Primjena L-funkcija u teoriji brojeva

Patljak, Marija

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:907159

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marija Patljak

PRIMJENA L-FUNKCIJA U TEORIJI BROJEVA

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, veljača 2016.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Mojim roditeljima i braći.

Sadržaj

Uvod

Aritmetički niz neparnih brojeva $1, 3, 5, ..., 2n+1, ...$ sadrži beskonačno mnogo prostih brojeva. Prirodno je pitati se imaju li i drugi aritmetički nizovi takvo svojstvo. Aritmetički niz s prvim članom h i diferencijom k je niz brojeva oblika

$$kn + h, n = 0, 1, 2, ...$$

Ako je $d > 1$ zajednički djelitelj od h i k, tada je svaki član niza djeljiv s d i niz ne može sadržavati više od jednog prostog člana u nizu. Drugim riječima, nužan uvjet da bi tako definiran aritmetički niz sadržavao beskonačno mnogo prostih članova je da $(h, k) = 1$. Dirichlet je bio prvi koji je dokazao kako je taj uvjet ujedno i dovoljan. Dakle, ako $(h, k) = 1$, tada aritmetički niz sadrži beskonačno mnogo prostih brojeva. Ovaj rezultat, poznat kao *Dirichletov teorem* ćemo dokazati u ovom radu.

U prvom poglavlju su dane osnovne definicije i svojstva funkcija koje koristimo u radu. U drugom poglavlju se upoznajemo s karakterima i $L(1, \chi)$ funkcijom. Sam dokaz Dirichletovog teorema je iznesen u trećem poglavlju.

Poglavlje 1

Uvodno poglavlje

1.1 Osnovni pojmovi

Za početak, definirajmo osnovne pojmove.

Definicija 1.1.1. *Neka su a i b cijeli brojevi. Cijeli broj d zovemo zajednički djelitelj od a i b ako $d|a$ i $d|b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od a i b. Najveći medu njima zove se najveći zajednički djelitelj od a i b i označava se s (a, b). Ako je $(a, b) = 1$, tada za a i b kažemo da su relativno prosti.*

Definicija 1.1.2. *Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako vrijedi*

1. $f(1) = 1$,
2. $f(mn) = f(m)f(n)$, *za sve m i n takve da $(m, n) = 1$.*

Aritmetičke funkcije

Potrebno je definirati i neke funkcije te njihova svojstva.

Definicija 1.1.3. *Eulerova funkcija $\varphi(n)$ je broj pozitivnih cijelih brojeva $\leq n$ koji su relativno prosti s n.*

Definicija 1.1.4. *Möbiusova funkcija $\mu(n)$, za $n \in \mathbb{N}$ definirana je sa*

$$\mu(n) = \begin{cases} (-1)^k, & n = p_1 p_2 \cdots p_k, \\ 0, & \text{inače}. \end{cases}$$

Specijalno, $\mu(1) = 1$.

Definicija 1.1.5. *Za dvije aritmetičke funkcije f i g definiramo njihov Dirichletov produkt (ili Dirichletovu konvoluciju) kao aritmetičku funkciju h definiranu s*

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Pišemo $f * g$ za h i $(f * g)(n)$ za $h(n)$.

Sljedeći teorem poznat nam je kao *Möbiusova formula inverzije*.

Teorem 1.1.6. *Relacija*

$$f(n) = \sum_{d|n} g(d),$$

implicira

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Također, vrijedi i obrat.

Iz ovog teorema slijedi relacija koja povezuje Eulerovu i Möbiusovu funkciju:

$$n = \sum_{d|n} \varphi(d), \quad \varphi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right).$$

Definicija 1.1.7. *Von Mangoldtova funkcija $\Lambda(n)$, za $n \in \mathbb{N}$ definirana je s*

$$\Lambda(n) = \begin{cases} \log p, & n = p^m, \\ 0, & \textit{inače}, \end{cases}$$

gdje su p prost broj i $m \geq 1$.

Neka je F realna ili kompleksna funkcija definirana na $< 0, +\infty >$ takva da je $F(x) = 0$ za $0 < x < 1$. Promatrat ćemo funkcije oblika

$$\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right),$$

gdje je α neka aritmetička funkcija. Ova suma definira novu funkciju G na $< 0, +\infty >$ koja je isto jednaka nuli za $0 < x < 1$. Funkciju G pišemo $\alpha \circ F$. Prema tome,

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Ako je $F(x) = 0$ za sve $x \notin N$, tada je restikcija od F na prirodne brojeve m aritmetička funkcija i vrijedi

$$(\alpha \circ F)(m) = (\alpha * F)(m),$$

te operaciju $\circ$ smatramo generalizacijom Dirichletovog produkta $*$.

Sljedeći teorem poznat je kao generalizirana formula inverza.

Teorem 1.1.8. *Ako α ima Dirichletov inverz α^{-1}, tada vrijedi sljedeće*

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \quad \Leftrightarrow \quad F(x) = \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right).$$

Specijalno, za α potpuno multiplikativnu funkciju i $\alpha^{-1}(n) = \mu(n)\alpha(n)$ dobivamo *generaliziranu Möbiusovu formulu inverzije*.

Dokaz. Neka je $G = \alpha \circ F$. Tada slijedi

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F,$$

gdje je I identiteta. Analogno se pokaže obrat tvrdnje. □

Kongruencije i sustav ostataka

Definicija 1.1.9. *Neka su a,b i m cijeli brojevi, $m > 0$. Kažemo da je a kongruentno b modulo m i pišemo $a \equiv b \pmod{m}$, ako m dijeli razliku $a - b$.*

Simbol za kongruencije $\equiv$ je izabrao Gauss kako bi sugestirao sličnost sa znakom jednakosti $=$. Osim sličnosti znakova, te dvije relacije imaju i mnoga zajednička svojstva. Jedno od njih dano je u sljedećem teoremu.

Teorem 1.1.10. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$. Dakle, vrijedi sljedeće:*

1. $a \equiv a \pmod{m}$ *(refleksivnost)*
2. $a \equiv b \pmod{m} \quad \Rightarrow \quad b \equiv a \pmod{m}$ *(simetričnost)*
3. $a \equiv b \pmod{m} \quad i \quad b \equiv c \pmod{m} \quad \Leftrightarrow \quad a \equiv c \pmod{m}$ *(tranzitivnost)*

Dokaz. Dokaz slijedi direktno iz svojstava djeljivosti:
1. $m \mid 0$.
2. Ako $m \mid (a - b)$, tada $m \mid (b - a)$.
3. Ako $m \mid (a - b)$ i $m \mid (b - c)$, tada $m \mid (a - b) + m \mid (b - c) = a - c$. □

Definicija 1.1.11. *Neka je m prirodan broj. Skup â predstavlja skup svih cijelih brojeva x takvih da je* $x \equiv a \pmod{m}$ *i skup â nazivamo ostatkom od a. Drugim riječima, vrijedi:*

$$[\hat{a}] = \{x + km | k \in \mathbb{Z}\} = x + m\mathbb{Z}.$$

Definicija 1.1.12. *Skup* $\{x_1, x_2, ..., x_m\}$ *se zove potpuni sustav ostataka modulo m, ako za svaki* $y \in \mathbb{Z}$ *postoji točno jedan* x_i *takav da je* $y \equiv x_i \pmod{m}$.

Definicija 1.1.13. *Reducirani sustav ostataka modulo m je skup cijelih brojeva* r_i *takvih da* $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ *za* $r_i \neq r_j$ *te da za svaki cijeli broj x takav da* $(x, m) = 1$ *postoji* r_i *takav da* $x \equiv r_i \pmod{m}$.

Teorem 1.1.14. Euler-Fermatov teorem. *Neka je* $(a, m) = 1$. *Tada vrijedi*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Kriteriji konvergencije reda

Navest ćemo neke od kriterija za konvergenciju reda i to samo one koje ćemo koristiti u dokazima u ovom radu.

Teorem 1.1.15. Cauchyjev kriterij. *Neka je* (a_n) *niz kompleksnih brojeva.*

1. *Ako postoje* $m \in \mathbb{N}$ *i* $q \in < 0, 1 >$ *takvi da je*

$$\sqrt[n]{|a_n|} \leq q, \quad \forall n \geq m,$$

   tada red $\sum a_n$ *apsolutno konvergira.*

2. *Ako postoji* $m \in \mathbb{N}$ *takav da je*

$$\sqrt[n]{|a_n|} \geq 1, \quad \forall n \geq m,$$

   tada red $\sum a_n$ *apsolutno divergira.*

Teorem 1.1.16. Integralni kriterij konvergencije reda (Cauchy). *Neka je* $f : [a, \infty > \rightarrow [0, \infty >$ *neprekidna i padajuća funkcija, gdje je* $a > 0$. *Tada*

$$\textit{red} \sum f(n) \quad \textit{konvergira} \quad \Leftrightarrow \quad \textit{nepravi integral} \int_a^\infty f(x)dx \quad \textit{konvergira}.$$

Teorem 1.1.17. Usporedni kriterij. *Neka su* $\sum a_n$ *i* $\sum b_n$ *redovi s pozitivnim članovima i neka postoje* $m \in \mathbb{N}$ *i* $K > 0$ *takvi da je*

$$a_n \leq K \cdot b_n, \quad \forall n \geq m.$$

1. *Ako* $\sum b_n$ *konvergira, onda konvergira i* $\sum a_n$ *i vrijedi*

$$\sum_{n=1}^{\infty} a_n \leq \sum_{n=1}^{\infty} b_n.$$

2. *Ako* $\sum a_n$ *divergira, onda divergira i* $\sum b_n$.

1.2 Osnovni primjeri

Nekoliko matematičara se istaknulo u dokazivanju beskonačnosti skupa prostih brojeva. Osnovni teorem koji to dokazuje je *Euklidov teorem.*

Teorem 1.2.1. Euklidov teorem. *Skup svih prostih brojeva je beskonačan.*

Dokaz. Pretpostavimo da su $p_1, p_2, ...p_n$ svi prosti brojevi. Promatramo

$$N = 1 + p_1 p_2 \cdots p_n.$$

Uočimo da N nije djeljiv ni sa jednim od prostih brojeva p_i. Dakle, svaki prosti faktor p od N je različit od $p_1, p_2, ..., p_n$. Budući da je N ili prost ili ima prosti faktor, dobili smo prost broj različit od $p_1, p_2, ..., p_n$, što je kontradikcija. □

Divergenciju reda $\sum p^{-1}$ recipročnih prostih brojeva je prvi dokazao Euler 1737. godine.

Teorem 1.2.2. *Red prostih brojeva* $\sum_{n=1}^{\infty} \frac{1}{p_n}$ *divergira.*

Dokaz. Pretpostavimo suprotno, odnosno da ovaj red konvergira. Ako red konvergira, tada postoji $k \in \mathbb{Z}$ takav da

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}.$$

Neka je $Q = p_1 \cdots p_k$, te promatrajmo brojeve oblika $1 + nQ$ za $n = 1, 2, ...$ Nijedan od njih nije djeljiv prostim brojevima $p_1, ..., p_k$. Dakle, svi prosti faktori od $1 + nQ$ se nalaze među prostim brojevima oblika $p_{k+1}, p_{k+2}, ...$ Stoga, za svaki $r \geq 1$ vrijedi

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t,$$

pošto suma zdesna među svojim članovima sadrži sve članove sume slijeva. Ali desna strana je dominirana konvergentnim geometrijskim redom

$$\sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t.$$

Dakle, red $\sum_{n=1}^{\infty} \frac{1}{1+nQ}$ ima ograničene parcijalne sume i stoga konvergira. No to je kontradikcija jer po integralnom testu konvergencije i testu usporedbe znamo da takav red divergira. □

Dirichlet je 1837. godine iznio plan kako analitičkom metodom restringirati Eulerov dokaz na proste brojeve u aritmetičkom nizu. Njegov dokaz je kasnije pojednostavilo nekoliko matematičara. Jedan od njih je bio Harold N. Shapiro koji je 1950. godine objavio pojednostavljeni dokaz da red oblika $\sum p^{-1} \log p$ divergira, umjesto za red $\sum p^{-1}$ kako je Dirichlet zamislio. Pokažimo sada kako je za specijalne oblike nizova lako dokazati Dirichletov teorem ako modificiramo Euklidov dokaz o beskonačnosti prostih brojeva.

Teorem 1.2.3. *Postoji beskonačno mnogo prostih brojeva oblika* $4n - 1$.

Dokaz. Dokaz po kontrapoziciji. Pretpostavimo da postoji konačno mnogo prostih brojeva tog oblika te neka je p najveći takav. Promotrimo broj

$$N = 2^2 \cdot 3 \cdot 5 \cdots p - 1.$$

Faktori produkta $3 \cdot 5 \cdots p$ su svi neparni brojevi $\leq p$. Očito je N oblika $4n - 1$, no N ne može biti prost jer $N > p$. Nijedan prosti broj $\leq p$ ne dijeli N pa svi prosti faktori od N moraju biti veći od p. Ali svi prosti faktori od N ne mogu biti oblika $4n + 1$ jer je produkt dva takva broja opet istog oblika. Stoga neki od prostih faktora broja N mora biti oblika $4n - 1$. Time smo dobili kontradikciju. □

Teorem 1.2.4. *Postoji beskonačno mnogo prostih brojeva oblika* $4n + 1$.

Dokaz. Neka je N prirodan te > 1. Pokazat ćemo da postoji prost broj $p > N$ takav da je $p \equiv 1 \pmod 4$. Neka je

$$m = (N!)^2 + 1.$$

Uočimo da je m neparan broj, za sve $m > 1$. Neka je p najmanji prosti faktor od m. Nijedan od brojeva $2, 3, ..., N$ ne dijeli m, stoga je $p > N$. Također, vrijedi i

$$(N!)^2 \equiv (-1)^{\frac{p-1}{2}} \pmod p.$$

No po Euler-Fermatovom teoremu je $(N!)^{p-1} \equiv 1 \pmod p$ pa

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Razlika brojeva $(-1)^{\frac{p-1}{2}}$ i 1 je ili 0 ili -2, no -2 ne može biti promatrana razlika jer je -2 dijeljivo s p pa ta razlika mora biti 0. Dakle,

$$(-1)^{\frac{p-1}{2}} = 1.$$

Ali to sada znači da je $\frac{p-1}{2}$ paran broj, pa je $p \equiv 1 \pmod 4$. Drugim riječima, pokazali smo da za svaki prirodan $N > 1$ postoji prost broj $p > N$ takav da je $p \equiv 1 \pmod 4$. Dakle, postoji beskonačno mnogo prostih brojeva oblika $4n + 1$. □

Jednostavni argumenti dani za proste brojeve oblika $4n - 1$ i $4n + 1$ mogu se poopćiti na druge specijalne oblike aritmetičkih nizova kao što su $5n - 1$, $8n - 1$, $8n - 3$ i $8n + 3$. No još uvijek nismo pokazali za generalni oblik aritmetičkog niza $kn + h$.

1.3 Prosječne vrijednosti aritmetičkih funkcija

Često nam je interes ispitati asimptotsko ponašanje aritmetičkih funkcija, tj. ocijeniti sume oblika $\sum_{n \le x} f(n)$, gdje je x dovoljno velik realan broj.

Definicija 1.3.1. *Ako je $g(x) > 0$, $\forall x \ge n$, pišemo*

$$f(x) = O(g(x))$$

te je pritom kvocijent $f(x)/g(x)$ ograničen za sve $x \ge n$. Odnosno, postoji konstanta $M > 0$ takva da je

$$|f(x)| \le Mg(x), \quad \forall x \ge n.$$

Relacija

$$f(x) = h(x) + O(g(x))$$

znači da je $f(x) - h(x) = O(g(x))$.

Definicija 1.3.2. *Ako vrijedi*

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1,$$

kažemo da je $f(x)$ asimptotski jednaka $g(x)$ kada te pišemo

$$f(x) \sim g(x), \quad kada \quad x \to \infty.$$

Ponekad se asimptotska vrijednost parcijalne sume dobiva usporedbom s integralom. Formula za sumu koju je izveo Euler nam daje točan izraz za grešku nastalu takvom aproksimacijom. U formuli će $[t]$ označavati najveći cijeli broj $\le t$.

Teorem 1.3.3. Eulerova sumacijska formula. *Ako je f monotona na segmentu $[y, x]$, za $0 < y < x$, tada vrijedi*

$$\begin{aligned} \sum_{y < n \le x} f(n) = \int_y^x f(t)\, dt + \int_y^x (t - [t]) f'(t)\, dt \\ + f(x)([x] - x) - f(y)([y] - y). \end{aligned} \tag{1.1}$$

Dokaz. Za cijele brojeve n i $n-1$ iz segmenta $[y, x]$ imamo

$$\begin{aligned}\int_{n-1}^{n} [t]f'(t)\,dt &= \int_{n-1}^{n} (n-1)f'(t)\,dt = (n-1)\left(f(n)-f(n-1)\right)\\ &= (nf(n)-(n-1)f(n-1))-f(n).\end{aligned}$$

Sumirajući sve integrale od $n = [y]+2$ do $n = [x]$ uočavamo da se sljedeći integral dobiva teleskopiranjem, stoga

$$\begin{aligned}\int_{[y]+1}^{[x]} [t]f'(t)\,dt &= [x]f([x]) - ([y]+1)f([y]+1) - \sum_{n=[y]+2}^{[x]} f(n)\\ &= [x]f([x]) - [y]f([y]+1) - \sum_{y<n\le x} f(n).\end{aligned}$$

Sada imamo

$$\begin{aligned}\sum_{y<n\le x} f(n) &= -\int_{[y]+1}^{[x]} [t]f'(t)\,dt + [x]f([x]) - [y]f([y]+1)\\ &= -\int_{y}^{x} [t]f'(t)\,dt + [x]f(x) - [y]f(y).\end{aligned} \tag{1.2}$$

Parcijalnom integracijom dobivamo formulu

$$\int_y^x f(t)\,dt = xf(x) - yf(y) - \int_y^x tf'(t)dt,$$

te kada ju uvrstimo u (1.2) dobivamo (1.1). □

Važna posljedica Eulerove sumacijske formule je sljedeća relacija:

$$\sum_{n\le x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right). \tag{1.3}$$

Dokažimo ju:

Dokaz. Uvrstimo u Eulerovu sumacijsku formulu $f(t) = 1/t$ kako bismo dobili sljedeće:

$$\begin{aligned}\sum_{n\le x} \frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{t-[t]}{t^2}dt + \frac{[x]-x}{x} - 1([1]-1)\\ &= \log x - \int_1^x \frac{t-[t]}{t^2}dt + 1 - \frac{x-[x]}{x}\\ &= \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}dt + \int_x^\infty \frac{t-[t]}{t^2}dt + O\left(\frac{1}{x}\right)\end{aligned}$$

Nepravi integral $\int_1^\infty (t-[t])t^{-2}\,dt$ postoji budući da je dominiran s nepravim integralom $\int_1^\infty t^{-2}\,dt$. Dakle,

$$0 \le \int_x^\infty \frac{t-[t]}{t^2}dt \le \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x}$$

pa sada slijedi

$$\sum_{n\le x}\frac{1}{n} = \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}dt + O\left(\frac{1}{x}\right).$$

Stavimo li da je

$$C = 1 - \int_1^\infty \frac{t-[t]}{t^2}dt,$$

dokazali smo relaciju (1.3). □

Sada ćemo bez dokaza navesti još neke rezultate koji su nastali kao posljedica Eulerove sumacijske formule.

Teorem 1.3.4. *Za $x \ge 2$ vrijedi*

$$\log[x]! = x\log x - x + O(\log x), \tag{1.4}$$

te stoga vrijedi i

$$\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right] = x\log x - x + O(\log x). \tag{1.5}$$

Kao posljedica tvrdnje (1.5) proizlazi sljedeći teorem:

Teorem 1.3.5. *Za $x \ge 2$ i sve proste brojeve $p \le x$ vrijedi*

$$\sum_{p\le x}\left[\frac{x}{p}\right]\log p = x\log x + O(x). \tag{1.6}$$

U Teoremu 1.3.4 smo izveli formulu $\sum_{n\le x}\Lambda(n)\left[\frac{x}{n}\right] = x\log x - x + O(\log x)$. Ta suma je težinski prosjek Mangoldtove funkcije $\Lambda(n)$ gdje je $\Lambda(n)$ pomnožena s težinskim faktorom $[x/n]$. Teoremi koji su vezani uz različite težinske prosjeke iste funkcije nazivamo *Tauberianovim teoremima*. Dokazat ćemo Tauberianov teorem kojega je 1950. godine dokazao H. N. Shapiro. Ovaj teorem povezuje sume oblika $\sum_{n\le x}a(n)$ sa onima oblika $\sum_{n\le x}a(n)[x/n]$, za nenegativne funkcije $a(n)$.

Teorem 1.3.6. Shapirov teorem. *Neka je a(n) nenegativni niz takav da je*

$$\sum_{n\le x}a(n)\left[\frac{x}{n}\right] = x\log x + O(x), \quad \forall x \ge 1. \tag{1.7}$$

1. *Za* $x \geq 1$ *vrijedi*
$$\sum_{n \leq x} \frac{a(n)}{n} = \log x + O(1).$$

2. *Postoji konstanta* $B > 0$ *takva da je*
$$\sum_{n \leq x} a(n) \leq Bx, \quad \forall x \geq 1.$$

Dokaz. Neka su
$$S(x) = \sum_{n \leq x} a(n), \quad T(x) = \sum_{n \leq x} a(n) \left[\frac{x}{n}\right].$$
Najprije ćemo dokazati drugu tvrdnju teorema. Tvrdimo kako vrijedi sljedeća nejednakost:
$$S(x) - S\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right). \tag{1.8}$$
Pišemo
$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n \leq x} \left[\frac{x}{n}\right] a(n) - 2 \sum_{n \leq x/2} \left[\frac{x}{2n}\right] a(n) \\ &= \sum_{n \leq x/2} \left(\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]\right) a(n) + \sum_{x/2 < n \leq x} \left[\frac{x}{n}\right] a(n). \end{aligned}$$
Budući da je razlika $[2y] - 2[y]$ jednaka ili 0 ili 1, prva suma je nenegativna, pa vrijedi
$$T(x) - 2T\left(\frac{x}{2}\right) \geq \sum_{x/2 < n \leq x} \left[\frac{x}{n}\right] a(n) = \sum_{x/2 < n \leq x} a(n) = S(x) - S\left(\frac{x}{2}\right).$$
Time smo pokazali nejednakost (1.8). No, (1.7) implicira
$$T(x) - 2T\left(\frac{x}{2}\right) = x \log x + O(x) - 2\left(\frac{x}{2} \log \frac{x}{2} + O(x)\right) = O(x).$$
Stoga (1.8) implicira da je $S(x) - S(x/2) = O(x)$. To znači da postoji konstanta $K > 0$ takva da je
$$S(x) - S\left(\frac{x}{2}\right) \leq Kx, \quad \forall x \geq 1.$$
Zamijenimo x redom s $x/2, x/4, \ldots$ kako bismo dobili
$$S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) \leq K\frac{x}{2},$$

$$S\left(\frac{x}{4}\right) - S\left(\frac{x}{8}\right) \leq K\frac{x}{4},$$

itd. Uočimo da je $S(x/2^n) = 0$, kada je $2^n > x$. Zbrojimo li sve nejednakosti dobivamo

$$S(x) \leq Kx\left(1 + \frac{1}{2} + \frac{1}{2} + \cdots\right) = 2Kx.$$

Uzmemo li da je $B = 2K$, dokazali smo drugu tvrdnju teorema.

Dokažimo sada prvu tvrdnju teorema. Pišemo li $[x/n] = (x/n) + O(1)$, dobivamo

$$\begin{aligned} T(x) &= \sum_{n\leq x}\left[\frac{x}{n}\right]a(n) = \sum_{n\leq x}\left(\frac{x}{n} + O(1)\right)a(n) \\ &= x\sum_{n\leq x}\frac{a(n)}{n} + O\left(\sum_{n\leq x}a(n)\right) \\ &= x\sum_{n\leq x}\frac{a(n)}{n} + O(x), \end{aligned}$$

po drugoj tvrdnji teorema. Stoga

$$\sum_{n\leq x}\frac{a(n)}{n} = \frac{1}{x}T(x) + O(1) = \log x + O(1).$$

Time smo dokazali i prvu tvrdnju teorema. □

Relacija (1.5) implicira

$$\sum_{n\leq x}\Lambda\left[\frac{x}{n}\right] = x\log x + O(x).$$

Budući da je $\Lambda(n) \geq 0$, možemo primijeniti Shapirov teorem definiramo li $a(n) = \Lambda(n)$.

Teorem 1.3.7. *Za svaki $x \geq 1$ vrijedi*

$$\sum_{n\leq x}\frac{\Lambda(n)}{n} = \log x + O(1). \tag{1.9}$$

Također, postoje pozitivne konstante c_1 i c_2 takve da je

$$\psi(x) \leq c_1 x, \quad \forall x \geq 1$$

i

$$\psi(x) \geq c_2 x, \quad \textit{za svaki dovoljno veliki } x.$$

Još jedna primjena Shapirovog teorema se može izvući iz formule

$$\sum_{p\le x}\left[\frac{x}{p}\right]\log p = x\log x + O(x)$$

dokazane u Teoremu 1.3.5. To pak možemo pisati u sljedećem obliku:

$$\sum_{n\le x}\Lambda_1(n)\left[\frac{x}{n}\right] = x\log x + O(x), \tag{1.10}$$

gdje je funkcija Λ_1 definirana na sljedeći način:

$$\Lambda_1(n) = \begin{cases}\log p, & n \text{ je prosti broj } p,\\ 0, & \text{inače.}\end{cases}$$

Budući da je $\Lambda_1(n) \ge 0$, formula (1.10) nam pokazuje da izraz $a(n) = \Lambda_1(n)$ zadovoljava hipoteze Shapirovog teorema. Obzirom da je $\vartheta(x) = \sum_{n\le x}\Lambda_1(n)$, iz prve tvrdnje Shapirovog teorema slijedi sljedeća formula:

Teorem 1.3.8. *Za sve $x \ge 1$ vrijedi*

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1). \tag{1.11}$$

Također, postoje pozitivne konstante c_1 i c_2 takve da je

$$\vartheta(x) \le c_1 x, \quad \forall x \ge 1$$

i

$$\vartheta(x) \ge c_2 x, \quad \textit{za svaki dovoljno veliki } x.$$

Poglavlje 2

Dirichletovi karakteri i L-funkcija

2.1 Karakteri konačne Abelove grupe

Jedan od ključnih pojmova koji će se javiti u dokazu Dirichletovog teorema će biti *Dirichletovi karakteri*. Da bismo mogli iznijeti svojstva ove aritmetičke funkcije, najprije ćemo uvesti mali dio teorije grupa koji nam je potreban za teoriju Dirichletovih karaktera.

Abelove grupe i karakteri

Definicija 2.1.1. *Grupa G je neprazni skup elemenata s binarnom operacijom $\cdot$ koji zadovoljava određene aksiome:*

1. Zatvorenost. $(\forall a, b \in G) \quad a \cdot b \in G$.
2. Asocijativnost. $(\forall a, b, c \in G) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Postojanje neutralnog elementa. $(\exists! e \in G) \quad t.d. \quad (\forall a \in G) \quad a \cdot e = e \cdot a = a$.
4. Postojanje inverza. $(\forall a \in G)\ (\exists! b \in G) \quad t.d. \quad a \cdot b = b \cdot a = e$.

Definicija 2.1.2. Abelova grupa. *Grupa G je Abelova ako svaki par elemenata komutira, odnosno, ako je $ab = ba$, $\forall a, b \in G$.*

Definicija 2.1.3. Konačna grupa. *Grupa G je konačna ako je G konačan skup. Broj elemenata od G zovemo redom od G.*

Definicija 2.1.4. *Neka je G prozvoljna grupa. Homomorfizam $f : G \to \mathbb{C}^x$ zovemo karakterom od G ako f ima multiplikativno svojstvo*

$$f(ab) = f(a)f(b), \quad \forall a, b \in G,$$

te ako je $f(c) \neq 0$, za neki $c \in G$.

Svaka grupa G ima barem jedan karakter, funkciju koja šalje svaki element iz G u 1. Taj karakter zovemo glavnim karakterom.

Relacija ortogonalnosti za karaktere

Neka je G konačna Abelova grupa reda n koja sadrži elemente $a_1, a_2, ..., a_n$ te neka su $f_1, f_2, ..., f_n$ karakteri od G, pri čemu je f_1 glavni karakter.

S $A = A(G)$ ćemo označavati $n \times n$ matricu $[a_{ij}]$ kojoj je element a_{ij} u i-tom retku i j-tom stupcu jednak

$$a_{ij} = f_i(a_j).$$

Pokazat ćemo da je matrica A invertibilna te iskoristiti to kako bi pokazali svojstvo ortogonalnosti među karakterima. Najprije, definirajmo sumu elemeata u svakom retku matrice A.

Teorem 2.1.5. *Suma elemenata u i-tom retku matrice A je dana s*

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n, & i = 1, \\ 0, & \textit{inače}. \end{cases}$$

Dokaz. Označimo s S sumu u iskazu teorema. Ako je $f_i = f_1$, tada je svaki sumand jednak 1 i $S = n$. Za $f_i \neq f_1$ postoji element $b \in G$ takav da je $f_i(b) \neq 1$. Kako a_r ide po svim elementima od G, tako ide i umnožak ba_r. Stoga vrijedi

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S.$$

Dakle, $S(1 - f_i(b)) = 0$. Pošto je $f_i(b) \neq 1$, slijedi $S = 0$. □

Iskoristimo sada ovaj teorem da bismo pokazali kako A ima inverz.

Teorem 2.1.6. *Neka je A^* hermitski adjungirana matrica matrice A. Tada imamo*

$$AA^* = nI,$$

gdje je I $n \times n$ jedinična matrica. Dakle, $n^{-1}A^*$ je inverz od A.

Dokaz. Neka je $B = AA^*$. Element u i-tom retku i j-tom stupcu matrice B dan je s

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\bar{f}_j(a_r) = \sum_{r=1}^{n} (f_i\bar{f}_j)(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

gdje je $f_k = f_i\bar{f}_j = \frac{f_i}{f_j}$. Znamo da je $\frac{f_i}{f_j} = f_1$ ako i samo ako je $i = j$. Stoga, iz prethodnog teorema slijedi

$$b_{ij} = \begin{cases} n, & \text{ako je} \quad i = j, \\ 0, & \text{ako je} \quad i \neq j. \end{cases}$$

Drugim riječima, $B = nI$. □

Teorem 2.1.7. Relacije ortogonalnosti među karakterima. *Vrijedi:*

$$\sum_{r=1}^{n} \bar{f}_r(a_i) f_r(a_j) = \begin{cases} n, & ako\, je \quad a_i = a_j, \\ 0, & ako\, je \quad a_i \neq a_j. \end{cases}$$

Dokaz. Iskoristimo činjenicu da matrica komutira sa svojim inverzom pa je $AA^* = A^*A = nI$. Sada tvrdnja slijedi direktno jer je element u i-tom retku i j-tom stupcu matrice A^*A jednak sumi u teoremu. □

2.2 Dirichletovi karakteri

Neka je G reducirani sustav ostataka modulo fiksni prirodni broj k. Najprije pokažimo kako uz dobro definirano množenje, G zaista čini multiplikativnu grupu.

Prisjetimo se, reducirani sustav ostataka modulo k je skup od $\varphi(k)$ prirodnih brojeva $\{a_1, a_2, ..., a_{\varphi(k)}\}$ međusobno nekongruentnih modulo k. Pritom je svaki od njih relativno prost s k. Također, za svaki cijeli broj a, ostatak $\hat{a}$ je skup svih cijelih brojeva kongruentnih s a modulo k. Sada možemo definirati množenje ostataka relacijom:

$$\hat{a} \cdot \hat{b} = \hat{ab}.$$

Teorem 2.2.1. *Uz množenje definirano kao u gornjoj relaciji, reducirani sustav ostataka modulo k je konačna Abelova grupa reda $\varphi(k)$. Neutralni element ove grupe je $\hat{1}$. Inverz ostatka $\hat{a}$ je ostatak $\hat{b}$ takav da je $ab \equiv 1 \pmod{k}$.*

Dokaz. Iz definicije množenja ostataka slijedi svojstvo zatvorenosti. Očito je ostatak $\hat{1}$ neutralni element. Ako vrijedi $(a, b) = 1$, tada postoji jedinstveni b takav da je $ab \equiv 1 \pmod{k}$. Stoga je inverz od $\hat{a}$ jednak $\hat{b}$. Konačno, jasno je da je grupa Abelova te da je reda $\varphi(k)$. □

Definicija 2.2.2. Dirichletov karakter. *Neka je grupa G reducirani sustav ostataka modulo k. Za svaki karakter f grupe G definiramo aritmetičku funkciju $\chi = \chi_f$ na sljedeći način:*

$$\chi(n) = \begin{cases} f(\hat{n}), & (n, k) = 1, \\ 0, & (n, k) > 1. \end{cases}$$

Funkciju χ nazivamo Dirichletov karakter modulo k. Glavni karakter χ_1 je onaj sa svojstvom

$$\chi_1(n) = \begin{cases} 1, & (n,k) = 1, \\ 0, & (n,k) > 1. \end{cases}$$

Teorem 2.2.3. *Svaki Dirichletov karakter modulo k je multiplikativan i periodičan s periodom k. Odnosno, vrijedi*

$$\chi(mn) = \chi(m)\chi(n), \quad \forall m, n, \tag{2.1}$$

i

$$\chi(n+k) = \chi(n), \quad \forall n. \tag{2.2}$$

Obratno, ako je χ multiplikativna funkcija i periodična s periodom k te je za $(n,k) > 1$ $\chi(n) = 0$, tada je χ jedan od Dirichletovih karaktera modulo k.

Dokaz. Svojstvo multiplikativnosti (2.1) od χ_f naslijeđeno je od f, onda kada su m i n relativno prosti s k. Ako jedno od m ili n nije relativno prosto s k, tada nije ni mn relativno prosto s k, pa bi obje strane u (2.1) bile jednake nuli. Svojstvo periodičnosti slijedi iz činjenice da je $\chi_f = f(\hat{n})$ i da $a \equiv b \pmod{k}$ implicira $(a,k) = (b,k)$.

Kako bi pokazali obrat primijetimo da je funkcija f definirana na G izrazom

$$f(\hat{n}) = \chi(n), \quad \textit{ako je} \quad (n,k) = 1$$

karakter grupe G, pa je χ Dirichletov karakter modulo k. □

Sada navodimo relaciju ortogonalnosti za Dirichletove karaktere:

Teorem 2.2.4. *Neka su $\chi_1, \chi_1, ..., \chi_{\varphi(k)}$ $\varphi(k)$ Dirichletovih karaktera modulo k te $m, n \in \mathbb{N}$ takvi da je $(n,k) = 1$. Tada vrijedi:*

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\bar{\chi}_r(n) = \begin{cases} \varphi(k), & m \equiv n \pmod{k}, \\ 0, & m \not\equiv n \pmod{k}. \end{cases}$$

Dokaz. Ako je $(m,k) = 1$, dovoljno je uzeti $a_i = \hat{n}$ i $a_j = \hat{m}$ i iskoristiti relaciju ortogonalnosti pokazanu prije. Uočimo kako je $\hat{m} = \hat{n}$ ako i samo ako je $m \equiv n \pmod{k}$. Ako je $(m,k) > 1$, tada su svi sumandi jednaki nuli i $m \not\equiv n \pmod{k}$. □

Sume koje sadrže Dirichletove karaktere

Pokazat ćemo kako se razvijaju sume koje uključuju Dirichletove karaktere. Napomenimo kako su netrivijalni karakteri f oni sa svojstvom da je $f(g) \neq 1$, za $g \in G$, gdje je G konačna Abelova grupa.

Teorem 2.2.5. *Neka je χ netrivijalni karakter modulo k te f nenegativna funkcija koja ima negativnu prvu derivaciju $f'(x)$ za sve $x \geq x_0$. Tada za svaki $y \geq x \geq x_0$ vrijedi*

$$\sum_{x<n\leq y} \chi(n)f(n) = O(f(x)). \tag{2.3}$$

Ako dodatno vrijedi još i $f(x) \to 0$ kada $x \to \infty$, tada beskonačna suma reda

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

konvergira, i za sve $x \geq x_0$ vrijedi

$$\sum_{n\leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x)). \tag{2.4}$$

Dokaz. Neka je $A(x) = \sum_{n\leq x} \chi(n)$. Budući da je χ netrivijalna funkcija, imamo

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

Zbog periodičnosti slijedi da je $A(nk) = 0$, za $n = 2, 3, ...$, pa je $|A(x)| < \varphi(k), \forall x$. Drugim riječima, $A(x) = O(1)$.

Pošto je $\chi(n)$ aritmetička funkcija, f ima negativnu prvu derivaciju na $[x, y]$ te $A(x) = \sum_{n\leq x} \chi(n)$, možemo iskoristiti Abelov identitet (v. [1], Teorem 4.2) kako bi sumu u (2.3) izrazili kao integral. To nam daje sljedeće:

$$\begin{aligned}\sum_{x<n\leq y} \chi(n)f(n) &= f(y)A(y) - f(x)A(x) - \int_x^y A(t)f'(t)\,dt \\ &= O(f(y)) + O(f(x)) + O\left(\int_x^y (-f'(t))\,dt\right) \\ &= O(f(x))\end{aligned}$$

Time je dokazana relacija (2.3). Ako $f(x) \to 0$ kada $x \to \infty$, tada iz relacije (2.3) slijedi da niz

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

konvergira po Cauchyjevom kriteriju konvergencije. Kako bi pokazali (2.4), potrebno je uočiti da

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n\leq x} \chi(n)f(n) + \lim_{y\to\infty} \sum_{x<n\leq y} \chi(n)f(n).$$

Zbog (2.3) je limes na desnoj strani jednakosti jednak $O(f(x))$. Time je teorem dokazan. □

Primijenimo li ovaj teorem na funkcije $f(x) = 1/x$, $f(x) = (\log x)/x$ i $f(x) = 1/\sqrt{x}$, za $x \geq 1$ dobivamo rezultate bitne za dokazivanje Dirichletovog teorema:

$$\sum_{n\leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right), \tag{2.5}$$

$$\sum_{n\leq x} \frac{\chi(n)\log n}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n} + O\left(\frac{\log x}{x}\right), \tag{2.6}$$

$$\sum_{n\leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right). \tag{2.7}$$

2.3 Funkcija $L(1,\chi)$

S $L(1,\chi)$ ćemo označavati sumu reda (2.3). Dakle,

$$L(1,\chi) = \sum_{n\leq x} \frac{\chi(n)}{n}.$$

U dokazu Dirichletova teorema ćemo koristiti činjenicu da je $L(1,\chi) \neq 0$, kada je χ netrivijalni karakter. Sada ćemo dokazati kako to vrijedi za realne netrivijalne karaktere.

Teorem 2.3.1. *Neka je χ neki realni karakter modulo k i*

$$A(n) = \sum_{d|n} \chi(d).$$

Tada je $A(n) \geq 0$, $\forall n$, i specijalno $A(n) \geq 1$, ako je n kvadrat.

Dokaz. Za potencije prostih brojeva imamo

$$A(p^a) = \sum_{t=0}^{a} \chi(p^t) = 1 + \sum_{t=1}^{a} \chi^t(p).$$

Pošto je χ realna funkcija, jedine moguće vrijednosti koje ona postiže su 0, 1 i -1. Ako je $\chi(p) = 0$, tada je $A(p^a) = 1$; za $\chi(p) = 1$ je $A(p^a) = a + 1$; te je za $\chi(p) = -1$

$$A(p^a) = \begin{cases} 0, & \text{ako je } a \text{ neparan,} \\ 1, & \text{ako je } a \text{ paran.} \end{cases}$$

U svim slučajevima je $A(p^a) \geq 1$ ako je a paran.

Budući da je A multiplikativna, za $n = p_1^{a_1} \cdots p_r^{a_r}$ vrijedi $A(n) = A(p_1^{a_1}) \cdots A(p_r^{a_r})$. Svaki je od faktora $A(p_i^{a_i}) \geq 0$ pa je i $A(n) \geq 0$. Također, ako je n kvadrat, svaki eksponent a_i je paran, stoga je i svaki faktor $A(p_i^{a_i}) \geq 1$ pa je i $A(n) \geq 1$. □

Teorem 2.3.2. *Uzmimo za svaki realni netrivijalni karakter χ modulo k da je*

$$A(n) = \sum_{d|n} \chi(d) \quad i \quad B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}}.$$

Tada imamo:

1. $B(x) \to \infty$ *kada* $x \to \infty$.
2. $B(x) = 2\sqrt{x}L(1,\chi) + O(1)$, $\forall x \geq 1$.

Iz čega slijedi da je $L(1,\chi) \neq 0$.

Dokaz. Kako bismo dokazali prvi dio teorema, koristimo prethodni teorem te imamo

$$B(x) \geq \sum_{\substack{n \leq x \\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m}.$$

Pošto harmonijski red $\sum 1/m$ divergira, posljednja suma teži ka ∞ kada $x \to \infty$.

Da bismo dokazali drugi dio teorema, pisat ćemo

$$B(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q,d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}}.$$

Sjetimo se Dirichletovog produkta iz prvog poglavlja. Definiramo li funkcije na sljedeći način:

$$F(x) = \sum_{n \leq x} f(n), \quad G(x) = \sum_{n \leq x} g(n) \quad i \quad H(x) = \sum_{n \leq x} (f * g)(n),$$

tada za $a, b \in \mathbb{R}$ takve da je $ab = x$ vrijedi

$$\sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) = \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b).$$

Uzmemo li da je $a = b = \sqrt{x}$ i $f(n) = \chi(n)/\sqrt{n}$, $g(n) = 1/\sqrt{n}$, dobivamo relaciju

$$B(x) = \sum_{\substack{q,d \\ qd \leq x}} \frac{\chi(d)}{\sqrt{qd}} = \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}). \tag{2.8}$$

Primijenimo sada Eulerovu sumacijsku formulu (Teorem 1.3.3) kako bismo dobili

$$G(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right)$$

gdje je A konstanta, a prema (2.7) imamo

$$F(x) = \sum_{n \le x} \frac{\chi(n)}{\sqrt{n}} = B + O\left(\frac{1}{\sqrt{x}}\right),$$

gdje je $B = \sum_{n=1}^{\infty} \chi(n)/\sqrt{n}$. Budući da je $F(\sqrt{x})G(\sqrt{x}) = 2Bx^{1/4} + O(1)$, iz relacije (2.8) dobivamo sljedeće:

$$\begin{aligned} B(x) = &\sum_{n \le \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \left[2\sqrt{\frac{x}{n}} + A + O\left(\sqrt{\frac{n}{x}}\right)\right] \\ &+ \sum_{n \le \sqrt{x}} \frac{1}{\sqrt{n}} \left[B + O\left(\sqrt{\frac{n}{x}}\right)\right] - 2Bx^{1/4} + O(1) \\ =&2\sqrt{x} \sum_{n \le \sqrt{x}} \frac{\chi(n)}{n} + A \sum_{n \le \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \le \sqrt{x}} |\chi(n)|\right) \\ &+ B \sum_{n \le \sqrt{x}} \frac{1}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \le \sqrt{x}} 1\right) - 2Bx^{1/4} + O(1) \\ =&2\sqrt{x} L(1, \chi) + O(1). \end{aligned}$$

Ovime je dokazan drugi dio teorema. Sada je očito da prvi i drugi dio zajedno impliciraju kako je $L(1, \chi) \neq 0$. □

Zanimljivo je spomenuti kako je funkcija $L(s, \chi)$, $s \in \mathbb{C}$, generalizacija tzv. *Riemmanove zeta funkcije*. Kako u dokazu Dirichletovog teorema koristimo samo svojstvo $L(1, \chi) \neq 0$, za netrivijalne karaktere χ, funkciju zeta ćemo samo definirati.

Definicija 2.3.3. *Riemmanova zeta funkcija je definirana s*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in \mathbb{C}.$$

Da bi ovaj red bio konvergentan, nužno je da $\operatorname{Re} s > 1$.

Osnovnu vezu između Riemmanove zeta funkcije i prostih brojeva daje *Eulerova produktna formula*:

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

Dokaz ove formule nalazi se u [1], Teorem 11.6.

Poglavlje 3

Dokaz Dirichletovog teorema

3.1 Dokaz

Cilj ovog rada je dokazati Dirichletov teorem, odnosno da aritmetički niz oblika

$$kn + h, \quad n = 0, 1, 2...$$

sadrži beskonačno mnogo prostih brojeva kada je k pozitivan i $(h, k) = 1$.

Plan dokaza Dirichletovog teorema

U Teoremu 1.3.8 smo izveli asimptotsku formulu

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1), \tag{3.1}$$

gdje suma ide po svim prostim brojevima p, $p \leq x$. Dirichletov teorem ćemo dokazati kao posljedicu sljedeće asimptotske formule.

Teorem 3.1.1. *Za $k > 0$ takav da je $(h, k) = 1$ vrijedi*

$$\sum_{\substack{p \leq x \\ p \equiv h \pmod{k}}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1), \tag{3.2}$$

gdje je $x > 1$ i suma ide po svim prostim brojevima p takvima da je $p \leq x$ i p je kongruentno h modulo k.

Budući da $\log x \to \infty$ kada $x \to \infty$, ova relacija implicira da postoji beskonačno mnogo prostih brojeva $p \equiv h \pmod{k}$, dakle beskonačno ih je mnogo u aritmetičkom nizu

$nk + h, n = 0, 1, 2, ...$ Primijetimo kako izraz zdesna u (3.2) ne ovisi o h te stoga (3.2) implicira Dirichletov teorem.

Kako bi dokazali Teorem 3.1.1, potrebno je najprije dokazati nekoliko lema koje prethode dokazivanju istoga.
Navodim oznake koje ćemo koristiti u sljedećim lemama: k je pozitivni cijeli broj, a h cijeli broj relativno prost sa k, $\varphi(k)$ Dirichletovih karaktera modulo k indeksiramo s

$$\chi_1, \chi_2, ..., \chi_{\varphi(k)}$$

gdje je χ_1 glavni karakter. Za $\chi \neq \chi_1$ su $L(1,\chi)$ i $L'(1,\chi)$ oznake za sljedeće sume:

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n},$$

$$L'(1,\chi) = -\sum_{n=1}^{\infty} \frac{\chi(n)\log n}{n}.$$

Prema Teoremu 2.2.5 znamo kako ove dvije sume konvengiraju. Štoviše, znamo i da je $L(1,\chi) \neq 0$ za realne χ. Prost broj označavamo s p, a $\sum_{p\leq x}$ označava sumu po svim prostim brojevima $p \leq x$.

Lema 3.1.2. *Za $x > 1$ vrijedi*

$$\sum_{\substack{p\leq x \\ p\equiv h \,(\mathrm{mod}\ k)}} \frac{\log p}{p} = \frac{1}{\varphi(k)}\log x + \frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p} + O(1).$$

Očito ova lema implicira Teorem 3.1.1 ukoliko pokažemo da za svaki $\chi \neq \chi_1$ vrijedi

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = O(1). \tag{3.3}$$

Sljedeća lema prikazuje ovu sumu u formi koja nije izražena pomoću prostih brojeva.

Lema 3.1.3. *Za sve $x > 1$ i $\chi \neq \chi_1$ vrijedi*

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = -L'(1,\chi)\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + O(1).$$

Dakle, Lema 3.1.3 implicira (3.3) ako pokažemo da je

$$\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = O(1). \tag{3.4}$$

Ova tvrdnja izvedena je iz sljedeće leme.

Lema 3.1.4. *Za sve $x > 1$ i $\chi \neq \chi_1$ vrijedi*

$$L(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} = O(1). \tag{3.5}$$

Kada bi vrijedilo $L(1,\chi) \neq 0$, mogli bismo iz (3.5) dobiti (3.4). Dakle, dokaz Dirichletovog teorema ovisi o vrijednosti $L(1,\chi)$ za $\chi \neq \chi_1$ (ne smije biti jednak 0). Kako je već dokazano u Teoremu 2.3.2, $L(1,\chi) \neq 0$ za realne $\chi \neq \chi_1$. Stoga nam sada preostaje pokazati kako to vrijedi za sve $\chi \neq \chi_1$ koji osim realnih postižu i kompleksne vrijednosti.

Uvodimo oznaku $N(k)$ koja predstavlja broj netrivijalnih karaktera χ modulo k za koje je $L(1,\chi) = 0$. Ako je $L(1,\chi) = 0$, tada vrijedi $L(1,\bar{\chi}) = 0$ i $\chi \neq \bar{\chi}$ pošto χ nije realan. Dakle, karakteri χ za koje je $L(1,\chi) = 0$ se pojavljuju u konjugiranim parovima pa je $N(k)$ paran broj. Naš cilj je pokazati da je $N(k) = 0$, a to ćemo izvesti iz sljedeće formule.

Lema 3.1.5. *Za sve $x > 1$ vrijedi*

$$\sum_{\substack{p\leq x\\ p\equiv h \,(\mathrm{mod}\ k)}}\frac{\log p}{p} = \frac{1-N(k)}{\varphi(k)}\log x + O(1). \tag{3.6}$$

Ukoliko $N(k) \neq 0$, tada je $N(k) \geq 2$ pošto je $N(k)$ paran, pa je predznak od $\log x$ u (3.6) negativan i desna strana jednakosti teži u $-\infty$ kada $x \to \infty$. To je pak kontradikcija jer su svi sumandi slijeva pozitivni. Dakle, Lema 3.1.5 implicira da je $N(k) = 0$. Dokaz Leme 3.1.5 ćemo izvesti iz sljedeće formule.

Lema 3.1.6. *Za sve $\chi \neq \chi_1$ i $L(1,\chi) = 0$ vrijedi*

$$L'(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} = \log x + O(1).$$

Dokaz Leme 3.1.2

Dokaz. Dokaz Leme 3.1.2 počinjemo s asimptotskom formulom (3.1) spomenutom na početku poglavlja

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + O(1).$$

Trebamo izvući izraze u sumi koji se javljaju za proste brojeve p takve da $p \equiv h \pmod{k}$. To ćemo napraviti pomoću relacije ortogonalnosti koja vrijedi za Dirichletove karaktere, kako smo izrazili u Teoremu 2.2.4:

$$\sum_{r=1}^{\varphi(k)}\chi_r(m)\bar{\chi}_r(n) = \begin{cases}\varphi(k), & m \equiv n \pmod{k},\\ 0, & m \not\equiv n \pmod{k}.\end{cases}$$

To vrijedi za $(n,k)=1$. Neka je $m=p$ i $n=h$, za $(h,k)=1$. Pomnožimo obje strane s $p^{-1}\log p$ te sumirajmo po svim $p\leq x$. Tada dobivamo:

$$\sum_{p\leq x}\sum_{r=1}^{\varphi(k)}\chi_r(p)\bar{\chi}_r(h)\frac{\log p}{p}=\varphi(k)\sum_{\substack{p\leq x\\ p\equiv h\,(\mathrm{mod}\ k)}}\frac{\log p}{p}. \tag{3.7}$$

Ako u sumi slijeva izdvojimo samo sumande koji uključuju glavni karakter χ_1, dobivamo novi izraz

$$\varphi(k)\sum_{\substack{p\leq x\\ p\equiv h\,(\mathrm{mod}\ k)}}\frac{\log p}{p}=\bar{\chi}_1(h)\sum_{p\leq x}\frac{\chi_1(p)\log p}{p}+\sum_{r=2}^{\varphi(k)}\bar{\chi}_r(h)\sum_{p\leq x}\frac{\chi_r(p)\log p}{p}. \tag{3.8}$$

Sada su $\bar{\chi}_1(h)=1$ i $\chi_1(p)=0$, osim za $(p,k)=1$ i tada je $\chi_1(p)=1$.
Stoga prvi izraz na desnoj strani daje

$$\sum_{\substack{p\leq x\\ (p,k)=1}}\frac{\log p}{p}=\sum_{p\leq x}\frac{\log p}{p}-\sum_{\substack{p\leq x\\ p|k}}\frac{\log p}{p}=\sum_{p\leq x}\frac{\log p}{p}+O(1), \tag{3.9}$$

jer postoji samo konačno mnogo prostih brojeva koji dijele k. Kombinacijom izraza (3.8) i (3.9) slijedi

$$\varphi(k)\sum_{\substack{p\leq x\\ p\equiv h\,(\mathrm{mod}\ k)}}\frac{\log p}{p}=\sum_{p\leq x}\frac{\log p}{p}+\sum_{r=2}^{\varphi(k)}\bar{\chi}_r(h)\sum_{p\leq x}\frac{\chi_r(p)\log p}{p}+O(1).$$

Korištenjem tvrdnje (3.1) i dijeljenjem s $\varphi(k)$ je dokazana Lema 3.1.2. □

Dokaz Leme 3.1.3

Dokaz. Počinjemo sa sumom

$$\sum_{n\leq x}\frac{\chi(n)\Lambda(n)}{n},$$

gdje je $\Lambda(n)$ Van Mangoldtova funkcija te izrazimo gornju sumu na dva načina.
Najprije primjetimo kako iz definicije od $\Lambda(n)$ slijedi

$$\sum_{n\leq x}\frac{\chi(n)\Lambda(n)}{n}=\sum_{\substack{p\leq x\\ p^a\leq x}}\sum_{a=1}^{\infty}\frac{\chi(p^a)\log p}{p^a}.$$

Izlučimo li izraze sa $a = 1$, dobivamo sljedeće

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = \sum_{p\le x}\frac{\chi(p)\log p}{p} + \sum_{\substack{p\le x\\ p^a\le x}}\sum_{a=2}^{\infty}\frac{\chi(p^a)\log p}{p^a}. \tag{3.10}$$

Druga suma zdesna je omeđena s

$$\sum_{p}\log p\sum_{a=2}^{\infty}\frac{1}{p^a} = \sum_{p}\frac{\log p}{p(p-1)} < \sum_{n=2}^{\infty}\frac{\log n}{n(n-1)} = O(1),$$

pa iz (3.10) slijedi

$$\sum_{p\le x}\frac{\chi(p)\log p}{p} = \sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} + O(1). \tag{3.11}$$

Sada se sjetimo kako je $\Lambda(n) = \sum_{d|n}\mu(d)\log(n/d)$, stoga je

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = \sum_{n\le x}\frac{\chi(n)}{n}\sum_{d|n}\mu(d)\log\left(\frac{n}{d}\right).$$

U zadnjoj sumi pišemo $n = cd$ i koristimo svojstvo multiplikativnosti od χ kako bismo dobili

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = \sum_{d\le x}\frac{\mu(d)\chi(d)}{d}\sum_{c\le x/d}\frac{\chi(c)\log(c)}{c}. \tag{3.12}$$

Pošto je $x/d \ge 1$, u sumi po c možemo koristiti formulu (2.6) te dobijemo

$$\sum_{c\le x/d}\frac{\chi(c)\log c}{c} = -L'(1,\chi) + O\left(\frac{\log x/d}{x/d}\right).$$

Sada je formula (3.12) jednaka formuli

$$\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n} = -L'(1,\chi)\sum_{d\le x}\frac{\mu(d)\chi(d)}{d} + O\left(\sum_{d\le x}\frac{1}{d}\frac{\log x/d}{x/d}\right). \tag{3.13}$$

Suma u greški jednaka je

$$\frac{1}{x}\sum_{d\le x}(\log x - \log d) = \frac{1}{x}\left([x]\log x - \sum_{d\le x}\log d\right) = O(1)$$

jer je

$$\sum_{d\le x}\log d = \log[x]! = x\log x + O(x).$$

Stoga, (3.13) jednako je

$$\sum_{n\leq x}\frac{\chi(n)\Lambda(n)}{n} = -L'(1,\chi)\sum_{d\leq x}\frac{\mu(d)\chi(d)}{d} + O(1)$$

što zajedno s (3.11) dokazuje Lemu 3.1.3.

□

Dokaz Leme 3.1.4

U dokazu ove leme koristimo generaliziranu Möbiusovu formulu inverzije, dokazanu u Teoremu 1.1.8, koja tvrdi da za potpuno multiplikativnu funkciju α vrijedi

$$G(x) = \sum_{n\leq x}\alpha(n)F\left(\frac{x}{n}\right) \quad \Leftrightarrow \quad F(x) = \sum_{n\leq x}\mu(n)\alpha(n)G\left(\frac{x}{n}\right). \tag{3.14}$$

Neka su $\alpha(n) = \chi(n)$ i $F(x) = x$. Tada dobivamo sljedeće

$$x = \sum_{n\leq x}\mu(n)\chi(n)G\left(\frac{x}{n}\right), \tag{3.15}$$

gdje je

$$G(x) = \sum_{n\leq x}\chi(n)\frac{x}{n} = x\sum_{n\leq x}\frac{\chi(n)}{n}.$$

Prema formuli (2.5), možemo pisati $G(x) = xL(1,\chi)+O(1)$. Koristeći to u (3.15) dobivamo

$$x = \sum_{n\leq x}\mu(n)\chi(n)\left\{\frac{x}{n}L(1,\chi) + O(1)\right\} = xL(1,\chi)\sum_{n\leq x}\frac{\mu(n)\chi(n)}{n} + O(1).$$

Dijeljenjem ovog izraza s x je dokazana Lema 3.1.4.

Dokaz Leme 3.1.6

Dokaz. Dokazat ćemo Lemu 3.1.6 te ju iskoristiti kako bismo dokazali Lemu 3.1.5. Opet koristimo generaliziranu Möbiusovu formulu inverzije (3.14).
Neka je $F(x) = x\log x$. Tada vrijedi

$$x\log x = \sum_{n\leq x}\mu(n)\chi(n)G\left(\frac{x}{n}\right), \tag{3.16}$$

gdje je

$$G(x) = \sum_{n\leq x}\chi(n)\frac{x}{n}\log\frac{x}{n} = x\log x\sum_{n\leq x}\frac{\chi(n)}{n} - x\sum_{n\leq x}\frac{\chi(n)\log n}{n}.$$

Sada, pošto pretpostavljamo $L(1,\chi) = 0$, iskoristimo formule (2.5) i (2.6) kako bismo dobili

$$\begin{aligned} G(x) &= x\log x\left\{L(1,\chi) + O\left(\frac{1}{x}\right)\right\} + x\left\{L'(1,\chi) + O\left(\frac{\log x}{x}\right)\right\} \\ &= xL'(1,\chi) + O(\log x). \end{aligned}$$

Stoga iz (3.16) dobivamo

$$\begin{aligned} x\log x &= \sum_{n\le x}\mu(n)\chi(n)\left\{\frac{x}{n}L'(1,\chi) + O\left(\log\frac{x}{n}\right)\right\} \\ &= xL'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n} + O\left(\sum_{n\le x}(\log x - \log n)\right). \end{aligned}$$

Iz dokaza Leme 3.1.3 znamo kako je izraz u greški jednak $O(x)$. Pa imamo

$$x\log x = xL'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n} + O(x),$$

iz čega dijeljenjem s x slijedi tvrdnja Leme 3.1.6.

□

Dokaz Leme 3.1.5

Dokaz. Uvrstimo li $h = 1$ u Lemu 3.1.2, dobivamo

$$\sum_{\substack{p\le x\\ p\equiv 1 \pmod k}}\frac{\log p}{p} = \frac{1}{\varphi(k)}\log x + \frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\sum_{p\le x}\frac{\chi_r(p)\log p}{p} + O(1). \tag{3.17}$$

U sumi po p zdesna koristimo Lemu 3.1.3 po kojoj je

$$\sum_{p\le x}\frac{\chi_r(p)\log p}{p} = -L'(1,\chi_r)\sum_{n\le x}\frac{\mu(n)\chi_r(n)}{n} + O(1).$$

Ako je $L(1,\chi_r) \neq 0$, tada je po Lemi 3.1.4 desna strana prethodne jednakosti jednaka $O(1)$. No, ako je $L(1,\chi_r) = 0$, tada Lema 3.1.6 implicira

$$-L'(1,\chi_r)\sum_{n\le x}\frac{\mu(n)\chi_r(n)}{n} = -\log x + O(1).$$

Dakle, desna strana jednakosti (3.17) jednaka je

$$\frac{1}{\varphi(k)}\{-N(k)\log x + O(1)\},$$

pa je (3.17) zapravo

$$\sum_{\substack{p\leq x \\ p\equiv 1 \pmod{k}}} \frac{\log p}{p} = \frac{1-N(k)}{\varphi(k)}\log x + O(1).$$

□

Kao što smo na početku poglavlja naglasili, Teorem 3.1.1 implicira Dirichletov teorem:

Teorem 3.1.7. *Ako je $k > 0$ i $(h,k) = 1$, tada postoji beskonačno mnogo prostih brojeva u aritmetičkom nizu oblika $nk + h, n = 0, 1, 2, ...$*

3.2 Distribucija prostih brojeva u aritmetičkim nizovima

Za $k > 0$ i $(a,k) = 1$ definiramo

$$\pi_a(x) = \sum_{\substack{p\leq x \\ p\equiv a \pmod{k}}} 1.$$

Dakle, funkcija $\pi_a(x)$ nam vraća broj prostih brojeva $\leq x$ u nizu $nk + a, n = 0, 1, 2, ...$ Dirichletov teorem nam govori kako $\pi_a(x) \to \infty$ kada $x \to \infty$. Postoji i teorem o prostim brojevima za aritmetičke nizove koji tvrdi da za $(a,k) = 1$ vrijedi

$$\pi_a(x) \sim \frac{\pi(x)}{\varphi(k)} \sim \frac{1}{\varphi(k)}\frac{x}{\log x}, \quad \text{kada} \quad x \to \infty, \tag{3.18}$$

pri čemu je za $x > 0$, $\pi(x)$ broj prostih brojeva koji nisu veći od x.

Formula (3.1)

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

sugestira teorem o prostim brojevima za aritmetičke nizove. Budući da glavni izraz ne ovisi o h, čini se kako su prosti brojevi podjednako distribuirani među $\varphi(k)$ reduciranih klasa ostataka modulo k te je relacija (3.18) zapravo precizna bilješka ove činjenice.

Ovo poglavlje ćemo zaključiti s alternativnom formulacijom teorema o prostim brojevima za aritmetičke nizove.

Teorem 3.2.1. *Ako relacija*

$$\pi_a(x) \sim \frac{\pi(x)}{\varphi(k)}, \quad kada \quad x \to \infty \tag{3.19}$$

vrijedi za svaki cijeli broj a relativno prost s k, tada vrijedi i

$$\pi_a(x) \sim \pi_b(x), \quad kada \quad x \to \infty \tag{3.20}$$

za sve b takve da je $(a, k) = (a, k) = 1$. *Vrijedi i obratno, (3.20) implicira (3.19).*

Dokaz. Prvi smjer je očit. Kako bi dokazali obrat, pretpostavimo da vrijedi (3.20) i neka je $A(k)$ broj prostih brojeva koji dijele d. Za $x > k$ imamo

$$\begin{aligned}\pi(x) &= \sum_{p \le x} 1 = A(k) + \sum_{\substack{p \le x \\ p \nmid k}} 1 \\ &= A(k) + \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \left(\sum_{\substack{p \le x \\ p \equiv a \pmod{k}}} 1 \right) = A(k) + \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \pi_a(x).\end{aligned}$$

Sada slijedi

$$\frac{\pi(x) - A(x)}{\pi_b(x)} = \sum_{\substack{a=1 \\ (a,k)=1}}^{k} \frac{\pi_a(x)}{\pi_b(x)}.$$

Prema (3.20), svaki izraz u sumi teži k 1, kada $x \to \infty$ pa suma teži prema $\varphi(k)$. Stoga

$$\frac{\pi(x)}{\pi_b(x)} - \frac{A(x)}{\pi_b(x)} \to \varphi(k), \quad \text{kada} \quad x \to \infty.$$

No $A(k)/\pi_b(x) \to 0$ pa $\pi(x)/\pi_b(x) \to \varphi(x)$, što dokazuje (3.19). □

Bibliografija

[1] T. M. Apostol, *Introduction to analytic number theory*, Springer, New York, 1976.

Sažetak

U ovom radu je dokazan Dirichletov teorem, rezultat koji dokazuje kako aritmetički niz oblika

$$kn + h, \quad (h, k) = 1, \quad n = 0, 1, 2, ...,$$

sadrži beskonačno mnogo prostih brojeva.

U prvom poglavlju su dane osnovne definicije i svojstva funkcija koje koristimo u radu. Najvažniji rezultat izveden u ovom poglavlju je dokaz Harolda N. Shapira da red $\sum p^{-1} \log p$ divergira, gdje se sumira po svim prostim brojevima p. Također, dokazani su i osnovni teoremi koji pokazuju kako je skup prostih brojeva beskonačan.

U drugom poglavlju se upoznajemo s karakterima konačne Abelove grupe. Od velike važnosti za dokaz Dirichletovog teorema su Dirichletovi karakteri χ i funkcija $L(1, \chi)$. Osobito je bitan dokaz kako je $L(1, \chi) \neq 0$ za sve realne netrivijalne karaktere χ.

Sam dokaz Dirichletovog teorema je izveden u trećem, ujedno i posljednjem, poglavlju. Nizom lema smo dokazali Dirichletov teorem kao posljedicu Shapirove formule (iz prvog poglavlja), proširene uvjetom na proste brojeve p kongruentne s h modulo k.

Summary

This thesis proves Dirichlet's theorem, a result that states that any arithmetic progression of the form

$$kn + h \quad (h, k) = 1, \quad n = 0, 1, 2, ...,$$

contains infinitely many primes.

In the first chapter we give basic definitions and properties of functions that are used in this thesis. The most important result derived in this section is the proof by Harold N. Shapiro that shows that the series $\sum p^{-1} \log p$, extended over all primes, diverges. Also, the basic theorems that show that the set of prime numbers is infinite are proven.

In the second chapter we become familiar with characters of finite Abelian groups. Of great importance for the proof of Dirichlet's theorem are Dirichlet characters χ and the functions $L(1, \chi)$. It is particularly important to know that $L(1, \chi) \neq 0$ for all real nonprincipal characters χ.

The proof of Dirichlet's theorem is carried out in the third, and the last, chapter. Through series of lemmas we prove Dirichlet's theorem as a consequence of Shapiro's formula (from the first chapter), extended over all primes p which are congruent to h mod k.

Životopis

Rođena sam 22. veljače 1992. godine u Zagrebu. Osnovnoškolsko obrazovanje sam stekla u Osnovnoj školi Brezovica. Nakon toga upisala sam V. gimnaziju u Zagrebu, gdje sam maturirala 2010. godine. Iste godine sam upisala preddiplomski sveučilišni studij Matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Preddiplomski studij sam završila 2013. godine te sam iste godine upisala diplomski sveučilišni studij Financijske i poslovne matematike na istom fakultetu, kojeg završavam ovim radom.

Aktivno se bavim folklorom već 18 godina, od čega zadnjih pet godina plešem u Folklornom ansamblu Zagreb-Markovac.