Prosti brojevi u aritmetičkim nizovima

Škoro, Igor

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Igor Škoro

PROSTI BROJEVI U ARITMETIčKIM NIZOVIMA

Diplomski rad

Voditelj rada:
prof. dr. sc. Marko Tadić

Zagreb, Rujan, 2022

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. _____

Ovaj rad posvećujem svojoj djevojci Ivi, koja je svojom ljubavi i podrškom nemjerljivo pomogla u njegovom nastanku.

Sadržaj

Uvod

Proučavanje prostih brojeva je pratilo mnoge velike civilizacije kroz povijest, Stari Grci, prije više od dva tisućljeća, su među prvima primjenjivali rigorozne dokaze. Jedan od najvažnijih teorema o prostim brojevima dokazao je Euklid:

Postoji beskonačno mnogo prostih brojeva.

Euklidov je teorem dokazao preko kontradikcije, koristeći domišljat produkt prostih brojeva. 2000 godina kasnije, slavni švicarski matematičar Leonhard Euler objavio je svoju verziju dokaza pomoću analitičkih metoda. Njegova metoda se temelji na korištenju produkta

$$\prod_p \frac{1}{1-\frac{1}{p}}$$

nad prostim brojevima, gdje je svaki faktor ovog produkta zapisao kao beskonačni geometrijski red. Ovaj dokaz predstavlja prekretnicu u metodama dokazivanja u teoriji brojeva; algebarske metode poput Euklidove se zamjenjuju s analitičkim metodama.

Često pitanje u analitičkoj teoriji brojeva je koji podskupovi od $\mathbb{Z}$ sadrže beskonačno mnogo prostih brojeva. U ovom radu, pručavati ćemo aritmetičke nizove, i pokazati ćemo koji aritmetički nizovi sadrže beskonačno mnogo prostih brojeva. Ovim pitanjem se bavio Euler, ali kompletan dokaz predstavio je 1837. njemački matematičar Peter Gustav Lejeune Dirichlet. Dirichletov teorem nam govori da postoji beskonačno mnogo prostih brojeva u aritmetičkom nizu $a + km$, $k \in \mathbb{N}$, ukoliko su a i m relativno prosti prirodni brojevi.

U prvom poglavlju baviti ćemo se osnovnim pojmovima i teoremima koji će nam služiti u ostatku rada. Definirati ćemo Legendrov simbol, i dokazati neka osnovna svojstva. Iskazati ćemo Zakon kvadratnog reciprociteta, koji će nam biti od velike važnosti. Također, navesti ćemo bitne pojmove i teoreme iz kompleksne analize koji će nam trebati za analitičke dokaze.

U drugom poglavlju, baviti ćemo se prvo karakterima konačnih Abelovih grupa, i dokazati ćemo neka osnovna svojstva. Posebno bitni će nam biti modularni karakteri, tj. karakteri grupe $\mathbb{Z}/m\mathbb{Z}$, gdje je $m \in \mathbb{N}$. Zatim ćemo proučavati Dirichletove redove, kao i L-funkcije, koje definiramo pomoću modularnih karaktera. Konačno, uvesti ćemo pojam Dirichletove gustoće, te ćemo dokazati Dirichletov teorem, u jačoj veriziji, pa ćemo

verziju izrečenu ovdje dobiti kao korolar. Na kraju, iskoristiti ćemo Dirichletov teorem da dokažemo tvrdnju o tome kako su prosti brojevi distribuirani s obzirom na Legendrov simbol.

Poglavlje 1

Osnovni pojmovi

1.1 Algebra i teorija brojeva

Za dokaz Dirichletovog teorema bit će nam važan pojam Legendrovog simbola, koji definiramo pomoću kvadratnih ostataka.

Definicija 1.1.1. *Neka je $n \in \mathbb{N}$, $a \in \mathbb{Z}$ i $(a, n) = 1$. Broj a nazivamo kvadratni ostatak modulo n ako postoji $x \in \mathbb{N}$ takav da vrijedi kongruencija*

$$x^2 \equiv a \ (mod\ n)$$

Ako je $(a, n) = 1$ i gore prikazana kongruencija nema rješenja, broj a nazivamo kvadratni neostatak modulo n.

Definicija 1.1.2. *Neka je p prost cijeli broj. Za cijeli broj n definiramo Legendrov simbol*

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{ako je } n \text{ kvadratni ostatak modulo } p \text{ i vrijedi } n \not\equiv 0 \pmod{p} \\ -1 & \text{ako je } n \text{ kvadratni neostatak modulo } p \\ 0 & n \equiv 0 \pmod{p} \end{cases}$$

Definicija 1.1.3. *Za cijeli broj n kažemo da je kvadratno slobodan ako ne postoji cijeli broj x takav da $x^2 \mid n$*

Primjer 1.1.4. *Kvadratni ostatci modulo 5 su 1 i 4, a kvadratni neostatci su 2 i 3.*

Definicija 1.1.5. *Za neparan cijeli broj n definiramo $\epsilon(n)$, $\omega(n) \in \{0, 1\}$ na sljedeći način*

$$\epsilon(n) \equiv \frac{n-1}{2} \quad (mod\ 2) = \begin{cases} 0 & \text{ako je } n \equiv 1 \ (mod\ 4) \\ 1 & \text{ako je } n \equiv -1 \ (mod\ 4) \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \pmod 2 = \begin{cases} 0 & ako\ je\ n \equiv \pm 1 \pmod 8 \\ 1 & ako\ je\ n \equiv \pm 5 \pmod 8 \end{cases}$$

Lema 1.1.6. *Ako za cijele brojeve a, b vrijedi $a \equiv b \pmod p$, onda je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

Dokaz. Ako p dijeli a, onda je $a \equiv 0 \pmod p$. Slijedi da je $b \equiv 0 \pmod p$, pa onda p dijeli b te vrijedi $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 0$. Pretpostavimo da je $a \not\equiv 0 \pmod p$. Onda je a kvadratni ostatak ako i samo ako je $a \equiv x^2 \pmod p$ za neki x. Kako je $a \equiv b \pmod p$, onda slijedi da je $b \equiv x^2 \pmod p$ ako i samo ako je $a \equiv x^2 \pmod p$. Dakle, ako je $a \equiv b \pmod p$, onda su a i b oboje ili kvadratni ostatci, ili kvadratni neostatci. □

Lema 1.1.7. *Neka je p prost broj te $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Onda vrijedi $a^{\epsilon(p)} \equiv 1 \pmod p$ ako i samo ako je a kvadratni ostatak mod p.*

Dokaz. Neka je a kvadratni ostatak, tj neka je $a \equiv x^2 \pmod p$ za neki cijeli broj x, te neka je $x \not\equiv 0 \pmod p$. Onda vrijedi:

$$a^{\epsilon(p)} \equiv (x^2)^{\epsilon(p)} \equiv x^{p-1} \equiv 1 \pmod p$$

Gdje posljednja kongruencija vrijedi po Fematovom malom teoremu.

Kako je $\mathbb{Z}/p\mathbb{Z}$ polje, kongruencija $a^{\epsilon(p)} \equiv 1 \pmod p$ ima najviše $\frac{p-1}{2}$ rješenja u $\mathbb{Z}/p\mathbb{Z}$. Kako je svaki kvadratni ostatak rješenje, onda trebamo provjeriti koliko kvadratnih ostataka mod p postoji. Jedina rješenja od $t^2 \equiv 1 \pmod p$ su $t = \pm 1 \pmod p$, pa homomorfizam $(\mathbb{Z}/p\mathbb{Z})^* \mapsto (\mathbb{Z}/p\mathbb{Z})^*$, koji svaki element preslikava u svoj kvadrat, ima jezgru reda 2. Slijedi da je red slike homomorfizma reda $\frac{p-1}{2}$. Dakle, $\frac{p-1}{2}$ elemenata od $(\mathbb{Z}/p\mathbb{Z})^*$ su kvadratni ostatci, pa su onda rješenja kongruencije $a^{\epsilon(p)} \equiv 1 \pmod p$ su upravo kvadratni ostatci mod p. □

Teorem 1.1.8. *Za svaki cijeli broj a vrijedi:*

$$\left(\frac{a}{p}\right) \equiv a^{\epsilon(p)} \pmod p$$

Dokaz. Tvrdnja trivijalno vrijedi ako p dijeli a, pa pretpostavimo da p ne dijeli a. Slijedi da je $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Ako je a kvadratni ostatak mod p, onda je po prethodnoj lemi $a^{\epsilon(p)} \equiv 1 \pmod p$ i po definiciji vrijedi $\left(\frac{a}{p}\right) = 1$. U suprotnom, ako je a kvadratni neostatak mod p, onda je po prethodnoj lemi $a^{\epsilon(p)} \not\equiv 1 \pmod p$ te je $\left(\frac{a}{p}\right) = -1$. Kako vrijedi:

$$(a^{\epsilon(p)})^2 \equiv a^{p-1} \equiv 1 \pmod p$$

i kako je $a^{\epsilon(p)} \not\equiv 1 \pmod p$, mora vrijediti $a^{\epsilon(p)} \equiv -1 \pmod p$. □

Korolar 1.1.9. *Legendrov simbol je multiplikativan, tj. za sve cijele brojeve a, b vrijedi:*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Dokaz. Iz teorema slijedi:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\epsilon(p)}b^{\epsilon(p)} \pmod{p}$$

i

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\epsilon(p)} \pmod{p}$$

Međutim, vrijedi $a^{\epsilon(p)}b^{\epsilon(p)} = (ab)^{\epsilon(p)}$, pa je onda

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

Kako $0, 1, -1$ nisu kongruentni mod p, onda slijedi

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right)$$

□

Teorem 1.1.10. *Za svaki neparni prosti broj vrijedi:*

$$\left(\frac{-1}{p}\right) = (-1)^{\epsilon(p)}$$

Dokaz. Uvrštavajući $a = -1$ u prethodni teorem dobivamo:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\epsilon(p)} \pmod{p}$$

Kako je:

$$\left(\frac{-1}{p}\right) = \pm 1 \quad \text{i} \quad (-1)^{\epsilon(p)} = \pm 1$$

te je $1 \not\equiv -1 \pmod{p}$, mora vrijediti tvrdnja teorema. □

Teorem 1.1.11. *Za svaki neparni prosti broj p vrijedi:*

$$\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

Dokaz. Dovoljno je dokazati da je 2 kvadratni ostatak ako je $p \equiv 1, 7 \pmod 8$ a kvadratni neostatak ako je $p \equiv 3, 5 \pmod 8$.

Pretpostavimo da je $p \equiv 1 \pmod 4$. Onda vrijedi:

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdots (\frac{p-1}{2}) \\ &= 2 \cdot 4 \cdot 6 \cdots (p-1) \\ &= 2 \cdot 4 \cdot \cdot 6 \cdots (\frac{p-1}{2})(\frac{p+3}{2}) \cdots (p-3)(p-1) \\ &\equiv 2 \cdot 4 \cdot \cdot 6 \cdots (\frac{p-1}{2})(\frac{3-p}{2}) \cdots (-3)(-1) \pmod p \\ &\equiv 2 \cdot 4 \cdot \cdot 6 \cdots (\frac{p-1}{2})(\frac{p-3}{2}) \cdots (3)(1)(-1)^{\frac{p-1}{4}} \pmod p \\ &\equiv 1 \cdot 2 \cdot \cdot 3 \cdots (\frac{p-1}{2})(-1)^{\frac{p-1}{4}} \pmod p \\ &\equiv (-1)^{\frac{p-1}{4}}\left(\frac{p-1}{2}\right)! \pmod p \end{aligned} \tag{1.1}$$

Kako je $(\frac{p-1}{2})!$ produkt invertibilnih elemenata mod p, i on je invertibilan mod p. Dakle, vrijedi da je $2^{\epsilon(p)} \equiv (-1)^{\frac{p-1}{4}} \pmod p$. Uvrštavajući $p \equiv 1 \pmod 8$ sa $p = 8k+1$ dobivamo $2^{\epsilon(p)} = (-1)^{2k} \equiv 1 \pmod p$, dok uvrštavajući $p \equiv 5 \pmod 8$ sa $p = 8k+5$ dobivamo $2^{\epsilon(p)} \equiv (-1)^{2k+1} \equiv -1 \pmod p$. Dakle, 2 je kvadratni ostatak kada je $p \equiv 1 \pmod p$, ali kvadratni neostatak kada je $p \equiv 5 \pmod 8$.

Analogno postupamo za slučaj da je $p \equiv 3 \pmod 4$. Računamo:

$$\begin{aligned} 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= 2 \cdot 4 \cdot \cdot 6 \cdots (\frac{p-3}{2})(\frac{p+1}{2}) \cdots (p-3)(p-1) \\ &\equiv 2 \cdot 4 \cdot \cdot 6 \cdots (\frac{p-3}{2})(\frac{1-p}{2}) \cdots (-3)(-1) \pmod p \\ &\equiv 1 \cdot 2 \cdot \cdot 3 \cdots (\frac{p-1}{2})(-1)^{\frac{p+1}{4}} \pmod p \\ &\equiv (-1)^{\frac{p+1}{4}}\left(\frac{p-1}{2}\right)! \pmod p \end{aligned} \tag{1.2}$$

Iz ovoga slijedi da je $2^{\epsilon(p)} \equiv (-1)^{\frac{p+1}{4}} \pmod p$. Uvrštavajući $p \equiv 3 \pmod p$ dobivamo $2^{\epsilon(p)} \equiv -1 \pmod p$. S druge strane, ako je $p \equiv 7 \pmod 8$ onda je $2^{\epsilon(p)} = 1 \pmod p$ i slijedi tvrdnja teorema. □

Sljedeći teorem navodim bez dokaza (dokaz se može pronaći u [3]):

Teorem 1.1.12. ***(Zakon kvadratnog reciprciteta)*** *Neka su p i q različiti neparni prosti brojevi. Onda vrijedi*

$$\left(\frac{q}{p}\right) = (-1)^{\epsilon(q)\epsilon(p)}\left(\frac{p}{q}\right)$$

Za kraj definiramo djeljive grupe, što će nam biti od koristi pri proučavanju homomorfizama između Abelovih grupa u idućem poglavlju.

Definicija 1.1.13. *Za Abelovu grupu $(G, \cdot)$ kazemo da je djeljiva, ako za svaki $g \in G$ i za svaki $n \in \mathbb{N}$ postoji $y \in G$ takav da je $y^n = g$.*

Primjer 1.1.14. *Grupa racionalnih brojeva $\mathbb{Q}$ sa relacijom zbrajanja je djeljiva.*

Primjer 1.1.15. *Multiplikativna grupa kompleksnih brojeva $\mathbb{C}$ je djeljiva.*

1.2 Kompleksna analiza

U ovom potpoglavlju prisjetiti ćemo se nekih definicija i činjenica iz kompleksne analize koje ćemo koristiti kasnije. Teoreme navodim bez dokaza (za dokaze vidjeti [2] i [5]).

Definicija 1.2.1. *Neka je f kompleksna funkcija kompleksne varijable te neka je z_0 iz domene od f. Za funkciju kazemo da je kompleksno-diferencijabilna u točki z_0 ako postoji limes*

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

i ako je konačan. Vrijednost limesa označavamo sa $f'(z_0)$ i zovemo derivacija od f u z_0.

Definicija 1.2.2. *Neka je $U \subset \mathbb{C}$ otvoren skup i $f : U \to \mathbb{C}$. Za funkciju f kažemo da je holomorfna u točki $z_0 \in U$ ako je kompleksno diferencijabilna na nekoj okolini od z_0. Ako je f holomorfna u svakoj točki $z \in U$ onda kažemo da je f holomorfna na U.*

Teorem 1.2.3. *Neka je $f : \Omega \to \mathbb{C}$ derivabilna funkcija, $\Gamma \subseteq \Omega$ pozitivno orijentirana kontura čije je unutrašnje područje sadržano u Ω, i neka točka z pripada tom unutrašnjem području. Onda vrijedi*

$$f(z) = \frac{1}{2\pi i}\int_\Gamma \frac{f(\xi)}{\xi - z}d\xi$$

Teorem 1.2.4. *Neka je γ po dijelovima gladak put u $\mathbb{C}$ i neka je $\psi : \operatorname{Im}\gamma \to \mathbb{C}$ neprekidna funkcija. Tada je funkcija $f : \mathbb{C} \setminus \operatorname{Im}\gamma \to \mathbb{C}$ definirana sa*

$$f(z) := \int_\gamma \frac{\psi(\xi)}{\xi - z}d\xi,$$

derivabilna na $\mathbb{C} \setminus \operatorname{Im}\gamma$*, i njezina derivacija je jednaka*

$$f'(z) = \int_\gamma \frac{\psi(\xi)}{(\xi - z)^2} d\xi \,.$$

Nadalje, funkcija $f' : \mathbb{C} \setminus \operatorname{Im}\gamma \to \mathbb{C}$ *je neprekidna.*

Teorem 1.2.5. *Neka je* $\Omega \subseteq \mathbb{C}$ *otvoren skup, a* $f : \Omega \to \mathbb{C}$ *neprekidna funkcija sa svojstvom da za svaku točku* $z \in \Omega$*, postoji* $r_z > 0$*, dovoljno malen da je* $K(z, r_z) \subseteq \Omega$*, i takav da za svaki pravokutnik* $I \subseteq K(z, r_z)$ *vrijedi* $\int_{\partial I} f dz = 0$*. Tada je* f *holomorfna na* Ω*.*

Teorem 1.2.6. *Neka je* $\gamma : [a, b] \to \mathbb{C}$ *po dijelovima gladak put, a* $f_n : \operatorname{Im}\gamma \to \mathbb{C}$*,* $n \in \mathbb{N}$*, niz neprekidnih funkcija koje konvergiraju lokalno uniformno funkciji* $f : \operatorname{Im}\gamma \to \mathbb{C}$*. Tada je* $\int_\gamma f dz = \lim_{n\to\infty} \int_\gamma f_n dz$*.*

Teorem 1.2.7. *Neka je* $\gamma : [a, b] \to \mathbb{C}$ *po dijelovima gladak put duljine* $l(\gamma)$*, i neka je* $f : \operatorname{Im}\gamma \to \mathbb{C}$ *neprekidna funkcija, te neka je* $M := max\{|f(z)| : z \in \operatorname{Im}\gamma\}$*. Tada je:*

$$\left| \int_\gamma f dz \right| \leq M \cdot l(\gamma)$$

Definicija 1.2.8. *Neka je* $S \subseteq \mathbb{C}$ *te* $f_n : S \to \mathbb{C}$*,* $n \in \mathbb{N}$*, niz funkcija. Kažemo da niz* (f_n) *konvergira lokalno uniformno na* S*, ako za svaki* $z \in S$ *postoji* $r_z > 0$ *takav da niz restrikcija* $f_{n|K(z,r_z)\cap S}$ *konvergira uniformno na* $K(z, r_z) \cap S$*.*

Teorem 1.2.9. *Neka je* $f_n : S \to \mathbb{C}$*,* $n \in \mathbb{N}$*, niz neprekidnih funkcija koji lokalno uniformno konvergira funkciji* $f : S \to \mathbb{C}$*. Tada je i funkcija* f *neprekidna.*

Za točku $z_0 \in \mathbb{C}$ i pozitivne brojeve $0 < r < R$ označavat ćemo s $V(z_0; r, R)$ kružni vijenac, tj. skup $\{z \in \mathbb{C} : r < |z - z_0| < R\}$.

Teorem 1.2.10. ***Laurentov teorem*** *Neka je funkcija* f *holomorfna na kružnom vijencu* $V := V(z_0; r, R)$*. Tada za svaki* $z \in V$ *vrijedi*

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

, gdje su koeficijenti a_n *dani sa*

$$a_n = \frac{1}{2\pi i} \int_{\Gamma_0} \frac{f(\xi)}{(\xi - z_0)^{n+1}} d\xi$$

, a Γ_0 *je pozitivno orijentirana kružnica oko* z_0 *radijusa* ρ*,* $r < \rho < R$*.*

Red iz prethodnog teorema nazivamo Laurentov red funkcije f oko točke z_0.

Definicija 1.2.11. *Neka je $\Omega \subseteq \mathbb{C}$ otvoren skup, a $f : \Omega \to \mathbb{C}$ funkcija. Kažemo da je točka $z_0 \in Int(\overline{\Omega})$ singularitet funkcije f ako u točki z_0 funkcija f nije holomorfna ili uopće nije definirana u toj točki.*

Postoje razne vrste singulariteta, ali nama od zanimanja su samo tzv. izolirani singulariteti, koje definiramo na sljedeći način.

Definicija 1.2.12. *Za singularitet z_0 kažemo da je izolirani singularitet funkcije f, ako je f holomorfna funkcija na nekom probušenom krugu $K^*(z_0, R)$ oko točke z_0.*

Probušeni krug iz prethodne definicije definiramo kao skup $K(z_0, R) \setminus \{z_o\}$.

Napomena 1.2.13. *Funkcija može imati beskonačno mnogo izoliranih singulariteta, ali najviše prebrojivo mnogo. Ako funkcija f ima samo izolirane singularitete, onda svaki kompaktan skup u domeni od f sadrži konačno mnogo izoliranih singulariteta.*

Za izoliran singularitet z_0 funkcije f kažemo da je uklonjiv, ako u točki z_0 možemo funkciju f predefinirati, ili, u slučaju da f nije u z_0 definirana, dodefinirati, tako da postane holomorfna na nekom krugu $K(z_0, R)$ oko točke z_0.

Za izolirani singularitet z_0 funkcije f kažemo da je pol, ako u Laurentovom razvoju funkcije f oko točke z_0 ima konačno mnogo, ali barem jedan, član sa potencijama od $\frac{1}{z-z_0}$ različit od nule. Red pola je red najveće potencije od $\frac{1}{z-z_0}$ koja se pojavljuje u tom Laurentovom redu s koeficijentom različitim od nule. Pol reda 1 zovemo jednostavan pol.

Teorem 1.2.14. *Neka je funkcija f holomorfna na probušenom krugu $K^*(z_0, R)$. Onda su sljedeće tvrdnje ekvivalentne:*

i) z_0 je pol funkcije f reda m.
ii) z_0 nije uklonjiv singularitet funkcije f, ali postoji $k \in \mathbb{N}$ takav da je z_0 uklonjiv singularitet od funkcije $z \mapsto (z - z_0)^k f(z)$ i m je najmanji takav k.
iii) $\lim_{z \to z_0} |f(z)| = \infty$.

Definicija 1.2.15. *Neka je X skup i Y normiran prostor. Za niz funkcija (f_n) sa X u Y kažemo da konvergira normalno ako konvergira red*

$$\sum_{n=1}^{\infty} \|f_n\|_\infty$$

gdje je $\|f_n\|_\infty = sup\{\|f_n(x)\| \ : x \in X\}$

Propozicija 1.2.16. *Ako red funkcija $\sum_{n=1}^{\infty} f_n$ konvergira normalno, onda red*

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

konvergira uniformno i apsolutno.

Propozicija 1.2.17. *Neka red funkcija $\sum_{n=1}^{\infty} f_n$ konvergira normalno i neka je $\tau : \mathbb{N} \to \mathbb{N}$ bijekcija. Onda red $\sum_{n=1}^{\infty} f_{\tau(n)}$ konvergira normalno.*

Poglavlje 2

Dirichletov teorem

Iskažimo formalno Dirichletov teorem koji smo naveli u uvodu rada:

Teorem 2.0.1. ***(Dirichlet)*** *Neka su a i m relativno prosti prirodni brojevi. Postoji beskonačno mnogo prostih brojeva p takvih da je $p \equiv a \pmod{m}$.*

Neki slučajevi gornjeg teorema se mogu dokazati koristeći samo elementarne, algebarske metode. Dokazati ćemo nekoliko jednostavnijih primjera.

Teorem 2.0.2. *Postoji beskonačno mnogo prostih brojeva oblika $4n-1$, gdje je n prirodan broj.*

Dokaz. Pretpostavimo suprotno, tj. neka postoji samo konačno mnogo prostih brojeva oblika $4n-1$ te označimo sa p najveći od njih. Promatramo sljedeći prirodan broj

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

gdje je $3 \cdot 5 \cdots p$ produkt svih prostih brojeva manjih ili jednakih p. N je oblika $4n-1$ i veći je od p, pa onda slijedi da ne može biti prost. Nijedan prost broj manji od p ne dijeli N jer su svi sadržani u produktu $3 \cdot 5 \cdots p$ pa su onda svi prosti faktori od N veci od p. Ne mogu svi ti faktori biti oblika $4n+1$ jer bi onda bio i N takav. Dakle, postoji prost faktor od N oblika $4n-1$ koji je veći od p, čime dolazimo do kontradikcije. □

Teorem 2.0.3. *Postoji beskonačno mnogo prostih brojeva oblika $4n+1$, gdje je n prirodan broj.*

Dokaz. Neka je $N > 1$ prirodan broj i stavimo $m = (N!)^2 + 1$. Kako $N!$ sadrzi 2, onda je m neparan broj. Neka je p najmanji prosti faktor od m. Nijedan prost broj manji od N ne dijeli m jer su svi sadržani u $N!$, pa je onda $p > N$. Slijedi

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

pa je onda

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

Međutim, po Eulerovom teoremu vrijedi

$$(N!)^{p-1} = 1 \pmod{p}$$

pa onda mora vrijediti

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

Razlika $(-1)^{\frac{p-1}{2}} - 1$ mora biti jednaka 0 ili -2. Kako je p neparan, onda zbog prethodne kongruencije mora biti jednaka 0. Slijedi da je

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

pa je $\frac{p-1}{2}$ paran broj. Iz toga slijedi da je $p \equiv 1 \pmod{4}$. Dakle, za svaki prirodan broj $N > 1$, postoji prost broj $p > N$ takav da je $p \equiv 1 \pmod{4}$, čime je teorem dokazan. □

Teorem 2.0.4. *Postoji beskonačno mnogo prostih brojeva oblika* $12n + 7$*, gdje je n nenegativan cijeli broj.*

Dokaz. Pretpostavimo suprotno, tj. neka je skup prostih brojeva oblika $12n + 7$ dan sa $p_1, \ldots, p_r$. Ovaj skup je očito neprazan, jer sadrži 7. Neka je $N = (2p_1 \cdots p_r)^2 + 3$. Ovaj broj je ocito veći od 1, pa ima proste djelitelje. Ako su svi prosti djelitelji od N oblika $12n + 1$, onda je to i N. Međutim, vrijedi $p_1, \ldots p_r \equiv 7 \pmod{12}$, pa je onda $p_1 \cdots p_r \equiv 1 \pmod{12}$ ili $p_1 \cdots p_r \equiv 7 \pmod{12}$ U oba slučaja vrijedi $(p_1 \cdots p_r)^2 \equiv 1 \pmod{12}$, pa slijedi $(2p_1 \cdots p_r)^2 + 3 \equiv 7 \pmod{12}$, što je u kontradikciji sa činjenicom da su svi prosti djelitelji od N oblika $12n + 1$. Neka je p prosti djelitelj od N koji nije oblika $12n + 1$. p ne može biti jednak 2 jer je N neparan, i ne moze biti jednak 3. Naime, onda bi 3 djelio $N - 3$, pa i $(2p_1 \cdots p_r)^2$, što povlači da je $3 \in \{p_1, \ldots, p_r\}$ čime dolazi do kontradikcije jer su svi ti prosti brojevi oblika $12n + 7$. Dakle, p nije jednak 2 niti 3. Nadalje, vrijedi da p dijeli N ili $(2p_1 \cdots p_r)^2 \equiv -3 \pmod{p}$ te je:

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod{12} \\ -1 & p \equiv 5, 11 \pmod{12} \end{cases}$$

Iz ovog slijedi da je p oblika $12n + 7$ jer smo pretpostavili da nije oblika $12n + 1$. Također, p nije sadržan u $\{p_1 \ldots p_r\}$ jer bi onda dijelio $N - (2p_1 \cdots p_r)^2$, pa i 3, što je nemoguće. Dakle, p je prosti broj oblika $12n + 7$ različit od $p_1 \ldots p_r$, što je kontradikcija, pa slijedi tvrdnja teorema. □

Teorem 2.0.5. *Postoji beskonačno mnogo prostih brojeva oblika* $12n + 11$.

Dokaz. Pretpostavimo suprotno, tj. neka je skup prostih brojeva oblika $12n + 11$ dan sa $p_1, \ldots, p_r$. Ovaj skup je neprazan, jer sadrži 11. Neka je $x = p_1 \cdots p_r$ te $N = 2x^4 - 6x^2 - 9$. Vrijedi $x = p_1 \cdots p_r \equiv (-1)^r \pmod{12}$, pa je onda $x^2 \equiv x^4 \equiv 1 \pmod{12}$, te je $2x^4 - 6x^2 - 9 \equiv -1 \pmod{12}$. Ne mogu svi djelitelji od N biti oblika $12n+1$, jer bi onda to bio i N, što je u kontradikciji sa prethodnom kongruencijom. Neka je p prosti djelitelj koji nije tog oblika. Jednstavno se provjeri da su svi korijeni polinoma $2y^4 - 6y^2 - 9 + 1$ manji od 3, sto povlači da je $N = 2x^4 - 6x^2 - 9 > 1$ jer je $x \geq 11$. Kako je N očito neparan broj, onda je p različit od 2. Nadalje, p ne može biti 3 jer bi onda vrijedilo:

$$3 \mid N \implies 3 \mid (N + 6x^2 + 9) \implies 3 \mid (2x^4) \implies 3 \mid x$$

što je nemoguće, jer su svi $p_1, \ldots, p_r$ oblika $12n+11$. N možemo zapisati na sljedeći način:

$$N = 2x^4 - 6x^2 - 9 = 3x^4 - x^4 - 6x^2 - 9 = 3x^4 - (x + 3)^2$$

iz čega slijedi da je $3x^4 \equiv (x^2 + 3)^2 \pmod{p}$. Ako p dijeli x, onda je:

$$p \mid (N - (2x^4 - 6x^2)) \implies p \mid 9 \implies p \mid 3$$

što je nemoguće. Dakle, p ne dijeli x pa postoji y takav da je $xy \equiv 1 \pmod{p}$. Iz kongruencije $3x^4 \equiv (x^2 + 3)^2 \pmod{p}$, množeći obje strane sa $y^4 \equiv y^4 \pmod{12}$ dobivamo:

$$3x^4y^4 \equiv 3 \equiv (y^2(x^2 + 3))^2 \pmod{p}$$

Iz ovoga slijedi da je $\left(\frac{3}{p}\right) = 1$. Međutim, vrijedi da je:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1, 11 \pmod{12} \\ -1 & p \equiv 5, 7 \pmod{12} \end{cases}$$

pa je onda p oblika $12n+1$ ili $12n+11$. Kako je p odabran tako da nije oblika $12n+1$, onda mora biti oblika $12n + 11$. Nadalje, p je očito različit od brojeva $p_1, \ldots, p_r$, pa dolazimo do kontradikcije. Dakle, postoji beskonačno mnogo prostih brojeva oblika $12n + 11$. □

Teorem 2.0.6. *Postoji beskonačno mnogo prostih brojeva oblika* $12n + 1$*, gdje je n nenegativan cijel broj.*

Dokaz. Kao u prethodnih dokazima, pretpostavimo suprotno te sa $p_1, \ldots, p_r$ označimo sve proste brojeve oblika $12n + 1$. Neka je $x = p_1 \cdots p_r$ te p prost djelitelj od $x^4 - x^2 + 1$. Ako vrijedi $p \mid x$ onda je i $p \mid (x^4 - x^2)$ pa i $p \mid 1$. Dakle, mora vrijediti $p \nmid x$, pa onda x ima multiplikativni inverz $\pmod{p}$, tj postoji cijeli broj y takav da je $xy \equiv 1 \pmod{p}$. Kako je $p \mid (x^4 - x^2 + 1)$, onda slijedi:

$$x^4 - x^2 + 1 \equiv 0 \pmod{p} \implies x^4 - 2x^2 + 1 + x^2 \equiv 0 \pmod{p} \implies (x^2 - 1)^2 \equiv (-1)x^2 \pmod{p}$$

Množeći obje strane sa $y^2 \equiv y^2 \pmod{p}$ dobivamo:

$$(y(x^2-1))^2 \equiv (-1)(xy)^2 \equiv -1 \pmod{p}$$

Dakle, vrijedi $\left(\frac{-1}{p}\right) = 1$. Iz zakona o kvadratnom reciprocitetu slijedi:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

iz čega slijedi

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1,5 \pmod{12} \\ -1 & p \equiv 3,7,11 \pmod{12} \end{cases}$$

pa p mora biti oblika $12n+1$ ili $12n+5$. Iz $p \mid (x^4 - x^2 + 1)$ takodjer slijedi:

$$x^4 - x^2 + 1 \equiv 0 \pmod p \implies x^4 + 2x^2 + 1 - 3x^2 \equiv 0 \pmod p \implies (x^2+1)^2 \equiv 3x^2 \pmod p$$

Množeći sa $y^2 \equiv y^2 \pmod{p}$ dobivamo:

$$(y(x^2-1))^2 \equiv 3(xy)^2 \equiv 3 \pmod{p}$$

Dakle, vrijedi $\left(\frac{3}{p}\right) = 1$. Kako je po kvadratnom reciprocitetu također:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1,11 \pmod{12} \\ -1 & p \equiv 5,7 \pmod{12} \end{cases}$$

onda p mora biti oblika $12n+1$ ili $12n+11$. Iz ova dva uvjeta za oblik broja p slijedi da je p oblika $12n+1$. Dakle, pronašli smo prost broj p, koji je različit od $p_1, \ldots, p_r$, koji je oblika $12n+1$ čime dolazimo do kontradikcije. □

2.1 Karakteri konačnih Abelovih grupa

Definicija 2.1.1. *Neka je G konačna Abelova grupa. Homomorfizam sa G u multiplikativnu grupu kompleksnih brojeva $\mathbb{C}^*$ nazivamo karakter od G.*

Skup svih karaktera od G tvori grupu, koju zovemo dualom grupe G i označavamo sa $Hom(G, \mathbb{C}^*)$, odnosno $\hat{G}$.

Lema 2.1.2. *Neka je G ciklička grupa reda n. Onda je je $\hat{G}$ takodjer ciklička grupa reda n.*

Dokaz. Neka je g generator od G te χ karakter od G. Kako je χ homomorfizam, onda za $w = \chi(g)$ vrijedi $w^n = 1$ tj. w je n-ti korijen iz jedinice. S druge strane, neka je w n-ti korijen iz jedinice. Za preslikavanje određeno sa $g^a \mapsto w^a$ vrijedi da je karakter od G. Iz ovoga slijedi da je preslikavanje određeno sa $\chi \mapsto \chi(g)$ izomorfizam između $\hat{G}$ i grupe μ_n svih n-tih korijena iz jedinice. Tvrdnja slijedi iz cinjenice da je μ_n ciklička grupa reda n. □

Propozicija 2.1.3. *Neka je H podgrupa od konacne Abelove grupe G. Svaki karakter od H se može proširiti do karaktera od G.*

Dokaz. Dokaz provodimo indukcijom po indeksu H u G. Ako je $[G : H] = 1$ onda je $G = H$ pa tvrdnja slijedi trivijalno. Pretpostavimo da tvrdnja vrijedi za $[G : H] = n - 1$ te neka je K podgrupa od G takva da je $[G : K] = n$. Odaberimo proizvoljan element $x \in G \setminus K$ te označimo sa m najmanji cijeli broj takav da je $x^m \in K$. Neka je χ karakter od K te stavimo $t = \chi(x^m)$. Kako je $\mathbb{C}^*$ djeljiva grupa, onda postoji kompleksan broj w takav da je $w^m = t$. Neka je K' podgrupa od G generirana sa K i x. Svaki element k' od K' se može zapisati u obliku $k' = kx^a$ za neki $k \in K$ te $a \in \mathbb{Z}$. Definiramo funkciju $\chi' : K' \to \mathbb{C}^*$ na sljedeći nacin:

$$\chi'(k') = \chi(k)w^a$$

Trebamo pokazati da je ovo preslikavanje dobro definirano, tj. da ne ovisi o izboru dekompozicije od k'. Neka su $k' = kx^a = jx^b$, gdje su $k, j \in K$ te $a, b \in \mathbb{Z}$, dva različita prikaza od k'. Koristeći činjenicu da je χ homomorfizam računamo:

$$\begin{aligned} 1 &= \chi(1_K)w^0 = \chi'(1_K x^0) = \chi'(1_{K'}) = \chi'(k'(k')^{-1}) = \chi'(kx^a(jx^b)^{-1}) \\ &= \chi'(kj^{-1}x^{a-b}) = \chi(kj^{-1})w^{a-b} = \chi(k)w^a\chi(j^{-1})w^{-b} = \chi(k)w^a\chi(j)^{-1}w^{-b} \end{aligned} \tag{2.1}$$

Dakle vrijedi $\chi(k)w^a = \chi(j)w^b$ pa je χ dobro definirano preslikavanje.

Ova funkcija je očito karakter od K' koji proširuje χ. Kako je K strogo sadrzano u K' onda slijedi da je $[G : K'] < [G : K]$. Sada možemo primjeniti induktivnu pretpostavku i dobivamo karakter od G koji proširuje χ. □

Napomena 2.1.4. *Pomoću restrikcije možemo na očit način definirati preslikavanje $f : \hat{G} \to \hat{H}$. Ako je $\chi \in \hat{H}$, onda po prethodnoj propoziciji postoji karakter od G koji proširuje χ, pa je onda preslikavanje f surjektivno. Jezgra ovog preslikavanja je skup svih karaktera χ od G takvih da je $\chi(h) = 1$ za svaki $h \in H$, iz čega slijedi da je jezgra izomorfna grupi $\widehat{G/H}$. Dakle, sljedeći niz je egzaktan*

$$\{1\} \to \widehat{G/H} \to \hat{G} \to \hat{H} \to \{1\}$$

Propozicija 2.1.5. *Grupa $\hat{G}$ je istog reda kao i grupa G.*

Dokaz. Dokaz provodimo indukcijom po redu grupe G. Ako je G grupa reda 1, onda tvrdnja trivijalno vrijedi. Pretpostavimo da tvrdnja vrijedi za grupe reda $n-1$ te neka je G grupa reda n. Označimo sa H netrivijalnu cikličku podgrupu od G. Po prethodnoj napomeni vrijedi da je red grupe $\hat{G}$ jednak umnošku reda grupe $\hat{H}$ i $\widehat{G/H}$. Kako je H ciklička grupa, onda po lemi 2.1.2 slijedi da je njen red jednak redu grupe $\hat{H}$. Kako je red grupe G/H strogo manji od n, onda po induktivnoj pretpostavci slijedi da je red grupe $\hat{G}$ jednak umnošku reda grupe H i G/H, što je jednako redu grupe G. □

Za proizvoljan $x \in G$ je preslikavanje definirano sa $\chi \mapsto \chi(x)$, koje preslikava sa $\widehat{G}$ u $\mathbb{C}^*$, homomorfizam grupa, pa je time i karakter od $\hat{G}$. Označimo sa $\epsilon(x)$ preslikavanje određeno sa x na ovaj način. Očito vrijedi da je ϵ homomorfizam sa G u $\hat{\hat{G}}$. Štoviše, vrijedi i više:

Propozicija 2.1.6. *Homomorfizam ϵ je izomorfizam između G i $\hat{\hat{G}}$.*

Dokaz. Primjenom prethodne propozicije dobivamo da je red od G jednak redu od $\hat{\hat{G}}$, pa je onda dovoljno dokazati da je preslikavanje ϵ injektivno. Dovoljno je dokazati da za $x \neq 1$ postoji $\chi \in \hat{G}$ takav da je $\chi(x) \neq 1$. Neka je H ciklička grupa koju generira element x. Prema dokazu leme 2.1.2 jasno je da postoji karakter χ od H takav da je $\chi(x) \neq 1$. Prema propoziciji 2.1.3 karakter χ se moze proširiti do karaktera od G. □

Propozicija 2.1.7. *Neka je G grupa reda n i neka je $\chi \in \hat{G}$. Onda vrijedi:*

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \chi = 1 \\ 0 & \chi \neq 1 \end{cases}$$

Dokaz. U slučaju $\chi = 1$ formula očito vrijedi jer G ima n različitih elemenata. Pretpostavimo da je $\chi \neq 1$. Onda postoji element $y \in G$ takav da je $\chi(y) \neq 1$. Slijedi:

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(y)\chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x)$$

Iz prvog i zadnjeg izraza slijedi:

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0$$

Kako je $\chi(y) \neq 1$ onda mora vrijediti:

$$\sum_{x \in G} \chi(x) = 0$$

. □

Primjenom prethodne propozicije na grupu $\hat{G}$ slijedi

Korolar 2.1.8. *Neka je G grupa reda n i $x \in G$. Onda je:*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n & x = 1 \\ 0 & x \neq 1 \end{cases}$$

2.2 Modularni karakteri

Neka je $m \geq 1$ prirodan broj. Sa $G(m)$ označavamo multiplikativnu grupu $(\mathbb{Z}/m\mathbb{Z})^*$ invertibilnih elemenata prstena $\mathbb{Z}/m\mathbb{Z}$. Poznato je da je ovo Abelova grupa reda $\phi(m)$. Element χ duala od $G(m)$ zovemo karakter modulo m. Ovaj karakter možemo promatrati kao funkciju, čija je domena skup svih cijelih brojeva koji su relativno prosti sa m, a kodomena $\mathbb{C}^*$, te za koju vrijedi $\chi(a)\chi(b) = \chi(ab)$. Korisno će nam biti proširiti χ na čitav $\mathbb{Z}$ tako što stavimo da je $\chi(a) = 0$ ako a nije relativno prosto sa m.

Funkciju χ možemo i precizno iskazati. Za $a \in \mathbb{Z}$ vrijedi:

$$\chi(a) = \begin{cases} \chi(k) & (a,m) = 1, \quad a \equiv k \pmod{m} \\ 0 & (a,m) \neq 1 \end{cases}$$

Napomena 2.2.1. *Ako su a i m relativno prosti, onda po Eulerovom teoremu vrijedi:*

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

Pa je onda za $\chi \in \widehat{G(m)}$:

$$1 = \chi(1) = \chi(a^{\phi(m)}) = \chi(a)^{\phi(m)}$$

Primjer 2.2.2. *Za $m = 4$, grupa $G(4)$ je reda $\phi(4) = 2$, pa ima samo jedan netrivijalan karakter, koji je određen sa:*

$$x \mapsto (-1)^{\epsilon(x)}$$

Primjer 2.2.3. *Za $m = p$ gdje je p neparan prost broj, grupa $G(m)$ je ciklička reda $p - 1$, pa ima jedinstven karakter reda 2 koji je određen sa $x \mapsto \left(\frac{x}{p}\right)$ i koji nazivamo Legendreov karakter.*

Primjer 2.2.4. *Za $m = 7$ grupa $G(7)$ je ciklička grupa reda 6, pa ima dva karaktera reda 3. Jedan od njih je zadan sa*

$$\begin{aligned} \chi(x) &= 1 && \text{ako je } x \equiv \pm 1 \ (mod\ 7) \\ \chi(x) &= e^{\frac{2\pi i}{3}} && \text{ako je } x \equiv \pm 2 \ (mod\ 7) \\ \chi(x) &= e^{\frac{4\pi i}{3}} && \text{ako je } x \equiv \pm 3 \ (mod\ 7) \end{aligned}$$

Propozicija 2.2.5. *Neka je $a \neq 0$ kvadratno slobodan cijeli broj i neka je $m = 4|a|$. Onda postoji jedinstven karakter χ_a modulo m takav da vrijede sljedeća svojstva*

i) $\chi_a(p) = \left(\frac{a}{p}\right)$ *za svaki prost broj p koji ne dijeli m*
ii) $\chi_a^2 = 1$
iii) $\chi_a \neq 1$ *ako je* $a \neq 1$

Dokaz. Dokažimo prvo egzistenciju karaktera χ_a. Pretpostavimo da se a može zapisati u obliku $a = p_1 p_2 \cdots p_l$, gdje su $p_1, p_2, ..., p_l$ međusobno različiti neparni prosti brojevi. Stavimo

$$\chi_a(x) = -1^{\epsilon(x)\epsilon(a)} \left(\frac{x}{p_1}\right)\left(\frac{x}{p_2}\right)\cdots\left(\frac{x}{p_l}\right)$$

Ako je p neparan prost broj različit od svih p_i, onda po zakonu kvadratnog reciprociteta za neki paran broj m vrijedi

$$\begin{aligned}
\chi_a(p) &= (-1)^{\epsilon(p)\epsilon(a)} \left(\frac{p}{p_1}\right)\left(\frac{p}{p_2}\right)\cdots\left(\frac{p}{p_l}\right) \\
&= (-1)^{\epsilon(p)\epsilon(a)}(-1)^{\epsilon(p)(\epsilon(p_1)+\epsilon(p_2)+...+\epsilon(p_l))} \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\cdots\left(\frac{p_l}{p}\right) \\
&= (-1)^{\epsilon(p)\epsilon(a)}(-1)^{\epsilon(p)(\epsilon(a)+m)} \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\cdots\left(\frac{p_l}{p}\right) \qquad (2.2) \\
&= \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\cdots\left(\frac{p_l}{p}\right) \\
&= \left(\frac{a}{p}\right)
\end{aligned}$$

Jedinstvenost karaktera x_a slijedi iz činjenice da se svi prosti brojevi koji su međusobno prosti sa m mogu zapisati kao produkt prostih brojeva koji ne dijele m. Iz definicije karaktera x_a je očito da vrijedi tvrdnja *ii*).

Ako je $a \neq 1$, onda odaberimo x takav da je:

$$\left(\frac{x}{p_1}\right) = -1 \quad \text{i} \quad x \equiv 1 \pmod{4p_2 \cdots p_l}$$

Direktnim računom se pokaže da je onda $x_a(x) = -1$. U slučaju da je a oblika $-b$, prikazimo b kao produkt neparnih prostih brojeva kao i prije, te neka je:

$$\chi_a(x) = \chi_b(x) \cdot (-1)^{\epsilon(x)}$$

Na isti način kao u prethodnom slucaju slijedi da je $\chi_a \neq 1$. Analogno se tvrdnja dokaže u slučaju da je a oblika $2b$, odnosno $-2b$, ako stavimo da je

$$\chi_a(x) = \chi_b(x) \cdot (-1)^{\omega(x)} \quad \text{odnosno} \quad \chi_a(x) = \chi_b(x) \cdot (-1)^{\epsilon(x)+\omega(x)}$$

□

2.3 Dirichletovi redovi

Od velike koristi u ovom potpoglavlju bit će nam tzv. Weierstrassov teorem o limesu niza holomorfnih funkcija.

Lema 2.3.1. ***(Weierstrass)*** *Neka je Ω otvoreni podskup od $\mathbb{C}$ i neka je (f_n) niz holomorfnih funkcija sa Ω koje na Ω uniformno konvergiraju nekoj funkciji f. Onda je i funkcija f holomorfna na Ω te niz funkcija f_n' konvergira uniformno na skupu Ω funkciji f'.*

Dokaz. Prema teoremu 1.2.9 je funkcija f neprekidna. Neka je $z \in \Omega$ proizvoljna točka te neka je $r_z > 0$ takav da je kugla $K(z, r_z)$ sadržana u Ω. Tada po Cauchyevom teoremu i teoremu 1.2.6, za svaki pravokutnik sadržan u $K(z, r_z)$ vrijedi

$$\int_{\partial I} f dz = \lim_{n\to\infty} \int_{\partial I} f_n dz = 0$$

Iz teorema 1.2.5 onda slijedi da je f holomorfna na Ω.

Neka je $z_0 \in \Omega$ proizvoljna točka i neka je $r > 0$ takav da je $\overline{K}(z_0, 2r) \subseteq \Omega$. Označimo sa $\Gamma := \partial K(z_0, 2r)$ pozitivno orijentiranu kružnicu. Kako je skup Γ kompaktan, onda niz funkcija (f_n) na Ω konvergira uniformno funkciji f. Slijedi da za svaki $\epsilon > 0$ postoji $n_0 \in \mathbb{N}$ takav da za sve $n \geq n_0$ i sve $\xi \in \Gamma$ vrijedi $|f_n(\xi) - f(\xi)| < \epsilon\frac{r}{2}$. Kako su funkcije $f, f_n, n \in \mathbb{N}$ holomorfne na Ω, prema teoremima 1.2.3 i 1.2.4 za svaki $z \in K(z_0, r)$ vrijedi

$$f'(z) = \frac{1}{2\pi i} \int_\Gamma \frac{f(\xi)}{(\xi - z)^2} d\xi$$

.

$$f_n'(z) = \frac{1}{2\pi i} \int_\Gamma \frac{f_n(\xi)}{(\xi - z)^2} d\xi$$

. Kako za sve $z \in K(z_0, r)$ i sve $\xi \in \Gamma$ vrijedi $|\xi - z| > r$, onda po teoremu 1.2.7 vrijedi

$$|f_n'(z) - f'(z)| = \left| \frac{1}{2\pi i} \int_\Gamma \frac{f_n(\xi) - f(\xi)}{(\xi - z)^2} d\xi \right| < \frac{1}{2\pi} \cdot \epsilon \cdot \frac{r}{2} \cdot \frac{1}{r^2} \cdot 2 \cdot 2r\pi = \epsilon$$

Dakle, (f_n') konvergira uniformno funkciji f' na okolini $K(z_0, r)$ točke z_0 pa slijedi da niz funkcija (f_n') konvergira lokalno uniformno funkciji f'. □

Definicija 2.3.2. *Neka je (λ_n) rastući niz nenegativnih realnih brojeva koji teži beskonačnosti. Onda red oblika*

$$\sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$$

gdje su z i $a_n, n \in \mathbb{N}$ kompleksni brojevi nazivamo Dirichletovim redom.

Primjer 2.3.3. *Za $\lambda_n = n$ dobivamo red potencija:*

$$\sum_{n=1}^{\infty} a_n \left(e^{-z}\right)^n$$

Primjer 2.3.4. *Za $\lambda_n = \ln n$ dobivamo tzv. obični Dirichletov red:*

$$\sum_{n=1}^{\infty} \frac{a_n}{n^z}$$

Ako je pritom i $a_n = 1$, onda dolazimo do tzv. Riemannove Zeta funkcije:

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

Mi ćemo je u ostatku rada zvati samo Zeta funkcija.

Prirodno se postavlja pitanje za koje kompleksne brojeve z Dirichletov red konvergira. Za tu svrhu potrebne su sljedeće dvije leme.

Lema 2.3.5. *Neka su (a_n) i (b_n) nizovi realnih brojeva te za $p, m, m' \in \mathbb{N}$, $p \leq m'$, $m \leq m'$ stavimo*

$$A_{m,p} = \sum_{n=m}^{p} a_n \quad i \quad S_{m,m'} = \sum_{n=m}^{m'} a_n b_n$$

Onda je:

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'}$$

Dokaz. Uvrštavajući $a_n = A_{m,n} - A_{m,n-1}$ dobivamo:

$$\begin{aligned} S_{m,m'} &= \sum_{n=m}^{m'} (A_{m,n} - A_{m,n-1}) b_n \\ &= \sum_{n=m}^{m'} (A_{m,n} b_n - A_{m,n-1} b_n) \\ &= \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'} b_{m'} \end{aligned} \tag{2.3}$$

□

gdje smo u posljednjoj jednakosti grupirali drukčije članove sume.

Lema 2.3.6. *Neka su α i β realni brojevi takvi da je $0 < \alpha < \beta$. Onda za kompleksni broj $z = x + yi$, gdje je $x > 0$ vrijedi:*

$$\left|e^{-\alpha z} - e^{-\beta z}\right| \leq \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x})$$

Dokaz. Vrijedi:

$$e^{-\alpha z} - e^{-\beta z} = z \int_{\alpha}^{\beta} e^{-tz} dt$$

Pa je onda:

$$\begin{aligned} \left|e^{-\alpha z} - e^{-\beta z}\right| &= \left|z \int_{\alpha}^{\beta} e^{-tz} dt\right| \\ &\leq |z| \int_{\alpha}^{\beta} \left|e^{-tx}\right| dt \\ &= |z| \int_{\alpha}^{\beta} e^{-tx} dt \\ &\leq \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x}) \end{aligned} \tag{2.4}$$

□

U ostatku poglavlja, sa $f(z)$ ćemo označavati:

$$f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$$

Propozicija 2.3.7. *Ako Dirichletov red $f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ konvergira za $z = z_0$, onda konvergira uniformno na svakom skupu oblika $\{z \in \mathbb{C} : Re(z - z_0) \geq 0, Arg(z - z_0) \leq \alpha\}$, gdje je $\alpha < \frac{\pi}{2}$.*

Dokaz. Pretpostavimo prvo da je $z_0 = 0$. Pomoću translacije tvrdnja onda vrijedi za općeniti z_0. Uvrštavajući $z = z_0$ u funkciju $f(z)$ dobivamo da red

$$f(z_0) = f(0) = \sum_{n=1}^{\infty} a_n$$

konvergira. Dovoljno je dokazati da konvergira uniformno na svakom skupu oblika $Re(z - z_0) = Re(z) \geq 0$, $\frac{|z|}{Re(z)} \leq k$, gdje je k prirodan broj. Neka je $\epsilon > 0$ proizvoljan. Iz konvergencije reda $f(0)$ slijedi da postoji N takav da ako za prirodne brojeve m, m' vrijedi $m, m' \geq N$

onda je $|A_{m,m'}| \leq \epsilon$. Iz 2.3.5, za $b_n = e^{-\lambda_n z}$ slijedi

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z} +) + A_{m,m'} e^{-\lambda_{m'} z}$$

Uz oznaku $z = x + yi$ iz 2.3.6 slijedi

$$|S_{m,m'}| \leq \epsilon \left(1 + \frac{|z|}{x} \sum_{n=m}^{m'-1} (e^{-\lambda_n x} - e^{-\lambda_{n+1} x})\right)$$

Onda je

$$|S_{m,m'}| \leq \epsilon \left(1 + k(e^{-\lambda_m x} - e^{-\lambda_{m'} x})\right)$$

odnosno

$$|S_{m,m'}| \leq \epsilon\,(1 + k)$$

Dakle, funkcija f uniformno konvergira na navedenom skupu pa slijedi tvrdnja propozicije. □

Korolar 2.3.8. *Ako funkcija f konvergira za $z = z_0$, onda konvergira i za svaki z takav da je $Re(z) > Re(z_0)$ i funkcija f, definirana Dirichletovim redom, je onda holomorfna na tom skupu.*

Dokaz. Tvrdnja slijedi direktno iz teorema te leme 2.3.1. □

Korolar 2.3.9. *Skup konvergencije od f sadrži maksimalnu otvorenu poluravninu.*

Poluravninu iz prethodnog korolara nazivamo poluravnina konvergencije reda. Ako je poluravnina konvergencije zadana sa $Re(z) > \rho$, kažemo da je ρ apscisa konvergencije reda. U slučaju da je poluravnina konvergencije jednaka $\emptyset$, onda apscisu označavmao sa $\rho = +\infty$, a u slučaju da je jednaka $\mathbb{C}$ sa $\rho = -\infty$.

Poluravnina konvergencije za red $\sum |a_n| e^{-\lambda_n z}$ nazivamo poluravnina apsolutne konvergencije od f, te apscisu konvergencije ovoga reda označavamo sa ρ^+.

Korolar 2.3.10. *Za funkciju f iz korolara 2.3.8 vrijedi da $f(z)$ konvergira ka $f(z_0)$, kada z teži ka z_0 na skupu*

$$\{z \in mathbbC : R(z - z_0) \geq 0,\ |Arg(z - z_0)| \leq \alpha,\ \ \alpha < \frac{\pi}{2}\}$$

Dokaz. Iz propozicije direktno slijedi da na navedenoj skupu vrijedi

$$f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z} \to \sum_{n=1}^{\infty} a_n e^{-\lambda_n z_0} = f(z_0)$$

jer svi ovakvi redovi konvergiraju. □

Korolar 2.3.11. *Funkcija f je nul-funkcija ako i samo ako su svi a_n jednaki 0.*

Dokaz. Pretpostavimo da je f nul-funkcija. Pokažimo prvo da je $a_0 = 0$. Vrijedi:

$$\begin{aligned} f(z)e^{\lambda_0 z} &= e^{\lambda_0 z} \sum_{n=1}^{\infty} a_n e^{-\lambda_n z} \\ &= a_0 + \sum_{n=2}^{\infty} a_n e^{-\lambda_n z + \lambda_0 z} \end{aligned} \tag{2.5}$$

Uzmimo da su z realni brojevi, te uzmimo limes kada z teži ka ∞:

$$\lim_{z\to\infty} f(z)e^{\lambda_0 z} = \lim_{z\to\infty} \left(a_0 + \sum_{n=2}^{\infty} a_n e^{-\lambda_n z + \lambda_0 z} \right)$$

onda je

$$\lim_{z\to\infty} f(z)e^{\lambda_0 z} = a_0$$

iz čega slijedi da je $a_0 = 0$. Sasvim analogne se pokaže da je $a_n = 0$ za $n = 1, 2, 3....$ Obratan smjer je trivijalan. □

Propozicija 2.3.12. *Neka je $f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z}$ Dirichletov red za koji vrijedi da je $a_n \geq 0$ za svaki n. Pretpostavimo da f konvergira na skupu $Re(z) \geq \rho$ za $\rho \in \mathbb{R}$ i da se f može proširiti analitički do funkcije koja je holomorfna na nekoj okolini oko tocke $z = \rho$. Onda postoji $\epsilon > 0$ takav da f konvergira na skupu $Re(z) > \rho - \epsilon$.*

Dokaz. Dovoljno je tvrdnju dokazati za $\rho = 0$, opći slučaj onda slijedi preko zamjene z sa $z - \rho$. Kako je funkcija f holomorfna kada je $Re(z) > 0$ i na nekoj okolini od 0, onda je holomorfna i na disku $|z - 1| \leq 1 + \epsilon$, za dovoljno mali $\epsilon > 0$. Iz toga slijedi da Taylorov red funkcije konvergira na tom disku. Iz druge tvrdnje leme 2.3.1 slijedi da je

$$f^{(m)}(z) = \sum_{n=1}^{\infty} a_n (-\lambda_n)^m e^{-\lambda_n z} \quad , Re(z) > 0$$

. Uvrštavajući $z = 1$ dobivamo

$$f^{(m)}(1) = (-1)^m \sum_{n=1}^{\infty} \lambda_n^m a_n e^{-\lambda_n}$$

Taylovor red funkcije f je dan sa

$$f(z) = \sum_{m=0}^{\infty} \frac{1}{m!} (z-1)^m f^{(m)}(1).$$

Ako uvrstimo $z = -\epsilon$ onda je

$$f(-\epsilon) = \sum_{m=0}^{\infty} \frac{1}{m!}(1+\epsilon)^m(-1)^m f^{(m)}(1).$$

Iz prethodnih jednadžbi sada dobivamo

$$\begin{aligned} f(-\epsilon) &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{1}{m!}(1+\epsilon)^m(-1)^m(-1)^m\lambda_n^m a_n e^{-\lambda_n} \\ &= \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a_n\frac{1}{m!}(1+\epsilon)^m\lambda_n^m e^{-\lambda_n} \\ &= \sum_{n=0}^{\infty} a_n e^{-\lambda_n}\sum_{m=0}^{\infty}\frac{1}{m!}(1+\epsilon)^m\lambda_n^m \\ &= \sum_{n=0}^{\infty} a_n e^{-\lambda_n}e^{\lambda_n(1+\epsilon)} \\ &= \sum_{n=0}^{\infty} a_n e^{\lambda_n\epsilon} \end{aligned}$$

Dakle, red $f(z)$ konvergira kada je $z = -\epsilon$, pa po korolaru 2.3.8 konvergira i za sve z takve da je $Re(z) > -\epsilon$. □

Promatrajmo sada obični Dirichletov red iz primjera 2.3.4:

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

Propozicija 2.3.13. *Ako je niz (a_n) ograničen, onda red $f(z)$ apsolutno konvergira na skupu $Re(z) > 1$.*

Dokaz. Neka je $M > 0$ takav da za svaki $n \in \mathbb{N}$ vrijedi $|a_n| \leq M$. Onda je:

$$\sum_{n=1}^{\infty}\left|\frac{a_n}{n^z}\right| \leq M\sum_{n=1}^{\infty}\left|\frac{1}{n^z}\right| < \infty$$

□

U idućoj propoziciji koristimo sume definirane u lemi 2.3.5.

Propozicija 2.3.14. *Ako su sve sume $A_{m,p} = \sum_{n=m}^{p} a_n$ ograničene, onda f konvergira na skupu $Re(z) > 0$.*

Dokaz. Neka je $K > 0$ takav da je $|A_{m,p}| \leq K$ za svaki $m, p \in \mathbb{N}$. Iz leme 2.3.5, za $b_n = n^{-z}$ slijedi da je

$$|S_{m,m'}| \leq K\left(\sum_{n=m}^{m'-1} |n^{-z} - (n+1)^{-z}| + |m'^{-z}|\right)$$

Možemo pretpostaviti da je z realan broj, pa je onda

$$|S_{m,m'}| \leq \frac{K}{m^z}$$

iz čega direktno slijedi konvergencija. □

2.4 L-funkcije

Definicija 2.4.1. *Za funkciju $f : \mathbb{N} \to \mathbb{C}$ kažemo da je multiplikativna ako je $f(1) = 1$ i ako vrijedi*

$$f(mn) = f(m)f(n)$$

za svake $m, n \in \mathbb{N}$, $(m, n) = 1$.

Ako jednakost vrijedi za sve $m, n \in \mathbb{N}$ onda za f kažemo da je strogo multiplikativna.

U ostatku poglavlja sa f ćemo označavati funkciju za koju pretpostavljamo da je multiplikativna i ograničena. Nadalje, P će označavati skup prostih brojeva.

Lema 2.4.2. *Dirichletov red $\sum_{n=1}^{\infty} \frac{f(n)}{n^z}$ konvergira apsolutno na skupu $Re(z) > 1$ i na ovom skupu je jednak*

$$\prod_{p \in P}(1 + f(p)p^{-z} + ... + f(p^m)p^{-mz} + ...)$$

Dokaz. Prva tvrdnja slijedi direktno iz propozicije 2.3.13 jer je f ograničena funkcija.

Neka je S_k konačan skup prostih brojeva manjih od k te neka je $\mathbb{N}(S_k)$ skup svih prirodnih brojeva čiji su prosti faktori sadržani u S_k. Lako se vidi da radi multiplikativnosti funkcije f vrijedi

$$\sum_{n \in \mathbb{N}(S_k)} \frac{f(n)}{n^z} = \prod_{p \in S_k}\left(\sum_{m=0}^{\infty} \frac{f(p^m)}{p^{mz}}\right)$$

Uzimajući limes po k skup $\mathbb{N}(S_n)$ teži ka $\mathbb{N}$ iz čega slijedi ostatak leme. □

Lema 2.4.3. *Ako je f strogo multiplikativna onda vrijedi*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^z} = \prod_{p \in P} \frac{1}{1 - \frac{f(p)}{p^z}}$$

Dokaz. Kako je f strogo multiplikativna, onda za svaki m vrijedi $f(p^m) = f(p)^m$. Iz prethodne leme slijedi

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{f(n)}{n^z} &= \prod_{p\in P}\left(\sum_{m=0}^{\infty} \frac{f(p^m)}{p^{mz}}\right) \\ &= \prod_{p\in P}\left(\sum_{m=0}^{\infty} \left(\frac{f(p)}{p^z}\right)^m\right) \\ &= \prod_{p\in P} \frac{1}{1-\frac{f(p)}{p^z}}\end{aligned} \tag{2.6}$$

□

Promatrajmo sada Zeta funkciju iz primjera 2.3.4

$$\xi(z) = \sum_{n=1}^{\infty} \frac{1}{n^z} = \prod_{p\in P} \frac{1}{1-\frac{1}{p^z}}$$

gdje druga jednakost slijedi vrijedi na skupu $Re(z) > 1$ po lemi 2.4.2. Iz ovoga odmah slijedi da je Zeta funkcija različita od nule na $Re(z) > 1$, te da je na tom skupu holomorfna.

Propozicija 2.4.4. *Postoji funkcija ϕ holomorfna na $Re(z) > 0$ za koju vrijedi*

$$\xi(z) = \frac{1}{z-1} + \phi(z)$$

Dokaz. Primjetimo da vrijedi

$$\frac{1}{z-1} = \int_1^{\infty} t^{-z}dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-z}dt$$

pa je onda

$$\begin{aligned}\xi(z) = = \frac{1}{z-1} &+ \sum_{n=1}^{\infty}\left(\frac{1}{n^z} - \int_n^{n+1} t^{-z}dt\right) \\ = \frac{1}{z-1} &+ \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-z} - t^{-z}dt)\end{aligned} \tag{2.7}$$

Stavimo

$$\phi_n(z) = \int_n^{n+1} (n^{-z} - t^{-z})dt, \qquad \phi(z) = \sum_{n=1}^{\infty} \phi_n(z)$$

Jasno je da su funkcije ϕ_n dobro definirane i holomorfne na skupu $R(z) > 0$. Ako pokažemo da suma $\sum_{n=1}^{\infty} \phi_n(z)$ konvergira normalno na svim kompaktnim podskupovima od $R(z) > 0$, onda će to vrijediti i za funkciju ϕ. Vrijedi:

$$|\phi_n(z)| \leq \sup_{n \leq t \leq n+1} |n^{-z} - t^{-z}|$$

Iz činjenice da je $\frac{s}{t^{s+1}}$ derivacija od $n^{-z} - t^{-z}$ slijedi:

$$|\phi_n(z)| \leq \frac{|z|}{n^{Re(z)+1}}$$

Dakle, suma $\sum_{n=1}^{\infty} \phi_n(z)$ konvergira normalno na skupu $R(z) \geq \epsilon$, za svaki $\epsilon > 0$. □

Direktna posljedica prethodne propozicije je

Korolar 2.4.5. *Zeta funkcija ima jednostavan pol u točki* $z = 1$

Napomena 2.4.6. *Iz prethodnog korolara slijedi da je:*

$$\log \zeta(z) \sim \log \frac{1}{z-1}$$

Korolar 2.4.7. *Kada z teži ka* 1*, onda vrijedi* $\sum_{p \in P} p^{-z} \sim \log \frac{1}{z-1}$*, te suma* $\sum_{p,k \geq 2} p^{-kz}$ *ostaje ograničena.*

Dokaz. Vrijedi:

$$\log \zeta(z) = \sum_{p \in P,\ k \geq 1} \frac{1}{k p^{kz}} = \sum_{p \in P} p^{-z} + \xi(z)$$

gdje je $\xi(z) = \sum_{p \in P} \sum_{k \geq 2} (\frac{1}{kp^{kz}})$. Ova suma je majorirana sa:

$$\sum p^{-kz} = \sum \frac{1}{p^z(p^z - 1)} \leq \sum \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

Dakle, ξ je ograničena, pa iz prethodne napomene slijedi tvrdnja leme.

□

Neka je m prirodan broj i neka je χ karakter mod m. Definiramo Dirichletovu L-funkciju odredjenu sa χ na sljedeći način

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

Kako vrijedi $|\chi(n) n^{-z}| \leq n^{-z}$ onda ovaj red konvergira i funkcija je neprekidna za svaki z takav da je $Re(z) > 1$.

Napomena 2.4.8. *Kako je χ ograničena i strogo multiplikativna funkcija, primjenom leme 2.4.3 dolazimo do sljedeće formule*

$$L(z,\chi) = \prod_{p\in P} \frac{1}{1-\frac{\chi(p)}{p^z}}$$

Propozicija 2.4.9. *Ako je $\chi = 1$, onda vrijedi*

$$L(z,1) = \zeta(z)\prod_{p|m}(1-p^{-z})$$

Posebno, $L(z,1)$ se može proširiti analitički do $Re(z) > 0$ i ima jednostavan pol u $z = 1$.

Dokaz. Kako je $\chi(p) = 0$ za $p \mid m$ onda iz 2.4.3 slijedi:

$$\begin{aligned} L(z,1) &= \prod_{p\nmid m}(1-p^{-z})^{-1} \\ &= \prod_{p|m}(1-p^{-z})\prod_{p}(1-p^{-z})^{-1} \\ &= \xi(z)\prod_{p|m}(1-p^{-z}) \end{aligned} \tag{2.8}$$

□

Propozicija 2.4.10. *Ako je $\chi \neq 1$ onda red $L(z,\chi)$ konvergira apsolutno na skupu $Re(z) > 1$ i konvergira na skupu $Re(z) > 0$.*

Dokaz. Prva tvrdnja slijedi direktno iz leme 2.4.2.

Za dokaz druge tvrdnje, po propoziciji 2.3.14, dovoljno je dokazati da su sume

$$A_{u,v} = \sum_{n=u}^{v}\chi(n)$$

ograničene. Iz propozicije 2.1.7 slijedi da je:

$$\sum_{n=u}^{n=u+m-1}\chi(n) = 0$$

pa je dovoljno majorizirati sume za $u - v < m$. Vrijedi:

$$|A_{u,v}| \leq \phi(m)$$

pa slijedi tvrdnja propozicije. □

Neka je m proizvoljan prirodan broj. Ako je p prost broj koji ne dijeli m, sa $\tilde{p}$ oznacavamo sliku od p u grupi $G(m)$ i sa $f(p)$ njen red. Dakle, $f(p)$ je najmanji cijeli broj veci od 1 takav da je $p^{f(p)} \equiv 1 \pmod{m}$. Označimo sa $g(p)$ red kvocijentne grupe G po $(\tilde{p})$. Onda vrijedi

$$g(p) = \frac{\phi(m)}{f(p)}$$

Lema 2.4.11. *Ako p ne dijeli m, onda za svaki kompleksan broj T vrijedi*

$$\prod_{\chi \in \widehat{G(m)}} (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}$$

Dokaz. Neka je W skup svih $f(p)$-tih korijena iz jedinice. Jednostavnim računom dolazimo do sljedeće jednadžbe:

$$\prod_{w \in W} (1 - wT) = 1 - T^{f(p)}$$

Očito vrijedi da $\tilde{p} \in G(m)$, koji je reda $f(p)$, svaki karakter grupe $G(m)$ preslikava u $f(p)$-ti korijen iz jedinice, što znači da vrijedi $\chi(\tilde{p}) = w$, za neki $w \in W$ i za svaki $\chi \in \widehat{G(m)}$. Kako je grupa $G(m)$ reda $\phi(m)$, a red grupe W je $f(p)$, onda za svaki $w \in W$ postoji $\frac{\phi(m)}{f(p)} = g(p)$ karaktera χ grupe $G(m)$ takvih da vrijedi $\chi(\tilde{p}) = w$. Iz ove činjenice te prethodne jednadžbe onda slijedi:

$$\prod_{\chi \in \widehat{G(m)}} (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}$$

□

Definicija 2.4.12. *Za prirodan broj m definiramo funkciju $\zeta_m(z)$ na sljedeći način:*

$$\zeta_m(z) = \prod_{\chi \in \widehat{G(m)}} L(z, \chi)$$

Propozicija 2.4.13. *Za funkciju ζ_m vrijedi*

$$\zeta_m(z) = \prod_{p \nmid m} \frac{1}{\left(1 - \frac{1}{p^{f(p)z}}\right)^{g(p)}}$$

Dokaz. Funkciju ζ_m možemo pomoću napomene 2.4.8 zapisati na sljedeći način:

$$\begin{aligned}\zeta_m &= \prod_{\chi\in\widehat{G(m)}}\prod_{p\in P}\frac{1}{1-\frac{\chi(p)}{p^z}}\\ &= \prod_{\chi\in\widehat{G(m)}}\prod_{p\nmid m}\frac{1}{1-\frac{\chi(p)}{p^z}}\\ &= \prod_{p\nmid m}\prod_{\chi\in\widehat{G(m)}}\frac{1}{1-\frac{\chi(p)}{p^z}}\\ &= \prod_{p\nmid m}\frac{1}{\left(1-\frac{1}{p^{f(p)z}}\right)^{g(p)}}\end{aligned} \tag{2.9}$$

gdje je u pretposljednjem koraku iskorištena lema 2.4.11 sa $T = p^{-z}$. □

Teorem 2.4.14. *Ako je $\chi \neq 1$, onda je $L(1, z) \neq 0$.*

Dokaz. Pretpostavimo suprotno, neka je $\chi \neq 1$ karakter takav da vrijedi $L(1,\chi) = 0$. Onda je funkcija ζ_m holomorfna u tocki $z = 1$, pa onda i na skupu $Re(z) > 0$. Kako je ζ_m Dirichletov red sa pozitivnim koeficijentima, onda po propoziciji 2.3.12 slijedi da konvergira na tom istom skupu. Međutim, za faktore od ζ_m iz prethodne propozicije vrijedi:

$$\frac{1}{\left(1-\frac{1}{p^{f(p)z}}\right)^{g(p)}} = (1 + p^{-f(p)z} + p^{-2f(p)z} + \dots)^{g(p)}$$

Kako je $\phi(m) \geq f(p)$, onda je $-f(p)z \geq -\phi(m)$ te je $g(p) \geq 1$. Iz ovoga slijedi da prethodni red dominira red

$$1 + p^{-\phi(m)z} + p^{-2\phi(m)z} + \dots$$

pa slijedi da su svi koeficijenti od ζ_m veći od koeficijenata reda

$$\sum_{(n,m)=1} n^{-\phi(m)z}$$

Ovaj red divergira za $z = \frac{1}{\phi(m)}$, što je u kontradikciji sa činjenicom da ζ_m konvergira na skupu $Re(z) > 0$ □

Korolar 2.4.15. *Funkcija ζ_m ima jednostavan pol u točki $z = 1$.*

Dokaz. Tvrdnja slijedi direktno iz teorema i činjenice da ζ ima jednostavan pol u $z = 1$. □

2.5 Gustoća i Dirichletov teorem

U ovom potpoglavlju ćemo konačno dokazati Dirichletov teorem. U tu svrhu, definiramo pojam Dirichletove gustoće:

Definicija 2.5.1. *Neka je A podskup od P. Kažemo da je broj k (Dirichletova) gustoća skupa A ako limes*

$$\lim_{z\to 1} \frac{\sum_{p\in A} \frac{1}{p^z}}{\sum_{p\in P} \frac{1}{p^z}}$$

postoji i jednak je k.

Za gustoću skupa k očito vrijedi da je $0 \leq k \leq 1$.

Napomena 2.5.2. *Ako gustoća skupa $A \subset P$ postoji, onda je po korolaru 2.4.7 $\sum_{p\in P} p^{-z} \sim \log \frac{1}{z-1}$, pa slijedi da je*

$$k = \lim_{z\to 1} \frac{\sum_{p\in A} \frac{1}{p^z}}{\log \frac{1}{z-1}}$$

Definicija 2.5.3. *Za $\chi \in G(m)$ definiramo $f_\chi(z)$ na sljedeći način*

$$f\chi(z) = \sum_{p\nmid m} \frac{\chi(p)}{p^z}$$

gdje je $z > 1$.

Lema 2.5.4. *Ako je $\chi = 1$ onda je $f_\chi \sim \log \frac{1}{z-1}$.*

Dokaz. Vrijedi

$$f_1(z) = \sum_{p\nmid m} \frac{1}{p^z}$$

Tvrdnja vrijedi iz napomene 2.4.6 i činjenice da se $f_1(z)$ dobije iz $\sum_{p\in P} \frac{1}{p^z}$ uklanjanjem konačno mnogo članova sume. □

Za dokaz sljedeće leme trebati će nam logaritam L-funkcije. Potrebno je prvo pojasniti što točno "logaritam" znači u ovom kontekstu. Za $\alpha \in \mathbb{C}$ takav da je $|\alpha| < 1$ definiramo logaritam od $(1-\alpha)^{-1}$ na sljedeći način

$$\log \frac{1}{1-\alpha} = \sum_{n=1}^{\infty} \frac{\alpha^n}{n}$$

Pokazali smo da vrijedi $L(s,\chi) = \prod_{p\in P}(1-\chi(p)p^{-s})^{-1}$ pa onda definiramo logaritam od $L(z,\chi)$ na sljedeći način

$$\begin{aligned}\log L(z,\chi) &= \sum_{p\in P}\log\frac{1}{1-\chi(p)p^{-z}}\\ &= \sum_{n\in\mathbb{N},p\in P}\frac{\chi(p)^n}{np^{nz}}\end{aligned} \tag{2.10}$$

Nadalje, ako označimo

$$F_\chi(z) = \sum_{n\geq 2,p}\frac{\chi(p)^n}{np^{nz}}$$

onda prethodni logaritam možemo zapisati na sljedeći način

$$\log L(s,\chi) = f_\chi + F_\chi$$

Lema 2.5.5. *Ako je $\chi \neq 1$, onda $f_\chi(z)$ ostaje ograničeno kada $z \to 1$.*

Dokaz. Iz teorema 2.4.14 te korolara 2.4.7 slijedi da $\log L(s,\chi)$ i $F_\chi(z)$ ostaju ograničeni kada z teži ka 1. Tvrdnja leme slijedi iz prethodne jednakosti. □

Označimo sa P_a skup svih prostih brojeva p za koje vrijedi $p \equiv a \pmod m$.

Lema 2.5.6. *Za P_a vrijedi*

$$\sum_{p\in P_a}\frac{1}{p^z} = \frac{1}{\phi(m)}\sum_{\chi\in\widehat{G(m)}}\chi(a)^{-1}f_\chi(z)$$

Dokaz. Po korolaru 2.1.8 vrijedi da je $\sum_\chi \chi(a^{-1}p)$ jednako $\phi(m)$ ukoliko je $a^{-1}p \equiv 1 \pmod m$, a 0 u suprotnom. Iz toga slijedi

$$\begin{aligned}\sum_{\chi\in\widehat{G(m)}}\chi(a)^{-1}f_\chi(z) &= \sum_{\chi\in\widehat{G(m)}}\chi(a^{-1})\sum_{p\nmid m}\frac{\chi(p)}{p^z}\\ &= \sum_{\chi\in\widehat{G(m)}}\sum_{p\nmid m}\frac{\chi(a^{-1})\chi(p)}{p^z}\\ &= \sum_{\chi\in\widehat{G(m)}}\sum_{p\nmid m}\frac{\chi(a^{-1}p)}{p^z}\\ &= \phi(m)\sum_{p\in P_a}\frac{1}{p^z}\end{aligned} \tag{2.11}$$

□

Teorem 2.5.7. *Neka je $m \geq 1$ i neka je a prirodan broj takav da je su a i m relativno prosti. Označimo sa P_a skup svih prostih brojeva p za koje vrijedi $p \equiv a \pmod{m}$. Onda je gustoca skupa P_a jednaka $\frac{1}{\phi(m)}$.*

Dokaz. Ako je $\chi = 1$, onda je po lemi 2.5.5 f_χ ostaju ograničene, a ako je $f_\chi = 1$, onda je po lemi 2.5.4 $f_\chi(z) \sim \log \frac{1}{z-1}$. Iz leme 2.5.6 onda slijedi da je

$$\sum_{p \in P_a} \frac{1}{p^z} \sim \frac{1}{\phi(m)} \log \frac{1}{z-1}$$

Uvrštavajući u definiciju gustoće dobivamo da je gustoća od P_a jednaka $\frac{1}{\phi(m)}$. □

Korolar 2.5.8. *Skup P_a je beskonačan.*

Dokaz. Pretpostavimo suprotno, neka je P_a konačan skup. Onda vrijedi

$$k = \lim_{z \to 1} \frac{\sum_{p \in P_a} \frac{1}{p^z}}{\sum_{p \in P} \frac{1}{p^z}} = 0$$

sto je u kontradikciji sa prethodnim teoremom. Dakle, skup P_a je beskonačan. □

2.6 Primjena Dirichletovog teorema

Za kraj, iskoristiti ćemo Dirichletov teorem da dokažemo bitan teorem o distribuciji prostih brojeva sa obzirom na Legendrov simbol $\left(\frac{a}{p}\right)$.

Lema 2.6.1. *Za svaki prirodan broj a vrijedi da ako je $p \equiv 4a \pmod{4a}$ onda je $\left(\frac{a}{p}\right) = 1$*

Dokaz. Dokaz provodimo indukcijom po $|a|$. U slučaju kada je $a = 1$ tvrdnja očito vrijedi, a u slučaju $a = -1$ slijedi iz formule $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Ako je $|a| > 1$, onda postoji prost djelitelj q od a. Neka je a' prirodan broj takav da je $a = qa'$. Slijedi da je:

$$\left(\frac{a}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{a'}{p}\right)$$

Kako je $|a'| < |a|$ i $p \equiv 1 \pmod{4a'}$, onda po induktivnoj pretpostavci slijedi da je $\left(\frac{a'}{p}\right) = 1$. Također, vrijedi $p \equiv 1 \pmod{4q}$. Ako je $q = 2$ onda je $p \equiv 1 \pmod{8}$, pa slijedi $\left(\frac{q}{p}\right) = \left(\frac{2}{p}\right) = 1$. U suprotnom, ako je q neparan, onda vrijedi:

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

Iz $p \equiv 1 \pmod 4$ slijedi $(-1)^{\frac{p-1}{2}} = 1$, dok iz $p \equiv 1 \pmod q$ slijedi $\left(\frac{p}{q}\right) = 1$. Uvrštavajući u prethodnu jednadžbu dobivamo $\left(\frac{q}{p}\right) = 1$. Konačno, vrijedi:

$$\left(\frac{a}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{a'}{p}\right) = 1$$

□

Teorem 2.6.2. *Za svaki cijeli broj a, različit od nule, koji nije potpuni kvadrat postoji beskonačno mnogo neparnih prostih brojeva p takvih da je* $\left(\frac{a}{p}\right) = -1$.

Dokaz. Pretpostavimo prvo da je a kvadratno slobodan. ako je $a = -1$, onda iz Dirichletovog teorema slijedi da postoji beskonačno mnogo prostih brojeva oblika $4n + 3$, tj. prostih brojeva p za koje je $p \equiv 3 \pmod 4$. Ako je $a \neq -1$, onda a ima prosti faktor q. Neka je a' cijeli broj takav da je $a = qa'$. Očito je $(q, a') = 1$. Ako je a neparan, odaberimo cijeli broj x takav da $x \pmod q$ nije kvadrat niti jednog cijelog broja. Po Kineskom teoremu o ostatcima, postoji cijeli broj y takav da je

$$y = \begin{cases} x & \pmod q \\ 1 & \pmod{4a'} \end{cases}$$

te iz $(x, q) = 1$ slijedi da je $(y, 4qa') = 1$. Po Dirichletovom teoremu, postoji beskonačno mnogo prostih brojeva p takvih da je $p \equiv y \pmod{4a}$. Također, za svaki takav p vrijedi:

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

Vrijedi da je $p \equiv 1 \pmod 4$, pa je $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1$. Također vrijedi da je $\left(\frac{p}{q}\right) = \left(\frac{x}{q}\right) = -1$ te iz $p \equiv 1 \pmod{4a'}$ slijedi da je $\left(\frac{a'}{p}\right) = 1$. Dakle, vrijedi:

$$\left(\frac{a}{p}\right) = (1)(-1)(1) = -1$$

Ako je a paran, stavimo da je $q = 2$. Iz činjenice da je a kvadratno slobodan, slijedi da je a' neparan. Po Kineskom teoremu o ostacima, postoji cijeli broj m takav da je:

$$m = \begin{cases} 5 & \pmod 8 \\ 1 & \pmod{a'} \end{cases}$$

te je $(m, 8a') = 1$. Po Dirichletovom teoremu, postoji beskonačno mnogo prostih brojeva p takvih da je $p \equiv m \pmod{4a}$. Za svaki takav p, vrijedi

$$\left(\frac{a}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{a'}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a'}{p}\right)$$

Iz $p \equiv 5 \pmod 8$ slijedi $\left(\frac{2}{p}\right) = -1$. Kako je $p \equiv 1 \pmod 4$ i $p \equiv 1 \pmod{a'}$, vrijedi da je $p \equiv 1 \pmod{4a'}$, pa je $\left(\frac{a'}{p}\right) = 1$. Dakle, vrijedi $\left(\frac{a}{p}\right) = (-1)(1) = -1$.

Ako a nije kvadratno slobodan, onda vrijedi da je $a = bc^2$, gdje je b kvadratno slobodan te je $b \neq 1$. Slijedi da je:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{c}{p}\right)^2$$

Ako p ne dijeli c, onda vrijedi $\left(\frac{c}{p}\right)^2 = 1$ i $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Iz prethodnog slučaja, za sve neparne p koji zadovoljavaju odredjenu kongruenciju mod $4b$, vrijedi $\left(\frac{b}{p}\right) = -1$. Iz Dirichletovog teorema slijedi da ovakvih p postoji beskonačno mnogo, i beskonačno mnogo ih ne dijeli c. Za takve p, vrijedi $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$.

□

Korolar 2.6.3. *Za cijeli broj a, različit od nule, vrijedi da je potpuni kvadrat ako i samo ako vrijedi* $\left(\frac{a}{p}\right) = 1$ *za sve osim za konačno mnogo neparnih prostih brojeva p.*

Dokaz. Ako a nije potpuni kvadrat, onda po teoremu slijedi da postoji beskonačno mnogo neparnih prostih brojeva p takvih da je $\left(\frac{a}{p}\right) = 1$. Po principu kontrapozicije onda vrijedi da ako je $\left(\frac{a}{p}\right) = 1$ za sve osim konačno mnogo neparnih prostih brojeva p, onda je a savršen kvadrat.
Obratno, pretpostavimo da je a savršen kvadrat. Onda je $a = k^2$ za neki cijeli broj k i vrijedi:

$$\left(\frac{a}{p}\right) = \left(\frac{k^2}{p}\right) = \left(\frac{k}{p}\right)^2$$

Ako p ne dijeli a, onda očito p ne dijeli k, pa je onda:

$$\left(\frac{a}{p}\right) = \left(\frac{k}{p}\right)^2 = (\pm 1)^2 = 1$$

□

Bibliografija

[1] L. J. Goldstein, *Analytic Number Theory*, Prentice-Hall, Inc., New Jersey, 1971.

[2] H. Kraljević S. Kurepa, *Matematička analiza* 4. *Kompleksne funkcije*, Tehnička knjiga, Zagreb, 1979.

[3] J. P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.

[4] H. Shapiro, *On primes in arithmetic progression*, Annals of Mathematics **52** (1950), br. 1, 231–243.

[5] Š. Ungar, *Matematička analiza u* $\mathbb{R}^n$, Golden Marketing - Tehnička knjiga, Zagreb, 2005.

Sažetak

U radu se proučavaju prosti brojevi u aritmetičkim nizovima. Glavni cilj rada je pokazati koji artimetički nizovi sadrže beskonačno mnogo prostih brojeva. U prvom poglavlju, navesti ćemo osnovne definicije i dokaze iz polja algebre, teorije brojeva i kompleksne analize, koji će nam trebati u ostatku rada. U drugom poglavlju cilj nam je dokazati Dirichletov teorem o prostim brojevima, koji govori da aritmetički niz $ak+m$, $k \in \mathbb{N}$ sadrži beskonačno mnogo prostih brojeva ukoliko su a i m relativno prosti. U ovom poglavlju, prvo ćemo razmotriti nekoliko aritmetičkih nizova, za koje je jednostavno pokazati da sadrže beskonačno mnogo prostih brojeva. Zatim ćemo uvesti pojam Karaktera konačne Abelove grupe, Dirichletovih redova, L-funkcija i Dirichletove gustoće, koji će nam biti potrebni da onda dokažemo Dirichletov teorem. Na kraju, navesti ćemo primjenu Dirichletovog teorema u teoriji brojeva.

Summary

In this thesis we examine prime numbers in arithmetic progressions. The main purpose of the thesis is to show which arithmetic progressions contain infinitely many prime numbers. In the first chapter, we will state definitions and theorems from the fields of algebra, number theory and complex analysis, which we will use in the rest of the thesis. In the second chapter, our goal is to prove Dirichlet's theorem on arithmetic progression, which states that the arithmetic progression $ak + m$, $k \in \mathbb{N}$, contains infinitely many primes if a and m are relatively prime. In this chapter, we will first consider a few arithmetic progressions, for which it is easy to show that they contain infinitely many primes. Next, we will introduce the ideas of group characters, Dirichlet series, L-functions and Dirichlet density, which we will then use to prove Dirichlet's theorem. Finally, we will show an application of Dirichlet's theorem in number theory.

Životopis

Rođen sam 10. prosinca 1994. godine u Mostaru u Bosni i Hercegovini. Osnovnu školu završio sam u Mostaru. Nakon završetka osnovne škole, upisao sam srednju školu Gimnazija Mostar. Godine 2013. upisao sam preddiplomski studij matematike na Fakultetu prirodoslovno-matematičkih i odgojnih znanosti u Mostaru. Po završetku, upisao sam diplomski studij Matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu.