Univerzitet u Beogradu
Matematički fakultet

MASTER RAD

Rimanova hipoteza za eliptičke krive nad konačnim poljima

Student: Mladen Zekić

Mentor: dr Goran Đanković

Beograd, 2014.

„*Επ' αυτω ηλπισεν η καρδια μου, και εβοηθηθην*"
$\Psi\alpha\lambda.\ 27, 7$

Sadržaj

Uvod

Kada bih se probudio nakon sna od hiljadu godina, moje prvo pitanje bi bilo: da li je dokazana Rimanova hipoteza?

David Hilbert

Na drugom međunarodnom kongresu matematičara u Parizu 1900. godine, njemački matematičar David Hilbert održao je čuveno predavanje o najvažnijim otvorenim problemima tog vremena. Tada je predstavio 10 problema, a kompletna lista od 23 Hilbertova problema je objavljena kasnije. Sto godina kasnije, na ulasku u novi milenijum, vodeći svjetski matematičari su pod okriljem matematičkog instituta Klej izabrali sedam značajnih matematičkih problema koji do danas nisu riješeni, poznatih kao *milenijumski problemi.* Za rješenje svakog od njih pripremljena je nagrada od milion dolara.

Rimanova hipoteza se nalazi i među Hilbertovim problemima i među milenijumskim problemima matematičkog instituta Klej. Prvi put formulisana 1859. godine, i pored velikih napora ostala je neriješena do danas.

Postoje razne generalizacije i analogne formulacije Rimanove hipoteze, predložene od mnogih matematičara; između ostalih i od Dirihlea, Dedekinda, F. K. Šmita i Vejla. Slučaj Rimanove hipoteze za eliptičke krive nad konačnim poljima je originalno formulisao Artin, a dokazao njemački matematičar Helmut Hase, 1936. godine, pa se zbog toga još zove i Haseova teorema (Haseova nejednakost).

Cilj ovog rada je da predstavi dokaz Haseove teoreme. Rad je podijeljen u 4 poglavlja.

U prvom poglavlju se govori uopšte o Rimanovoj zeta-funkciji. Glavni rezultat u tom poglavlju je teorema u kojoj se izvodi funkcionalna jednačina zeta-funkcije i dokazuje da postoji meromorfno raširenje zeta-funkcije na cijelu kompleksnu ravan. Na osnovu toga kasnije se izvode neki zaključi o nulama zeta-funkcije.

Drugo poglavlje je uvodnog karaktera i u njemu su predstavljene najvažnije činjenice o eliptičkim krivama koje će biti korišćene u ostatku rada. Izbjegava se definicija eliptičke krive preko *roda*, jer bi uvođenje pojma roda zahtjevalo previše prostora, pa bi se skrenula pažnja sa glavnog cilja rada. Akcenat je stavljen na uvođenje grupnog zakona na eliptičkim krivama. Ovo poglavlje obiluje slikama koje su crtane u programskim paketima *Wolfram Mathematica 9* i *GeoGebra 4.4*. Odjeljci 2.4 i 2.5 su preglednog karaktera i služe kao dopuna prethodnog izlaganja ili motivacija za ono što slijedi.

Cilj treće glave je da se pokaže ekvivalencija između Rimanove hipoteze za eliptičke krive nad konačnim poljima i Haseove teoreme. Prvo je generalizovana Rimanova zeta-funkcija na slučaj globalnih polja, a zatim je odatle izvedena definicija zeta-funkcije pridružene krivoj nad konačnim poljem. Specijalno, izvodi se zeta-funkcija za eliptičku krivu nad konačnim poljem. Zatim se za tu krivu formuliše Rimanova hipoteza i dokazuje pomenuta ekvivalencija sa Haseovom teoremom.

U četvrtom poglavlju je izveden dokaz Haseove teoreme za eliptičke krive, baziran na radovima [2] i [3]. Time je dokazana i Rimanova hipoteza za eliptičke krive nad konačnim poljima.

Na kraju rada dat je spisak matematičara koji se pominju u radu sa nekoliko rečenica koje opisuju njihov doprinos matematici.

Zahvaljujem se mentoru docentu dr Goranu Đankoviću na predloženoj temi, na iskrenoj i strpljivoj pomoći, dugačkim mejlovima, i na prijedlozima i sugestijama kroz višestruko, pažljivo čitanje ovog rada. Takođe, zahvaljujem se profesoru dr Zoranu Petroviću na korisnim sugestijama. Na kraju, zahvaljujem se dragim prijateljima i kolegama Veliboru Bojkoviću, koji mi je davao podršku i pomagao u razumijevanju mnogih pojmova i Lazaru Vasiljeviću na tehničkoj pomoći.

Glava 1

Rimanova ζ-funkcija

1.1 Ojlerov proizvod

U svom čuvenom radu *O broju prostih brojeva manjih od zadate veličine*[1] iz 1859. godine, Riman je definisao zeta-funkciju i dokazao njene osnovne osobine.

Definicija 1.1. Kompleksnu funkciju $\zeta : \mathbb{C} \to \mathbb{C}$ definisanu za $\Re(s) > 1$ sa

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} \tag{1.1}$$

nazivamo *Rimanova zeta-funkcija.*

U ovom radu ćemo se pridržavati neobične ali široko prihvaćene konvencije da promjenljivu zeta-funkcije označavamo sa s umjesto uobičajene oznake z. Takođe, realni i imaginarni dio od s ćemo označavati sa σ i t, pa imamo

$$s = \sigma + it.$$

Ovakav način označavanja potiče od Rimana. Primjetimo da red (1.1) apsolutno konvergira za $\sigma > 1$, pa definiše holomorfnu funkciju.

U nastavku ćemo izvesti neke od osnovnih osobina zeta-funkcije. Između ostalog, dokazaćemo da funkcija definisana sa (1.1) ima meromorfno raširenje na cijelu kompleksnu ravan $\mathbb{C}$ i jedino u $s = 1$ ima prost pol. Nakon toga, zeta funkcija će biti definisana za svaki kompleksan broj $s \neq 1$. Počinjemo sa sljedećom teoremom koja se često naziva *Ojlerov proizvod za zeta-funkciju.*

Teorema 1.1. *Za Rimanovu zeta-funkciju definisanu sa* (1.1) *važi sljedeći identitet*

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}, \tag{1.2}$$

pri čemu proizvod u prethodnoj jednakosti prolazi kroz sve proste brojeve p.

[1] Über die Anzahl der Primzahlen unter einer gegebenen Grösse

Dokaz. U dokazu koristimo ideju na kojoj se zasniva *Eratostenovo sito.* Neka je

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots \tag{1.3}$$

Tada je

$$\frac{1}{2^s}\,\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \dots \tag{1.4}$$

Oduzimanjem jednakosti (1.4) od (1.3) dobijamo:

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \dots \tag{1.5}$$

Sada, množenjem prethodne jednakosti sa $1/3^s$ dobijamo

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \dots \tag{1.6}$$

Oduzimanjem (1.6) od (1.5) dobijamo

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \dots \tag{1.7}$$

Dakle, sada smo na desnoj strani osim jedinice dobili sumu brojeva n^{-s}, gdje prirodni brojevi n nisu djeljivi sa 2 i 3. Neka je $S_k(s)$ suma koja se dobije poslije k opisanih koraka, pri čemu je p_k k-ti prost broj. Dakle, $S_k(s)$ je suma brojeva oblika n^{-s}, gdje prirodni brojevi n nisu djeljivi ni sa jednim prostim brojem manjim ili jednakim od p_k, to jest

$$S_k(s) = \sum_{\substack{n\in\mathbb{N}\\ p_1,\dots,p_k \nmid n}} n^{-s}.$$

Tada je za svako $k \in \mathbb{N}$

$$|S_k(s)| \le S_k(\sigma) < T_k(\sigma),$$

gdje je

$$T_k(\sigma) = \sum_{n>p_k} n^{-\sigma}.$$

Pošto za $\sigma > 1$ važi $\lim_{k\to\infty} T_k(\sigma) = 0$, slijedi da je i $\lim_{k\to\infty} S_k(s) = 0$. Dakle, ponavljajući k puta postupak prikazan u jednakostima (1.3)-(1.7) dobijamo

$$\left(1 - \frac{1}{p_k^s}\right)\cdots\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + S_k(s).$$

Puštajući u prethodnoj jednakosti da $k \to \infty$ i imajući u vidu da je $\lim_{k\to\infty} S_k(s) = 0$ dobijamo

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

odakle slijedi jednakost (1.2). □

1.2 Puasonova sumaciona formula

U ovom odjeljku ćemo dokazati Puasonovu formulu koja će nam trebati za izvođenje funkcionalne jednačine ζ-funkcije. Međutim, prvo moramo uvesti neku terminologiju.

Definicija 1.2. Kažemo da je $f : \mathbb{R} \to \mathbb{C}$ *Švarcova funkcija* ako za svako $c \in \mathbb{R}$ i svako $n \in \mathbb{N}_0$ važi da je

$$|f^{(n)}(x)| = o(|x|^c),$$

kada $|x| \to \infty$, to jest ako je

$$\lim_{|x|\to\infty} \frac{|f^{(n)}(x)|}{|x|^c} = 0.$$

Drugim riječima, f je Švarcova funkcija ako zajedno sa svim svojim izvodima opada brže nego bilo koji stepen od $1/|x|$, kada $|x| \to \infty$.

Definicija 1.3. Neka je $f : \mathbb{R} \to \mathbb{C}$ integrabilna funkcija. Tada je njena *Furijeova transformacija* $\hat{f} : \mathbb{R} \to \mathbb{C}$ definisana sa

$$\hat{f}(y) = \int_{-\infty}^{+\infty} e^{-2\pi i x y} f(x)\,\mathrm{d}x.$$

Formulišimo sada i dokažimo Puasonovu sumacionu formulu.

Teorema 1.2. *Neka je $f : \mathbb{R} \to \mathbb{C}$ Švarcova funkcija i neka je $\hat{f}$ njena Furijeova transformacija. Tada važi*

$$\sum_{m=-\infty}^{\infty} f(m) = \sum_{n=-\infty}^{\infty} \hat{f}(n). \tag{1.8}$$

Dokaz. U dokazu koristimo razvoj funkcije u Furijeov red. Neka je

$$F(x) = \sum_{m=-\infty}^{\infty} f(x+m).$$

Tada je funkcija $F(x)$ 1-periodična i možemo je razviti u Furijeov red. Koristeći kompleksni oblik Furijeovog reda dobijamo

$$F(x) = \sum_{k=-\infty}^{\infty} c_k\, e^{2k\pi i x},$$

gdje su Furijeovi koeficijenti dati sa

$$c_k = \int_0^1 \sum_{m=-\infty}^{\infty} f(x+m)\, e^{-2k\pi i x}\,\mathrm{d}x.$$

Pošto je f Švarcova funkcija i pošto važi $|e^{-2k\pi ix}| \leq 1$, red $\sum_{m=-\infty}^{\infty} f(x+m)\, e^{-2k\pi ix}$ ravnomjerno konvergira na osnovu Vajerštrasovog kriterijuma, pa ga možemo integraliti član po član. Dakle, imamo

$$\begin{aligned} c_k &= \sum_{m=-\infty}^{\infty} \int_0^1 f(x+m)\, e^{-2k\pi ix}\, \mathrm{d}x \\ &= \sum_{m=-\infty}^{\infty} \int_m^{m+1} f(x)\, e^{-2k\pi ix}\, \mathrm{d}x \\ &= \int_{-\infty}^{+\infty} f(x)\, e^{-2k\pi ix}\, \mathrm{d}x \\ &= \hat{f}(k). \end{aligned}$$

Iz prethodnog slijedi da je

$$F(x) = \sum_{k=-\infty}^{\infty} \hat{f}(k)\, e^{2k\pi ix}.$$

Uzimajući u prethodnoj jednakosti $x = 0$, dobijamo

$$\sum_{m=-\infty}^{\infty} f(m) = \sum_{n=-\infty}^{\infty} \hat{f}(n),$$

što je i trebalo dokazati. □

1.3 Jakobijev transformacioni identitet

U ovom odjeljku ćemo korišćenjem Puasonove sumacione formule izvesti *Jakobijev transformacioni identitet*, koji će imati ključnu ulogu u izvođenju funkcionalne jednačine zeta-funkcije. Definišimo prvo Jakobijevu teta-funkciju.

Definicija 1.4. Funkciju $\theta : \mathbb{C} \to \mathbb{C}$ definisanu sa

$$\theta(u) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 u} = 1 + 2(e^{-\pi u} + e^{-4\pi u} + e^{-9\pi u} + \cdots) \tag{1.9}$$

nazivamo *Jakobijeva teta-funkcija*.

Primjetimo da red $\sum_{n=-\infty}^{\infty} e^{-\pi n^2 u}$ apsolutno konvergira za sve kompleksne brojeve u za koje je $\Re(u) > 0$, te u desnoj poluravni definiše holomorfnu funkciju.

Napomena. Jakobi je u stvari definisao četiri teta-funkcije dvije promjenljive. Funkcija $\theta(u)$ koju ćemo koristiti je zapravo $\theta_3(0, e^{-\pi u})$. Ali, možemo je zvati $\theta(u)$ pošto nećemo koristiti $\theta_1, \theta_2, \theta_4$ ni $\theta_3(z, q)$ za $z \neq 0$.

Dokažimo sada pomenuti Jakobijev identitet za teta-funkciju.

Teorema 1.3. *Neka je $\theta(u)$ teta-funkcija definisana u* (1.9)*. Tada važi sljedeći identitet*

$$\theta(1/u) = u^{1/2}\theta(u). \tag{1.10}$$

Dokaz. Ova teorema je zapravo specijalni slučaj Puasonove sumacione formule za funkciju $f(x) = e^{-\pi u x^2}$. Lako se provjeri da $f(x)$ jeste Švarcova funkcija, pa jednakost (1.8) važi. Lijeva strana jednakosti (1.8) je samo $\theta(u)$. Da bismo dobili desnu stranu, treba da nađemo Furijeovu transformaciju od f. To se svodi na izračunavanje integrala

$$\hat{f}(y) = \int_{-\infty}^{+\infty} e^{-2\pi i x y - \pi u x^2}\,\mathrm{d}x.$$

On se rješava svođenjem na poznati Gausov integral, kada ga napišemo u obliku

$$\hat{f}(y) = \int_{-\infty}^{+\infty} e^{-\pi y^2/u - ((\pi u)^{1/2}x + (\pi/u)^{1/2} i y)^2}\,\mathrm{d}x,$$

i uvedemo smjenu $(\pi u)^{1/2}x + (\pi/u)^{1/2} i y = t$. Nakon kraćeg računa dobijamo da je

$$\hat{f}(y) = u^{-1/2} e^{-\pi y^2/u}.$$

Dakle, desna strana jednakosti (1.8) je $u^{-1/2}\theta(1/u)$, pa imamo

$$\theta(u) = u^{-1/2}\theta(1/u),$$

odakle se množenjem sa $u^{1/2}$ dobija jednakost (1.10). □

1.4 Funkcionalne jednačine

Prije nego što formulišemo teoremu o funkcionalnoj jednačini zeta-funkcije, podsjetićemo se definicije gama-funkcije.

Definicija 1.5. Gama-funkcija $\Gamma : \mathbb{C} \to \mathbb{C}$ ili *Ojlerov integral druge vrste* je za $\Re(s) > 0$ definisana sa

$$\Gamma(s) = \int_0^{\infty} x^s e^{-x} \frac{\mathrm{d}x}{x},$$

a za ostale vrijednosti $s \neq 0, -1, -2, \ldots$ funkcionalnom jednačinom

$$\Gamma(s+1) = s\,\Gamma(s).$$

Napomenimo da je gama-funkcija meromorfna na $\mathbb{C}$ i da je holomorfna svuda osim u $s = -n$, za cijele brojeve $n \geq 0$, gdje ima proste polove.

Teorema 1.4 (Riman, 1859)**.** *Zeta-funkcija $\zeta(s)$ ima meromorfno raširenje na cijelu kompleksnu ravan $\mathbb{C}$. Holomorfna je svuda osim u $s = 1$ gdje ima prost pol, i za $s \neq 1$ zadovoljava funkcionalnu jednačinu*

$$\pi^{-s/2}\,\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\,\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s). \tag{1.11}$$

Dokaz. Uvedimo funkciju $\xi(s) = \pi^{-s/2}\,\Gamma(s/2)\,\zeta(s)$. Integracijom član po član, dobijamo da za $\Re(s) > 1$ važi

$$2\xi(s) = \int_0^\infty (\theta(u) - 1)\, u^{s/2}\, \frac{\mathrm{d}u}{u}.$$

Napišimo prethodni integral za $2\xi(s)$ u obliku

$$\begin{aligned} 2\xi(s) &= \int_0^1 (\theta(u) - 1)\, u^{s/2}\, \frac{\mathrm{d}u}{u} + \int_1^\infty (\theta(u) - 1)\, u^{s/2}\, \frac{\mathrm{d}u}{u} \\ &= -\frac{2}{s} + \int_0^1 \theta(u)\, u^{s/2}\, \frac{\mathrm{d}u}{u} + \int_1^\infty (\theta(u) - 1)\, u^{s/2}\, \frac{\mathrm{d}u}{u}. \end{aligned} \tag{1.12}$$

Nakon smjene promjenljive $u \to 1/u$ i koristeći Jakobijev transformacioni identitet (1.10) dobijamo

$$\begin{aligned} \int_0^1 \theta(u)\, u^{s/2}\, \frac{\mathrm{d}u}{u} &= \int_1^\infty \theta(1/u)\, u^{-s/2}\, \frac{\mathrm{d}u}{u} \\ &= \int_1^\infty \theta(u)\, u^{(1-s)/2}\, \frac{\mathrm{d}u}{u} \\ &= \frac{2}{s-1} + \int_1^\infty (\theta(u) - 1)\, u^{(1-s)/2}\, \frac{\mathrm{d}u}{u}. \end{aligned} \tag{1.13}$$

Iz jednakosti (1.12) i (1.13) slijedi

$$\xi(s) = \frac{1}{2}\int_1^\infty (\theta(u) - 1)\,(u^{s/2} + u^{(1-s)/2})\, \frac{\mathrm{d}u}{u} - \frac{1}{s} - \frac{1}{1-s}. \tag{1.14}$$

Podsjetimo se da smo prethodnu jednakost izveli pod uslovom $\Re(s) > 1$. Međutim, integral u formuli (1.14) konvergira za sve vrijednosti $s \in \mathbb{C}$ jer $\theta(u)$ eksponencijalno opada kada $u \to \infty$, pa pomenuti integral definiše cijelu funkciju po s. Dakle, desna strana jednakosti (1.14) definiše meromorfno raširenje funkcije $\xi(s)$ na cijeli skup $\mathbb{C}$, te je funkcija $\xi(s)$ holomorfna svuda osim u $s = 0$ i $s = 1$, pošto su ove vrijednosti singulariteti izraza na desnoj strani. Međutim $s = 0$ je otklonjivi singularitet zeta-funkcije, jer kada izrazimo $\zeta(s)$ iz jednakosti (1.14), jedini „problematični" član je

$$\frac{1}{s\,\Gamma(s/2)} = \frac{1}{2 \cdot s/2\,\Gamma(s/2)} = \frac{1}{2\Gamma(s/2+1)},$$

što teži $1/2$ kada s teži 0. Pošto je desna strana od (1.14) simetrična pri smjeni $s \to 1-s$, slijedi da važi funkcionalna jednačina (1.11). □

Primjedba. Primjetimo da koristeći funkciju $\xi(s)$ iz prethodnog dokaza funkcionalnu jednačinu (1.11) možemo jednostavnije zapisati na sljedeći način

$$\xi(s) = \xi(1-s).$$

Zahvaljujući prethodnoj teoremi, sada možemo dati sljedeću, širu definiciju zeta-funkcije, gdje je $\zeta(s)$ definisana za sve kompleksne brojeve $s \neq 1$.

Definicija 1.6. Kompleksnu funkciju $\zeta : \mathbb{C} \to \mathbb{C}$ definisanu za $\Re(s) > 1$ sa

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

a za ostale vrijednosti $s \neq 1$ funkcionalnom jednačinom (1.11) nazivamo *Rimanova zeta-funkcija.*

Navedimo sada i jednu jednostavnu posljedicu prethodne teoreme.

Posljedica 1.1. *Neka je zeta-funkcija $\zeta(s)$ definisana funkcionalnom jednačinom* (1.11)*. Tada važi*

$$\zeta(0) = -\frac{1}{2}.$$

Dokaz. Pošto za $s \neq 0, -2, -4, \ldots$ važi

$$\Gamma(s/2) = \frac{s/2\,\Gamma(s/2)}{s/2} = \frac{\Gamma(s/2+1)}{s/2}$$

slijedi $\Gamma(s/2) \sim (s/2)^{-1}$ kada $s \to 0$, pa množenjem jednakosti (1.14) sa $s/2$ i uzimanjem da $s \to 0$ dobijamo rezultat. □

U sljedećoj teoremi ćemo izvesti još dvije funkcionalne jednačine zeta-funkcije, iz kojih ćemo lakše moći da odredimo njene nule.

Teorema 1.5. *Neka je funkcija $\zeta(s)$ definisana funkcionalnom jednačinom* (1.11)*. Tada $\zeta(s)$ zadovoljava i sljedeću funkcionalnu jednačinu*

$$\zeta(s) = 2^s\,\pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\,\zeta(1-s), \tag{1.15}$$

ili ekvivalentno

$$\zeta(1-s) = 2^{1-s}\,\pi^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s)\,\zeta(s). \tag{1.16}$$

Dokaz. U dokazu koristimo sljedeće dvije osobine gama-funkcije, za $z \neq 0, -1, -2, \ldots$ (za izvođenje formula vidjeti [1])

$$\Gamma(1-z)\Gamma(z) = \frac{\pi}{\sin(\pi z)} \tag{1.17}$$

$$\Gamma(z)\Gamma\left(z+\frac{1}{2}\right) = 2^{1-2z}\sqrt{\pi}\,\Gamma(2z). \tag{1.18}$$

Kada pomnožimo jednačinu (1.11) sa $\Gamma(1-s/2)$, korišćenjem identiteta (1.17) na lijevoj strani ćemo imati član

$$\Gamma\left(\frac{s}{2}\right)\Gamma\left(1-\frac{s}{2}\right) = \frac{\pi}{\sin(\pi s/2)},$$

a korišćenjem identiteta (1.18) na desnoj strani ćemo imati član

$$\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right) = \Gamma\left(\frac{1-s}{2}\right)\Gamma\left(\frac{1-s}{2}+\frac{1}{2}\right) = 2^s\sqrt{\pi}\Gamma(1-s).$$

Iz prethodnog lako dobijamo jednačinu (1.15). Jednačina (1.16) se dobija iz (1.15) kada s zamjenimo sa $1-s$. □

1.5 Nule zeta-funkcije

Teorema 1.6. *Zeta-funkcija $\zeta(s)$ definisana funkcionalnom jednačinom* (1.11) *ima nule u negativnim parnim cijelim brojevima $-2, -4, -6, \ldots$ i nema drugih nula izvan oblasti $D = \{s \in \mathbb{C} \mid 0 \leq \Re(s) \leq 1\}$.*

Dokaz. Iz funkcionalne jednačine (1.15) slijedi da je za $s = -2, -4, -6, \ldots$ gama-funkcija dobro definisana, dok je izraz $\sin(\pi s/2)$ jednak nuli, pa je i $\zeta(s)$ jednaka nuli za ove vrijednosti. Takođe, iz Ojlerovog proizvoda (1.2) slijedi da $\zeta(s)$ nema nula u poluravni $\Re(s) > 1$, jer konvergentni beskonačni proizvod može biti jednak nuli samo ako je neki od njegovih faktora jednak nuli. Pretpostavimo sada da je $\zeta(s) = 0$ i da je $\Re(s) < 0$. Tada je $1 - \Re(s) > 1$, pa je $\zeta(1 - s) \neq 0$. Sada iz jednačine (1.15) slijedi da mora biti

$$\Gamma(1 - s) \sin\left(\frac{\pi s}{2}\right) = 0.$$

Međutim, kako gama-funkcija nema nula, zaključujemo da je prethodna jednakost moguća jedino za $s = -2n,\ n \in \mathbb{N}$, što su upravo pomenute nule u negativnim parnim cijelim brojevima. Dakle, $\zeta(s)$ nema drugih nula izvan oblasti D. □

Definicija 1.7. Nule $s = -2n,\ n \in \mathbb{N}$ od $\zeta(s)$ nazivamo *trivijalne nule* Rimanove zeta-funkcije. Oblast $D = \{s \in \mathbb{C} \mid 0 \leq \sigma \leq 1\}$ u kojoj se nalaze sve netrivijalne nule zeta-funkcije naziva se *kritična traka.*

Primjetimo da ako je ρ neka netrivijalna nula zeta-funkcije, da je i $1 - \rho$ takođe njena nula. To znači da su netrivijalne nule zeta-funkcije simetrične u odnosu na pravu $\Re(s) = 1/2$, koja se naziva *kritična linija* zeta-funkcije. U pomenutom radu *O broju prostih brojeva manjih od zadate veličine*, Riman je dao sljedeću hipotezu o netrivijalnim nulama-zeta funkcije.

Rimanova hipoteza. *Sve netrivijalne nule zeta-funkcije $\zeta(s)$ imaju realni dio jednak* $1/2$, *tj. nalaze se na pravoj $\Re(s) = 1/2$.*

Ova hipoteza do danas nije dokazana i po mišljenju mnogih matematičara predstavlja najvažniji otvoreni problem matematike.

Glava 2

Eliptičke krive

2.1 Vajerštrasove jednačine

U ovoj glavi, k će nam uvijek označavati proizvoljno polje. Da bismo stigli do definicije eliptičke krive, prvo ćemo definisati Vajerštrasovu kubnu krivu (kubiku).

Definicija 2.1. *Vajerštrasova kubika* je par (E, O) gdje je E skup tačaka u projektivnoj ravni $\mathbb{P}_2(k)$ čije koordinate predstavljaju rješenja jednačine

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (a_1, \ldots, a_6 \in k), \tag{2.1}$$

a $O \in E$ je *bazna tačka* koja ima koordinate $O = [0 : 1 : 0]$. Jednačinu (2.1) nazivamo *Vajerštrasov opšti oblik* kubne krive.

Napomena. Jednačina (2.1) je *projektivna* Vajerštrasova jednačina. Kubna kriva takođe može biti definisana i *afinom jednačinom* uvođenjem *ne-homogenih koordinata*

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}.$$

U tom slučaju jednačina (2.1) glasi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, \ldots, a_6 \in k), \tag{2.2}$$

a bazna tačka postaje *beskonačno daleka tačka* koju ne možemo vidjeti u afinoj ravni, ali za koju ćemo smatrati da se nalazi na svakoj vertikalnoj pravoj $x = c,\ c \in k$. Jednačinu (2.2) ćemo takođe nazivati Vajerštrasov opšti oblik kubike. Kasnije će biti razjašnjeno zašto su koeficijenti označeni na ovaj način.

Takođe, može se dokazati da se svaka kubna kriva može svesti na jednačinu (2.1) „dobrim" izborom osa u projektivnoj ravni i projektivnim transformacijama (za izvođenje pogledati [12] i [11].)

Za uvođenje grupnog zakona na eliptičkoj krivoj (što će biti razmatrano u sljedećem odjeljku) biće nam potrebno da svaka prava siječe Vajerštrasovu kubiku u 3 tačke (računajući višestrukosti). Kada posmatramo Vajerštrasovu kubiku u projektivnoj ravni, taj

uslov je ispunjen. Međutim, u afinoj jednačini (2.2) primjećujemo da, pošto nema člana y^3, svaka vertikalna prava $x = c$ siječe krivu E u dvije tačke. Ali, ako se uzme u obzir da beskonačno daleka tačka O takođe pripada krivoj E, tada dobijamo i treću presječnu tačku.

U slučaju kada za polje k važe određeni dodatni uslovi, jednačina (2.2) može biti još pojednostavljena, o čemu govori sljedeći stav.

Stav 2.1. *Neka je kubna kriva E definisana jednačinom* (2.2) *nad poljem k čija je karakteristika različita od 2 i 3. Tada jednačina* (2.2) *može da se svede na sljedeći oblik*

$$y^2 = x^3 + ax + b. \tag{2.3}$$

Dokaz. Pošto je karakteristika polja k različita od 2, možemo kompletirati kvadrat na desnoj strani jednakosti (2.2). Smjenom

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

dobijamo jednačinu

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdje je

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

Sada se vidi zašto su koeficijenti u krivoj (2.2) tako označeni. Naime, indeksi su izabrani tako da sve prethodne formule budu „homogene" u indeksu. Dalje, pošto je karakteristika polja k različita i od 3, smjenom

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

eliminišemo član x^2, tako da dobijamo traženu jednačinu

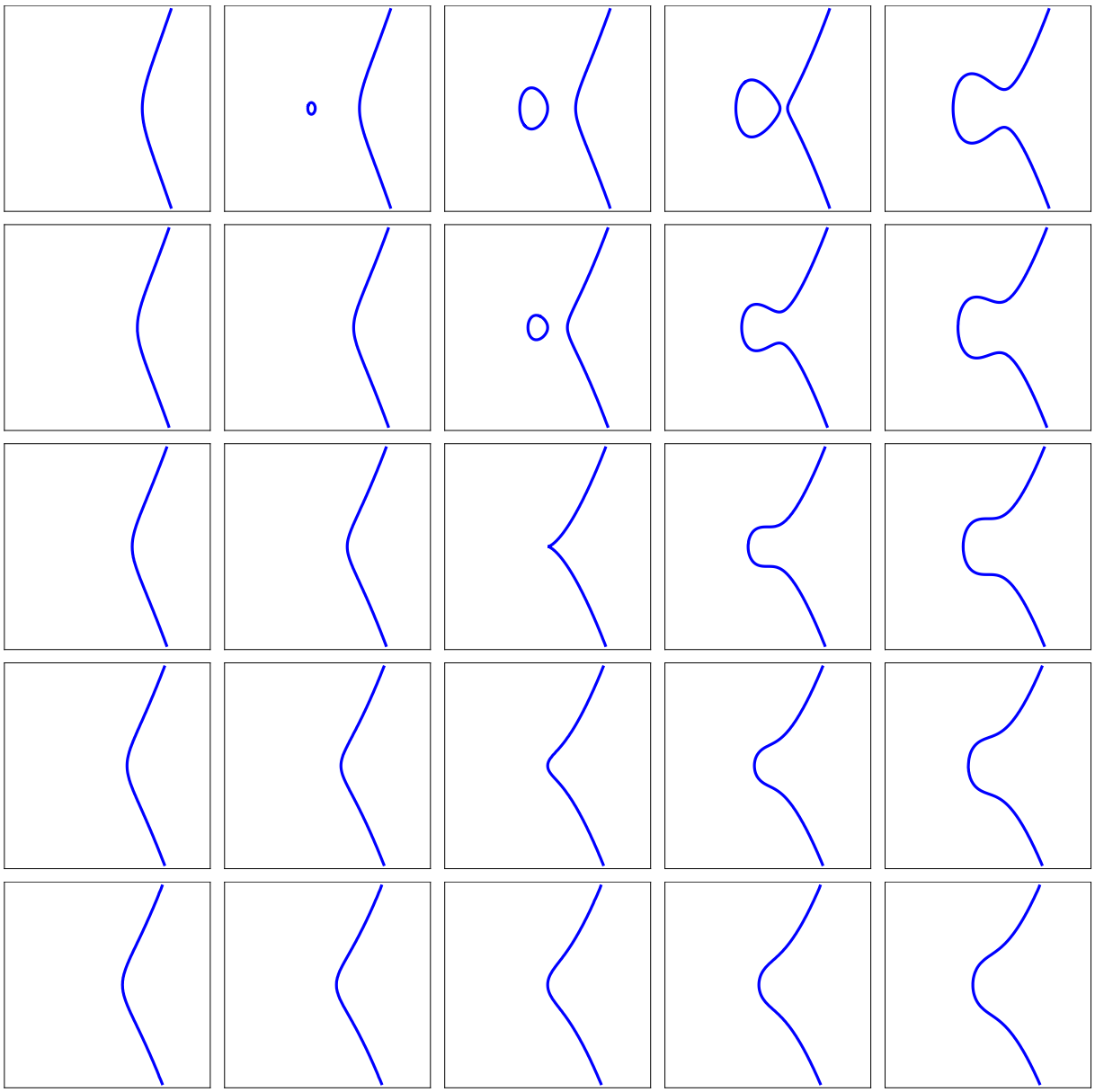
$$y^2 = x^3 + ax + b,$$

gdje je

$$a = -27(b_2^2 - 24b_4), \quad b = 54(b_2^3 - 36b_2b_4 + 216b_6). \qquad \square$$

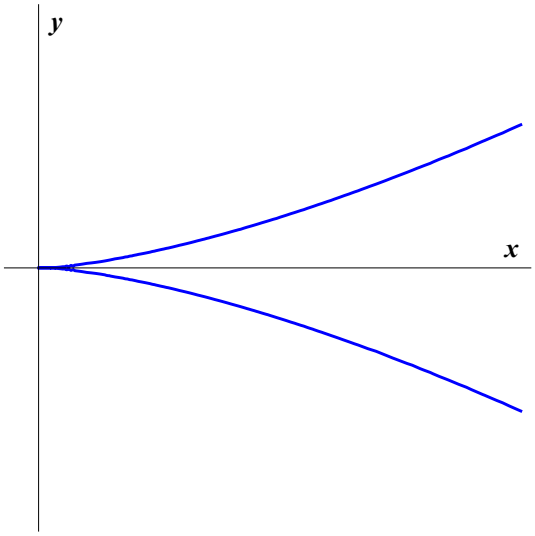
Definicija 2.2. Jednačinu (2.3) nazivamo *Vajerštrasov normalni oblik* kubne krive.

Uglavnom, nad većinom polja, nije moguće dati smislenu sliku Vajerštrasove kubike. Međutim, korisno je razmotriti grafike Vajerštrasovih krivih nad realnim brojevima. Na slici 2.1 prikazani su neki grafici Vajerštrasovih kubika u normalnom obliku.

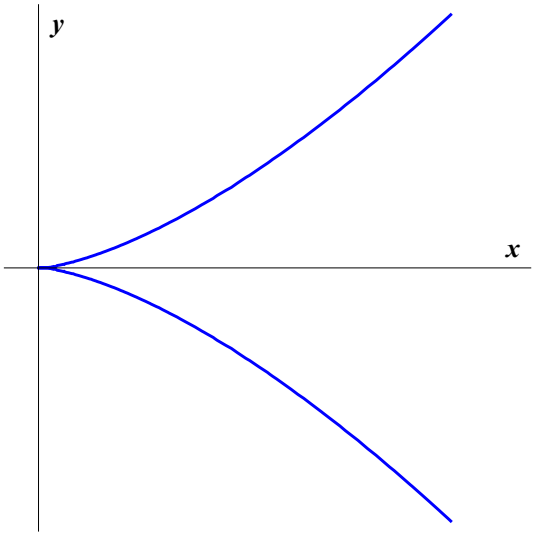


Slika 2.1: Krive oblika $y^2 = x^3 + ax + b$. Koeficijent $a \in \mathbb{Z}$ ide od -2 do 2 odozgo na dole i konstantan je po vrstama, a koeficijent $b \in \mathbb{Z}$ ide od -2 do 2 slijeva na desno i konstantan je po kolonama.

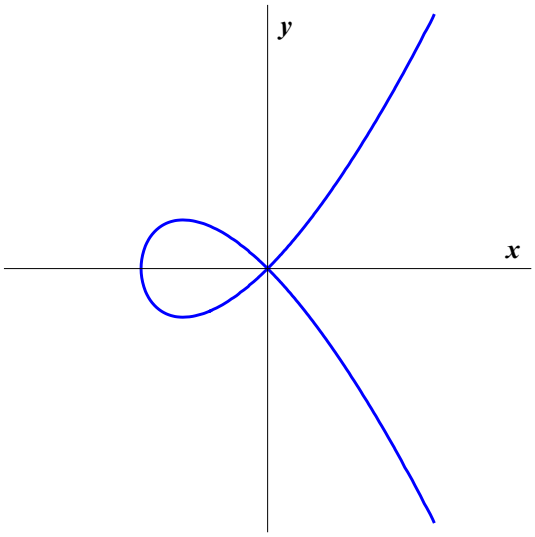
U slučaju Vajerštrasovih kubika nad $\mathbb{R}$ možemo „intuitivno" opisati pojam „glatkosti" krive. Naime, kriva je *glatka* ili *ne-singularna* ako ima definisanu tangentu u svakoj tački. U suprotnom, kriva je *singularna.* Postoje dva moguća oblika realne singularne kubike, koja zavise od toga da li polinom $x^3 + ax + b$ ima dvostruki ili trostruki realni korijen. U slučaju kada realna kubika ima trostruki realni korijen, ona ima singularitet koji nazivamo *špic.* Ovaj tip singulariteta je prikazan na slikama 2.2 i 2.3. Kada realna kubika ima dvostruki realni korijen, taj tip singulariteta nazivamo *čvor* ili *tačka samopresjeka.* On je prikazan na slkama 2.4 i 2.5.



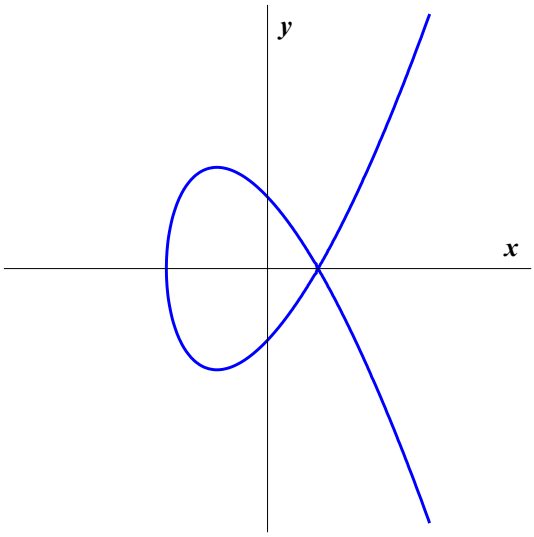
Slika 2.2: Singularna kriva $y^2 = x^3$



Slika 2.3: Singularna kriva $y^2 = 5x^3$



Slika 2.4: Singularna kriva $y^2 = x^3 + x^2$



Slika 2.5: Singularna kriva $y^2 = x^3 - 3x + 2$

Definišimo sada jednu važnu veličinu koju pridružujemo kubnoj krivoj u Vajerštrasovom normalnom obliku.

Definicija 2.3. Neka je kubna kriva zadata jednačinom (2.2) u Vajrštrasovom normalnom obliku. Veličinu

$$\Delta = -16(4a^3 + 27b^2)$$

nazivamo *diskriminanta* Vajerštrasove kubike E.

Iako se faktor -16 čini nebitan u prethodnoj definiciji, ispostavlja se da je zgodan u naprednijem proučavanju eliptičkih krivih. Pomoću diskriminante možemo dati kriterijum kada je kriva ne-singularna, a kada ima koji tip singulariteta.

Teorema 2.1. *Neka je kubna kriva E definisana jednačinom* (2.3) *u Vajerštrasovom normalnom obliku. Tada važi*

(1) Kriva E je ne-singularna ako i samo ako je $\Delta \neq O$.

(2) Kriva E ima čvor ako i samo ako je $\Delta = 0$, i $a \neq 0$.

(3) Kriva E ima špic ako i samo ako je $\Delta = a = 0$.

Dokaz. Napišimo jednačinu (2.3) u obliku $F(x, y) = y^2 - f(x)$, gdje je $f(x) = ax^3 + bx + c$. Tada važi

$$\frac{\partial F}{\partial x} = -f'(x), \qquad \frac{\partial F}{\partial y} = 2y. \tag{2.4}$$

Kriva je ne-singularna ako ne postoji nijedna tačka na krivoj u kojoj su parcijalni izvodi (2.4) istovremeno jednaki nuli. To znači da u svakoj tački na krivoj postoji dobro definisana tangenta. Pretpostavimo sada da su parcijalni izvodi (2.4) istovremeno jednaki nuli u tački (x_0, y_0). Tada mora biti $y_0 = 0$, odakle slijedi i $f(x_0) = 0$. Dakle, $f(x)$ i $f'(x)$ imaju zajednički korijen x_0. To znači da je x_0 dvostruki korijen od $f(x)$, odakle slijedi da je $4a^3 + 27b^2 = 0$, pa je i $\Delta = 0$. Obrnuto, ako je $\Delta = 0$, tada $f(x)$ ima višestruki korijen x_0, odakle slijedi da je $(x_0, 0)$ singularna tačka krive (2.3). Ovime je tvrđenje (1) dokazano. Dokaz tvrđenja (2) i (3) nećemo izvoditi pošto nam neće trebati u ostatku rada, a zainteresovanog čitaoca upućujemo na [11], Stav 1.4. □

Sada napokon možemo definisati eliptičku krivu kao *glatku Vajerštrasovu kubiku.* Iako je eliptička kriva *projektivna kriva*, mi ćemo je definisati *afinom jednačinom*, jer će nam ta definicija biti pogodnija u ostatku rada. Takođe, pošto ćemo u nastavku razmatrati samo polja čija je karakteristika različita od 2 i 3, koristićemo Vajerštrasovu jednačinu kubike u normalnom obliku.

Definicija 2.4. Eliptička kriva (E, O) nad poljem k karakteristike različite od 2 i 3 je Vajerštrasova kubika zadata afinom jednačinom

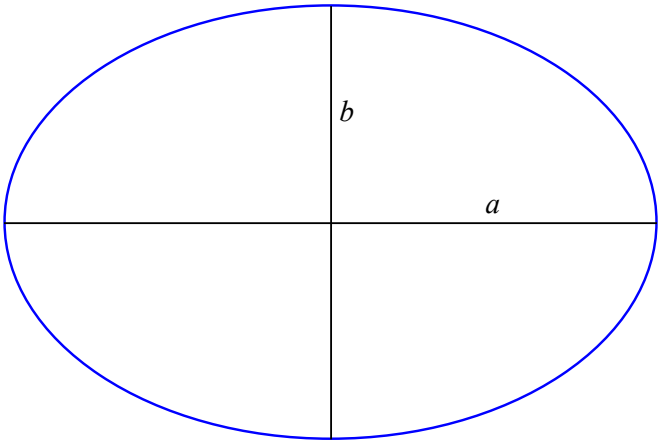
$$y^2 = x^3 + ax + b, \quad (a, b \in k), \tag{2.5}$$

pri čemu je $O \in E$ beskonačno daleka tačka i važi da je diskriminanta $\Delta \neq 0$.

Često ćemo umjesto (E, O) pisati samo E, kada je jasno koju tačku O smo izabrali.

Sada možemo dati i objašnjenje odakle potiče naziv „eliptička kriva." Istorijski, pojam „eliptička kriva" je nastao od pojma „eliptički integral", koji se pojavljuje u problemu izračunavanja obima elipse. Iz početnih kurseva analize je poznata formula za izračunavanje dužine luka krive: ako je $y = f(x)$ neprekidna funkcija koja ima neprekidan izvod na segmentu $[a, b]$, tada je dužina L_a^b krive data sa

$$L_a^b = \int_a^b \sqrt{1 + (f'(x))^2}\, \mathrm{d}x.$$



Slika 2.6: Elipsa $x^2/9 + y^2/4 = 1$

Iskoristimo ovu formulu za nalaženje dužine luka elipse između, recimo x_0 i x_1. Neka su a i b pozitivni brojevi, pri čemu je $a > b$. Razmotrimo elipsu

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

čije su poluose a i b (slika 2.6). Kada riješimo ovu jednačinu po y i uzmemo pozitivan kvadratni korijen, dobijamo funkciju

$$y = f(x) = \frac{b}{a}\sqrt{a^2 - x^2}.$$

Zatim, kada izračunamo $\sqrt{1 + (f'(x))^2}$ i stavimo $k = \sqrt{b^2 - a^2}/a$, formula za dužinu luka postaje

$$L_{x_0}^{x_1} = \int_{x_0}^{x_1} \frac{a^2 - k^2x^2}{\sqrt{(a^2 - x^2)(a^2 - k^2x^2)}}\,\mathrm{d}x,$$

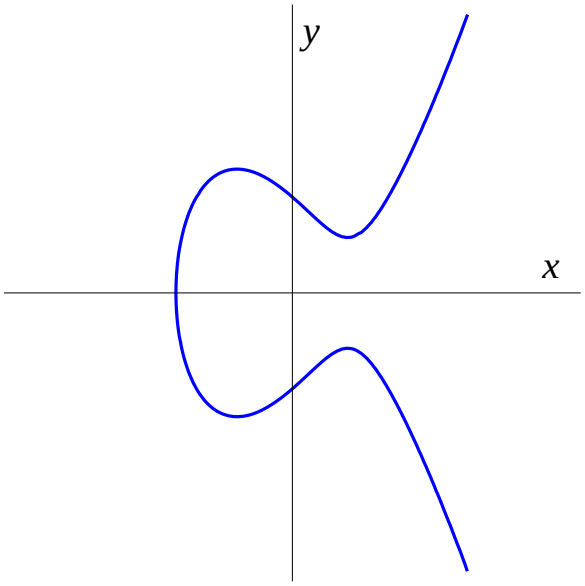
odakle se dobija da je obim elipse dat sa

$$L = \int_0^a \frac{a^2 - k^2x^2}{\sqrt{(a^2 - x^2)(a^2 - k^2x^2)}}\,\mathrm{d}x.$$

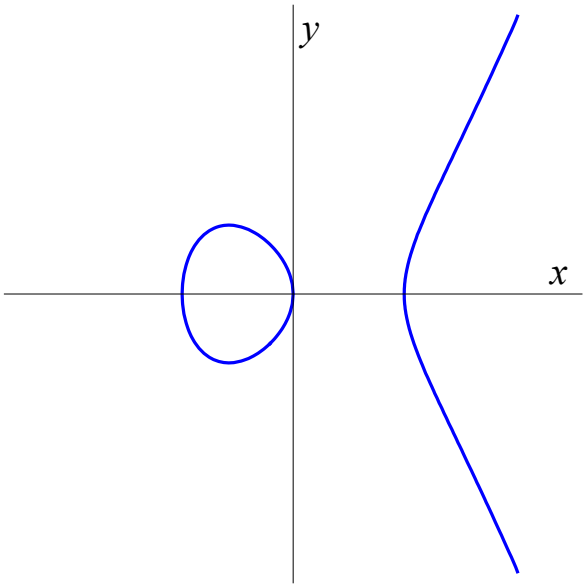
Prethodni integral se naziva *eliptički integral druge vrste.*

Danas se pod eliptičkim integralima podrazumijevaju uopšte integrali racionalnih funkcija koje u sebi sadrže kvadratne korijene polinoma trećeg ili četvrtog stepena. Dakle, integral funkcije $y = \sqrt{x^3 + ax + b}$ je eliptički integral pa odatle potiče naziv „eliptička kriva" za implicitno zadatu funkciju $y^2 = x^3 + ax + b$. Za detaljniji uvid u istorijski razvoj pojma „eliptička kriva" pogledati rad [10].

Razmotrimo sada grafike eliptičkih krivih nad $\mathbb{R}$. Oni mogu imati dva osnovna oblika, prikazana na slikama 2.7 i 2.8.



Slika 2.7: Eliptička kriva $y^2 = x^3 - 3x + 3$



Slika 2.8: Eliptička kriva $y^2 = x^3 - x$

Ako polinom x^3+ax+b ima jedan realan korijen, tada se grafik eliptičke krive sastoji od jedne komponente (slika 2.7), a ako ima tri različita realna korijena, njen grafik se sastoji od dvije komponente (slika 2.8). Međutim, poznato je da kubni polinom $x^3 + ax + b$ ima jedan realan korijen kada je $4a^3 + 27b^2 > 0$, a tri različita realna korijena kada je $4a^3 + 27b^2 < 0$. Odavde slijedi da eliptička kriva nad $\mathbb{R}$ ima jednu komponentu ako je $D < 0$, a dvije ako je $D > 0$. U ovo se možemo uvjeriti i na primjerima eliptičkih krivih prikazanih na slikama 2.7 i 2.8. Diskriminanta krive $y^2 = x^3 - 3x + 3$ je $\Delta = -2160$, dok za krivu $y^2 = x^3 - x$ važi da je $\Delta = 64$.

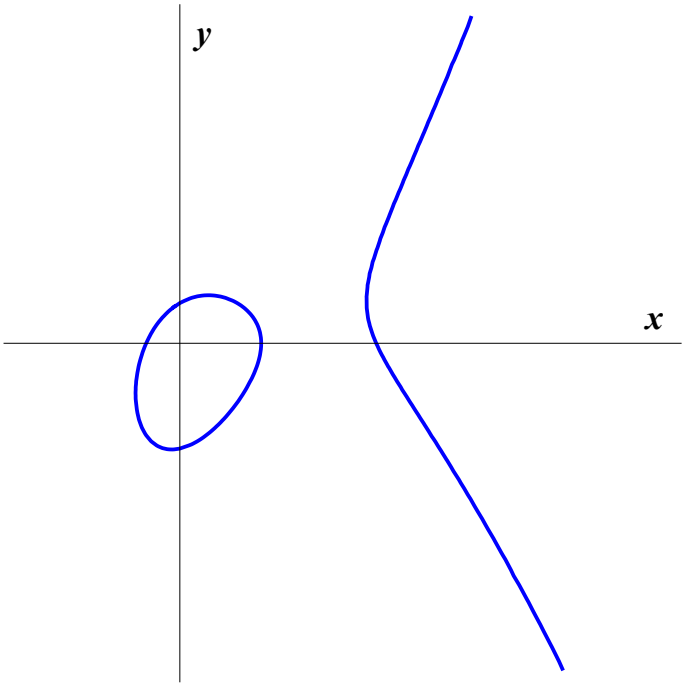
Takođe, napomenimo da su sve krive na slici 2.1 zapravo eliptičke krive, osim kubike u centru (slučaj $a = b = 0$), jer jedino ta kriva nije glatka, pa zato nije eliptička kriva.

I na kraju ovog odjeljka, navedimo primjer jedne krive u Vajerštrasovom opštem obliku (slika 2.9). Primjetimo da ona nije simetrična u odnosu na x-osu kao krive na prethodnim slikama.

2.2 Grupni zakon na eliptičkoj krivoj

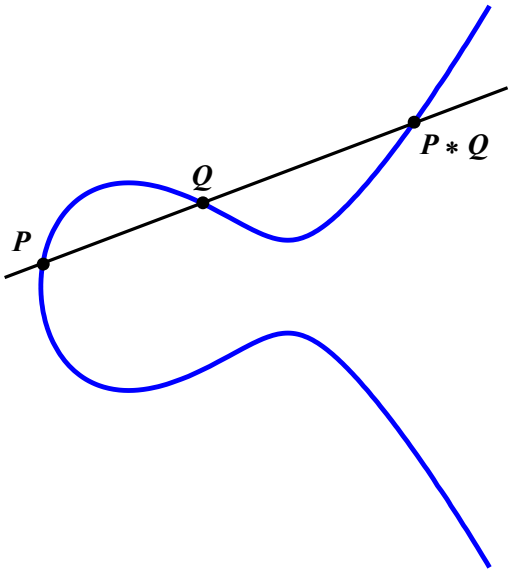
U ovom odjeljku ćemo uvesti grupni zakon na eliptičkoj krivoj. Da bismo to uradili, posmatraćemo eliptičke krive u projektivnoj ravni $\mathbb{P}_2(k)$. Kao što je već rečeno u prethodnom odjeljku, svaka prava siječe eliptičku krivu u tačno 3 tačke, računajući višestrukosti.

Ako imamo dvije različite tačke P i Q na eliptičkoj krivoj, tada možemo povući pravu p kroz P i Q i na taj način dobiti treću presječnu tačku na eliptičkoj krivoj koju označavamo sa $P*Q$. Naravno, ako je p tangenta na krivu E, tada P, Q i $P*Q$ ne moraju biti različite. Preciznije, imamo sljedeću definiciju.

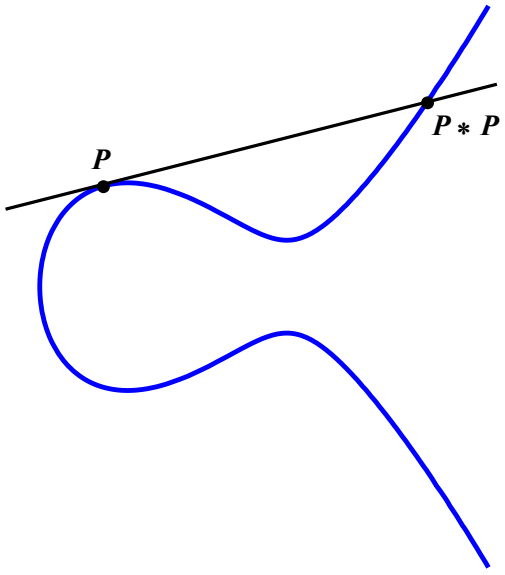


Slika 2.9: Eliptička kriva $y^2 - xy + y = x^3 - 3x^2 + x + 1$

Definicija 2.5. Neka su P i Q različite tačke na eliptičkoj krivoj E i naka je p prava određena tim tačkama. Neka je $P * Q$ treća presječna tačka prave p i krive E, ne nužno različita od P i Q. Tačku $P * Q$ nazivamo *kompozicijom* tačaka P i Q (slika 2.10).



Slika 2.10: Kompozicija različitih tačaka na eliptičkoj krivoj



Slika 2.11: Kompozicija tačke sa samom sobom

Iz prethodne definicije ostaje nejasno šta je kompozicija tačke P sa samom sobom.

Međutim, ako povučemo tangentu na eliptičku krivu kroz P, povukli smo, slobodnije govoreći, pravu kroz P i P, jer tačka dodira tangente i krive ima višestrukost presjeka 2. To nas dovodi do sljedeće definicije.

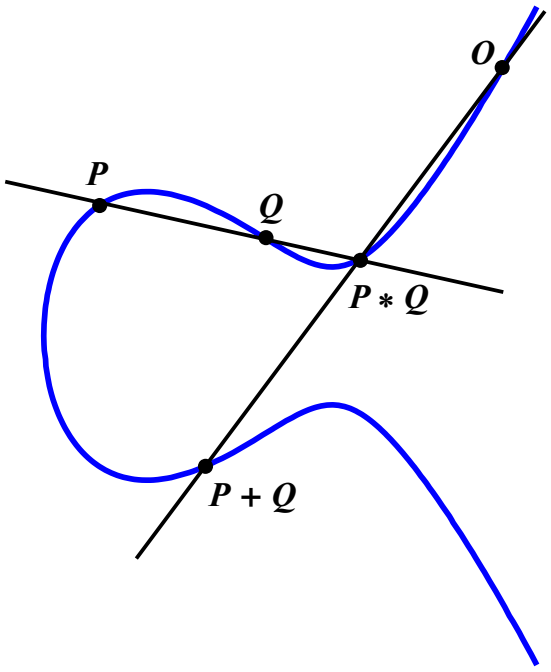
Definicija 2.6. Neka je P tačka na eliptičkoj krivoj E i neka je t tangenta na E u toj tački. Tada kompoziciju $P * P$ definišemo kao treću presječnu tačku tangente t i krive E (slika 2.11).

Dakle, za svake dvije (ne nužno različite) tačke P i Q sa eliptičke krive imamo definisanu treću tačku $P*Q$ koja takođe pripada toj krivoj. Razmotrimo algebarsku strukturu ovog skupa u odnosu na operaciju $*$. Jasno je da ta struktura nije grupa, jer nemamo neutral. Međutim, ako fiksiramo proizvoljnu tačku O na eliptičkoj krivoj koju ćemo smatrati neutralom i malo drugačije definišemo operaciju, možemo dobiti strukturu grupe. Definišimo sada tu operaciju koju ćemo nazivati *sabiranje tačaka na eliptičkoj krivoj.*

Definicija 2.7. Neka su P i Q dvije proizvoljne tačke na eliptičkoj krivoj smještenoj u projektivnoj ravni $\mathbb{P}_2$ na kojoj je fiksirana tačka O. Tada *zbir* tačaka P i Q definišemo kao

$$P + Q = O * (P * Q), \tag{2.6}$$

pri čemu $P * Q$ predstavlja kompoziciju tačaka P i Q (slika 2.12).



Slika 2.12: Sabiranje tačaka na eliptičkoj krivoj

U nastavku će biti dokazano da skup tačaka na eliptičkoj krivoj u odnosu na prethodno definisanu operaciju sabiranja ima strukturu Abelove grupe. Ali, prije toga, navedimo jednu teoremu koja će nam trebati za dokaz grupnog zakona na eliptičkoj krivoj. Ona ima i opštije oblike (vidjeti [12], Appendix A), ali za naše potrebe sljedeća formulacija je sasvim dovoljna.

Teorema 2.2 (Kejli-Baharah, 1886)**.** *Neka su C_1 i C_2 dvije kubike u projektivnoj ravni $\mathbb{P}_2(k)$ koje se sijeku u 9 tačaka (računajući višestrukosti) i neka je C treća kubika koja prolazi kroz 8 od 9 pomenutih tačaka presjeka. Tada C prolazi i kroz devetu presječnu tačku.*

Skica dokaza. Opšta jednačina kubike je zadata jednačinom

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

koja zavisi od 10 koeficijenata. Ako pomnožimo sve ove koeficijente ne-nula konstantom, jednačina definiše istu krivu. Zato je skup svih mogućih kubika 9-dimenzionalan nad k. Ako želimo da kubika prolazi kroz neku tačku čije su koordinate (x, y) fiksirane, to nam nameće jedan linearni uslov koji koeficijenti $a, b, \ldots, j$ treba da zadovoljavaju. Tako dobijamo da je skup kubika koje sadrže neku fiksiranu tačku 8-dimenzionalan.

Dakle, svaki put kada nametnemo uslov da kubika treba da sadrži neku tačku, imamo jedan dodatni linearni uslov za koeficijente. Tako dobijamo da je familija svih kubika koje prolaze kroz 8 presječnih tačaka krivih C_1 i C_2 zapravo jednodimenzionalna familija.

Neka su $F_1(x, y) = 0$ i $F_2(x, y) = 0$ jednačine kojima su zadate kubike C_1 i C_2. Tada možemo naći kubike koje prolaze kroz 8 zajedničkih tačaka krivih C_1, C_2 i C tako što ćemo uzeti linearne kombinacije $\lambda_1 F_1 + \lambda_2 F_2$, pri čemu je bar jedan od brojeva λ_1, λ_2 različit od nule. Ali još uvijek ne znamo da li se među ovim linearnim kombinacijama nalaze sve kubike koje sadrže 8 pomenutih tačaka presjeka.

Međutim, na osnovu prethodnog razmatranja, znamo da je familija svih kubika koje sadrže ovih 8 presječnih tačaka jednodimenzionalna. Sa druge strane, familija $\lambda_1 F_1 + \lambda_2 F_2$ je takođe jednodimenzionalna. Iako vidimo 2 parametra, možemo jednačinu $\lambda_1 F_1 + \lambda_2 F_2 = 0$ podijeliti sa jednim od njih (pošto je bar jedan različit od nule) pri čemu će jednačina da opisuje istu krivu. To znači da zapravo imamo jedan parametar.

Dakle, sada zaključujemo da familija $\lambda_1 F_1 + \lambda_2 F_2$ opisuje sve kubike koje prolaze kroz 8 zajedničkih tačaka krivih C_1, C_2 i C. To znači da i kriva C ima jednačinu $\lambda_1 F_1 + \lambda_2 F_2 = 0$ za neki izbor konstanti λ_1, λ_2.

Sada, pošto se deveta tačka nalazi i na krivoj C_1 i na C_2, slijedi da je i $F_1(x, y)$ i $F_2(x, y)$ jednako nuli u toj tački. Dakle, i $\lambda_1 F_1 + \lambda_2 F_2$ mora biti jednako nuli u toj tački, što upravo znači da kriva C sadrži tu tačku. □

Dokažimo sada grupni zakon na eliptičkoj krivoj.

Teorema 2.3. *Neka je E eliptička kriva nad poljem k i neka je $O \in E$ fiksirana tačka. Tada je E Abelova grupa u odnosu na operaciju sabiranja definisanu sa* (2.6)*, čiji je neutral tačka O.*

Dokaz. Sve aksiome grupe osim asocijativnosti se lako izvode. Zatvorenost i komutativnost direktno slijede iz definicije operacije sabiranja.

Provjerimo da tačka O zaista jeste neutral. Neka je p prava određena tačkama P i O i neka je Q treća presječna tačka prave p i krive E (slika 2.13). Naravno, ako je p tangenta na krivu E, tačke P, Q i O ne moraju biti različite. Tada na osnovu jednakosti (2.6) važi

$$P + O = O * (P * O) = O * Q = P.$$

Dakle, tačka O zaista jeste neutral za operaciju definisanu sa (2.6).

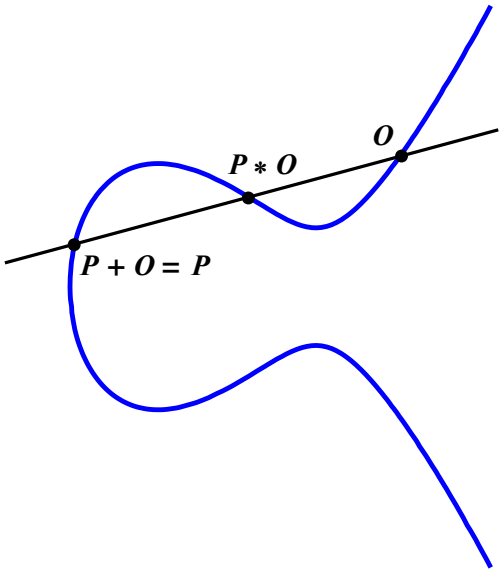
Nađimo sada inverz $-P$ tačke P. Neka je t tangenta na krivu E u tački O i neka je S druga presječna tačka prave t i krive E (slika 2.14). Označimo pravu određenu tačkama P i S sa s. Pokažimo da je inverz tačke P treća presječna tačka prave s i krive E, to jest da je

$$-P = P * S.$$

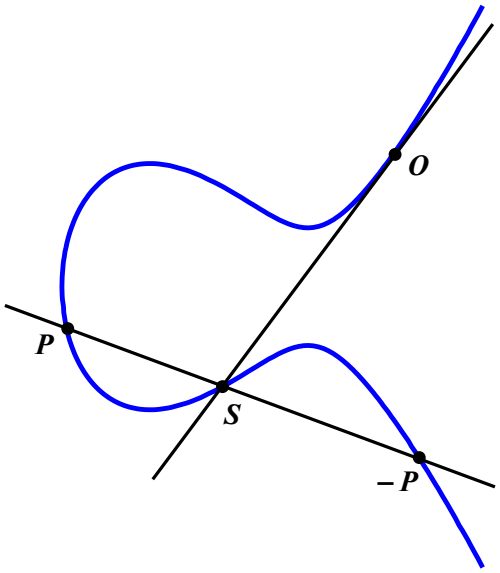
Važi

$$P + (-P) = P + (P * S) = O * (P * (P * S)) = O * S = O.$$

Jednakost $O * S = O$ važi jer prava t kroz O i S siječe krivu E „jednom" u tački S i „dvaput" u tački O.



Slika 2.13: Provjera da O jeste neutral

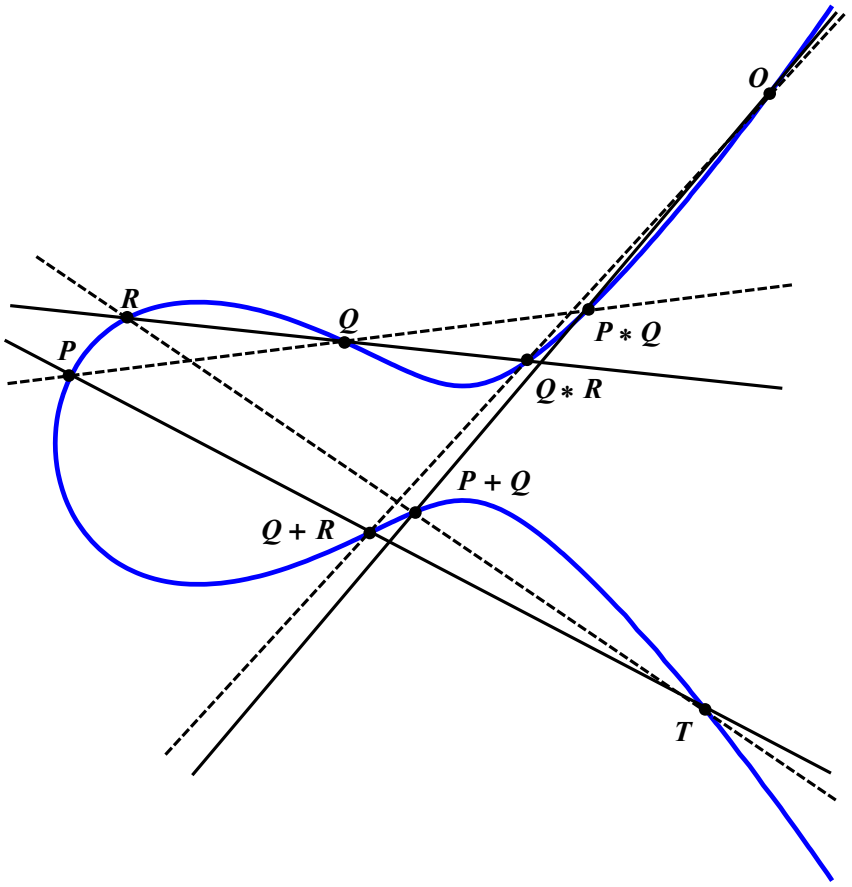


Slika 2.14: Inverz tačke P

Dokažimo još da važi i asocijativnost. Neka su P, Q i R tri tačke na eliptičkoj krivoj E. Treba dokazati da važi $(P + Q) + R = P + (Q + R)$, to jest

$$O * ((P + Q) * R) = O * (P * (Q + R)),$$

odakle je jasno da je dovoljno dokazati da važi $(P+Q)*R = P*(Q+R)$. Da bismo dobili $(P+Q)*R$ prvo treba da nađemo $P*Q$, zatim spojimo $P*Q$ sa O i kao treću presječnu tačku sa krivom dobijamo tačku $P+Q$. Dalje, $P+Q$ spojimo sa R i kao treću presječnu tačku dobijamo $(P+Q)*R$. Treba dokazati da se ova tačka poklapa sa tačkom $P*(Q+R)$. Na slici 2.15 svaka od tačaka O, P, Q, R, $P*Q$, $P+Q$, $Q*R$, $Q+R$ leži na jednoj punoj i jednoj isprekidanoj liniji. Posmatrajmo tačku T koja se dobije u presjeku pune linije određene sa P i $Q+R$ i isprekidane linije određene sa R i $P+Q$. Ako dokažemo da tačka T pripada krivoj E, dokazali smo asocijativnost.



Slika 2.15: Provjera asocijativnosti

Dakle, ukupno imamo 9 tačaka: O, P, Q, R, $P*Q$, $P+Q$, $Q*R$, $Q+R$ i T. Možemo smatrati da unija tri pune linije predstavlja neku degenerisanu kubiku C_1, a unija tri isprekidane linije degenerisanu kubiku C_2. Naime, prava je opisana linearnom jednačinom, a kada imamo tri lineane jednačine, njihovim množenjem dobijamo jednačinu trećeg stepena, to jest jednačinu kubike. Primjenimo sada Teoremu (2.2). Kubike C_1 i C_2 prolaze kroz svih devet pomenutih tačaka po konstrukciji. Naša eliptička kriva, kubika E, prolazi kroz osam od devet datih tačaka, tako da mora da sadrži i devetu tačku, to jest tačku T. Dakle, važi da je $(P+Q)*R = P*(Q+R)$ odakle slijedi asocijativnost. □

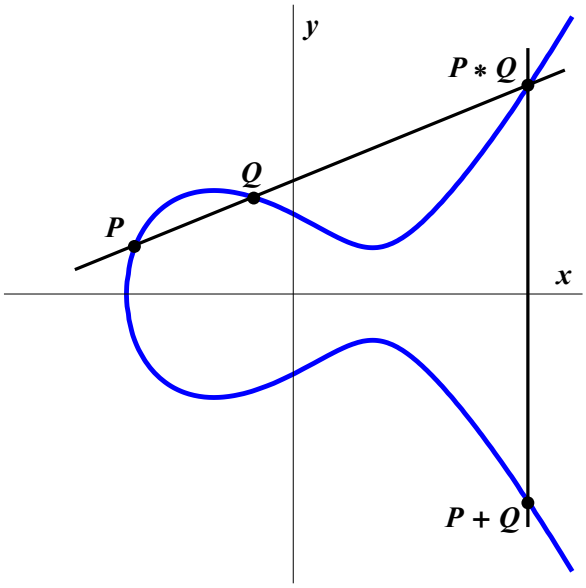
2.3 Eksplicitne formule za sabiranje tačaka

U ovom odjeljku izvešćemo eksplicitne formule za sabiranje na eliptičkoj krivoj datoj u Vajerštrasovom normalnom obliku. Da bismo to uradili, posmatraćemo eliptičku krivu E u afinoj umjesto u projektivnoj ravni. Uvođenjem homogenih koordinata $x = X/Z$ i $y = Y/Z$ jednačina (2.5) postaje

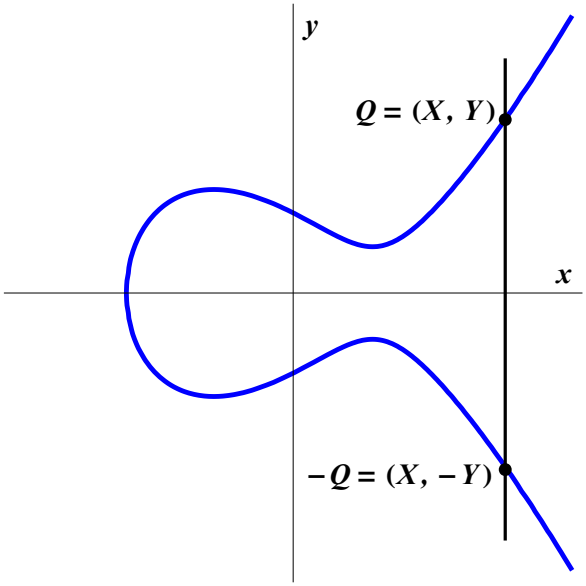
$$Y^2Z = X^3 + aXZ^2 + bZ^3. \tag{2.7}$$

Ispitajmo sada šta je presjek krive (2.7) i beskonačno daleke prave $Z = 0$. Kada zamjenimo $Z = 0$ u (2.7) dobijamo jednačinu $X^3 = 0$, koja ima trostruki korijen $X = 0$. To znači da eliptička kriva (2.7) i beskonačno daleka prava imaju „trostruki" presjek u jednoj, beskonačno dalekoj tački. Uzmimo ovu beskonačno daleku tačku da bude naša tačka O, koja ima ulogu neutrala u grupi na eliptičkoj krivoj, razmatranoj u prethodnom odjeljku. Sada možemo smatrati da se eliptička kriva sastoji od „običnih" tačaka u afinoj ravni xy, uključujući još samo jednu dodatnu, beskonačno daleku tačku O, koju ne možemo vidjeti u afinoj ravni.

Sada možemo provjeriti da svaka prava siječe eliptičku krivu u 3 tačke, računajući višestrukosti. Već smo vidjeli da beskonačno daleka prava i eliptička kriva imaju „trostruki" presjek. Dalje, vertikalna prava $x =$ const. siječe eliptičku krivu u 2 „obične" tačke i u beskonačno dalekoj tački O. I na kraju, ne-vertikalne prave sijeku eliptičku krivu u 3 tačke u afinoj xy ravni.



Slika 2.16: Sabiranje na eliptičkoj krivoj u afinoj ravni



Slika 2.17: Inverz tačke Q na eliptičkoj krivoj u afinoj ravni

Razmotrimo sada kako izgleda sabiranje tačaka na eliptičkoj krivoj E u afinoj xy ravni. Neka su P i Q dvije tačke na E. Da bismo dobili $P + Q$ prvo treba da nađemo tačku $P * Q$, koja se dobija kao treća presječna tačka prave određene tačkama P i Q i krive E. Dalje, prava kroz $P * Q$ i O je prosto vertikalna prava kroz $P * Q$. Pošto je eliptička kriva

u Vajerštrasovom normalnom obliku simetrična u odnosu na x-osu, tačku $P+Q$ ćemo dobiti kada $P*Q$ preslikamo osnom simetrijom u odnosu na x-osu (slika 2.16).

Dalje, pokažimo da je inverz tačke $Q=(X,Y)$ tačka $-Q=(X,-Y)$. Da bismo to provjerili, nađimo zbir $Q+(-Q)$. Naravno, prvo treba da nađemo tačku $Q*(-Q)$, a pošto je prava kroz Q i $-Q$ vertikalna, treća presječna tačka te prave sa krivom E biće tačka O. Sada ćemo tačku $Q+(-Q)$ dobiti kao treću presječnu tačku prave kroz O i $Q*(-Q)$. Međutim, ta prava je u stvari tangenta u tački O, to jest, beskonačno daleka prava, a treća presječna tačka sa krivom E je ponovo O jer beskonačno daleka prava i kriva E imaju u tački O trostruki presjek. Dakle, važi da je $Q+(-Q)=O$ (slika 2.17).

Sada možemo izvesti eskplicitne formule za sabiranje tačaka na eliptičkoj krivoj u afinoj xy ravni. Neka je $x(P)$ oznaka za x-koordinatu tačke P, a $y(P)$ za y-koordinatu. U sljedećoj teoremi ćemo izračunati $x(P_1+P_2)$ i $y(P_1+P_2)$, gdje su P_1 i P_2 tačke sa krive E i važi $P_1\neq\pm P_2$, a zatim ćemo razmotriti slučaj kada je $P_1=P_2$.

Teorema 2.4. (1) *Neka su $P_1=(X_1,Y_1)$ i $P_2=(X_2,Y_2)$ tačke na krivoj E, datoj u Vajerštrasovom normalnom obliku* (2.5)*, pri čemu je $P_1\neq\pm P_2$ i nijedna od tačaka P_1 i P_2 nije O. Tada je*

$$x(P_1+P_2)=\left(\frac{Y_2-Y_1}{X_2-X_1}\right)^2-(X_1+X_2), \tag{2.8}$$

$$y(P_1+P_2)=-\frac{Y_2-Y_1}{X_2-X_1}\,x(P_1+P_2)-\frac{Y_1X_2-Y_2X_1}{X_2-X_1}. \tag{2.9}$$

(2) *Neka je $P=(X,Y)\neq O$ i $Y\neq 0$. Tada je*

$$x(2P)=\frac{(3X^2+a)^2}{4(X^3+aX+b)}-2X, \tag{2.10}$$

$$y(2P)=-\frac{3X^2+a}{2Y}\,x(2P)-\frac{2Y^2-X(3X^2+a)}{2Y}. \tag{2.11}$$

Dokaz. (1) Da bismo izračunali $x(P_1+P_2)$, nađimo jednačinu prave kroz P_1 i P_2 :

$$y=\frac{Y_2-Y_1}{X_2-X_1}\,x+l. \tag{2.12}$$

Zatim, da bismo našli x-koordinatu X_3 tačke $P_3=(X_3,Y_3)$ koja se dobija u presjeku prave (2.12) sa krivom (2.5), zamjenićemo y iz jednačine (2.12) u jednačinu (2.5). Na taj način dobijamo jednačinu

$$x^3-\left(\frac{Y_2-Y_1}{X_2-X_1}\right)^2x^2+\cdots=0. \tag{2.13}$$

Pošto su X_1,X_2,X_3 tri rješenja jednačine (2.13), lijeva strana jednačine (2.13) je

$$(x-X_1)(x-X_2)(x-X_3)=x^3-(X_1+X_2+X_3)x^2+\cdots. \tag{2.14}$$

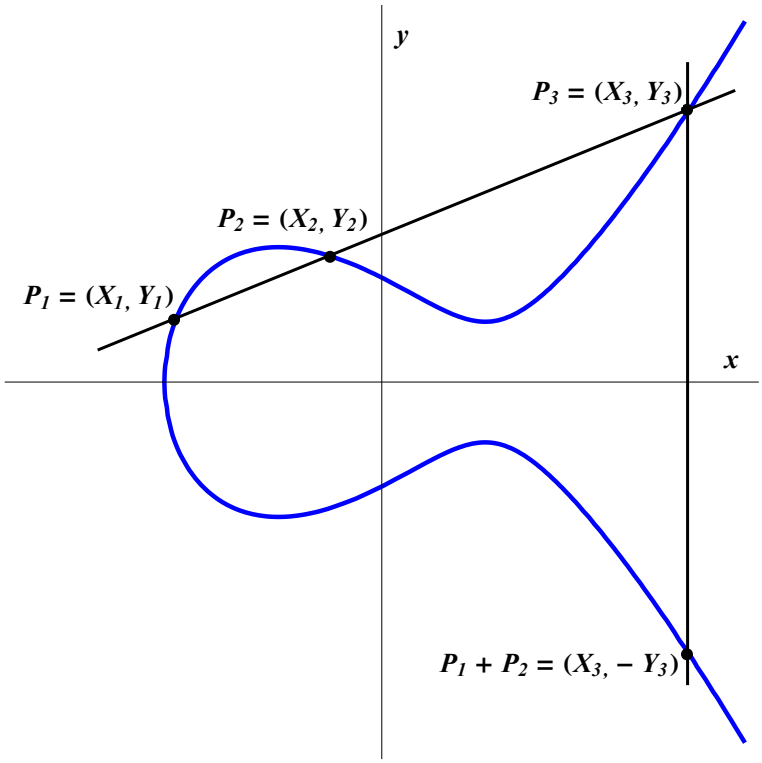
Upoređujući koeficijente uz x^2 u jednačinama (2.13) i (2.14) i imajući u vidu da tačke P_3 i $P_1 + P_2$ imaju istu x-koordinatu, dobijamo

$$x(P_1 + P_2) = X_3 = \left(\frac{Y_2 - Y_1}{X_2 - X_1}\right)^2 - (X_1 + X_2).$$

Da bismo dobili y-koordinatu tačke P_3, izračunaćemo l iz jednakosti (2.12). Pošto prava (2.12) sadrži tačku P_1, imamo

$$l = Y_1 - \frac{Y_2 - Y_1}{X_2 - X_1} X_1 = \frac{Y_1 X_2 - Y_2 X_1}{X_2 - X_1}.$$

Sada y-koordinatu tačke P_3 dobijamo kada zamjenimo dobijeni izraz za l u jednačinu (2.12). Formulu (2.9) dobijamo imajući u vidu da je y-koordinata tačke $P_1 + P_2$ simetrična tački P_3 u odnosu na x-osu, to jest da je $y(P_1 + P_2) = -Y_3$.



Slika 2.18: Izvođenje formula za sabiranje na eliptičkoj krivoj

(2) Da bismo izračunali $x(2P)$, treba nam jednačina tangente na krivu (2.5) u tački P. Iz teoreme o izvodu implicitne funkcije dobijamo koeficijent pravca tangente u tački P (uslovi teoreme su ispunjeni jer je $Y \neq 0$), pa je jednačina tangente data sa

$$y = \frac{3X^2 + a}{2Y} x + r. \tag{2.15}$$

Neka je $\tilde{P} = (\tilde{X}, \tilde{Y})$ tačka različita od P koja se dobija u presjeku tangente (2.15) sa

krivom (2.5). Koordinatu $\tilde{X}$ ćemo dobiti kada jednačinu (2.15) zamjenimo u (2.5). Dobijamo

$$x^3 - \frac{(3X^2+a)^2}{4Y^2}x^2 + \cdots = 0. \tag{2.16}$$

Znamo da su X i $\tilde{X}$ rješenja jednačine (2.16), pri čemu je rješenje X višestrukosti 2, pa iz

$$(x-X)^2(x-\tilde{X}) = x^3 - (2X+\tilde{X})x^2 + \cdots,$$

upoređujući koeficijente uz X^2 i imajući u vidu da je $Y^2 = X^3 + aX^2 + b$ dobijamo

$$x(2P) = \tilde{X} = \frac{(3X^2+a)^2}{4(X^3+aX+b)} - 2X.$$

Da bismo dobili y-koordinatu tačke $\tilde{P}$, treba da nađemo r iz jednačine tangente (2.15). Pošto tangenta (2.15) sadrži tačku P, dobijamo da je

$$r = Y - \frac{3X^2+a}{2Y}\,X = \frac{2Y^2 - X(3X^2+a)}{2Y}.$$

Sada $\tilde{Y}$ dobijamo kada r iz prethodne jednakosti zamjenimo u jednačinu tangente (2.15), a formula (2.11) slijedi iz jednakosti $y(2P) = -\tilde{Y}$. □

Navedimo sada jedan primjer koji će nam poslužiti kao ilustracija prethodne teoreme za sabiranje tačaka na eliptičkoj krivoj.

Primjer 2.1. Posmatrajmo eliptičku krivu

$$E:\ y^2 = x^3 + 17.$$

Lako se pronalaze sljedeće tačke sa cjelobrojnim koordinatama koje pripadaju krivoj E:

$$P_1 = (-2,3), \quad P_2 = (2,5), \quad P_3 = (-1,4), \quad P_4 = (4,9), \quad P_5 = (8,23),$$

a uz pomoć kompjuterske pretrage dobijamo i još neke:

$$P_6 = (43,282), \quad P_7 = (52,375), \quad P_8 = (5234,378661).$$

Koristeći formule za sabiranje izvedene u prethodnoj teoremi, možemo se uvjeriti da važe sljedeće relacije:

$$P_5 = -2P_1, \quad P_4 = P_1 - P_2, \quad P_7 = 3P_1 - P_2.$$

Naravno, postoji još mnogo tačaka sa racionalnim koeficijentima koje pripadaju krivoj E, na primjer

$$2P_3 = \left(\frac{127}{64}, -\frac{2651}{512}\right), \quad P_2 + P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

Sada je tačno, ali nije lako dokazati, da svaka racionalna tačka $P \in E(\mathbb{Q})$ može da se napiše u obliku

$$P = mP_1 + nP_2, \quad \text{za neke } m,n \in \mathbb{Z}.$$

To upravo znači da je grupa racionalnih tačaka $E(\mathbb{Q})$ na krivoj E izomorfna sa $\mathbb{Z} \times \mathbb{Z}$. Dalje, postoji samo 16 tačaka sa cjelobrojnim koordinatama koje pripadaju krivoj E, naime

$$\{\pm P_1, \pm P_2, \ldots, \pm P_8\}.$$

Ove činjenice ilustruju dvije fundamentalne teoreme iz aritmetike eliptičkih krivih, naime da je grupa racionalnih tačaka na eliptičkoj krivoj konačno generisana (Mordelova teorema) i da je skup tačaka sa cjelobrojnim koordinatama na eliptičkoj krivoj konačan (Zigelova teorema). ♢

Napomenimo još da se pomoću eksplicitnih formula (2.8)-(2.11) za sabiranje tačaka može dokazati i grupni zakon na eliptičkoj krivoj. Jasno je da takav dokaz postoji, ali se ispostavlja da je dokaz asocijativnosti teži nego što se čini na prvi pogled. Postoji mnogo specijalnih slučajeva koje treba posebno ispitati (na primjer kada je neka od tačaka jednaka O, kada je zbir dvije tačke jednak O, ili kada je zbir dvije tačke jednak trećoj, i slično). Takođe, za provjeru nekih identiteta je potrebno nekoliko sati na modernom kompjuteru, tako da ovaj dokaz nije ni bio izveden prije 1980-tih. Za detaljan i kompletan dokaz grupnog zakona korišćenjem samo eksplicitnih formula vidjeti rad [6].

2.4 Eliptičke krive nad $\mathbb{C}$

Cilj ovog odjeljka je da u osnovnim crtama prezentuje rezultat da su eliptičke krive nad kompleksnim brojevima izomorfne torusu. Skup tačaka eliptičke krive E sa koordinatama u $\mathbb{C}$ ćemo označavati sa $E(\mathbb{C})$. U daljem tekstu će biti objašnjeno kako je na torusu prirodno uvedena struktura grupe. Iz tog izomorfizma direktno slijedi grupni zakon za eliptičke krive nad kompleksnim brojevima. Takođe, pošto je torus površ *roda* 1, odatle se odmah vidi i da je *rod* eliptičke krive jednak 1.

Pošto je cilj ovog odjeljka samo da ilustruje grupni zakon za eliptičke krive na drugi način od onoga koji je predstavljen ranije, većina dokaza i detalja će biti preskočena, a čitaoca upućujemo na [11], Poglavlje VI ili [13], Poglavlje 9.

Počnimo sa definicijom *rešetke* na $\mathbb{C}$.

Definicija 2.8. Neka su ω_1 i ω_2 kompleksni brojevi linearno nezavisni nad $\mathbb{R}$. Tada skup

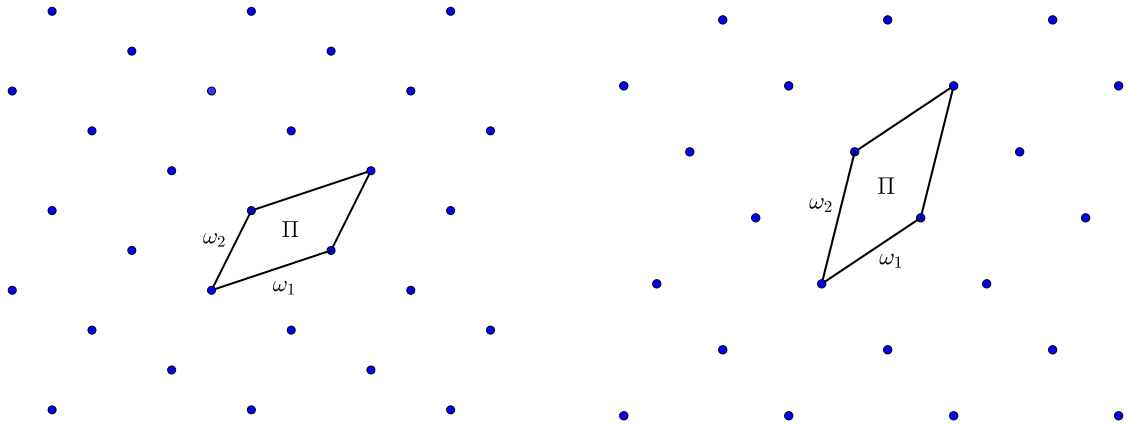
$$\Lambda = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\} \subset \mathbb{C},$$

nazivamo *rešetka* razapeta sa ω_1 i ω_2.

Rešetka Λ je podgrupa od $\mathbb{C}$, pa je i $\mathbb{C}/\Lambda$ takođe grupa. Skup:

$$\Pi = \{a_1\omega_1 + a_2\omega_2 \mid 0 \leq a_i < 1,\ i = 1, 2\}$$

nazivamo *fundamentalni paralelogram* rešetke Λ. Tada svaka klasa iz $\mathbb{C}/\Lambda$ ima po jednog svog predstavnika u Π. Operacija u grupi $\mathbb{C}/\Lambda$ je sabiranje kompleksnih brojeva *po modulu* Λ. Drugim riječima, svaka tačka iz $\mathbb{C}$ je kongruentna mod Λ tačno jednoj tački iz Π. Ovo znači da elemente iz $\mathbb{C}/\Lambda$ zapravo možemo smatrati elementima iz Π.



Slika 2.19: Primjeri različitih rešetki i fundamentalnih paralelograma

Međutim, ako posmatramo zatvorenje $\overline{\Pi}$, tada su naspramne stranice paralelograma $\overline{\Pi}$ identifikovane. Drugim riječima, $\mathbb{C}/\Lambda$ je ekvivalentno paralelogramu sa identifikovanim naspramnim stranicama, što je topološki ekvivalentno torusu. Dakle, $\mathbb{C}/\Lambda$ je topološki torus, na kome imamo strukturu količničke grupe $\mathbb{C}/\Lambda$ koju smo prethodno opisali.

Definišimo sada eliptičku funkciju.

Definicija 2.9. *Eliptička funkcija* u odnosu na rešetku Λ je meromorfna kompleksna funkcija f takva da za svako $z \in \mathbb{C}$ i svako $\omega \in \Lambda$ važi

$$f(z+\omega) = f(z).$$

Slijedi da je $f(z+\omega_1) = f(z+\omega_2)$, pa se eliptičke funkcije nazivaju i *dvostruko periodične* funkcije.

Važan i netrivijalan primjer eliptičke funkcije je *Vajerštrasova $\wp$-funkcija,* koja ima ključnu ulogu u konstruisanju izomorfizma između $\mathbb{C}/\Lambda$ i eliptičkih krivih nad $\mathbb{C}$.

Definicija 2.10. Neka je data rešetka Λ na $\mathbb{C}$. Tada Vajerštrasovu $\wp$-funkciju definišemo sljedećim redom

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{2.17}$$

U sljedećoj teoremi dajemo osnovne osobine Vajerštrasove $\wp$-funkcije. Teoremu navodimo bez dokaza, a čitaoca upućujemo na [13], Teorema 9.3.

Teorema 2.5. *Neka je data rešetka Λ na $\mathbb{C}$. Tada za Vajerštrasovu $\wp$-funkciju važe sljedeća tvrđenja:*

1. *Red (2.17) koji definiše $\wp(z)$ konvergira apsolutno i ravnomjerno na svakom kompaktnom skupu koji ne sadrži elemente iz Λ.*
2. *Funkcija $\wp(z)$ je meromorfna na $\mathbb{C}$ i ima dvostruki pol u svakom $\omega \in \Lambda$.*
3. *Za svako $z \in \mathbb{C}$ važi $\wp(-z) = \wp(z)$.*
4. *Funcija $\wp(z)$ je eliptička u odnosu na rešetku Λ, to jest važi $\wp(z+w) = \wp(z)$ za svako $\omega \in \Lambda$.*
5. *Skup svih eliptičkih funkcija u odnosu na rešetku Λ je $\mathbb{C}(\wp, \wp')$. Drugim riječima, svaka eliptička funkcija je racionalna kombinacija funkcije $\wp$ i njenog izvoda $\wp'$.* □

Da bismo pokazali da je kompleksni torus $\mathbb{C}/\Lambda$ izomorfan sa kompleksnim tačkama na eliptičkoj krivoj, potrebno je da uvedemo još jedan pojam.

Definicija 2.11. Neka je Λ rešetka na $\mathbb{C}$ i neka je k cijeli broj. *Ajzenštajnov red težine* $2k$, u odnosu na rešetku Λ je red

$$G_{2k} = G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-2k}.$$

Primjetimo da je $G_{2k+1} = 0$, jer se članovi $\omega^{-(2k+1)}$ i $(-\omega)^{-(2k+1)}$ poništavaju, pa zbog toga definišemo Ajzenštajnov red samo za parne cijele brojeve.

U sljedećoj teoremi je data veza između Vajerštrasove $\wp$-funkcije i Ajzenštajnovih redova.

Teorema 2.6. *Neka je $\wp(z)$ Vajerštrasova $\wp$-funkcija i G_{2k} Ajzenštajnov red. Tada je*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\,\wp(z) - 140G_6. \tag{2.18}$$

□

Uobičajeno je da se koriste oznake

$$g_2 = 60G_4, \quad g_3 = 140G_6.$$

Tada jednakost (2.18) glasi

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\,\wp(z) - g_3.$$

Dakle, tačke $(\wp(z), \wp'(z)$ leže na krivoj

$$y^2 = 4x^3 - g_2 x - g_3. \tag{2.19}$$

Tradicionalno se ostavlja 4 kao koeficijent uz x^3, umjesto da da se izvrši smjena promjenljivih kako bi koeficijent uz x^3 bio 1. Diskriminanta kubnog polinoma na desnoj strani je $16(g_2^3 - 27g_3^2)$. Označimo $\Delta = g_2^3 - 27g_3^2$. Tada važi sljedeće tvrđenje.

Stav 2.2. *Za kubni polinom* $4x^3 - g_2x - g_3$ *važi da je* $\Delta = g_2^3 - 27g_3^2 \neq 0$. □

Iz prethodnog stava slijedi da je kriva (2.19) zapravo eliptička kriva. Dakle, funkcija

$$z \mapsto (\wp(z), \wp'(z))$$

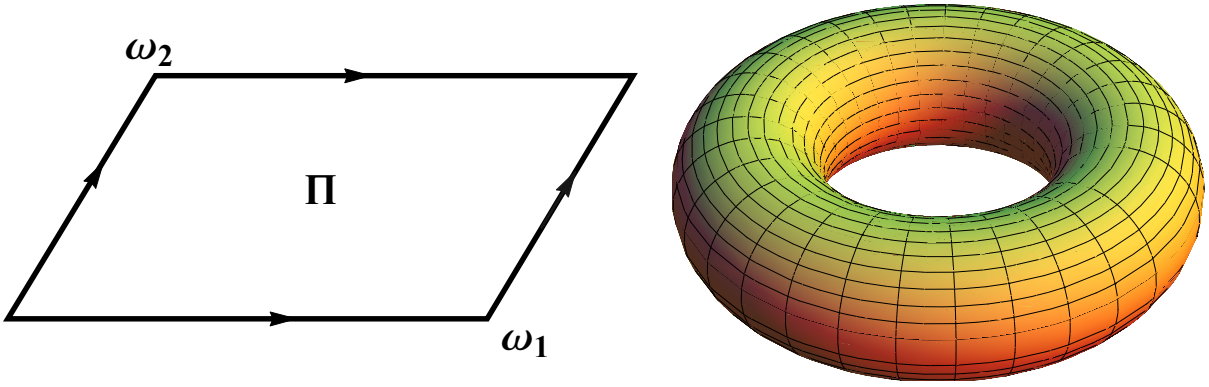
svakom kompleksnom broju pridružuje neku tačku na eliptičkoj krivoj. Ako promjenimo z za neki element iz Λ, vrijednost funkcija $\wp(z)$ i $\wp'(z)$ se neće promjeniti, jer su one dvostruko periodične. Dakle, $\wp(z)$ i $\wp'(z)$ zavise samo od z mod Λ, pa imamo preslikavanje iz $\mathbb{C}/\Lambda$ u $E(\mathbb{C})$.

Sada možemo formulisati osnovnu teoremu (za dokaz pogledati [13], Teorema 9.10).

Teorema 2.7. *Neka je* Λ *rešetka na* $\mathbb{C}$ *i neka je* E *eliptička kriva* $y^2 = 4x^3 - g_2x - g_3$. *Tada je preslikavanje* $\Phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ *definisano sa*

$$\begin{aligned} z &\mapsto (\wp(z), \wp'(z)) \\ 0 &\mapsto \infty \end{aligned}$$

izomorfizam između grupe $\mathbb{C}/\Lambda$ *(kompleksnog torusa) i* $E(\mathbb{C})$. □



Slika 2.20: Fundamentalni paralelogram sa identifikovanim naspramnim stranicama je torus koji je izomorfan eliptičkoj krivoj

2.5 Eliptičke krive nad $\mathbb{Q}$

Teorija Diofantovih jednačina je oblast teorije brojeva koja se bavi traženjem cjelobrojnih ili racionalnih rješenja polinomnih jednačina. Svakako, jedan od najpoznatijih problema iz ove oblasti je *Fermaova posljednja teorema.* Međutim, problem koji ćemo razmatati u ovom odjeljku je sljedeći.

Neka je $f(x, y)$ polinom trećeg stepena sa koeficijentima iz $\mathbb{Z}$. Posmatrajmo sljedeću jednačinu

$$f(x, y) = 0.$$

Postoji nekoliko prirodnih pitanja koja možemo postaviti u vezi prethodne jednačine:

(a) Da li postoji bar jedno cjelobrojno rješenje?

(b) Da li postoji bar jedno racionalno rješenje?

(c) Da li postoji beskonačno mnogo cjelobrojnih rješenja?

(d) Da li postoji beskonačno mnogo racionalnih rješenja?

Što se tiče pitanja (a) i (c), Zigel je 1920-tih dokazao da kubna jednačina ima samo konačno mnogo cjelobrojnih rješenja, a Bejker i Kouts su 1970. dokazali da postoji eksplicitna gornja granica za najveće cjelobrojno rješenje u funkciji koeficijenata polinoma $f(x, y)$. Dakle, postoje zadovoljavajući odgovori na pitanja (a) i (c).

Na pitanja (b) i (d) „djelimičan" odgovor daje *Mordelova teorema,* iz 1922. godine, sa kojom je započela moderna teorija Diofantovih jednačina.

Teorema 2.8 (Mordel, 1922)**.** *Neka je E eliptička kriva data jednačinom*

$$y^2 = x^3 + ax + b, \quad (a, b \in \mathbb{Q}).$$

Tada je grupa racionalnih tačaka $E(\mathbb{Q})$ konačno generisana Abelova grupa. Drugim riječima, postoji konačan skup tačaka $P_1, P_2, \ldots, P_t \in E(\mathbb{Q})$ takav da se svaka tačka $P \in E(\mathbb{Q})$ može predstaviti u obliku

$$P = n_1P_1 + n_2P_2 + \ldots + n_tP_t$$

za neke brojeve $n_1, n_2, \ldots, n_t \in \mathbb{Z}$. □

Iz osnovne teoreme o konačno generisanim Abelovim grupama slijedi da je

$$E(\mathbb{Q}) \cong T \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r},$$

gdje je T konačna grupa koja se naziva *torziona podgrupa* od $E(\mathbb{Q})$, a cijeli broj $r \geq 0$ se naziva *rang* od $E(\mathbb{Q})$.

Postoji veoma jednostavan opis svih mogućih torzionih podgrupa od $E(\mathbb{Q})$, iako je dokaz tog tvrđenja ekstremno težak.

Teorema 2.9 (Mazur, 1977)**.** *Torziona podgrupa T grupe racionalnih tačaka $E(\mathbb{Q})$ na eliptičkoj krivoj ima jedan od sljedeća dva oblika:*

(i) Ciklična grupa reda N, gdje je $1 \leq N \leq 10$ ili $N = 12$,

(ii) Proizvod ciklične grupe reda 2 i ciklične grupe reda $2N$, pri čemu je $1 \leq N \leq 4$.

Posebno, torziona podgrupa T može imati najviše 16 elemenata. □

Što se tiče ranga grupe $E(\mathbb{Q})$, njega je dosta teže opisati. Postoji sljedeća hipoteza.

Hipoteza. *Postoji eliptička kriva E čija je grupa racionalnih tačaka $E(\mathbb{Q})$ proizvoljno velikog ranga.*

Martin i Mekmilen su 2000. pronašli eliptičku krivu čija grupa racionalnih tačaka ima rang bar 24.[1] Postoji još samo jedan poznat primjer grupe racionalnih tačaka eliptičke krive koja ima veći rang. Taj primjer je pronašao Elkis, 2006. godine, a pomenuta grupa ima rang veći ili jednak od 28.[2]

Sada je jasno zašto smo rekli da Mordelova teorema daje „djelimičan" odgovor na pitanja (a) i (c). Međutim, da bismo razumjeli racionalne tačke $E(\mathbb{Q})$, možemo da posmatramo eliptičke krive nad konačnim poljima $\mathbb{F}_p$, pri čemu prost broj p ne dijeli diskriminantu eliptičke krive nad $\mathbb{Q}$. Ovaj uslov nam je potreban zbog toga što u slučaju kada p dijeli diskriminantu eliptičke krive nad $\mathbb{Q}$ imamo da je ta diskriminanta jednaka nuli u polju $\mathbb{F}_p$, pa je onda naša kriva singularna nad $\mathbb{F}_p$, a samim tim nije eliptička.

Dakle, umjesto da tražimo racionalne tačke eliptičkih krivih nad $\mathbb{Q}$, možemo posmatrati eliptičke krive nad $\mathbb{F}_p$ i tražiti racionalne tačke u polju $\mathbb{F}_p$, što je očigledno lakši problem jer je $\mathbb{F}_p$ konačno polje.

To upravo predstavlja motivaciju za proučavanje eliptičkih krivih nad konačnim poljima, o čemu će biti više riječi u ostatku rada.

[1] Roland Martin and William McMillen, *An elliptic curve over $\mathbb{Q}$ with rank at least 24*, Number Theory Listserver, May 2000.

[2] N. D. Elkies, *Some more rank records*, Number Theory Listserver, Jun 2006.

Glava 3

Zeta-funkcija za globalna polja

U ovoj glavi ćemo uvesti *zeta-funkciju za globalna polja* koja predstavlja generalizaciju Rimanove ζ-funkcije razmatrane u Glavi 1. Zatim ćemo uvesti i zeta-funkciju za krive nad konačnim poljima (specijalno i za eliptičke krive) i formulisati Rimanovu hipotezu za zeta-funkciju pridruženu eliptičkoj krivoj, čiji je ekvivalent *Haseova teorema* koju ćemo dokazati u Glavi 4. Za uvođenje zeta-funkcije pridružene globalnim poljima koristićemo pristup preko *valuacija polja.*

3.1 Definicija zeta-funkcije za globalna polja

Prije nego što uvedemo *globalno polje,* definišimo *funkcijsko polje* algebarske krive nad konačnim poljem.

Definicija 3.1. Neka je C algebarska kriva nad konačnim poljem $\mathbb{F}_q$ definisana ireducibilnim polinomom

$$F(x, y) = 0,$$

čiji su koeficijenti u $\mathbb{F}_q$. Tada *funkcijsko polje* krive C definišemo kao polje razlomaka domena (oblasti cijelih) $\mathbb{F}_q[x, y]/(F(x, y))$, gdje je $(F(x, y))$ prost ideal generisan polinomom $F(x, y)$.

Sada možemo definisati globalno polje.

Definicija 3.2. *Globalno polje* je polje jednog od sljedeća dva tipa

1. *Brojevno polje*, to jest konačno raširenje polja $\mathbb{Q}$,

2. *Funkcijsko polje* algebarske krive nad konačnim poljem $\mathbb{F}_q$.

3.1.1 Valuacije

Zeta-funkcija brojevnog polja K ili *Dedekindova zeta-funkcija*, koja predstavlja generalizaciju Rimanove ζ-funkcije na brojevna polja se najprirodnije uvodi pomoću *ideala* u prstenu cijelih polja K. Ako prsten cijelih brojevnog polja K označimo sa $\mathcal{O}_K$, tada je Dedekindova zeta-funkcija definisana sa

$$\zeta_K(s) = \sum_{I \subseteq \mathcal{O}_K} \frac{1}{(N_{K/\mathbb{Q}}(I))^s},$$

gdje I prolazi kroz sve nenula ideale prstena $\mathcal{O}_K$, a $N_{K/\mathbb{Q}}(I)$ predstavlja *normu* ideala I.

Međutim, pristup koji objedinjuje brojevna i funkcijska polja i koji je bolji za istovremeni rad sa oba tipa globalnog polja koristi *valuacije* i to je pristup koji ćemo slijediti u nastavku. Počnimo sa definicijom valuacije.

Definicija 3.3. Neka je K proizvoljno polje. *Valuacija* na polju K je preslikavanje $v : K \to \mathbb{Z} \cup \{\infty\}$ za koga važi

1. $v(x) = \infty$ ako i samo ako je $x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(a + b) \geq \min(v(x), v(y))$.

Skup valuacija polja K označavamo sa V_K.

Ključnu ulogu u defininisanju globalne zeta-funkcije će imati *p-adska valuacija* koju ćemo razmotriti u sljedećem primjeru.

Primjer 3.1. Neka je $K = \mathbb{Q}$. Fiksirajmo prost broj $p = 2, 3, 5, \ldots$ i neka je $x \neq 0$ element iz $\mathbb{Q}$. Tada se x može napisati kao

$$x = p^{v_p(x)} \cdot \frac{a}{b},$$

gdje je $v_p(x) \in \mathbb{Z}$, a za nenula cijele brojeve a, b važi $(p, ab) = 1$. Drugim riječima, $v_p(x)$ je cijeli broj (pozitivan, negativan ili nula) koji je eksponent od p u faktorizaciji racionalnog broja x na stepene različitih prostih brojeva. Na primjer, ako je $x = 4/5$, tada je $v_2(x) = 2$, $v_3(x) = 0$ i $v_5(x) = -1$. Homomorfizam grupa $v_p : \mathbb{Q} \to \mathbb{Z}$ nam daje valuaciju na $\mathbb{Q}$ koju nazivamo *p-adska valuacija.* ♢

3.1.2 Generalizacija Rimanove ζ-funkcije na globalna polja

Sada ćemo izvesti formulu kojom se definiše ζ-funkcija za globalno polje. Počećemo od Ojlerovog proizvoda za ζ-funkciju (vidjeti Teoremu 1.1):

$$\zeta(s) = \sum_{n=0}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \tag{3.1}$$

pri čemu proizvod u gornjoj formuli prolazi kroz sve proste brojeve p. Da bismo dobili generalizaciju koju želimo, treba da „prevedemo" formulu (3.1) u ekvivalentan oblik, koristeći samo valuacije na $\mathbb{Q}$. To će nam dati naznaku kako da pridružimo zeta-funkciju proizvoljnom globalnom polju, dobijajući Rimanovu ζ-funkciju u slučaju kada je to globalno polje jedanko samom polju $\mathbb{Q}$.

U nastavku će nam biti potrebne još neke dodatne definicije.

Definicija 3.4. Neka je K polje koje ima bar jednu netrivijalnu valuaciju i neka je v ta valuacija. Definišimo sljedeće podskupove polja K:

$$\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}, \tag{3.2}$$

$$\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}. \tag{3.3}$$

Iz definicije valuacije slijedi da su $\mathcal{O}_v$ i $\mathfrak{p}_v$ aditivne podgrupe od K. Primjetimo da je zapravo $\mathcal{O}_v$ podprsten od K, a $\mathfrak{p}_v$ maksimalni ideal u $\mathcal{O}_v$, iako to nije važno za nastavak našeg izvođenja. Iz maksimalnosti ideala $\mathfrak{p}$ slijedi da je količnicki skup $\mathcal{O}_v/\mathfrak{p}$ polje.

Definišimo sada normu valuacije v.

Definicija 3.5. Neka je K polje i v valuacija na K. Dalje, neka je $\mathcal{O}_v/\mathfrak{p}_v$ količničko polje, gdje su $\mathcal{O}_v$ i $\mathfrak{p}_v$ definisani sa (3.2) i (3.3). Ako je $\mathcal{O}_v/\mathfrak{p}_v$ konačno polje tada definišemo *normu* valuacije v kao

$$N_v = \#(\mathcal{O}_v/\mathfrak{p}_v),$$

gdje je # oznaka za broj elemenata skupa.

U sljedećoj lemi ćemo razmotriti normu p-adske valuacije.

Lema 3.1. *Neka je data p-adska valuacija v_p na polju $\mathbb{Q}$. Tada je*

$$N_{v_p} = p.$$

Dokaz. Primjetimo da u slučaju p-adske valuacije skup $\mathcal{O}_{v_p}$ čine razlomci čiji je imenilac uzajamno prost sa p, dok je $\mathfrak{p}_v$ podskup od $\mathcal{O}_{v_p}$ koga čine razlomci čiji je brojilac umnožak od p. Sada se lako provjeri da se $\mathcal{O}_v/\mathfrak{p}_v$ sastoji od klasa ekvivalencije elemenata $0, 1, \ldots p$, tako da je $N_{v_p} = p$, što je i trebalo dokazati. □

Koristeći formulu (3.1), sada možemo napisati Rimanovu ζ-funkciju na sljedeći način

$$\zeta(s) = \prod_{v \in V_{\mathbb{Q}}} \left(1 - \frac{1}{N_v^s}\right)^{-1}. \tag{3.4}$$

3.1.3 Definicija

Formulu (3.4) možemo odmah generalizovati na slučaj globalnih polja. Ključna stvar kod globalnih polja je ta što je za svaku valuaciju v količničko polje $\mathcal{O}_v/\mathfrak{p}_v$ konačno, tako da je norma valuacije N_v dobro definisana.

Definišimo sada zeta-funkciju pridruženu globalnom polju.

Definicija 3.6. Neka je K globalno polje i V_K skup valuacija polja K. Tada *zeta-funkciju pridruženu globalnom polju* K definišemo formulom

$$\zeta_K(s) = \prod_{v \in V_K} \left(1 - \frac{1}{N_v^s}\right)^{-1}. \tag{3.5}$$

Već smo vidjeli da je $\zeta_{\mathbb{Q}}(s) = \zeta(s)$, pa $\zeta_K(s)$ zaista jeste generalizacija koju smo tražili.

3.2 Zeta-funkcija za krive nad konačnim poljima

Neka je C glatka kriva definisana ireducibilnim polinomom

$$F(x, y) = 0$$

nad konačnim poljem $\mathbb{F}_q$ od q elemenata. Napomenimo da ćemo sada posmatrati i one tačke krive C koje imaju koordinate u nekom konačnom polju koje sadrži $\mathbb{F}_q$, to jest u nekom konačnom raširenju polja $\mathbb{F}_q$. Pretpostavimo i da je kriva C *kompletna,* što znači da smo joj dodali beskonačno daleku tačku. Dalje, neka je K funkcijsko polje krive C, to jest polje razlomaka domena $\mathbb{F}_q[x, y]/(F(x, y))$, gdje je $(F(x, y))$ prost ideal generisan polinomom $F(x, y)$. Cilj nam je da svakoj tački krive C koja pripada nekom konačnom raširenju od $\mathbb{F}_q$ dodijelimo jednu valuaciju na K. Neka su

$$R_1(x, y) = \frac{G_1(x, y)}{H_1(x, y)} \quad \text{i} \quad R_2(x, y) = \frac{G_2(x, y)}{H_2(x, y)}$$

dvije racionalne funkcije za koje važi da je

$$G_1(x, y) \sim G_2(x, y) \mod F(x, y)$$

$$H_1(x, y) \sim H_2(x, y) \mod F(x, y).$$

Tada $R_1(x, y)$ i $R_2(x, y)$ određuju isti element polja K. Dalje, neka je (a, b) neka tačka koja pripada krivoj C. Tada važi

$$R_1(a, b) = R_2(a, b),$$

tako da elemente polja K možemo posmatrati kao racionalne funkcije koje su dobro definisane na krivoj C, pošto možemo smatrati da racionalne funkcije $R_1(x, y)$ i $R_2(x, y)$ određuju istu funkciju na C.

Fiksirajmo sada tačku $P \in C$. Tada možemo dobiti valuaciju v_P na K tako što ćemo posmatrati red nule ili red *pola* svake nenula funkcije na K.

Primjer 3.2. Neka je K funkcijsko polje krive C i neka je racionalna funkcija $R = R(x, y) \in K$ definisana sa

$$R(x, y) = \frac{(x+1)^2}{x-3}.$$

Pošto funkcija R ne zavisi od y posmatraćemo samo x-koordinate tačaka na krivoj C. Tada je, na primjer,

$$v_{-1}(R) = 2, \quad v_2(R) = 0, \quad v_3(R) = -1,$$

pri čemu se lako provjeri da preslikavanje v zaista jeste valuacija na K. ♢

Dakle, svakoj tački krive C smo pridružili po jednu valuaciju na K. Međutim, može se desiti da različite tačke na krivoj C daju istu valuaciju. Ilustrujmo to sljedećim primjerom.

Primjer 3.3. Razmotrimo slučaj kada je $F(x, y) = y$, to jest kada je kriva C zadata jednačinom $y = 0$. Dakle, kriva C je u stvari *afina prava,* slična x-osi u Dekartovom koordinantnom sistemu. Tačke na krivoj C su jedinstveno određene x-koordinatom. (Zapravo, trebalo bi da krivoj C dodamo i beskonačno daleku tačku, ali to neće uticati na sadržaj primjera.)

Nađimo sada funkcijsko polje K krive C. Imamo da je $\mathbb{F}_3[x, y]/(y) \cong \mathbb{F}_3[x]$, pa je $K \cong \mathbb{F}_3(x)$. Primjetimo da polje $\mathbb{F}_3$ ne sadrži kvadratni korijen iz -1, pa ako označimo taj element sa i, imaćemo da je $\mathbb{F}_3[i] \cong \mathbb{F}_{3^2}$, jer je stepen raširenja $[\mathbb{F}_3[i] : \mathbb{F}] = 2$.

Posmatrajmo sada valuaciju na K indukovanu elementom i. Tada je, na primjer, $v_i(x^2 + 1) = 1$. Međutim, racionalne funkcije koje čine K imaju sve koeficijente u $\mathbb{F}_3$, pa svaka racionalna funkcija iz $\mathbb{F}(x)$ ima isti broj faktora $x + i$ kao i $x - i$, . Odatle slijedi da će valuacija indukovana sa i biti ista kao valuacija indukovana sa $-i$. ♢

Da bismo okarakterisali tačke krive C koje daju istu valuaciju na K biće nam potrebna sljedeća definicija.

Definicija 3.7. Neka je kriva C definisana nad konačnim poljem $\mathbb{F}_q$ i neka je $\mathbb{F}$ algebarsko zatvorenje od $\mathbb{F}_q$. Dalje, neka je $G = \mathrm{Gal}\,(\mathbb{F}/\mathbb{F}_q)$ apsolutna Galuaova grupa. Posmatrajmo dejstvo grupe G na skup $C(\mathbb{F})$ tačaka krive C koje pripadaju polju $\mathbb{F}$. Tada orbitu tačke $P \in C(\mathbb{F})$ nazivamo *Galuaova orbita* tačke P i označavamo sa $[P]$, a skup svih orbita krive C označavamo sa $\mathcal{C}$.

Ispostavlja se da sve tačke krive C koje daju istu valuaciju na K pripadaju jednoj *Galuaovoj orbiti,* što možemo vidjeti i iz Primjera 3.3. Dakle, umjesto da uzimamo sve tačke sa krive i posmatramo valuacije koje indukuju, možemo uzeti po jednu tačku iz svake orbite.

Neka je P tačka krive C koja ima koordinate u nekom polju $\mathbb{F}_{q^m}$, pri čemu te koordinate ne pripadaju nijednom pravom potpolju od $\mathbb{F}_{q^m}$. Tada postoji tačno m tačaka u orbiti

$[P]$, jer je Galuaova grupa $\mathrm{Gal}\,(\mathbb{F}_{q^m}/\mathbb{F}_q)$ ciklična i reda m. Takođe, može se dokazati da je norma valuacije koju indukuje orbita $[P]$ jednaka

$$N_{v_{[P]}} = q^m.$$

Neka je $\#P$ kardinalnost orbite $[P]$. Tada iz formule (3.5) slijedi sljedeća definicija zeta-funkcije krive nad konačnim poljem.

Definicija 3.8. Neka je C kriva nad konačnim poljem $\mathbb{F}_q$. Tada zeta-funkciju krive C, za $\Re(s) > 1$ definišemo kao

$$Z_C(s) = \prod_{[P]\in\mathcal{C}} \left(1 - \frac{1}{q^{\#Ps}}\right)^{-1}, \tag{3.6}$$

pri čemu proizvod u prethodnoj jednakosti prolazi kroz sve orbite krive C, to jest kroz sve valuacije polja K indukovane tim orbitama.

Često se uvodi smjena $t = q^{-s}$, pa formula (3.6) dobija oblik

$$Z_C(t) = \prod_{[P]\in\mathcal{C}} (1 - t^{\#P})^{-1}. \tag{3.7}$$

U sljedećoj teoremi ćemo dati ekvivalentan oblik formule (3.7), izražen preko broja tačaka krive C u polju $\mathbb{F}_{q^m}$.

Teorema 3.1. *Neka je zeta-funkcija krive C nad konačnim poljem $\mathbb{F}_q$ definisana sa* (3.7)*. Tada važi da je*

$$Z_C(t) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m}\, t^m\right). \tag{3.8}$$

Dokaz. Broj tačaka krive C koje se nalaze u polju $\mathbb{F}_{q^m}$ jednak

$$N_m = \sum_{d|m} d \sum_{\substack{[P]\in\mathcal{C} \\ \#P=d}} 1. \tag{3.9}$$

Dakle, klasirali smo orbite po broju elemenata i pomnožili ih sa brojem elemenata u jednoj orbiti, pri čemu broj elemenata d orbite u formuli (3.9) prolazi kroz stepene raširenja svih potpolja od $\mathbb{F}_{q^m}$, pa stoga d dijeli m.

Kada primjenimo logaritamski izvod na jednakost (3.8), a zatim dobijenu jednakost pomnožimo sa t imamo

$$t\,\frac{Z_C'(t)}{Z_C(t)} = \sum_{m=1}^{\infty} N_m\, t^m.$$

Kada iste operacije primjenimo na jednakost (3.7), imajući u vidu da je

$$\frac{1}{1-t} = \sum_{m=0}^{\infty} t^m,$$

jer je $|t| < 1$, dobijamo

$$t\,\frac{Z_C'(t)}{Z_C(t)} = \sum_{[P]\in\mathcal{C}} \#P \sum_{m=1}^{\infty} t^{\#Pm}.$$

Odredimo koeficijent a_m uz t^m u prethodnom formalnom redu za fiksiran prirodni broj m. Primjetimo da će članovi t^m da se pojave kada je $\#P = m$, ali i kada je $\#P$ djelilac od m jer će tada da postoji prirodan broj k takav da je $(t^{\#P})^k = t^m$. Neka su sada $m_1, m_2, \dots m_r$ svi djelioci od m. Tada je

$$a_m = m_1 \sum_{\substack{[P]\in\mathcal{C}\\ \#P=m_1}} 1 + m_2 \sum_{\substack{[P]\in\mathcal{C}\\ \#P=m_2}} 1 + \cdots + m_r \sum_{\substack{[P]\in\mathcal{C}\\ \#P=m_r}} 1 = \sum_{d|m} d \sum_{\substack{[P]\in\mathcal{C}\\ \#P=d}} 1.$$

Dakle, važi

$$t\,\frac{Z_C'(t)}{Z_C(t)} = \sum_{[P]\in\mathcal{C}} \#P \sum_{m=1}^{\infty} t^{\#Pm} = \sum_{m=1}^{\infty} t^m \Bigg(\sum_{d|m} d \sum_{\substack{[P]\in\mathcal{C}\\ \#P=d}} 1 \Bigg),$$

odakle slijedi tvrđenje teoreme. □

Kada pređemo na promjenljivu s, formula (3.8) dobija sljedeći oblik

$$Z_C(s) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m}\, q^{-ms} \right).$$

3.3 Formulacija Rimanove hipoteze za eliptičke krive

Razmotrimo prvo kako izgleda zeta-funkcija eliptičke krive nad nekim konačnim poljem. Za to će nam trebati sljedeća lema koju nećemo dokazivati jer ima (relativno) dug i tehnički zahtjevan dokaz, a čitaoca upućujemo na [13], Teorema 4.12.

Lema 3.2. *Neka je eliptička kriva E definisana nad konačnim poljem $\mathbb{F}_q$ i neka je $N_q = q + 1 - a_q$, gdje je N_q broj tačaka krive E čije koordinate pripadaju polju $\mathbb{F}_q$, uključujući i beskonačno daleku tačku. Napišimo $X^2 - a_q X + q = (X - \alpha)(X - \beta)$. Tada za svako $m \geq 1$ važi*

$$N_m = q^m + 1 - (\alpha^m + \beta^m),$$

pri čemu je N_m broj tačaka krive E koje pripadaju polju $\mathbb{F}_{q^m}$. □

Navedimo sada teoremu koja opisuje zeta-funkciju eliptičke krive.

Teorema 3.2. *Neka je E eliptička kriva definisana nad $\mathbb{F}_q$ i neka je $N_q = q+1-a_q$, gdje je N_q broj tačaka krive E u polju $\mathbb{F}_q$, uključujući i beskonačno daleku tačku. Tada je*

$$Z_E(t) = \frac{qt^2 - a_q t + 1}{(1-t)(1-qt)}. \tag{3.10}$$

Dokaz. Neka je $X^2 - a_q X + q = (X - \alpha)(X - \beta)$. Na osnovu prethodne leme slijedi

$$N_m = q^n + 1 - \alpha^m - \beta^m.$$

Stoga, koristeći razvoj

$$-\log(1-t) = \sum_{m=1}^{\infty} \frac{t^n}{n},$$

dobijamo

$$\begin{aligned} Z_E(t) &= \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m}\, t^m\right) \\ &= \exp\left(\sum_{m=1}^{\infty} (q^n + 1 - \alpha^m - \beta^m)\frac{t^n}{m}\right) \\ &= \exp\left(-\log(1-qt) - \log(1-t) + \log(1-\alpha t) + \log(1-\beta t)\right) \\ &= \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)} \\ &= \frac{qt^2 - a_q t + 1}{(1-t)(1-qt)}, \end{aligned}$$

što je i trebalo dokazati. □

Kada isključimo iz razmatranja beskonačno daleku tačku krive E, dobijamo da u afinoj ravni važi jednakost

$$a_q = q - N_q.$$

Formulišimo sada Rimanovu hipotezu za eliptičke krive nad konačnim poljima.

Rimanova hipoteza za eliptičke krive nad konačnim poljima. *Neka je zeta-funkcija eliptičke krive E nad $\mathbb{F}_q$ definisana sa* (3.10)*, pri čemu je $t = q^{-s}$. Ako je $Z_E(q^{-s}) = 0$, tada je $\Re(s) = 1/2$.*

Preformulišimo sada prethodno tvrđenje u ekvivalentan oblik, koji je pogodniji za razmatranje.

Teorema 3.3. *Neka je eliptička kriva E definisana afinom jednačinom* (2.5) *u Vajerštrasovom normalnom obliku nad konačnim poljem $\mathbb{F}_q$ čija je karakteristika različita od 2 i 3. Tada je Rimanova hipoteza za krivu E ekvivalentna sljedećoj nejednakosti*

$$|N_q - q| \leq 2\sqrt{q}, \tag{3.11}$$

gdje je N_q broj tačaka krive E koje pripadaju polju $\mathbb{F}_q$.

Dokaz. Ako je $Z_E(q^{-s}) = 0$, tada je q^s korijen polinoma

$$f(u) = u^2 - a_q u + q.$$

Primjetimo da nejednakost (3.11) važi ako i samo ako je diskriminanta $a_q^2 - 4q$ polinoma $f(u)$ manja ili jednaka od nule. To je ispunjeno ako i samo ako su korijeni u_1 i u_2 polinoma $f(u)$ ili strogo kompleksni ili međusobno jednaki, a ovo važi ako i samo ako je $|u_1| = |u_2|$. Pošto je slobodni član q polinoma $f(u)$ jednak proizvodu $u_1 u_2$, slijedi da su oba korijena u_1 i u_2 po apsolutnoj vrijednosti jednaka $\sqrt{q}$. Dakle, dobili smo da nejednakost (3.11) važi ako i samo ako za svako s za koje je $Z_E(q^{-s})$ važi da je $|q^s| = \sqrt{q}$, a posljednja jednakost upravo znači $\Re(s) = 1/2$. □

Nejednakost (3.11) je poznata kao *Haseova teorema* i u narednom poglavlju će biti izveden njen dokaz, a samim tim će biti dokazana i Rimanova hipoteza za eliptičke krive nad konačnim poljima.

Glava 4

Haseova teorema za eliptičke krive

4.1 Motivacija, formulacija i oznake

U narednom tekstu podrazumijevamo da je $\mathbb{F}_q$ konačno polje koje ima $q = p^m$ elemenata, pri čemu je prost broj p različit od 2 i 3. Ovaj uslov zapravo znači da je karakteristika polja $\mathbb{F}_q$ različita od 2 i 3, tako da možemo posmatrati eliptičke krive u Vajerštrasovom normalnom obliku

$$y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_q), \tag{4.1}$$

gdje je $\Delta = 4a^3 + 27b^2 \neq 0$, što je, podsjetimo se, uslov *glatkosti* ove krive, to jest, uslov koji nam obezbjeđuje da kriva E ima tangentu u svakoj tački. Napomenimo da je uslov glatkosti u algebarskoj geometriji definisan za proizvoljna polja, pa i za $\mathbb{F}_q$, bez korišćenja analize na $\mathbb{R}$ ili $\mathbb{C}$. Primjetimo da smo u *diskriminanti* Δ eliptičke krive E izostavili faktor -16, jer neće imati uticaja na razmatranja u narednom tekstu (vidjeti Definiciju 2.3).

Neka je N_q broj tačaka krive E u polju $\mathbb{F}_q$ i neka je $a_q = q - N_q$. U ovom poglavlju će biti dokazana Haseova teorema, koja predstavlja ekvivalent Rimanove hipoteze za eliptičke krive nad konačnim poljima (vidjeti Teoremu 3.3). Haseova teorema zapravo tvrdi da je izraz a_p ograničen, tačnije da se nalazi između $-2\sqrt{q}$ i $2\sqrt{q}$.

Uvjerimo se u ovo na sljedećem primjeru. Posmatrajmo krivu $y^2 = x^3 + x + 1$ i izračunajmo za nju vrijednosti a_p za prvih 200 prostih brojeva. Vrijednosti za N_p su dobijene uz pomoć matematičkog softvera SAGE, korišćenjem sljedećih komandi:

```
K = GF(p)
E = EllipticCurve(K,[0,0,0,1,1])
E.cardinality()
```

pri čemu umjesto p pišemo prost broj za koji hoćemo da izračunamo N_p, a uređena petorka $[0, 0, 0, 1, 1]$ predstavlja koeficijente eliptičke krive u Vajerštrasovom opštem obliku (2.2).

Vrijednosti a_p za krivu $y^2 = x^3 + x + 1$ za prvih 200 prostih brojeva su date u sljedećoj tabeli. Napomenimo da se u SAGE-u podrazumijeva da kriva E sadrži i beskonačno daleku tačku, tako da ćemo a_p računati kao $a_p = p + 1 - N_p$. Primjetimo da za $p = 2$ i $p = 31$ nemamo vrijednosti a_p jer u tim slučajevima p dijeli diskriminantu pomenute krive, pa ona nije glatka, a samim tim nije ni eliptička kriva.

p	N_p	a_p
2	-	-
3	4	0
5	9	-3
7	5	3
11	14	-2
13	18	-4
17	18	0
19	21	-1
23	28	-4
29	36	-6
31	-	-
37	48	-10
41	35	7
43	34	10
47	60	-12
53	58	-4
59	63	-3
61	50	12
67	56	12
71	59	13
73	72	2
79	86	-6
83	90	-6
89	100	-10
97	97	1
101	105	-3
103	87	17
107	105	3
109	123	-13
113	125	-11
127	126	2
131	128	4
137	126	12
139	126	14
149	136	14
151	154	-2
157	171	-13
163	189	-25
167	144	24
173	172	2
179	180	0
181	190	-8

p	N_p	a_p
191	217	-25
193	201	-7
197	222	-24
199	218	-18
211	223	-11
223	244	-20
227	228	0
229	232	-2
233	237	-3
239	262	-22
241	220	22
251	282	-30
257	249	9
263	260	4
269	294	-24
271	274	-2
277	256	22
281	289	-7
283	264	20
293	268	26
307	301	7
311	315	-3
313	346	-32
317	333	-15
331	342	-10
337	352	-14
347	332	16
349	336	14
353	358	-4
359	351	9
367	346	22
373	363	11
379	360	20
383	370	14
389	374	16
397	373	25
401	432	-30
409	402	8
419	407	13
421	425	-3
431	464	-32
433	436	-2

p	N_p	a_p
439	459	-19
443	433	11
449	468	-18
457	442	16
461	452	10
463	474	-10
467	443	25
479	445	35
487	520	-32
491	504	-12
499	530	-30
503	495	9
509	520	-10
521	492	30
523	524	0
541	531	11
547	525	23
557	562	-4
563	535	29
569	550	20
571	568	4
577	612	-34
587	604	-16
593	579	15
599	597	3
601	632	-30
607	616	-8
613	576	38
617	628	-10
619	634	-14
631	594	38
641	606	36
643	678	-34
647	660	-12
653	668	-14
659	623	37
661	699	-37
673	716	-42
677	676	2
683	649	35
691	675	17
701	735	-33

p	N_p	a_p
709	726	-16
719	698	22
727	691	37
733	717	17
739	778	-38
743	754	-10
751	727	25
757	776	-18
761	744	18
769	809	-39
773	800	-26
787	778	10
797	786	12
809	782	28
811	792	20
821	868	-46
823	776	48
827	852	-24
829	844	-14
839	864	-24
853	876	-22
857	816	42
859	880	-20
863	910	-46
877	825	53

p	N_p	a_p
881	934	-52
883	888	-4
887	841	47
907	947	-39
911	858	54
919	960	-40
929	910	20
937	936	2
941	972	-30
947	962	-14
953	930	24
967	980	-12
971	992	-20
977	987	-9
983	998	-14
991	952	40
997	995	3
1009	1034	-24
1013	966	48
1019	1052	-32
1021	1042	-20
1031	1032	0
1033	1061	-27
1039	1053	-13
1049	1080	-30

p	N_p	a_p
1051	1009	43
1061	1055	7
1063	1104	-40
1069	1042	28
1087	1123	-35
1091	1136	-44
1093	1067	27
1097	1066	32
1103	1101	3
1109	1144	-34
1117	1114	4
1123	1105	19
1129	1120	10
1151	1171	-19
1153	1196	-42
1163	1159	5
1171	1126	46
1181	1188	-6
1187	1200	-12
1193	1150	44
1201	1262	-60
1213	1264	-50
1217	1227	-9
1223	1167	57
1229	1269	-39

Tabela 4.1: Vrijednosti a_p krive $y^2 = x^3 + x + 1$ za prvih 200 prostih brojeva

Sada ćemo dati preciznu formulaciju Haseove teoreme, a u tekstu koji slijedi će biti izveden i njen dokaz.

Haseova teorema. *Neka je E eliptička kriva nad konačnim poljem $\mathbb{F}_q$, gdje je $q = p^m$ (prost broj $p \neq 2, 3$ $m \in \mathbb{N}$) definisana jednačinom* (4.1)*, pri čemu je $\Delta = 4a^3 + 27b^2 \neq 0$. Ako N_q označava broj tačaka na E, to jest broj rješenja jednačine* (4.1) *u $\mathbb{F}_q$, tada važi nejednakost*

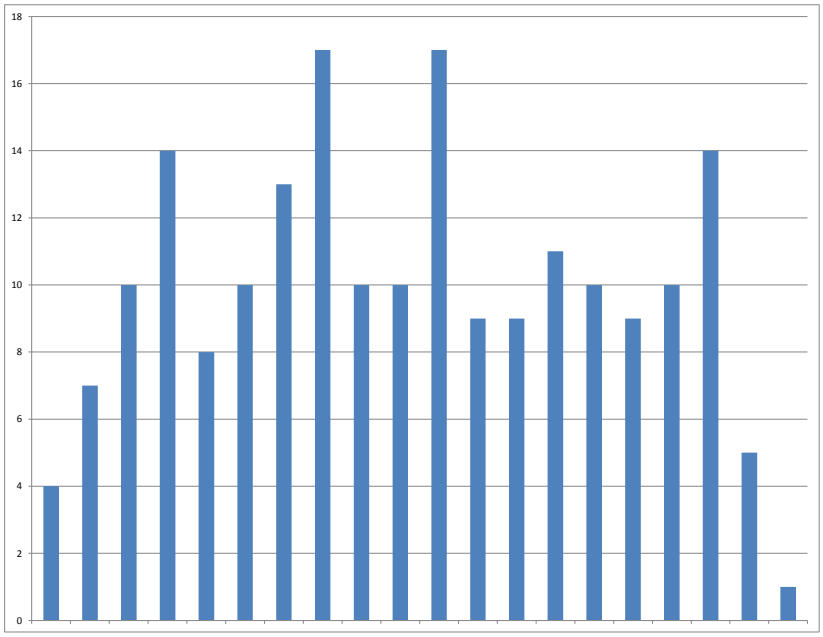
$$|N_q - q| \leq 2\sqrt{q}.$$

Posmatrajući tabelu 4.1 možemo se uvjeriti da Haseova teorema zaista važi za krivu $y^2 = x^3 + x + 1$ za prvih 200 prostih brojeva. To, naravno, nije dokaz teoreme, ali je dovoljno da nas donekle ubijedi da je ona tačna.

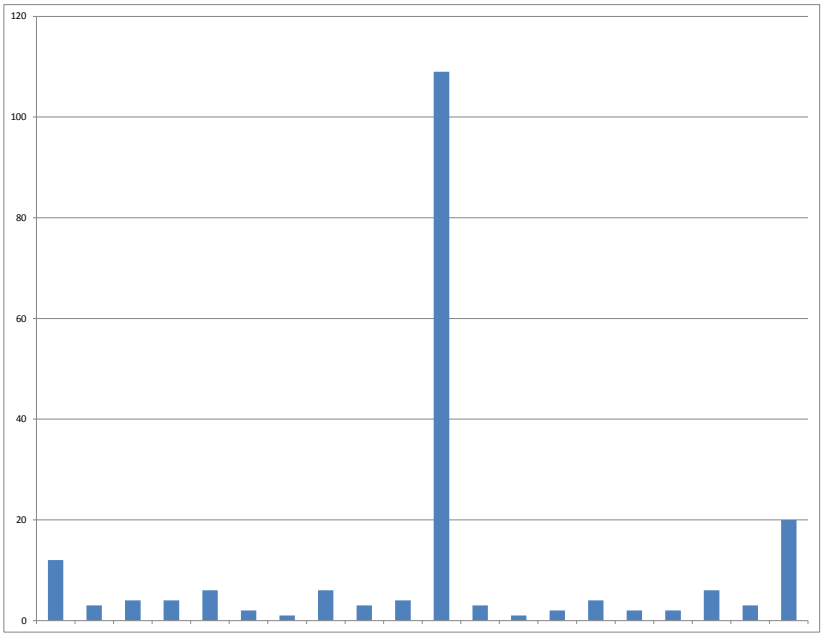
Na kraju ovog odjeljka dodajmo još jednu primjedbu. Posmatrajmo količnik

$$\frac{a_p}{2\sqrt{p}}. \tag{4.2}$$

Na osnovu Haseove teoreme, taj količnik se nalazi u intervalu $[-1, 1]$. Podijelimo interval $[0, 1]$ na podintervale dužine 0.1 i posmatrajmo koliko se vrijednosti količnika (4.2) nalazi u kom od tih intervala. Na osnovu toga možemo napraviti histograme.



Slika 4.1: Histogram za krivu $y^2 = x^3 + x + 1$



Slika 4.2: Histogram za krivu $y^2 = x^3 + 7$

Na slikama 4.1 i 4.2 prikazani su histogrami za neke krive za prvih 200 prostih brojeva, pri čemu su na x-osi predstavljeni intevali $[-1, -0.9)$, $[-0.9, -0, 8), \ldots, [0.9, 1]$.

Fenomen koji se uočava na slikama 4.1 i 4.2 je u skladu sa hipotezom Sato[1]-Tejta.[2] Pošto se količnik (4.2) nalazi u intervalu $[-1,1]$, postoji broj $\theta_p \in [0,\pi]$ takav da je

$$\frac{a_p}{2\sqrt{p}} = \cos\theta_p.$$

Hipoteza Sato-Tejta tvrdi da je za eliptičke krive koje nisu iz klase CM (Complex Multiplication) raspodjela za θ_p data sa

$$\frac{2}{\pi}\sin^2\theta \mathrm{d}\theta.$$

Kriva $y^2 = x^3 + x + 1$ nije iz klase CM, dok kriva $y^2 = x^3 + 7$ jeste. Na histogramima 4.1 i 4.2 možemo uočiti suštinski različito ponašanje raspodjela a_p za ove dvije krive, a za više detalja o ovom fenomenu čitaoca upućujemo na rad [9].

Dokaz Haseove teoreme koji će biti predstavljen u nastavku zasniva se na idejama ruskog matematičara Jurija Ivanoviča Manjina (vidjeti [14]). Počnimo sa razmatranjima opštijeg karaktera koja će nam biti potrebna u dokazu.

4.2 Pripremna tvrđenja

Jedan od važnih elemenata u dokazu Haseove nejednakosti je *Frobenijusovo preslikavanje* Φ i njegove osnovne osobine.

Definicija 4.1. Neka je $\mathbb{F}_q$ neko konačno polje i K bilo koje polje koje ga sadrži. Preslikavanje $\Phi = \Phi_q : K \to K$ definisano sa $\Phi(X) = X^q$ nazivamo Frobenijusovo preslikavanje.

Osnovne osobine Frobenijusovog preslikavanja koje će nam biti potrebne u dokazu Haseove teoreme, date su u sljedećoj teoremi.

Teorema 4.1. *Frobenijusovo preslikavanje $\Phi(X) = X^q$ ima sljedeće osobine:*

(1) $(XY)^q = X^q Y^q$.

(2) $(X+Y)^q = X^q + Y^q$.

(3) $\mathbb{F}_q = \{\alpha \in K \mid \Phi(\alpha) = \alpha\}$.

(4) *Za racionalnu funkciju $\phi(t) \in \mathbb{F}_q(t)$, važi $\Phi(\phi(t)) = \phi(t^q)$.*

Dokaz. (1) Jednakost $(XY)^q = X^q Y^q$ slijedi iz komutativnosti elemenata X i Y.

[1] Mikio Sato (rođen 1928), japanski matematičar.

[2] John Torrence Tate (rođen 1925), američki matematičar, dobitnik Abelove nagrade 2010.

(2) Ovo tvrđenje izvodimo indukcijom po $m = \log_p q$. Za $m = 1$ je $q = p$ i važi

$$(X+Y)^p = \sum_{j=0}^{p} \binom{p}{j} X^j Y^{p-j}.$$

Za $0 < j < p$ imamo

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = p \cdot r$$

za neki prirodan broj r, jer je $\binom{p}{j}$ također prirodan broj, a nijedan član iz imenioca se ne može skratiti sa p. Pošto je $p\alpha = 0$ za svako $\alpha \in K$, zaključujemo da (2) važi. Za $m > 1$, koristeći induktivnu pretpostavku dobijamo

$$(X+Y)^q = ((X+Y)^{p^{m-1}})^p = (X^{p^{m-1}} + Y^{p^{m-1}})^p = X^q + Y^q.$$

(3) Skup $\mathbb{F}_q^*$ nenula elemenata iz $\mathbb{F}_q$ je multiplikativna grupa reda $q-1$. Slijedi da za svaki element $\alpha \in \mathbb{F}_q^*$ važi $\alpha^{q-1} = 1$. Kada uzmemo u obzir i nulu iz $\mathbb{F}_q$ dobijamo da je svaki od q elemenata polja $\mathbb{F}_q$ korijen polinoma $t^q - t = t(t^{q-1} - 1)$ stepena q. Pošto polinom stepena q ne može imati više od q korijena, zaključujemo da se $\mathbb{F}_q$ sastoji upravo od elemenata $\alpha \in K$ koji su korijeni polinoma $t^q - t$. Dakle, važi $\alpha^q = \alpha$, to jest $\Phi(\alpha) = \alpha$.

(4) Direktno slijedi iz (1), (2) i (3). □

Sljedeća teorema predstavlja uopštenje Ojlerovog kriterijuma pa ćemo je nazvati *Ojlerov opšti kriterijum*. Dok u standarnom Ojlerovom kriterijumu figuriše prost broj p, u našoj teoremi se umjesto njega pojavljuje stepen prostog broja $q = p^m$.

Teorema 4.2 (Ojlerov opšti kriterijum)**.** *Neka je $\mathbb{F}_q$ konačno polje sa q elemenata, pri čemu je q neparan, i neka je $\alpha \in \mathbb{F}_q$. Tada važi*

$$\alpha^{\frac{q-1}{2}} = \begin{cases} 1, & \text{ako i samo ako je } \alpha \text{ potpun kvadrat;} \\ -1, & \text{ako i samo ako } \alpha \text{ nije potpun kvadrat.} \end{cases}$$

Dokaz. U dokazu koristimo činjenicu da je multiplikativna grupa $\mathbb{F}_q^*$ konačnog polja $\mathbb{F}_q$ ciklična i reda $q-1$. Tada je $\alpha^{q-1} = 1$, odakle slijedi jednakost

$$\left(\alpha^{\frac{q-1}{2}} - 1\right)\left(\alpha^{\frac{q-1}{2}} - 1\right) = 0.$$

Dakle, za svaki element α iz $\mathbb{F}_q$ važi da je $\alpha^{(q-1)/2} = \pm 1$, tako da je dovoljno dokazati da je $\alpha^{(q-1)/2} = 1$ ako i samo ako je α potpun kvadrat u $\mathbb{F}_q$, odakle će slijediti i dio tvrđenja za elemente koji nisu kvadrati. Pretpostavimo da je α kvadrat u $\mathbb{F}_q$. Neka je $\alpha = \beta^2$, za neko $\beta \in \mathbb{F}_q$. Tada je

$$\alpha^{\frac{q-1}{2}} = \beta^{q-1} = 1.$$

Ostaje još drugi smjer ekvivalencije. Pretpostavimo da važi $\alpha^{(q-1)/2} = 1$. Ova jednačina ima u $\mathbb{F}_q$ najviše $(q-1)/2$ različitih rješenja. Međutim, elemenata koji su potpuni kvadrati

u $\mathbb{F}_q$ takođe ima $(q-1)/2$. (To su svi elementi oblika g^{2k}, gdje je g generator grupe $\mathbb{F}_q^*$ i važi $1 \leq k \leq (q-1)/2$. Primjetimo da su oni međusobno različtiti.) Dakle, pokazali smo ako je $\alpha^{(q-1)/2} = 1$ da je α potpun kvadrat u $\mathbb{F}_q$. Iz prethodnog slijedi da je $\alpha^{(q-1)/2} = -1$ ako i samo ako α nije potpun kvadrat u $\mathbb{F}_q$. □

4.3 Uvrtanje eliptičke krive i pomoćni niz tačaka

Iako je Haseova teorema rezultat koji važi nad poljem $\mathbb{F}_q$, u dokazu ćemo koristiti eliptičke krive definisane nad poljem racionalnih funkcija $\mathbb{F}_q(t)$. Slobodnje govoreći, prelazimo na „veće" polje, koje nam obezbjeđuje veću fleksibilnost. Napomenimo da je ovo ključna ideja u dokazu. Definišimo sada krive koje će nam biti potrebne.

Definicija 4.2. Eliptičku krivu definisanu nad poljem racionalnih funkcija $K = \mathbb{F}_q(t)$ jednačinom

$$\lambda(t)y^2 = x^3 + ax + b, \tag{4.3}$$

gdje je $\lambda(t) = t^3 + at + b$, nazivamo *uvrtanje* od E i označavamo sa E_λ.

U daljem tekstu ćemo često umjesto $\lambda(t)$ pisati samo λ. Jednačina (4.3) nije u standardnom Vajerštrasovom obliku, pa će za nju važiti sljedeće modifikovane formule za sabiranje tačaka, koje se izvode na isti način kao i formule u Teoremi 2.4 iz Glave 2, pa ćemo to izvođenje preskočiti. Navodimo samo formule za x-koordinate, jer će nam samo one biti potrebne. Podsjetimo se, $x(P)$ je oznaka za x-koordinatu tačke P.

1. Ako su $P_1 = (X_1, Y_1)$ i $P_2 = (X_2, Y_2)$ tačke na krivoj E_λ, pri čemu je $P_1 \neq \pm P_2$ i nijedna od tačaka P_1 i P_2 nije O, tada važi

$$x(P_1 + P_2) = \lambda \left(\frac{Y_1 - Y_2}{X_1 - X_2} \right)^2 - (X_1 + X_2). \tag{4.4}$$

2. Ako je $P = (X, Y) \neq O$ i $Y \neq 0$, tada je

$$x(2P) = \frac{(3X^2 + a)^2}{4(X^3 + aX + b)} - 2X. \tag{4.5}$$

Koristićemo osobine Frobenijusovog preslikavanja i uvrtanja eliptičke krive $E_\lambda(K)$ da bismo izbrojali rješenja jednačine $y^2 = x^3 + ax + b$ ($a, b \in \mathbb{F}_q, q = p^m, \Delta = 4a^3 + 27b^2 \neq 0$) u polju $\mathbb{F}_q$. Pri korišćenju Frobenijusovog preslikavanja podrazumijevamo da je odgovarajuće polje K iz definicije 4.1, u stvari $\mathbb{F}_q(t)$.

Očigledno, tačka $(t, 1)$ i njen inverz $-(t, 1) = (t, -1)$ pripadaju krivoj $E_\lambda(K)$. Koristeći osobine (1) i (2) Frobenijusovog preslikavanja iz Teoreme 4.1 dobijamo da i tačka

$$P_0 = (t^q, (t^3 + at + b)^{(q-1)/2})$$

takođe pripada $E_\lambda(K)$.

Definicija 4.3. Neka je $E_\lambda(K)$ uvrtanje eliptičke krive E nad poljem $K = \mathbb{F}_q(t)$. Neka je, zatim, $P_0 = (t^q, (t^3 + at + b)^{(q-1)/2})$ i $n \in \mathbb{Z}$. Tada niz tačaka na eliptičkoj krivoj E_λ definisan sa

$$P_n = P_0 + n(t, 1) \tag{4.6}$$

nazivamo *pomoćni niz tačaka* i označavamo ga sa $\{P_n\}$.

Napomenimo da je $n(t, 1)$ upravo množenje sa n u grupi eliptičke krive. Takođe, primjetimo da je pomoćni niz tačaka u stari koset jedne ciklične podgrupe u toj grupi. U narednom tekstu uvodimo jedan od najvažnijih pojmova koji će nam trebati za dokaz Haseove teoreme.

4.4 Visina n-te tačke pomoćnog niza

Neka je $P_n = (X_n, Y_n)$. Kada je $X_n \neq 0$ možemo X_n napisati u svedenom obliku $X_n = f_n/g_n$, pri čemu su $f_n, g_n \in \mathbb{F}_q[t]$. Prije nego što definišemo visinu n-te tačke pomoćnog niza, navodimo sljedeću lemu koja karakteriše tačke tog niza.

Lema 4.1. *Ako je $P_n = (X_n, Y_n) \neq O$, tada je $X_n \neq 0$. Neka je $X_n(t) = f_n(t)/g_n(t)$, gdje su f_n, g_n iz $\mathbb{F}_q[t]$. Tada je* $\deg f_n > \deg g_n$.

Dokaz. Dokaz izvodimo indukcijom. Tvrđenje je očigledno tačno za $n = 0$. Pretpostavimo da tvrđenje važi za neko n i dokažimo da važi i za $n + 1$. Ako je $P_n = O$, tada je $P_{n+1} = P_n + (t, 1) = O + (t, 1) = (t, 1)$, pa tvrđenje leme važi. Pretpostavimo zato da je $P_n \neq O$. Da bismo dokazali da je stepen brojioca u racionalnoj funkciji $R(t)$ strogo veći od stepena imenioca, izračunaćemo $R(t)$ u $t = \infty$ i pokazati da važi $R(t)|_\infty = \infty$. Neka je $P_{n+1} \neq O$. Pretpostavimo suprotno: ili je $X_n = 0$ ili je $\deg f_{n+1} \leq \deg g_{n+1}$. Tada iz

$$Y_{n+1}^2 = \frac{X_{n+1}^3 + aX_{n+1} + b}{t^3 + at + b}$$

slijedi da je $Y_{n+1}|_\infty = 0$. Pošto je $(X_n, Y_n)+(t, 1) = (X_{n+1}, Y_{n+1})$ važi da je $(X_{n+1}, -Y_{n+1})+(X_n, Y_n)+(t, 1) = O$, pa su tačke $(X_{n+1}, -Y_{n+1})$, (X_n, Y_n) i $(t, 1)$ kolinearne. Dakle, tačka $(X_{n+1}, -Y_{n+1})$ pripada pravoj koja je određena tačkama (X_n, Y_n) i $(t, 1)$, tako da važi jednakost

$$Y_{n+1} = \frac{1 - Y_n}{t - X_n}(t - X_{n+1}) - 1.$$

Koristeći da je $Y_{n+1}|_\infty = 0$, dobijamo

$$0 = Y_{n+1}|_\infty = \left\{ \frac{1 - Y_n}{1 - X_n/t}(1 - X_{n+1}/t) - 1 \right\}\Bigg|_\infty . \tag{4.7}$$

Iz pretpostavke da je ili $X_{n+1} = 0$ ili $\deg f_{n+1} \leq \deg g_{n+1}$ dobijamo da važi $X_{n+1}/t|_\infty = 0$. Stoga, iz (4.7) slijedi

$$\frac{1 - Y_n}{1 - X_n/t}\Bigg|_\infty = 1. \tag{4.8}$$

Kada formulu (4.4) primjenimo na tačke (X_n, Y_n) i $(t, 1)$ dobijamo

$$X_{n+1} = \left(\frac{1-Y_n}{t-X_n}\right)^2 (t^3 + at + b) - t - X_n,$$

odakle slijedi

$$\frac{X_{n+1}}{t} = \left(\frac{1-Y_n}{1-X_n/t}\right)^2 \left(1 + \frac{a}{t^2} + \frac{b}{t^3}\right) - 1 - \frac{X_n}{t}.$$

Koristeći induktivnu pretpostavku za X_n i jednakost (4.8) dobijamo

$$0 = \left.\frac{X_{n+1}}{t}\right|_\infty = \left.\left\{\left(\frac{1-Y_n}{1-X_n/t}\right)^2 \left(1 + \frac{a}{t^2} + \frac{b}{t^3}\right) - 1 - \frac{X_n}{t}\right\}\right|_\infty = -\frac{X_n}{t} \neq 0,$$

što je kontradikcija. Ovim je lema dokazana za $n \leq 0$. Slučaj $n \geq 0$ se izvodi na sličan način. □

Definišimo sada visinu n-te tačke pomoćnog niza.

Definicija 4.4. Neka je $P_n = (X_n, Y_n)$ n-ta tačka pomoćnog niza i neka je, za $X_n \neq 0$, $X_n = f_n(t)/g_n(t)$. Funkciju $d : \mathbb{Z} \to \{0, 1, 2, \ldots\}$ definisanu sa

$$d(n) = d_n = \begin{cases} 0, & \text{ako je } P_n = O; \\ \deg f_n, & \text{inače.} \end{cases}$$

nazivamo visina n-te tačke pomoćnog niza.

U algebarskoj geometriji, visina tačke mjeri, slobodnije rečeno, njenu *aritmetičku kompleksnost.* Intuitivno, složenije tačke imaju i veću visinu. Pošto se za visinu taške uzima veći broj između stepena brojioca i stepena imenioca, Lema 4.1 u stvari objašnjava zašto se u prethodnoj definiciji visine n-te tačke pomoćnog niza uzima samo $\deg f_n$. Dakle, funkcija d_n mjeri *komplikovanost* tačaka na eliptičkoj krivoj.

Navedimo sada jednu jednostavnu posljedicu Leme 4.1.

Posljedica 4.1. *Ako je $P_n \neq O$, tada je $d_n > 0$.*

Dokaz. Najmanji stepen polinoma u imeniocu izraza X_n može biti 0, pa iz Leme 4.1 slijedi da stepen polinoma u brojiocu mora biti strogo veći od 0, što upravo znači da je $d_n > 0$. □

U narednom tekstu ćemo ispitati osnovne osobine funkcije d_n. Prvo ćemo dokazati osnovni identitet za funkciju d_n, odakle će slijediti da je d_n zapravo kvadratni polinom po n, čija će diskriminanta imati centralnu ulogu u dokazu Haseove teoreme. Za dokaz osnovnog identiteta će nam biti potrebna sljedeća lema opštijeg karaktera.

Lema 4.2. *Neka su f i g polinomi nad poljem $\mathbb{K}$, i neka je R racionalna funkcija nad tim poljem, $R \neq 0$, pri čemu je $R^2 g$ polinom nad $\mathbb{K}$. Tada je i Rg polinom nad $\mathbb{K}$. Pretpostavimo da je f nerastavljiv nad $\mathbb{K}$ i da f dijeli $R^2 g$. Tada f dijeli i Rg.*

Dokaz. Neka je $R = f_1/g_1$, gdje su f_1 i g_1 uzajamno prosti polinomi. Tada zbog uslova da je $R^2 g$ polinom važi da $g_1^2 \mid g$. Odatle slijedi $g_1 \mid g$, pa je Rg također polinom. Ako f dijeli f_1, tvrđenje je dokazano, tako da ćemo pretpostaviti da f ne dijeli f_1. Neka je $g = g_1^2 g_2$. Iz $f \mid R^2 g$ slijedi $f \mid f_1^2 g_2$. Kako je f nerastavljiv i kako f ne dijeli f_1, pa ni f_1^2, zaključujemo da f dijeli g_2. Pošto je $Rg = f_1 g_1 g_2$, slijedi da $f \mid Rg$. □

Stav 4.1 (Osnovni identitet)**.** *Neka je $\{P_n\}$ pomoćni niz tačaka definisan jednakošću* (4.6) *i neka je d_n visina n-te tačke pomoćnog niza. Tada važi sljedeća jednakost*

$$d_{n-1} + d_{n+1} = 2d_n + 2. \tag{4.9}$$

Dokaz. Pošto je dokaz relativno dug i tehnički zahtjevan, izvodićemo ga postepeno, korak po korak. Počinjemo sa razmatranjem slučaja kada je neka od tačaka P_{n-1}, P_n, P_{n+1} jednaka O.

Korak 1. Ako je $P_n = O$, tada iz $P_{n+1} = P_n + (t, 1)$ i $P_{n-1} = P_n + (t, -1)$ dobijamo da je $X_{n-1} = X_{n+1} = t$. Dakle, $d_n = 0$, a $d_{n-1} = d_{n+1} = 1$, pa tvrđenje stava važi. Ako je $P_{n-1} = O$, tada je $X_n = (t, 1)$, pa iz formule (4.4) za sabiranje dobijamo

$$X_{n+1} = \frac{t^4 - 2at^2 - 8bt + a^2}{4(t^3 + at + b)}.$$

Lako se provjeri da je ovaj izraz za X_{n+1} u svedenom obliku, tako da imamo $d_{n-1} = 0$, $d_n = 1$ i $d_{n+1} = 4$. Dakle, opet tvrđenje leme važi. Posljednja mogućnost $P_{n+1} = 0$ se razmatra na sličan način kao i za P_{n-1}.

Korak 2. Pretpostavimo sada, bez gubitka opštosti, da nijedna od tačaka P_{n-1}, P_n, P_{n+1} nije jednaka O. U ovom koraku ćemo izvesti formule za X_{n-1} i X_{n+1}. Koristeći formulu (4.4) i svodeći izraz na zajednički imenilac, imamo

$$X_{n-1} = \frac{-(tg_n + f_n)(tg_n - f_n)^2 + (1 + Y_n)^2(t^3 + at + b)g_n^3}{g_n(tg_n - f_n)^2}. \tag{4.10}$$

Pošto tačka (X_n, Y_n) pripada krivoj, važi $(t^3 + at + b)Y_n^2 = (f_n/g_n)^3 + a(f_n/g_n) + b$, to jest

$$g_n^3(t^3 + at + b)Y_n^2 = f_n^3 + af_n g_n^2 + bg_n^3.$$

Koristeći prethodnu formulu, jednakost (4.10) se transformiše na sljedeći način

$$\begin{aligned} X_{n-1} &= \frac{(tg_n + f_n)(tf_n + ag_n) + 2bg_n^2 + 2Y_n(t^3 + at + b)g_n^2}{(tg_n - f_n)^2} \\ &= \frac{R}{(tg_n - f_n)^2}. \end{aligned} \tag{4.11}$$

Slično,

$$\begin{aligned} X_{n+1} &= \frac{-(tg_n+f_n)(tg_n-f_n)^2+(1-Y_n)^2(t^3+at+b)g_n^3}{g_n(tg_n-f_n)^2} \\ &= \frac{(tg_n+f_n)(tf_n+ag_n)+2bg_n^2-2Y_n(t^3+at+b)g_n^2}{(tg_n-f_n)^2} \\ &= \frac{S}{(tg_n-f_n)^2}. \end{aligned} \tag{4.12}$$

Primjetimo da iz $\lambda Y_n^2 = X_n^3 + aX_n + b$ slijedi da je $(Y_n(t^3+at+b)g_n^2)^2$ polinom, pa je i $Y_n(t^3+at+b)g_n^2$ polinom, odakle dobijamo da $R, S \in \mathbb{F}_q[t]$.

Korak 3. Pokažimo sada da ako važi, do na nenula konstantu, da je

$$g_{n-1}g_{n+1} = (tg_n - f_n)^2, \tag{4.13}$$

onda iz te jednakosti slijedi tvrđenje stava. Množenjem izraza za X_{n-1} i X_{n+1} dobijamo

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n-f_n)^4} = \frac{(tf_n-ag_n)^2-4bg_n(tg_n+f_n)}{(tg_n-f_n)^2}. \tag{4.14}$$

Ako bi važila jednakost (4.13), tada bi iz jednakosti (4.14) slijedilo

$$f_{n-1}f_{n+1} = (tf_n-ag_n)^2 - 4bg_n(tg_n+f_n).$$

Iz Leme 4.1 je $\deg f_n > \deg g_n$, pa je $\deg f_n^2 \geq \deg(f_n g_n)$. Zato važi

$$d_{n-1} + d_{n+1} = \deg(f_{n-1}f_{n+1}) = \deg(t^2 f_n^2) = 2d_n + 2.$$

U nastavku ćemo dokazati da važi jednakost (4.13), odakle će slijediti i tvrđenje stava.

Korak 4. Dokažimo da $g_{n-1}g_{n+1} \mid (tg_n - f_n)^2$. Iz (4.14) slijedi da $(tg_n - f_n)^2 \mid RS$. Neka je $(tg_n - f_n)^2 = R_1S_1$, gdje su $S_1, R_1 \in \mathbb{F}_q[t]$, pri čemu važi $R_1 \mid R$ i $S_1 \mid S$. Pošto je

$$X_{n-1} = \frac{R}{(tg_n-f_n)^2} = \frac{R/R_1}{S_1}$$

i pošto je f_{n-1}/g_{n-1} svedeni oblik od X_{n-1} zaključujemo da važi $g_{n-1} \mid S_1$. Slično se dobija da i $g_{n+1} \mid R_1$, odakle slijedi da $g_{n-1}g_{n+1} \mid (tg_n - f_n)^2$.

Ostaje još da se dokaže da $(tg_n - f_n)^2 \mid g_{n-1}g_{n+1}$. Pošto je ovo najsloženiji dio dokaza, podijelićemo ga u tri koraka.

Korak 5. Pretpostavimo suprotno, to jest da $(tg_n - f_n)^2$ ne dijeli $g_{n-1}g_{n+1}$. Neka je f neki nerastavljiv faktor od $tg_n - f_n$ i neka je $v_f(tg_n - f_n)^2$ njegov stepen u faktorizaciji od $(tg_n - f_n)^2$. U ovom koraku dokazaćemo da f dijeli izraze R i S. Pošto smo pretpostavili da $(tg_n - f_n)^2$ ne dijeli $g_{n-1}g_{n+1}$, važi da je

$$v_f(tg_n - f_n)^2 > v_f(g_{n-1}g_{n+1}). \tag{4.15}$$

Prema tome, iz jednakosti (4.14) slijedi

$$f \mid (tf_n - ag_n)^2 - 4bg_n(tg_n + f_n) = T.$$

Dokažimo sada da f dijeli i R i S. Jasno je da mora da dijeli bar jednog od njih, jer dijeli T. Pretpostavimo zato, bez gubitka opštosti da f dijeli R, ali ne i S. Pošto je f_{n+1}/g_{n+1} svedeni oblik za X_{n+1} iz jednakosti (4.12) i koristeći činjenicu da f dijeli $tg_n - f_n$, ali ne dijeli S dobijamo da važi

$$v_f(g_{n+1}) = v_f(tg_n - f_n)^2 > 0. \tag{4.16}$$

Takođe, jasno je da mora biti $v_f(f_{n+1}) = 0$, jer su f_{n+1} i g_{n+1} uzajamno prosti. Na osnovu toga i (4.16), iz jednakosti (4.12) zaključujemo da je

$$0 < v_f(T) = v_f(f_{n-1}) - v_f(g_{n-1}). \tag{4.17}$$

Međutim, pošto su f_{n-1} i g_{n-1} uzajamno prosti, slijedi da ne mogu oba biti djeljiva sa f, što znači da će u jednom od njih stepen od f biti jednak 0. Ali kako je razlika stepena pozitivna, slijedi da je $v_f(g_{n-1}) = 0$. Odatle i iz jednakosti (4.16) slijedi da je

$$v_f(g_{n-1}g_{n+1}) = v_f(tg_n - f_n)^2,$$

što je kontradikcija sa (4.15). Dakle, f dijeli i R i S.

Korak 6. Pokažimo sada da iz prethodnog koraka slijedi da f dijeli t^3+at+b. Jasno je da f ne dijeli g_n, jer bi u suprotnom slijedilo da f dijeli i f_n, pa f_n i g_n ne bi bili uzajamno prosti. Pošto je

$$R = \frac{-(tg_n + f_n)(tg_n - f_n)^2 + (1 + Y_n)^2(t^3 + at + b)g_n^3}{g_n} = \frac{\tilde{R}}{g_n}$$

polinom i f dijeli R, ali ne dijeli g_n, važi da $f \mid \tilde{R}$, odakle slijedi da $f \mid (1+Y_n)^2(t^3+at+b)g_n^3$. (Lako se provjeri da $(1+Y_n)^2(t^3+at+b)g_n^3$ zaista jeste polinom.) Iz Leme 4.2 slijedi da f dijeli $(1+Y_n)(t^3+at+b)g_n^3$. Na sličan način, koristeći da f dijeli S, dobijamo da f dijeli i $(1-Y_n)(t^3+at+b)g_n^3$. Jasno je da f dijeli i zbir ova dva izraza, odakle dobijamo da $f \mid t^3+at+b$, koristeći ponovo činjenicu da f ne dijeli g_n.

Korak 7. Dobijanje kontradikcije. Dijeljenjem izraza T sa $tg_n - f_n$ imamo

$$T = -(tg_n - f_n)[tf_n^2 + (t^3 - 2at - 4b)g_n] + (t^4 - 2at^2 - 8bt + a^2)g_n^2,$$

odakle slijedi da $f \mid t^4 - 2at^2 - 8bt + a^2$. Ali, kako $f \mid t^3 + at + b$ i pošto je

$$(3t^2 + 4a)(t^4 - 2at^2 - 8bt + a^2) - (3t^3 - 5at - 27b)(t^3 + at + b) = \Delta \neq 0,$$

slijedi da f dijeli nenula konstantu $\Delta = 4a^3 + 27b^2$, što je kontradikcija. Dakle, dokazano je da $(tg_n - f_n)^2 \mid g_{n-1}g_{n+1}$, čime je dokaz kompletiran. □

Sada dobijamo sljedeću posljedicu koja nam jasnije opisuje funkciju d_n i koja će imati važnu ulogu u dokazu Haseove nejednakosti.

Posljedica 4.2. *Funkcija visine $d(n)$ je polinom stepena 2 po n. Tačnije, važi jednakost*

$$d(n) = n^2 - (d_{-1} - d_0 - 1)n + d_0. \tag{4.18}$$

Dokaz. Dokaz izvodimo indukcijom po n. Tvrđenje je trivijalno za $n = -1, 0$. Pretpostavimo da važi za $n-1$ i n, pri čemu je $n \geq -1$. Tada iz osnovnog identiteta slijedi

$$\begin{aligned} d_{n+1} &= 2d_n - d_{n-1} + 2 \\ &= 2[n^2 - (d_{-1} - d_0 - 1)n + d_0] \\ &\quad -[(n-1)^2 - (d_{-1} - d_0 - 1)(n-1) + d_0] + 2 \\ &= (n+1)^2 - (d_{-1} - d_0 - 1)(n+1) + d_0. \end{aligned}$$

Dakle, tvrđenje važi za $n+1$, čime je stav dokazan za $n \geq -1$. Slučaj $n \leq 0$ se dokazuje na sličan način. □

4.5 Dokaz Haseove teoreme

Naredna teorema, u kojoj je data veza funkcije visine $d(n)$ sa brojem rješenja jednačine $y^2 = x^3 + ax + b$ u polju $\mathbb{F}_q$ predstavlja glavni element u dokazu Haseove nejednakosti.

Teorema 4.3. *Neka je N_q broj rješenja jednačine $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{F}_q)$ u $\mathbb{F}_q$. Tada važi jednakost*

$$N_q = d_{-1} - 1. \tag{4.19}$$

Dokaz. Pošto je $P_0 \neq (t, 1)$, imamo da je $P_{-1} \neq O$. Neka je $X_{-1} = f_{-1}/g_{-1}$ svedeni oblik racionalne funkcije X_{-1}. Da bismo našli visinu d_{-1}, potrebno je da odredimo X_{-1} i da vidimo koliki je stepen polinoma f_{-1}.

Iz $P_{-1} = P_0 - (t, 1)$ primjenom formule (4.4) slijedi

$$X_{-1} = \frac{(t^3 + at + b)[(t^3 + at + b)^{(q-1)/2} + 1]^2}{(t^q - t)^2} - (t^q + t). \tag{4.20}$$

Svođenjem na zajednički imenilac i korišćenjem osobine (4) Frobenijuosvog preslikavanja dobijamo

$$X_{-1} = \frac{t^{2q+1} + h_{2q}(t)}{(t^q - t)^2}$$

pri čemu je $h_{2q}(t)$ polinom stepena najviše $2q$.

Cilj nam je da skratimo sve zajedničke činioce u posljednjem izrazu. Međutim, posmatrajući jednakost (4.20), vidimo da je dovoljno da izvršimo skraćivanje samo u prvom sabirku tog izraza, pošto je imenilac izraza $t^q + t$ jednak 1. Osobina (3) Frobenijusovog preslikavanja, kao što slijedi iz dokaza, je ekvivalentna činjenici da se $\mathbb{F}_q$ sastoji od q korijena polinoma $t^q - t$. Dakle,

$$t^q - t = \prod_{\alpha \in \mathbb{F}_q} (t - \alpha).$$

Sada, da bismo našli d_{-1}, treba da skratimo zajedničke faktore u razlomku

$$\frac{(t^3+at+b)[(t^3+at+b)^{(q-1)/2}+1]^2}{\prod_{\alpha\in\mathbb{F}_q}(t-\alpha)}. \tag{4.21}$$

Primjetimo da α ne može da poništava oba faktora u brojiocu razlomka (4.21), jer su ti faktori uzajamno prosti, kao i da $(t-\alpha)^2$ ne može da dijeli t^3+at+b, jer je po pretpostavci $\Delta = 4a^3+27b^2 \neq 0$, pa ovaj polinom nema višestrukih nula.

Dakle, jedini faktori iz imenioca koji se mogu skratiti sa nekim faktorima u brojiocu su

- $(t-\alpha)^2$, pri čemu je $(\alpha^3+a\alpha+b)^{(q-1)/2}+1=0$, ili
- $t-\alpha$, pri čemu je $\alpha^3+a\alpha+b=0$.

Neka je k broj faktora oblika $(t-\alpha)^2$, a l broj faktora oblika $t-\alpha$ koji učestvuju u skraćivanju. Pošto su faktori iz prve grupe uzajamno prosti sa faktorima iz druge grupe, zaključujemo da je

$$d_{-1} = 2q+1-2k-l. \tag{4.22}$$

Sa druge strane, neka je α neki element iz $\mathbb{F}_q$ za koga važi $\alpha^3+a\alpha+b=0$. Tada imamo jedno rješenje jednačine $y^2=x^3+ax+b$ u $\mathbb{F}_q$, dato sa $(\alpha,0)$. Međutim, ako je $\alpha^3+a\alpha+b$ jednako nekom nenula kvadratu u $\mathbb{F}_q$, npr. $\alpha^3+a\alpha+b=\beta^2$, $\beta\in\mathbb{F}_q$, $\beta\neq 0$, tada jednačina $y^2=x^3+ax+b$ ima dva rješenja u $\mathbb{F}_q$ data sa (α,β) i $(\alpha,-\beta)$.

Iz Ojlerovog opšteg kriterijuma (Teorema 4.2) slijedi da $\alpha^3+a\alpha+b$ nije kvadrat u $\mathbb{F}_q$ ako i samo ako je $(\alpha^3+a\alpha+b)^{(q-1)/2}=-1$, a ova jednakost upravo važi u slučaju kada član $(t-\alpha)^2$ može da se skrati sa nekim faktorom u brojiocu razlomka (4.21). Dakle, zaključujemo da u $\mathbb{F}_q$ postoji tačno k elemenata koji nisu kvadrati.

Iz prethodnog slijedi da broj rješenja jednačine $y^2=x^3+ac+b$ u $\mathbb{F}_q$ iznosi

$$N_q = 2(q-k-l)+l,$$

odakle se dobija

$$N_q = 2q-2k-l. \tag{4.23}$$

Iz (4.22) i (4.23) slijedi jednakost (4.19), čime je teorema dokazana. □

Sada ćemo, zbog preglednosti, još jednom formulisati Haseovu teoremu za eliptičke krive, a zatim i kompletirati njen dokaz.

Teorema 4.4 (Hase, 1936)**.** *Neka je E eliptička kriva nad konačnim poljem $\mathbb{F}_q$ zadata jednačinom*

$$y^2 = x^3+ax+b \quad (a,b\in\mathbb{F}_q) \tag{4.24}$$

gdje je $q=p^m$ (prost broj $p\neq 2,3$, $m\in\mathbb{N}$) i važi $\Delta = 4a^3+27b^2\neq 0$. Ako N_q označava broj tačaka na E, to jest broj rješenja jednačine (4.24) u $\mathbb{F}_q$, tada važi nejednakost

$$|N_q - q| \leq 2\sqrt{q}. \tag{4.25}$$

Dokaz. Neka su x_1 i x_2 korijeni kvadratnog polinoma

$$d(x) = x^2 - (N_q - q)x + q.$$

Primjetimo da je prethodni polinom isti kao polinom iz Posljedice 4.2, pri čemu smo koristili Teoremu 4.3 da zamjenimo $d_{-1} - d_0 - 1$ sa $N_q - q$ i činjenicu da je $d_0 = q$. Krećemo baš od ovog polinoma zato što od znaka njegove diskriminante zavisi da li će nejednakost (4.25) važiti. Preciznije, nejednakost (4.25) važi ako i samo ako je diskriminanta polinoma $d(x)$ manja ili jednaka od nule.

Pretpostavimo sada da (4.25) ne važi. Tada je diskriminanta $(N_q - q)^2 - 4q$ polinoma $d(x)$ pozitivna. To znači da su x_1 i x_2 različiti realni brojevi. Neka je, recimo, $x_1 < x_2$. Zbog načina na koji je konstruisan, $d(x)$ uzima samo vrijednosti nenegativnih cijelih brojeva na $\mathbb{Z}$, tako da mora postojati neko $n \in \mathbb{Z}$ tako da važi

$$n \leq x_1 < x_2 \leq n + 1. \tag{4.26}$$

(Ako bi postojao neki cijeli broj r između x_1 i x_2, tada bi $d(r)$ bio negativan, što je suprotno tome da $d(x)$ uzima na $\mathbb{Z}$ samo vrijednosti nenegativnih cijelih brojeva.) Pošto su koeficijenti polinoma $d(x)$ iz $\mathbb{Z}$, iz Vijetovih formula imamo da su $x_1 + x_2$ i $x_1 x_2$ takođe iz $\mathbb{Z}$. Kako je

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 \in \mathbb{Z},$$

slijedi da je $(x_1 - x_2)^2$ takođe cijeli broj. Iz (4.26) slijedi da je $(x_1 - x_2)^2 \leq 1$, pa mora biti $(x_1 - x_2)^2 = 1$. Pošto je $x_1 < x_2$ slijedi da važi $x_1 - x_2 = -1$, odakle, imajući u vidu (4.26) zaključujemo da je $x_1 = n$ i $x_2 = n + 1$.

Drugim riječima, mora biti $d_n = d_{n+1} = 0$. Međutim, iz jednakosti $P_{n+1} = P_n + (t, 1)$ slijedi da tačke P_n i P_{n+1} sa krive E ne mogu biti istovremeno jednake tački O. To znači, na osnovu Posljedice 4.1, da je bar jedna od visina d_n, d_{n+1} strogo veća od nule. Dakle, dobili smo kontradikciju, čime je dokaz Haseove teoreme kompletiran. □

Matematičari koji se pominju u radu

Abel (Niels Henrik Abel, 1802-1829), norveški matematičar, poznat po svom radu na jednačini 5. stepena, teoriji grupa i eliptičkim integralima. Takođe, proučavao je i eliptičke funkcije; njegov rad *Ispitivanja eliptičkih funkcija* označava početak teorije dvostruko periodičnih funkcija. *Abelova nagrada* je priznanje za izuzetan naučni doprinos na polju matematike i predstavlja ekvivalent Nobelovoj nagradi.

Ajzenštajn (Gotthold Eisenstein, 1823-1852), njemački matematičar jevrejskog porijekla, poznat po svom kriterijumu o ireducibilnosti polinoma, po Ajzenštajnovim redovima u teoriji modularnih formi i po svojim dokazima zakona reciprociteta.

Artin (Emil Artin, 1898-1962), austrijsko-američki matematičar, jedan od najuticajnijih algebrista u istoriji. Poznat po svom radu u algebarskoj teoriji brojeva, po definiciji *Artinovih L-funkcija* i po *Artinovoj hipotezi* o tim L-funkcijama.

Baharah (Isaak Bacharach, 1854-1942), njemački matematičar jevrejskog porijekla, predavao u Erlangenu, a stradao u koncentracionom logoru. Poznat po teoremi Kejli-Baharaha o presjeku kubnih krivih.

Bejker (Alan Baker, rođen 1939), engleski matematičar poznat po svom radu u teoriji brojeva i teoriji Diofantovih jednačina. Dobio Fildsovu medalju 1970. godine.

Dedekind (Richard Dedekind, 1831-1916), njemački matematičar, poznat po važnom doprinosu algebri (posebno teoriji prstena - Dedekindovi prsteni), algebarskoj teoriji brojeva i zasnivanju realnih brojeva.

Dekart (René Descartes, 1596-1650), francuski matematičar i filozof, poznat po *Dekartovom koordinatnom sistemu* koji je razvio u svom poznatom djelu „Geometrija", filozofiji racionalizma i izreci „Cogito ergo sum."

Diofant (oko 210 - oko 294), starogrčki matematičar iz Aleksandrije, poznat kao „otac algebre", autor poznate knjige *Aritmetika* u kojoj je razmatrao cjelobrojna rješenja algebraskih jednačina, koje su po njemu i nazvane *Diofantove jednačine.*

Dirihle (Johann Peter Gustav Lejeune Dirichlet, 1805-1859), njemački matematičar, poznat kao tvorac analitičke teorije brojeva, dokazao *Dirihleovu teoremu o jedinicama* u prstenima cijelih brojevnih polja, poznat i po mnogim doprinosima analizi, posebno teoriji Furijeovih redova. Dirihleu se pripisuje moderna, formalna definicija funkcije.

Elkis (Noam David Elkies, rođen 1966), američki matematičar, šahovski velemajstor i kompozitor. Poznat po dokazu da eliptičke krive nad $\mathbb{Q}$ imaju beskonačno mnogo *supersingularnih* prostih brojeva, 2006. godine pronašao eliptičku krivu čija grupa racionalnih tačaka ima najveći do sada poznati red.

Eratosten (276 p.n.e. - 194 p.n.e.), starogrčki matematičar, geograf i astronom iz Kirene, poznat kao prva osoba koja je izmjerila obim Zemlje i po *Eratostenovom situ.*

Ferma (Pierre de Fermat, 1601-1665), francuski matematičar, advokat po zanimanju, poznat po svom radu na Diofantovim jednačinama i po *Velikoj Fermaovoj teoremi* koju je dokazao Endrju Vajls[3] 1995. godine i koja se smatra najpoznatijom i najuticajnijom teoremom u matematici.

Frobenijus (Ferdinand Georg Frobenius, 1849-1917), njemački matematičar, poznat po svom doprinosu teoriji grupa i njihovih reprezentacija, teoriji eliptičkih funkcija i algebarskoj teoriji brojeva.

Furije (Joseph Fourier, 1768-1830), francuski matematičar i fizičar, poznat po svom fundamentalnom radu o provođenju toplote, odgovarajućoj parcijalnoj diferencijalnoj jednačini i razvoju *Furijeovih redova* koji su doveli do stvaranja Furijeove analize koja je, osim u matematici, fundamentalna i u mnogim drugim prirodnim i tehničkim naukama.

Galua (Évariste Galois, 1811-1832), francuski matematičar, jedan od najvećih talenata i genija matematike, poznat po svom radu o rješivosti polinomnih jednačina u radikalima, tvorac teorije grupa i Galuaove teorije, poginuo u dvoboju sa 20 godina.

Gaus (Johann Carl Friedrich Gauss, 1777-1855), njemački matematičar, poznat kao „princ matematičara", jedan od najvećih i najuticajnijih matematičara u istoriji, dao značajan doprinos u skoro svim oblastima matematike.

Hase (Helmut Hasse, 1898-1979), njemački matematičar poznat po svom radu u algebarskoj teoriji brojeva, po fundamentalnim rezultatima u teoriji globalnih polja, po *Haseovom principu* u teoriji lokalnih polja i lokalnoj zeta-funkciji.

Hilbert (David Hilbert, 1862-1943), njemački matematičar, jedan od najuticajnijih matematičara u istoriji, poznat po *Hilbertovim problemima*, listi od 23 otvorena problema koji su imali velki uticaj na razvoj matematike, po Hilbertovoj teoremi o bazi, po fundamentalnim doprinosima algebri, algebarskoj teoriji brojeva i geometriji.

Jakobi (Karl Gustav Jacob Jacobi, 1804-1851), njemački matematičar jevrejskog porijekla, poznat po svom radu u teoriji eliptičkih funkcija, teoriji brojeva, Jakobijevoj matrici i njenoj determinanti koja se naziva *Jakobijan.*

Kejli (Arthur Cayley, 1821-1895), britanski matematičar, jedan od osnivača moderne britanske škole čiste matematike. Poznat po radu u projektivnoj geometriji, po Kejli-Hamiltonovoj teoremi iz linearne algebre, po modernoj definiciji pojma grupe i po Kejlijevoj teoremi u teoriji grupa.

Kouts (John Henry Coates, rođen 1945), australijski matematičar poznat po radu na *Ivasava teoriji* i p-adskim L-funkcijama. Zajedno sa Endrju Vajlsom, kome je bio mentor na doktorskim studijama, dokazao specijalni slučaj hipoteze Berča[4] i Svinerton-Dajera[5], koja predstavlja jedan od sedam milenijumskih problema u matematici.

[3]Andrew Wiles (rođen 1953), britanski matematičar.
[4]Bryan John Birch (rođen 1931), britanski matematičar.
[5]Peter Swinnerton-Dyer (rođen 1927), britanski matematičar.

Manjin (Jurij Ivanovič Manjin, rođen 1937), ruski matematičar, poznat po svom radu u algebarskoj geometriji, diofantskoj geometriji, po rezultatima u matematičkoj logici i teorijskoj fizici i po *Manjinovoj hipotezi* o raspodjeli racionalnih tačaka na algebarskim varijetetima.

Mazur (Barry Charles Mazur, rođen 1937), američki matematičar, poznat po radu u diofantskoj geometriji, Mazurovom paradoksu i Mazurovoj torzionoj teoremi, čiji su elementi dokaza bili ključni za Vajlsov dokaz Fermaove posljednje teoreme.

Mordel (Louis Joel Mordell, 1888-1972), britanski matematičar, poznat po dokazu Mordel-Vejlove teoreme i po dokazu multiplikativnosti Ramanudžanove τ-funkcije u teoriji modularnih formi.

Ojler (Leonhard Euler, 1707-1783), švajcarski matematičar i fizičar, jedan od najvećih i najplodnijih matematičara u istoriji, poznat po fundamentalnim rezultatima u raznim oblastima matematike, kao što su matematička analiza, teorija brojeva, teorija grafova, analitička geometrija i primjenjena matematika.

Puason (Siméon Denis Poisson, 1781-1840), francuski matematičar i fizičar, poznat po Puasonovoj parcijalnoj jednačini, Puasonovoj raspodjeli, Puasonovom procesu u teoriji vjerovatnoća i po radu u Furijeovoj analizi (Puasonova sumaciona formula).

Riman (Georg Friedrich Bernhard Riemann, 1826-1866), njemački matematičar, jedan od najvećih matematičara u istoriji, poznat po svojoj hipotezi o nulama zeta-funkciije, koja predstavlja jedan od sedam milenijumskih problema, i po fundamentalnim doprinosima u analizi, diferencijalnoj geometriji i analitičkoj teoriji brojeva.

Šmit (Friedrich Karl Schmidt, 1901-1977), njemački matematičar poznat po značajnim doprinosima u algebri i teoriji brojeva. Ne treba ga miješati sa Erhardom Šmitom (po kome je dobio ime Gram-Šmitov postupak u linearnoj algebri) i Volfgangom Šmitom.

Švarc (Laurent Schwartz, 1915-2002), francuski matematičar jevrejskog porijekla, dobitnik Fildsove medalje 1950. godine, jedan od tvoraca teorije distribucija, poznat po *Švarcovim prostorima.* Ne treba ga miješati sa njemačkim matematičarem Hermanom Švarcom, po kome nosi naziv čuvena nejednakost.

Vajerštras (Karl Theodor Wilhelm Weierstrass, 1815-1897), njemački matematičar, „otac moderne analize", poznat po svojim radovima u varijacionom računu, diferencijalnoj geometriji, po Vajerštrasovom kriterijumu konvergencije funkcionalnog reda i po Vajerštrasovoj $\wp$-funkciji.

Vejl (André Weil, 1906-1998), francuski matematičar jevrejskog porijekla, poznat po svom fundamentalnom radu u teoriji brojeva, algebarskoj geometriji i po vezama između ove dvije discipline, po definiciji prstena adela, po dokazu Rimanove hipoteze za zeta-funkcije pridružene krivama nad konačnim poljima, po *Vejlovim hipotezama*, jedan od lidera grupe „Burbaki."

Vijet (François Viéte, 1540-1603), francuski matematičar poznat po uvođenju simboličke notacije u algebri, po Vijetovim formulama koje povezuju korijene i koeficijente polinoma i po formuli za razvoj broja π.

Zigel (Carl Ludwig Siegel, 1896-1981), njemački matematičar, poznat po značajnom doprinosu teoriji brojeva, posebno teoriji diofantskih aproksimacija, teoriji kvadratnih formi (Zigelova formula mase), diofantskoj geometriji (Zigelova teorema o konačnosti cjelobrojnih tačaka na krivama) i po radu u analitičkoj teoriji brojeva.

Literatura

[1] G. E. Andrews, R. Askey, R. Roy, *Special Functions*, Cambridge University Press, 1999.

[2] J. S. Chahal, *Manin's proof of the Hasse inequality revisited*, Nieuw Arch. Wiskd. **13** (1995) 219-232.

[3] J. S. Chahal, B. Osserman, *The Riemman Hypothesis for Elliptic Curves*, American Mathematical Monthly, vol. 115, **5** (2008) 431-442.

[4] G. Đanković, *Teorija brojeva*, Matematički fakultet, Beograd, 2013.

[5] N. D. Elkies, *The Riemman zeta function and its functional equations*, Lecture notes for Math 259: Introduction to Analytic Number Theory, 2003.

[6] S. Friedl, *An elementary proof of the group law for elliptic curves*, `http://math.rice.edu/friedl/papers/AAELLIPTIC.PDF` (accessed August 23, 2014).

[7] D. Husemöler, *Elliptic Curves* (2nd ed.), Graduate Texts in Mathematics, vol. 111, Springer-Verlag, 2004.

[8] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, American Mathematical Society, Providence, Rhode Island, 2004.

[9] B. Mazur, *Finding meaning in error terms*, Bulletin (New Series) of the American Mathematical Society, vol. 45, **2** (2008) 185-228.

[10] A. Rice, E. Brown, *Why Ellipses Are Not Elliptic Curves*, Mathematics Magazine **85** (2012) 163-176.

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves* (2nd ed.), Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 2009.

[12] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[13] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography* (2nd ed.), Chapman & Hall/CRC, 2008.

[14] Yu. I. Manin, *On cubic congruences to a prime modules*, Izv. Akad. Nauk SSSR Ser. Mat. vol. 20, **5** (1956) 673-678.