# Lokalna rješivost kvadratnih zavrtaja krivulja genusa 1

**Novak, Lukas**

**SVEUČILIŠTE U ZAGREBU**

**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**

**MATEMATIČKI ODSJEK**

Lukas Novak

# LOKALNA RJEŠIVOST KVADRATNIH ZAVRTAJA KRIVULJA GENUSA 1

Diplomski rad

Zagreb, 9. 2022.

**SVEUČILIŠTE U ZAGREBU**

**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**

**MATEMATIČKI ODSJEK**

Lukas Novak

# LOKALNA RJEŠIVOST KVADRATNIH ZAVRTAJA KRIVULJA GENUSA 1

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Matija Kazalicki

Zagreb, 9. 2022.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

*Zahvaljujem se roditeljima i prijateljima koji su mi pružali neizmjerno veliku podršku tijekom mog odrastanja i školovanja. Posebno se zahvaljujem i svim profesorima matematike kroz osnovnu i srednju školu. Oni su me upoznali s predivnim svijetom Matematike i također mi pružili veliku potporu da nastavim kročiti tim putem. Bez njih se možda ne bih odlučio dalje baviti i razvijati interes za Matematiku. Zahvaljujem se i mentoru izv. prof. dr. sc. Matiji Kazalickom na brojnim korisnim savjetima i svoj podršci koju mi je pružio tijekom pisanja ovog rada.*

# Sadržaj

**Sadržaj** **iv**

**Uvod** **1**

**1 Problem** **3**
1.1 Lokalna rješivost . . . . . 3
1.2 Brojaća funkcija za $q$-ove i pripadni Dirichletov red . . . . . 9

**2 Svojstva funkcije $f(s)$** **13**
2.1 Apsolutna konvergencija na $\mathrm{Re}(s) \geq c > 1$ . . . . . 13
2.2 Uniformna konvergencija na $\mathrm{Re}(s) \geq c > 1$ . . . . . 13
2.3 Analitičko proširenje od $f(s)$ na $\mathrm{Re}(s) > \frac{1}{2}$ . . . . . 14
2.4 Reziduum od $f(s)$ u $s = 1$ . . . . . 15
2.5 Gornja ograda za $|f(s)|$ na $\mathrm{Re}(s) = \frac{1}{2} + \delta$ . . . . . 16

**3 Perronova formula i ocjena greške** **19**

**4 Asimptotika brojaće funkcije $A(x)$** **23**
4.1 Kontura ključanice . . . . . 23
4.2 Ocjene integrala . . . . . 24
4.3 Asimptotika . . . . . 29

**Bibliografija** **31**

# Uvod

Cilj ovog diplomskog rada je odrediti asimptotiku broja kvadratno slobodnih brojeva $q \in \mathbb{Z}$ za koje krivulja $qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ ima rješenje u $\mathbb{Q}_p$ za svaki prost broj $p$, tj. ima rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki prosti broj $p$ i svaki $n \in \mathbb{N}$. Za određivanje tražene asimptotike ćemo koristiti metode iz analitičke teorije brojeva. Ovaj problem je motiviran teorijom Diofantovih $m$-torki te koristi slične metode kao u klasičnom problemu određivanja asimptotike brojeva koji se mogu prikazati kao suma dva kvadrata. Radi pojednostavljenja izvoda tražene asimptotike u radu je pretpostavljeno da vrijedi *generalizirana Riemannova hipoteza*. Sam rad je podjeljen u četiri poglavlja.

U prvom poglavlju proučavamo koje to nužne i dovoljne uvjete mora zadovoljavati $q$ tako da krivulja $qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ bude *svugdje lokalno rješiva*, odnosno da ima rješenje u $\mathbb{Q}_p$ za svaki prost broj $p$. Nakon određivanja nužnih i dovoljnih uvjeta za $q$-ove prelazimo na definiciju određenog niza brojeva. Pomoću tog niza brojeva zatim definiramo brojeću funkciju za $q$-ove i pripadni Dirichletov red pridružen tom niz. Na kraju poglavlja detaljnije promatramo prije definiran Dirichletov red te ga zapisujemo pomoću *Riemannove zeta funkcije* i određene *Dirichletove* L-funkcije koristeći nužne i dovoljne uvjete za $q$-ove.

Drugo poglavlje se bavi proučavanjem raznih svojstava našeg Dirichletovog reda : apsolutna i uniformna konvergencija na području $\mathrm{Re}(s) \geq c > 1$, mogućnost analitičkog proširenja na $\mathrm{Re}(s) > \frac{1}{2}$, reziduumom u $s = 1$ te ocjenom na $\mathrm{Re}(s) = \frac{1}{2} + \delta$.

Treće poglavlje se bavi ocjenom greške koja proizlazi iz *Perronove formule*. Cilj tog poglavlja je pojednostaviti dobiveni izraz za grešku kada primjenimo *Perronovu formulu* na prethodno definiran Dirichletov red. Taj pojednostavljeni izraz za grešku će nam kasnije olakšati analizu traženog asimptotskog ponašanja brojaće funkcije za $q$-ove.

U zadnjem poglavlju primjenjujemo *Perronovu formulu* na naš Dirichletov red i uvodimo *konturu ključanice* (*key-hole contour*). Ta kontura nam omogućuje da integral koji dobijemo nakon primjene *Perronove formule* svedemo na integrale po drugim krivuljama. U nastavku poglavlja ocijenjujemo posebno svaki od tih integrala koristeći razna svojstva našeg Dirichletovog reda iz Poglavlja 2. Nakon ocjene tih integrala, konačno dolazimo do tražene asimptotike brojaće funkcije.

# Poglavlje 1

# Problem

**Problem:** Odredite asimptotiku broja kvadratno slobodnih brojeva $q \in \mathbb{Z}$ za koje krivulja

$$qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$$

ima rješenje u $\mathbb{Q}_p$ za svaki prosti broj $p$.

Metoda za rješavanje navedenog problema se bazira na korištenju alata iz analitičke teorije brojeva, konkretno na primjeni **Perronove formule** i velikim djelom prati [1]. Rješenje problema ćemo podjeliti u nekoliko koraka.

Prvi korak će biti određivanje nužnih i dovoljnih uvjeta na $q$-ove za koje će krivulja $qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ imati rješenje u $\mathbb{Q}_p$ za svaki prosti broj $p$, odnosno za koje će imati rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki prosti broj $p$ i za svaki prirodan broj $n$.

Drugi korak se sastoji od definicije određenog niza brojeva $(a_n)_{n\in\mathbb{N}}$ za koje će funkcija $A(x) = \sum_{n\leq x} a_n$ biti brojaća funkcija za $q$-ove koji zadovoljavaju uvjete problema i promatranja pripadnog Dirichletov red $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ pridruženom nizu $(a_n)_{n\in\mathbb{N}}$.

U zadnjem koraku ćemo primjeniti *Perronovu formulu* na gornji Dirichletov red i pomoću *konture ključanice* integral koji dobijemo iz *Perronove formule* svesti na integrale po drugim krivuljama. Nakon toga ćemo svaki od tih integrala posebno ocjeniti i time u konačnici dobiti traženu asimptotiku.

## 1.1 Lokalna rješivost

Za $q \in \mathbb{Z}$ promatramo krivulju

$$E_q : \quad qy^2 = (x^2 - x - 3)(x^2 + 2x - 12) \tag{1.1}$$

Cilj nam je odrediti nužne i dovoljne uvjete za $q$ tako da krivulja $E_q$ bude *svugdje lokalno rješiva*, odnosno da ima rješenje u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki prosti broj $p$ i za svaki prirodan broj $n$. Pri određivanju tih uvjeta ćemo koristiti sljedeće teoreme.

**Teorem 1.1.1.** ***(Henselova lema)*** *Neka je $f(x)$ polinom s cijelobrojnim koeficijentima i neka je $a \in \mathbb{Z}$. Ako je $f(a) \equiv 0 \pmod{p^j}$ za neki $j \in \mathbb{N}$ i $f'(a) \not\equiv 0 \pmod{p}$, tada postoji jedinstveni $t \in \{0, 1, 2, \ldots, p-1\}$ takav da je $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.*

*Henselova lema* se dokazuje sasvim analogno kao Teorem 1.1.2 (*Henselova lema za polinome u dvije varijable*).

**Teorem 1.1.2.** ***(Henselova lema za polinome u dvije varijable)*** *Neka je $f(x, y) \in \mathbb{Z}[x, y]$ polinom s cijelobrojnim koeficijentima u dvije varijable, $p$ prost broj, $j \in \mathbb{N}$ te $a, b \in \mathbb{Z}$. Ako je $f(a, b) \equiv 0 \pmod{p^j}$ i $\Big(\partial_x f(a, b) \not\equiv 0 \pmod{p}$ ili $\partial_y f(a, b) \not\equiv 0 \pmod{p}\Big)$, tada postoje $t, s \in \{0, 1, 2, \ldots, p-1\}$ takvi da je $f(a + tp^j, b + sp^j) \equiv 0 \pmod{p^{j+1}}$.*

*Dokaz.* Označimo sa $n = \deg f$ stupanj polinoma $f$. Razvojem polinoma $f$ u Taylorov red oko točke $(a, b)$ dobijemo da za sve $x, y \in \mathbb{Z}$ vrijedi

$$\begin{aligned} f(x, y) &= \sum_{|\alpha| \le n} \frac{\partial^\alpha f(a, b)}{\alpha!} (x - a, y - b)^\alpha \\ &= f(a, b) + \partial_x f(a, b)(x - a) + \partial_y f(a, b)(y - b) + \sum_{2 \le |\alpha| \le n} \frac{\partial^\alpha f(a, b)}{\alpha!} (x - a, y - b)^\alpha \end{aligned}$$

gdje je $\alpha = (\alpha_1, \alpha_2) \in \mathbb{N}_0^2$ multiindeks, $|\alpha| = \alpha_1 + \alpha_2$, $\partial^\alpha = \partial_x^{\alpha_1} \partial_y^{\alpha_2}$, $\alpha! = \alpha_1! \cdot \alpha_2!$ i $(x, y)^\alpha = x^\alpha y^{\alpha_2}$.

Uvrštavanjem $x = a + tp^j$ i $y = b + sp^j$ za $t, s \in \mathbb{Z}$ dobijemo

$$\begin{aligned} f(a + tp^j, b + sp^j) &= f(a, b) + \partial_x f(a, b) tp^j + \partial_y f(a, b) sp^j + \sum_{2 \le |\alpha| \le n} \frac{\partial^\alpha f(a, b)}{\alpha!} (tp^j, sp^j)^\alpha \\ &= f(a, b) + \partial_x f(a, b) tp^j + \partial_y f(a, b) sp^j + \sum_{2 \le |\alpha| \le n} \frac{\partial^\alpha f(a, b)}{\alpha!} (t, s)^\alpha p^{j|\alpha|} \end{aligned}$$

Kako je u gornjoj sumi $|\alpha| \ge 2$ imamo da je $j|\alpha| \ge 2j \ge j + 1$ pa iz gornje jednakosti slijedi

$$f(a + tp^j, b + sp^j) \equiv f(a, b) + \partial_x f(a, b) tp^j + \partial_y f(a, b) sp^j \pmod{p^{j+1}} \tag{1.2}$$

Budući da je $f(a, b) \equiv 0 \pmod{p^j}$ imamo da je $f(a, b) = cp^j$ za neki $c \in \mathbb{Z}$. Dakle, da bi vrijedilo $f(a + tp^j, b + sp^j) \equiv 0 \pmod{p^{j+1}}$ iz (1.2) vidimo da nam je dovoljno naći $t$ i $s$ takve da vrijedi

$$c + \partial_x f(a, b) t + \partial_y f(a, b) s \equiv 0 \pmod{p}$$

Iz pretpostavke teorema imamo da je $\partial_x f(a,b) \not\equiv 0 \pmod{p}$ ili $\partial_y f(a,b) \not\equiv 0 \pmod{p}$. Zbog simetrije u gornjoj kongruenciji bez smanjenja općenitosti možemo pretpostaviti da je $\partial_x f(a,b) \not\equiv 0 \pmod{p}$. Stavljenjem $s = 0$ se gornja kongruencija svodi na rješavanje $\partial_x f(a,b)t \equiv -c \pmod{p}$, a pošto je $\partial_x f(a,b) \not\equiv 0 \pmod{p}$ onda znamo da postoji jedinstveni $t \in \{0,1,2,\ldots,p-1\}$ koji zadovoljava tu kongruenciju. Time imamo da su tako odabrani $t, s \in \{0,1,2,\ldots,p-1\}$ i vrijedi $f(a+tp^j, b+sp^j) \equiv 0 \pmod{p^{j+1}}$. □

Obje verzije *Henselove leme* će nam biti iznimno koristan alat pomoću kojih ćemo rješenje od $E_q$ u $\mathbb{Z}/p\mathbb{Z}$ podići do rješenja u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki prirodan broj $n$.

**Teorem 1.1.3.** ***(Hasse)*** *Neka je $\left|E(\mathbb{F}_q)\right|$ broj točaka na eliptičkoj krivulji $E$ nad konačnim poljem $\mathbb{F}_q$ . Tada vrijedi*

$$q + 1 - 2\sqrt{q} \leq \left|E(\mathbb{F}_q)\right| \leq q + 1 + 2\sqrt{q}$$

Dokaz *Hasseovog teorema* se može naći u [6] (Poglavlje 5, Teorem 1.1).

Pretpostavimo da je $E_q$ svugdje lokalno rješiva za neki kvadratno slobodan $q \in \mathbb{Z}$ . Neka je $p$ prost broj takav da $p \mid q$. Pokažimo prvo da je $p \neq 2$.

U tu svrhu pretpostavimo suprotno, tj. da je $p = 2$. Kako 2 djeli $q$ onda možemo zapisati $q = 2q_1$ pri čemu je $q_1 \in \mathbb{Z}$ neki neparan kvadratno slobodan broj. Iz lokalne rješivosti od $E_q$ imamo da postoji rješenje u $\mathbb{Z}/8\mathbb{Z}$, odnosno imamo da postoje cijeli brojevi $x$ i $y$ za koje vrijedi

$$2q_1y^2 \equiv (x^2 - x - 3)(x^2 + 2x - 12) \pmod{8} \tag{1.3}$$

Odavde imamo da $2 \mid (x^2 - x - 3)(x^2 + 2x - 12)$. Kako je $x^2 - x - 3$ očito neparan onda mora biti $2 \mid (x^2 + 2x - 12)$, odnosno imamo da je $x$ paran. Zapišimo $x = 2a$ gdje je $a$ neki cijeli broj. Uvrštavanjem u (1.3) dobijemo

$$2q_1y^2 \equiv 4(4a^2 - 2a - 3)(a^2 + a - 3) \equiv 4 \pmod{8}$$

Međutim, kako je $q_1$ neparan imamo da je $q_1 \equiv \pm 1, \pm 3 \pmod{8}$. Imamo da je i $2y^2 \equiv 0, 2 \pmod{8}$. Iz toga slijedi da je $2q_1y^2 \equiv 0, \pm 2 \pmod{8}$ što je u kontradikciji s gornjom kongruencijom. Dakle, mora biti $p \neq 2$.

Iz lokalne rješivosti od $E_q$ imamo da postoji rješenje u $\mathbb{Z}/p\mathbb{Z}$, tj. postoje cijeli brojevi $x$ i $y$ za koje vrijedi

$$qy^2 \equiv (x^2 - x - 3)(x^2 + 2x - 12) \pmod{p}$$

Kako $p$ dijeli $q$ imamo da je onda $(x^2 - x - 3)(x^2 + 2x - 12) \equiv 0 \pmod{p}$. Dakle, $x^2 - x - 3 \equiv 0 \pmod{p}$ ili $x^2 + 2x - 12 \equiv 0 \pmod{p}$.

Pretpostavimo da je $x^2 - x - 3 \equiv 0 \pmod{p}$. Množenjem te kongruencije s 4 i sređivanjem dobijemo $(2x-1)^2 \equiv 13 \pmod{p}$. Dakle, $p = 13$ ili je 13 kvadratni ostatak modulo $p$, tj. $\left(\frac{13}{p}\right) = 1$. Prije smo već pokazali da je $p \neq 2$, tj. $p$ je neparan prost broj. Primjenom *Gaussovog zakona o kvadratnom reciprocitetu* imamo da je $\left(\frac{p}{13}\right) = \left(\frac{13}{p}\right) = 1$, odnosno $p$ je kvadratni ostatak modulo 13.

Pretpostavimo da je $x^2 + 2x - 12 \equiv 0 \pmod{p}$. Tada je $(x+1)^2 \equiv 13 \pmod{p}$. Iz ovog sada analogno kao i u prijašnjem slučaju dobijemo da mora biti $p = 13$ ili je $p$ kvadratni ostatak modulo 13.

Iz ovog zaključujemo : ako je $E_q$ svugdje lokalno rješiva onda za proste faktore $p$ od $q$ vrijedi da je $p = 13$ ili je $p$ kvadratni ostatak modulo 13.

Pokažimo da vrijedi i obrat, tj. ako je $q$ kvadratno slobodan broj za koji vrijedi : ako je $p$ prosti broj koji djeli $q$, tada je $p = 13$ ili je $p$ kvadratni ostatak modulo 13, onda je $E_q$ svugdje lokalno rješiva.

Neka je $q \in \mathbb{Z}$ kvadratno slobodan broj tako da za svaki prosti faktor $p$ od $q$ vrijedi da je $p = 13$ ili je $p$ kvadratni ostatak modulo 13. Uzmimo prosti broj $p$. Promotrimo sljedeće slučajeve :

1. $p \mid q$ : U ovom slučaju je $p$ prosti faktor od $q$ pa imamo da je $p = 13$ ili je $p$ kvadratni ostatak modulo 13.

   Pretpostavimo da je $p = 13$. Onda je $q = 13q_1$ pri čemu je $q_1 \in \mathbb{Z}$ kvadratno slobodan broj, svi prosti faktori od $q_1$ su kvadrati modulo 13 te $13 \nmid q_1$. Kako su svi prosti faktori od $q_1$ kvadrati modulo 13 imamo da je i sam $q_1$ kvadrat modulo 13. Nadalje, kako $13 \nmid q_1$ primjenom *Henselove leme* (1.1.1) dobijemo da je $q_1$ kvadrat modulo $13^n$ za svaki prirodan broj $n$. Zbog toga što je $q_1$ kvadrat modulo $13^n$ za svaki prirodan broj $n$ provjera lokalne rješivosti od $E_q$ za $p = 13$ se svodi na provjeru lokalne rješivosti od $13y^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ za $p = 13$. Uočimo da je $(x, y) = (-1, 1)$ globalno rješenje iz čega onda posebno slijedi da je $13y^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ lokalno rješiva za $p = 13$.

   Ako je $p \neq 13$ onda imamo da je $p$ kvadrat modulo 13, tj. $\left(\frac{p}{13}\right) = 1$. Kako 2 nije kvadrat modulo 13 imamo da je $p \neq 2$, odnosno da je $p$ neparan. Primjenom *Gaussovog zakona o kvadratnom reciprocitetu* dobijemo da je $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = 1$. Iz ovog imamo da postoji $a \in \mathbb{Z}$ za koji vrijedi $a^2 \equiv 13 \pmod{p}$ i $p \nmid a$. Označimo $f(x) = x^2 + 2x - 12$. Uvrštavanjem $x = a - 1$ imamo

   $$f(a-1) = a^2 - 13 \equiv 0 \pmod{p}$$

   Nadalje, kako $p \nmid a$ i $p \neq 2$ imamo

   $$f'(a-1) = 2a \not\equiv 0 \pmod{p}$$

Ovo nam sada omogućuje da rješenje $(x, y) = (a - 1, 0)$ u $\mathbb{Z}/p\mathbb{Z}$ *Henselovom lemom* (1.1.1) podignemo do rješenja u $\mathbb{Z}/p^n\mathbb{Z}$. Time i u ovom slučaju imamo lokalnu rješivost za $p$.

2. $p \mid 2 \cdot \operatorname{disc}\left((x^2 - x - 3)(x^2 + 2x - 12)\right)$ : Imamo da je

$$\operatorname{disc}\left((x^2 - x - 3)(x^2 + 2x - 12)\right) = 492804 = 2^2 \cdot 3^6 \cdot 13^2$$

Zbog toga lokalnu rješivost od $E_q$ provjeravamo za $p = 2$, 3 i 13. Nadalje, bez smanjenja općenitosti možemo pretpostaviti da $p \nmid q$ jer bi u suprotnome se vratili u prvi slučaj.

Pretpostavimo da je $p = 2$. Promotrimo polinom

$$p(x, y) = (x^2 - x - 3)(x^2 + 2x - 12) - qy^2 = x^4 + x^3 - 17x^2 + 6x + 36 - qy^2$$

Kako $p \nmid q$ imamo da je $q$ neparan pa je $p(1, 1) \equiv 0 \pmod 2$, tj. $(1, 1)$ je na $E_q$ nad $\mathbb{Z}/2\mathbb{Z}$. Također je $\partial_x p(1, 1) = -21 \not\equiv 0 \pmod 2$ pa primjenom *Henselove leme za polinome u dvije varijable* (1.1.2) dobijemo da rješenje $(1, 1)$ možemo podići do rješenja u $\mathbb{Z}/2^n\mathbb{Z}$ za svaki prirodan broj $n$, odnosno imamo lokalnu rješivost od $E_q$ za $p = 2$.

Pretpostavimo da je $p = 3$. Promotrimo polinom $f(x) = x^2 - x - 3$. Za $x = 0$ imamo da je $f(0) \equiv 0 \pmod 3$ i $f'(0) = -1 \not\equiv 0 \pmod 3$ pa prema *Henselovoj lemi* (1.1.1) slijedi da za svaki prirodni broj $n$ postoji $x_n \in \mathbb{Z}$ tako da vrijedi $f(x_n) \equiv 0 \pmod{3^n}$. Ovime imamo da se $(x_n, 0)$ nalazi na $E_q$ nad $\mathbb{Z}/3^n\mathbb{Z}$ za svaki prirodan broj $n$, odnosno imamo lokalnu rješivost od $E_q$ za $p = 3$.

Pretpostavimo da je $p = 13$. Iz $13 \nmid q$ slijedi da su svi prosti faktori od $q$ kvadrati modulo 13 pa je samim time i $q$ kvadratni ostatak modulo 13. Promotrimo polinom $p(x, y)$ definiran kao prije. Uvrštavanjem $x = 0$ imamo da je $p(0, y) = 36 - qy^2$. Promotrimo kongruenciju $qy^2 \equiv 36 \pmod{13}$. Kako su $q$ i 36 kvadratni ostaci modulo 13 i $13 \nmid q$ imamo da postoji rješenje gornje kongruencije i označimo ga s $b$. Uočimo da iz $qb^2 \equiv 36 \pmod{13}$ slijedi da $13 \nmid b$. Ovime sada imamo da vrijedi $p(0, b) \equiv 0 \pmod{13}$ i $\partial_y p(0, b) = 2qb \not\equiv 0 \pmod{13}$ pa primjenom *Henselove leme za polinome u dvije varijable* (1.1.2) dobijemo da rješenje $(0, b)$ možemo podići do rješenja u $\mathbb{Z}/13^n\mathbb{Z}$ za svaki prirodan broj $n$, odnosno imamo lokalnu rješivost od $E_q$ za $p = 13$.

3. $p \nmid q, 2 \cdot \operatorname{disc}\left((x^2 - x - 3)(x^2 + 2x - 12)\right)$ : Promotrimo ponovo polinom

$$p(x, y) = (x^2 - x - 3)(x^2 + 2x - 12) - qy^2$$

Iz $p \nmid q$, $2 \cdot \text{disc}\left((x^2 - x - 3)(x^2 + 2x - 12)\right)$ slijedi da $E_q$ ima *dobru redukciju* modulo $p$, tj. $\partial_x p(x, y) \not\equiv 0 \pmod{p}$ ili $\partial_y p(x, y) \not\equiv 0 \pmod{p}$ za sve $x, y \in \mathbb{Q}$ .

Uočimo da nam je zbog toga za dokaz lokalne rješivosti od $E_q$ u $p$ dovoljno naći $x$, $y \in \mathbb{Z}$ tako da vrijed $p(x, y) \equiv 0 \pmod{p}$ jer tada korištenjem dobre redukcije od $E_q$ modulo $p$ možemo primjeniti *Henselovu lemu za polinome u dvije varijable* (1.1.2) te dobijemo da rješenje $(x, y)$ možemo podići do rješenja u $\mathbb{Z}/p^n\mathbb{Z}$ za svaki prirodan broj $n$.

U tu svrhu pretpostavimo suprotno, tj. da ne postoje $x, y \in \mathbb{Z}$ takvi da vrijedi $p(x, y) \equiv 0 \pmod{p}$.

Promotrimo krivulju $E$ nad $\mathbb{Q}$ danu s

$$E: \quad y^2 = (x^2 - x - 3)(x^2 + 2x - 12)$$

Krivulja $E$ je također genusa 1 jer polinom na desnoj strani nema višestrukih nultočki. Kako $p \nmid 2 \cdot \text{disc}\left((x^2 - x - 3)(x^2 + 2x - 12)\right)$ imamo da i krivulja $E$ ima dobru redukciju modulo $p$.

Promotrimo još i eliptičku krivulju $\tilde{E}$ koja je *biracijonalno izomorfna* krivulji $E$. Može se pokazati da je krivulja $\tilde{E}$ sljedećeg oblika :

$$\tilde{E}: \quad y^2 = x^3 + x^2 - 234x + 1296$$

Također se može pokazati da $\tilde{E}(\mathbb{Q})$ ima dvije točke više nego $E(\mathbb{Q})$ koje se dobiju razrješenjem singulariteta u beskonačnosti. Promotrimo sada dva slučaja.

Ako je $q$ kvadratni ostatak modulo $p$ onda će $qy^2$ prolaziti kroz sve kvadratne ostatke modulo $p$ uključujući i 0 dok $y$ prolazi po svim ostacima modulo $p$. Zbog pretpostavke da ne postoje $x, y \in \mathbb{Z}$ takvi da vrijedi $p(x, y) \equiv 0 \pmod{p}$ slijedi da $(x^2 - x - 3)(x^2 + 2x - 12)$ nije 0 ili kvadratni ostatak modulo $p$ za sve $x \in \mathbb{Z}$ . Međutim to je kontradikcija jer za $x = 0$ je $(x^2 - x - 3)(x^2 + 2x - 12) = 36$ što je očito kvadrat modulo $p$.

Ako $q$ nije kvadratni ostatak modulo $p$ onda će $qy^2$ prolaziti kroz sve kvadratne neostatke modulo $p$ uključujući i 0 dok $y$ prolazi po svim ostacima modulo $p$. Zbog pretpostavke da ne postoje $x, y \in \mathbb{Z}$ takvi da vrijedi $p(x, y) \equiv 0 \pmod{p}$ slijedi da će $(x^2 - x - 3)(x^2 + 2x - 12)$ uvijek biti kvadratni ostatak modulo $p$ (ne uključujući 0) za svaki $x \in \mathbb{Z}$ . Iz toga onda imamo da će za svaki $x \in \mathbb{F}_p$ postojati dvije različite točke $(x, y)$ i $(x, -y)$ u $E(\mathbb{F}_p)$. Time imamo da je $\left|E(\mathbb{F}_p)\right| = 2p$, odnosno $\left|\tilde{E}(\mathbb{F}_p)\right| = 2p + 2$ (jer $\tilde{E}(\mathbb{Q})$ ima dvije točke više nego $E(\mathbb{Q})$ ). S druge strane primjenom *Hasseovog teorema* na krivulju $\tilde{E}$ dobijemo da je $\left|\tilde{E}(\mathbb{F}_p)\right| \leq p + 2\sqrt{p} + 1$. Iz toga imamo da onda mora biti $2p + 2 \leq p + 2\sqrt{p} + 1$, odnosno da je $\left(\sqrt{p} - 1\right)^2 \leq 0$ što je jedino moguće za $p = 1$. Međutim to daje kontradikciju jer je $p$ prost broj.

Ovime smo u oba slučaja došli do kontradikcija pa zaključujemo da moraju postojati $x, y \in \mathbb{Z}$ takvi da je $p(x, y) \equiv 0 \pmod{p}$, a samim time onda imamo i lokalnu rješivost od $E_q$ u $p$.

Ovime smo dokazali sljedeću propoziciju :

**Propozicija 1.1.4.** *Neka je $q \in \mathbb{Z}$ kvadratno slobodan broj i*

$$E_q : \quad qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$$

*Krivulja $E_q$ je svugdje lokalno rješiva ako i samo ako za svaki prosti faktor $p$ od $q$ vrijedi da je $p$ kvadratni ostatak modulo* 13 *ili* $p = 13$.

## 1.2 Brojaća funkcija za $q$-ove i pripadni Dirichletov red

Definirajmo niz $(a_n)_{n\in\mathbb{N}}$ sa :

$$a_n = \begin{cases} 1 & \text{, ako } n \text{ zadovoljava uvjet za } q\text{-ove iz Propozicije 1.1.4} \\ 0 & \text{, inače.} \end{cases}$$

Definirajmo funkciju $A : \mathbb{R} \to \mathbb{R}$ sa :

$$A(x) = \sum_{n \le x} a_n \tag{1.4}$$

Uočimo da je $A(x)$ upravo brojeća funkcija za tražene $q$-ove, tj. broji sve naše $q$-ove između 1 i $x$. Definirajmo pripadni Dirichletov red za niz $(a_n)_{n\in\mathbb{N}}$ sa :

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ za } \operatorname{Re}(s) > 1$$

Kako red $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ apsolutno knvergira za $\operatorname{Re}(s) > 1$ (za dokaz vidi 2.1) imamo da je funkcija $f(s)$ dobro definirana za $\operatorname{Re}(s) > 1$.

Iz definicije niza $(a_n)_{n\in\mathbb{N}}$ te korištenjem osnovnog teorema aritmetike i činjenice da članovima sume u $f(s)$ možemo zamijeniti redoslijed sumiranja (zbog apsolutne konvergencije of $f(s)$ na $\operatorname{Re}(s) > 1$) lagano dobijemo sljedeću jednakost :

$$f(s) = \left(1 + \frac{1}{13^s}\right) \cdot \prod_{(A)} \left(1 + \frac{1}{p^s}\right) \text{ za } \operatorname{Re}(s) > 1 \tag{1.5}$$

Ovdje $\prod_{(A)}$ označava produkt po svim prostim brojevima $p \neq 13$ koji daju kvadratni ostatak (mod 13).

Za *Riemannovu zeta funkciju* vrijedi

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

Zato je

$$\begin{aligned}\zeta(2s) &= \prod_p \left(1 - \frac{1}{p^{2s}}\right)^{-1} \\ &= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_p \left(1 + \frac{1}{p^s}\right)^{-1}\end{aligned}$$

Djeljenjem gornjih jednakosti dobijemo :

$$\frac{\zeta(s)}{\zeta(2s)} = \prod_p \left(1 + \frac{1}{p^s}\right) \text{ za } \operatorname{Re}(s) > 1 \tag{1.6}$$

Neka je $\chi : \mathbb{Z} \to \mathbb{C}$ Dirichletov karakter modulo 13 definiran sa

$$\chi(n) = \begin{cases} 1 & \text{, ako } 13 \nmid n \text{ i } n \text{ kvadratni ostatak } \pmod{13} \\ -1 & \text{, ako } n \text{ nije kvadratni ostatak } \pmod{13} \\ 0 & \text{, ako } 13 \mid n, \end{cases} \tag{1.7}$$

odnosno imamo da je $\chi(n) = \left(\frac{n}{13}\right)$ gdje $\left(\frac{\cdot}{13}\right)$ označava *Legendreov simbol*.

Promotrimo pripadnu *Dirichletovu* L-funkciju $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$. Uočimo da taj red možemo zapisati na sljedeći način :

$$\begin{aligned}L(s,\chi) &= \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \\ &= \prod_{(A)} \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{(B)} \left(1 + \frac{1}{p^s}\right)^{-1}\end{aligned}$$

Ovdje $\prod_{(A)}$ označava produkt po svim prostim brojevima $p \neq 13$ koji daju kvadratni ostatak $\pmod{13}$, a $\prod_{(B)}$ označava produkt po svim prostim brojevima $p \neq 13$ koji ne daju

kvadratni ostatak (mod 13). Iz toga slijedi da je

$$\begin{aligned} L(2s,\chi) &= \prod_{(A)} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \cdot \prod_{(B)} \left(1 + \frac{1}{p^{2s}}\right)^{-1} \\ &= \prod_{(A)} \left[\left(1 - \frac{1}{p^{s}}\right)^{-1} \left(1 + \frac{1}{p^{s}}\right)^{-1}\right] \cdot \prod_{(B)} \left(1 + \frac{1}{p^{2s}}\right)^{-1} \end{aligned}$$

Djeljenjem gornjih jednakosti dobijemo :

$$\frac{L(s,\chi)}{L(2s,\chi)} = \prod_{(A)} \left(1 + \frac{1}{p^{s}}\right) \cdot \prod_{(B)} \left[\left(1 + \frac{1}{p^{2s}}\right)\left(1 + \frac{1}{p^{s}}\right)^{-1}\right] \tag{1.8}$$

Iz (1.5) i (1.6) imamo

$$\frac{\zeta(s)}{\zeta(2s)} = f(s) \cdot \prod_{(B)} \left(1 + \frac{1}{p^{s}}\right)$$

Dok iz (1.5) i (1.8) dobijemo

$$\frac{L(s,\chi)}{L(2s,\chi)} = f(s) \cdot \left(1 + \frac{1}{13^{s}}\right)^{-1} \cdot \prod_{(B)} \left[\left(1 + \frac{1}{p^{2s}}\right)\left(1 + \frac{1}{p^{s}}\right)^{-1}\right]$$

Množenjem gornjih izraza i sređivanjem konačno dobijemo da na $\mathrm{Re}(s) > 1$ vrijedi:

$$f(s)^2 = \left(1 + \frac{1}{13^{s}}\right) \cdot \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s,\chi)}{L(2s,\chi)} \cdot \prod_{(B)} \left(1 + \frac{1}{p^{2s}}\right)^{-1} \tag{1.9}$$

**Napomena 1.2.1.** *U navedenom računu smo koristili apsolutnu konvergenciju navedenih redova na* $\mathrm{Re}(s) > 1$ *što nam je omogućilo slobodnu zamjenu poretka sumiranja u sumama i faktora u produktima.*

Radi pojednostavljenja računa i analize nekih svojstava od funkcije $f(s)$ u nastavku pretpostavljamo da vrijedi **generalizirana Riemannova hipoteza (GRH)**. GRH kaže da za sve $s \in \mathbb{C}$ za koje je $L(s,\chi) = 0$ ako $s$ nije negativan realan broj tada je nužno $\mathrm{Re}(s) = \frac{1}{2}$.

Uočimo da je desna strana u (1.9) analitička funkcija na $\mathrm{Re}(s) > \frac{1}{2}$. Naime, zadnji faktor zbog uniformne konvergencije na $\mathrm{Re}(s) > \frac{1}{2}$ definira na tom području analitičku funkciju (dokaz ide sasvim analogno kao i za $f(s)$; vidi sljedeće poglavlje), a za ostale faktore je poznato da definiraju analitičke funkcije npr. na $\mathrm{Re}(s) > 0$ te iz GRH imamo da $\zeta(2s) \neq 0$ i $L(2s,\chi) \neq 0$ na $\mathrm{Re}(s) > \frac{1}{2}$. Zato ćemo u nastavku $f(s)^2$ smatrati upravo tim analitičkim proširenjem na $\mathrm{Re}(s) > \frac{1}{2}$.

# Poglavlje 2

# Svojstva funkcije $f(s)$

U ovom poglavlju ćemo promotriti neka svojstva funkcije $f(s)$. Radi jednostavnije analize tih svojstava ćemo u nekim djelovima ovog poglavlja pretpostaviti da vrijedi GRH.

Posebno važno će nam biti analitičko proširenje funkcije $f(s)$ na $\mathrm{Re}(s) > \frac{1}{2}$ što će nam poslije omogućiti lakšu ocjenu integral koji će se pojaviti kod primjene *Perronove formule* na $f(s)$ (Poglavlje 4).

## 2.1 Apsolutna konvergencija na $\mathrm{Re}(s) \geq c > 1$

Neka je $s = \sigma + it \in \mathbb{C}$ tako da je $\sigma \geq c > 1$. Kako je $a_n \in \{0, 1\}$ za sve $n \in \mathbb{N}$ imamo redom

$$\begin{aligned}\sum_{n=1}^{\infty} \left|\frac{a_n}{n^s}\right| &\leq \sum_{n=1}^{\infty} \frac{1}{|n^{\sigma+it}|} = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} \\ &\leq 1 + \int_1^{+\infty} \frac{dx}{x^{\sigma}} = 1 + \frac{1}{\sigma - 1}\end{aligned}$$

Dakle, red kojim je definirana funkcija $f(s)$ zaista apsolutno konvergira na $\mathrm{Re}(s) \geq c > 1$. Uočimo da iz gornjeg računa za $s = \sigma + it \in \mathbb{C}$ tako da je $\sigma \geq c > 1$ vrijedi :

$$|f(s)| \leq 1 + \frac{1}{\sigma - 1} \tag{2.1}$$

## 2.2 Uniformna konvergencija na $\mathrm{Re}(s) \geq c > 1$

Uzmimo $\varepsilon > 0$. Kako je $c > 1$ imamo da red $\sum_{n=1}^{\infty} \frac{1}{n^c}$ konvergira. Zbog toga postoji dovoljno veliki $N \in \mathbb{N}$ za kojeg je $\sum_{n>N} \frac{1}{n^c} < \varepsilon$.

Sada za sve $s = \sigma + it \in \mathbb{C}$ takve da je $\sigma \geq c > 1$ imamo

$$\left| f(s) - \sum_{n=1}^{N} \frac{a_n}{n^s} \right| = \left| \sum_{n>N} \frac{a_n}{n^s} \right| \leq \sum_{n>N} \frac{1}{|n^s|} = \sum_{n>N} \frac{1}{n^\sigma}$$
$$\leq \sum_{n>N} \frac{1}{n^c} < \varepsilon$$

Pri čemu smo u prvoj nejednakosti koristili nejednakost trokuta i $a_n \in \{0, 1\}$, a u drugoj $\sigma \geq c$. Iz gornjeg dobivamo da red kojim je definirana funkcija $f(s)$ konvergira uniformno na $\mathrm{Re}(s) \geq c > 1$.

Uočimo još da su sve parcijalne sume reda kojim je definirana $f(s)$ analitičke funkcije na $\mathrm{Re}(s) \geq c > 1$ pa iz uniformne konvergencije dobijemo da je i $f(s)$ analitička na $\mathrm{Re}(s) \geq c > 1$.

## 2.3 Analitičko proširenje od $f(s)$ na $\mathrm{Re}(s) > \frac{1}{2}$

Neka je $s = \sigma + it \in \mathbb{C}$ takav da je $\sigma > 1$. Iz $f(s) - 1 = \sum_{n=2}^{\infty} \frac{a_n}{n^s}$ analognim računom koji nas je doveo do (2.1) dobijemo $|f(s) - 1| \leq \frac{1}{\sigma - 1}$.

Promortimo područje $\mathrm{Re}(s) > 3$, tj. $\sigma > 3$. Kako je to otvoren i povezan podskup od $\mathbb{C}$ onda možemo zapisati $f(s) = 1 + (f(s) - 1)$. Posebno za $\sigma > 3$ imamo $|f(s) - 1| \leq \frac{1}{\sigma - 1} \leq \frac{1}{2}$. Iz nejednakosti trokuta dobijemo da na $\mathrm{Re}(s) > 3$ vrijedi

$$|f(s)| = |1 + (f(s) - 1)| \geq 1 - |f(s) - 1| \geq \frac{1}{2} \tag{2.2}$$

Nadalje, uočimo da na $\mathrm{Re}(s) > 3$ vrijedi $|f(s) - 1| \leq \frac{1}{2}$ što znači da je $f(s) \in \overline{\mathrm{K}}(1, \frac{1}{2})$ gdje je $\overline{\mathrm{K}}(1, \frac{1}{2})$ zatvoreni krug oko 1 radijusa $\frac{1}{2}$ u $\mathbb{C}$. Iz toga dobijemo da je na $\mathrm{Re}(s) > 3$ $|Arg\,(f(s))|$ manji ili jednak kutu koji zatvaraju tangenta iz ishodišta na $\overline{\mathrm{K}}(1, \frac{1}{2})$ i realna os. Laganom trigonometrijom se dobije da taj kut iznosi $\frac{\pi}{6}$. Prema tome na $\mathrm{Re}(s) > 3$ vrijedi

$$Arg(f(s)) \in \left\langle -\frac{\pi}{6}, \frac{\pi}{6} \right\rangle \tag{2.3}$$

Zbog (2.2) i (2.3) pri uzimanju glavne vrijednosti kvadratnog korijena od $f(s)^2$ na $\mathrm{Re}(s) > 3$ ćemo zato dobiti $f(s)$, a ne $-f(s)$. Dakle, vrijedi

$$f(s) = \sqrt{f(s)^2} \quad \text{na } \mathrm{Re}(s) > 3 \tag{2.4}$$

Za analitičko proširenje od $f(s)$ na $\mathrm{Re}(s) > \frac{1}{2}$ ćemo koristiti sljedeći rezultati iz kompleksne analize :

**Teorem 2.3.1.** ***(Monodromy theorem)*** *Neka je $U$ otvoren krug u $\mathbb{C}$ sa središtem u točki $P$ i neka je $f : U \to \mathbb{C}$ analitička funkcija. Ako je $W$ otvoren i jednostavno povezan podskup od $\mathbb{C}$ takav da je $U \subseteq W$ te ako je moguće $f$ analitički proširiti duž bilo koje krivulje sadržane u $W$ s početkom u točki $P$, tada $f$ možemo analitički proširiti na $W$, tj. postoji analitička funkcija $F : W \to \mathbb{C}$ takva da je $F|_U = f$*

Dokaz ovog teorema se može naći u [2] (vidi Poglavlje 8, Paragraf 25). Sada pomoću (2.4) i formule (1.9) koja nam daje analitičko proširenje od $f(s)^2$ na $\mathrm{Re}(s) > \frac{1}{2}$ pomoću gornjeg teorema za područje $W \coloneqq \left\{s \in \mathbb{C} : \mathrm{Re}(s) > \frac{1}{2}\right\}$ možemo pokušati proširiti $f(s)$ na $W$ tako da definiramo

$$f(s) \coloneqq \sqrt{f(s)^2} \quad \text{za } \mathrm{Re}(s) > \frac{1}{2}\,. \tag{2.5}$$

Uočimo da je sa (2.5) $f(s)$ dobro definiran osim za nule i polove od $f(s)^2$. Naime, te nule i polovi će davati točke grananja kada ćemo uzimati kvadratni korijen. Kako smo prije pretpostavili da vrijedi GRH imamo da je na $W$ jedini problem točka $s = 1$ koja stvara pol u $f(s)$ (dolazi od pola funkcije $\zeta(s)$ u $s = 1$). Zato ćemo iz $W$ izbaciti zraku $\langle -\infty, 1]$ jer duž te zrake $f(s)$ neće biti analitička. Ovime konačno dobijemo da je sada $f(s)$ definirana formulom (2.5) analitička na $R = \left\{s \in \mathbb{C} : \mathrm{Re}(s) > \frac{1}{2}\right\} \setminus \langle -\infty, 1]$

**Napomena 2.3.2.** *U poglavlju 4 ćemo integrirati na području* $\mathrm{Re}(s) > \frac{1}{2}$ *po konturi "ključanice" i to će nam omogućiti da zaobiđemo zraku* $\langle -\infty, 1]$ *tako da nam izbacivanje te zrake iz domene funkcije $f(s)$ zapravo ne stvara problem.*

## 2.4 Reziduum od $f(s)$ u $s = 1$

Uočimo da prema (1.9) pol od $f(s)$ u $s = 1$ dolazi od pola funkcije $\zeta(s)$ u $s = 1$. Kako $\zeta(s)$ ima jednostavni pol u $s = 1$ onda možemo zapisati $\zeta(s) = \frac{H(s)}{s-1}$ gdje je $H(s)$ analitička funkcija. Time je onda $f(s)^2 = \frac{F(s)}{s-1}$ gdje je $F(s)$ analitička funkcija na $\mathrm{Re}(s) > \frac{1}{2}$. Iz ovog imamo da za odrađivanje reziduuma of $f(s)$ u $s = 1$ trebamo zapravo odrediti reziduum od $\frac{1}{\sqrt{s-1}}$ u $s = 1$, odnosno od $\frac{1}{\sqrt{s}}$ u $s = 0$ (nakon što napravimo odgovarajuću translaciju).

Neka je $\gamma = S(0, r)$ pozitivno orijentirana kružnica oko ishodišta radijusa $r > 0$ u $\mathbb{C}$. Tada je

$$\int_\gamma \frac{1}{\sqrt{s}}\,ds = \int_0^{2\pi} \frac{ire^{i\varphi}}{r^{\frac{1}{2}} e^{\frac{i\varphi}{2}}}\,d\varphi = ir^{\frac{1}{2}} \int_0^{2\pi} e^{\frac{i\varphi}{2}}\,d\varphi = -4r^{\frac{1}{2}}$$

Puštanjem $r \to 0$ vidimo da gornji integral teži k 0. Time je traženi reziduum 0 pa je zato i reziduum od $f(s)$ u $s = 1$ isto 0.

## 2.5 Gornja ograda za $|f(s)|$ na $\mathrm{Re}(s) = \frac{1}{2} + \delta$

Neka je $\delta > 0$ i $s \in \mathbb{C}$ takav da je $\mathrm{Re}(s) = \frac{1}{2} + \delta$. Tada vrijedi :

$$\left|1 + \frac{1}{13^s}\right| = \frac{\left|1 + e^{s \ln 13}\right|}{\left|e^{s \ln 13}\right|} \leq \frac{1 + 13^{\frac{1}{2}+\delta}}{13^{\frac{1}{2}+\delta}} = O(1) \tag{2.6}$$

$$\begin{aligned}\left|\prod_{(B)}\left(1 + \frac{1}{p^{2s}}\right)^{-1}\right| &= \prod_{(B)} \frac{\left|p^{2s}\right|}{\left|p^{2s}+1\right|} \leq \prod_{(B)} \frac{p^{1+2\delta}}{p^{1+2\delta}-1} = \prod_{(B)}\left(1 - \frac{1}{p^{1+2\delta}}\right)^{-1} \\ &\leq \prod_{p}\left(1 - \frac{1}{p^{1+2\delta}}\right)^{-1} = \zeta(1+2\delta) = O(1)\end{aligned} \tag{2.7}$$

Poznato je da za *Riemannovu zeta funkciju* $\zeta(s)$ vrijedi sljedeća funkcijaska jednadžba

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s) \tag{2.8}$$

gdje $\Gamma(s)$ označava gama-funkciju. Dokaz gornje jednakosti se može naći u [5] (vidi Teorem 2.7). Za gornju ogradu od $\zeta(s)$ ćemo koristiti sljedeći teorem :

**Teorem 2.5.1.** *Postoji funkcija $\mu$ definirana sa*

$$\mu(\sigma) = \inf\{a \in \mathbb{R} : |\zeta(\sigma + it)| = O\left(|t|^a\right) \text{ kada } t \to \infty\}$$

*Funkcija $\mu$ je konveksna i zadovoljava*

$$\mu(\sigma) = 0 \quad za\ \sigma > 1$$
$$\mu(\sigma) = \frac{1}{2} - \sigma \quad za\ \sigma < 0$$

Dokaz ovog teorema koristi funkcijsku jednadžbu (2.8) i *Phragmén–Lindelöf teorem* i može se naći u [5] (vidi Teorem 2.12 i poglavlje 5.2). Posebno iz ovog teorema zbog konveksnosti od funkcije $\mu$ slijedi $\mu(\frac{1}{2} + \delta) \leq \frac{1}{4} - \frac{\delta}{2} < \frac{1}{4}$. Iz definicije funkcije $\mu$ imamo da za $\mathrm{Re}(s) = \frac{1}{2} + \delta$ postoji $0 < \varepsilon < \frac{1}{4}$ tako da vrijedi

$$|\zeta(s)| = O\left(|t|^{\varepsilon}\right) \tag{2.9}$$

Prema [3] ( Korolar 10.9 ) za našu *Dirichletovu L*-funkciju vrijedi sljedeća funkcijska jednadžba

$$L(s,\chi) = \varepsilon(\chi)2^s 13^{\frac{1}{2}-s}\pi^{s-1}\sin\left(\frac{\pi s}{2}\right)\Gamma(1-s)L(1-s,\chi) \tag{2.10}$$

Pri čemu je $\varepsilon(\chi) = \frac{\sum_{n=1}^{13}\chi(n)\exp(2\pi i n/q)}{\sqrt{13}}$ i vrijedi da je $|\varepsilon(\chi)| = 1$. Iz gornje funkcijske jednadže i korištenjem istih tehnika kao u 2.5.1 dobijemo sljedeću ogradu za $L(s,\chi)$.
Za $\mathrm{Re}(s) = \frac{1}{2} + \delta$ postoji $0 < \varepsilon < \frac{1}{4}$ tako da vrijedi

$$|L(s,\chi)| = O\left(|t|^{\varepsilon}\right) \tag{2.11}$$

Za gornju ogradu od $\frac{1}{\zeta(2s)L(2s,\chi)}$ ćemo koristiti *Dedekindovu zeta funkciju*.

**Definicija 2.5.2.** *Neka je K polje algebarskih brojeva i R prsten cijelih u K. Za $s \in \mathbb{C}$ takav da je* $\mathrm{Re}(s) > 1$ *definiramo Dedekindovu zeta funkciju polja K sa*

$$\zeta_K(s) = \sum_{I\subseteq R}\frac{1}{\|I\|^s}$$

*pri tome gornja suma ide po svim ne-nul idealina I od R, a $\|I\|$ označava normu ideala I.*

Korištenjem jedinstvene faktorizacije ne-nul ideala u $R$ na proste ideale se može pokazati da vrijedi sljedeća produktna formula za *Dedekindovu zeta funkciju*

$$\zeta_K(s) = \prod_{\substack{P\subseteq R\\ P\text{ prost}}}\left(1 - \frac{1}{\|P\|^s}\right)^{-1} \tag{2.12}$$

Nadalje, u slučaju kvadratnog proširenja $\mathbb{Q} \subset K$ poznato je da se *Dedekindovu zeta funkciju* može zapisati kao produkt *Riemannove zeta funkcije* i *Dirichletove L*-funkcije kvadratnog *Dirichletovog karaktera* $\chi$. U našem slučaju za polje $K = \mathbb{Q}[\sqrt{13}]$ imamo da je $\zeta_K(s) = \zeta(s)L(s,\chi)$ gdje je $\chi$ definiran kao u (1.7).

Uzimanjem kompleksnog logaritma u (2.12) i korištenjem Taylorovog razvoja od $\ln(1-z)$ dobijemo da za $s = \sigma + it$ vrijedi

$$\ln\zeta_K(s) = -\sum_{\substack{P\subseteq R\\ P\text{ prost}}}\sum_{n=1}^{\infty}\frac{1}{n\|P\|^{ns}} = -\sum_{\substack{P\subseteq R\\ P\text{ prost}}}\sum_{n=1}^{\infty}\frac{\cos(nt\ln\|P\|) - i\sin(nt\ln\|P\|)}{n\|P\|^{n\sigma}}$$

Iz gornje jednakosti slijedi da je

$$|\zeta_K(\sigma+it)| = \exp\left(\sum_{\substack{P\subseteq R\\ P\text{ prost}}}\sum_{n=1}^{\infty}\frac{\cos(nt\ln\|P\|)}{n\|P\|^{n\sigma}}\right)$$

Korištenjem nejednakosti $3 + 4\cos x + \cos(2x) = 2(1 + \cos x)^2 \geq 0$ dobijemo

$$\left|\zeta_K(\sigma)^3 \zeta_K(\sigma + it)^4 \zeta_K(\sigma + 2it)\right| = \exp\left( \sum_{\substack{P \subseteq R \\ P \text{ prost}}} \sum_{n=1}^{\infty} \frac{3 + 4\cos(nt \ln \|P\|) + \cos(2nt \ln \|P\|)}{n \|P\|^{n\sigma}} \right) \geq 1$$

Iz čega slijedi

$$\frac{1}{|\zeta_K(\sigma + it)|} \leq |\zeta_K(\sigma)|^{\frac{3}{4}} |\zeta_K(\sigma + 2it)|^{\frac{1}{4}} \tag{2.13}$$

Posebno, za $\mathrm{Re}(s) = \sigma = \frac{1}{2} + \delta$ imamo da je $\zeta_K(2\sigma) = \zeta_K(1 + 2\delta) = O(1)$ i $|\zeta_K(2\sigma + 4it)| \leq |\zeta_K(2\sigma)| = O(1)$. Time iz (2.13) dobijemo da za $\mathrm{Re}(s) = \sigma = \frac{1}{2} + \delta$ vrijedi sljedeća ograda

$$\frac{1}{|\zeta(2s)L(2s, \chi)|} = \frac{1}{|\zeta_K(2s)|} = O(1) \tag{2.14}$$

Konačno iz (1.9) i ograda (2.6), (2.7), (2.9), (2.11) i (2.14) dobijemo da za $\mathrm{Re}(s) = \sigma = \frac{1}{2} + \delta$ postoji $0 < \varepsilon < \frac{1}{4}$ tako da vrijedi

$$|f(s)| = O\left(|t|^{\varepsilon}\right) \tag{2.15}$$

# Poglavlje 3

# Perronova formula i ocjena greške

**Teorem 3.0.1.** ***(Perronova formula)*** *Neka je* $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *Dirichletov red koji apsolutno konvergira na* $\mathrm{Re}(s) > 1$. *Tada za* $x$ *koji nije cijeli broj,* $c > 1$ *i* $T > 0$ *vrijedi*

$$\sum_{n \leq x} a_n = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} f(s) \frac{x^s}{s}\, ds + O\left( \sum_{n=1}^{\infty} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln \frac{x}{n}\right|}\right\}\right)$$

Dokaz teorema se može naći u [4] (vidi Poglavlje 4, zadatak 4.4.15). Odmah je jasno da ćemo primjenom gornje formule na naš Dirichletov red $f(s)$ definiran u Poglavlju 1 dobiti upravo našu brojaću funkciju $A(x)$. U nastavku ćemo modificirati ocjenu greške koju nam daje *Perronova formula* za našu funkciju $f(s)$ da bismo kasnije lakše mogli analizrati traženu asimptotiku od $A(x)$.

Stavimo $c = 1 + \frac{1}{\ln x}$. Tada je $x^c = e^{c \ln x} = e^{\ln x + 1} = ex$. Nadalje, podijelimo sumu na dva djela

$$\sum_{n=1}^{\infty} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln \frac{x}{n}\right|}\right\} = I_1 + I_2 \tag{3.1}$$

gdje su

$$I_1 = \sum_{\substack{n \geq 1 \\ |n-x| > \frac{x}{4}}} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln \frac{x}{n}\right|}\right\}$$

$$I_2 = \sum_{\substack{n \geq 1 \\ |n-x| \leq \frac{x}{4}}} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln \frac{x}{n}\right|}\right\}$$

Imamo da je

$$I_1 = \sum_{\substack{n\geq 1\\ |n-x|>\frac{x}{4}}} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\} = ex \sum_{\substack{n\geq 1\\ |n-x|>\frac{x}{4}}} \frac{a_n}{n^c} \min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\}$$
$$\leq ex \sum_{n=1}^{\infty} \frac{1}{\ln\frac{4}{3}} \cdot \frac{|a_n|}{n^c} \cdot \frac{1}{T} = \frac{e}{\ln\frac{4}{3}} f(c)\frac{x}{T}$$

Pri čemu smo u drugoj jednakosti iskoristili da je $x^c = ex$ i da je $a_n \geq 0$. Kod nejednakosti smo iskoristili da za prirodne brojeve $n$ koji zadovoljavaju $|x-n| > \frac{x}{4}$ vrijedi $\left|\ln\frac{x}{n}\right| > \ln\frac{4}{3}$. Zato je $\min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\} \leq \frac{1}{T\ln\frac{4}{3}}$ i poslije smo još povećali granice za $n$ po kojima sumiramo. U zadnjoj jednakosti smo koristili definiciju funkcije $f(s)$.

Promotrimo sada ponašanje od $f(c(x))$ za $c = 1 + \frac{1}{\ln x}$ kada $x \to +\infty$. Iz (1.9) znamo da na $\mathrm{Re}(s) > \frac{1}{2}$ funkcija $f(s)$ ima pol u $s = 1$ zbog $\sqrt{\zeta(s)}$. Zato možemo zapisati $f(s) = \frac{F(s)}{\sqrt{s-1}}$ gdje je $F(s)$ analitička oko $s = 1$. Iz neprekidnosti od $F$ imamo da je $F(s)$ "blizu" $F(1)$ što je neka konstanta. Time je onda $f(c(x)) = O\left(\frac{1}{\sqrt{c(x)-1}}\right) = O\left(\sqrt{\ln x}\right)$.

Uvrštavanjem u gornju nejednakost dobijemo

$$I_1 = O\left(\frac{x\sqrt{\ln x}}{T}\right) \tag{3.2}$$

Za prirodan broj $n$ koji zadovoljava $|x-n| \leq \frac{x}{4}$ imamo da je $n \in \left[\frac{3}{4}x, \frac{5}{4}x\right]$. Rastavimo sada $I_2 = J_1 + J_2$ gdje su

$$J_1 = \sum_{n\in[\frac{3}{4}x, x\rangle} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\}$$
$$J_2 = \sum_{n\in\langle x, \frac{5}{4}x]} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\}$$

Ocjenimo sada izraz $J_1$. Označimo sa $x_1$ najveći $n \in [\frac{3}{4}x, x\rangle$ za koji je $a_n = 1$. Član u $x_1$ kod $J_1$ pridonosi s $O(1)$. Zapišimo ostale članove tog intervala sa $n = x_1 - m$ gdje $m$ ide po prirodnim brojevima iz intervala $\langle 0, \frac{x}{4}\rangle$. Tada je

$$\left|\ln\frac{x}{n}\right| \geq \left|\ln\frac{x_1}{n}\right| = \left|\ln\frac{n}{x_1}\right| = \left|\ln\frac{x_1-m}{x_1}\right|$$
$$\geq \left|\ln\left(1-\frac{m}{x_1}\right)\right| \geq \frac{m}{x_1}$$

Ovdje smo u prvoj nejednakosti koristili da je $\frac{x}{n} \geq \frac{x_1}{n} > 1$. U drugoj nejednakosti smo koristili nejednakost $|\ln(1-y)| \geq y$ koja se lako dobije iz Taylorovog reda $\ln(1-y) = -\sum_{n=1}^{\infty} \frac{1}{n} y^n$. Pomoću gornje nejednakosti i korištenjem da je $\left(\frac{x}{n}\right)^c$ ograničen za $n \in \langle \frac{3}{4}x, x \rangle$ za dovoljno velike $T$ imamo ocjenu ostalih članova u $J_1$ :

$$\begin{aligned}\sum_{\substack{n\in\langle \frac{3}{4}x,x\rangle \\ n\neq x_1}} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\} &<< \frac{1}{T} \sum_{m\in\langle 0,\frac{x}{4}\rangle} a_n \frac{x_1}{m} \leq \frac{x}{T} \sum_{m\in\langle 0,\frac{x}{4}\rangle} \frac{1}{m} \\ &<< \frac{x}{T} \int_1^{\frac{x}{4}} \frac{1}{u}\, du = \frac{x}{T} \ln\frac{x}{4} \\ &<< \frac{x \ln x}{T}\end{aligned}$$

Pri čemu smo u drugoj nejednakosti koristili $x_1 \leq x$ i $a_n \leq 1$. Ovime konačno dobijemo

$$J_1 = O\left(\frac{x \ln x}{T} + 1\right) \tag{3.3}$$

Ocjenu za $J_2$ radimo sasvim analogno gledajući $x_1$ koji je najmanji $n \in \langle x, \frac{5}{4}x]$ za koji je $a_n = 1$. Iz toga dobijemo

$$J_2 = O\left(\frac{x \ln x}{T} + 1\right) \tag{3.4}$$

Korištenjem ocjena (3.2), (3.3) i (3.4) iz (3.1) dobijemo

$$\sum_{n=1}^{\infty} \left(\frac{x}{n}\right)^c |a_n| \min\left\{1, \frac{1}{T\left|\ln\frac{x}{n}\right|}\right\} = O\left(\frac{x \ln x}{T} + 1\right)$$

Iz Perronove formule i gornje ocjene dobijemo da za našu funkciju $f(s)$ vrijedi :

$$A(x) = \sum_{n\leq x} a_n = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} f(s) \frac{x^s}{s}\, ds + O\left(\frac{x \ln x}{T} + 1\right) \tag{3.5}$$

# Poglavlje 4

# Asimptotika brojaće funkcije $A(x)$

Integral koji se javlja u *Perronovoj formuli* (3.5) je kompliciran za računanje, zato uvodimo *konturu ključanice* (*key-hole contour*). Tom konturom ćemo integral iz *Perronove formule* svesti na integrale po drugim krivuljama na kojima će ih biti lakše ocjeniti i time u konačnici dobiti traženu asimptotiku za $A(x)$. Napomenimo da smo u ovom izvodu asimptotike funkcije $A(x)$ pretpostavili da vrijedi GRH.

## 4.1 Kontura ključanice

Neka su $r > 0$, $d > 0$, $\delta > 0$, $c > 1$ i $T > 0$. *Kontura ključanice* $K$ se sastoji od krivulja $A$, $B$, $C$, $C'$, $D$ i $D'$ označenih na slici 4.1.

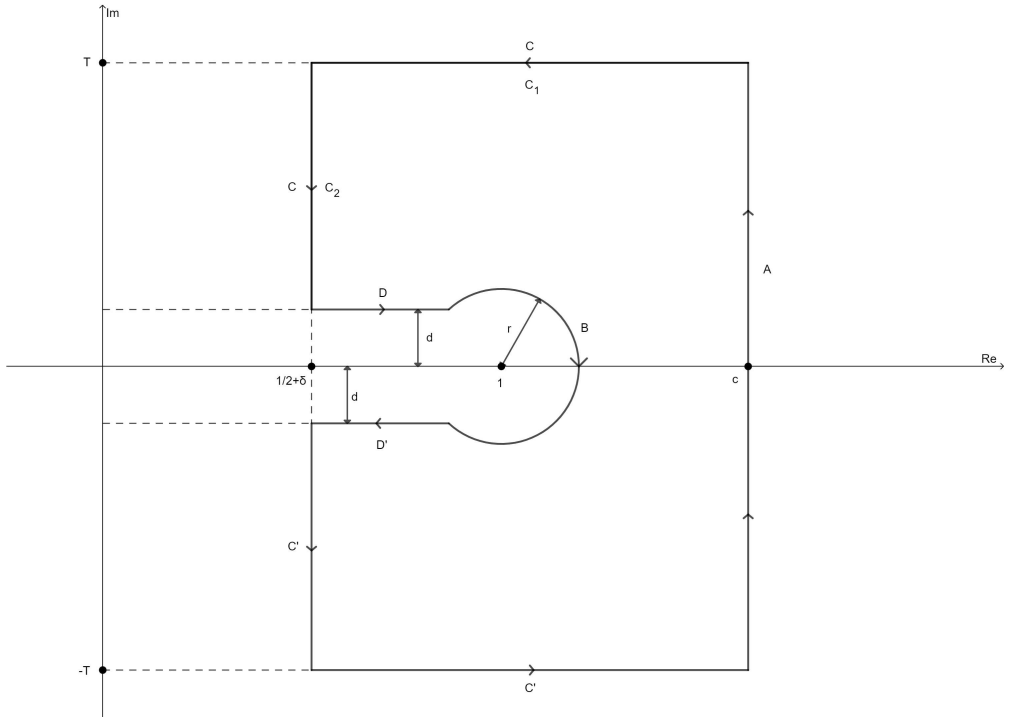
Krivulja $A$ je segment od $c - iT$ do $c + iT$. Krivulja $B$ je dio kružnice oko 1 radijusa $r$. Krivulja $C$ se sastoji od segmenta koji ide od $c + iT$ do $\frac{1}{2} + \delta + iT$ i segmenta koji ide od $\frac{1}{2} + \delta + iT$ do $\frac{1}{2} + \delta + id$. Krivulja $C'$ se sastoji od segmenta koji ide od $\frac{1}{2} + \delta - id$ do $\frac{1}{2} + \delta - iT$ i segmenta koji ide od $\frac{1}{2} + \delta - iT$ do $c - iT$. Krivulja $D$ je segment paralelan s realnom osi koji spaja $\frac{1}{2} + \delta + id$ i prvu točku presjeka s kružnicom oko 1 radijusa $r$. Krivulja $D'$ je segment paralelan s realnom osi koji spaja $\frac{1}{2} + \delta - id$ i prvu točku presjeka s kružnicom oko 1 radijusa $r$.

Kako unutar konture $K$ funkcija $f(s)\frac{x^s}{s}$ nema polova po *teoremu o reziduumu* imamo

$$\int_K f(s)\frac{x^s}{s}\,ds = 0 \quad \text{, odnosno}$$

$$\int_A f(s)\frac{x^s}{s}\,ds = -\int_{C+D+B+D'+C'} f(s)\frac{x^s}{s}\,ds \tag{4.1}$$

Ovime smo sveli integral koji se javlja u *Perronovoj formuli* (integral po $A$) na integrale po krivuljama $C$, $D$, $B$, $D'$ i $C'$. U nastavku ćemo posebno ocjeniti svaki od tih integrala.




Slika 4.1: Kontura ključanice (key-hole contour)

## 4.2 Ocjene integrala

### Integral po $B$

Fiksirajmo $r > 0$. Neka je $\gamma$ kružnica oko 1 radijusa $r$ iste orijentacije kao i $B$. Označimo redom s $P$ i $Q$ početak i kraj krivulje $B$. Neka je krivulja $B'$ dio kružnice $\gamma$ koji spaja $Q$ i $P$ iste orijentacije kao $B$. Označimo sa $\alpha$ veličinu središnjeg kuta nad lukom $B'$ kružnice $\gamma$ u radijanima (vidi sliku 4.2).

Imamo da je

$$\int_B f(s)\frac{x^s}{s}\,ds = \int_\gamma f(s)\frac{x^s}{s}\,ds - \int_{B'} f(s)\frac{x^s}{s}\,ds \tag{4.2}$$

U 2.4 smo pokazali da je $\mathrm{Res}(f(s), 1) = 0$ pa je time i $\mathrm{Res}(f(s)\frac{x^s}{s}, 1) = 0$. Kako funkcije $f(s)\frac{x^s}{s}$ unutar $\gamma$ ima jedino pol u $s = 1$ po *teoremu o reziduumu* imamo

$$\int_\gamma f(s)\frac{x^s}{s}\,ds = 0 \tag{4.3}$$

Kako je funkcija $f(s)\frac{x^s}{s}$ neprekidna na kompaktnom skupu $\gamma$ onda njena apsolutna vrijednost postiže neki maksimum na $\gamma$. Označimo taj maksimum s $M$ (koji ovisi o $r$). Tada imamo da je $\left|f(s)\frac{x^s}{s}\right| \leq M$ za sve točke $s$ na $\gamma$. Time dobivamo sljedeću ocjenu

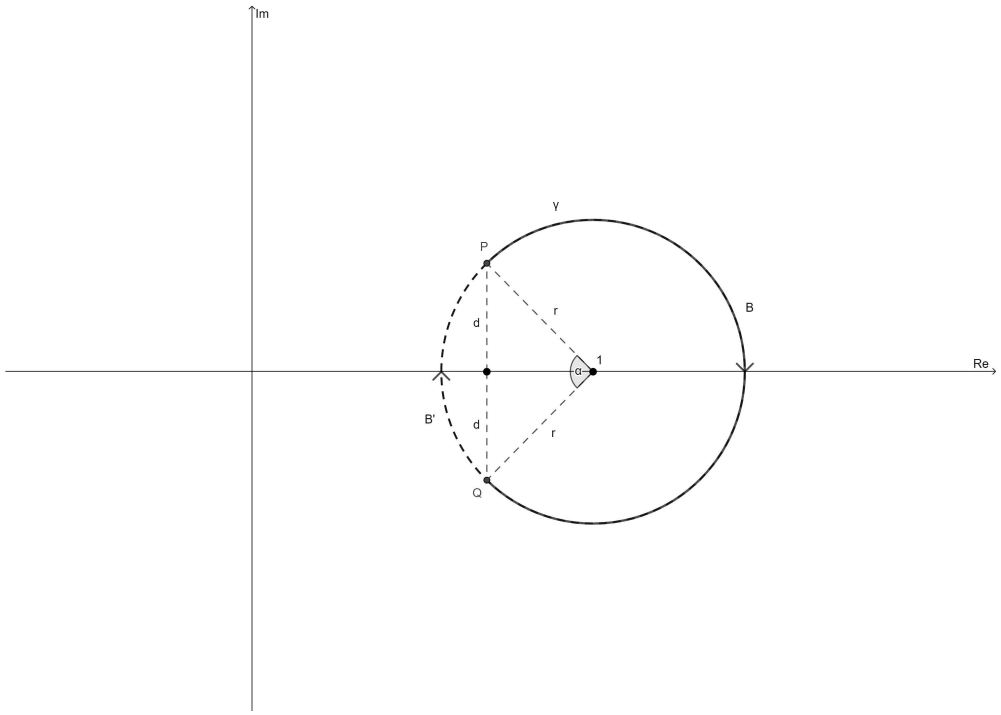
$$\left|\int_{B'} f(s)\frac{x^s}{s}\,ds\right| \leq M \cdot l(B') \tag{4.4}$$

gdje $l(B')$ označava duljinu krivulje $B'$. Kako je $B'$ luk sa središnji kutem $\alpha$ imamo da je $l(B') = r\alpha$. Pomoću trigonometrije lagano dobijemo da je $\alpha = 2\arcsin\frac{d}{r}$. Puštanjem da $d$ teži k 0 imamo da $\alpha \to 0$ pa samim time i $l(B') \to 0$. Sada primjenom *teorema o sendviču* iz (4.4) dobijemo

$$\lim_{d\to 0^+} \int_{B'} f(s)\frac{x^s}{s}\,ds = 0 \tag{4.5}$$

Konačno puštanjem da $d$ teži k 0 u (4.2) i korištenjem (4.3) i (4.5) imamo

$$\lim_{d\to 0^+} \int_{B} f(s)\frac{x^s}{s}\,ds = 0 \tag{4.6}$$




Slika 4.2: Krivulje $B$, $B'$ i $\gamma$

## Integral po $C$ i $C'$

Označimo sa $C_1$ segment od $c+iT$ do $\frac{1}{2}+\delta+iT$ i sa $C_2$ segment od $\frac{1}{2}+\delta+iT$ do $\frac{1}{2}+\delta+id$. Podsjetimo se ograde (2.15), tj. da za $s=\sigma+it$ na $\mathrm{Re}(s)=\frac{1}{2}+\delta$ vrijedi $|f(s)|=O(|t|^{\varepsilon})$ za neki $0<\varepsilon<\frac{1}{4}$. Nadalje, za $s=\sigma+it$ na $\mathrm{Re}(s)=c>1$ imamo da je $|\zeta(s)L(s,\chi)|=|\zeta_K(s)|\leq\zeta_K(c)=O(1)$ te korištenjem (2.13) imamo da je $\frac{1}{|\zeta(2s)L(2s,\chi)|}=\frac{1}{|\zeta_K(2s)|}=O(1)$. Iz gornjih ograda sada lagano slijedi da je $|f(s)|=O(1)$ na $\mathrm{Re}(s)=c$. Konačno iz gornjih ocjena na $\mathrm{Re}(s)=\frac{1}{2}+\delta$ i $\mathrm{Re}(s)=c$ primjenom *Phragmén–Lindelöfova teorema* dobijemo da za dovoljno veliki $T$ vrijedi $|f(s)|=O(T^{\varepsilon})$ na $C_1$, tj. imamo da postoji neka konstanta $K>0$ tako da je $|f(s)|\leq KT^{\varepsilon}$ na $C_1$.

Sada možemo ocjeniti integral po $C_1$.

$$\begin{aligned}\left|\int_{C_1} f(s)\frac{x^s}{s}\,ds\right| &= \left|\int_{\frac{1}{2}+\delta+iT}^{c+iT} f(s)\frac{x^s}{s}\,ds\right| \leq \int_{\frac{1}{2}+\delta}^{c} |f(\sigma+iT)|\,\frac{\left|x^{\sigma+iT}\right|}{\sqrt{\sigma^2+T^2}}\,d\sigma\\ &\leq K\int_{\frac{1}{2}+\delta}^{c} T^{\varepsilon}\,\frac{\left|e^{(\sigma+iT)\ln x}\right|}{\sqrt{\sigma^2+T^2}}\,d\sigma\\ &\leq K\int_{\frac{1}{2}}^{c} T^{\varepsilon-1}e^{\sigma\ln x}\,d\sigma = KT^{\varepsilon-1}\frac{ex-x^{\frac{1}{2}+\delta}}{\ln x}\\ &= O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right) \quad \text{za dovoljno mali } \delta\end{aligned}$$

Dakle, imamo da za dovoljno mali $\delta$ vrijedi

$$\int_{C_1} f(s)\frac{x^s}{s}\,ds = O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right). \tag{4.7}$$

Na $C_2$ pomoću ograde (2.15) imamo sljedeću ocjenu :

$$\begin{aligned}\left|\int_{C_2} f(s)\frac{x^s}{s}\,ds\right| &= \left|\int_{\frac{1}{2}+\delta+id}^{\frac{1}{2}+\delta+iT} f(s)\frac{x^s}{s}\,ds\right| \leq \int_0^T \left|f\left(\frac{1}{2}+\delta+it\right)\right|\,\frac{\left|e^{(\frac{1}{2}+\delta+it)\ln x}\right|}{\sqrt{(\frac{1}{2}+\delta)^2+t^2}}\,dt\\ &\leq M\int_0^T t^{\varepsilon}\frac{x^{\frac{1}{2}+\delta}}{t}\,dt = Mx^{\frac{1}{2}+\delta}\int_0^T t^{\varepsilon-1}\,dt = \frac{M}{\varepsilon}T^{\varepsilon}x^{\frac{1}{2}+\delta}\end{aligned}$$

gdje je $M>0$ konstanta takva da vrijedi $\left|f\left(\frac{1}{2}+\delta+it\right)\right|\leq M|t|^{\varepsilon}$. Odnosno imamo da je

$$\int_{C_2} f(s)\frac{x^s}{s}\,ds = O\left(T^{\varepsilon}x^{\frac{1}{2}+\delta}\right) \tag{4.8}$$

Iz (4.7) i (4.8) imamo :

$$\int_C f(s)\frac{x^s}{s}\,ds = \int_{C_1} f(s)\frac{x^s}{s}\,ds + \int_{C_2} f(s)\frac{x^s}{s}\,ds = O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right) + O\left(T^{\varepsilon}x^{\frac{1}{2}+\delta}\right)$$

Analognim računom za $C'$ dobijemo :

$$\int_{C'} f(s)\frac{x^s}{s}\,ds = O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right) + O\left(T^{\varepsilon}x^{\frac{1}{2}+\delta}\right)$$

Time konačno dobivamo da vrijedi sljedeća ocjena

$$\int_{C+C'} f(s)\frac{x^s}{s}\,ds = O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right) + O\left(T^{\varepsilon}x^{\frac{1}{2}+\delta}\right) \tag{4.9}$$

## Integral po $D$ i $D'$

Uočimo da puštanjem $r \to 0^+$ krivulja $D$ postaje segment od $\frac{1}{2}+\delta+id$ do $1+id$, a krivulja $D'$ segment od $1-id$ do $\frac{1}{2}+\delta-id$. Iz toga slijedi da je

$$\int_{D+D'} f(s)\frac{x^s}{s}\,ds = \int_{\frac{1}{2}+\delta}^{1} f(\sigma+id)\frac{x^{\sigma+id}}{\sigma+id}\,d\sigma - \int_{\frac{1}{2}+\delta}^{1} f(\sigma-id)\frac{x^{\sigma-id}}{\sigma-id}\,d\sigma \tag{4.10}$$

Iz (1.9) imamo da je $f(\sigma+id) = \sqrt{x+iy}$ (u smislu glavne vrijednosti drugog korijena) gdje $x$ i $y$ ovise o $\sigma$ i $d$. Nadalje, iz uniformne konvergencije Dirichletovog reda kojim je definirana funkcija $f(s)$ dobijemo da kada $d$ teži k 0 da onda $\sqrt{x} \to f(\sigma)$, a $y \to 0$. Zapišimo sada $x+iy = \sqrt{x^2+y^2}e^{i\varphi}$ gdje je $\varphi$ argument od $x+iy$. Uočimo da zbog $y \to 0$ kada $d$ teži k 0 imamo da i $\varphi \to 0$ kada $d$ teži k 0. Iz ovog konačno imamo

$$\lim_{d\to 0^+} f(\sigma+id) = \lim_{d\to 0^+} \left(x^2+y^2\right)^{\frac{1}{4}} e^{\frac{i\varphi}{2}} = f(\sigma)\,. \tag{4.11}$$

Kako je $f(\sigma+id) = \sqrt{x+iy}$ iz definicije od $f(s)$ dobijemo da je $f(\sigma-id) = \sqrt{x-iy}$ (u smislu glavne vrijednosti drugog korijena). Uočimo da je $x-iy = \sqrt{x^2+y^2}e^{2\pi i-i\varphi}$.
Iz toga sada dobijemo

$$\lim_{d\to 0^+} f(\sigma-id) = \lim_{d\to 0^+} \left(x^2+y^2\right)^{\frac{1}{4}} e^{\frac{2\pi i-i\varphi}{2}} = -f(\sigma)\,. \tag{4.12}$$

Sada iz (4.10) primjenom *Lebesgueovog teorema o dominiranoj konvergenciji* i korištenja (4.11) i (4.12) dobijemo

$$\lim_{d\to 0^+} -\frac{1}{2\pi i}\int_{D+D'} f(s)\frac{x^s}{s}\,ds = -\frac{1}{\pi i}\int_{\frac{1}{2}+\delta}^{1} f(\sigma)\frac{x^{\sigma}}{\sigma}\,d\sigma$$

Radi lijepšeg zapisa stavimo da je $\frac{1}{2}+\delta = 1-L$, odnosno da je $L = \frac{1}{2}-\delta$. Immo sljedeće :

$$-\frac{1}{\pi i}\int_{\frac{1}{2}+\delta}^{1} f(\sigma)\frac{x^{\sigma}}{\sigma}\,d\sigma = -\frac{1}{\pi i}\int_{1-L}^{1} f(\sigma)\frac{x^{\sigma}}{\sigma}\,d\sigma = \begin{bmatrix}\sigma = 1-t\\ d\sigma = -\,dt\end{bmatrix} = -\frac{1}{\pi i}\int_{0}^{L} f\,(1-t)\,\frac{x^{1-t}}{1-t}\,dt$$
$$= \int_{0}^{L} g(t)x^{1-t}\,dt \tag{4.13}$$

Gdje je $g(t) = \frac{-1}{\pi i(1-t)}f\,(1-t) = \frac{i}{\pi(1-t)}f\,(1-t)$. Nakon uvrštavanja (1.9) i sređivanja imamo da je $\frac{i}{\pi(1-t)}f\,(1-t) = \frac{1}{\sqrt{t}}h(t)$ pri čemu je

$$h(t) = \frac{\left(1+13^{t-1}\right)^{\frac{1}{2}}}{\pi}\sqrt{\frac{-t\zeta(1-t)L(1-t,\chi)}{(1-t)^2\zeta(2-2t)L(2-2t,\chi)}}\prod_{(B)}\left(1+p^{2t-2}\right)^{-\frac{1}{2}}$$

Uočimo da je $h(t)$ analitička funkcija oko $t=0$ jer je $-t\zeta(1-t)$ analitička (uklonjen je singularitet u 1) te $\zeta(2)\neq 0$ i $L(2,\chi)\neq 0$. To nam omogućuje da $h(t)$ razvijemo u Taylorov red oko 0, tj. imamo da je

$$h(t) = \sum_{n=0}^{N}\frac{h^{(n)}(0)}{n!}t^n + O\left(t^{N+1}\right) \quad \text{za svaki } N\in\mathbb{N}_0 \text{ i za sve dovoljno male } t.$$

Time se račun u (4.13) svodi na računanje integrala oblika $\int_0^L t^{n-\frac{1}{2}}x^{1-t}\,dt$.

$$\int_0^L t^{n-\frac{1}{2}}x^{1-t}\,dt = x\int_0^L e^{-t\ln x}t^{n-\frac{1}{2}}\,dt = \begin{bmatrix}u = t\ln x\\ du = \ln x\,dt\end{bmatrix} =$$
$$= \frac{x}{\ln x}\int_0^{L\ln x} e^{-u}\left(\frac{u}{\ln x}\right)^{n-\frac{1}{2}}\,du = \frac{x}{(\ln x)^{n+\frac{1}{2}}}\int_0^{L\ln x} e^{-u}u^{n-\frac{1}{2}}\,du =$$
$$= \frac{x}{(\ln x)^{n+\frac{1}{2}}}\left(\int_0^{+\infty} e^{-u}u^{n-\frac{1}{2}}\,du - \int_{L\ln x}^{+\infty} e^{-u}u^{n-\frac{1}{2}}\,du\right) =$$
$$= \frac{x}{(\ln x)^{n+\frac{1}{2}}}\Gamma\left(n+\frac{1}{2}\right) - \frac{x}{(\ln x)^{n+\frac{1}{2}}}\int_{L\ln x}^{+\infty} e^{-u}u^{n-\frac{1}{2}}\,du\,.$$

Fiksirajmo neki "mali" $\gamma>0$. Kako je $u^{n-\frac{1}{2}} = e^{\left(n-\frac{1}{2}\right)\ln u}$ imamo da postoji neka konstanta $K_n>0$ (ovisna o $n$) tako da vrijedi $u^{n-\frac{1}{2}}\leq K_n e^{\gamma u}$. Stoga je

$$\int_{L\ln x}^{+\infty} e^{-u}u^{n-\frac{1}{2}}\,du \leq K_n\int_{L\ln x}^{+\infty} e^{-u(1-\gamma)}\,du = \frac{K_n}{1-\gamma}x^{-L(1-\gamma)} = O\left(x^{-L(1-\gamma)}\right)\,.$$

Iz gornjeg računa sada imamo

$$\int_0^L t^{n-\frac{1}{2}} x^{1-t}\, dt = \frac{x}{(\ln x)^{n+\frac{1}{2}}}\Gamma\left(n+\frac{1}{2}\right) + O\left(\frac{x^{1-L(1-\gamma)}}{(\ln x)^{n+\frac{1}{2}}}\right).$$

Posebno, za grešku u Taylorovom razvoju imamo

$$\int_0^L t^{N+\frac{1}{2}} x^{1-t}\, dt = O\left(\frac{x}{(\ln x)^{N+\frac{3}{2}}}\right).$$

Iz toga konačno dobijemo

$$\begin{aligned} -\frac{1}{2\pi i}\int_{D+D'} f(s)\frac{x^s}{s}\, ds &= \sum_{n=0}^{N} c_n \frac{x}{(\ln x)^{n+\frac{1}{2}}} + O\left(\frac{x^{1-L(1-\gamma)}}{(\ln x)^{\frac{1}{2}}}\right) + O\left(\frac{x}{(\ln x)^{N+\frac{3}{2}}}\right) \\ &= \frac{x}{\sqrt{\ln x}}\sum_{n=0}^{N}\frac{c_n}{(\ln x)^n} + O\left(\frac{x^{1-L(1-\gamma)}}{(\ln x)^{\frac{1}{2}}}\right) + O\left(\frac{x}{(\ln x)^{N+\frac{3}{2}}}\right) \end{aligned} \tag{4.14}$$

gdje je $c_n = \frac{h^{(n)}(0)}{n!}\cdot\Gamma\left(n+\frac{1}{2}\right)$ za svaki prirodan broj $n$.

## 4.3 Asimptotika

Uvrštavanjem (4.1), (4.6), (4.9) i (4.14) u (3.5) konačno dobijemo

$$\begin{aligned} A(x) =& \frac{x}{\sqrt{\ln x}}\sum_{n=0}^{N}\frac{c_n}{(\ln x)^n} \\ &+ O\left(\frac{x}{(\ln x)^{N+\frac{3}{2}}}\right) + O\left(\frac{x^{1-L(1-\gamma)}}{(\ln x)^{\frac{1}{2}}}\right) + O\left(\frac{x\ln x}{T}+1\right) + O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right) + O\left(T^{\varepsilon}x^{\frac{1}{2}+\delta}\right) \end{aligned}$$

Stavljanjem $T = x^{\frac{1}{2}}$ i $\delta = \frac{\varepsilon}{2}$ možemo malo pojednostaviti izraz za grečku.

$$\begin{aligned} &O\left(\frac{x\ln x}{T}+1\right) + O\left(T^{\varepsilon-1}\frac{x}{\ln x}\right) + O\left(T^{\varepsilon}x^{\frac{1}{2}+\delta}\right) = \\ &= O\left(x^{\frac{1}{2}}\ln x\right) + O\left(x^{\frac{\varepsilon}{2}+\frac{1}{2}}\cdot\frac{1}{\ln x}\right) + O\left(x^{\varepsilon+\frac{1}{2}}\right) = \\ &= O\left(x^{\varepsilon+\frac{1}{2}}\right) \end{aligned}$$

Time je

$$A(x) = \frac{x}{\sqrt{\ln x}} \sum_{n=0}^{N} \frac{c_n}{(\ln x)^n} + O\left(\frac{x}{(\ln x)^{N+\frac{3}{2}}}\right) + O\left(\frac{x^{1-L(1-\gamma)}}{(\ln x)^{\frac{1}{2}}}\right) + O\left(x^{\varepsilon+\frac{1}{2}}\right)$$

Nadalje, kako je $\varepsilon < \frac{1}{4}$ imamo da $\frac{x^{\varepsilon+\frac{1}{2}}}{x/\sqrt{\ln x}} = \frac{\sqrt{\ln x}}{x^{\frac{1}{2}-\varepsilon}} \to 0$ kada $x \to \infty$ iz čega konačno dobijemo traženu asimptotiku :

$$\lim_{x\to+\infty} \frac{A(x)}{x/\sqrt{\ln x}} = c_0 \tag{4.15}$$

Pri čemu je

$$\begin{aligned}
c_0 &= \Gamma\left(\frac{1}{2}\right) h(0) = \\
&= \sqrt{\pi} \lim_{t\to 0^+} \frac{\left(1+13^{t-1}\right)^{\frac{1}{2}}}{\pi} \sqrt{\frac{-t\zeta(1-t)L(1-t,\chi)}{(1-t)^2\zeta(2-2t)L(2-2t,\chi)}} \prod_{(B)} \left(1+p^{2t-2}\right)^{-\frac{1}{2}} = \\
&= \sqrt{\pi} \cdot \frac{\left(1+\frac{1}{13}\right)^{\frac{1}{2}}}{\pi} \left[\prod_{(B)} \left(1+\frac{1}{p^2}\right)\right]^{-\frac{1}{2}} \cdot \sqrt{\frac{L(1,\chi)}{L(2,\chi)}} \cdot \frac{\sqrt{6}}{\pi} = \\
&= \frac{2\sqrt{273}}{13} \pi^{-\frac{3}{2}} \left[\prod_{(A)} \left(1+\frac{1}{p}\right) \cdot \prod_{(B)} \left(1+\frac{1}{p}\right)^{-1}\right]^{\frac{1}{2}} = \\
&= \frac{2\sqrt{273}}{13} \pi^{-\frac{3}{2}} \prod_{p} \left(1+\frac{1}{p}\right)^{\frac{\chi(p)}{2}}
\end{aligned}$$

# Bibliografija


[1] Ivar Eriksson i Lukas Gustafsson, *On the Asymptotic Behaviour of Sums of Two Squares: Theoretical and Numerical Studies of the Counting Function B (x)*, 2018.

[2] Konrad Knopp, *Theory of functions, Parts I and II*, Courier Corporation, 2013.

[3] Hugh L Montgomery i Robert C Vaughan, *Multiplicative number theory I: Classical theory*, br. 97, Cambridge university press, 2007.

[4] M Ram Murty, *Problems in analytic number theory*, sv. 206, Springer Science & Business Media, 2008.

[5] Samuel J Patterson, *An introduction to the theory of the Riemann zeta-function*, br. 14, Cambridge University Press, 1995.

[6] Joseph H Silverman, *The arithmetic of elliptic curves*, sv. 106, Springer, 2009.

# Sažetak

U ovom radu određujemo asimptotiku kvadratno slobodnih brojeva $q \in \mathbb{Z}$ za koje je krivulja $qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ svugdje lokalno rješiva, tj. ima rješenje u $\mathbb{Q}_p$ za svaki prosti broj $p$. Postupak određivanja tražene asimptotike prati metode klasičnog rezultata o asimptotici brojeva koji se mogu prikazati kao suma dva kvadrata.

Rješenje određivanja tražene asimptotike je podijeljeno u nekoliko koraka. Prvi korak se sastoji u određivanju nužnih i dovoljnih uvjeta za $q$ za koje će promatrana krivulja biti svugdje lokalno rješiva. U drugom koraku se definira određen niz brojeva pomoću kojeg se zatim definira brojaća funkcija za tražene $q$-ove i pripadni Dirichletov red. Nakon toga se proučavaju svojsta tog Dirichletovog reda : apsolutna i uniformna konvergencija na području $\mathrm{Re}(s) \geq c > 1$, analitičko proširenje na $\mathrm{Re}(s) > \frac{1}{2}$, reziduum u $s = 1$ te gornja ograda na $\mathrm{Re}(s) = \frac{1}{2} + \delta$. U zadnjem koraku se primjenjuje *Perronova formula* te se uvodi *kontura ključanice* (*key-hole contour*) koja omogućuje ocijeniti integral dobiven u Perronovoj formuli. Iz te ocjene napokon dobijemo željenu asimptotiku.

# Summary

In this paper we study the asymptotic behaviour of the number of square-free integers $q \in \mathbb{Z}$ for which the curve $qy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$ is everywhere locally solvable, i.e. for which it has a solution in $\mathbb{Q}_p$ for every prime number $p$. The process for obtaining this asymptotic follows the methods used in the classical problem of determining the asymptotic of numbers that can be written as the sum of two squares.

The solution for obtaining the wanted asymptotic is divided in several steps. The first step consists of finding the necessary and sufficient conditions on $q$ for which the given curve is everywhere locally solvable. In the second step we define a certain sequence of numbers by which we then define the counting function for our $q$'s and a Dirichlet's series that belongs to that sequence of numbers. After that we study the properties of this Dirichlet's series : absolute and uniform convergence in region $\mathrm{Re}(s) \geq c > 1$, analytical continuation to $\mathrm{Re}(s) > \frac{1}{2}$, residue in $s = 1$ and upper bound on $\mathrm{Re}(s) = \frac{1}{2} + \delta$. In the last step we use *Perron's formula* and introduce the *key-hole contour* which helps us to assess the integral obtained from Perron's formula. From there we finally get the wanted asymptotic behaviour.

# Životopis

Rođen sam 06.05.1998. godine u Čakovcu. U razdoblju od 2005./2006. do 2012./2013. sam pohađao 1. osnovnu školu Čakovec. Tijekom osnovne škole sudjelovao sam na brojnim matematičkim natjecanjima te bio državni prvak u šestom, sedmom i osmom razredu. Svoje školovanje sam nastavio od 2013./2014.do 2016./2017. u Gimnaziji Josipa Slavenskog Čakovec, prirodoslovno-matematički smjer. Tokom srednje škole sam nastavio s natjecanjima iz Matematike. U drugom razredu sam osvojio prvo mjesto, a u prvom, trećem i četvrtom razredu sam dobio drugu nagradu na državnom natjecanju iz Matematika. Tijekom srednje škole sam također sudjelovao i na međunarodnim natjecanjima iz Matematike, odnosno na Srednje europskoj matematičkoj olimpijadi (MEMO), na Romanian Master in Mathematics (RMM) i na Međunarodnoj matematičkoj olimpijadi (IMO). U prvom razredu sam osvojio brončanu medalju pojedinačno i ekipno na MEMO-u. U drugom razredu sam prvi puta sudjelovao na RMM-u i IMO-u. U trećem razredu sam osvojio srebro u pojedinačnoj kategoriji i zlato u ekipnoj kategoriji na MEMO-u. U četvrtom razredu sam ponovo sudjelovao na RMM-u i IMO-u. Na RMM-u sam osvojio pohvalu, a na IMO-u sam osvojio srebrnu medalju. Akademske godine 2017./2018. sam upisao Prirodoslovno-matematički fakultet u Zagrebu, preddiplomski studij, matematika, inženjerski smjer. Akademske godine 2019./2020. sam završio preddiplomski studij i stekao titulu sveučilišnog prvostupnika matematike. Nakon toga akademske godine 2020./2021. sam upisao diplomski studij, matematika, smjer Teorijska matematika. Tijekom studija sam držao demonstrature iz Matematičke analize 1 i 2, Elementarne matematike 1 i 2, Diskretne matematike i Kompleksne analize te osvojio Pročelnikovu nagradu za izniman uspjeh u studiju (2020., 2022.) i Dekanovu nagradu za najboljeg studenta (2020., 2022.). Akademske godine 2021./2022. sam postao članom Povjerenstva HMD-a za međunarodna matematička natjecanja te se tako dalje aktivno bavim natjecanjima iz Matematike. Osim matematike u slobodno vrijeme volim rješavati razne zagonetke, voziti bicikl, ići u šetnje i igrati stolni tenis.