Prosti brojevi u aritmetičkim nizovima

Kasum, Iva

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Iva Kasum

PROSTI BROJEVI U ARITMETIČKIM NIZOVIMA

Diplomski rad

Voditelj rada:
prof. dr. sc. Marko Tadić

Zagreb, veljača 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. _____

Zahvaljujem svom mentoru prof. dr. sc. Marku Tadiću na zanimljivoj temi, pomoći, te velikom razumijevanju i strpljenju. Također, veliko hvala obitelji i prijateljima koji su mi pružali podršku tijekom pisanja ovog rada, a posebno Dinki Mahovac, koja je svojim poticanjem i bezuvjetnom podrškom nemjerljivo pomogla u njegovom nastanku.

Sadržaj

Uvod

Glavni cilj ovog rada je dokaz Dirichletovog teorema o prostim brojevima u aritmetičkim nizovima, koji nam govori da prostih brojeva u aritmetičkom nizu oblika $a + km$, $k \in \mathbb{N}_0$, ima beskonačno mnogo ako su a i m relativno prosti. Taj dokaz bit će proveden metodama analitičke teorije brojeva, koja koristi metode iz matematičke analize za rješavanje problema u vezi cijelih brojeva. U prva dva poglavlja ovog rada za rješavanje takvih problema upotrebljavat ćemo, za razliku od toga, algebarske metode, pa ćemo tako vidjeti koje su glavne razlike u ta dva pristupa, te koje su prednosti jednih, a koje drugih metoda.

U prvom poglavlju bavit ćemo se konačnim poljima, odrediti im strukturu, te promotriti neka njihova svojstva, kao i vidjeti kakav je kardinalitet skupa zajedničkih nultočaka određenih skupova polinoma nad konačnim poljem. Također, uvest ćemo pojam Legendreovog simbola, koji će nam biti potreban pri dokazivanju najvažnijeg rezultata ovog poglavlja, Gaussovog zakona kvadratnog reciprociteta. Pomoću tog zakona određujemo ima li neka kvadratna jednadžba, promatrana modulo p (gdje je p prost broj), rješenje, što nam je u mnogim situacijama važno znati.

U drugom poglavlju objekt našeg promatranja bit će p-adska polja, pri čemu je p također prost broj. Vidjet ćemo što je prsten p-adskih cijelih brojeva, $\mathbb{Z}_p$, kao i polje njegovih razlomaka, $\mathbb{Q}_p$. Nakon toga ćemo se pozabaviti rješavanjem jednadžbi čiji su koeficijenti p-adski cijeli brojevi, tj. pokazivanjem kako se od rješenja modulo p^n dolazi do pravog rješenja takve jednadžbe, s koeficijentima u $\mathbb{Z}_p$.

Dok smo u prva dva poglavlja na spomenutim temama ilustrirali primjenu algebarskih metoda na rješavanje problema vezanih uz cijele brojeve, u trećem poglavlju ćemo se baviti karakterima konačnih Abelovih grupa, koje ćemo koristiti pri dokazivanju Dirichletovog teorema. Prvo ćemo proučiti osnovna svojstva karaktera neke konačne Abelove grupe G, kao i grupu karaktera te grupe, $\hat{G}$. Zatim ćemo se posvetiti modularnim karakterima, tj. karakterima grupe $G(m) = (\mathbb{Z}/m\mathbb{Z})^*$, gdje je $m \in \mathbb{N}$, koji će nam trebati pri definiranju L-funkcija, funkcija koje imaju ključnu ulogu u dokazu Dirichletovog teorema.

Konačno, u završnom poglavlju dokazujemo Dirichletov teorem, i to u jačoj verziji, koja nam govori da su prosti brojevi asimptotski jednako distribuirani između različitih klasa kongruencije modulo m koje sadrže a-ove relativno proste sa m, tj. da je gustoća odgovarajućeg skupa $\mathbb{P}_a$ (čiji su elementi prosti brojevi p za koje vrijedi $p \equiv a \ (mod\ m)$)

jednaka $\frac{1}{\phi(m)}$; njen je korolar verzija izrečena na početku ovog uvoda. Pri dokazivanju se služimo metodama analitičke teorije brojeva, koja se počela razvijati Dirichletovim uvođenjem L-funkcija u svrhu dokazivanja baš ovog teorema, tj. korištenjem koncepata matematičke analize pri rješavanju algebarskog problema. U dokazu koristimo i Eulerov rad, povezujući Riemannovu zeta funkciju s distribucijom prostih brojeva. Na početku poglavlja promatramo Dirichletove redove, koji će nam trebati za definiranje i proučavanje zeta funkcije (veoma bitne u analitičkoj teoriji brojeva), odnosno L-funkcija. Zatim dokazujemo jednu od ključnih stvari u dokazu Dirichletovog teorema, činjenicu da zeta funkcija ima jednostavni pol u $s = 1$, te nakon toga esencijalnu tvrdnju u ovom dokazu, činjenicu da je $L(1,\chi)$ različito od nule za nejedinične karaktere χ od $G(m)$, gdje je $m \in \mathbb{N}$ fiksiran. Nakon što uvedemo pojam (analitičke) gustoće nekog podskupa skupa prostih brojeva, imamo sve potrebno za završetak dokaza našeg teorema, kojeg potom i dajemo. Na kraju rada još ćemo navesti neke posljedice i primjene tog teorema, kao i analogne rezultate za druge tipove jednadžbi, te ćemo spomenuti pojam prirodne gustoće.

Poglavlje 1

Konačna polja

U početnom poglavlju pokazat ćemo da su sva konačna polja sa $q = p^f$ elemenata (pri čemu je p prost broj) izomorfna polju $\mathbb{F}_q$, skupu korijena polinoma $X^q - X$, dati neka svojstva takvih polja i uvesti pojam Legendreovog simbola koji nam govori je li neki element kvadrat u promatranom polju. Na kraju poglavlja ćemo dokazati Gaussov zakon kvadratnog reciprociteta pomoću kojeg određujemo ima li neka kvadratna jednadžba, promatrana modulo p, rješenje.

Za sva polja promatrana u ovom poglavlju uzimamo da su komutativna.

1.1 Osnovne činjenice

Neka je K polje. Slika od $\mathbb{Z}$ pri preslikavanju $z \mapsto z \cdot 1_K$ (gdje je 1_K jedinični element u K), tj. slika od $\mathbb{Z}$ u K, je integralna domena, dakle izomorfna ili sa $\mathbb{Z}$ ili sa $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, pri čemu je p prost broj. U prvom slučaju kažemo da je karakteristika polja K, char(K), jednaka 0, a u drugom da je K karakteristike p, i tada je p najmanji prirodni broj koji pomnožen s jedinicom daje nulu.

Ako je K konačno polje, iz gore navedenog vidimo da je tada njegova karakteristika prosti broj p. Označimo li sa f stupanj proširenja $K/\mathbb{F}_p$ jasno je da je card(K)=p^f. Označimo taj broj sa q.

Teorem 1.1.1. *Sva konačna polja sa q elemenata su izomorfna polju $\mathbb{F}_q$, polju razlaganja polinoma $X^q - X$.*

Dokaz. Neka je Ω algebarski zatvoreno polje karakteristike p. Pokazat ćemo da postoji jedinstveno potpolje od Ω koje ima q elemenata i da je ono upravo polje $\mathbb{F}_q$.

Lako se vidi da je preslikavanje $\sigma : x \mapsto x^p$ automorfizam od Ω, pa je onda i preslikavanje $x \mapsto x^q$ automorfizam od Ω (jednako je σ^f). Prema tome, $x \in \Omega$ koji su invarijantni za

to preslikavanje (tj. koji se preslikavaju sami u sebe, odnosno takvi da vrijedi $x^q = x$) čine potpolje od Ω. Ti elementi su korijeni polinoma $X^q - X$, pa je to potpolje $\mathbb{F}_q$. Derivacija tog polinoma jednaka je

$$qX^{q-1} - 1 = p \cdot p^{f-1}X^{q-1} - 1 = 0 - 1 = -1 \neq 0. \tag{1.1}$$

S obzirom da je Ω algebarski zatvoreno, to povlači da promatrani polinom ima q različitih korijena, tj. card($\mathbb{F}_q$)=q.

Obratno, ako je K potpolje od Ω kardinaliteta q, K^*(multiplikativna grupa koja se sastoji od nenul elemenata iz K) ima $q-1$ elemenata. Prema tome, za $x \in K^*$ vrijedi $x^{q-1} = 1$, tj. $x^q = x$, a ta jednakost vrijedi i za nulu, pa vrijedi za svaki $x \in K$, što povlači da su svi elementi iz K korijeni polinoma $X^q - X$. Dakle, $K \subseteq \mathbb{F}_q$. Kako je card(K)=card($\mathbb{F}_q$)=q, zaključujemo da je $K = \mathbb{F}_q$, čime je početna tvrdnja dokazana.

Sva polja sa q elemenata mogu se uložiti u Ω (jer je algebarski zatvoreno) pa iz gore dokazanog dobivamo da je svako takvo polje izomorfno sa $\mathbb{F}_q$, što je i trebalo dokazati. □

Proučimo sada $\mathbb{F}_q^*$, multiplikativnu grupu od $\mathbb{F}_q$.

Definicija 1.1.2. *Eulerova ϕ funkcija za prirodni broj d jednaka je broju prirodnih brojeva manjih ili jednakih d koji su relativno prosti s njime.*

Očigledno je da su slike takvih brojeva u $\mathbb{Z}/d\mathbb{Z}$ generatori te grupe iz čega je vidljivo da je broj generatora cikličke grupe reda d jednak $\phi(d)$ (to je ujedno i broj invertibilnih elemenata te grupe).

Teorem 1.1.3. *$\mathbb{F}_q^*$ je ciklička grupa reda $q-1$.*

Za dokaz ovog teorema bit će nam potrebna sljedeća lema.

Lema 1.1.4. *Neka je H konačna grupa reda n. Pretpostavimo da za sve djelitelje d od n skup $x \in H$ takvih da je $x^d = 1$ ima najviše d elemenata. Tada je H ciklička grupa.*

Dokaz. Neka je d djelitelj od n. Pokazat ćemo da postoji $x \in H$ reda d, za svaki takav d.

Ako je x reda d, tada je podgrupa $(x) = \{1, x, ..., x^{d-1}\}$ ciklička reda d, tj. svi njeni elementi potencirani s d daju 1. Tada po pretpostavci svi $y \in H$ takvi da je $y^d = 1$ moraju biti u (x). Posebno, svi elementi iz H reda d su generatori od (x), a njih ima $\phi(d)$. Prema tome, elemenata grupe H reda d ima ili 0 ili $\phi(d)$.

Sada iz formule

$$n = \sum_{d|n} \phi(d) \tag{1.2}$$

vidimo da ne postoji d takav da elemenata reda d u H ima nula jer bi u suprotnom broj elemenata grupe H bio manji od n. Dakle, za svaki d djelitelj od n postoji element iz H reda d.

Posebno, postoji $x \in H$ reda n pa je H zapravo jednaka cikličkoj grupi (x), čime je lema dokazana. □

Teorem sad direktno slijedi iz upravo dokazane leme, primijenjene na $H = \mathbb{F}_q^*$ i $n = q-1$. Očigledno je da je pretpostavka leme zadovoljena, jer polinom $X^d - 1$, koji je stupnja d, nema više od d korijena u $\mathbb{F}_q$.

1.2 Jednadžbe nad konačnim poljima

U ovom potpoglavlju dokazat ćemo teorem o kardinalitetu skupa zajedničkih nultočaka određenih skupova polinoma nad konačnim poljem K.

I sada je q potencija prostog broja p, a K je polje kardinaliteta q.

Promotrimo prvo sume potencija elemenata iz K. Definiramo:

$$S(X^u) = \sum_{x \in K} x^u, \tag{1.3}$$

gdje je $u \in \mathbb{N}_0$. Po dogovoru, $x^0 = 1$, za sve $x \in K$.

Lema 1.2.1. *$S(X^u)$ je jednako -1 ako je $u \geq 1$ i djeljiv s $q-1$, a 0 inače.*

Dokaz. Promatramo 3 slučaja:

1. $u = 0$
Svi članovi sume su jednaki 1 pa je $S(X^u) = card(K) = q = p \cdot p^{f-1} = 0$.

2. $u \geq 1$ i djeljiv s $q-1$
Imamo $0^u = 0$ i $x^u = 1$ za $x \neq 0$ (jer je u djeljiv s $q-1$, a K^* ima $q-1$ elemenata). Prema tome, $S(X^u) = 0 + (q-1) \cdot 1 = q - 1 = p \cdot p^{f-1} - 1 = -1$.

3. $u \geq 1$ i nije djeljiv s $q-1$
Iz činjenice da je K^* ciklička reda $q-1$ (teorem 1.1.3) zaključujemo da postoji $y \in K^*$ takav da je $y^u \neq 1$. Sada imamo:

$$S(X^u) = \sum_{x \in K^*} x^u = \sum_{x \in K^*} y^u x^u = y^u S(X^u), \tag{1.4}$$

tj.

$$(1 - y^u)S(X^u) = 0. \tag{1.5}$$

Kako je $y^u \neq 1$, slijedi da je $S(X^u) = 0$. □

Sada ćemo dokazati da je broj zajedničkih nultočaka u K^n skupa polinoma u n varijabli nad K čiji je zbroj stupnjeva manji od n djeljiv s p, tj. preciznije:

Teorem 1.2.2. *Neka su $f_\alpha \in K[X_1, \ldots, X_n]$ polinomi u n varijabli takvi da vrijedi $\sum_\alpha st\ f_\alpha < n$ i neka je V skup njihovih zajedničkih nultočaka u K^n. Tada vrijedi:*

$$card(V) \equiv 0 \pmod p. \tag{1.6}$$

Dokaz. Definirajmo polinom P na sljedeći način:

$$P = \prod_\alpha (1 - f_\alpha^{q-1}). \tag{1.7}$$

Pokazat ćemo da je P zapravo karakteristična funkcija skupa V.

Neka je $x \in K^n$. Ako je $x \in V$, tj. x je zajednička nultočka svih polinoma f_α, svi $1 - f_\alpha^{q-1}(x)$ su jednaki 1 pa je i $P(x) = 1$. Ako $x \notin V$, barem jedan od izraza $f_\alpha(x)$ nije 0 pa je dakle za njega $f_\alpha^{q-1}(x) = 1$ (jer je K^* reda $q - 1$), odnosno $1 - f_\alpha^{q-1}(x) = 0$. Prema tome, u tom slučaju je $P(x) = 0$, i P je doista karakteristična funkcija od V.

Stavimo sada $S(f) = \sum_{x \in K^n} f(x)$, za svaki polinom f. Imamo:

$$S(P) = \sum_{x \in K^n} P(x) = \sum_{x \in V} P(x) + \sum_{x \notin V} P(x) = \sum_{x \in V} 1 \equiv card(V) \pmod p. \tag{1.8}$$

Dakle, da dokažemo tvrdnju teorema trebamo pokazati da je $S(P) = 0$.

Vidimo da je $st\ P = \sum_\alpha st\ f_\alpha \cdot (q-1) < n(q-1)$. Iz toga slijedi da je P linearna kombinacija monoma oblika $X_1^{u_1} \ldots X_n^{u_n}$, pri čemu je $\sum_{i=1}^n u_i < n(q-1)$ pa je dovoljno pokazati da za takav monom X^u vrijedi $S(X^u) = 0$.

Ako su svi $u_i \geq q - 1$, onda je $\sum_{i=1}^n u_i \geq n(q-1)$ pa dolazimo do kontradikcije. Dakle, barem jedan u_i je manji od $q - 1$, tj. nije djeljiv s $q - 1$ (ili je jednak nula) pa iz prethodno dokazane leme slijedi željena tvrdnja. □

Spomenimo i dva korolara ovog teorema.

Korolar 1.2.3. *Ako je* $\sum_{\alpha} st\ f_\alpha < n$ *i ako nijedan od* f_α *nema slobodni član, tada taj skup polinoma ima netrivijalnu zajedničku nultočku.*

Dokaz. Kako niti jedan od polinoma f_α nema slobodni član, 0 je njihova zajednička nultočka. No, ako bi bilo $V = \{0\}$, tj. $card(V) = 1$, to bi bilo u kontradikciji s time da je $card(V)$ djeljiv s p. Prema tome, ti polinomi imaju još neku, netrivijalnu, zajedničku nultočku. □

Drugi korolar govori nam o postojanju netrivijalne nultočke jedne vrste homogenih polinoma (nemaju slobodni član).

Korolar 1.2.4. *Sve kvadratne forme (homogeni polinomi drugog stupnja) u barem* 3 *varijable nad K imaju netrivijalnu nultočku.*

1.3 Zakon kvadratnog reciprociteta

U ovom potpoglavlju vidjet ćemo koji elementi polja $\mathbb{F}_q$ su kvadrati, i u vezi s time definirati Legendreov simbol i promotriti neka njegova svojstva. Na kraju ćemo dokazati glavni rezultat ovog poglavlja, Gaussov zakon kvadratnog reciprociteta.

Neka q i dalje bude potencija prostog broja p.

Sljedeći teorem govori nam koji elementi polja $\mathbb{F}_q$ su kvadrati, pri čemu razlikujemo slučajeve kad je q potencija broja 2 i kad je potencija nekog drugog prostog broja.

Teorem 1.3.1. (*a*) *Ako je* $p = 2$*, tada su svi elementi polja* $\mathbb{F}_q$ *kvadrati.*
(*b*) *Ako je* $p \neq 2$*, tada kvadrati u* $\mathbb{F}_q^*$ *tvore podgrupu (označimo je sa* $\mathbb{F}_q^{*2}$*) indeksa* 2 *u* $\mathbb{F}_q^*$*, i ta podgrupa je jezgra homomorfizma* $x \mapsto x^{(q-1)/2}$*, koji označimo s h, i koji poprima vrijednosti* $\{\pm 1\}$.

Dokaz. (*a*) Za preslikavanje $x \mapsto x^2$ za $p = 2$ se lako vidi da je automorfizam od $\mathbb{F}_q$ iz čega odmah zaključujemo da su u ovom slučaju svi elementi polja $\mathbb{F}_q$ kvadrati.
(*b*) Neka je Ω algebarsko zatvorenje od $\mathbb{F}_q$ pa za svaki $x \in \mathbb{F}_q^*$ postoji $y \in \Omega$ takav da je $y^2 = x$. Da bi x bio kvadrat u $\mathbb{F}_q$ nužno je i dovoljno da je $y \in \mathbb{F}_q^*$, tj. da vrijedi $y^{q-1} = 1$. Imamo:

$$y^{q-1} = x^{(q-1)/2} = \pm 1, \tag{1.9}$$

jer je $x^{q-1} = 1$. Iz toga vidimo da je skup svih x koji su kvadrati jednak jezgri preslikavanja $x \mapsto x^{(q-1)/2}$, tj. $\mathbb{F}_q^{*2}$=*Ker h*. Preslikavanje h je očigledno homomorfizam, i poprima vrijednosti $\{\pm 1\}$.

Ostalo je još dokazati da je podgrupa $\mathbb{F}_q^{*2}$ indeksa 2 u $\mathbb{F}_q^*$. To odmah slijedi iz činjenice da ako imamo preslikavanje $\varphi : G \to H$ koje je homomorfizam grupa, onda je indeks od $Ker\ \varphi$ u G jednak redu od $Im\ \varphi$. Primijenimo li to na naše preslikavanje h, dobivamo da je $[\mathbb{F}_q^* : \mathbb{F}_q^{*2}] = |\{\pm 1\}| = 2$, što smo i trebali dokazati.

Ovime je teorem u potpunosti dokazan za sve slučajeve. □

U vezi s kvadratima u polju $\mathbb{F}_p$ definiramo sada Legendreov simbol.

Definicija 1.3.2. *Neka je $p \neq 2$ prost broj i neka je $x \in \mathbb{F}_p^*$. Legendreov simbol od x označavamo sa $\left(\frac{x}{p}\right)$ i on je jednak broju $x^{(p-1)/2}$.*

S obzirom da je $x^{p-1} = 1$, $\forall x \in \mathbb{F}_p^*$, jasno je da Legendreov simbol u tom slučaju poprima jedino vrijednosti 1 i -1.

Legendreov simbol proširujemo na cijeli $\mathbb{F}_p$ tako da stavimo da je $\left(\frac{0}{p}\right) = 0$.

Moguće ga je proširiti i na cijeli skup $\mathbb{Z}$ tako da za $x \in \mathbb{Z}$ definiramo $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$, gdje je x' slika od x u polju $\mathbb{F}_p$.

Očito je da je Legendreov simbol karakter grupe $\mathbb{F}_p^*$ jer vrijedi $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$.

U teoremu 1.3.1 smo vidjeli da je $\mathbb{F}_p^{*2}$=$Ker\ h$, gdje je h preslikavanje $x \mapsto x^{(p-1)/2}$, pa iz toga zaključujemo da vrijedi:

$$x \in \mathbb{F}_p^{*2} \iff \left(\frac{x}{p}\right) = 1. \tag{1.10}$$

Ako je y kvadratni korijen od $x \in \mathbb{F}_p^*$ u algebarskom zatvorenju od $\mathbb{F}_p$, tj. ako vrijedi $y^2 = x$, onda imamo $\left(\frac{x}{p}\right) = x^{(p-1)/2} = y^{p-1}$.

Iz gornjih razmatranja vidimo vezu između Legendreovog simbola i elemenata skupa $\mathbb{F}_p^{*2}$; odredimo sada Legendreove simbole za $x = 1, -1$ i 2, tj. provjerimo za koje p su ti brojevi elementi skupa $\mathbb{F}_p^{*2}$, a za koje nisu.

Prvo definirajmo dvije funkcije koje će nam biti od pomoći pri tome.

Definicija 1.3.3. *Za $n \in \mathbb{Z}$ neparan, definirajmo funkcije ε i ω na sljedeći način:*

$$\varepsilon(n) \equiv \frac{n-1}{2} \pmod 2 = \begin{cases} 0, & ako\ n \equiv 1 \pmod 4 \\ 1, & ako\ n \equiv -1 \pmod 4. \end{cases} \tag{1.11}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \pmod 2 = \begin{cases} 0, & ako\ n \equiv \pm 1 \pmod 8 \\ 1, & ako\ n \equiv \pm 5 \pmod 8. \end{cases} \tag{1.12}$$

Iz definicije je očito da su $\varepsilon : (\mathbb{Z}/4\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z}$ i $\omega : (\mathbb{Z}/8\mathbb{Z})^* \to \mathbb{Z}/2\mathbb{Z}$ homomorfizmi.

Sada ćemo dokazati teorem koji nam govori koje su vrijednosti Legendreovog simbola za $x = 1, -1$ i 2.

Teorem 1.3.4. *Vrijede sljedeće formule:*
$(a) \left(\frac{1}{p}\right) = 1$
$(b) \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$
$(c) \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$.

Dokaz. Tvrdnje (a) i (b) očito vrijede, po samoj definiciji Legendreovog simbola. Dokažimo sada tvrdnju (c).

Označimo sa α primitivni osmi korijen iz jedinice u algebarskom zatvorenju Ω od $\mathbb{F}_p$. Tada imamo $\alpha^8 = 1$ i 8 je najmanji prirodni broj za koji to vrijedi.

Pronađimo sada element koji kvadriran daje 2, kako bismo mogli izračunati odgovarajući Legendreov simbol. Promotrimo $y = \alpha + \alpha^{-1}$. Za njega vrijedi:

$$y^2 = \alpha^2 + 2 + \alpha^{-2}. \tag{1.13}$$

S obzirom da je $\alpha^4 = \sqrt{\alpha^8} = \sqrt{1}$, i iz činjenice da je 8 najmanji prirodni broj k za koji je $\alpha^k = 1$, slijedi da je $\alpha^4 = -1$, tj. $\alpha^4 + 1 = 0$, odnosno $\alpha^2 + \alpha^{-2} = 0$. Prema tome, $y^2 = 2$, i time smo pronašli traženi element.

Također, imamo $y^p = \alpha^p + \alpha^{-p}$, jer je Ω karakteristike p.

Sada odredimo $\left(\frac{2}{p}\right)$ u ovisnosti o p. Promatramo dva slučaja:

$1. p \equiv \pm 1 \pmod 8$
Tada imamo:

$$y^p = \alpha + \alpha^{-1} = y, \tag{1.14}$$

jer je $\alpha^8 = 1$.
Dakle, u tom slučaju je $\left(\frac{2}{p}\right) = y^{p-1} = \frac{y^p}{y} = 1$.

2. $p \equiv \pm 5 \pmod 8$
Tada imamo:

$$y^p = \alpha^5 + \alpha^{-5} = -\alpha - \alpha^{-1} = -(\alpha + \alpha^{-1}) = -y, \tag{1.15}$$

jer je $\alpha^8 = 1$ i $\alpha^5 = \alpha^4 \cdot \alpha = -1 \cdot \alpha = -\alpha$.
Dakle, u tom slučaju je $\left(\frac{2}{p}\right) = y^{p-1} = \frac{y^p}{y} = -1$.

Ovime smo upravo pokazali da je $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$, tj. da i tvrdnja (c) vrijedi. □

Prema tome, možemo zaključiti sljedeće:
- $1 \in \mathbb{F}_p^{*\,2}$ uvijek, tj. 1 je uvijek kvadrat $(mod\ p)$
- -1 je kvadrat $(mod\ p)$ ako i samo ako je $p \equiv 1 \pmod 4$
- 2 je kvadrat $(mod\ p)$ ako i samo ako je $p \equiv \pm 1 \pmod 8$.

Sada smo spremni da iskažemo i dokažemo najbitniji rezultat ovog poglavlja, Gaussov zakon kvadratnog reciprociteta.

Teorem 1.3.5. *Neka su $l \neq 2$ i $p \neq 2$ dva međusobno različita prosta broja. Tada vrijedi:*

$$\left(\frac{l}{p}\right) = (-1)^{\varepsilon(l)\varepsilon(p)} \left(\frac{p}{l}\right). \tag{1.16}$$

Dokaz. Neka je Ω algebarsko zatvorenje od $\mathbb{F}_p$, i neka je $w \in \Omega$ primitivni l.-ti korijen iz jedinice, tj. $w^l = 1$ i l je najmanji prirodni broj za koji to vrijedi. Zbog toga je w^x dobro definiran za $x \in \mathbb{F}_l$. Stoga možemo formirati takozvanu Gaussovu sumu:

$$y = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) w^x. \tag{1.17}$$

Za tako formirani y vrijedi:

1. $y^2 = (-1)^{\varepsilon(l)} l$

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

Dokažimo to.

Radi jednostavnosti, sa l ćemo također označavati i sliku od l u polju $\mathbb{F}_p$.

Imamo:

$$y^2 = \left(\sum_{x\in\mathbb{F}_l}\left(\frac{x}{l}\right)w^x\right)\cdot\left(\sum_{z\in\mathbb{F}_l}\left(\frac{z}{l}\right)w^z\right) = \sum_{x,z\in\mathbb{F}_l}\left(\frac{xz}{l}\right)w^{x+z} = \sum_{u\in\mathbb{F}_l}w^u\left(\sum_{t\in\mathbb{F}_l}\left(\frac{t(u-t)}{l}\right)\right), \tag{1.18}$$

pri čemu smo u zadnjoj jednakosti izvršili supstituciju $u = x + z$, $t = x$, iz čega slijedi $z = u - t$.

Sada za $t \neq 0$ (za $t = 0$ odgovarajući član sume jednak je 0) dobivamo:

$$\left(\frac{t(u-t)}{l}\right) = \left(\frac{-t^2(1-ut^{-1}}{l}\right) = \left(\frac{-t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{t^2}{l}\right)\left(\frac{1-ut^{-1}}{l}\right) = (-1)^{\varepsilon(l)}\left(\frac{1-ut^{-1}}{l}\right). \tag{1.19}$$

Koristili smo teorem 1.3.4, tvrdnju (b), kao i činjenicu da je $\left(\frac{t^2}{l}\right) = 1$ za sve $t \in \mathbb{F}_l^*$.
Ako uvedemo oznaku

$$C_u = \sum_{t\in\mathbb{F}_l^*}\left(\frac{1-ut^{-1}}{l}\right), \tag{1.20}$$

iz toga slijedi da vrijedi:

$$(-1)^{\varepsilon(l)}y^2 = \sum_{u\in\mathbb{F}_l}C_u w^u. \tag{1.21}$$

Nadalje, $C_0 = \sum\limits_{t\in\mathbb{F}_l^*}\left(\frac{1}{l}\right) = \sum\limits_{t\in\mathbb{F}_l^*}1 = card(\mathbb{F}_l^*) = l - 1$. Ako je $u \neq 0$ onda $s = 1 - ut^{-1}$ ide po $\mathbb{F}_l \setminus \{1\}$ i imamo:

$$C_u = \sum_{s\in\mathbb{F}_l}\left(\frac{s}{l}\right) - \left(\frac{1}{l}\right) = -\left(\frac{1}{l}\right) = -1, \tag{1.22}$$

jer je $\sum\limits_{s\in\mathbb{F}_l}\left(\frac{s}{l}\right) = 0$, a to je tako jer je u $\mathbb{F}_l^*$ jednak broj elemenata koji su kvadrati i onih koji to nisu pa se odgovarajuće vrijednosti poništavaju. (To slijedi iz teorema 1.3.1, iz činjenice da je $[\mathbb{F}_l^* : \mathbb{F}_l^{*2}] = 2$ pa je dakle $|\mathbb{F}_l^{*2}| = \frac{|\mathbb{F}_l^*|}{2} = \frac{l-1}{2}$, a isto toliko je onda i elemenata koji nisu

kvadrati u $\mathbb{F}_l^*$.)
Iz toga imamo:

$$\sum_{u\in\mathbb{F}_l} C_u w^u = C_0 + \sum_{u\in\mathbb{F}_l^*} C_u w^u = l - 1 + \sum_{u\in\mathbb{F}_l^*} (-1)\cdot w^u = l - 1 - \sum_{u\in\mathbb{F}_l^*} w^u. \tag{1.23}$$

Odredimo sada $\sum_{u\in\mathbb{F}_l^*} w^u$.

$$\sum_{u\in\mathbb{F}_l^*} w^u = \sum_{u\in\mathbb{F}_l} w^u - 1 = \frac{w^l - 1}{w - 1} - 1 = 0 - 1 = -1, \tag{1.24}$$

jer je w l.-ti primitivni korijen iz jedinice. Dakle:

$$\sum_{u\in\mathbb{F}_l} C_u w^u = l - 1 - (-1) = l. \tag{1.25}$$

Sada iz (1.21) imamo

$$y^2 = (-1)^{\varepsilon(l)} l, \tag{1.26}$$

i time je prva tvrdnja dokazana.

Odredimo sada y^{p-1}. Kako je $char(\Omega) = p$, uz supstituciju $z = xp$ iz čega slijedi $x = zp^{-1}$, imamo:

$$y^p = \sum_{x\in\mathbb{F}_l} \left(\frac{x}{l}\right) w^{xp} = \sum_{z\in\mathbb{F}_l} \left(\frac{zp^{-1}}{l}\right) w^z = \sum_{z\in\mathbb{F}_l} \left(\frac{z}{l}\right)\left(\frac{p^{-1}}{l}\right) w^z = \left(\frac{p^{-1}}{l}\right) \sum_{z\in\mathbb{F}_l} \left(\frac{z}{l}\right) w^z = \left(\frac{p^{-1}}{l}\right) y = \left(\frac{p}{l}\right) y, \tag{1.27}$$

gdje smo iskoristili činjenicu da je p kvadrat u $\mathbb{F}_l^*$ ako i samo ako je i p^{-1} kvadrat u $\mathbb{F}_l^*$. Iz gore pokazanog dobivamo

$$y^{p-1} = \left(\frac{p}{l}\right), \tag{1.28}$$

čime smo dokazali i drugu tvrdnju.

Sada pomoću njih lako dokazujemo tvrdnju teorema. Naime, imamo:

$$\left(\frac{(-1)^{\varepsilon(l)} l}{p}\right) = \left(\frac{y^2}{p}\right) = y^{p-1} = \left(\frac{p}{l}\right). \tag{1.29}$$

Vrijedi:

$$\left(\frac{(-1)^{\varepsilon(l)}}{p}\right) = \left(\frac{-1}{p}\right)^{\varepsilon(l)} = (-1)^{\varepsilon(p)\varepsilon(l)}. \tag{1.30}$$

Tu smo iskoristili teorem 1.3.4, tvrdnju (*b*).
Sada iz (1.29) i (1.30) slijedi

$$\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\varepsilon(l)}l}{p}\right) = \left(\frac{(-1)^{\varepsilon(l)}}{p}\right)\left(\frac{l}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(l)}\left(\frac{l}{p}\right), \tag{1.31}$$

odnosno

$$\left(\frac{l}{p}\right) = (-1)^{\varepsilon(l)\varepsilon(p)}\left(\frac{p}{l}\right), \tag{1.32}$$

što smo i trebali dokazati.

□

Drugim riječima, ako sa lRp označimo da je l kvadrat (*mod* p) (još kažemo da je l kvadratni ostatak modulo p), tj. da je $\left(\frac{l}{p}\right) = 1$, a sa lNp da l nije kvadrat (*mod* p), Gaussov teorem nam govori sljedeće:

- $lRp \iff pRl$ ako je p ili $l \equiv 1$ (*mod* 4)
- $lRp \iff pNl$ ako su i p i $l \equiv -1$ (*mod* 4).

Notacijom Legendreovih simbola to možemo zapisati ovako:

- $\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right)$ ako je p ili $l \equiv 1$ (*mod* 4)
- $\left(\frac{l}{p}\right) = -\left(\frac{p}{l}\right)$ ako su i p i $l \equiv -1$ (*mod* 4).

Premda nam Gaussov zakon kvadratnog reciprociteta za svaku kvadratnu jednadžbu govori ima li rješenje modulo p, on nam nimalo ne pomaže da to rješenje i pronađemo.

Na kraju poglavlja promotrimo jedan primjer u kojem pomoću dokazanih tvrdnji provjeravamo ima li dana kvadratna jednadžba rješenje.

Primjer 1.3.6. *Odredimo je li* 29 *kvadrat u* $\mathbb{F}_{43}^*$, *tj. ima li jednadžba* $x^2 \equiv 29$ (*mod* 43) *rješenje. To ćemo odrediti tako da izračunamo* $\left(\frac{29}{43}\right)$. *Imamo:*

$\left(\frac{29}{43}\right)$=*(jer je* 29 $\equiv$ 1 (*mod* 4)*)*= $\left(\frac{43}{29}\right)$ =*(slika od* 43 *u* $\mathbb{F}_{29}$ *je* 14*)*= $\left(\frac{14}{29}\right)$ =*(Legendreov*

simbol je karakter)$= \left(\frac{2}{29}\right)\left(\frac{7}{29}\right)$ *=(teorem 1.3.4, tvrdnja* (c)*)*$= -1 \cdot \left(\frac{7}{29}\right)$ *=(jer je* $29 \equiv 1 \pmod 4$*)*$= -\left(\frac{29}{7}\right)$ *=(slika od* 29 *u* $\mathbb{F}_7$ *je* 1*)*$= -\left(\frac{1}{7}\right)$ *=(teorem 1.3.4, tvrdnja* (a)*)*$= -1$.

Dakle, zaključujemo da promatrana jednadžba nema rješenje.

Poglavlje 2

p-adska polja

U ovom poglavlju definirat ćemo prsten p-adskih cijelih brojeva, $\mathbb{Z}_p$, i polje njegovih razlomaka, $\mathbb{Q}_p$, i promotriti neka njihova svojstva. Nakon toga ćemo proučiti p-adske jednadžbe, čiji su koeficijenti p-adski cijeli brojevi, i pokazati kako se od rješenja ($mod\ p^n$) dolazi do pravog rješenja jednadžbe (tj. s koeficijentima u $\mathbb{Z}_p$).

U cijelom poglavlju p označava prost broj.

2.1 Prsten $\mathbb{Z}_p$ i polje $\mathbb{Q}_p$

U ovom potpoglavlju dat ćemo osnovne definicije i svojstva promatranih objekata.

Neka je $A_n = \mathbb{Z}/p^n\mathbb{Z}, \forall n \geq 1$. To je prsten klasa cijelih brojeva ($mod\ p^n$). Definirajmo preslikavanje $\phi_n : A_n \to A_{n-1}$ na sljedeći način:

$$\phi_n(a) = a\ (mod\ p^{n-1}), \forall a \in A_n. \tag{2.1}$$

To preslikavanje je očigledno homomorfizam, surjektivno je, a jezgra mu je $p^{n-1}A_n$.

Tada niz

$$\ldots \to A_n \to A_{n-1} \to \ldots \to A_2 \to A_1 \tag{2.2}$$

s odgovarajućim homomorfizmima formira "projektivni sistem" (slobodnije govoreći), indeksiran prirodnim brojevima.

Definicija 2.1.1. *Prsten p-adskih cijelih brojeva $\mathbb{Z}_p$ je projektivni limes sistema (A_n, ϕ_n) definiranog gore.*

Iz te definicije vidimo da je element prstena $\mathbb{Z}_p = \varprojlim (A_n, \phi_n)$ niz $x = (\cdots, x_n, \cdots, x_1)$, pri čemu je $x_n \in A_n, \forall n \geq 1$ i $\phi_n(x_n) = x_{n-1}, \forall n \geq 2$. Zbrajanje i množenje u $\mathbb{Z}_p$ definirani su standardno, po koordinatama. Drugim riječima, $\mathbb{Z}_p$ je potprsten direktnog produkta $\prod_{n\geq 1} A_n$ s navedenim svojstvima.

Sada kad smo ga definirali, ispitajmo svojstva prstena $\mathbb{Z}_p$.

Neka je $\varepsilon_n : \mathbb{Z}_p \to A_n$ funkcija definirana na sljedeći način:

$$\varepsilon_n(x) = x_n, \tag{2.3}$$

gdje je $x \in \mathbb{Z}_p$.

Propozicija 2.1.2. *Niz* $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ *je egzaktni niz Abelovih grupa.*

Dokaz. Po definiciji egzaktnog niza, kako bismo ovo dokazali trebamo provjeriti ove jednakosti:

1. $Ker(p^n) = 0$

2. $Im(p^n) = Ker(\varepsilon_n)$

3. $Im(\varepsilon_n) = A_n$

Dokažimo da one vrijede.

1. Dokazat ćemo da je množenje sa p injektivno u $\mathbb{Z}_p$, a iz toga odmah slijedi da je i množenje sa p^n u $\mathbb{Z}_p$ injektivno kao kompozicija n injekcija, tj. da je $Ker(p^n) = 0$. Uzmimo $x = (x_n) \in \mathbb{Z}_p$ takav da je $px = 0$. Kako bismo dokazali traženu injektivnost, trebamo pokazati da je tada $x = 0$. Iz $px = 0$ slijedi $px_{n+1} = 0, \forall n$. Očito je da je $x_{n+1} = p^n y_{n+1}$, za neki $y_{n+1} \in A_{n+1}$. Sada imamo:

$$x_n = \phi_{n+1}(x_{n+1}) = \phi_{n+1}(p^n y_{n+1}) = 0 \tag{2.4}$$

jer je ϕ_{n+1} homomorfizam s jezgrom $p^n A_{n+1}$. Dakle, $x_n = 0, \forall n$ pa je prema tome i $x = 0$, čime je tvrdnja dokazana.

2. $Im(p^n) = p^n\mathbb{Z}_p$, pa ako uzmemo element iz $Im(p^n)$ on je oblika $p^n x$, gdje je $x = (x_n) \in \mathbb{Z}_p$. Tada je $\varepsilon_n(p^n x) = p^n x_n = 0$, tj. $Im(p^n) \subseteq Ker(\varepsilon_n)$. Obratno, ako je $x = (x_m) \in Ker(\varepsilon_m)$, imamo $x_m = 0$ u A_m, tj. p^m dijeli x_m. Iz toga slijedi da je $x_m \equiv 0 \ (mod\ p^n), \forall m \geq n$,

što znači da postoji dobro definiran $y_{m-n} \in A_{m-n}$ takav da njegova slika po izomorfizmu $A_{m-n} \to p^n\mathbb{Z}/p^m\mathbb{Z} \subset A_m$ zadovoljava $x_m = p^n y_{m-n}$. Ti y_i definiraju element y iz $\mathbb{Z}_p = \varprojlim A_i$, i odmah se vidi da je $p^n y = x$, tj. $x \in p^n\mathbb{Z}_p = Im(p^n)$ pa je $Ker(\varepsilon_n) \subseteq Im(p^n)$. Dakle, $Im(p^n) = Ker(\varepsilon_n)$, čime je dokazana i druga tvrdnja.

3. Očito je da je ε_n surjekcija, tj. da je $Im(\varepsilon_n) = A_n$ pa i treća tvrdnja vrijedi.

Ovime je propozicija u potpunosti dokazana. □

Promatrani egzaktni niz zapravo je kratki egzaktni niz Abelovih grupa, pa zbog toga vrijedi sljedeće:

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong A_n, \tag{2.5}$$

odnosno

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}, \tag{2.6}$$

pa možemo identificirati $\mathbb{Z}_p/p^n\mathbb{Z}_p$ sa $\mathbb{Z}/p^n\mathbb{Z}$.

Sljedeća propozicija govori nam koji su invertibilni elementi u $\mathbb{Z}_p$ i o prikazu bilo kojeg elementa iz $\mathbb{Z}_p$ pomoću njih.

Propozicija 2.1.3. (*a*) *Da bi neki element iz $\mathbb{Z}_p$ (odnosno iz A_n) bio invertibilan nužno je i dovoljno da nije djeljiv s p.*
(*b*) *Ako s $\mathbb{U}$ označimo grupu invertibilnih elemenata u $\mathbb{Z}_p$, svaki element iz $\mathbb{Z}_p$ različit od nule može se na jedinstven način napisati u obliku $p^n u$, gdje je $u \in \mathbb{U}$ (takav element zovemo p-adska jedinica) i $n \geq 0$.*

Dokaz. (*a*) Dovoljno je dokazati tvrdnju za A_n jer će iz nje odmah slijediti tvrdnja i za $\mathbb{Z}_p$. Uzmimo sada $x \in A_n$ koji nije djeljiv sa p, tj. koji ne pripada skupu pA_n. Pronaći ćemo $t \in A_n$ takav da je $xt = 1$, čime ćemo pokazati da je x invertibilan.

Slika od x u $A_1 = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ nije nula, pa je invertibilna. Prema tome, postoje $y, z \in A_n$ takvi da je $xy + pz = (x, p) = 1$, odnosno takvi da je $xy = 1 - pz$. Sada imamo:

$$xy(1 + pz + \cdots + p^{n-1}z^{n-1}) = (1 - pz)(1 + pz + \cdots + p^{n-1}z^{n-1}) = 1 - p^n z^n = 1, \tag{2.7}$$

jer je $p^n z^n$ jednako 0 u A_n.
Ako stavimo $t = y(1 + pz + \cdots + p^{n-1}z^{n-1})$, vidimo da je $t \in A_n$ i da je $xt = 1$, tj. pronašli smo traženi t.

Obrat odmah slijedi iz definicije invertibilnosti.

(b) Neka je $x \in \mathbb{Z}_p$ proizvoljni element različit od 0. Tada postoji najveći $n \in \mathbb{N}$ za koji je $x_n = 0$ (jer ako je neki član niza x nula, onda su i svi prethodni članovi 0 zbog svojstva niza da je $\phi_n(x_n) = x_{n-1}$ pa za $x \neq 0$ mora postojati član najvećeg indeksa koji je jednak nuli) ili su svi članovi niza različiti od nule i tada uzimamo $n = 0$. x je u tom slučaju djeljiv sa p^n, a nije djeljiv s p^{n+1} pa ga možemo zapisati u obliku $x = p^n u$, pri čemu je $n \geq 0$, a $u \in \mathbb{Z}_p$ nije djeljiv s p. Tada je po (a) u invertibilan, odnosno $u \in \mathbb{U}$, čime smo dokazali postojanje traženog prikaza. Jedinstvenost prikaza je očigledna, pa je i (b) dio propozicije dokazan. □

Uvedimo sad oznaku koja će nam olakšati daljnje baratanje ovim prikazom elemenata.

Neka je $x \in \mathbb{Z}_p$ različit od nule. Napišimo ga u obliku $p^n u$, gdje je $u \in \mathbb{U}$ i $n \geq 0$. Tada n nazivamo p-adskom vrijednošću od x i označavamo sa $v_p(x)$. Proširujemo oznaku na cijeli $\mathbb{Z}_p$ tako da stavimo $v_p(0) = +\infty$. Sada imamo:

$$v_p(xy) = v_p(x) + v_p(y) \tag{2.8}$$

i

$$v_p(x + y) \geq \inf(v_p(x), v_p(y)). \tag{2.9}$$

Iz toga odmah slijedi da je $\mathbb{Z}_p$ integralna domena.

Definirajmo sada polje $\mathbb{Q}_p$.

Definicija 2.1.4. *Polje p-adskih brojeva, u oznaci $\mathbb{Q}_p$, je polje razlomaka prstena $\mathbb{Z}_p$.*

Vidljivo je da je $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. Iz toga i propozicije 2.1.3, dio (b), jasno je da svaki $x \in \mathbb{Q}_p^*$ ima jedinstven prikaz u obliku $p^n u$, gdje je $n \in \mathbb{Z}$ i $u \in \mathbb{U}$; i ovdje n nazivamo p-adskom vrijednošću od x i označavamo sa $v_p(x)$. Također, očito je da vrijedi:

$$v_p(x) \geq 0 \iff x \in \mathbb{Z}_p. \tag{2.10}$$

2.2 p-adske jednadžbe

U ovom potpoglavlju prvo ćemo vidjeti kakva je veza između nultočaka polinoma s koeficijentima u $\mathbb{Z}_p$ i polinoma dobivenih njihovom redukcijom ($mod\ p^n$), čiji su koeficijenti u A_n. Tada ćemo promotriti kako od rješenja p-adskih jednadžbi ($mod\ p^n$) doći do pravih rješenja, s koeficijentima u $\mathbb{Z}_p$.

Definicija 2.2.1. *Neka je $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ polinom s koeficijentima u $\mathbb{Z}_p$ i $n \in \mathbb{N}$. Tada sa f_n označavamo polinom s koeficijentima u A_n dobiven iz f redukcijom ($mod\ p^n$).*

Sljedeća propozicija nam govori o zajedničkim nultočkama skupa polinoma s koeficijentima u $\mathbb{Z}_p$ i skupa polinoma dobivenih njihovom redukcijom $(mod\ p^n)$.

Propozicija 2.2.2. *Neka su $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ polinomi čiji su koeficijenti p-adski cijeli brojevi. Sljedeće tvrdnje su ekvivalentne:*

(*i*) *Polinomi $f^{(i)}$ imaju zajedničku nultočku u $(\mathbb{Z}_p)^m$.*

(*ii*) *Polinomi $f_n^{(i)}$ imaju zajedničku nultočku u $(A_n)^m$, $\forall n > 1$.*

Za dokaz ove propozicije bit će nam potrebna sljedeća lema.

Lema 2.2.3. *Neka je $\ldots \to D_n \to D_{n-1} \to \ldots \to D_1$ projektivni sistem i neka je $D = \varprojlim D_n$ njegov projektivni limes. Ako su D_n konačni i neprazni, onda je i D neprazan.*

Dokaz. Ako su preslikavanja $D_n \to D_{n-1}$ surjektivna za $n > 1$ očito je da je $D \neq \emptyset$. Zato ćemo svesti ovu lemu na taj posebni slučaj. U tu svrhu označimo sa $D_{n,p}$ sliku od D_{n+p} u D_n. Ako fiksiramo n, odmah se vidi da $D_{n,p}$ tvore padajuću familiju konačnih nepraznih podskupova pa je ta familija stacionarna, odnosno $D_{n,p}$ je neovisan o p za dovoljno velike p. Stoga limes skupova $D_{n,p}$ ovisi samo o n; označimo ga sa E_n. Očigledno je da $D_n \to D_{n-1}$ prenosi E_n u E_{n-1}, i to surjektivno, pa smo lemu sveli na slučaj promatran na početku (E_n su neprazni i konačni). Dakle, imamo $\varprojlim E_n \neq \emptyset$ pa onda pogotovo vrijedi $D = \varprojlim D_n \neq \emptyset$, što smo i trebali dokazati. □

Kad imamo ovaj rezultat, dokaz propozicije lagano slijedi. Označimo sa D skup zajedničkih nultočaka polinoma $f^{(i)}$ u $(\mathbb{Z}_p)^m$ i sa D_n skup zajedničkih nultočaka polinoma $f_n^{(i)}$ u $(A_n)^m$, $\forall n > 1$. Skupovi D_n su konačni i vrijedi $D = \varprojlim D_n$. Po gornjoj lemi, D je neprazan ako i samo ako su D_n neprazni (drugi smjer je očit), a to upravo propozicija i kaže, čime je dokaz gotov.

Uvedimo sad pojam primitivnog elementa.

Definicija 2.2.4. *Za element $x = (x_1, \ldots, x_m)$ iz $(\mathbb{Z}_p)^m$ kažemo da je primitivan ako je neki x_i invertibilan, tj. iz $\mathbb{U}$, odnosno ako nisu svi x_i djeljivi s p.*
Analogno se definiraju primitivni elementi u $(A_n)^m$.

U vezi s njima imamo sljedeći rezultat:

Propozicija 2.2.5. *Neka su $f^{(i)} \in \mathbb{Z}_p[X_1, \ldots, X_m]$ homogeni polinomi čiji su koeficijenti p-adski cijeli brojevi. Sljedeće tvrdnje su ekvivalentne:*

(*a*) *Polinomi* $f^{(i)}$ *imaju netrivijalnu zajedničku nultočku u* $(\mathbb{Q}_p)^m$.

(*b*) *Polinomi* $f^{(i)}$ *imaju zajedničku primitivnu nultočku u* $(\mathbb{Z}_p)^m$.

(*c*) *Polinomi* $f_n^{(i)}$ *imaju zajedničku primitivnu nultočku u* $(A_n)^m$, $\forall n > 1$.

Dokaz. Dokažimo prvo da je $(a) \iff (b)$. $(b) \implies (a)$ je trivijalno jasno (primitivna nultočka je po definiciji različita od nule). Obratno, ako je $x = (x_1, \ldots, x_m)$ netrivijalna zajednička nultočka polinoma $f^{(i)}$ u $(\mathbb{Q}_p)^m$ stavimo:

$$h = \inf(v_p(x_1), \ldots, v_p(x_m)) \tag{2.11}$$

i

$$y = p^{-h}x. \tag{2.12}$$

Iz definicije od y očito je da je $y \in (\mathbb{Z}_p)^m$ i da je primitivan, kao i da je zajednička nultočka polinoma $f^{(i)}$ (homogeni su, pa faktor p^{-h} "ne smeta"), što je upravo tvrdnja (b). Dakle, i $(a) \implies (b)$ pa je $(a) \iff (b)$.

$(b) \iff (c)$ slijedi iz gornje leme, analogno kao u dokazu prethodne propozicije. □

U nastavku ovog potpoglavlja dat ćemo rezultate koji poboljšavaju aproksimativna rješenja, tj. razmotrit ćemo kako od rješenja $(mod\ p^n)$ doći do pravog rješenja jednadžbe, onog s koeficijentima u $\mathbb{Z}_p$.

Pri tome će nam trebati sljedeća lema, koja je p-adski analog Newtonove metode.

Lema 2.2.6. *Neka je* $f \in \mathbb{Z}_p[X]$ *i* f' *derivacija tog polinoma. Neka je* $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}$ *takvi da je* $0 \leq 2k < n$, $f(x) \equiv 0\ (mod\ p^n)$, $v_p(f'(x)) = k$. *Tada postoji* $y \in \mathbb{Z}_p$ *takav da vrijedi:*

$$f(y) \equiv 0\ (mod\ p^{n+1}), \quad v_p(f'(y)) = k, \quad y \equiv x\ (mod\ p^{n-k}). \tag{2.13}$$

Dokaz. Uzmimo $y = x + p^{n-k}z$, $z \in \mathbb{Z}_p$. Takvim odabirom zadovoljeno je treće potrebno svojstvo. Odaberimo sad z takav da i preostala dva svojstva budu zadovoljena.

Iz Taylorovog teorema imamo:

$$f(y) = f(x) + (y-x)f'(x) + (y-x)^2\frac{f''(x)}{2} + \ldots = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a, \tag{2.14}$$

gdje je $a \in \mathbb{Z}_p$.

Po pretpostavkama leme vrijedi $f(x) = p^n b$ i $f'(x) = p^k c$, pri čemu je $b \in \mathbb{Z}_p$ i $c \in \mathbb{U}$. Prema tome, možemo izabrati z takav da vrijedi:

$$b + zc \equiv 0 \ (mod\ p). \tag{2.15}$$

Pokažimo sada da uz z tako odabran y zadovoljava i preostala dva svojstva.

Iz (2.14) dobivamo:

$$f(y) = p^n b + p^{n-k} z p^k c + p^{2n-2k} a = p^n (b + zc) + p^{2n-2k} a \equiv 0 \ (mod\ p^{n+1}), \tag{2.16}$$

zbog (2.15) i $n - 2k > 0$, odnosno $2n - 2k > n$. Ovime smo dokazali prvo željeno svojstvo.

Konačno, primijenimo li Taylorovu formulu na f' odmah dobivamo:

$$f'(y) \equiv p^k c \ (mod\ p^{n-k}). \tag{2.17}$$

Sada iz $n > 2k$ imamo $n - k > k$, iz čega slijedi $f'(y) = p^k c$, gdje je $c \in \mathbb{U}$. Iz toga je vidljivo da je $v_p(f'(y)) = k$, čime je i drugo svojstvo dokazano pa je naš $y \in \mathbb{Z}_p$ upravo onaj traženi. □

Uz pomoć upravo dokazane leme dokazat ćemo sljedeći veoma koristan teorem, koji nam govori kako se od rješenja $(mod\ p^n)$ dolazi do rješenja jednadžbe s koeficijentima u $\mathbb{Z}_p$.

Teorem 2.2.7. *Neka je $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k, j \in \mathbb{Z}$ takvi da $0 \leq j \leq m$, $0 < 2k < n$. Pretpostavimo da je*

$$f(x) \equiv 0 \ (mod\ p^n), \quad v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k. \tag{2.18}$$

Tada postoji nultočka y od f u $(\mathbb{Z}_p)^m$ za koju vrijedi $y \equiv x \ (mod\ p^{n-k})$.

Dokaz. Promotrimo prvo slučaj kada je $m = 1$. Primijenivši gornju lemu na $x^{(0)} = x$ (zadovoljava sve pretpostavke) dobivamo $x^{(1)} \in \mathbb{Z}_p$ za koji vrijedi:

$$f(x^{(1)}) \equiv 0 \ (mod\ p^{n+1}), \quad v_p(f'(x^{(1)})) = k, \quad x^{(1)} \equiv x^{(0)} \ (mod\ p^{n-k}). \tag{2.19}$$

Na dobiveni $x^{(1)}$ također možemo primijeniti lemu, uz zamjenu n sa $n + 1$. Nastavljajući dalje tako, konstruiramo niz $x^{(0)}, \ldots, x^{(q)}, \ldots$ takav da je:

$$f(x^{(q)}) \equiv 0 \ (mod\ p^{n+q}), \quad v_p(f'(x^{(q)})) = k, \quad x^{(q+1)} \equiv x^{(q)} \ (mod\ p^{n+q-k}). \tag{2.20}$$

Taj niz je, uz metriku na $\mathbb{Z}_p$ definiranu sa $d(x,y) = e^{-v_p(x-y)}$, očigledno Cauchyjev niz, zbog treće jednakosti u (2.20). On je onda i konvergentan jer je $\mathbb{Z}_p$, uz promatranu metriku, potpun metrički prostor. Dakle, postoji $y = \lim_q x^{(q)}$ i za njega iz prve jednakosti u (2.20) očigledno vrijedi $f(y) = 0$ u $\mathbb{Z}_p$, a uzastopnom primjenom treće jednakosti dobivamo da je $y \equiv x \ (mod\ p^{n-k})$. Prema tome, pronašli smo traženi y i time je teorem za $m = 1$ dokazan.

Promotrimo sad opći slučaj, $m > 1$. On može biti sveden na slučaj $m = 1$ tako da baratamo samo sa x_j. Preciznije, to ćemo uraditi na sljedeći način.

Neka je $\tilde{f} \in \mathbb{Z}_p[X_j]$ polinom u jednoj varijabli kojeg dobivamo iz $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ tako da X_i zamijenimo s x_i (odnosno koordinatama iz našeg x), $\forall i \neq j$, odnosno $\tilde{f}(z) = f(x_1, \ldots, z, \ldots, x_m)$, $\forall z \in X_j$. Primijenimo li iznad dokazano na $\tilde{f}$ i x_j (zbog pretpostavki teorema zadovoljavaju potrebne uvjete), dobivamo da postoji $y_j \in \mathbb{Z}_p$ takav da vrijedi $\tilde{f}(y_j) = 0$ i $y_j \equiv x_j \ (mod\ p^{n-k})$. Ako sad stavimo $y_i = x_i$, $\forall i \neq j$, dobivamo element $y = (y_i)$ koji zadovoljava tražene uvjete. Doista, tada je $f(y) = f(x_1, \ldots, y_j, \ldots, x_m) = \tilde{f}(y_j) = 0$ i očigledno je $y \equiv x \ (mod\ p^{n-k})$, čime je teorem dokazan. □

Za kraj ćemo navesti, s dokazima, neke korolare ovog teorema, u kojima ćemo vidjeti njegovu uporabu u pojedinim specijalnim slučajevima.

Korolar 2.2.8. *Od svake jednostavne nultočke redukcije modulo p polinoma f možemo doći do nultočke od f s koeficijentima u $\mathbb{Z}_p$.*

Dokaz. Neka je x jednostavna nultočka redukcije modulo p polinoma f. Po definiciji, barem jedna parcijalna derivacija od f modulo p je različita od nule u x. U našem slučaju, s obzirom da promatramo polinom modulo p, to znači da možemo primijeniti teorem za $n = 1$ i $k = 0$ i iz toga direktno dobivamo traženu tvrdnju. □

Korolar 2.2.9. *Neka je $p \neq 2$ i $f(X) = \sum_{i,j} a_{ij} X_i X_j$, gdje je $a_{ij} = a_{ji}, \forall i, j$, kvadratna forma s koeficijentima u $\mathbb{Z}_p$ čija diskriminanta, $det(a_{ij})$, je invertibilna. Neka je $a \in \mathbb{Z}_p$. Od svakog primitivnog rješenja jednadžbe $f(x) \equiv a \ (mod\ p)$ možemo doći do pravog rješenja.*

Dokaz. Dovoljno je dokazati da nisu sve parcijalne derivacije od f modulo p jednake nuli u x; to znači da je x jednostavna nultočka i iz korolara 2.2.8 slijedi tražena tvrdnja. Dokažimo to.

Lakim računom dobivamo:

$$\frac{\partial f}{\partial X_i} = 2 \sum_j a_{ij} X_j, \forall i. \tag{2.21}$$

S obzirom da je $det(a_{ij})$ invertibilna, ona nije djeljiva sa p, a kako je $x = (x_i)$ primitivno rješenje, nisu svi x_i djeljivi s p. Iz toga slijedi da postoji parcijalna derivacija od f koja nije djeljiva sa p u x, odnosno nije jednaka nula modulo p u x, što je i trebalo dokazati. □

Korolar 2.2.10. *Neka je* $p = 2$ *i* $f(X) = \sum_{i,j} a_{ij}X_iX_j$, *gdje je* $a_{ij} = a_{ji}, \forall i, j$, *kvadratna forma s koeficijentima u* $\mathbb{Z}_2$. *Neka je* $a \in \mathbb{Z}_2$. *Od svakog primitivnog rješenja jednadžbe* $f(x) \equiv a \pmod 8$ *možemo doći do pravog rješenja, uz uvjet da postoji parcijalna derivacija od* f *modulo* 4 *koja nije jednaka nuli u* x. *Taj uvjet je ispunjen ako je det*(a_{ij}) *invertibilna.*

Dokaz. Prva tvrdnja slijedi direktno iz teorema, za $n = 3$ i $k = 1$.

Druga tvrdnja dokazuje se analogno kao i prethodni korolar, uzimajući u obzir faktor 2. □

Poglavlje 3

Karakteri konačnih Abelovih grupa

U ovom poglavlju uvest ćemo pojam karaktera grupe. Prvo ćemo dati neka osnovna svojstva karaktera, a zatim ćemo proučiti modularne karaktere, koji će nam biti od važnosti u sljedećem poglavlju, pri definiciji L-funkcije.

U cijelom poglavlju G je konačna Abelova grupa, promatrana s operacijom množenja.

3.1 Osnovna svojstva

U ovom potpoglavlju dat ćemo definiciju karaktera i odrediti strukturu grupe karaktera grupe G, u oznaci $\hat{G}$, koju zovemo dual od G. Zatim ćemo vidjeti kako je grupa G povezana sa svojim bidualom, $\hat{\hat{G}}$, tj. grupom karaktera grupe $\hat{G}$. Na kraju ćemo dokazati dvije važne ortogonalne relacije u vezi s karakterima.

Definicija 3.1.1. *Karakter grupe G je homomorfizam sa G u multiplikativnu grupu kompleksnih brojeva, $\mathbb{C}^*$, tj. funkcija $\chi : G \to \mathbb{C}^*$ za koju vrijedi $\chi(g_1 g_2) = \chi(g1)\chi(g_2), \forall g_1, g_2 \in G$.*

Grupu $Hom(G, \mathbb{C}^*)$, koju tvore karakteri grupe G, označavamo sa $\hat{G}$ i zovemo dual od G.

Promotrimo sada grupu karaktera cikličke grupe.

Propozicija 3.1.2. *Neka je G ciklička grupa reda n. Tada je i $\hat{G}$ ciklička reda n.*

Dokaz. Ideja dokaza je konstruirati izomorfizam između $\hat{G}$ i neke grupe koja je ciklička reda n. Uradimo to.

Neka je s generator od G i χ karakter od G, tj. $\chi \in \hat{G}$. Stavimo $w = \chi(s)$. Tada imamo:

$$w^n = \chi(s)^n = \chi(s^n) = \chi(1_G) = 1, \tag{3.1}$$

jer je χ karakter pa je homomorfizam i preslikava jedinicu od G u 1, a s je generator od G, cikličke grupe reda n, pa je $s^n = 1_G$. Dakle, dobili smo da je w n.-ti korijen iz jedinice, tj. svaki karakter grupe G definira na navedeni način neki n.-ti korijen iz jedinice.

Obratno, i svaki n.-ti korijen iz jedinice definira neki karakter od G. Doista, ako je w n.-ti korijen iz jedinice, odgovarajući karakter $\chi \in \hat{G}$ definiran je preslikavanjem $s^a \mapsto w^a$, odnosno tako da vrijedi $\chi(s) = w$.

Iz iznad rečenog lako vidimo da je preslikavanje $\chi \mapsto \chi(s)$ izomorfizam sa $\hat{G}$ u grupu n.-tih korijena iz jedinice, μ_n, koja je ciklička reda n. Dakle, i $\hat{G}$ je ciklička reda n i dokaz je gotov. □

Karakter podgrupe uvijek se može proširiti do karaktera grupe. Sada ćemo to i dokazati.

Propozicija 3.1.3. *Neka je H podgrupa od G. Svaki karakter grupe H može se proširiti do karaktera grupe G.*

Dokaz. Tvrdnju ćemo dokazati indukcijom po indeksu od H u G, $(G : H)$. Baza indukcije trivijalno vrijedi, jer ako je $(G : H) = 1$ onda je $G = H$. U suprotnom, neka je $x \in G \setminus H$ i neka je $n \in \mathbb{N}$ najmanji prirodni broj veći od 1 za koji je $x^n \in H$. Neka je χ karakter grupe H; želimo dokazati da se on može proširiti do karaktera grupe G.

Stavimo $t = \chi(x^n)$ i izaberimo $w \in \mathbb{C}^*$ takav da je $w^n = t$. Promotrimo sada podgrupu od G generiranu sa H i x, u oznaci H'. Proširit ćemo χ do karaktera grupe H'. U tu svrhu definirajmo preslikavanje χ' na sljedeći način:

$$\chi'(h') = \chi(h)w^a, \tag{3.2}$$

pri čemu je $h' \in H'$ koji se očito može napisati u obliku $h' = hx^a$, gdje je $h \in H$ i $a \in \mathbb{Z}$.

Dokažimo da je to preslikavanje dobro definirano i da je $\chi' \in \widehat{H'}$, te da je $\chi'|_H = \chi$, odnosno da je χ' traženo proširenje od χ do karaktera grupe H'.

Prvo ćemo pokazati da je preslikavanje dobro definirano, odosno da je njegova vrijednost u proizvoljnom $h' \in H'$ neovisna o izboru dekompozicije od h'. U tu svrhu, neka su $h' = hx^a = ix^b$, gdje su $h, i \in H$ i $a, b \in \mathbb{Z}$, dva različita prikaza od h'. Trebamo pokazati da je tada $\chi(h)w^a = \chi(i)w^b$. Koristeći svojstva homomorfizma χ i definiciju od χ' imamo:

$$1 = \chi(1_H)w^0 = \chi'(1_H x^0) = \chi'(1_{H'}) = \chi'(h'(h')^{-1}) = \chi'(hx^a(ix^b)^{-1}) = \tag{3.3}$$

$$= \chi'(hi^{-1}x^{a-b}) = \chi(hi^{-1})w^{a-b} = \chi(h)w^a\chi(i^{-1})w^{-b} = \chi(h)w^a\chi(i)^{-1}w^{-b}, \tag{3.4}$$

tj. $\chi(h)w^a = \chi(i)w^b$, što je i trebalo dokazati. Prema tome, χ' je dobro definirano preslikavanje.

Dokažimo sada da je $\chi' \in \widehat{H'}$. Za proizvoljne $h' = hx^a, i' = ix^b \in H'$, gdje su $h, i \in H$ i $a, b \in \mathbb{Z}$, koristeći svojstva homomorfizma χ i definiciju od χ' imamo:

$$\chi'(h'i') = \chi'(hx^a ix^b) = \chi'(hix^{a+b}) = \chi(hi)w^{a+b} = \chi(h)w^a\chi(i)w^b = \chi'(h')\chi'(i'), \tag{3.5}$$

iz čega zaključujemo da je χ' homomorfizam sa H' u $\mathbb{C}^*$, odnosno da je χ' karakter grupe H'.

Konačno, iz same definicije od χ' vidimo da je, za $h \in H$, $\chi'(h) = \chi(h)$, jer je u tom slučaju odgovarajući a jednak nuli, odnosno da je $\chi'|_H = \chi$.

Dakle, χ' je doista traženo proširenje od χ, karaktera podgrupe H, do karaktera grupe H'.

S obzirom da je $H < H'$, imamo $(G : H') < (G : H)$ pa po pretpostavci indukcije možemo χ', karakter grupe H', proširiti do karaktera grupe G. Kako je χ' proširenje od χ, time smo χ, karakter podgrupe H, proširili do karaktera grupe G, što je i trebalo uraditi. □

Navedimo sada jednu zanimljivu posljedicu ove propozicije.

Operacija restrikcije karaktera grupe G na karaktere njene podgrupe H definira preslikavanje

$$\rho : \hat{G} \to \hat{H}, \tag{3.6}$$

koje je očigledno homomorfizam.
Sljedeći niz je egzaktan:

$$\{1\} \to (\widehat{G/H}) \xrightarrow{u} \hat{G} \xrightarrow{\rho} \hat{H} \to \{1\}, \tag{3.7}$$

gdje je $u : (\widehat{G/H}) \to \hat{G}$ ulaganje.

Doista, u je injektivno preslikavanje pa je $Ker(u) = \{1\}$. Nadalje, jezgra od ρ je skup svih karaktera grupe G koji su jednaki nuli na H; prema tome, $Ker(\rho) \cong (\widehat{G/H})$, tj. $Ker(\rho) \cong Im(u)$. Konačno, iz propozicije 3.1.3 imamo da je ρ surjekcija (jer za svaki karakter podgrupe H možemo naći karakter grupe G koji ga proširuje, odnosno karakter grupe G čija je restrikcija promatrani karakter podgrupe H) pa je $Im(\rho) = \hat{H}$, čime je egzaktnost gornjeg niza dokazana.

Taj niz zapravo je kratki egzaktni niz Abelovih grupa pa vrijedi:

$$\hat{G}/(\widehat{G/H}) \cong \hat{H}. \tag{3.8}$$

Sada ćemo iznijeti i dokazati važan rezultat koji nam govori o strukturi grupe $\hat{G}$.

Propozicija 3.1.4. *Grupa $\hat{G}$ je konačna Abelova grupa čiji je red jednak redu grupe G.*

Dokaz. I ovu tvrdnju ćemo dokazati korištenjem indukcije, ovaj put po redu n grupe G. Ako je $n = 1$, tvrdnja je trivijalna. U suprotnom, izaberimo neku netrivijalnu cikličku podgrupu H od G (to uvijek možemo uraditi). Iz (3.8) vidimo da je $|\hat{G}| = |\hat{H}| \cdot |(\widehat{G/H})|$. Red grupe $\hat{H}$ je jednak redu od H (to imamo iz propozicije 3.1.2), a red grupe $(\widehat{G/H})$ redu grupe G/H (po pretpostavci indukcije, jer je red od G/H strogo manji od n, reda grupe G). Stoga imamo:

$$|\hat{G}| = |H| \cdot |G/H| = |H| \cdot \frac{|G|}{|H|} = |G|. \tag{3.9}$$

$\hat{G}$ je očigledno Abelova grupa pa je dokaz ove propozicije završen. □

Moguće je dokazati i precizniji rezultat: grupa $\hat{G}$ izomorfna je grupi G. To se pokazuje dekomponiranjem konačne Abelove grupe G u direktni produkt cikličkih grupa, čiji su redovi potencije prostih brojeva. O egzistenciji tog produkta govori nam Kroneckerov teorem o dekompoziciji.

Dokažimo sada jednu bitnu činjenicu o bidualu grupe G, grupi $\hat{\hat{G}}$.

Neka je $x \in G$. Tada je funkcija $A : \hat{G} \to \mathbb{C}^*$, definirana sa $A(\chi) = \chi(x)$, $\forall \chi \in \hat{G}$, očito karakter grupe $\hat{G}$, tj. $A \in \hat{\hat{G}}$. Dakle, imamo homomorfizam $\varepsilon : G \to \hat{\hat{G}}$ definiran na sljedeći način:

$$\varepsilon(x) = A. \tag{3.10}$$

Prema tome, vrijedi:

$$\varepsilon(x)(\chi) = \chi(x), \forall \chi \in \hat{G}. \tag{3.11}$$

Propozicija 3.1.5. *Homomorfizam ε je izomorfizam grupe G i njenog biduala $\hat{\hat{G}}$.*

Dokaz. S obzirom da po propoziciji 3.1.4 vrijedi $|\hat{\hat{G}}| = |\hat{G}| = |G|$, dovoljno je dokazati da je ε injektivno preslikavanje. To znači da trebamo dokazati da je $Ker(\varepsilon) = \{1_G\}$, odnosno da ako je $x \in G$ različit od jedinice, onda i A nije jedinični karakter grupe $\hat{G}$, tj. postoji $\chi \in \hat{G}$ takav da je $\chi(x) \neq 1$. Dokažimo to.

Neka je H ciklička podgrupa od G generirana sa x. Kako je $x \neq 1_G$, očito je da postoji karakter χ' grupe H takav da je $\chi'(x) \neq 1$. Sada se po propoziciji 3.1.3 taj karakter može proširiti do karaktera χ grupe G za kojeg je onda također $\chi(x) \neq 1$, čime je propozicija dokazana. □

Za kraj ovog potpoglavlja dokazat ćemo dvije jednakosti u vezi s karakterima grupe G, koje zovemo ortogonalne relacije.

Propozicija 3.1.6. *Neka je $n = card(G)$ i $\chi \in \hat{G}$. Tada vrijedi:*

$$\sum_{x \in G} \chi(x) = \begin{cases} n, & ako\ \chi = 1 \\ 0, & ako\ \chi \neq 1. \end{cases} \tag{3.12}$$

$$\tag{3.13}$$

Dokaz. Slučaj kada je $\chi = 1$ je očigledan, jer je tada $\chi(x) = 1, \forall x \in G$ pa je $\sum\limits_{x \in G} \chi(x) = card(G) = n$.

Neka je sada $\chi \neq 1$. Zbog toga možemo izabrati $y \in G$ takav da je $\chi(y) \neq 1$. Tada imamo, jer je χ homomorfizam:

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(x)\chi(y) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x), \tag{3.14}$$

dakle vrijedi:

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0. \tag{3.15}$$

S obzirom da je y izabran tako da je $\chi(y) \neq 1$, slijedi da je u ovom slučaju $\sum\limits_{x \in G} \chi(x) = 0$. □

Korolar 3.1.7. *Neka je $n = card(G)$ i $x \in G$. Tada vrijedi:*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n, & ako\ x = 1 \\ 0, & ako\ x \neq 1. \end{cases} \tag{3.16}$$

$$\tag{3.17}$$

Dokaz. Ovaj rezultat odmah slijedi iz propozicije 3.1.6, primijenjene na dualnu grupu $\hat{G}$, i uzevši u obzir da su grupa G i njen bidual $\hat{\hat{G}}$ izomorfni. □

3.2 Modularni karakteri

U ovom potpoglavlju uvest ćemo pojam modularnih karaktera koji će nam biti važni u idućem poglavlju pri dokazivanju glavnog cilja ovog rada, Dirichletovog teorema o prostim brojevima u aritmetičkim nizovima.

Neka je $m \in \mathbb{N}$. Označimo sa $G(m)$ multiplikativnu grupu $(\mathbb{Z}/m\mathbb{Z})^*$ invertibilnih elemenata prstena $\mathbb{Z}/m\mathbb{Z}$. To je Abelova grupa reda $\phi(m)$, gdje je ϕ Eulerova funkcija (definicija 1.1.2). Element χ duala od $G(m)$ zovemo karakterom modulo m. Taj karakter se može promatrati kao funkcija definirana na skupu cijelih brojeva relativno prostih sa m (pri čemu je njena vrijednost u nekom broju jednaka vrijednosti u njegovom ostatku pri dijeljenju sa m, tj. promatramo brojeve modulo m, tako da budu elementi grupe $G(m)$) sa vrijednostima u $\mathbb{C}^*$, za koju vrijedi $\chi(ab) = \chi(a)\chi(b)$. Tu funkciju možemo proširiti na cijeli $\mathbb{Z}$ tako da stavimo $\chi(a) = 0$ ako a nije relativno prost sa m, i u tom slučaju ona poprima vrijednosti u $\mathbb{C}$. Preciznije rečeno, za $a \in \mathbb{Z}$ imamo:

$$\chi(a) = \begin{cases} \chi(k), & \text{ako } (a,m) = 1, a \equiv k \ (mod\ m) \\ 0, & \text{ako } (a,m) \neq 1. \end{cases} \tag{3.18}$$

(3.19)

Očito je da je to periodička funkcija, s periodom m.

Nadalje, iz Eulerovog teorema, za a i m relativno proste i za $\chi \in \widehat{G(m)}$, imamo:

$$a^{\phi(m)} \equiv 1 \ (mod\ m), \tag{3.20}$$

pa po (3.18) vrijedi:

$$1 = \chi(1) = \chi(a^{\phi(m)}) = \chi(a)^{\phi(m)}. \tag{3.21}$$

Dakle, ako je $(a,m) = 1$ i χ karakter modulo m, onda je $\chi(a)$ $\phi(m)$.-ti korijen iz jedinice, tj. vrijednost karaktera modulo m u nekom broju koji je relativno prost sa m može biti samo neki $\phi(m)$.-ti korijen iz jedinice.

Promotrimo sada nekoliko primjera modularnih karaktera, za različite vrijednosti od m.

(1) $m = 4$

U ovom slučaju imamo $|\widehat{G(4)}| = |G(4)| = \phi(4) = 2$ pa postoji samo jedan netrivijalni (tj. različit od jediničnog) karakter modulo 4. Odredimo ga.

Kako karakter uvijek jedinicu preslikava u jedinicu, imamo $\chi(1) = 1$. Preostalo nam je još odrediti $\chi(3)$. S obzirom da vrijedi $\chi(3)\chi(3) = \chi(9) = \chi(1) = 1$, vidimo da je $\chi(3)$ drugi

korijen iz jedinice. On mora biti različit od 1 jer bi inače i ovaj karakter bio jedinični pa dakle slijedi $\chi(3) = -1$. Sažetije zapisano, ovaj karakter definiran je sa $\chi(x) = (-1)^{\varepsilon(x)}$.

(2) $m = 8$

Grupa $G(8)$ ima $\phi(8) = 4$ elementa, pa tako i grupa karaktera modulo 8, dakle postoje 3 takva netrivijalna karaktera. Odredimo ih.

Znamo da je $\chi(1) = 1$ pa je potrebno odrediti $\chi(3), \chi(5)$ i $\chi(7)$. Iz $\chi(3)^2 = \chi(9) = \chi(1) = 1$ imamo da je $\chi(3) = 1$ ili $\chi(3) = -1$. Ako je $\chi(3) = 1$, tada imamo $\chi(3)\chi(5) = \chi(15) = \chi(7)$, odnosno $\chi(5) = \chi(7)$. Ako bi te vrijednosti bile 1, imali bismo jedinični karakter, prema tome mora biti $\chi(5) = \chi(7) = -1$. Vidimo da je dakle ovaj karakter definiran sa $\chi(x) = (-1)^{\varepsilon(x)+\omega(x)}$.

Sada, ako je $\chi(3) = -1$, onda imamo $\chi(5) = -\chi(7)$. Analogno kao i za $\chi(3)$ dobiva se da je $\chi(5)^2 = \chi(7)^2 = 1$, pa su moguće vrijednosti za ta dva broja 1 i -1. Prema tome, imamo $\chi(5) = 1$ i $\chi(7) = -1$ ili $\chi(5) = -1$ i $\chi(7) = 1$. U prvom slučaju dobivamo karakter definiran sa $\chi(x) = (-1)^{\varepsilon(x)}$, a u drugom karakter definiran sa $\chi(x) = (-1)^{\omega(x)}$. Time su pronađeni svi karakteri modulo 8.

Karakter $\chi(x) = (-1)^{\varepsilon(x)+\omega(x)}$ mogli smo dobiti i tako da pomnožimo preostala dva dobivena karaktera modulo 8, jer oni čine grupu s obzirom na množenje.

(3) $m = p$, gdje je $p \neq 2$ prost broj

Grupa $G(p) = (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^*$ je ciklička reda $p - 1$ (teorem 1.1.3), pa to vrijedi i za grupu karaktera modulo p (propozicija 3.1.2). Iz činjenice da je broj elemenata reda d u grupi sa n elemenata, ako d dijeli n, jednak $\phi(d)$, slijedi da karaktera reda 2 (koji dijeli $p-1$ jer je to paran broj za $p \neq 2$ prost) u ovoj grupi ima $\phi(2) = 1$. Odredimo taj karakter.

Kao što smo vidjeli u prvom poglavlju, Legendreov simbol je karakter grupe $G(p) = \mathbb{F}_p^*$, a kako on poprima samo vrijednosti 1 i -1 on je karakter reda 2 (nije reda 1 jer poprima uvijek i vrijednost -1). Iznad smo vidjeli da je u grupi $G(p)$ karakter reda 2 jedinstven pa iz ovoga slijedi da je taj karakter dan sa $\chi(x) = \left(\frac{x}{p}\right)$, i nazivamo ga Legendreov karakter.

(4) $m = 7$

Grupa $G(7)$, pa onda i grupa karaktera modulo 7, je ciklička reda 6 (jer je 7 prost broj različit od 2). Kako 3 dijeli 6, u toj grupi su $\phi(3) = 2$ elementa reda 3, tj. imamo 2 karaktera modulo 7 koji su reda 3. Odredimo te karaktere.

Karakter modulo 7 je u potpunosti određen sa svojom vrijednošću u 3 jer je 3 generator grupe $G(7)$ pa je dakle dovoljno odrediti $\chi(3)$. Zanimaju nas karakteri reda 3, što znači da mora vrijediti $\chi(3)^3 = 1$, tj. $\chi(3)$ mora biti treći korijen iz jedinice. Mogućnost da je $\chi(3) = 1$ otpada jer bi u tom slučaju imali trivijalni karakter. Ostaju nam dakle mogućnosti $\chi(3) = e^{2\pi i/3}$ i $\chi(3) = e^{4\pi i/3}$, i s tim vrijednostima su traženi karakteri u potpunosti određeni. Lakim računom (primjerice, imamo $\chi(5) = \chi(3^5) = \chi(3)^5 = (e^{2\pi i/3})^5 = e^{10\pi i/3} = e^{2\pi i}$.

$e^{4\pi i/3} = 1 \cdot e^{4\pi i/3} = e^{4\pi i/3}$; analogno dobivamo i ostale vrijednosti) vidi se da je prvi od njih dan sa:

$$\chi(x) = 1, \qquad \text{ako } x \equiv \pm 1 \ (mod\ 7) \tag{3.22}$$

$$\chi(x) = e^{4\pi i/3}, \ \text{ako } x \equiv \pm 2 \ (mod\ 7) \tag{3.23}$$

$$\chi(x) = e^{2\pi i/3}, \ \text{ako } x \equiv \pm 3 \ (mod\ 7), \tag{3.24}$$

a drugi sa:

$$\chi(x) = 1, \qquad \text{ako } x \equiv \pm 1 \ (mod\ 7) \tag{3.25}$$

$$\chi(x) = e^{2\pi i/3}, \ \text{ako } x \equiv \pm 2 \ (mod\ 7) \tag{3.26}$$

$$\chi(x) = e^{4\pi i/3}, \ \text{ako } x \equiv \pm 3 \ (mod\ 7). \tag{3.27}$$

Vidljivo je da su ta dva karaktera međusobno kompleksno konjugirana.

U primjeru (3) vidjeli smo da su karakteri reda 2 blisko povezani sa Legendreovim karakterima. Preciznije, imamo sljedeći rezultat:

Propozicija 3.2.1. *Neka je a kvadratno slobodan cijeli broj različit od nula i neka je $m = 4|a|$. Tada postoji jedinstveni karakter χ_a modulo m takav da je $\chi_a(p) = \left(\frac{a}{p}\right)$ za sve proste brojeve p koji ne dijele m. Taj karakter je reda 2, tj. vrijedi $\chi_a^2 = 1$, i $\chi_a \neq 1$ ako je $a \neq 1$.*

Dokaz. Ako χ_a postoji, jedinstvenost je jasna, i slijedi iz činjenice da je svaki cijeli broj relativno prost sa m produkt prostih brojeva koji ne dijele m, a vrijednost od χ_a je u njima jedinstveno određena jer je karakter χ_a definiran svojim vrijednostima u njima, pa je jedinstveno određena i za svaki cijeli broj relativno prost sa m. Isti argument, uzevši u obzir da je vrijednost Legendreovog simbola uvijek 1 ili -1, tada pokazuje i da je χ_a reda 2.

Dokažimo sada egzistenciju takvog karaktera. Promotrit ćemo dva slučaja, kada je a pozitivan i nije djeljiv sa 2 i kada a nije takav.

U prvom slučaju a možemo zapisati u obliku $a = l_1 \dots l_k$, gdje su $l_i, \forall i = 1, \dots, k$ međusobno različiti prosti brojevi (jer je a kvadratno slobodan, pa je $v_p(a) = 0$ ili 1, za svaki prost broj p), različiti od 2. Tada za χ_a uzimamo karakter definiran na sljedeći način:

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \left(\frac{x}{l_1}\right) \dots \left(\frac{x}{l_k}\right). \tag{3.28}$$

Pokažimo sada da ovaj karakter ima traženo svojstvo. Doista, ako je p prost broj različit od 2 i $l_i, \forall i = 1, \ldots, k$ (tj. ako p ne dijeli $m = 4|a|$), koristeći zakon kvadratnog reciprociteta (teorem 1.3.5) imamo:

$$\chi_a(p) = (-1)^{\varepsilon(p)\varepsilon(a)} \left(\frac{p}{l_1}\right) \ldots \left(\frac{p}{l_k}\right) = (-1)^{\varepsilon(p)\varepsilon(a)} (-1)^{\varepsilon(p)\varepsilon(l_1)} \left(\frac{l_1}{p}\right) \ldots (-1)^{\varepsilon(p)\varepsilon(l_k)} \left(\frac{l_k}{p}\right), \quad (3.29)$$

odnosno

$$\chi_a(p) = (-1)^{\varepsilon(p)\varepsilon(a)+\varepsilon(p)\varepsilon(l_1)+\ldots+\varepsilon(p)\varepsilon(l_k)} \left(\frac{l_1}{p}\right) \ldots \left(\frac{l_k}{p}\right), \quad (3.30)$$

pa uzevši u obzir da je karakter homomorfizam dobivamo:

$$\chi_a(p) = (-1)^{\varepsilon(p)\varepsilon(a)+\varepsilon(p)\varepsilon(l_1)+\ldots+\varepsilon(p)\varepsilon(l_k)} \left(\frac{l_1 l_2 \ldots l_k}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(a)+\varepsilon(p)\varepsilon(l_1)+\ldots+\varepsilon(p)\varepsilon(l_k)} \left(\frac{a}{p}\right). \quad (3.31)$$

Iskoristivši činjenicu da umnožak dva prosta broja različita od 2 koji daju iste ostatke pri dijeljenju sa 4 daje ostatak 1 pri dijeljenju sa 4, a ako su ti ostaci različiti onda daje ostatak 3 pri dijeljenju sa 4, lakim računom konačno imamo:

$$\chi_a(p) = \left(\frac{a}{p}\right). \quad (3.32)$$

Još nam je u ovom slučaju preostalo dokazati da je $\chi_a \neq 1$ ako je $a \neq 1$ (za $a = 1$ taj karakter je trivijalno jedinični). To ćemo uraditi tako da pronađemo x za koji je $\chi_a(x) = -1$. Cilj nam je da za takav x odgovarajući Legendreovi simboli budu 1 osim za jedan l_i (pa ćemo ga odabrati tako da daje ostatak 1 pri dijeljenju sa svim l_i osim jednog, a za taj ćemo staviti da je odgovarajući Legendreov simbol jednak -1) i da je $\varepsilon(x) = 0$, tj. da daje ostatak 1 i pri dijeljenju sa 4. Zbog toga uzimamo x tako da je:

$$\left(\frac{x}{l_1}\right) = -1, \qquad x \equiv 1 \ (mod\ 4l_2 \ldots l_k). \quad (3.33)$$

Sada imamo:

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \left(\frac{x}{l_1}\right) \ldots \left(\frac{x}{l_k}\right) = (-1)^0 \cdot (-1) \left(\frac{1}{l_2}\right) \ldots \left(\frac{1}{l_k}\right) = 1 \cdot (-1) \cdot 1 \ldots \cdot 1 = -1, \quad (3.34)$$

pa odabrani x zadovoljava željeno, i time je dokaz za ovaj slučaj završen.

Ostalo nam je vidjeti što se zbiva kad je a negativan i/ili djeljiv sa 2, tj. kada je oblika $-b$, $2b$ ili $-2b$, gdje je $b = l_1 \ldots l_k$ kao u gornjem slučaju. Tada za χ_a uzimamo produkt χ_b

sa $(-1)^{\varepsilon(x)}$, $(-1)^{\omega(x)}$ ili $(-1)^{\varepsilon(x)+\omega(x)}$, redom (da su to karakteri vidjeli smo iznad u primjeru (2)). Iz teorema 1.3.4 i prvog slučaja jasno je da tako dobiveni karakteri imaju traženo svojstvo. Analogno kao u prvom slučaju se dokazuje i da je $\chi_a \neq 1$.

Ovime je propozicija u potpunosti dokazana. □

Poglavlje 4

Dirichletov teorem

U prva tri poglavlja koristili smo samo algebarske metode. Nasuprot tome, u ovom ćemo poglavlju koristiti metode analitičke teorije brojeva, koja koristi metode iz matematičke analize (npr. holomorfne funkcije) za rješavanje problema u vezi cijelih brojeva. Pomoću tih metoda dobijeni su važni rezultati o prostim brojevima (teorem o njihovoj asimptotskoj distribuciji, koristeći svojstva Riemannove zeta funkcije), kao i u aditivnoj teoriji brojeva (rezultati u vezi s Goldbachovom hipotezom). U analitičkoj teoriji brojeva ne teži se dobivanju egzaktnih strukturalnih rezultata o cijelim brojevima, za što su algebarske i geometrijske metode mnogo pogodnije, nego nam ona daje aproksimativne ograde i procjene za različite funkcije bitne u teoriji brojeva. Ta grana matematike počela se razvijati Dirichletovim uvođenjem L-funkcija u svrhu dokazivanja teorema o prostim brojevima u aritmetičkim nizovima (tj. korištenjem koncepata matematičke analize u rješavanju algebarskog problema). U ovom poglavlju ilustrirat ćemo primjenu takvih metoda upravo na tom teoremu, za kojeg je Legendre prvi pretpostavio da vrijedi i koristio ga, i koji ćemo sada iskazati. Njegov dokaz, koji je dao Dirichlet, je glavni cilj ovoga rada.

Teorem 4.0.2. *Neka su a i m relativno prosti prirodni brojevi. Tada postoji beskonačno mnogo prostih brojeva p takvih da vrijedi $p \equiv a \pmod{m}$.*

Drugim riječima, ovaj teorem nam govori da u aritmetičkom nizu a, $a + m$, $a + 2m, \ldots, a + km, \ldots$ ima beskonačno mnogo prostih brojeva ako su a i m relativno prosti.

Ovaj teorem proširuje Euklidov teorem koji kaže da ima beskonačno mnogo prostih brojeva.

Mi ćemo dokazati jaču verziju teorema koja kaže da za svaki takav aritmetički niz suma recipročnih vrijednosti prostih brojeva u njemu divergira i da različiti takvi nizovi, ali istog modula, imaju približno isti udio prostih brojeva, tj. da su prosti brojevi "jednako distribuirani" (asimptotski) između različitih klasa kongruencije modulo m koje sadrže a-ove

relativno proste sa m, odnosno da je gustoća odgovarajućeg skupa jednaka $1/\phi(m)$.

Metoda koju ćemo slijediti i koju je rabio i sam Dirichlet koristi svojstva L-funkcija. U dokazu se koristi i Eulerov rad, povezujući Riemannovu zeta funkciju s distribucijom prostih brojeva.

4.1 Dirichletovi redovi

U ovom potpoglavlju prvo ćemo definirati neke pojmove i iskazati neke tvrdnje u vezi funkcija kompleksne varijable. Zatim ćemo uvesti pojam Dirichletova reda i proučiti njegova svojstva, kao i vidjeti što se događa kada su mu koeficijenti nenegativni. Na kraju ćemo promotriti jedan poseban Dirichletov red, bitan za daljnja razmatranja.

Podsjetimo se prvo nekih definicija koje će nam biti potrebne u ovom poglavlju.

Definicija 4.1.1. *Ako je funkcija $f : U \to \mathbb{C}$, gdje je $U \subseteq \mathbb{C}$ otvoren skup, kompleksno diferencijabilna u svakoj točki $z_0 \in U$, kažemo da je f holomorfna na U.*

Kažemo da je f holomorfna u točki $z_0 \in U$ ako je holomorfna na nekoj okolini od z_0.

Kažemo da je f holomorfna na nekom skupu A koji nije otvoren ako je holomorfna na nekom otvorenom skupu koji sadrži A.

Holomorfnu funkciju kojoj je domena cijeli $\mathbb{C}$ zovemo cijela funkcija.

Definicija 4.1.2. *Za funkciju $f : U \to \mathbb{C}$, gdje je $U \subseteq \mathbb{C}$ otvoren skup, kažemo da je analitička na U ako za svaki $z_0 \in U$ vrijedi:*

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n, \tag{4.1}$$

gdje su $a_i \in \mathbb{C}, \forall i \in \mathbb{N}_0$, i gornji red konvergira ka $f(z)$ za z u nekoj okolini od z_0.

Alternativno, analitička funkcija na U je beskonačno diferencijabilna funkcija takva da njen Taylorov red u bilo kojoj točki $z_0 \in U$,

$$T(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!} (z - z_0)^n, \tag{4.2}$$

konvergira ka $f(z)$ za z u nekoj okolini od z_0 po točkama.

Kažemo da je f analitička u točki $z_0 \in U$ ako je analitička na nekoj okolini od z_0.

Glavni teorem kompleksne analize kaže da je funkcija kompleksno analitička ako i samo ako je holomorfna pa se ti pojmovi često koriste u istom značenju.

Definicija 4.1.3. *Neka je $U \subseteq \mathbb{C}$ otvoren skup, $a \in U$ i $f : U\backslash\{a\} \to \mathbb{C}$ funkcija holomorfna na svojoj domeni. Ako postoji holomorfna funkcija $g : U \to \mathbb{C}$ i $n \in \mathbb{N}$ tako da vrijedi:*

$$f(z) = \frac{g(z)}{(z-a)^n}, \forall z \in U \setminus \{a\}, \tag{4.3}$$

tada a zovemo pol funkcije f, a najmanji takav n red tog pola.

Pol reda 1 *zovemo jednostavni pol.*

Prikaz funkcije f u obliku:

$$f(z) = \frac{a_{-n}}{(z-a)^n} + \ldots + \frac{a_{-1}}{z-a} + \sum_{k\geq 0} a_k(z-a)^k \tag{4.4}$$

zovemo njenim Laurentovim redom oko a. Dio s negativnim eksponentima zovemo glavnim dijelom od f, a $\sum\limits_{k\geq 0} a_k(z-a)^k$ (to je holomorfna funkcija na U) zovemo njenim regularnim dijelom.

Vidimo da ako je a pol od f vrijedi $\lim\limits_{z\to a} f(z) = \infty$.

Definicija 4.1.4. *Za funkciju $f : U \to \mathbb{C}$, gdje je $U \subseteq \mathbb{C}$ otvoren skup, kažemo da je meromorfna na U ako je holomorfna na cijelom U osim na skupu izoliranih točaka (polova funkcije), i oko svake od tih točaka može se razviti u Laurentov red.*

Očigledno je da se svaka meromorfna funkcija na U može izraziti kao kvocijent dvije holomorfne funkcije na U, pri čemu ona druga nije jednaka nul funkciji, i tada je svaki pol ujedno i nultočka druge funkcije.

Sada, bez dokaza, donosimo neke tvrdnje koje ćemo koristiti u daljnjem tekstu.

Lema 4.1.5. *Neka je U otvoren podskup od $\mathbb{C}$ i neka je $(f_n)_{n\in\mathbb{N}}$ niz holomorfnih funkcija na U koje uniformno konvergiraju na svakom kompaktnom skupu k funkciji f. Tada je i f holomorfna na U, i derivacije f_n' od f_n također uniformno konvergiraju na svim kompaktnim podskupovima k derivaciji f' od f.*

Lema 4.1.6. *Neka su (a_n) i (b_n) dva niza. Stavimo:*

$$A_{m,p} = \sum_{n=m}^{p} a_n, \qquad S_{m,m'} = \sum_{n=m}^{m'} a_n b_n. \tag{4.5}$$

Tada vrijedi:

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(b_n - b_{n+1}) + A_{m,m'}b_{m'}. \tag{4.6}$$

Lema 4.1.7. *Neka su $\alpha, \beta \in \mathbb{R}$ takvi da je $0 < \alpha < \beta$. Neka je $z = x + iy$, pri čemu su $x, y \in \mathbb{R}$ i $x > 0$. Tada vrijedi:*

$$|e^{-\alpha z} - e^{-\beta z}| \leq \left|\frac{z}{x}\right| (e^{-\alpha x} - e^{-\beta x}). \tag{4.7}$$

Uvedimo sada pojam Dirichletova reda, koji će nam biti od presudne važnosti pri dokazu Dirichletovog teorema.

Neka je (λ_n) rastući niz realnih brojeva za kojeg vrijedi $\lim_{n\to\infty} \lambda_n = \infty$. Radi jednostavnosti, pretpostavit ćemo da je $\lambda_n \geq 0, \forall n$. To možemo uraditi jer je uvijek moguće početni slučaj svesti na takav izostavljanjem konačnog broja članova (onih u kojima je λ_n negativan, a njih je konačno jer naš niz ide u beskonačnost) reda kojeg ćemo u nastavku promatrati, jer to ne utječe na njegova bitna svojstva.

Dirichletov red s eksponentima (λ_n) je red oblika

$$\sum a_n e^{-\lambda_n z}, \tag{4.8}$$

pri čemu je $a_n \in \mathbb{C}, \forall n$, i $z \in \mathbb{C}$.

Navedimo sada dva primjera Dirichletovog reda.

(1) Uzmimo $\lambda_n = ln\ n$. Tada za odgovarajući Dirichletov red imamo:

$$\sum a_n e^{-\lambda_n z} = \sum a_n e^{-ln\ n \cdot z} = \sum a_n (e^{ln\ n})^{-z} = \sum a_n n^{-z} = \sum a_n / n^z, \tag{4.9}$$

tj. to je red $\sum a_n/n^z$.

(2) Uzmimo $\lambda_n = n$. Pripadni Dirichletov red, uz supstituciju $t = e^{-z}$, je:

$$\sum a_n e^{-\lambda_n z} = \sum a_n e^{-nz} = \sum a_n t^n, \tag{4.10}$$

tj. dobivamo red potencija u t, $\sum a_n t^n$.

Sljedeća propozicija nam govori u kakvoj domeni Dirichletov red, ako imamo konvergenciju u jednoj točki, uniformno konvergira.

Propozicija 4.1.8. *Ako red $f(z) = \sum a_n e^{-\lambda_n z}$ konvergira u $z = z_0$, tada on uniformno konvergira u svakoj domeni oblika $Re(z - z_0) \geq 0$, $Arg(z - z_0) \leq \alpha$, pri čemu je $\alpha < \pi/2$.*

Dokaz. Radi jednostavnosti, napravimo translaciju na z (tj. zamijenimo z sa $z - z_0$) pa možemo pretpostaviti da je $z_0 = 0$. Po pretpostavci onda imamo da red $f(z) = \sum a_n$

konvergira, i moramo dokazati da tada red $f(z) = \sum a_n e^{-\lambda_n z}$ uniformno konvergira u svakoj domeni oblika $Re(z) \geq 0$, $Arg(z) \leq \alpha$, gdje je $\alpha < \pi/2$. Drugi uvjet možemo napisati u obliku $\cos(Arg(z)) > 0$, pa postoji $k \in \mathbb{N}$ takav da je $\cos(Arg(z)) \geq \frac{1}{k}$. Iz definicije kosinusa tada slijedi $Re(z)/|z| \geq \frac{1}{k}$, tj. $|z|/Re(z) \leq k$.

Dokažimo sada traženu uniformnu konvergenciju. Neka je $\varepsilon > 0$. Trebamo dakle pronaći $N \in \mathbb{N}$ takav da za svaki $m, m' \geq N$ imamo $\left|\sum_{n=m}^{m'} a_n e^{-\lambda_n z}\right| < \varepsilon$ (jer to znači da je niz parcijalnih suma našeg reda Cauchyjev, a kako je $\mathbb{C}$ potpun prostor, on je tada i konvergentan, pa je to i promatrani red; ovo ćemo koristiti i kasnije), za svaki z iz promatrane domene. S obzirom da red $f(z) = \sum a_n$ konvergira, postoji $N \in \mathbb{N}$ takav da za svaki $m, m' \geq N$ vrijedi $\left|\sum_{n=m}^{m'} a_n\right| < \frac{\varepsilon}{1+k}$, odnosno primjenom notacije iz Abelove leme 4.1.6, $|A_{m,m'}| < \frac{\varepsilon}{1+k}$. Upotrebom te leme, uz $b_n = e^{-\lambda_n z}$ (tada je $S_{m,m'} = \sum_{n=m}^{m'} a_n e^{-\lambda_n z}$), dobivamo:

$$S_{m,m'} = \sum_{n=m}^{m'-1} A_{m,n}(e^{-\lambda_n z} - e^{-\lambda_{n+1} z}) + A_{m,m'} e^{-\lambda_{m'} z}. \tag{4.11}$$

Stavimo sada $z = x + iy$, pa iz zadanih uvjeta imamo $x \geq 0$ i $|z|/x \leq k$. Uz pomoć leme 4.1.7 (sve pretpostavke su zadovoljene) i činjenice da je $n \geq m \geq N$ slijedi:

$$|S_{m,m'}| < \frac{\varepsilon}{1+k}\left(\sum_{n=m}^{m'-1} |e^{-\lambda_n z} - e^{-\lambda_{n+1} z}| + |e^{-\lambda_{m'} z}|\right) \leq \frac{\varepsilon}{1+k}\left(\frac{|z|}{x}\sum_{n=m}^{m'-1}(e^{-\lambda_n x} - e^{-\lambda_{n+1} x}) + 1\right). \tag{4.12}$$

Sada, uz korištenje nejednakosti $|z|/x \leq k$, odmah vidimo da je

$$\left|\sum_{n=m}^{m'} a_n e^{-\lambda_n z}\right| = |S_{m,m'}| < \frac{\varepsilon}{1+k}\left(1 + k(e^{-\lambda_m x} - e^{-\lambda_{m'} x})\right) \leq \frac{\varepsilon}{1+k}(1+k) = \varepsilon \tag{4.13}$$

za svaki $m, m' \geq N$ i za svaki z iz promatrane domene.

Ovo je upravo ono što smo i trebali dokazati, tj. red $f(z) = \sum a_n e^{-\lambda_n z}$ uniformno konvergira (jer N ne ovisi o z) u svakoj domeni željenog oblika. □

Navedimo sada nekoliko posljedica ove propozicije.

Korolar 4.1.9. *Ako f konvergira za $z = z_0$ tada konvergira za svaki z takav da je $Re(z) > Re(z_0)$ i tako definirana funkcija je holomorfna.*

Dokaz. Prvi dio tvrdnje direktno slijedi iz upravo dokazane propozicije, a drugi iz leme 4.1.5, kada tvrdnju primijenimo na niz funkcija $f_n(z) = a_n e^{-\lambda_n z}$. □

Korolar 4.1.10. *Skup konvergencije reda f sadrži maksimalnu otvorenu poluravninu.*

Poluravninu iz gornjeg korolara zovemo poluravnina konvergencije.

Također, i $\emptyset$ i $\mathbb{C}$ smatramo otvorenim poluravninama.

Ako je poluravnina konvergencija dana sa $Re(z) > \rho$, kažemo da je ρ apscisa konvergencije promatranog reda. Kada su poluravnine u pitanju $\emptyset$ i $\mathbb{C}$, odgovarajuće apscise konvergencije su $\rho = +\infty$ i $\rho = -\infty$, redom.

Poluravnina konvergencije reda $|a_n|e^{-\lambda_n z}$ naziva se poluravninom aposlutne konvergencije reda f, i njegovu apscisu konvergencije označavamo sa ρ^+. Kada je $\lambda_n = n$, tj. kada imamo red potencija kao što smo vidjeli u (4.10), općepoznata je činjenica da je $\rho = \rho^+$. Ali, to ne vrijedi općenito. Na primjer, za L-red,

$$L(z) = 1 - \frac{1}{3^z} + \frac{1}{5^z} - \frac{1}{7^z} + \ldots, \tag{4.14}$$

vrijedi da je $\rho = 0$, a $\rho^+ = 1$, što ćemo kasnije i vidjeti.

Korolar 4.1.11. *Red $f(z)$ konvergira ka $f(z_0)$ kada $z \to z_0$ u domeni*

$$Re(z - z_0) \geq 0, \quad |Arg(z - z_0)| \leq \alpha, \tag{4.15}$$

pri čemu je $\alpha < \pi/2$.

Dokaz. Ovo odmah slijedi iz uniformne konvergencije promatranog reda i činjenice da $e^{-\lambda_n z} \to e^{-\lambda_n z_0}$ kada $z \to z_0$. □

Korolar 4.1.12. *Ako je funkcija $f(z)$ identički jednaka nuli, onda su svi njeni koeficijenti a_n nula.*

Dokaz. Pokažimo da ako je $f(z)$ identički jednaka nuli, onda je $a_0 = 0$. Pomnožimo f sa $e^{\lambda_0 z}$:

$$e^{\lambda_0 z} f(z) = a_0 + \sum_{n=1}^{\infty} a_n e^{(\lambda_0 - \lambda_n)z}. \tag{4.16}$$

Kako je $\lambda_0 \leq \lambda_n, \forall n \in \mathbb{N}$, ako $z \to +\infty$ (i uzmimo da je z realan broj), iz uniformne konvergencije imamo da tada $e^{\lambda_0 z} f \to a_0$. S obzirom da je f identički jednaka nuli, slijedi da je i $e^{\lambda_0 z} f$ identički jednaka nuli, tj. da je $a_0 = 0$. Analagno pokazujemo da su i ostali a_n jednaki nuli, čime je tvrdnja dokazana. □

Dokažimo sada jedan rezultat o Dirichletovim redovima s nenegativnim koeficijentima, u kojem ćemo vidjeti pod kojim uvjetom možemo proširiti domenu konvergencije tog reda.

Propozicija 4.1.13. *Neka je $f(z) = \sum a_n e^{-\lambda_n z}$ Dirichletov red takav da vrijedi $a_n \geq 0$, tj. da su mu koeficijenti nenegativni realni brojevi. Pretpostavimo da f konvergira za $Re(z) > \rho$, gdje je $\rho \in \mathbb{R}$, i da se funkcija f može proširiti analitički do funkcije holomorfne u okolini točke $z = \rho$. Tada postoji $\varepsilon > 0$ takav da f konvergira za $Re(z) > \rho - \varepsilon$.*

Dokaz. Nakon što zamijenimo z sa $z - \rho$, možemo pretpostaviti da je $\rho = 0$. Po pretpostavci je f tada holomorfna za $Re(z) > 0$ i u okolini od 0 pa postoji $\varepsilon > 0$ tako da je f holomorfna u disku $|z - 1| \leq 1 + \varepsilon$. Kako je funkcija kompleksno analitička ako i samo ako je holomorfna, slijedi da je f analitička u tom disku, odnosno njen Taylorov red konvergira u tom disku. Pokažimo sada da dani Dirichletov red konvergira za $z = -\varepsilon$.

Iz leme 4.1.5 za p.-tu derivaciju od f imamo:

$$f^{(p)}(z) = \sum_n (a_n e^{-\lambda_n z})^{(p)} = \sum_n a_n (-\lambda_n)^p e^{-\lambda_n z} = (-1)^p \sum_n \lambda_n^p a_n e^{-\lambda_n z} \tag{4.17}$$

za $Re(z) > 0$.

Prema tome, vrijedi

$$f^{(p)}(1) = (-1)^p \sum_n \lambda_n^p a_n e^{-\lambda_n}. \tag{4.18}$$

Taylorov red u pitanju, tj. Taylorov red od f oko 1, može se napisati na sljedeći način (jer on konvergira u disku $|z - 1| \leq 1 + \varepsilon$):

$$f(z) = \sum_{p=0}^{\infty} \frac{1}{p!} (z - 1)^p f^{(p)}(1), \tag{4.19}$$

za z takve da je $|z - 1| \leq 1 + \varepsilon$.

Posebno, za $z = -\varepsilon$ (unutar je promatranog diska), imamo:

$$f(-\varepsilon) = \sum_{p=0}^{\infty} \frac{1}{p!} (-\varepsilon - 1)^p f^{(p)}(1) = \sum_{p=0}^{\infty} \frac{1}{p!} (1 + \varepsilon)^p (-1)^p f^{(p)}(1), \tag{4.20}$$

i taj red je očito konvergentan.

Uz korištenje (4.18) dobivamo

$$(-1)^p f^{(p)}(1) = \sum_n \lambda_n^p a_n e^{-\lambda_n}, \tag{4.21}$$

i to je također konvergentan red, s nenegativnim koeficijentima.

Sada iz (4.20) i (4.21) dobivamo dvostruki red

$$f(-\varepsilon) = \sum_{p,n} a_n \frac{1}{p!}(1+\varepsilon)^p \lambda_n^p e^{-\lambda_n}, \tag{4.22}$$

koji po iznad rečenom konvergira i čiji su koeficijenti nenegativni. Zbog toga možemo pregrupirati članove (jer red apsolutno konvergira s obzirom da konvergira i da su mu koeficijenti nenegativni, a znamo da u tom slučaju suma reda ostaje ista kojim god redom mu zbrajali članove), pa vrijedi:

$$f(-\varepsilon) = \sum_n a_n e^{-\lambda_n} \sum_{p=0}^{\infty} \frac{1}{p!}(1+\varepsilon)^p \lambda_n^p = \sum_n a_n e^{-\lambda_n} e^{\lambda_n(1+\varepsilon)} = \sum_n a_n e^{\lambda_n \varepsilon}. \tag{4.23}$$

Ovo upravo znači da dani Dirichletov red konvergira za $z = -\varepsilon$ (jer mu je vrijednost jednaka vrijednosti funkcije f u toj točki). Po korolaru 4.1.9 imamo da tada f konvergira i za $Re(z) > -\varepsilon$, čime je dokaz gotov. □

Za kraj ovog potpoglavlja pobliže ćemo promotriti jedan poseban Dirichletov red koji će nam biti potreban kasnije.

Uzmimo $\lambda_n = ln\ n$. Kao što smo vidjeli u (4.9) tada je odgovarajući Dirichletov red

$$f(s) = \sum_{n=1}^{\infty} a_n / n^s. \tag{4.24}$$

Ovdje je s tradicionalna oznaka za varijablu.

Dokažimo sada dvije tvrdnje o konvergenciji ovog reda.

Propozicija 4.1.14. *Ako koeficijenti a_n čine omeđen niz, tada promatrani red apsolutno konvergira za $Re(s) > 1$.*

Dokaz. S obzirom da su koeficijenti a_n omeđeni, postoji $K \in \mathbb{R}$ takav da vrijedi $|a_n| \leq K$, $\forall n \in \mathbb{N}$. Zbog toga imamo:

$$\sum_{n=1}^{\infty} |a_n|/n^s \leq \sum_{n=1}^{\infty} K/n^s = K \sum_{n=1}^{\infty} 1/n^s. \tag{4.25}$$

Poznato je da red $\sum_{n=1}^{\infty} 1/n^\alpha$ konvergira za $\alpha > 1$ pa smo dakle red $\sum_{n=1}^{\infty} |a_n|/n^s$ ograničili s konvergentnim redom, za $s > 1$, odnosno $Re(s) > 1$. Prema tome, i on sam konvergira u toj domeni. Dakle, naš promatrani red apsolutno konvergira za $Re(s) > 1$, što smo i trebali dokazati. □

Propozicija 4.1.15. *Ako su parcijalne sume* $A_{m,p} = \sum_{n=m}^{p} a_n$ *omeđene, tada promatrani red konvergira (ne nužno apsolutno) za* $Re(s) > 0$.

Dokaz. Po pretpostavci postoji $K \in \mathbb{R}$ takav da je $|A_{m,p}| \leq K$, $\forall m, p \in \mathbb{N}$. Sada ćemo iskoristiti Abelovu lemu 4.1.6, za $b_n = 1/n^s$ (tada je $S_{m,m'} = \sum_{n=m}^{m'} a_n/n^s$):

$$|S_{m,m'}| \leq K\left(\sum_{n=m}^{m'-1}\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| + \left|\frac{1}{m'^s}\right|\right). \tag{4.26}$$

Po propoziciji 4.1.8 možemo pretpostaviti da je $s \in \mathbb{R}$ pa prethodnu nejednakost lakim računom pojednostavljujemo, te dobivamo:

$$|S_{m,m'}| \leq K/m^s. \tag{4.27}$$

Iz ovoga je jasno da, ako je $s > 0$, za svaki $\varepsilon > 0$ možemo naći $N \in \mathbb{N}$ takav da $\forall m, m' \geq N$ vrijedi $|S_{m,m'}| = |\sum_{n=m}^{m'} a_n/n^s| < \varepsilon$. To je upravo ono što smo i trebali dokazati, tj. red $f(s) = \sum_{n=1}^{\infty} a_n/n^s$ konvergira za $s > 0$, odnosno $Re(s) > 0$. □

4.2 Zeta funkcija i L-funkcije

U ovom potpoglavlju prvo ćemo promotriti multiplikativne funkcije i povezati ih s Dirichletovim redovima. Nakon toga ćemo definirati jednu veoma bitnu funkciju u analitičkoj teoriji brojeva, zeta funkciju, i proučiti neka njena svojstva. Zatim ćemo uvesti pojam L-funkcija, koje su povezane s modularnim karakterima, i imaju ključnu ulogu u dokazu Dirichletovog teorema, te ih pobliže promotriti. Na kraju potpoglavlja bavit ćemo se produktom L-funkcija po svim karakterima modulo m, gdje je $m \in \mathbb{N}$ fiksiran, i u vezi s time dokazati esencijalnu tvrdnju u dokazu Dirichletovog teorema.

U ovom potpoglavlju i nadalje, $\mathbb{P}$ označava skup prostih brojeva.

Za početak ćemo dati definiciju multiplikativne funkcije.

Definicija 4.2.1. *Funkciju* $f : \mathbb{N} \to \mathbb{C}$ *nazivamo multiplikativnom funkcijom ako zadovoljava sljedeća dva svojstva:*

$$f(1) = 1 \tag{4.28}$$

$$f(mn) = f(m)f(n), \tag{4.29}$$

za sve relativno proste m i n.

Primjer takve funkcije je Eulerova ϕ funkcija (definicija 1.1.2).

Neka je f omeđena multiplikativna funkcija. Sada ćemo dokazati dvije leme koje nam govore o konvergenciji Dirichletovog reda (4.24) s odgovarajućim koeficijentima jednakim $f(n)$, tj. daju nam njegov zapis (u odgovarajućoj domeni) pomoću Eulerovog produkta, beskonačnog produkta indeksiranog prostim brojevima.

Lema 4.2.2. *Dirichletov red* $\sum_{n=1}^{\infty} f(n)/n^s$ *apsolutno konvergira za* $Re(s) > 1$ *i njegova suma u toj domeni jednaka je konvergentnom beskonačnom produktu*

$$\prod_{p\in\mathbb{P}}(1 + f(p)p^{-s} + \ldots + f(p^m)p^{-ms} + \ldots). \tag{4.30}$$

Dokaz. Prva tvrdnja direktno slijedi iz propozicije 4.1.14, jer je u ovom slučaju $a_n = f(n)$, $\forall n \in \mathbb{N}$, a f je omeđena funkcija. Dokažimo sada i drugu tvrdnju.

Neka je S konačni skup prostih brojeva i neka je $\mathbb{N}(S)$ skup prirodnih brojeva čiji su svi prosti faktori iz S. Uz korištenje multiplikativnosti funkcije f, jasno je da tada vrijedi sljedeće:

$$\prod_{p\in S}(1 + f(p)p^{-s} + \ldots + f(p^m)p^{-ms} + \ldots) = \sum_{n\in\mathbb{N}(S)} f(n)/n^s, \tag{4.31}$$

odnosno

$$\sum_{n\in\mathbb{N}(S)} f(n)/n^s = \prod_{p\in S}\left(\sum_{m=0}^{\infty} f(p^m)p^{-ms}\right). \tag{4.32}$$

Kada skup S pustimo da "raste" u skup svih prostih brojeva, $\mathbb{P}$, suma s lijeve strane jednakosti iznad teži u sumu po svim prirodnim brojevima, tj. u $\sum_{n=1}^{\infty} f(n)/n^s$. Prema tome, beskonačni produkt $\prod_{p\in\mathbb{P}}(1 + f(p)p^{-s} + \ldots + f(p^m)p^{-ms} + \ldots) = \prod_{p\in\mathbb{P}}\left(\sum_{m=0}^{\infty} f(p^m)p^{-ms}\right)$ također konvergira za $Re(s) > 1$ i njegova vrijednost jednaka je $\sum_{n=1}^{\infty} f(n)/n^s$, a to je i trebalo dokazati. □

Lema 4.2.3. *Ako je f multiplikativna u strogom smislu (tj. ako je $f(nn') = f(n)f(n')$ za sve $n, n' \in \mathbb{N}$), tada vrijedi:*

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p\in\mathbb{P}} \frac{1}{1 - f(p)/p^s}. \tag{4.33}$$

Dokaz. S obzirom da je f multiplikativna u strogom smislu, vrijedi $f(p^m) = f(p)^m, \forall p \in \mathbb{P}, \forall m \in \mathbb{N}_0$. Sada iz toga i leme iznad slijedi:

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p\in\mathbb{P}}(1 + f(p)/p^s + \ldots + f(p)^m/(p^s)^m + \ldots) = \tag{4.34}$$

$$= \prod_{p\in\mathbb{P}}(1 + f(p)/p^s + \ldots + (f(p)/p^s)^m + \ldots) = \prod_{p\in\mathbb{P}} \frac{1}{1 - f(p)/p^s}, \tag{4.35}$$

pri čemu zadnja jednakost vrijedi jer je u pitanju geometrijski red; ovime je dokaz gotov. □

Sada ćemo prethodna razmatranja primijeniti na jedan specijalni slučaj, tj. uzet ćemo $f = 1$. S obzirom da je ta funkcija multiplikativna u strogom smislu, možemo primijeniti prethodnu lemu i tako dobivamo funkciju

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}, \tag{4.36}$$

znanu kao (Riemannova) zeta funkcija

Ova formula, po viđenom iznad, ima smisla za $Re(s) > 1$. Nju je dokazao Leonhard Euler i zato se takvi produkti nazivaju Eulerovim produktima.

Sljedeća propozicija govori nam o holomorfnosti zeta funkcije.

Propozicija 4.2.4. (*a*) *Zeta funkcija je holomorfna i različita od* 0 *u poluravnini* $Re(s) > 1$. (*b*) *Postoji funkcija* ϕ *holomorfna za* $Re(s) > 0$ *takva da vrijedi:*

$$\zeta(s) = \frac{1}{s-1} + \phi(s), \tag{4.37}$$

za sve s koji zadovoljavaju $Re(s) > 1$.

Dokaz. Tvrdnja (*a*) je jasna. Dokažimo sada tvrdnju (*b*).

Želimo $\zeta(s)$ prikazati u traženom obliku pa u tu svrhu krenimo od sljedećeg izraza koji očigledno vrijedi:

$$\frac{1}{s-1} = \int_1^{\infty} t^{-s}dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}dt. \tag{4.38}$$

Prema tome, $\zeta(s)$ možemo napisati kao

$$\zeta(s) = \frac{1}{s-1} + \sum_{n=1}^{\infty} \frac{1}{n^s} - \frac{1}{s-1} = \frac{1}{s-1} + \sum_{n=1}^{\infty} \left(\frac{1}{n^s} - \int_n^{n+1} t^{-s} dt \right) = \tag{4.39}$$

$$= \frac{1}{s-1} + \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s}) dt. \tag{4.40}$$

Sada stavimo

$$\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt \tag{4.41}$$

i

$$\phi(s) = \sum_{n=1}^{\infty} \phi_n(s), \tag{4.42}$$

pa tada imamo da je

$$\zeta(s) = \frac{1}{s-1} + \phi(s). \tag{4.43}$$

Preostalo nam je još pokazati da ϕ doista ima tražena svojstva, tj. da je definirana i holomorfna za $Re(s) > 0$. No, jasno je da ϕ_n, $\forall n \in \mathbb{N}$, imaju ta svojstva, pa je dovoljno dokazati da red $\sum \phi_n$ konvergira normalno na svim kompaktnim skupovima za $Re(s) > 0$. Dovoljnost toga slijedi iz činjenice da normalna konvergencija povlači uniformnu konvergenciju pa iz leme 4.1.5 tada dobivamo traženo. Dokažimo sada normalnu konvergenciju.

Po definiciji normalne konvergencije, kako bismo dokazali da red $\sum_{n=1}^{\infty} \phi_n(s)$ normalno konvergira trebamo pokazati da red uniformnih normi članova tog reda konvergira, tj. da vrijedi

$$\sum_{n=1}^{\infty} ||\phi_n|| = \sum_{n=1}^{\infty} \sup |\phi_n(s)| < \infty. \tag{4.44}$$

Ograničimo sad $\phi_n(s)$. Iz teorema srednje vrijednosti za integrale imamo:

$$\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s}) dt = n^{-s} - y^{-s}, \tag{4.45}$$

za neki $y \in < n, n+1 >$. Iz toga slijedi

$$|\phi_n(s)| = |n^{-s} - y^{-s}| \leq \sup_{n \leq t \leq n+1} |n^{-s} - t^{-s}|. \tag{4.46}$$

Kako je podintegralna funkcija rastuća, to znači da se supremum postiže u $n+1$:

$$|\phi_n(s)| \leq |n^{-s} - (n+1)^{-s}|. \tag{4.47}$$

No, derivacija podintegralne funkcije jednaka je s/t^{s+1} pa iz teorema srednje vrijednosti za tu funkciju slijedi

$$(n^{-s} - (n+1)^{-s}) - (n^{-s} - n^{-s}) = s/z^{s+1}, \tag{4.48}$$

za neki $z \in < n, n+1 >$, tj.

$$n^{-s} - (n+1)^{-s} = s/z^{s+1}. \tag{4.49}$$

Sada iz toga i (4.47) imamo

$$|\phi_n(s)| \leq |s/z^{s+1}|, \tag{4.50}$$

a kako je funkcija s/t^{s+1} padajuća, iz toga dobivamo

$$|\phi_n(s)| \leq |s/n^{s+1}|. \tag{4.51}$$

Konačno imamo

$$|\phi_n(s)| \leq \frac{|s|}{n^{x+1}}, \tag{4.52}$$

gdje je $x = Re(s)$.

Iskoristimo upravo dobiveno za određivanje potrebne sume iz (4.44):

$$\sum_{n=1}^{\infty} \sup |\phi_n(s)| \leq \sum_{n=1}^{\infty} \frac{|s|}{n^{x+1}} = |s| \sum_{n=1}^{\infty} \frac{1}{n^{x+1}}. \tag{4.53}$$

No, znamo da red u zadnjoj jednakosti konvergira za $x+1 > 1$, tj. za $x > 0$, odnosno $Re(s) > 0$, pa kako je red $\sum_{n=1}^{\infty} \sup |\phi_n(s)|$ ograničen njime i on konvergira u toj domeni. Dakle, prema gore rečenom, red $\sum_{n=1}^{\infty} \phi_n(s)$ normalno konvergira za $Re(s) > 0$, što smo i htjeli dokazati.

Ovime je postojanje funkcije ϕ traženih svojstva u potpunosti dokazano, pa i tvrdnja (b) vrijedi. □

Ova propozicija nam omogućuje da zeta funkciju holomorfno proširimo do meromorfne funkcije za $Re(s) > 0$ (odnosno holomorfne za $Re(s) > 0$, osim u skupu izoliranih točaka, tj. polova funkcije), te imamo sljedeći njen korolar:

Korolar 4.2.5. *$s = 1$ je jednostavni pol zeta funkcije.*

Navedimo sada još jedan korolar ove propozicije, koji će se kasnije pokazati veoma važnim.

Korolar 4.2.6. *Kada $s \to 1$, imamo*

$$\sum_{p\in\mathbb{P}} p^{-s} \sim ln\ \frac{1}{s-1}, \tag{4.54}$$

i suma

$$\sum_{p,k\geq 2} \frac{1}{p^{ks}} \tag{4.55}$$

ostaje omeđena.

Dokaz. U ovom dokazu koristit ćemo prirodni logaritam funkcije $\zeta(s)$. Kako prirodni logaritam na kompleksnim brojevima nije funkcija u pravom smislu te riječi (jer njena vrijednost nije jednoznačno određena u svakoj točki), prvo ćemo precizirati što mislimo pod tim izrazom.

$\zeta(s)$ je definirana produktom $\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}}$. Za $Re(s) > 1$ svaki faktor je oblika $1/(1-\alpha)$, pri čemu je očito $|\alpha| = \left|\frac{1}{p^s}\right| < 1$. Sada definiramo $ln\ \frac{1}{1-\alpha}$, za $|\alpha| < 1$, na sljedeći način:

$$ln\ \frac{1}{1-\alpha} = \sum_{k=1}^{\infty} \frac{\alpha^k}{k}, \tag{4.56}$$

pa zatim i ln $\zeta(s)$ pomoću reda:

$$ln\ \zeta(s) = ln \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^s}} = \sum_{p\in\mathbb{P}} ln\ \frac{1}{1-\frac{1}{p^s}} = \sum_{p\in\mathbb{P},k\geq 1} \frac{1}{k\cdot p^{ks}}. \tag{4.57}$$

Zadnja jednakost vrijedi po (4.56), za $\alpha = \frac{1}{p^s}$, pri čemu je $Re(s) > 1$; ovaj red je očito konvergentan.

Razdvojimo $\ln \zeta(s)$ u dva dijela:

$$ln\ \zeta(s) = \sum_{p\in\mathbb{P}} \frac{1}{p^s} + \psi(s), \tag{4.58}$$

gdje je $\psi(s) = \sum_{p\in\mathbb{P},k\geq 2} \frac{1}{k\cdot p^{ks}}$. Ograničimo sada red ψ:

$$\psi(s) \leq \sum_{p,k\geq 2} \frac{1}{p^{ks}} \leq \sum \frac{1}{p^s(p^s-1)} \leq \sum \frac{1}{p(p-1)} \leq \tag{4.59}$$

$$\leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n}\right) = 1. \tag{4.60}$$

Vidljivo je da $\sum_{p,k\geq 2} \frac{1}{p^{ks}}$, kada $s \to 1$, doista ostaje omeđena i druga tvrdnja je dokazana. Provjerimo sada da i prva tvrdnja vrijedi.

Iz gornjih nejednakosti vidimo da je i ψ omeđena, a iz prethodnog korolara da je $ln\ \zeta(s) \sim ln\ \frac{1}{s-1}$, kada $s \to 1$. Sada iz te dvije činjenice i (4.58) imamo da, kada $s \to 1$, onda $\sum_{p\in\mathbb{P}} p^{-s} \sim ln\ \frac{1}{s-1}$, a to je upravo prva tvrdnja, čime je dokaz gotov. □

Zeta funkcija od velike je važnosti u analitičkoj teoriji brojeva. Ona se može analitički proširiti do meromorfne funkcije na $\mathbb{C}$ s jedinim polom $s = 1$. Funkcija definirana sa $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ tada je meromorfna i zadovoljava funkcionalnu jednadžbu $\xi(s) = \xi(1-s)$.

Nadalje, zeta funkcija poprima racionalne vrijednosti u negativnim cijelim brojevima. Štoviše, svi parni negativni cijeli brojevi su njene nultočke, i one se nazivaju trivijalnim nultočkama. Riemannova hipoteza, jedan od najvažnijih neriješenih matematičkih problema današnjice, govori nam da su sve ostale, netrivijalne, nultočke od ζ na pravcu $Re(s) = \frac{1}{2}$. Ona je numerički provjerena za mnoge brojeve, i dokazano je da je beskonačno mnogo nultočaka na tom pravcu, ali još nije dokazano da niti jedna netrivijalna nultočka nije izvan njega, tj. da su sve na njemu, kao što nije pronađena niti jedna netrivijalna nultočka koja nije na njemu.

Sada ćemo uvesti pojam L-funkcije, koja je od presudne važnosti u dokazu Dirichletovog teorema. Neka je $m \in \mathbb{N}$, a χ karakter modulo m. Odgovarajuća L-funkcija tada je definirana ovim Dirichletovim redom:

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s. \tag{4.61}$$

Primijetimo da u ovoj sumi zapravo sudjeluju samo oni n koji su relativno prosti sa m, jer je u suprotnom $\chi(n) = 0$.

Pogledajmo sad što se zbiva ako za χ uzmemo jedinični karakter.

Propozicija 4.2.7. *Za $\chi = 1$ imamo*

$$L(s, 1) = F(s)\zeta(s), \tag{4.62}$$

gdje je

$$F(s) = \prod_{p|m}(1 - p^{-s}). \tag{4.63}$$

Posebno, $L(s, 1)$ se analitički proširuje za $Re(s) > 0$ i ima jednostavni pol u $s = 1$.

Dokaz. Prva tvrdnja slijedi iz formule

$$\zeta(s) = \sum_{n=1}^{\infty} 1/n^s = \prod_{p\in\mathbb{P}} \frac{1}{1 - p^{-s}}, \tag{4.64}$$

uzevši u obzir da je vrijednost jediničnog karaktera za p koji dijele m (odnosno za one koji nisu relativno prosti s njim) jednaka nuli, a za ostale proste brojeve (svi preostali su relativno prosti sa m) jednaka jedan.

Druga tvrdnja očito vrijedi, po razmatranjima koja smo ispred napravili o zeta funkciji. □

Dakle, ovaj slučaj nam ne donosi ništa bitno novo. Pogledajmo sada što se događa kada odgovarajući karakter nije jedinični.

Propozicija 4.2.8. *Za $\chi \neq 1$ red $L(s,\chi)$ konvergira (odnosno apsolutno konvergira) u poluravnini $Re(s) > 0$ (odnosno $Re(s) > 1$) te imamo*

$$L(s,\chi) = \prod_{p\in\mathbb{P}} \frac{1}{1 - \dfrac{\chi(p)}{p^s}}, \tag{4.65}$$

za $Re(s) > 1$.

Dokaz. Tvrdnje povezane s poluravninom $Re(s) > 1$ direktno slijede iz lema 4.2.2 i 4.2.3 jer je karakter multiplikativan u strogom smislu pa nam je još preostalo dokazati da ovaj red konvergira u poluravnini $Re(s) > 0$. Uradimo to.

Dovoljno je pokazati da su parcijalne sume

$$A_{u,v} = \sum_{n=u}^{v} \chi(n), \tag{4.66}$$

pri čemu je $u \leq v$, omeđene, jer tada po propoziciji 4.1.15 imamo konvergenciju reda $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$ za $Re(s) > 0$.

Kako je χ karakter modulo m i $\chi \neq 1$, iz propozicije 3.1.6 dobivamo

$$\sum_{n=u}^{u+m-1} \chi(n) = 0. \tag{4.67}$$

Prema tome, dovoljno je ograničiti parcijalne sume $A_{u,v}$ za $v - u < m$, jer ako je razlika veća, jednostavno "maknemo" sume gornjeg oblika, koje su jednake 0. Imamo:

$$|A_{u,v}| = |\sum_{n=u}^{v} \chi(n)| \leq \sum_{n=u}^{v} |\chi(n)|, \tag{4.68}$$

pri čemu je $v - u < m$. U trećem poglavlju vidjeli smo da ako je χ karakter modulo m i $(n,m) = 1$, onda je $\chi(n)$ $\phi(m)$.-ti korijen iz jedinice, tj. $|\chi(n)| = 1$. Brojeva manjih od m koji su relativno prosti sa m ima $\phi(m)$, a za ostale je vrijednost karaktera u njima jednaka 0, pa iz svega toga dobivamo

$$|A_{u,v}| \leq \sum_{n=u}^{v} |\chi(n)| \leq \phi(m) \cdot 1 = \phi(m). \tag{4.69}$$

Dakle, parcijalne sume $A_{u,v}$ su omeđene, što je i trebalo dokazati pa željena tvrdnja slijedi. □

Nakon ovog rezultata u stanju smo obrazložiti tvrdnju izrečenu u (4.14). Neka je χ karakter modulo 4, različit od jediničnog. U prethodnom poglavlju smo vidjeli da je on definiran sa $\chi(n) = (-1)^{\varepsilon(n)}$ (u parnim brojevima vrijednost mu je očigledno nula). Odgovarajući L-red tada je jednak

$$1 - 1/3^s + 1/5^s - 1/7^s + 1/9^s - 1/11^s + \ldots, \tag{4.70}$$

i po gornjoj propoziciji on konvergira za $Re(s) > 0$ (tj. $\rho = 0$), a konvergira apsolutno za $Re(s) > 1$ (tj. $\rho^+ = 1$), što smo tada i rekli.

Posebno, iz gornje propozicije vidimo da red $L(1,\chi)$ konvergira za $\chi \neq 1$, tj. da je konačan za $\chi \neq 1$. Ključna točka u Dirichletovom dokazu sastoji se od toga da pokažemo

da je $L(1,\chi)$ različit od nula za $\chi \neq 1$. Pozabavimo se sada dokazom te tvrdnje. Za to će nam biti potrebna funkcija koja je definirana kao produkt L-funkcija po svim karakterima modulo m, koju ćemo označavati sa ζ_m.

U tu svrhu, neka je $m \in \mathbb{N}$ fiksiran. Ako p ne dijeli m, označimo sa $\bar{p}$ njegovu sliku u $G(m) = (\mathbb{Z}/m\mathbb{Z})^*$ (koja je tada različita od nule) i sa $f(p)$ red od $\bar{p}$ u $G(m)$. Po definiciji, $f(p)$ je najmanji prirodni broj $f > 1$ takav da je $\bar{p}^f = 1$, tj. takav da je $p^f \equiv 1 \ (mod\ m)$. Stavimo

$$g(p) = \phi(m)/f(p). \tag{4.71}$$

Kako je

$$|G(m)/(\bar{p})| = \frac{|G(m)|}{|(\bar{p})|} = \frac{\phi(m)}{|\bar{p}|} = \frac{\phi(m)}{f(p)}, \tag{4.72}$$

vidimo da je $g(p)$ zapravo red kvocijenta od $G(m)$ po podgrupi $(\bar{p})$ generiranoj sa $\bar{p}$.

Dokažimo sada jedan identitet koji će nam biti potreban kasnije.

Lema 4.2.9. *Ako p ne dijeli m, vrijedi sljedeći identitet:*

$$\prod_{\chi \in \widehat{G(m)}} (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}. \tag{4.73}$$

Dokaz. Neka je W skup $f(p)$.-tih korijena iz jedinice. Tada lakim računom, koristeći svojstva korijena iz jedinice, dobivamo da vrijedi sljedeća jednakost:

$$\prod_{w \in W} (1 - wT) = 1 - T^{f(p)}. \tag{4.74}$$

Nadalje, očito je da će $\bar{p}$, kao element reda $f(p)$ u $G(m)$, svaki karakter grupe $G(m)$ preslikavati u $f(p)$.-ti korijen iz jedinice, tj. da će vrijediti $\chi(\bar{p}) = w$, za neki $w \in W$ i za svaki $\chi \in \widehat{G(m)}$. Kako karaktera grupe $G(m)$ ima $\phi(m)$, a $f(p)$.-tih korijena iz jedinice $f(p)$, za svaki $w \in W$ postoji $\phi(m)/f(p) = g(p)$ karaktera χ grupe $G(m)$ takvih da je $\chi(\bar{p}) = w$. Pomoću toga i gornje jednakosti dobivamo da vrijedi

$$\prod_{\chi \in \widehat{G(m)}} (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}, \tag{4.75}$$

čime je lema dokazana. □

Definirajmo sada funkciju $\zeta_m(s)$ na sljedeći način:

$$\zeta_m(s) = \prod_{\chi} L(s,\chi), \tag{4.76}$$

gdje produkt ide po svim karakterima χ grupe $G(m)$, tj. karakterima modulo m.

Propozicija 4.2.10. *Vrijedi:*

$$\zeta_m(s) = \prod_{p\nmid m} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}}. \tag{4.77}$$

To je Dirichletov red, s pozitivnim koeficijentima, koji konvergira u poluravnini $Re(s) > 1$.

Dokaz. Pomoću propozicije 4.2.8 imamo

$$\zeta_m(s) = \prod_{\chi} L(s,\chi) = \prod_{\chi}\prod_{p\in\mathbb{P}} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{\chi}\prod_{p\nmid m} \frac{1}{1 - \frac{\chi(p)}{p^s}}, \tag{4.78}$$

pri čemu zadnja jednakost vrijedi jer je za p koji dijele m $\chi(p) = 0$, tj. odgovarajući član u produktu je jednak 1.

Sada na dobiveno primijenimo prethodnu lemu, za $T = p^{-s}$, pa slijedi:

$$\zeta_m(s) = \prod_{p\nmid m} \frac{1}{\left(1 - \frac{1}{p^{f(p)s}}\right)^{g(p)}}, \tag{4.79}$$

čime smo dobili željeni prikaz od $\zeta_m(s)$ pomoću produkta.

Iz tog prikaza odmah se vidi da je to Dirichletov red s pozitivnim koeficijentima. Također, iz propozicije 4.2.8 je jasno da on konvergira za $Re(s) > 1$; ovime je dokaz gotov. □

Za kraj ovog potpoglavlja ćemo dokazati spominjanu ključnu tvrdnju u dokazu Dirichletovog teorema, za što će nam trebati i gore uvedena funkcija ζ_m.

Teorem 4.2.11. (*a*) ζ_m *ima jednostavni pol u* $s = 1$.
(*b*) $L(1,\chi) \neq 0$, *za sve* $\chi \neq 1$.

Dokaz. Ako tvrdnja (*b*) vrijedi, iz činjenice da $L(s,1)$ ima jednostavni pol u $s = 1$ (propozicija 4.2.7) i iz definicije funkcije ζ_m vidimo da tada i ζ_m ima jednostavni pol u $s = 1$, tj. vrijedi (*a*). Dakle, (*b*) $\Rightarrow$ (*a*). Preostalo nam je da dokažemo tvrdnju (*b*), što ćemo sada i

učiniti.

Pretpostavimo suprotno, tj. da $\exists \chi \neq 1$ takav da je $L(1,\chi) = 0$. Tada je funkcija ζ_m holomorfna u $s = 1$ (jer je tada $\zeta_m(1) = 0$), pa je onda ona holomorfna, a time i analitička, i za sve s takve da je $Re(s) > 0$, što slijedi iz propozicija 4.2.7 i 4.2.8. U propoziciji4.2.10 smo vidjeli da je ζ_m Dirichletov red s pozitivnim koeficijentima, pa tada po propoziciji 4.1.13 taj red i konvergira za sve s u domeni $Re(s) > 0$. No, to ne vrijedi, što ćemo i pokazati pronalaženjem reda koji je ograničen s našim redom, a divergira za neki s takav da je $Re(s) > 0$. Tada će slijediti da i naš red divergira za taj s, što je u kontradikciji s time da on konvergira za sve s takve da je $Re(s) > 0$. Prema tome, i početna pretpostavka je bila kriva, tj. $L(1,\chi) \neq 0$ za sve $\chi \neq 1$, što je upravo tvrdnja (b).

Pronađimo sada takav red. Faktor od ζ_m koji odgovara prostom broju p jednak je

$$\frac{1}{(1 - p^{-f(p)s})^{g(p)}} = (1 + p^{-f(p)s} + p^{-2f(p)s} + \ldots)^{g(p)}, \tag{4.80}$$

jer se radi o geometrijskom redu. On dominira red

$$1 + p^{-\phi(m)s} + p^{-2\phi(m)s} + \ldots \tag{4.81}$$

jer je $\phi(m) \geq f(p)$ po definiciji od $f(p)$, pa je zbog toga $-f(p)s \geq -\phi(m)s$ i $g(p) \geq 1$.

Iz toga odmah slijedi da ζ_m ima sve koeficijente veće od koeficijenata reda

$$\sum_{(n,m)=1} n^{-\phi(m)s}. \tag{4.82}$$

No, ako uzmemo $s = \dfrac{1}{\phi(m)}$ dobivamo red

$$\sum_{(n,m)=1} n^{-1}, \tag{4.83}$$

koji je divergentan, tj. red (4.82) divergira za $s = \dfrac{1}{\phi(m)} > 0$. Dakle, pronašli smo red koji je ograničen s našim redom i divergira za neki s takav da je $Re(s) > 0$, što smo i trebali uraditi, čime je dokaz gotov. □

4.3 Gustoća i Dirichletov teorem

U ovom završnom potpoglavlju konačno ćemo pomoću rezultata dobivenih do sada dokazati glavni cilj ovoga rada, Dirichletov teorem o prostim brojevima u aritmetičkim

nizovima. Prvo ćemo dati definiciju gustoće nekog podskupa skupa prostih brojeva te pomoću nje reformulirati iskaz Dirichletovog teorema, tj. izreći njegovu jaču verziju. Zatim ćemo dokazati neke pomoćne tvrdnje pomoću kojih ćemo onda dokazati naš teorem, u jačoj verziji, čiji će korolar biti slabija verzija, teorem 4.0.2. Na kraju ćemo navesti neke zanimljive posljedice i primjene tog teorema, kao i spomenuti "prirodnu gustoću" te je dovesti u vezu s našom, "analitičkom gustoćom".

Definirajmo sada gustoću nekog podskupa skupa prostih brojeva, $\mathbb{P}$. U korolaru 4.2.6 vidjeli smo da, ako $s \to 1$ (pri čemu je ovdje radi jednostavnosti s realan i veći od 1), onda vrijedi

$$\sum_{p\in\mathbb{P}} \frac{1}{p^s} \sim ln\ \frac{1}{s-1}. \tag{4.84}$$

Neka je A podskup od $\mathbb{P}$. Kažemo da A ima gustoću k, gdje je k realan broj, ako

$$\left(\sum_{p\in A} \frac{1}{p^s}\right) / \left(ln\ \frac{1}{s-1}\right) \to k \tag{4.85}$$

kada $s \to 1$ s desne strane (tj. za one s koji zadovoljavaju $s > 1$). Ta definicija je intuitivno jasna uzevši u obzir (4.84).

Iz definicije je jasno da ako skup ima gustoću, onda mora biti $0 \leq k \leq 1$, kao i da skup $\mathbb{P}$ ima gustoću 1.

Dirichletov teorem 4.0.2 sada se može reformulirati na sljedeći način:

Teorem 4.3.1. *Neka je $m \in \mathbb{N}$ i neka je a takav da je $(a, m) = 1$. Neka je $\mathbb{P}_a$ skup prostih brojeva takvih da vrijedi $p \equiv a\ (mod\ m)$. Tada skup $\mathbb{P}_a$ ima gustoću $1/\phi(m)$.*

Drugim riječima, ovaj teorem nam kaže da su prosti brojevi "jednako distribuirani" između različitih klasa modulo m, koje sadrže a-ove relativno proste sa m, jer je takvih klasa $\phi(m)$, a svaki skup $\mathbb{P}_a$ ima gustoću $1/\phi(m)$.

Ovaj teorem je jača verzija teorema 4.0.2, koji iz njega slijedi kao korolar:

Korolar 4.3.2. *Skup $\mathbb{P}_a$ je beskonačan, tj. ako su a i m relativno prosti prirodni brojevi, onda postoji beskonačno mnogo prostih brojeva takvih da vrijedi $p \equiv a\ (mod\ m)$.*

Dokaz. Doista, ako bi $\mathbb{P}_a$ bio konačan, tada bi $\sum_{p\in\mathbb{P}_a} \frac{1}{p^s}$ imao konačan broj članova, odnosno to bi bila konačna suma, pa bi bilo $k = 0$, tj. $\mathbb{P}_a$ bi imao gustoću 0. No, iz teorema 4.3.1

znamo da taj skup ima gustoću $\frac{1}{\phi(m)} > 0$, pa smo došli do kontradikcije. Dakle, skup $\mathbb{P}_a$ je beskonačan. □

Sada ćemo dokazati nekoliko lema koje će nam trebati za dokaz teorema 4.3.1.

Neka je χ karakter grupe $G(m)$. Definirajmo funkciju f_χ na sljedeći način:

$$f_\chi(s) = \sum_{p \nmid m} \chi(p)/p^s, \tag{4.86}$$

i iz prethodnih razmatranja vidimo da taj red konvergira za $s > 1$.

Lema 4.3.3. *Ako je $\chi = 1$, tada je $f_\chi \sim ln\ \frac{1}{s-1}$, za $s \to 1$.*

Dokaz. Iz definicije je vidljivo da se red f_1 razlikuje od reda $\sum_{p\in\mathbb{P}} \frac{1}{p^s}$ samo za konačan broj članova (jer prostih brojeva p koji dijele m ima konačno mnogo), a kako, kada $s \to 1$, vrijedi

$$\sum_{p\in\mathbb{P}} \frac{1}{p^s} \sim ln\ \frac{1}{s-1}, \tag{4.87}$$

onda je i $f_1 \sim ln\ \frac{1}{s-1}$, za $s \to 1$, što smo i trebali dokazati. □

Lema 4.3.4. *Ako je $\chi \neq 1$, f_χ ostaje omeđena kada $s \to 1$.*

Dokaz. Koristit ćemo prirodni logaritam funkcije $L(s,\chi)$. Sada analogno kao u dokazu korolara 4.2.6 dobivamo

$$ln\ L(s,\chi) = ln \prod_{p\in\mathbb{P}} \frac{1}{1-\frac{\chi(p)}{p^s}} = \sum_{p\in\mathbb{P}} ln\ \frac{1}{1-\frac{\chi(p)}{p^s}} = \sum_{p\in\mathbb{P},k\geq 1} \frac{\chi(p)^k}{k\cdot p^{ks}}, \tag{4.88}$$

pri čemu je $Re(s) > 1$, pa je $\left|\frac{\chi(p)}{p^s}\right| < 1$. Ovaj red je očito konvergentan.

Rastavimo sada $ln\ L(s,\chi)$ u dva dijela:

$$ln\ L(s,\chi) = f_\chi(s) + F_\chi(s). \tag{4.89}$$

Prvi dio odgovara članu sume za $k = 1$ (jer je za p koji dijele m $\chi(p) = 0$), pa je

$$F_\chi(s) = \sum_{p\in\mathbb{P},k\geq 2} \frac{\chi(p)^k}{k \cdot p^{ks}}. \tag{4.90}$$

Iz teorema 4.2.11, dio (b), imamo da $ln\ L(s,\chi)$ ostaje omeđen kada $s \to 1$, jer $L(1,\chi)$ nije jednako nuli za $\chi \neq 1$. Također, iz korolara 4.2.6 i činjenice da je $|\chi(p)| = 1$, za svaki p koji ne dijeli m (jer je $\chi(p)$ tada $\phi(m)$.-ti korijen iz jedinice), a 0 inače, imamo da $F_\chi(s)$ ostaje omeđena kada $s \to 1$. Iz toga i (4.89) tada slijedi da, ako je $\chi \neq 1$, i $f_\chi(s)$ ostaje omeđena kada $s \to 1$, čime je lema dokazana. □

Ovdje smo iskoristili ključnu stvar u Dirichletovom dokazu, činjenicu da je $L(1,\chi) \neq 0$ za sve $\chi \neq 1$.

Neka je sada

$$g_a(s) = \sum_{p\in\mathbb{P}_a} 1/p^s. \tag{4.91}$$

Kako bismo odredili gustoću skupa $\mathbb{P}_a$, trebamo ispitati ponašanje ove funkcije za $s \to 1$. Sljedeći identitet će nam pomoći u tome:

Lema 4.3.5. *Vrijedi:*

$$g_a(s) = \frac{1}{\phi(m)} \sum_\chi \chi(a)^{-1} f_\chi(s), \tag{4.92}$$

pri čemu suma ide po svim karakterima χ grupe $G(m)$.

Dokaz. Iz (4.86) imamo:

$$\sum_\chi \chi(a)^{-1} f_\chi(s) = \sum_\chi \chi(a)^{-1} \left(\sum_{p\nmid m} \chi(p)/p^s \right) = \sum_{p\nmid m} \left(\sum_\chi \chi(a)^{-1}\chi(p) \right) /p^s. \tag{4.93}$$

No, χ je karakter, pa vrijedi $\chi(a)^{-1}\chi(p) = \chi(a^{-1}p)$. Sada primjenom korolara 3.1.7, jer je χ karakter grupe $G(m)$, $a^{-1}p \in G(m)$ i $|G(m)| = \phi(m)$, dobivamo

$$\sum_\chi \chi(a^{-1}p) = \begin{cases} \phi(m), & \text{ako } a^{-1}p \equiv 1\ (mod\ m) \\ 0, & \text{inače} \end{cases} \tag{4.94}$$

$$, \tag{4.95}$$

tj.

$$\sum_{\chi} \chi(a^{-1}p) = \begin{cases} \phi(m), & \text{ako } p \equiv a \ (mod\ m) \\ 0, & \text{inače} \end{cases} \tag{4.96}$$

$$. \tag{4.97}$$

Iz svega toga slijedi

$$\sum_{\chi} \chi(a)^{-1} f_{\chi}(s) = \sum_{p \nmid m} \left(\sum_{\chi} \chi(a^{-1}p) \right) / p^s = \sum_{p \in \mathbb{P}_a} \phi(m)/p^s, \tag{4.98}$$

odnosno

$$\frac{1}{\phi(m)} \sum_{\chi} \chi(a)^{-1} f_{\chi}(s) = \sum_{p \in \mathbb{P}_a} 1/p^s, \tag{4.99}$$

iz čega uz uporabu (4.91) imamo:

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi} \chi(a)^{-1} f_{\chi}(s). \tag{4.100}$$

Ovime je dokaz gotov. □

Sada konačno možemo dokazati naš teorem 4.3.1. Kada $s \to 1$, iz leme 4.3.3 slijedi da je $f_{\chi}(s) \sim \ln \frac{1}{s-1}$ za $\chi = 1$, a iz leme 4.3.4 da $f_{\chi}(s)$ ostaje omeđeno za sve $\chi \neq 1$. Koristeći lemu 4.3.5 iz toga vidimo da je $g_a(s) = \sum\limits_{p \in \mathbb{P}_a} 1/p^s \sim \frac{1}{\phi(m)} \ln \frac{1}{s-1}$, kada $s \to 1$, odnosno

$$\left(\sum_{p \in \mathbb{P}_a} 1/p^s \right) / \left(ln\, \frac{1}{s-1} \right) \to \frac{1}{\phi(m)}, \tag{4.101}$$

kada $s \to 1$. Po definiciji gustoće iz ovoga slijedi da skup $\mathbb{P}_a$ ima gustoću $\frac{1}{\phi(m)}$, što je i trebalo dokazati.

Ovime je dokaz Dirichletovog teorema o prostim brojevima u aritmetičkim nizovima u potpunosti dovršen.

Sada navodimo neke posljedice i primjene ovog teorema, kao i analogne rezultate za druge tipove jednadžbi.

Propozicija 4.3.6. *Neka je a cijeli broj koji nije potpuni kvadrat. Tada skup prostih brojeva p takvih da je $\left(\frac{a}{p}\right) = 1$ ima gustoću $\frac{1}{2}$.*

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da je a kvadratno slobodan, jer ako je $a = k^2 b$, onda imamo $\left(\frac{a}{p}\right) = \left(\frac{k^2}{p}\right)\left(\frac{b}{p}\right) = 1 \cdot \left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)$ pa sve kvadrate možemo "maknuti" iz a bez da promijenimo vrijednost odgovarajućeg Legendreovog simbola. Neka je sada $m = 4|a|$ i χ_a jedinstveni karakter modulo m definiran u propoziciji 3.2.1, tj. takav da je $\chi_a(p) = \left(\frac{a}{p}\right)$, za sve proste brojeve p koji ne dijele m, te neka je $H \subset G(m)$ jezgra od χ_a u $G(m)$. Ako je p prost broj koji ne dijeli m, tada sa $\bar{p}$ označimo njegovu sliku u $G(m)$. Jasno je da onda vrijedi:

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \bar{p} \in H. \tag{4.102}$$

Po teoremu 4.3.1 imamo da skup prostih brojeva p koji zadovoljavaju uvjet $\bar{p} \in H$ ima za gustoću inverz od indeksa od H u $G(m)$. Taj indeks je, kao što smo vidjeli u dijelu teksta o Legendreovom simbolu, jednak 2, pa je odgovarajuća gustoća $\frac{1}{2}$. Dakle, po tome i (4.102) skup prostih brojeva p takvih da je $\left(\frac{a}{p}\right) = 1$ ima gustoću $\frac{1}{2}$, čime je dokaz gotov. □

Ovaj rezultat ima zanimljiv korolar:

Korolar 4.3.7. *Neka je a cijeli broj. Ako jednadžba $X^2 - a = 0$ ima rješenje modulo p za skoro sve $p \in \mathbb{P}$, onda ona ima rješenje u $\mathbb{Z}$.*

Dokaz. Ako jednadžba $X^2 - a = 0$ ima rješenje modulo p, to znači da je $\left(\frac{a}{p}\right) = 1$. Naša jednadžba ima rješenje modulo p za skoro sve $p \in \mathbb{P}$, tj. za sve osim njih konačno mnogo. Prema tome, gustoća skupa prostih brojeva p takvih da je $\left(\frac{a}{p}\right) = 1$ očigledno je jednaka 1, tj. različita od $\frac{1}{2}$. Iz prethodne propozicije sada slijedi da je a potpuni kvadrat u $\mathbb{Z}$, odnosno da jednadžba $X^2 - a = 0$ ima rješenje u $\mathbb{Z}$, i time je korolar dokazan. □

Dirichletov teorem ima svoje analoge za druge tipove jednadžbi. Pogledajmo neke primjere takvih rezultata.

Neka je $f(x) = a_n X^n + \ldots + a_0$ polinom stupnja n s cjelobrojnim koeficijentima, koji je ireducibilan nad $\mathbb{Q}$ (tj. koji se ne može rastaviti u produkt dva nekonstantna polinoma s koeficijentima u $\mathbb{Q}$). Neka je K polje generirano s korijenima od f (u algebarski zatvorenom

proširenju od $\mathbb{Q}$) i neka je $N = [K : \mathbb{Q}]$. Tada je $N \geq n$, jer f nema niti jedan korijen u $\mathbb{Q}$ s obzirom da je ireducibilan nad $\mathbb{Q}$. Označimo sa $\mathbb{P}_f$ skup prostih brojeva p takvih da se f "dekomponira potpuno modulo p", tj. takvih da svi korijeni od f $(mod\ p)$ pripadaju skupu $\mathbb{F}_p$. Tada se može dokazati da $\mathbb{P}_f$ ima gustoću $\frac{1}{N}$ (i to metodom analognom onoj koja se upotrebljava u dokazu Dirichletovog teorema; koristi se činjenica da zeta funkcija polja K ima jednostavni pol u $s = 1$). Također, ako sa $\mathbb{P}'_f$ označimo skup prostih brojeva p takvih da redukcija od f $(mod\ p)$ ima barem jedan korijen u $\mathbb{F}_p$, može se dokazati da taj skup ima za gustoću broj oblika $\frac{q}{N}$, pri čemu je $1 \leq q < N$. Iz definicije tih skupova jasno je da skup $\mathbb{P}'_f$ ima gustoću veću ili jednaku od gustoće skupa $\mathbb{P}_f$, što rezultati i pokazuju.

Općenitije, neka je $\{f_\alpha(x_1, \ldots, x_n)\}$ familija polinoma u n varijabli s cjelobrojnim koeficijentima i neka je Q skup svih prostih brojeva p takvih da redukcije od f_α $(mod\ p)$, $\forall\alpha$, imaju zajedničku nultočku u $(\mathbb{F}_p)^n$. Može se dokazati da skup Q ima gustoću; štoviše, ta gustoća je racionalni broj i jednaka je nuli samo ako je Q konačan.

Za kraj ovog rada definirat ćemo prirodnu gustoću i povezati je s do sada promatranom, analitičkom gustoćom.

U ovom potpoglavlju korištena analitička, ili Dirichletova gustoća, unatoč svojoj kompleksnosti, vrlo je prikladna za uporabu. Postoji i druga gustoća koju možemo promatrati, i koju nazivamo prirodna gustoća, čija je definicija intuitivnija: za podskup A od $\mathbb{P}$ kažemo da ima prirodnu gustoću k ako omjer broja elemenata od A koji su manji ili jednaki n i broja elemenata od $\mathbb{P}$ koji su manji ili jednaki n teži ka k kada $n \to \infty$.

Može se dokazati da ako skup A ima prirodnu gustoću k, tada A ima i analitičku gustoću i ona je također jednaka k. No, obrat ne vrijedi, tj. postoje skupovi koji imaju analitičku, ali nemaju prirodnu gustoću. Navedimo jedan primjer takvog skupa. Neka je $\mathbb{P}^1$ skup prostih brojeva čija je prva znamenka u dekadskom zapisu jednaka 1. Skup $\mathbb{P}^1$ nema prirodnu gustoću, dok njegova analitička gustoća postoji i jednaka je $log_{10}2$.

No, skupovi prostih brojeva koje smo proučavali u ovom potpoglavlju se u tom smislu ponašaju lijepo, tj. imaju i analitičku i prirodnu gustoću, koje su po gore rečenom jednake. Tako skup prostih brojeva p takvih da je $p \equiv a\ (mod\ m)$ ima prirodnu gustoću (jednaku $1/\phi(m)$, ako je $(a, m) = 1$); isto vrijedi i za skupove $\mathbb{P}_f$, $\mathbb{P}'_f$ i Q, promatrane iznad.

Bibliografija

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

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

[3] *Wikipedia, the free encyclopedia*, http://en.wikipedia.org

Sažetak

U ovom radu se bavimo određenim problemima teorije brojeva, s posebnim naglaskom na Dirichletov teorem o prostim brojevima u aritmetičkim nizovima, pri čemu se prvo služimo algebarskim, a kasnije analitičkim metodama.

U prvom poglavlju opisujemo konačna polja, definiramo Legendreov simbol i dokazujemo zakon kvadratnog reciprociteta.

U drugom poglavlju bavimo se p-adskim poljima. Pobliže proučavamo prsten p-adskih cijelih brojeva, $\mathbb{Z}_p$, i polje njegovih razlomaka, $\mathbb{Q}_p$, te dobivamo neke važne rezultate o rješenjima p-adskih jednadžbi, čiji su koeficijenti p-adski cijeli brojevi.

U trećem poglavlju objekti našeg promatranja su karakteri konačnih Abelovih grupa; prvo općeniti, a zatim se koncentriramo na karaktere grupe $G(m)$, i dokazujemo neka njihova svojstva.

U četvrtom, posljednjem, poglavlju, dokazujemo glavni cilj ovoga rada, Dirichletov teorem o prostim brojevima u aritmetičkim nizovima, točnije, njegovu jaču verziju, i to činimo metodama analitičke teorije brojeva. Proučavamo zeta funkciju i L-funkcije, te definiramo gustoću nekog podskupa skupa prostih brojeva, pa koristeći dobivene rezultate dajemo dokaz spomenutog teorema.

Summary

In this thesis we investigate some number theory problems, with special emphasis on Dirichlet's theorem on arithmetic progressions. We first use algebraic, and later analytic methods to solve our problems.

In the first chapter we describe finite fields, define Legendre symbol and prove quadratic reciprocity law.

In the second chapter we deal with p-adic fields. We study the ring of p-adic integers, $\mathbb{Z}_p$, and field of its fractions, $\mathbb{Q}_p$, and obtain some important results about the solutions of p-adic equations, whose coefficients are p-adic integers.

In the third chapter, the objects of our observation are characters of finite abelian groups. We first consider characters in general, and then we concentrate on the characters of $G(m)$, proving some of their properties.

In the fourth, final, chapter, we prove the main goal of this thesis, Dirichlet's theorem on arithmetic progressions. More specifically, we give a proof of its stronger version, using methods of analytic number theory. We study the zeta function and the L-functions, and define the density of some subset of the set of prime numbers, and then, using obtained results, we prove the theorem mentioned above.

Životopis

Rođena sam u Zagrebu 26.10.1987. godine. Od 1994. do 2002. pohađala sam Osnovnu školu Gustava Krkleca u Zagrebu, te sam nakon toga krenula u zagrebačku V. gimnaziju, koju sam završila 2006. godine. Iste godine sam upisala preddiplomski studij Matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu, koji sam završila 2009. godine, te sam odmah nakon toga upisala diplomski studij Teorijske matematike na istom fakultetu.