SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Mateja Škledar

DIRICHLETOV TEOREM

Diplomski rad

Voditelj rada:
Prof. dr. sc. Pavle Pandžić

Zagreb, rujan 2015.

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. _____

Mojoj obitelji na pruženoj podrški i povjerenju za vrijeme studija.

Sadržaj

Uvod

Dirichletov teorem o postojanju prostih brojeva u aritmetičkim nizovima jedan je od prvih teorema u analitičkoj teoriji brojeva koji otprilike 50 godina prethodi teoremu o prostim brojevima i koji je imao jednako važan utjecaj na razvoj analitičke teorije brojeva. Glavni zadatak ovog diplomskog rada je dokaz Dirichletovog teorema koji je pretpostavio Legendre, a dokazao Dirichlet, a on glasi:

Ako su dani pozitivni cijeli brojevi a i q za koje vrijedi $(a, q)=1$, tada postoji beskonačno mnogo prostih brojeva koji su kongrunetni a modulo q.

Prvo poglavlje sadrži kratak životopis Johanna Petera Gustava Lejeunea Dirichleta nakon čega su navedene neko osnovne činjenice iz teorije brojeva kao i iskazi Dirichletovog teorema.

Ključni pojmovi kod dokazivanja su Dirichletovi karakteri i Dirichletove L-funkcije čije su definicije i osnovna svojstva navedeni u drugom poglavlju rada.

Sam dokaz Dirichletovog teorema nalazi se u trećem poglavlju kao i razni pomoćni rezultati koji su potrebni za dokazivanje istog. U četvrtom poglavlju nalaze se još neka svojstva Dirichletovih L-funkcija kao i detaljnije objašnjenje jedne činjenice potrebne u dokazu Dirichletovog teorema.

U ovom diplomskom radu su svi pojmovi precizno definirani, a dokazi tvrdnji su matematički precizno utemeljeni.

Poglavlje 1

Dirichletov teorem

1.1 Johann Peter Gustav Lejeune Dirichlet

Johann Peter Gustav Lejeune Dirichlet rođen je 13. veljače 1805. godine u gradiću Düren koji se danas nalazi u Njemačkoj a u to vrijeme bio je pod Francuskom vlašću. U ranom djetinjstvu razvio je ljubav prema matematici te je tako kao 12-ogodišnjak sav svoj džeparac potrošio na matematičke knjige.

Roditelji su ga upisali u gimnaziju u Bonnu ali nakon dvije godine su odlučili prebaciti ga u židovsku školu u Cologni gdje je imao sreće te ga je podučavao Ohm. U 16-oj godini završio je gimnaziju i odlučio da će studirati u Parizu jer mu standardi i prilike na njemačkim sveučilištima nisu bili zadovoljavajući. Uz sebe je uvijek imao knjigu *Disquisitiones arithmeticae* velikog Gaussa koji mu je bio jedan od najvećih uzora. U Parizu su ga podučavali neki od vodećih matematičara onoga vremena pa je tako došao u kontakt s raznim matematičarima kao što su Legendre, Poisson, Laplace, Biot, Lacroix, Fourier.

Od ljeta 1823. godine Dirichlet je radio za genarala Maximiliena Sebastiana Foya koji je bio jedan od glavnih generala tijekom Napoleonovih ratova.
Njegovo prvo djelo mu je donijelo instant slavu. On je djelomično dokazao Fermatov posljednji teorem za slučaj $n = 5$ kojeg je kasnije dovršio Adrien Marie Legendre. Kasnije je Dirichlet dokazao teorem za slučaj $n = 14$.
28.studenog 1825. godine Foy je umro i Dirichlet je odlučio da se vraća u Njemačku. Tamo je imao nekih problema oko dobivanja priznanja učitelja matematike. Kada se to riješilo počeo je predavati na vojnom sveučilištu.

Godine 1831. oženio se Rebeccom Henriette Mendelssohn Bartholdy koja je bila unuka filozofa Mosesa Mendelssohna i jedna od sestara skladatelja Felixa Mendelssohna Bartholdya. Nakon Gaussove smrti 1855. godine ponuđeno mu je njegovo radno mjesto na sveučilištu u Göttingenu koje je on ubrzo prihvatio.
U ljeto 1858. godine Dirichlet je otišao na konferenciju u švicarski grad Montreux gdje je

pretrpio srčani udar nakon kojeg je bio lošeg zdravstvenog stanja.

Umro je 5.svibnja 1859. godine u Göttingenu. Nakon njegove smrti, Dirichletova predavanja je skupio, priredio i objavio njegov prijatelj Richard Dedekind pod naslovom *Vorlesungen über Zahlentheorie* (Predavanja o teoriji brojeva).

1.2 Iskaz Dirichletovog teorema

Za početak navest ćemo neke osnovne činjenice iz teorije brojeva.

Definicija 1.2.1.
Prirodan broj p, $p > 1$ *zove se prost broj ako nema niti jednog djelitelja d tako da je* $1 < d < p$. *Ako prirodan broj n,* $n > 1$ *nije prost, onda kažemo da je složen.*

Teorem 1.2.2.
Svaki prirodan broj n, $n > 1$ *može se prikazati kao produkt prostih faktora.*

Dokaz.
Broj n je ili prost ili složen.
Za prvi slučaj, kada je n prost, tvrdnja je očita.
Pogledajmo sada drugi slučaj kada je n složen.
Po definiciji postoji d takav da je

$$1 < d < n \quad i \quad d|n.$$

Neka je m najmanji takav djelitelj.
Tada m mora biti prost; inače bi postojao k takav da je

$$1 < k < m \quad i \quad k|m.$$

To bi povlačilo da

$$k|n \quad i \quad 1 < k < m$$

što je u kontradikciji s minimalnošću od m.
Pa pretpostavimo da je m jednak prostom broju p_1. Tada pišemo

$$n = p_1 \cdot r, \quad 1 < r < n.$$

Ponavljamo postupak za r i dobijemo

$$n = p_1 \cdot p_2 \cdot s$$

gdje je

$$p_1 \geq p_2 \quad i \quad 1 \leq s < r < n.$$

Postupak očigledno staje nakon konačno mnogo koraka jer postoji samo konačno mnogo prostih brojeva između 1 i n.
Imamo

$$n = p_1 \cdot ... \cdot p_r, \quad p_1 \leq p_2 \leq ... \leq p_r.$$

Dakle, svaki se prirodan broj može prikazati kao produkt prostih faktora. □

Teoriju kongruencije uveo je u svom djelu *Disquisitiones Arithmeticae* iz 1801. godine Carl Friedrich Gauss. On je također uveo i oznaku za kongruenciju koju i danas rabimo.

Definicija 1.2.3.
Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je a kongruentan b modulo m i pišemo

$$a \equiv b \mod m.$$

U protivnom, kažemo da a nije kongruentan b modulo m i pišemo

$$a \not\equiv b \mod m.$$

Teorem 1.2.4.
Neka je $n \in \mathbb{N}$. Relacija "biti kongruentan modulo n" je relacija ekvivalencije na skupu $\mathbb{N}$

Dokaz.
Trebamo provjeriti refleksivnost, simetričnost i tranzitivnost.
Refleksivnost: Iz $m|0$ slijedi $a \equiv a \mod n$.
Simetričnost: Ako je $a \equiv b \mod n$, onda postoji $k \in \mathbb{Z}$ takav da je $a - b = nk$. Sada je $b - a = n \cdot (-k)$, pa je $b \equiv a \mod n$.
Tranzitivnost: Iz $a \equiv b \mod n$ i $b \equiv c \mod n$ slijedi da postoje $k, l \in \mathbb{Z}$ takvi da je $a - b = nk$ i $c - b = nl$. Zbrajanjem dobivamo $a - c = n(k + l)$ što povlači $a \equiv c \mod n$.
□

Iskažimo sada Dirichletov teorem.

Teorem 1.2.5. ***Dirichletov teorem***
Ako su dani pozitivni cijeli brojevi a i q za koje vrijedi (a, q)=1, tada postoji beskonačno mnogo prostih brojeva koji su kongrunetni a modulo q.
Drugim riječima, svaki od aritmetičkih nizova

$$\{qn + a : n = 0, 1, 2, ...\}, \quad q, a \in \mathbb{N}, \quad (a, q) = 1$$

sadrži neograničeno mnogo prostih brojeva.

Gore navedeni teorem je analogan je Euklidovom teoremu o neograničenosti prostih brojeva. Naš će dokaz zapravo dati jači rezultat, naime rezultat analogan Mertensovoj ocjeni o prostim brojevima u aritmetičkim nizovima.

Teorem 1.2.6. ***Dirichletov teorem, kvantitativna verzija***
Ako su dani pozitivni cijeli brojevi a i q za koje vrijedi (a, q)*=1, imamo*

$$\sum_{\substack{p \leq x \\ p \equiv a \mod q}} \frac{1}{p} = \frac{1}{\phi(q)} \log\log(x) + O_q(1)$$

,
pri čemu je $\phi : \mathbb{N} \to \mathbb{N}$ *Eulerova funkcija koja svakom prirodnom broju u nizu* $1, 2, ..., n$ *pridružuje brojeve koji su relativno prosti s n.*

Primjećujemo da je uvjet $(a, q) = 1$ u Dirichletovu teoremu potreban, budući da ako je $(a, q) = d > 1$, onda je svaki cijeli broj kongruentan s a modulo q djeljiv s d, te stoga može postojati najviše jedan takav prosti broj (tj. d, ako je d prost). Stoga za dani q, svi osim konačno mnogo prostih brojeva spadaju u jednu od grupa ostataka $a \mod q$, s mjerom $(a, q) = 1$.
Prema definiciji Eulerove ϕ funkcije, postoje $\phi(q)$ takvih grupa ostataka, a ako pretpostavimo da su prosti brojevi otprilike ravnomjerno raspodijeljeni među tim grupama ostataka, onda se može očekivati da dana grupa a modulo q, s mjerom $(a, q) = 1$ sadrži omjer $1/\phi(q)$ svih prostih brojeva. Stoga je faktor $1/\phi(q)$ ovdje zaista „korektan“ faktor.
Prirodni pokušaj dokazivanja Dirichletova teorema bio bi pokušati imitirati Euklidov dokaz neograničenosti prostih brojeva kojeg i navodimo.

Teorem 1.2.7. ***Euklidov teorem***
Skup prostih brojeva je beskonačan.

Dokaz.
Neka su $2, 3, ..., p$ svi prosti brojevi do p i pogledajmo

$$q = (2 \cdot 3 \cdot ... \cdot p) + 1.$$

S obzirom da je $q > 1$, ili je sam q prost broj veći od p, ili je djeljiv s prostim brojem koji je veći od p.
U oba slučaja postoji prost broj koji je veći od p.
Dakle, skup prostih brojeva je beskonačan. □

U određenim posebnim slučajevima zaista je moguće na sličan način dokazati Dirichletov teorem.

1.3 Neki jednostavniji slučajevi Dirichletovog teorema

Primjer 1.3.1. *Pokažimo da postoji beskonačno mnogo prostih brojeva koji su kongruentni* 3 *modulo* 4.
Pretpostavimo da postoji samo konačno mnogo prostih brojeva koji su kongruentni $3 \mod 4$*, i neka su to* $p_1, p_2, ...p_n$ *(*p_i *su neparni). Promotrimo broj*

$$N = p_1^2 ... p_n^2 + 2.$$

Budući da je

$$p_i^2 \equiv 3^2 \equiv 1 \mod 4 \quad \forall i,$$

N mora biti kongurentan 3 *modulo* 4.
Budući da je N neparan broj, svi su njegovi prosti faktori neparni brojevi, i time kongurentni ili 1 ili 3 *modulo* 4.
Štoviše, N mora biti djeljiv s najmanje jednim prostim brojem kongruentnim s 3 *modulo* 4*, i stoga s jednim od prostih brojeva* p_i*, jer bi inače N bio umnožak prostih brojeva kongurentnih 1 modulo 4 i time sam kongruentan* 1 *modulo* 4.
No to nije moguće jer bi onda p_i *bio djelitelj i broja N i broja N–*2*, i stoga također* $N–(N–2) = 2$.

Primjer 1.3.2. *Pokažimo da postoji beskonačno mnogo prostih brojeva oblika* $3n + 1$ *i oblika* $3n + 2$
Pokažimo prvo tvrdnju za oblik $3n + 2$*. Pretpostavimo da su* $p_1, ..., p_k$ *svi prosti brojevi kongruenti* 2 *modulo* 3 *i neka je* $x = p_1 p_2 ... p_k$*. Ako je* $x \equiv 1 \mod 3$ *onda je* $x + 1 \equiv 2 \mod 3$*. Dakle, mora postojati prost broj koji je kongruentan* 2 *modulo* 3 *i koji dijeli* $x + 1$*. Ali pošto* $p|p_1 ... p_k$*, p ne može dijeliti* $x + 1$.
Ako je $x \equiv 2 \mod 3$*, tada je* $x + 3 \equiv 2 \mod 3$*. Kao i prije, mora postojati prosti broj* $p \equiv 2 \mod 3$ *koji dijeli* $x + 3$*. Ali pošto* $p|x$*, p ne može dijeliti* $x + 3$.
Te dvije kontradikcije dovode do zaključka da postoji beskonačno mnogo prostih brojeva oblika $3n + 2$.

Da bismo pokazali tvrdnju za oblik $3n + 1$ *moramo koristiti Legendreove simbole i Gaussov kvadratni zakon reciprociteta, koji navodimo bez dokaza.*

Definicija 1.3.3.
Neka je q neparan prost broj i neka je n cijeli broj. Legendreov simbol $\left(\frac{n}{q}\right)$ *je definiran sa:*

$$\left(\frac{n}{q}\right) = \begin{cases} 1 & \text{ako je n kvadratni ostatak modulo } q \\ 0 & \text{ako } \quad q|n \\ -1 & \text{ako je n kvadratni ne-ostatak modulo } q \end{cases}$$

Teorem 1.3.4. ***Gaussov kvadratni zakon reciprociteta***
Ako su p i q različiti neparni prosti brojevi, tada vrijedi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Vratimo se sada primjeru. Razmotrimo neparan broj p,

$$(-3/p) = (-1/p)(3/p).$$

Sada je

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

i

$$(3/p) = (-1)^{\frac{p-1}{2}}(p/3).$$

Prema tome,

$$(-3/p) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}(p/3) = (p/3).$$

Tada direktno imamo

$$(p/3) = \begin{cases} 1 & ako\ je \quad p \equiv 1 \mod 3 \\ -1 & ako\ je \quad p \equiv -1 \mod 3 \end{cases}$$

Dakle, -3 je kvadratni ostatak modulo p samo ako je $p \equiv 1 \mod 3$.
Sada pretpostavimo da postoji samo konačno mnogo prostih brojeva oblika $3n+1$ $(p_1, ..., p_k)$. Neka je $x = 2p_q...p_k$ i neka je p prost djelitelj od $x^2 + 3$. Tada $p \equiv 1 \mod 3$, ali kao i prije p ne može biti jedan od p_i. Stoga zaključujemo da postoji beskonačno mnogo prostih brojeva oblika $3n + 1$.

Na sličan, ali kompliciraniji način, elementarni argumenti mogu biti dani i za određene druge posebne aritmetičke nizove, ali općeniti slučaj Dirichletova teorema ne može se dokazati ovim metodama.

Odlučujući napredak koji je doveo do dokaza Dirichletova teorema u cijeloj njegovoj općenitosti došao je uvođenjem analitičkih metoda. Ključne metode koje je Dirichlet uveo i koje su sada nazvane prema njemu su Dirichletovi karakteri i Dirichletove *L*-funkcije. Dirichletovi karakteri su izvjesne aritmetičke funkcije dok su Dirichletove *L*-funkcije redovi povezani s Dirichletovim karakterima. Analitička svojstva tih Dirichletovih redova, a posebice mjesto njihovih nultočaka, igraju ključnu ulogu u argumentu. Zapravo najteži dio dokaza sastoji se u dokazivanju da točka $s = 1$ nije nula za Dirichletovu *L*-funkciju.

Poglavlje 2

Dirichletovi karakteri i L-funkcija

2.1 Dirichletovi karakteri

Jedna od ključnih stvari koje je Dirichlet uveo su Dirichletovi karakteri. Da bi što jasnije shvatili pojam Dirichletovog karaktera, prisjetimo se definicije aritmetičke funkcije.

Definicija 2.1.1.
Aritmetička funkcija je funkcija koja je definirana na prirodnim brojevima s vrijednostima u skupu realnih ili kompleksnih brojeva. Za aritmetičku funkciju f kažemo da je multiplikativna ako je $f(1) = 1$ te $f(mn) = f(m)f(n)$ za $(m, n) = 1$.
Ako je $f(mn) = f(m)f(n) \quad \forall m, n \in \mathbb{N}$, onda kažemo da je funkcija potpuno multiplikativna.

Osnovna definicija karaktera je sljedeća:

Definicija 2.1.2.
Neka je q pozitivan cijeli broj. Dirichletov karakter modulo q je aritmetička funkcija χ sa sljedećim svojstvima:

1. *χ je periodičan modulo q, t.j. $\chi(n + q) = \chi(n) \quad \forall n \in \mathbb{N}$.*
2. *χ je potpuno multiplikativan, t.j. $\chi(nm) = \chi(n)\chi(m) \quad \forall n, m \in \mathbb{N} \quad i \quad \chi(1) = 1$.*
3. *$\chi(n) \neq 0$ ako i samo ako je $(n, q) = 1$.*

Primjer 2.1.3.
Aritmetička funkcija $\chi_0 = \chi_{0,q}$ definirana s

$$\chi_0(n) = \begin{cases} 1 & \text{ako je } (n,q)=1; \\ 0 & \text{inače} \end{cases}$$

je karakteristična funkcija cijelih brojeva uzajamno prostih s q i naziva se glavni karakter modulo q, a da je glavni karakter χ_0 zapravo Dirichletov karakter može se vidjeti iz sljedećeg;
uvjet 1. *proizlazi iz relacije* $(n, q) = (n + q, q)$,
uvjet 2. *proizlazi iz činjenice da* $(nm, q) = 1$ *vrijedi ako i samo ako je* $(n, q) = 1$ *i* $(m, q) = 1$,
uvjet 3. *vrijedi po definiciji* χ_0.
Oznaka χ_0 postala je standardna oznaka za glavni karakter. Moramo imati na umu da χ_0 ovisi o q, iako to nije izričito navedeno u standardnoj oznaci.
Analogno grupi ostataka oznake $a \mod q$, *oznaka* $\chi \mod q$ *upotrebljava se kako bismo ukazali na to da je χ Dirichletov karakter modulo q.*

Primjeri karaktera

Primjer 2.1.4. ***Karakteri modulo 1***
Konstantna funkcija 1 *očito zadovoljava uvjete prije navedene definicije s* $q = 1$.
Štoviše, budući da svaki karakter modulo 1 *mora biti periodičan modulo* 1 *i mora biti jednak* 1 *na* 1, $\chi \equiv 1$ *jedini je Dirichletov karakter modulo* 1.
Napominjemo da je taj karakter glavni karakter modulo 1.

Primjer 2.1.5. ***Karakteri modulo 2***
Uvjet 3 povlači da svaki karakter modulo 2 *mora biti* 0 *na parnim cijelim brojevima, a uvjet periodičnosti zajedno sa zahtjevom* $\chi(1) = 1$ *povlači da* $\chi(n)$ *mora biti jednak 1 za neparne cijele brojeve n.*
Stoga, kao i u slučaju $q = 1$ *postoji samo jedan karakter modulo* 2, *naime glavni karakter χ_0 definiran sa*

$$\chi_0(n) = \begin{cases} 1 & \textit{ako je } (n,2)=1; \\ 0 & \textit{inače} \end{cases}$$

Primjer 2.1.6. ***Karakteri modulo*** 3
Opet imamo glavni karakter $\chi_0(n)$, koji je definiran sa

$$\chi_0(n) = \begin{cases} 1 & \textit{ako je } (n,3)=1; \\ 0 & \textit{inače} \end{cases}$$

Pokazat ćemo da postoji točno jedan drugi karakter modulo 3.
Pretpostavimo da je χ karakter modulo 3.
Tada svojstva 1. *do* 3. *znače da je*

$$\chi(1) = 1, \quad \chi(3) = 0$$

i

$$\chi(2)^2 = \chi(4) = \chi(1) = 1,$$

tako da je $\chi(2) = \pm 1$.
Ako je $\chi(2) = 1$*, tada je* χ *jednako* χ_0 *budući da su obje funkcije periodične modulo 3 i imaju iste vrijednosti u* $n = 1, 2, 3$.
Ako je $\chi(2) = -1$*, tada je* $\chi = \chi_1$ *gdje je* χ_1 *jedinstvena periodična funkcija modulo* 3 *definirana sa*

$$\chi_1(1) = 1, \quad \chi_1(2) = -1$$

i

$$\chi_1(3) = 0$$

Jasno je da χ_1 *zadovoljava svojstva* 1. *i* 3. *Potpuna multiplikativnost nije odmah očigledna, ali može se pokazati na sljedeći način.*
Definirajmo mulitplikativnu funkciju f*: Neka je* $f(3) = 0$ *i neka je za prost broj* p

$$f(p) = -1 \quad \textit{ako je} \quad p \equiv -1 \mod 3$$

i

$$f(p) = 1 \quad \textit{ako je} \quad p \equiv 1 \mod 3.$$

Za složene brojeve n*,* $f(n)$ *definiramo po multiplikativnosti: ako je*

$$n = p_1^{r_1} \dots p_k^{r_k},$$

stavimo

$$f(n) = f(p_1)^{r_1} \dots f(p_k)^{r_k}.$$

Tada je

$$f(n) = \chi_1(n) \quad \textit{za} \quad n = 1, 2, 3,$$

tako da je za dokazivanje da je $f = \chi_1$ *(i stoga da je* χ_1 *potpuno multiplikativna) dovoljno pokazati da je* f *periodična s periodom* 3.
Dakle, primijetimo da ako je $n \equiv 0 \mod 3$*, tada je* $f(n) = 0$*. Inače je* $n \equiv \pm 1 \mod 3$*, a u tom slučaju* n *možemo pisati kao*

$$n = \prod_{i \in I} p_i \prod_{j \in J} p_j$$

gdje su produkti od $i \in I$ *i* $j \in J$ *konačni (eventualno prazni), a prosti brojevi* $p_i, i \in I$ *i* p_j*,* $j \in J$ *kongruentni* 1*, odnosno* -1*, modulo* 3*. Tada imamo*

$$f(n) = \prod_{i \in I} f(p_i) \prod_{j \in J} f(p_j) = (-1)^{|J|}.$$

S druge strane, budući da je

$$p_i \equiv 1 \mod 3$$

i

$$p_j \equiv -1 \mod 3,$$

imamo

$$n \equiv (-1)^{|J|} \mod 3.$$

Stoga, ako je $|J|$ paran broj, tada je

$$n \equiv 1 \mod 3$$

i

$$f(n) = 1 = f(1),$$

a ako je $|J|$ neparan broj, tada je

$$n \equiv 2 \mod 3$$

i

$$f(n) = -1 = f(2).$$

Dakle je f periodična s periodom 3, kao što smo htjeli pokazati.

Primjer 2.1.7. ***Legendreovi simboli kao karakteri***
Neka je q neparan prosti broj, a neka $\chi(n) = (\frac{n}{q})$ označava Legendreov simbol modulo q definiran kao u (1.3.3). Tada je $\chi(n)$ karakter modulo q.
Zaista, svojstva 1. (periodičnost) i 3. (uzajamno prosti brojevi) proizlaze izravno iz definicije Legendreova simbola, dok 2. (popuna multiplikativnost) slijedi iz $\left(\frac{nm}{q}\right) = \left(\frac{n}{q}\right)\left(\frac{m}{q}\right)$, što je poznat rezultat iz elementarne teorije brojeva.
Karakter χ, koji je na ovaj način proizašao iz Legendreova simbola, uzima samo vrijednosti $0, \pm 1$ i stoga ispunjava uvjet $\chi^2 = \chi_0$, ali $\chi \neq \chi_0$. Karakteri sa zadnje navedena dva svojstva nazivaju se kvadratni karakteri. Napominjemo da karakter koji uzima samo realne vrijednosti (takav se karakter naziva realnim karakterom) nužno sve svoje vrijednosti ima u $\{0, \pm 1\}$, što ćemo vidjeti u sljedećem teoremu, pa je tako ili glavni karakter ili kvadratni karakter.

Da bismo si što jasnije mogli predočiti Dirichletove karaktere, sada ćemo iz definicije karaktera izvesti određene jednostavne posljedice.

Teorem 2.1.8. ***Elementarna svojstva Dirichletovih karaktera***
Neka je q pozitivan cijeli broj.

(i) Vrijednosti Dirichletova karaktera χ modulo q su ili 0 ili $\phi(q)$-ti korijeni jedinice, tj. za svaki n imamo ili $\chi(n) = 0$ ili $\chi(n) = e^{2\pi i v/\phi(q)}$ za neki $v \in \mathbb{N}$.

(ii) Karakteri modulo q čine grupu s obzirom na množenje po točkama koje je definirano sa

$$(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n).$$

Glavni karakter χ_0 je neutralni element ove grupe, a inverz od karaktera χ dan je karakterom $\overline{\chi}$ koji je definiran kao $\overline{\chi}(n) = \overline{\chi(n)}$.

Dokaz.

(i) Ako je $\chi(n) \neq 0$, onda je $(n, q) = 1$.
Iz Eulerove generalizacije Fermatovog malog teorema tada imamo

$$n^{\phi(q)} \equiv 1 \mod q.$$

Prema potpunoj multiplikativnosti i periodičnosti karaktera χ to implicira da je

$$\chi(n)^{\phi(q)} = \chi(n^{\phi(q)}) = \chi(1) = 1,$$

kao što se i tvrdilo.

(ii) Svojstva grupe proizlaze izravno iz definicije karaktera pri čemu je

$$\chi(n)^{-1} = \overline{\chi(n)}.$$

□

Da bismo izveli daljnje informacije o svojstvima grupe karaktera potreban nam je dobro poznati rezultat iz algebre koji ovdje navodimo bez dokaza.

Lema 2.1.9. ***Osnovni teorem za konačne Abelove grupe***
Svaka konačna Abelova grupa direktni je produkt cikličkih grupa. To jest, za svaku konačnu Abelovu grupu G postoje elementi $g_1, ..., g_r \in G$ pripadajućih redova $h_1, ..., h_r$ tako da svaki element $g \in G$ ima jedinstveni prikaz

$$g = \prod_{k=1}^{r} g_k^{v_k} \quad s \quad 0 \leq v_k < h_k.$$

Štoviše, imamo

$$\prod_{k=1}^{r} h_k = |G| .$$

Ako specijaliziramo grupu G iz prethodne Leme kao multiplikativnu grupu $(\mathbb{Z}/q\mathbb{Z})$ grupe ostataka modulo q, rezultat postaje:

Lema 2.1.10. ***Osnovni teorem za grupe ostataka modulo*** q
Neka je q pozitivan cijeli broj. Tada postoje pozitivni cijeli brojevi $g_1, ..., g_r$*, svi relativno prosti s q i pripadajućih redova* $h_1, ..., h_r$ *modulo q (tj.* h_k *je najmanji pozitivan cijeli broj h, tako da je* $g_k^h \equiv 1 \mod q$*), sa sljedećim svojstvom:*
Za svaki cijeli broj n za koji vrijedi $(n, q) = 1$ *postoje jedinstveni cijeli brojevi* v_k
sa $0 \leq v_k < h_k$*, takvi da je*

$$n \equiv \prod_{k=1}^{r} g_k^{v_k} \mod q.$$

Štoviše, imamo

$$\prod_{k=1}^{r} h_k = \phi(q).$$

Primjeri

Primjer 2.1.11.
Ako je $q = p^m$ *potencija prostog broja, pri čemu je p neparan prosti broj, tada kao rezultat elementarne teorije brojeva postoji primitivni korijen g modulo* p^m *, tj. element g koji generira multiplikativnu grupu modulo* p^m*. Dakle, ta je grupa sama po sebi ciklička, a osnovni teorem je važeći za* $r = 1$ *i* $g_1 = g$*. (Situacija je malo kompliciranija za potencije broja 2, budući da odgovarajuće grupe ostataka općenito nisu cikličke.)*

Primjer 2.1.12.
Neka je $q = 15 = 3 \cdot 5$*. Tvrdimo da je* $(g_1, g_2) = (2, 11)$ *baza. Jednostavno je provjeriti da su redovi od* g_1 *i od* g_2 *jednaki* $h_1 = 4$ *i* $h_2 = 2$*.*
Također napominjemo da je

$$h_1 h_2 = 4 \cdot 2 = \phi(5)\phi(3) = \phi(15),$$

u skladu s teoremom. Jednostavna provjera od slučaja do slučaja tada pokazuje da klase kongruentnosti

$$2^{v_1} 11^{v_2} \quad sa \quad 0 \leq v_1 < 4 \quad i \quad 0 \leq v_2 < 2$$

svaku klasu ostataka a $\mod q$*, pri čemu je* $(a, 15) = 1$*, obuhvaćaju točno jednom.*

Glavna primjena Leme (2.1.10) dana je u sljedećoj lemi.

Lema 2.1.13. ***Broj karaktera modulo*** q
Neka je q pozitivan cijeli broj. Tada postoji točno $\phi(q)$ *Dirichletovih karaktera modulo q. Štoviše, za svaki cijeli broj a za koji vrijedi* $(a, q) = 1$ *i* $a \not\equiv 1 \mod q$ *postoji karakter* χ *sa* $\chi(a) \neq 1$*.*

Dokaz.
Neka su $q_1, ...q_r$ i $h_1, ...h_r$ definirani kao u Lemi (2.1.10) i neka je $\omega_j = e^{2\pi\, i\, /h_j}$.
Stoga su $\omega_j^v, \quad v = 0, 1, ..., h_j - 1$ različiti h_j-ti korijeni jedinice.
Tvrdimo da postoji podudaranje jedan na jedan između r-torki

$$v = (v_1, ..., v_r) \quad 0 \leq \ v_k < h_k$$

i karaktera modulo q.
Kako bismo to pokazali prvo pretpostavimo da je χ karakter modulo q.
Tada je $\chi(n) = 0$ za $(n, q) > 1$, prema definiciji karaktera.
S druge strane, ako je $(n, q) = 1$ tada prema Lemi (2.1.10) imamo

$$n \equiv \prod_{k=1}^{r} g_k^{\mu_k} \mod q$$

za neku jedinstvenu r-torku $\mu = (\mu_1, ..., \mu_r)$ za koju vrijedi $0 \leq \mu_k < h_k$.
Svojstva perodičnosti i potpune multiplikativnosti tada impliciraju

$$\chi(n) = \chi\left(\prod_{k=1}^{r} g_k^{\mu_k}\right) = \prod_{k=1}^{r} \chi(g_k)^{\mu_k} \tag{2.1}$$

Premo tome, χ je jedinstveno određen svojim vrijednostima na generatorima g_k. Štoviše, budući da je g_k reda h_k imamo

$$\chi(g_k)^{h_k} = \chi(g_k^{h_k}) = \chi(1) = 1$$

Dakle, $\chi(g_k)$ mora biti h_k-ti korijen jedinice, pa imamo

$$\chi(g_k) = \omega_k^{v_k} \ (k = 1, ..., r), \tag{2.2}$$

za jedinstvenu r-torku $v = (v_1, ...v_r)$ takvu da je $0 \leq \ v_k < h_k$.
Prema tome, svaki karakter χ modulo q daje jedinstvenu r-torku v gore navedenog oblika.
Obratno, ako imamo r-torku v tog oblika, definiramo aritmetičku funkciju $\chi = \chi_v$ sa

$$\chi(n) = \begin{cases} 0 & \text{ako je} \quad (n, q) > 1 \\ \prod_{k=1}^{r} (\omega_k^{v_k})^{\mu_k} & \text{ako je} \quad n \equiv \prod_{k=1}^{r} g_k^{\mu_k} \mod q \end{cases}$$

Prema tome, χ je Dirichletov karakter modulo q.
Dakle, pokazali smo da postoji podudaranje karaktera modulo q i r-torki v oblika
$v = (v_1, ..., v_r)$ sa $0 \leq \ v_k < h_k$. Budući da je prema Lemi (2.1.10) broj takvih r-torki v jednak $h_1...h_r = \phi(q)$, proizlazi da postoji $\phi(q)$ karaktera modulo q. To dokazuje prvi dio Leme (4.1.2).

Dokažimo sada i drugi dio.
Neka je zadan cijeli broj a takav da je $(a, q) = 1$ i $a \not\equiv 1 \mod q$. Prema Lemi (2.1.10) imamo

$$a \equiv \prod_{k=1}^{r} g_k^{\mu_k} \mod q$$

s odgovarajućim eksponentima μ_k, $0 \leq \mu_k < h_k$.
Budući da je $a \not\equiv 1 \mod q$, najmanje jedan od eksponenata mora biti različit od 0.
Bez smanjenja općenitosti pretpostavimo da je $\mu_1 \neq 0$. Definirajmo karakter χ sa $\chi(g_1) = \omega_1$ i $\chi(g_k) = 1$ za $k = 2, ..., r$. Tada je

$$\chi(a) = \chi(g_k^{\mu_1}) = \chi(g_k)^{\mu_1} = \exp\left\{\frac{2\pi i \mu_1}{h_1}\right\} \neq 1$$

budući da je $0 < \mu_1 < h_1$. □

Glavni rezultat ovog poglavlja dan je u sljedećem teoremu.

Teorem 2.1.14. ***Relacija ortogonalnosti za Dirichletove karaktere***
Neka je q pozitivan cijeli broj.

(i) Za bilo koji Dirichletov karakter χ modulo q imamo

$$\sum_{a=1}^{q} \chi(a) = \begin{cases} \phi(q) & \text{ako je } \chi = \chi_0; \\ 0 & \text{inače} \end{cases}$$

gdje je χ_0 glavni karakter modulo q.

(ii) Za bilo koji broj $a \in \mathbb{N}$ imamo

$$\sum_{\chi \bmod q} \chi(a) = \begin{cases} \phi(q) & \text{ako je } a \equiv 1 \mod q \\ 0 & \text{inače} \end{cases}$$

gdje suma obuhvaća sve Dirichletove karaktere modulo q.

(iii) Za bilo koje Dirichletove karaktere χ_1, χ_2 modulo q imamo

$$\sum_{a=1}^{q} \chi_1(a)\overline{\chi_2(a)} = \begin{cases} \phi(q) & \text{ako je } \chi_1 = \chi_2; \\ 0 & \text{inače} \end{cases}$$

(iv) Za bilo koje brojeve $a_1, a_2 \in \mathbb{N}$ imamo

$$\sum_{\chi \bmod q} \chi(a_1)\overline{\chi(a_2)} = \begin{cases} \phi(q) & \text{ako je } a_1 \equiv a_2 \mod q \quad i \quad (a_1, q) = 1; \\ 0 & \text{inače} \end{cases}$$

gdje suma obuhvaća sve Dirichletove karaktere modulo q.

Dokaz.

(i) Sumu na lijevoj strani označimo sa S.
Ako je $\chi = \chi_0$, tada je $\chi(a) = 1$ ako je $(a, q) = 1$,a inače je $\chi(a) = 0$, tako da je $S = \phi(q)$.
Pretpostavimo sada da je $\chi \neq \chi_0$.
Tada postoji broj a_1 za koji vrijedi $(a_1, q) = 1$ tako da je $\chi(a_1) \neq 1$. Napominjemo da, budući da je $\chi(a) = 0$ ako je $(a, q) > 1$ zbroj pod (i) može biti restringiran na
$(a, q) = 1, 1 \leq a \leq q$.
Također napominjem da ako a zadovoljava te uvjete onda ih zadovoljava i $b = aa_1$ nakon reduciranja modulo q.
Stoga

$$\chi(a_1)S = \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \chi(a_1)\chi(a) = \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \chi(a_1a) = \sum_{\substack{1\leq b\leq q\\(b,q)=1}} \chi(b) = S.$$

Budući da je $\chi(a_1) \neq 1$, to implicira da je $S = 0$. Time smo dokazali (i) dio.

(ii) Neka S označava sumu na lijevoj strani.
Ako je $(a, q) > 1$, tada su svi članovi u ovom zbroju jednaki 0, dakle $S = 0$.
Ako je $(a, q) = 1$ i $a \equiv 1 \mod q$, tada je $\chi(a) = \chi(1) = 1$ za sve karaktere χ modulo q, a budući da prema Lemi (4.1.2) postoji točno $\phi(q)$ takvih karaktera, u ovom slučaju imamo $S = \phi(q)$.
Sada pretpostavimo da je $(a, q) = 1$ i $a \equiv 1 \mod q$. Prema Lemi 2.1.10. postoji karakter χ_1 modulo q za koji vrijedi $\chi_1(a) \neq 1$. Budući da karakteri modulo q čine grupu, ako χ prolazi kroz sve karaktere modulo q, to čini i $\chi_1\chi$. Stoga imamo

$$\chi_1(a)S = \sum_{\chi \bmod q} \chi_1(a)\chi(a) = \sum_{\chi \bmod q} (\chi_1\chi)(a) = \sum_{\psi \bmod q} \psi(a) = S$$

gdje zadnja suma obuhvaća sve karaktere ψ modulo q.
Budući da je $\chi_1(a) \neq 1$, to implicira da je $S = 0$ kao što smo i htjeli pokazati.

(iii) Ovaj dio proizlazi iz (i) s karakterom $\chi = \chi_1\overline{\chi_2}$ i ako uzmemo u obzir da je $\chi = \chi_0$ ako i samo ako je $\chi_1 = \chi_2$.

(iv) Možemo pretpostaviti da je $(a_1, q) = (a_2, q) = 1$ budući da je suma inače 0, a rezultat je trivijalno istinit. Stoga a_2 ima multiplikativni inverz $\overline{a_2}$ modulo q. Ako primijenimo (ii) za $a = a_1\overline{a_2}$ primjećujemo da je

$$\chi(a_2)\chi(a) = \chi(a_2a) = \chi(a_2a_1\overline{a_2}) = \chi(a_1)$$

i stoga

$$\chi(a) = \frac{\chi(a_1)}{\chi(a_2)} = \chi(a_1)\overline{\chi(a_2)}.$$

Također $a = a_1\overline{a_2} \equiv 1 \mod q$ ako i samo ako je $a_1 \equiv a_2 \mod q$, te dobivamo željenu relaciju. □

Nama je najvažniji zadnji dio Teorema (2.1.14). Taj nam identitet dozvoljava da iz sume izdvojimo izraze koji zadovoljavaju danu kongruentnost. Primijenit ćemo ga za a_2, fiksirane klase kongruentnosti $a \mod q$ i za a_1 koji prolazi kroz sve proste brojeve p kako bismo izdvojili one proste brojeve koji pripadaju klasi kongruentnost $a \mod q$. Taj identitet, sam, često se naziva relacijom ortogonalnosti za Dirichletove karaktere.

Sljedeći korolar je posjedica (i) dijela prethodnog teorema.

Korolar 2.1.15.
Neka je q pozitivan cijeli broj i χ karakter modulo q.

(i) Ako χ nije glavni karakter χ_0 modulo q, tada

$$\left|\sum_{n\leq x}\chi(n)\right| \leq \phi(q) \quad (x \geq 1)$$

(ii) Ako je $\chi = \chi_0$, tada

$$\left|\sum_{n\leq x}\chi(n) - \frac{\phi(q)}{q}x\right| \leq 2\phi(q) \quad (x \geq 1)$$

Dokaz. Budući da je χ periodičan modulo q, imamo, za bilo koji $x \geq 1$

$$\sum_{n\leq x}\chi(n) = [x/q]S + R$$

gdje su

$$S = \sum_{a=1}^{q}\chi(a) \quad i \quad |R| \leq \sum_{a=1}^{q}|\chi(n)|$$

Jasno je da je $|R| \leq \phi(q)$, a prema (i) dijelu Teorema (2.1.14) imamo $S = 0$ ako je $\chi \neq \chi_0$, i $S = \phi(q)$ ako je $\chi = \chi_0$. □

2.2 Dirichletova L-funkcija

Druga jako bitna stvar uz Dirichletove karaktere koju je Dirichlet uveo su takozvane Dirichletove L-funkcije.

Definicija 2.2.1.
Neka je zadan Dirichletov karakter χ. Funkcija

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s} \tag{2.3}$$

se naziva Dirichletovom L-funkcijom ili Dirichletovim L-redom.

Analitičko ponašanje Dirichletovih L-funkcija ima ključnu ulogu u dokazivanju Dirichletovog teorema. Sljedeći teorem obuhvaća glavna analitička svojstva L-funkcija koja će nam biti potrebna za dokazivanje Dirichletova teorema. Ključno svojstvo o kojem ovisi uspješnost argumenta je zadnje, koje potvrđuje da L-funkcije nisu 0 u točki $s = 1$.

Teorem 2.2.2. ***Analitička svojstva L-funkcija***
Neka je χ Dirichletov karakter modulo q, i neka $L(s,\chi)$ predstavlja Dirichletovu L-funkciju.

(i) Ako je $\chi \neq \chi_0$ gdje je χ_0 glavni karakter modulo q, tada je funkcija $L(s,\chi)$ analitička u poluravnini $\sigma > 0$, pri čemu je σ realni dio od s ($\sigma = Res$).

(ii) Ako je $\chi = \chi_0$, tada funkcija $L(s,\chi)$ ima jednostavan pol u $s = 1$ s reziduumom $\phi(q)/q$ te je analitička u svim drugim točkama poluravnine $\sigma > 0$.

(iii) Ako je $\chi \neq \chi_0$, tada je $L(1,\chi) \neq 0$.

Dokaz.
Sada ćemo dokazati prvi i drugi dio teorema, dok ćemo zadnji dio dokazati u četvrtom poglavlju.
Ako je $\chi \neq \chi_0$, tada su prema Korolaru (2.1.15) parcijalne sume $\sum_{n\leq x} f(n)n^{-s}$ ograničene, tako da Dirichletov red

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

konvergira u poluravnini $\sigma > 0$ te je stoga funkcija $F(s)$ u toj poluravnini analitička.
S druge strane, ako napišemo

$$\chi_0(n) = f(n) + \phi(q)/q$$

vidimo da je

$$L(s,\chi_0) = F(s) + (\phi(q)/q)\zeta(s) \quad za \quad \sigma > 1,$$

pri čemu je $\zeta(s)$ Riemanova zeta funkcija:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Budući da je $F(s)$ analitička u poluravnini $\sigma > 0$ i $\zeta(s)$ analitička u poluravnini $\sigma > 0$ uz iznimku pola u $s = 1$ s reziduumom 1, zaključujemo da je $L(s,\chi_0)$ analitička u poluravnini $\sigma > 0$ uz iznimku pola u $s = 1$ s reziduumom $\phi(q)/q$ □

Poglavlje 3

Dokaz Dirichletovog teorema

3.1 Dokaz

Ovdje ćemo dokazati Dirichletov teorem u kvantitativnoj verziji danoj u Teoremu (1.2.6), modulo rezultat o neiščezavanju za $L(1,\chi)$ naveden u dijelu (*iii*) Teorema (2.2.2) koji će biti kasnije dokazan.
Fiksirajmo pozitivne cijele brojeve a i q takve da je $(a,q) = 1$ i definirajmo funkcije

$$S_{a,q}(x) = \sum_{\substack{p \le x \\ p \equiv a \mod q}} \frac{1}{p} \quad (x \ge 2)$$

$$F_{a,q}(s) = \sum_{\substack{p \\ p \equiv a \mod q}} \frac{1}{p^s} \quad (\sigma > 1)$$

$$F_{\chi}(s) = \sum_{p} \frac{\chi(p)}{p^s} \quad (\sigma > 1).$$

Napominjemo da su redovi koji definiraju Dirichletove funkcije $F_{a,q}(s)$ i $F_{\chi}(s)$ apsolutno konvergentni u poluravnini $\sigma > 1$. Te funkcije ćemo koristiti samo u toj poluravnini.
U gore navedenim oznakama ocjena Teorema (1.2.6) poprima oblik

$$S_{a,q}(x) = \frac{1}{\phi(q)} \log\log x + O_q(1) \quad (x \ge 3). \tag{3.1}$$

Tu ocjenu utvrdit ćemo nizom koraka koji pak reduciraju ocjenu $S_{a,q}(x)$ na funkcije $F_{a,q}(s)$, $F_{\chi}(s)$, $L(s,\chi)$ i konačno na rezultat o neiščezavanju $L(1,\chi)$ za $\chi \neq \chi_0$.
Kako bismo smanjili oznake, nećemo izričito navesti ovisnost pogreške relacije o q. Napominjemo, da u daljnjem dokazu, sve O-konstante smiju ovisiti o q.

Redukcija na $F_{a,q}(s)$
Za početak ćemo, bez dokaza, navesti Mertensovu i Chebyshevljevu ocjenu koje su koriste u ovom dijelu. Mertensov teorem je skup klasičnih ocjena koje se odnose na distribuciju prostih brostih brojeva.

Teorem 3.1.1. ***Mertensov teorem***
Ako $x \to \infty$, imamo

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

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

Teorem 3.1.2. ***Chebyshevljeva ocjena***
Postoje pozitivne konstatnte A_1 i A_2 takve da je

$$A_1 \frac{x}{\log x} < \pi(x) < A_2 \frac{x}{\log x}$$

za svaki $x \ge 2$. Pri tome je $\pi(x)$ funcija prostih brojeva koja označava broj prostih brojeva p takvih da je $p \le x$, $x \in [2, \infty\rangle$.

Prvo ćemo pokazati da (3.1) proizlazi iz

$$F_{a,q}(\sigma) = \frac{1}{\phi(q)} \log \frac{1}{\sigma - 1} + O(1) \quad (\sigma > 1). \tag{3.2}$$

Neka je $x \ge 3$ i uzmimo da je $\sigma = \sigma_x = 1 + \frac{1}{\log x}$ u (3.2). Tada je glavni član s desne strane (3.2) jednak glavnom članu s desne strane u (3.1) i pogreška relacije u (3.2) ima željeni red, $O(1)$. Stoga je dovoljno pokazati da se lijeve strane tih relacija, tj $S_{a,q}(x)$ i $F_{a,q}(\sigma_x)$, razlikuju najviše za $O(1)$.
Kako bismo to pokazali uzmimo

$$S_{a,q}(x) - F_{a,q}(\sigma_x) = \sum_{\substack{p \le x \\ p \equiv a \mod q}} \frac{1 - p^{1-\sigma_x}}{p} - \sum_{\substack{p > x \\ p \equiv a \mod q}} \frac{1}{p^{\sigma_x}} = \sum\nolimits_1 - \sum\nolimits_2. \tag{3.3}$$

Budući da je

$$1 - p^{1-\sigma_x} = 1 - \exp\left\{-\frac{\log p}{\log x}\right\} << \frac{\log p}{p} \quad (p \le x)$$

imamo

$$\sum\nolimits_1 << \frac{1}{\log x} \sum_{p \le x} \frac{\log p}{p} << 1$$

prema Mertensovoj ocjeni (3.1.1).
Štoviše, parcijalnom sumom i prema Chebyshevljevoj ocjeni (3.1.2) dobivamo

$$\begin{aligned}\sum_{2} \leq \sum_{p>x} \frac{1}{p^{\sigma_x}} &= -\frac{\pi(x)}{x^{\sigma_x}} + \sigma_x \int_x^{\infty} \frac{\pi(u)}{u^{\sigma_x+1}} du \\ &<< \frac{1}{\log x} + \int_x^{\infty} \frac{1}{u^{\sigma_x} \log u} du \\ &\leq \frac{1}{\log x} + \frac{x^{1-\sigma_x}}{(\sigma_x - 1)(log x)} << 1.\end{aligned}$$

Stoga su oba člana s desne strane (3.3) reda $O(1)$ što smo htjeli i pokazati.

Redukcija na $F_\chi(s)$
Neka je $\sigma > 1$ tako da su fukcije $F_{a,q}(\sigma)$ i $F_\chi(\sigma)$ apsolutno konvergentne. Prema relaciji ortogonalnosti za karaktere ((*iv*) dio Teorema (2.1.14)) imamo

$$\begin{aligned}F_{a,q}(\sigma) &= \sum_p \frac{1}{p^\sigma} \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \chi(p) \\ &= \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^\sigma} \\ &= \frac{1}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} F_\chi(\sigma).\end{aligned} \tag{3.4}$$

Redukcija na Dirichletovu L-funkciju
Budući da je Dirichletov karakter potpuno multiplikativan i ima apsolutnu vrijednost najviše 1, pripadna L-funkcija $L(s,\chi)$ ima oblik Eulerova produkta u poluravnini $\sigma > 1$ i dana je s

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Ako uzmemo logaritme na obje strane (koristeći glavnu granu logaritma) dobijemo za $\sigma > 1$

$$\begin{aligned}\log L(s,\chi) &= -\sum_p \log\left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_p \sum_{m=1}^{\infty} \frac{\chi(p)^m}{m p^{ms}} \\ &= F_\chi(s) + R_\chi(s),\end{aligned} \tag{3.5}$$

gdje je

$$F_\chi(s) = \sum_p \chi(p)p^{-s}$$

a

$$R_\chi(s) = \sum_{m=1}^{\infty} \frac{\chi(p)^{m-1}}{mp^m}$$

pa imamo

$$\begin{aligned} |R_\chi(s)| &\leq \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}} \\ &\leq \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^m} \\ &<< \sum_p \frac{1}{p^2} < \infty. \end{aligned} \tag{3.6}$$

Prema tome imamo

$$F_\chi(s) = \log L(s,\chi) + O(1) \quad (\sigma > 1). \tag{3.7}$$

Doprinos glavnog karaktera

Ako je $\chi = \chi_0$, tada prema dijelu (*ii*) Teorema (2.2.2), $L(s,\chi_0)$ ima pol s reziduumom $\frac{\phi(q)}{q}$ u $s = 1$ te je analitička drugdje u poluravnini $\sigma > 0$.
Prema tome, za $\sigma > 0$ imamo

$$L(s,\chi_0) = \frac{\phi(q)}{q}\frac{1}{\sigma - 1} + H(s)$$

gdje je $H(s) = H_{\chi_0(s)}$ analitička funkcija u $\sigma > 0$. $H(s)$ je posebno ograničen na bilo kojem kompaktnom skupu sadržanom u toj poluravnini te stoga zadovoljava

$$|H(\sigma)| \leq \frac{\phi(q)}{2q(\sigma - 1} \quad (1 < \sigma < \sigma_0), \tag{3.8}$$

gdje je σ_0 odgovarajuća konstanta koja ovisi o q.
Prema tome

$$\begin{aligned} \log L(\sigma,\chi_0) &= \log(\frac{\phi(q)/q}{\sigma - 1}(1 + H(\sigma)(\sigma - 1)\frac{q}{\phi(q}})) \\ &= \log(\phi(q)/q) + \log\frac{1}{\sigma - 1} + \log(1 + H(\sigma)(\sigma - 1)\frac{q}{\phi(q)}) \\ &= \log\frac{1}{\sigma - 1} + O(1) \quad (1 < \sigma \leq \sigma_0) \end{aligned} \tag{3.9}$$

gdje smo u zadnjem koraku upotrijebili (3.8). Prema (3.7) slijedi

$$F_{\chi_0} = log\frac{1}{\sigma - 1} + O(1) \tag{3.10}$$

u početku samo u intervalu $1 < \sigma \leq \sigma_0$, ali s obzirom na trivijalno ograničenje

$$|F_{\chi_0}| \leq \sum_p \frac{1}{p^\sigma} \leq \sum_p \frac{1}{p^{\sigma_0}} < \infty \quad (\sigma > \sigma_0)$$

u punom rasponu $\sigma > 1$.

Doprinos ne-glavnih karaktera
Ako je $\chi \neq \chi_0$, tada je prema (*i*) dijelu Teorema (2.2.2) $L(s,\chi)$ analitička u poluravnini $\sigma > 0$ te je stoga neprekidna u $a = 1$. Štoviše, prema zadnjem dijelu tog rezultata, $L(1,\chi) \neq 0$. Stoga je $\log L(s,\chi)$ analitička i neprekidna u okolini $s = 1$.
Naime, postoji $\sigma_0 > 1$ takav da je $\log L(s,\chi)$ ograničen na $1 < \sigma \leq \sigma_0$.
S obzirom na to (3.7) implicira

$$F_\chi(\sigma) = O(1) \quad (\chi \neq \chi_0), \tag{3.11}$$

prvo za $1 < \sigma \leq \sigma_0$, a zatim, budući da je kao i prije $F_\chi(\sigma)$ ograničen na $\sigma \geq \sigma_0$, za cijeli raspon $\sigma > 1$.

Dokaz Dirichletovog teorema
Ako uvrstimo ocjene (3.10) i (3.11) u (3.4)dobijemo

$$\begin{aligned} F_{a,q}(\sigma) &= \frac{1}{\phi(q)}\overline{\chi_0(a)}F_{\chi_0}(\sigma) + O(1) \\ &= \frac{1}{\phi(q)}\log\frac{1}{\sigma - 1} + O(1) \quad (1 < \sigma \leq 2), \end{aligned} \tag{3.12}$$

budući da je $\chi_0(a) = 1$ po definiciji glavnog karaktera i pretpostavci $(a, q) = 1$. To dokazuje (3.2) dakle i (3.1), odnosno Teorem (1.2.6).

Poglavlje 4

Funkcija $L(1,\chi)$

4.1 Funkcija $L(1,\chi)$

U ovome dijelu dokazat ćemo (*iii*) dio Teorema (2.2.2) pa ga navodim još jednom.

Teorem 4.1.1. ***Neponištavanje funkcije*** $L(1,\chi)$
Neka je q pozitivan cijeli broj i neka je χ ne-glavni karakter modulo q. Tada je $L(1,\chi) \neq 0$.

Za dokaz nam je potrebno nekoliko pomoćnih Lema.

Lema 4.1.2.
Neka je

$$P(s) = P_q(s) = \prod_{\chi \mod q} L(s,\chi)$$

Tada je, za $\sigma \geq 1$

$$P(\sigma) \geq 1.$$

Dokaz.
Ako Dirichletovu funkciju $L(s,\chi)$ razvijemo u Eulerov produkt i ako uzmemo logaritme,

dobivamo za $\sigma > 1$

$$\begin{aligned}\log P(\sigma) &= \sum_{\chi \bmod q} \log L(\sigma,\chi) \\ &= \sum_{\chi \bmod q} \sum_{p} \log\left(1 - \frac{\chi(p)}{p^{\sigma}}\right)^{-1} \\ &= \sum_{\chi \bmod q} \sum_{p} \sum_{m=1}^{\infty} \frac{\chi(p)^m}{p^{m\sigma}} \\ &= \sum_{p} \sum_{m=1}^{\infty} \frac{1}{p^{m\sigma}} \sum_{\chi \bmod q} \chi(p)^m\end{aligned}$$

Budući da je

$$\sum_{\chi \bmod q} \chi(p)^m = \sum_{\chi \bmod q} \chi(p^m) = \begin{cases} \phi(q) & \text{ako je } \quad p^m \equiv 1 \mod q, \\ 0 & \text{inače} \end{cases}$$

prema potpunoj multiplikativnosti karaktera χ i relaciji ortogonalnosti za karaktere (dio (*ii*) Teorema (2.1.14)), desna strana gornje jednakosti je zbroj nenegativnih članova, što dokazuje tvrdnju leme. □

Dokaz Teorema (4.1.1) za kompleksne karaktere χ
Koristit ćemo gore navedenu lemu kako bismo pokazali da je $L(s,\chi) \neq 0$ u slučaju da je χ kompleksan karakter modulo q, tj. da χ ne poprima samo realne vrijednosti.
Pretpostavljamo da je $L(1,\chi_1) = 0$ za određene kompleksne karaktere modulo q. Izvest ćemo kontradikciju iz ove pretpostavke.
Prvo napominjemo da su, budući da je χ_1 kompleksan karakter, karakteri χ_1 i $\overline{\chi_1}$ različiti, a nijedan od njih nije jednak glavnom karakteru χ_0. Stoga, $\chi_0, \chi_1, \overline{\chi_1}$ svaki doprinose po faktor produktu $P(\sigma)$ u Lemi (4.1.2).
Ako ta tri faktora izdvojimo, dobivamo, za $\sigma > 1$,

$$P(\sigma) = L(\sigma,\chi_0)L(\sigma,\chi_1)L(\sigma,\overline{\chi_1})Q(\sigma) \tag{4.1}$$

gdje je

$$Q(\sigma) = \prod_{\substack{\chi \bmod q \\ \chi \neq \chi_0, \chi_1, \overline{\chi_1}}} L(\sigma,\chi).$$

Sada promotrimo ponašanje svakog faktora s desne strane (4.1) kod $\sigma \to 1+$.
Prvo, prema dijelu (*ii*) Teorema (2.2.2), $L(s,\chi_0)$ ima jednostavan pol u $s = 1$, tako da imamo

$$L(\sigma,\chi_0) = O(\frac{1}{\sigma - 1}) \quad \text{za} \quad \sigma \to 1 + .$$

Nadalje, naša pretpostavka da je $L(1,\chi_1) = 0$ i analitičnost od $L(s,\chi_1)$ u $s = 1$ impliciraju $L(\sigma,\chi_1) = O(\sigma - 1)$, a budući da je

$$L(\sigma,\overline{\chi_1}) = \sum_{n=1}^{\infty} \frac{\overline{\chi_1(n)}}{n^\sigma} = \overline{\sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^\sigma}} = \overline{L(\sigma,\chi_1)},$$

također imamo $L(\sigma,\overline{\chi_1}) = O(\sigma - 1)$.
Konačno, prema dijelu (i) Teorema (2.2.2), $Q(\sigma)$ je ograničen kod $\sigma \to 1+$.
Iz ovih ocjena slijedi da je $P(\sigma) = O(\sigma - 1)$ za $\sigma \to 1+$. To je proturječno nejednakosti $P(\sigma) \geq 1$ iz Leme (4.1.2). Prema tome $L(1,\chi_1)$ ne može biti jednako 0.

Gornji argument ne vrijedi u slučaju realnog karaktera χ_1, budući da je $\overline{\chi_1} = \chi_1$, te bi se u gore navedenoj faktorizaciji produkta $P(\sigma)$ pojavila samo jedna L-funkcija koja bi odgovarala χ_1, tako da bi pretpostavka da je $L(1,\chi_1) = 0$ dala samo jednu ocjenu $P(\sigma) = O(1)$, što nije dovoljno da dobijemo kontradikciju. Da bismo dokazali neiščezavanje od $L(1,\chi)$ za realne karaktere potreban je potpuno drugačiji, kompliciraniji argument. Prvo ćemo navesti nekoliko pomoćnih rezultata.

Lema 4.1.3.
Neka je χ realan karakter i neka je f multiplikativna funkcija zadana sa $f(p^m) = 1 + \sum_{k=1}^{m} \chi(p)^k$ za prosti broj p. Tada je $f(n) \geq 0$ za svaki n, a $f(n) \geq 1$ ako je n kvadrat.

Dokaz.
Budući da su i χ i f multiplikativni te da je χ realan karakter modulo q, imamo $\chi(p) = \pm 1$ ako p ne dijeli q, a $\chi(p) = 0$ ako $p|q$. Stoga, kod potencije prostih brojeva p^m imamo

$$f(p^m) = 1 + \sum_{k=1}^{m} \chi(p)^k = \begin{cases} 1 & \text{ako p ne dijeli q,} \\ m+1 & \text{ako p ne dijeli q} \quad i \quad \chi(p) = 1, \\ 0 & \text{ako p ne dijeli q,} \quad \chi(p) = -1 \quad i \quad \text{m je neparan,} \\ 1 & \text{ako p ne dijeli q,} \quad \chi(p) = -1 \quad i \quad \text{m je paran} \end{cases}$$

Iz toga slijedi da je $f(p^m) \geq 1$ ako je m paran i $f(p^m) \geq 0$ ako je m neparan. Zbog multiplikativnosti funkcije f to dokazuje tvrdnju leme. □

Lema 4.1.4.
Imamo

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

gdje je A konstanta.

Dokaz.
Prema Eulerovoj formuli imamo

$$\begin{aligned}\sum_{n\le x}\frac{1}{\sqrt{n}} &= 1 - xx^{-1/2} + \int_1^x u^{-1/2}du + \int_1^x u(-1/2)u^{-3/2}du \\ &= 1 + O\left(\frac{1}{\sqrt{x}}\right) + 2(\sqrt{x}-1) - \int_x^\infty uu^{-3/2}du + O\left(\int_x^\infty u^{-3/2du}\right) \qquad (4.2)\\ &= 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right)\end{aligned}$$

gdje je $A = -1 - \left(\frac{1}{2}\right)\int_1^\infty uu^{-3/2}du$. □

Lema 4.1.5.
Neka je χ ne-glavni karakter modulo q i neka je s kompleksan broj u poluravnini $\sigma > 0$. Tada imamo

$$\sum_{n\le x}\frac{\chi(n)}{n^s} = L(s,\chi) + O_{q,s}(x^{-\sigma}) \quad (x \ge 1). \qquad (4.3)$$

Dokaz.
Neka je

$$M(u) = M(\chi,u) = \sum_{n\le u}\chi(n).$$

Parcijalnim sumiranjem imamo, za $y > x$

$$\sum_{x<n\le y}\frac{\chi(n)}{n^s} = \frac{M(y)}{y^s} - \frac{M(x)}{x^s} + s\int_x^y M(u)u^{-s-1}du.$$

Budući da je χ ne-glavni karakter, prema Korolaru (2.1.15) slijedi da je

$$M(u) = O_q(1)$$

tako da je desna strana gornje jedankosti ograničena sa

$$<<_q x^{-\sigma} + |s|\int_x^y u^{-\sigma-1}du <<_{q,s} x^{-\sigma}.$$

Ako pustimo da $y \to \infty$, onda lijeva strana teži k

$$L(s,\chi) - \sum_{n\le x}\chi(n)n^{-s}$$

što dokazuje lemu. □

Dokaz Teorema (4.1.1) za realne karaktere χ
Fiksiramo realan, ne-glavni karakter χ modulo q. U cijelom dokazu pustit ćemo da konstante u O-ocjenama ovise o χ, i stoga također o q, bez izričitog navođenja te ovisnosti. Neka je f definirana kao u Lemi (4.1.3), pa razmotrimo sumu

$$S(x) = \sum_{n \le x} \frac{f(n)}{\sqrt{n}}.$$

S jedne strane, prema Lemi (4.1.3) imamo

$$S(x) \ge \sum_{m^2 \le x} \frac{f(m^2)}{\sqrt{m^2}} \ge \sum_{m \le \sqrt{x}} \frac{1}{m} >> \log x \quad (x \ge 2) \tag{4.4}$$

S druge strane možemo ocijeniti $S(x)$ ako napišemo

$$f(n) = \sum_{d|n} \chi(d) = \sum_{dm=n} \chi(d)$$

i ako podijelimo dvostruku sumu koju dobijemo prema Dirichletovoj metodi hiperbole:

$$S(x) = \sum_{\substack{d,m \le x \\ dm \le x}} \frac{\chi(d)}{\sqrt{d}\sqrt{m}} = \Sigma_1 + \Sigma_2 - \Sigma_3 \tag{4.5}$$

gdje su

$$\Sigma_1 = \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le \frac{x}{d}} \frac{1}{\sqrt{m}}$$

$$\Sigma_2 = \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}} \sum_{d \le \frac{x}{m}} \frac{\chi(d)}{\sqrt{d}}$$

$$\Sigma_3 = \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m \le \sqrt{x}} \frac{1}{\sqrt{m}}.$$

Te tri sume možemo ocijeniti koristeći Leme (4.1.4) i (4.1.5). Dobivamo:

$$\begin{aligned}
\Sigma_1 &= \sum_{d \le \sqrt{x}} \left(2\sqrt{\frac{x}{d}} + A + O\left(\frac{1}{\sqrt{\frac{x}{d}}} \right) \right) \\
&= 2\sqrt{x} \sum_{d \le \sqrt{x}} \frac{\chi(d)}{d} + A \sum_{d \le \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + O\left(\sum_{d \le \sqrt{x}} \frac{1}{\sqrt{x}} \right) \\
&= 2\sqrt{x}(L(1,\chi) + O(\frac{1}{\sqrt{x}})) + A(L(\frac{1}{2},\chi) + O(\frac{1}{x^{\frac{1}{4}}})) + O(1) \\
&= 2\sqrt{x}L(1,\chi) + O(1)
\end{aligned}$$

$$\begin{aligned}\sum_2 &= \sum_{m\le\sqrt{x}} \frac{1}{\sqrt{m}}\left(L\left(\frac{1}{2},\chi\right)+O\left(\frac{1}{\sqrt{\frac{x}{m}}}\right)\right)\\ &= L\left(\frac{1}{2},\chi\right)\left(2x^{1/4}+O(1)\right)+O\left(\sum_{m\le\sqrt{x}}\frac{1}{\sqrt{x}}\right)\\ &= L\left(\frac{1}{2},\chi\right)2x^{1/4}+O(1)\end{aligned}$$

$$\begin{aligned}\sum_3 &= \left(L\left(\frac{1}{2},\chi\right)+O\left(\frac{1}{x^{1/4}}\right)\right)\left(2x^{1/4}+O(1)\right)\\ &= L\left(\frac{1}{2},\chi\right)2x^{1/4}+O(1).\end{aligned}$$

Ako te ocjene uvrtimo u (4.5) dobivamo

$$S(x) = 2\sqrt{x}L(1,\chi)+O(1).$$

Ako je sada $L(1,\chi)=0$ tada bismo imali $S(x)=O(1)$ što je u kontradikciji s (4.3). Stoga je $L(1,\chi)\neq 0$ i dokaz Teorema (4.1.1) je potpun.

Bibliografija

1. T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

2. A.J. Hildebrand, *Introduction to Analytic Number Theory*,
dostupno na http://www.math.uiuc.edu/ hildebr/ant/

3. http://www-history.mcs.st-and.ac.uk/Biographies/Dirichlet.html (pristupljeno: kolovoz 2015.)

Sažetak

Ovaj diplomski rad podijelili smo na 4 poglavlja.

Prvo poglavlje opisuje životopis J.P.G.L. Dirichleta i sadrži iskaze Dirichletovog teorema.

U drugom poglavlju definirani su ključni pojmovi za dokazivanje Dirichletovog teorema. To su Dirichletovi karakteri i Dirichletove L-funkcije.

Na kraju rada dokazan je Dirichletov teorem u kvantitativnoj verziji kao i neke Leme potrebne za dokazivanje istog.

Summary

This thesis consists of four chapters.

The first chapter gives a biography of J.P.G.L. Dirichlet and contains the statements of Dirichlet's Theorem.

The second chapter contains definitions of key notions necessary for the proof of Dirichlet's Theorem. These notions are Dirichlet characters and Dirichlet L-functions.

The last two chapters contain the proof of Dirichlet's Theorem, together with some lemmas necessary for the proof.

Životopis

Rođena sam 2.5.1989. godine u Zagrebu. Osnovnoškolsko obrazovanje započinjem 1996. godine u Osnovnoj školi Dragutina Domjanića u Bedenici. Godine 2004. upisujem opću gimnaziju Dragutina Stražimira u Svetom Ivanu Zelini gdje sam 2008. godine maturirala s odličnim uspjehom. Iste godine nastavljam školovanje na Prirodoslovno - matematičkom fakultetu u Zagrebu. Godine 2012. nakon završenog preddiplomskog studija matematike; smjer: nastavnički, upisujem Diplomski sveučilišni studij Matematike; smjer:nastavnički.