hipoteza te otvorenih pitanja. Već smo prije spomenuli čuvenu Riemannovu hipotezu, a u ovom poglavlju navodimo još neke.

Zasigurno jedna od najpoznatijih i najstarijih, još uvijek nedokazanih tvrdnji, je takozvana jaka Goldbachova slutnja:

Svaki se paran prirodni broj veći od 2 može zapisati kao zbroj dva prosta broja.

Tvrdnju je vrlo jednostavno provjeriti za prvih nekoliko parnih brojeva:

$$\begin{gathered} 4 = 2 + 2, \\ 6 = 3 + 3, \\ 8 = 3 + 5, \\ \vdots \end{gathered}$$

Goldbachova originalna slutnja napisana 1742. u pismu Euleru je glasila:

Svaki se prirodan broj veći od 2 može zapisati kao suma tri prosta broja.

Pri ovoj je tvrdnji Goldbach smatrao da je 1 prost broj (konvencija koja je danas napuštena), zbog čega je kasnije Euler dao ekvivalentnu tvrdnju koja danas nosi naziv Goldbachova slutnja.

Kako raste broj n, raste i broj njegovih mogućih zapisa u obliku zbroja dvaju prostih brojeva. Na primjer, za broj 4 postoji jedinstven prikaz kao 2+2, dok za broj 100 000 000 postoji 219 400 takvih prikaza. Upravo zbog toga mnogi matematičari vjeruju u istinitost ove tvrdnje, barem za dovoljno velike prirodne brojeve, uglavnom pozivajući se na vjerojatnosnu distribuciju prostih brojeva. Što je veći broj, postoji više načina za prikazati taj broj kao zbroj dva broja, što znači da je šansa veća da ti brojevi u zbroju budu prosti. Posljednji broj n takav da Goldbachova slutnja vrijedi za brojeve manje od n, pronašao je 2012. godine brazilski matematičar Oliveira e Silva i on iznosi $4 \cdot 10^{18}$.

Poznata je i takozvana "slaba" Goldbachova slutnja koja glasi:

Svaki neparan prirodan broj ≥ 7 se može zapisati kao zbroj tri neparna prosta broja.

Ova se tvrdnja naziva slabom jer kada bi se dokazala jaka Goldbachova slutnja, ova bi tvrdnja bila automatski dokazana.

Prvi značajniji pokušaj dokaza slabe Goldbachove slutnje dao je ruski matematičar I. Vinogradov 1937. godine. On je tvrdnju pokazao za dovoljno velike neparne prirodne brojeve, to jest za sve neparne brojeve veće od nekog n_0, ali nije nikada uspio dobiti točnu vrijednost tog broja. Njegov je student K. Borozdkin 1956. godine pokazao da je $n_0 < 3^{3^{15}}$. Kasnije je ta granica smanjena na otprilike 10^{1346}, što je i dalje prevelika ograda kako bi se mogle izvršiti provjere uporabom računala.

Druga tvrdnja koju ćemo u ovom poglavlju spomenuti vezana je uz parove prostih brojeva blizanaca. Za početak ih definirajmo:

Definicija 5.1. *Par prostih brojeva blizanaca je par prostih brojeva oblika p i $p+2$.*

Na primjer, brojevi 3 i 5 te 11 i 13 su prosti brojevi blizanci. Do sada je poznato preko sto tisuća parova prostih brojeva blizanaca. Posljednji najveći par prostih brojeva blizanaca otkriven 2016. godine je $2996863034895 \cdot 2^{1290000} \pm 1$. Svaki od prostih brojeva u tom paru ima 388 342 znamenki. No ipak, nikada nije dokazana poznata slutnja vezana za parove prostih brojeva blizance koja glasi:

Parova prostih brojeva blizanaca ima beskonačno mnogo.

Najbliži dokazivanju ove slutnje bio je američki matematičar R. F. Arenstorf 2004. godine. Njegov je dokaz kasnije odbijen zbog pogreške, čime je ova slutnja i dalje ostala samo nagađanje.

6 Zaključak

Cilj ovog rada bio je definirati i opisati funkcije koje su povezane s distribucijom prostih brojeva. Za početak smo prikazali kako se prosti brojevi mogu vizualizirati u obliku Ulamove spirale te u obliku kvadrata. Nakon što smo uveli osnovne pojmove iz teorije brojeva i kompleksne analize, koji su potrebni za razumjevanje rada, ukratko smo opisali proste brojeve kroz povijest. U glavnom dijelu rada definirali smo i opisali Čebiševljeve funkcije, Riemannovu zeta-funkciju te Dirichletovu L-funkciju. Povezali smo ih s distribucijom prostih brojeva preko Teorema o prostim brojevima, za kojeg smo dali skicu dokaza, te s Dirichletovim teoremom o prostim brojevima u aritmeičkom nizu. Za kraj smo naveli i opisali neke nedokazane tvrdnje vezane uz proste brojeve. Važno je napomenuti da nisu sve tvrdnje navedene u radu ovdje i dokazane, ali je dana literatura u kojoj se mogu naći potrebni dokazi.

Popis slika

Popis tablica

Literatura

[1] Baillie, R., How the Zeros of the Zeta Function Predict the Distribution of Primes, Wolfram Demonstrations Project, 2011, online: http://demonstrations.wolfram.com/HowTheZerosOfTheZetaFunction PredictTheDistributionOfPrimes/

[2] Chan, H. H., Analytic number theory for undergraduates, Monographs in number theory volume 3, National University of Singapore, Singapore, 2009.

[3] Dujella, A., Teorija brojeva, Školska knjiga, Zagreb, 2019.

[4] Edwards, H. M., Riemann's zeta function, Academic press, New York, 1974.

[5] Franušić, Z. i Pavlinić N., O distribuciji prostih brojeva, Acta mathematica spalatensia, Series didactica, Vol.1, pp. 41-50, 2018.

[6] Golden, J., Distribution of Primes, GeoGebra, online: https://www.geogebra.org/m/nhg2JjzV?fbclid=IwAR2wJKhEX bUosh8orRLlYzT5Ny-DC5erab81DMq3F4L_G8259zomvS3ZK48

[7] Goldfeld, D., The elementary proof of the prime number theorem: An historical perspective, online: https://www.math.columbia.edu/ goldfeld/ErdosSelbergDispute.pdf

[8] Goldstein, L. J., A History of the Prime Number Theorem, The American Mathematical Monthly, Vol. 80, No. 6, pp. 599-615, 1973.

[9] Gurdon, A., Prosti brojevi i testovi prostosti, Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku, 2020.

[10] Kennard, L., Two classic theorems from number theory: The Prime Number Theorem and Dirichlet's Theorem Senior Exercise in Mathematics, 2006.

[11] Kraljević, H., Odabrana poglavlja teorije analitičkih funkcija, Matematički odjel Sveučilišta u Zagrebu, Zagreb, 2010.

[12] Kuhl, K. H., Prime numbers-things long known and things new found, Parkstein, 2020.

[13] Kuzek, A., O nekim otvorenim problemima iz teorije brojeva, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, 2017.

[14] Limbachia, V., On Erdos & Selberg's proof of Prime Number Theorem, 2020., online: https://scholar.princeton.edu/sites/default/files/ashvin/files/math229xfinalproject.pdf

[15] O'Connor J. J. and Robertson E. F., Prime numbers, MacTutor, 2018, online: https://mathshistory.st-andrews.ac.uk/HistTopics/Prime_numbers/

[16] Riffer-Reinert, B.,The zeta function and its relation to the prime number theorem, online: http://www.math.uchicago.edu/ may/VIGRE/VIGRE2011/REUPapers/Riffer-Reinert.pdf

[17] Selberg, A., An Elementary Proof of the Prime-Number Theorem, Annals of Mathematics, Second Series, Vol. 50, No. 2, pp. 305-313, 1949.

[18] Stein, E. M., Complex analysis, Princeton lectures in anaylsis, Princeton University press, New Jersey, 2003.

[19] The largest known prime by year: A brief history, Prime pages, 2021, online: https://primes.utm.edu/notes/by_year.html

[20] Weisstein, E. W., "Goldbach Conjecture", From MathWorld–A Wolfram Web Resource, online: https://mathworld.wolfram.com/GoldbachConjecture.html

[21] Weisstein, E. W., "Riemann Prime Counting Function." From MathWorld–A Wolfram Web Resource, online: https://mathworld.wolfram.com/RiemannPrimeCountingFunction.html