Izogenije eliptičkih krivulja

Orlić, Petar

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Petar Orlić

IZOGENIJE ELIPTIČKIH KRIVULJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Filip Najman

Zagreb, srpanj 2021.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

Sadržaj **v**

Uvod **2**

1 Eliptičke krivulje i izogenije **3**
1.1 Osnovno o eliptičkim krivuljama 3
1.2 Izogenije 6

2 Modularne krivulje **11**

3 Mazurov teorem za krivulju $X_0(N)$ **19**
3.1 Redukcija mod p 19
3.2 Galoisove reprezentacije i karakter izogenije 23
3.3 Frobeniusov trag 27
3.4 Dokaz Mazurovog teorema 30

Bibliografija **35**

Uvod

Tema ovog rada su eliptičke krivulje i izogenije između njih. Eliptičke krivulje su posebna vrsta algebarskih krivulja koje imaju svojstvo da se na njima može definirati binarna operacija koja daje strukturu Abelove grupe. Izogenije su racionalna preslikavanja između eliptičkih krivulja koja preslikavaju neutralni element jedne u neutralni element druge krivulje. Teorija eliptičkih krivulja je bogata i razgranata, a mi ćemo u ovom radu spomenuti samo neke od rezultata.

Eliptičke krivulje imaju široku primjenu. Jedna od najvažnijih primjena je u kriptografiji jer omogućuju šifriranje poruka s manjim ključevima u usporedbi s ostalim metodama uz jednaku sigurnost. Mogu se koristiti i za dokazivanje prostosti te faktorizaciju velikih brojeva. Više o tome može se naći u [3].

Vrlo važni objekti u teoriji eliptičkih krivulja su i modularne krivulje. Modularne krivulje kojima ćemo se baviti su $X_0(N)$ i $X_1(N)$. Ispostavlja se da su te krivulje definirane nad $\mathbb{Q}$ te da parametriziraju klase eliptičkih krivulja s nekim dodatnim svojstvom. To je iznimno koristan rezultat koji nam omogućuje da preko modularnih krivulja dokažemo brojna svojstva eliptičkih krivulja.

Centralni teorem u ovom radu je Mazurov teorem za krivulju $X_0(N)$. Taj teorem je 1978. u članku [10] dokazao američki matematičar Barry Mazur, a njegove posljedice su brojne. Jedna od najvažnijih je Mazurov teorem o torziji koji govori kakvu strukturu može imati grupa točaka na eliptičkoj krivulji nad $\mathbb{Q}$. Zanimljivo da je Kenku od 1979. do 1981. u seriji od četiri članka [5, 6, 7, 8] dokazao jači teorem od Mazurovog.

U prvom poglavlju ovog rada definiramo eliptičke krivulje, operaciju zbrajanja točaka i osnovna svojstva te operacije. Nakon toga definiramo i dajemo primjere izogenija te navodimo neka njihova osnovna svojstva koja ćemo koristiti kasnije u radu.

U drugom poglavlju definiramo modularnu grupu, kongruencijske podgrupe i modularne krivulje $X_0(N)$ i $X_1(N)$. Nakon toga navodimo neka njihova svojstva te dokazujemo da točke na modularnim krivuljama parametriziraju klase eliptičkih krivulja. Za kraj poglavlja dajemo primjere modularnih krivulja koji ilustriraju njihov značaj u teoriji eliptičkih krivulja.

U trećem poglavlju, koje je posvećeno Mazurovom teoremu, obrađujemo rezultate potrebne za dokaz teorema.

Prva tema poglavlja su redukcije mod p. To je vrlo opširna tema i mi ćemo je samo dotaknuti. Uz već poznate pojmove dobre i loše redukcije, definirat ćemo potencijalno dobru i potencijalno multiplikativnu redukciju. Nakon toga ćemo definirati Atkin-Lehnerovu involuciju te dokazati rezultat koji će nam trebati u dokazu teorema.

Onda prelazimo na Galoisove reprezentacije i karakter izogenije. Nakon što definiramo te pojmove, pokazat ćemo u kakvoj su vezi te izreći neka njihova svojstva. Također ćemo definirati Frobeniusov trag eliptičke krivulje i iskazati rezultat koji ga povezuje s karakterom izogenije. Na kraju poglavlja dokazujemo Mazurov teorem.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Lieje-vih algebri.

Poglavlje 1

Eliptičke krivulje i izogenije

U ovom poglavlju definirat ćemo eliptičke krivulje i navesti njihova osnovna svojstva. Zatim ćemo definirati izogenije eliptičkih krivulja i iskazati rezultate koji će nam biti korisni za daljnja razmatranja.

1.1 Osnovno o eliptičkim krivuljama

Definicija 1.1.1. *Eliptička krivulja je glatka projektivna algebarska krivulja genusa* 1 *na kojoj postoji posebna točka* $\mathcal{O}$*.*

Svaka eliptička krivulja nad poljem K se može zadati dugom Weierstrassovom jednadžbom

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.1}$$

gdje su $a_1, a_2, a_3, a_4, a_6 \in K$, $\Delta(E) \neq 0$, a ako je K karakteristike različite od 2 i 3 i kratkom Weierstrassovom jednadžbom

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1.2}$$

gdje su $a, b \in K$ i $\Delta(E) = -16(4a^3 + 27b^2) \neq 0$.

Vrijednost $\Delta(E)$ je diskriminanta krivulje E. Primijetimo da je za krivulju E zadanu kratkom Weierstrassovom jednadžbom $\Delta(E) \neq 0$ ako i samo ako polinom $f(x) = x^3 + ax + b$ nema višestrukih nultočaka. Formula za diskriminantu krivulje zadane dugom Weierstrassovom jednadžbm je dosta duga i kompliciranа i stoga nije ovdje navedena. Može se naći npr. u [3, Poglavlje 1.2].

Odsada nadalje za eliptičku krivulju zadanu dugom ili kratkom Weierstrassovom jednadžbom smatrat ćemo da je $\mathcal{O} = [0, 1, 0]$ (trivijalno se vidi da je ta točka stvarno na krivulji).

Definicija 1.1.2. *Neka je E eliptička krivulja nad K zadana jednadžbom (1.1). Skup svih K-racionalnih točaka krivulje E je skup svih točaka projektivne ravnine $\mathbb{P}^2(K)$ koje zadovoljavaju jednadžbu (1.1). Taj skup ćemo označavati s $E(K)$.*

Primijetimo da je $\mathcal{O}$ K-racionalna točka svake eliptičke krivulje i uz to jedina točka u beskonačnosti koja se nalazi na krivulji. Naime, neka se neka takva točka $[X, Y, 0]$ nalazi na krivulji. Tada uvrštavanjem u jednadžbu dobivamo $X = 0$ što znači da je $[X, Y, 0] = [0, Y, 0] = [0, 1, 0]$. Ova diskusija opravdava naziv "točka u beskonačnosti" za točku $\mathcal{O}$.

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe [3]. Tu operaciju ćemo zvati zbrajanje i označavati s $+$, a definiramo je na sljedeći način:

Neka su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke na krivulji E zadanoj kratkom Weierstrassovom jednadžbom (1.2). Tada je $P + Q = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = -y_1 + \lambda(x_1 - x_3),$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + a}{2y_1} & \text{ako je } x_2 = x_1. \end{cases}$$

Definicija se lako proširuje na točke u projektivnom prostoru.

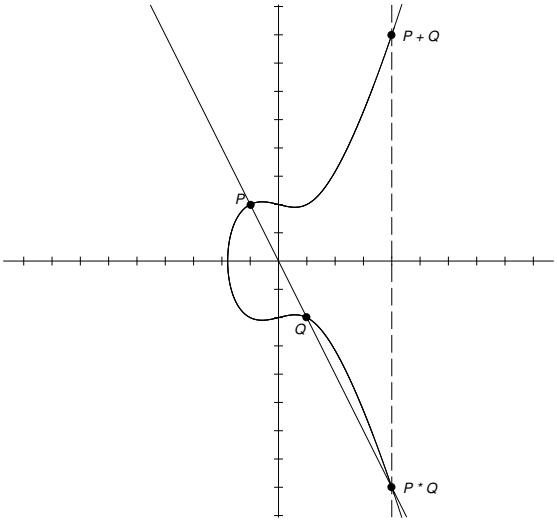
Ovdje se može pojaviti problem ako je $y_1 = 0$ u slučaju $x_2 = x_1$. Međutim, prelaskom na projektivni prostor dobivamo da je u tom slučaju $P + Q = \mathcal{O}$.

Za ovako definiranu operaciju zbrajanja nije odmah jasno da je zatvorena, odnosno da točka $P + Q$ stvarno leži na krivulji E. Dokaz zatvorenosti je računski i može se naći u [13, Poglavlje III.2].

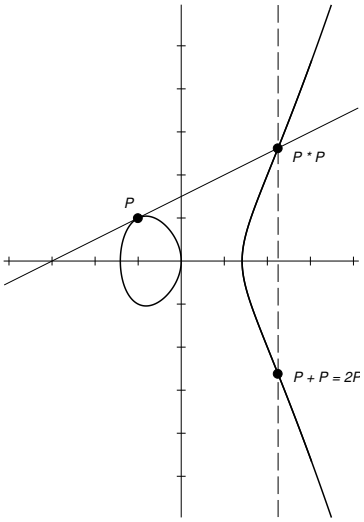
Kao što smo već rekli, uz ovakvo zbrajanje točke na eliptičkoj krivulji čine Abelovu grupu s neutralnim elementom $\mathcal{O}$. Inverzni element točke $P = (x, y)$ je $-P = (x, -y)$, komutativnost se lako provjerava, a za asocijativnost treba malo više posla. Dokaz asocijativnosti se također može naći u [13, Poglavlje III.2].

Ovako definirano zbrajanje ima i geometrijsku interpretaciju kad je krivulja E definirana nad $\mathbb{R}$. Naime, neka su P i Q različite točke na $E(\mathbb{R})$. Pravac kroz P i Q siječe krivulju $E(\mathbb{R})$ u točno 3 točke, pri čemu jedna od njih može biti i $\mathcal{O}$. Ako treću točku presjeka označimo s $P * Q$, tada se može pokazati da je $P + Q = -(P * Q)$. Slično tome, točku $2P = P + P$ možemo dobiti kao inverz točke koju dobijemo kao presjek $E(\mathbb{R})$ i tangente na krivulju u P.

Na sljedećim slikama je prikazano upravo opisano zbrajanje točaka na $E(\mathbb{R})$ (slike preuzete iz [3]).



Slika 1.1: Zbrajanje različitih točaka



Slika 1.2: Zbrajanje točke same sa sobom

Osim prethodno spomenute diskriminante, još jedna važna veličina eliptičke krivulje je i njezina j-invarijanta. Za krivulju E zadanu kratkom Weierstrassovom jednadžbom pripadna j-invarijanta dana je formulom

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Kao ni za diskriminantu, ni za j-invarijantu nećemo navesti formulu kad je krivulja zadana dugom Weierstrassovom jednadžbom.

j-invarijanta ima brojna korisna svojstva, npr. može se pokazati da su dvije eliptičke krivulje izomorfne nad $\overline{K}$ ako i samo ako imaju istu j-invarijantu. To svojstvo i druge činjenice vezane uz j-invarijantu ćemo kasnije detaljnije proučiti.

Za kraj ovog odjeljka definirat ćemo torzijsku podgrupu eliptičke krivulje. Nećemo još iskazati njezina svojstva, već ćemo to napraviti u idućem odjeljku nakon što dokažemo tvrdnje potrebne za dokaz tih svojstava.

Definicija 1.1.3. *Neka je E eliptička krivulja i $m \in \mathbb{N}$. m-torzijska podgrupa E, koju označavamo $E[m]$, je skup točaka E reda m, tj.*

$$E[m] = \{P \in E : mP = \mathcal{O}\}.$$

Torzijska podgrupa E, koju označavamo E_{tors}, je skup točaka E konačnog reda, tj.

$$E_{tors} = \bigcup_{m=1}^{\infty} E[m].$$

Ako je E definirana nad K, tada $E(K)_{tors}$ označava skup točaka konačnog reda u $E(K)$.

U slučaju kad je K polje algebarskih brojeva, Mordell-Weilov teorem kaže da je grupa $E(K)$ konačno generirana. Kako je svaka konačno generirana Abelova grupa izomorfna produktu oblika $\mathbb{Z}^r \times \mathbb{Z}/k_1\mathbb{Z} \times \ldots \times \mathbb{Z}/k_m\mathbb{Z}$ gdje $k_1 \mid \ldots \mid k_m$, dobivamo $E(K) \cong E(K)_{tors} \times \mathbb{Z}^r$ za neki $r \geq 0$. Taj r zovemo rang $E(K)$ i označavamo $\text{rank}(E(K))$.

Kad je $K = \mathbb{Q}$, vrijedi i jači rezultat. Mazur je 1978. godine dokazao da postoji točno 15 mogućih torzijskih grupa za eliptičke krivulje nad $\mathbb{Q}$ [3]. To su grupe

$$\mathbb{Z}/k\mathbb{Z} : k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$$
$$\text{i } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} : k = 2, 4, 6, 8.$$

1.2 Izogenije

Definicija 1.2.1. *Neka su E_1 i E_2 eliptičke krivulje. Izogenija iz E_1 u E_2 je morfizam $\phi : E_1 \to E_2$ za koji vrijedi $\phi(\mathcal{O}) = \mathcal{O}$. Krivulje E_1 i E_2 definirane nad K su izogene ako postoji $\overline{K}$ algebarsko zatvorenje K i ne-nul izogenija definirana nad $\overline{K}$ iz E_1 u E_2. Također, označimo sa $\text{Hom}(E_1, E_2)$ skup svih izogenija iz E_1 u E_2 i neka je $\text{End}(E) = \text{Hom}(E, E)$.*

Primijetimo da smo u definiciji rabili pojam morfizma koji nismo ovdje definirali. Precizna definicija dana je u [13, poglavlje I.3]. Intuitivno, morfizam je racionalno preslikavanje između algebarskih krivulja koje ne mora nužno biti definirano u svakoj točki krivulje, ali se u točkama u kojima nije definirano može proširiti množenjem s multiplikatorom.

Pogledajmo sad neke primjere izogenija.

Primjer 1.2.2. *Neka je $K = \mathbb{Q}$ i E krivulja dana jednadžbom $y^2 = x^3 - x$. Definirajmo $\phi : E \to E$, $\phi(x, y) = (-x, iy)$ pri čemu je $i^2 = -1$. Tada je ϕ izogenija definirana nad $\mathbb{Q}[i]$ iz E u E.*

Primjer 1.2.3. *Neka je E eliptička krivulja nad K dana jednadžbom $y^2 = x^3 + ax + b$. Za $m \in \mathbb{Z}$ Definirajmo $[m] : E \to E$, $[m](P) = mP$.*

Iz definicije trivijalno slijedi da je $[m](\mathcal{O}) = \mathcal{O}$ za sve $m \in \mathbb{Z}$ te da je $[0]$ nul-izogenija. Iz formula za zbrajanje točaka na krivulji induktivno možemo zaključiti da je za $m > 0$ $[m]$ racionalno preslikavanje definirano nad K. Također, za $m < 0$ preslikavanje $[m]$ je kompozicija $[-m]$ i preslikavanja $(x, y) \to (x, -y)$ te stoga racionalno kao kompozicija dva racionalna preslikavanja.

Dakle, za svaki $m \in \mathbb{Z}$ preslikavanje $[m]$ je izogenija definirana nad K iz E u E.

Primjer 1.2.4. *Neka su $a, b \in \mathbb{Q}$ takvi da vrijedi $b \neq 0$ i $r = a^2 - 4b \neq 0$. Promotrimo eliptičke krivulje zadane jednadžbama*

$$E_1 : y^2 = x^3 + ax^2 + bx,$$
$$E_2 : Y^2 = X^3 - 2aX^2 + rX$$

i definirajmo preslikavanja između tih krivulja

$$\phi : E_1 \to E_2, (x, y) \to \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$
$$\hat{\phi} : E_2 \to E_1, (X, Y) \to \left(\frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2} \right).$$

Može se provjeriti da su ϕ i $\hat{\phi}$ izogenije definirane nad $\mathbb{Q}$ te da vrijedi $\hat{\phi} \circ \phi = [2]$ na E_1 i $\phi \circ \hat{\phi} = [2]$ na E_2 [13]. Izogenije ϕ i $\hat{\phi}$ su primjer dualnih izogenija, pojma vrlo važnog za teoriju eliptičkih krivulja.

Napomenimo da je "biti izogen" relacija ekvivalencije na skupu eliptičkih krivulja nad K. Dokaz te tvrdnje koristi prethodno spomenute dualne izogenije i može se naći u [13, Teorem III.6.1].

Izogenije možemo zbrajati i komponirati po točkama. Definirajmo prvo zbrajanje izogenija.

Definicija 1.2.5. *Neka su E_1, E_2 eliptičke krivulje definirane nad K i $\phi, \psi : E_1 \to E_2$ izogenije definirane nad $\overline{K}$. Tada je izogenija $\phi + \psi : E_1 \to E_2$ definirana na sljedeći način:*

$$(\phi + \psi)(P) = \phi(P) + \psi(P), \forall P \in E_1.$$

Lako se vidi da je $(\phi + \psi)(\mathcal{O}) = \mathcal{O}$. Iz činjenice da su ϕ i ψ morfizmi te formula za zbrajanje točaka na krivulji zaključujemo da je $\phi + \psi$ morfizam iz E_1 u E_2. Dakle, $\phi + \psi$ je izogenija iz E_1 u E_2 definirana nad $\overline{K}$.

Definirajmo sad i kompoziciju izogenija.

Definicija 1.2.6. *Neka su E_1, E_2 eliptičke krivulje definirane nad K i $\phi : E_1 \to E_2$, $\psi : E_2 \to E_3$ izogenije definirane nad $\overline{K}$. Tada je izogenija $\psi \circ \phi : E_1 \to E_3$ definirana na sljedeći način:*

$$(\psi \circ \phi)(P) = \psi(\phi(P)), \forall P \in E_1.$$

Opet se lako vidi da je $(\psi \circ \phi)(\mathcal{O}) = \mathcal{O}$. Kako kompozicijom morfizama opet dobivamo morfizam, zaključujemo da je $\psi \circ \phi$ morfizam iz E_1 u E_3. Dakle, $\psi \circ \phi$ je izogenija iz E_1 u E_3 definirana nad $\overline{K}$.

Uz ovako definirane operacije $\mathrm{Hom}(E_1, E_2)$ postaje Abelova grupa, a $\mathrm{End}(E)$ prsten. Pri tome je za izogeniju ϕ njoj suprotna izogenija $-\phi = [-1] \circ \phi$.

Od svih svojstava jedino netrivijalno svojstvo grupa i prstena koje treba provjeriti je lijeva distributivnost komponiranja prema zbrajanju. To svojstvo ćemo uskoro dokazati u ovom poglavlju.

Sad kad smo definirali kompoziciju izogenija možemo definirati i pojam izomorfizma eliptičkih krivulja.

Definicija 1.2.7. *Neka su E_1 i E_2 eliptičke krivulje nad K. Izogenija $\phi : E_1 \to E_2$ definirana nad $\overline{K}$ je izomorfizam krivulja ako postoji izogenija $\psi : E_2 \to E_1$ definirana nad $\overline{K}$ za koju vrijedi $\psi \circ \phi = [1]_{E_1}$ i $\phi \circ \psi = [1]_{E_2}$. Krivulje E_1 i E_2 su izomorfne ako postoji bar jedan izomorfizam između njih.*

Iz definicije se odmah vidi da je "biti izomorfan" relacija ekvivalencije na skupu eliptičkih krivulja nad K. Također, vrijedi i prije spomenuta tvrdnja da su eliptičke krivulje definirane nad K izomorfne nad $\overline{K}$ ako i samo ako imaju istu j-invarijantu. Dokaz te tvrdnje je dan u [13, Propozicija III.1.4].

Za krivulje zadane kratkom Weierstrassovom jednadžbom vrijedi i jača tvrdnja: jedini izomorfizmi između takvih krivulja su oblika $(x, y) \to (u^2x, u^3y)$ za neki $u \in \overline{K}^\times$. Lako se vidi da takva preslikavanja čuvaju j-invarijantu.

Primjer 1.2.8. *Krivulje $y^2 = x^3 - 4x$ i $y^2 = x^3 - 25x$ obje imaju $j = 1728$. Prva od njih ima konačno mnogo racionalnih točaka, dok ih druga ima beskonačno mnogo (točka $(-4, 6)$ je beskonačnog reda) [3].*

Kad bi te krivulje bile izomorfne nad $\mathbb{Q}$, taj bi izomorfizam, kao racionalno preslikavanje, dao bijekciju između racionalnih točaka na njima što nije moguće. Dakle, ove krivulje nisu izomorfne nad $\mathbb{Q}$, ali jesu nad $\mathbb{Q}(\sqrt{10})$. Izomorfizam nad $\mathbb{Q}(\sqrt{10})$ je $(x, y) \to (u^2x, u^3y)$, $u = \frac{\sqrt{10}}{2}$.

Izogenije imaju i brojna druga zanimljiva svojstva. Ovdje ćemo nabrojiti samo neka od njih.

Teorem 1.2.9. *Svaka ne-nul izogenija je surjektivna.*

Dokaz. Ovaj teorem slijedi iz sličnog teorema za općenite morfizme algebarskih krivulja. Dokaz tog teorema nije nimalo trivijalan i može se naći u [4]. □

Teorem 1.2.10. *Neka je $\phi : E_1 \to E_2$ izogenija. Tada vrijedi $\phi(P+Q) = \phi(P)+\phi(Q)$ za sve $P, Q \in E_1$.*

Dokaz. Dokaz se može naći u [13, Teorem II.2.3]. □

Korolar 1.2.11 (lijeva distributivnost)**.** *Neka su $\phi_1, \phi_2 : E_1 \to E_2$ i $\psi : E_2 \to E_3$ izogenije. Tada vrijedi $\psi \circ (\phi_1 + \phi_2) = \psi \circ \phi_1 + \psi \circ \phi_2$.*

Dokaz. Za sve točke P na krivulji E_1 vrijedi

$$(\psi \circ (\phi_1 + \phi_2))(P) = \psi((\phi_1 + \phi_2)(P)) = \psi(\phi_1(P) + \phi_2(P)) =$$

$$= \psi(\phi_1(P)) + \psi(\phi_2(P)) = (\psi \circ \phi_1 + \psi \circ \phi_2)(P)$$

što znači da je $\psi \circ (\phi_1 + \phi_2) = \psi \circ \phi_1 + \psi \circ \phi_2$. □

Korolar 1.2.12. *Neka je $\phi : E_1 \to E_2$ ne-nul izogenija. Tada je $\ker \phi = \phi^{-1}(\mathcal{O})$ konačna grupa.*

Dokaz. Kako je zbog Teorema 1.2.10 ϕ homomorfizam grupa, slijedi da je $\ker \phi$ podgrupa E_1. Također, to je i konačan skup zbog [13, Propozicija II.2.6a]. □

Također, vrijedi i svojevrsni obrat ove tvrdnje.

Teorem 1.2.13. *Neka je E krivulja definirana nad K i Φ konačna podgrupa E. Tada postoji krivulja E' nad $\overline{K}$ i izogenija $\phi : E \to E'$ t.d. $\ker \phi = \Phi$. Štoviše, ako je Φ G_K-invarijantna, tada se E' i ϕ mogu definirati nad K.*

Dokaz. Tvrdnja slijedi iz [13, Propozicija III.4.12] i [13, Opaska III.4.13.2]. □

Vratimo se sad na torzijske podgrupe. Kako je $E[m]$ zapravo jezgra izogenije $[m]$, korolar 1.2.12 nam kaže da je ta grupa konačna. Međutim, u slučaju kad je E definirana nad poljem K karakteristike 0 (npr. $K = \mathbb{Q}$) vrijedi i nešto jača tvrdnja. Ako sa $\#E[m]$ označimo broj elemenata $E[m]$, tada vrijedi

$$\#E[m] = m^2.$$

Dokaz te tvrdnje može se naći u [13, Teorem III.4.10c]. Pomoću nje može se dokazati još jača tvrdnja za $E[m]$.

Propozicija 1.2.14. *Neka je E eliptička krivulja nad poljem K karakteristike 0. Tada vrijedi*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Dokaz. Kako je $\#E[m] = m^2$, grupa $E[m]$ je izomorfna produktu oblika $\mathbb{Z}/k_1\mathbb{Z} \times \ldots \times \mathbb{Z}/k_n\mathbb{Z}$ pri čemu $k_1 \mid \ldots \mid k_n$ i $k_1 \ldots k_n = m^2$. Također, svi elementi $E[m]$ su reda m pa je $k_n \leq m$.

Za svaki d djelitelj m isto tako vrijedi $\#E[d] = d^2$. Ako uzmemo $d = k_1$, iz prethodne faktorizacije dobivamo da u $E[m]$ postoji točno k_1^n elemenata reda k_1. To znači da mora biti $n = 2$ i $k_1 = k_2 = m$ čime je tvrdnja propozicije dokazana. □

Također, iz činjenica da je $E[m] = \ker[m]$ i $[m]$ izogenija definirana nad K slijedi da je $E[m]$ G_K-invarijantna.

Za kraj ovog poglavlja definirat ćemo pojam N-izogenije.

Definicija 1.2.15. *Neka je E krivulja definirana nad K. Kažemo da E ima N-izogeniju nad K ako postoje krivulja E' nad K i izogenija $\phi : E \to E'$ nad K t.d. je* $\ker \phi$ *ciklička G_K-invarijantna grupa reda N.*

Iz Teorema 1.2.13 slijedi da je za krivulju E postojanje N-izogenije nad K ekvivalentno s postojanjem cikličke G_K-invarijantne grupe reda N. Ovaj zaključak će nam biti koristan u dokazu Mazurovog teorema.

Poglavlje 2

Modularne krivulje

U ovom poglavlju definirat ćemo modularne krivulje $X_0(N)$ i $X_1(N)$ te objasniti vezu točaka na modularnim krivuljama i eliptičkih krivulja.

Definicija 2.0.1. *Modularna grupa* $\mathrm{SL}_2(\mathbb{Z})$ *je grupa* 2×2 *matrica s cjelobrojnim koeficijentima i determinantom* 1*, tj.*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Definirajmo preslikavanje

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (z) = \frac{az + b}{cz + d}, z \in \mathbb{C} \cup \{\infty\}.$$

Nije teško provjeriti da je ovako definirano preslikavanje djelovanje grupe $\mathrm{SL}_2(\mathbb{Z})$ na $\mathbb{C} \cup \{\infty\}$.

Nadalje, neka je $\mathcal{H} = \{z \in \mathbb{C}, Im(z) > 0\}$ gornja poluravnina skupa $\mathbb{C}$ i $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ proširena gornja poluravnina. Dokažimo da su skupovi $\mathcal{H}$ i $\mathcal{H}^*$ zatvoreni na djelovanje grupe $\mathrm{SL}_2(\mathbb{Z})$ na gore definiran način.

Dakle, neka je $z \in \mathcal{H}^*$, imamo 2 slučaja:

- $z \in \mathcal{H} \implies z = x + yi$, $x \in \mathbb{R}$, $y \in \mathbb{R}^+$. Vrijedi

$$\frac{az + b}{cz + d} = \frac{a(x + yi) + b}{c(x + yi) + d} = \frac{(a(x + yi) + b)(c(x - yi) + d)}{(cx + d)^2 + (cy)^2}.$$

Slijedi da je imaginarni dio jednak

$$\frac{ay(cx + d) - cy(ax + b)}{(cx + d)^2 + (cy)^2} = \frac{y(ad - bc)}{(cx + d)^2 + (cy)^2} = \frac{y}{(cx + d)^2 + (cy)^2} > 0$$

pa smo dobili $\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z) \in \mathcal{H}$.

- $z \in \mathbb{P}^1(\mathbb{Q})$

  Kako su a,b,c,d cijeli brojevi, lako se vidi da vrijedi $\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z) \in \mathbb{P}^1(\mathbb{Q})$.

Definicija 2.0.2. *Neka je $N \in \mathbb{N}$ i $\Gamma(N)$ podgrupa $\mathrm{SL}_2(\mathbb{Z})$ definirana na sljedeći način:*

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Kongruencijska podgrupa modularne grupe $\mathrm{SL}_2(\mathbb{Z})$ je svaka podgrupa $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$ koja sadrži $\Gamma(N)$ za neki $N \in \mathbb{N}$.

Ako je Γ kongruencijska podgrupa $\mathrm{SL}_2(\mathbb{Z})$, tada Γ na gore opisan način djeluje na $\mathcal{H}^*$ i možemo definirati kvocijentni prostor $\Gamma \setminus \mathcal{H}^* = \{\ \Gamma x : x \in \mathcal{H}^+\ \}$. Može se pokazati da takav prostor ima prirodnu strukturu Riemannove plohe [2].

Sad ćemo navesti dvije kongruencijske podgrupe koje će nam biti potrebne za definiciju modularnih krivulja $X_0(N)$ i $X_1(N)$.

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Iz definicije odmah slijedi da su $\Gamma_0(N)$ i $\Gamma_1(N)$ stvarno kongruencijske podgrupe modularne grupe $\mathrm{SL}_2(\mathbb{Z})$.

Teorem 2.0.3. *Postoje (otvorene) krivulje $Y_1(N)$ i $Y_0(N)$ definirane nad $\mathbb{Q}$ t.d.*

$$Y_1(N)(\mathbb{C}) \cong \Gamma_1(N) \setminus \mathcal{H} = \{\ \Gamma_1(N)x : x \in \mathcal{H}\ \},$$

$$Y_0(N)(\mathbb{C}) \cong \Gamma_0(N) \setminus \mathcal{H} = \{\ \Gamma_0(N)x : x \in \mathcal{H}\ \}.$$

Za njihova upotpunjenja $X_1(N)$ i $X_0(N)$ vrijedi

$$X_1(N)(\mathbb{C}) \cong \Gamma_1(N) \setminus \mathcal{H}^* = \{\ \Gamma_1(N)x : x \in \mathcal{H}^*\ \},$$

$$X_0(N)(\mathbb{C}) \cong \Gamma_0(N) \setminus \mathcal{H}^* = \{\ \Gamma_0(N)x : x \in \mathcal{H}^*\ \}.$$

Dokaz. Vidjeti [2, Poglavlje 2]. □

Skupove $X_1(N)\setminus Y_1(N)$ i $X_0(N)\setminus Y_0(N)$ zovemo kaspovi krivulja $X_1(N)$ i $X_0(N)$. Primijetimo da su kaspovi reprezentirani klasama $\Gamma_1(N)\setminus\mathbb{P}^1(\mathbb{Q})$ i $\Gamma_0(N)\setminus\mathbb{P}^1(\mathbb{Q})$.

Sljedeća propozicija će nam dati odgovor na pitanje koliko kaspova imaju krivulje $X_0(N)$ i $X_1(N)$. Za dokaz te propozicije trebat ćemo ovu pomoćnu lemu.

Lema 2.0.4. *Neka je N prost broj i $k\in\{1,\dots,N-1\}$. Tada postoje jedinstveni $a\in\{1,\dots,N-1\}$, $b\in\{0,\dots,N-2\}$ za koje vrijedi $ka=bN+1$.*

Dokaz. Kako su k i N relativno prosti, znamo da postoje $a',b'\in\mathbb{Z}$ t.d. $ka'=b'N+1$. Tada vrijedi i $k(a'+cN)=(b'+ck)N+1$ za sve $c\in\mathbb{Z}$.

Postoji jedinstveni c za koji je $a'+cN\in\{0,1,\dots,N-1\}$. Primijetimo da ne može biti $a'+cN=0$ jer bi tada vrijedilo $(b'+ck)N+1=0$ što nije moguće.

Definirajmo $a=a'+cN$, $b=b'+ck$. Iz prethodne diskusije znamo da je $a\in\{1,\dots,N-1\}$ te da vrijedi $ak=bN+1$. Zato je $b=\frac{ak-1}{N}\in\left\langle\frac{k-1}{N},\frac{(k-1)(N-1)}{N}\right\rangle\implies b\in\{0,\dots N-2\}$ (lako se provjeri da je $(k-1)(N-1)\leq N(N-2)$).

Dakle, ovako definirani a,b zadovoljavaju uvjete leme. Pretpostavimo sad da i neki drugi a_0, b_0 zadovoljavaju uvjete leme. Tada vrijedi $(a-a_0)k=(b-b_0)N$ iz čega slijedi $N\mid a-a_0$. Stoga je $a=a_0$ iz čega izravno dobivamo i $b=b_0$.

Dakle, takvi a,b su jedinstveni. □

Propozicija 2.0.5. *Neka je N prost broj. Tada krivulja $X_0(N)(\mathbb{C})$ ima točno 2, a $X_1(N)(\mathbb{C})$ točno $N-1$ kaspova.*

Dokaz. Dokažimo prvo tvrdnju za $X_0(N)(\mathbb{C})$. Nije teško vidjeti da vrijedi

$$\Gamma_0(N)\infty=\left\{\frac{a}{c}:a,c\in\mathbb{Z},M(a,N)=1,N\mid c\right\},$$
$$\Gamma_0(N)0=\left\{\frac{b}{d}:b,d\in\mathbb{Z},M(d,N)=1\right\}$$

iz čega slijedi da je $\{\Gamma_0(N)\infty,\ \Gamma_0(N)0\}$ particija skupa $\mathbb{P}_1(\mathbb{Q})$. To znači da $X_0(N)(\mathbb{C})$ ima točno 2 kaspa: $\Gamma_0(N)\infty$ i $\Gamma_0(N)0$.

Sad ćemo dokazati tvrdnju za $X_1(N)(\mathbb{C})$. Iz prethodne leme dobivamo da za svaki $k\in\{1,\dots,N-1\}$ postoje jedinstveni $x_k\in\{1,\dots,N-1\}$ i $y_k\in\{0,\dots,N-2\}$ t.d. $kx_k=y_kN+1$. Odmah vidimo da vrijedi $y_{x_k}=y_k$.

Iz definicije grupa $X_0(N)$ i $X_1(N)$ sada lako dobivamo

$$\Gamma_0(N)=\Gamma_1(N)\left\{\begin{bmatrix}k & y_k\\ N & x_k\end{bmatrix}:k=1,\dots,N-1\right\}$$

pa (uz podatak o kaspovima $X_0(N)(\mathbb{C})$) zaključujemo da su kaspovi $X_1(N)(\mathbb{C})$ točno

$$\left\{\Gamma_1(N)\begin{bmatrix}k & y_k\\ N & x_k\end{bmatrix}\infty : k=1,\dots,N-1\right\}\cup\left\{\Gamma_1(N)\begin{bmatrix}k & y_k\\ N & x_k\end{bmatrix}0 : k=1,\dots,N-1\right\}=$$
$$=\left\{\Gamma_1(N)\frac{k}{N} : k=1,\dots,N-1\right\}\cup\left\{\Gamma_1(N)\frac{y_k}{x_k} : k=1,\dots,N-1\right\}.$$

Može se provjeriti da vrijedi $\Gamma_1(N)\frac{k}{N}=\Gamma_1(N)\frac{N-k}{N}$, $\Gamma_1(N)\frac{y_k}{x_k}=\Gamma_1(N)\frac{y_{N-k}}{x_{N-k}}$ te da su to sve jednakosti klasa (detalji ostavljeni čitatelju) iz čega slijedi da $X_1(N)(\mathbb{C})$ ima točno $\frac{N-1}{2}+\frac{N-1}{2}=N-1$ kaspova. □

Pomoću sljedećih teorema ćemo objasniti vezu $\mathbb{Q}$-racionalnih točaka na modularnim krivuljama i eliptičkih krivulja nad $\mathbb{Q}$.

Teorem 2.0.6. *Svaka točka $Q\in Y_0(N)(\mathbb{Q})$ parametrizira klasu $[E,C]$, gdje je E eliptička krivulja nad $\mathbb{Q}$ i C ciklička $G_{\mathbb{Q}}$-invarijantna podgrupa reda N. (Definiramo da je $(E_1,C_1)\sim(E_2,C_2)$ ako postoji izomorfizam $\phi:E_1\to E_2$ t.d. $\phi(C_1)=C_2$.)*

Dokaz. Definirajmo grupe

$$H=\left\{\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}\in GL_2(\mathbb{Z}/N\mathbb{Z}) : b\in\mathbb{Z}/N\mathbb{Z}, a,d\in(\mathbb{Z}/N\mathbb{Z})^\times\right\},$$

$$H_0=\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\cap H.$$

Nije teško pokazati da vrijedi

$$\Gamma_0(N)=\{A\in\mathrm{SL}_2(\mathbb{Z}) : (A \mod N)\in H_0\}.$$

Kako vrijedi $-I\in H$, možemo primijeniti [12, Teorem 21] i zaključiti da Q parametrizira klasu $[E,\alpha]_H$, pri čemu je E eliptička krivulja definirana nad $\mathbb{Q}$ i $\alpha: E[N]\to(\mathbb{Z}/N\mathbb{Z})^2$ izomorfizam.

Po [12, Definicija 1], $(E_1,\alpha_1)\sim_H(E_2,\alpha_2)$ ako postoje $\phi:E_1\to E_2$ izomorfizam i $h\in H$ t.d. $\alpha_1=h\circ\alpha_2\circ\phi$ (nije teško provjeriti da je to relacija ekvivalencije).

Dokažimo da je to ekvivalentno sa sljedećom tvrdnjom: postoji $\psi:E_1\to E_2$ izomorfizam t.d. $\psi(\langle P_1\rangle)=\langle P_2\rangle$, gdje je $P_i=\alpha_i^{-1}(1,0)$ za $i=1,2$.

Pretpostavimo prvo da vrijedi $(E_1,\alpha_1)\sim_H(E_2,\alpha_2)$. Tada postoje $\phi:E_1\to E_2$ izomorfizam i $h\in H$ t.d. $\alpha_1=h\circ\alpha_2\circ\phi\implies\phi\circ\alpha_1^{-1}=\alpha_2^{-1}\circ h^{-1}$.

Neka je $h^{-1}=\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}$. Tada vrijedi

$$\phi(P_1)=\phi(\alpha_1^{-1}(1,0))=\alpha_2^{-1}(\begin{bmatrix}a & b\\ 0 & d\end{bmatrix}(1,0))=\alpha_2^{-1}(a,0)=aP_2$$

$$\implies \phi(\langle P_1\rangle) = \langle P_2\rangle$$

jer je $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Zaključujemo da je ϕ traženi izomorfizam.

Obrnuto, pretpostavimo da postoji $\psi : E_1 \to E_2$ izomorfizam t.d. $\psi(\langle P_1\rangle) = \langle P_2\rangle$. Iz toga slijedi $\psi(\alpha_1^{-1}(1,0)) = \alpha_2^{-1}(a,0)$ za neki $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Također, vrijedi i $\psi(\alpha_1^{-1}(0,1)) = \alpha_2^{-1}(b,d)$ za neke $b, d \in \mathbb{Z}/N\mathbb{Z}$.

Kako je ϕ izomorfizam, matrica $h = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ je regularna pa zaključujemo da vrijedi

$$\psi \circ \alpha_1^{-1} = \alpha_2^{-1} \circ h \implies \alpha_1 = h^{-1} \circ \alpha_2 \circ \psi$$

čime je i ovaj smjer dokazan.

Grupa $\langle P_1\rangle$ je ciklička reda N jer je $P_1 = \alpha_1^{-1}(1,0)$ reda N u $E[N]$. Dokažimo da je ta grupa $G_\mathbb{Q}$-invarijantna.

Iz [12, Teorem 21] dobivamo $\overline{\rho}_{E,N}(G_\mathbb{Q}) \subset H$ pa je djelovanje svakog elementa $G_\mathbb{Q}$ na $\langle P_1\rangle$ reprezentirano djelovanjem neke matrice iz H na $\langle(1,0)\rangle$. Kako vrijedi

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}(1,0) = (a,0) = a(1,0) \in \langle(1,0)\rangle$$

zaključujemo da je $\langle P_1\rangle$ $G_\mathbb{Q}$-invarijantna.

Dakle, dokazali smo da svaka točka $Q \in Y_0(N)(\mathbb{Q})$ parametrizira klasu $[E, C]$, gdje je E eliptička krivulja nad $\mathbb{Q}$ i C ciklička $G_\mathbb{Q}$-invarijantna podgrupa reda N čime je teorem dokazan.

□

Napomena 2.0.7. *[12, Teorem 21] je dokazan samo u slučaju kad $j(E) \neq 0, 1728$. Teorem vrijedi i kada $j(E) = 0$ ili $j(E) = 1728$, ali je tada dokaz kompliciraniji.*

Teorem 2.0.8. *Svaka točka $Q \in Y_1(N)(\mathbb{Q})$ parametrizira klasu $[E, P]$, gdje je E eliptička krivulja nad $\mathbb{Q}$ i P $\mathbb{Q}$-racionalna točka na E reda N. (Definiramo da je $(E_1, P_1) \sim (E_2, P_2)$ ako postoji izomorfizam $\phi : E_1 \to E_2$ t.d. $\phi(P_1) = P_2$).*

Dokaz. Dokaz će biti vrlo sličan dokazu teorema za $Y_0(N)$. Definirajmo grupe

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}) : b \in \mathbb{Z}/N\mathbb{Z}, d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\},$$

$$H_0 = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H.$$

Nije teško pokazati da vrijedi

$$\Gamma_1(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) : (A \mod N) \in H_0\}.$$

Kako vrijedi $-I \notin H$, možemo primijeniti [12, Teorem 22] i zaključiti da Q parametrizira klasu $[E, \alpha]_H$, pri čemu je E eliptička krivulja definirana nad $\mathbb{Q}$ i $\alpha : E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$ izomorfizam.

Slično kao u prošlom dokazu, možemo dokazati da je $(E_1, \alpha_1) \sim_H (E_2, \alpha_2)$ ako i samo ako postoji $\psi : E_1 \to E_2$ izomorfizam t.d. $\psi(P_1) = P_2$, gdje je $P_i = \alpha_i^{-1}(1, 0)$ za $i = 1, 2$.

Da bismo dokazali da je P_1 $\mathbb{Q}$-racionalna, dovoljno je vidjeti da je $P_1^\sigma = P_1$ za svaki $\sigma \in G_\mathbb{Q}$. Međutim, Iz [12, Teorem 22] dobivamo $\overline{\rho}_{E,N}(G_\mathbb{Q}) \subset H$ pa je djelovanje svakog $\sigma \in G_\mathbb{Q}$ na P_1 reprezentirano djelovanjem neke matrice iz H na $(1, 0)$. Kako vrijedi

$$\begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} (0, 1) = (0, 1),$$

zaključujemo da je $P_1^\sigma = P_1$ za svaki $\sigma \in G_\mathbb{Q}$ pa smo dokazali racionalnost točke P_1.

Dakle, svaka točka $Q \in Y_1(N)(\mathbb{Q})$ parametrizira klasu $[E, P]$, gdje je E eliptička krivulja nad $\mathbb{Q}$ i P $\mathbb{Q}$-racionalna točka na E reda N čime je teorem dokazan.

□

Napomena 2.0.9. *[12, Teorem 22] je također dokazan samo u slučaju kad* $j(E) \neq 0, 1728$. *Teorem vrijedi i kada* $j(E) = 0$ *ili* $j(E) = 1728$, *ali je tada dokaz kompliciraniji.*

Zanimljivo je da tvrdnje iz ova dva teorema vrijede i ako $\mathbb{Q}$ zamijenimo s općenitim poljem algebarskih brojeva K ili njegovim algebarskim zatvorenjem $\overline{K}$. Dokazi takvih poopćenih teorema za K mogu se naći u [12], a za $\overline{K}$ u [2].

Primjer 2.0.10. *Neka je* E *eliptička krivulja nad* K *i* $P \in E(K)$ *točka takva da vrijedi* $P, 2P, 3P \neq 0$. *Može se dokazati da tada postoji zamjena koordinata kojom se dobiva krivulja u Tateovoj normalnoj formi*

$$E_{u,v} : Y^2 + uXY + vY = X^3 + vX^2$$

gdje su $u, v \in K$ *i koja točku* P *šalje u točku* $(0, 0) \in E_{u,v}(K)$ *istog reda. Također,* $(0, 0)$ *je točka reda* 5 *ako i samo ako je* $u = v + 1$ *te se u tom slučaju klase* $[E, P]$ *i* $[E_{v+1,v}, (0, 0)]$ *podudaraju.*

Iz ovoga zaključujemo da svaka $\mathbb{Q}$*-racionalna točka na krivulji* $u = v + 1$ *parametrizira krivulju* $E_{v+1,v}$ *na kojoj je točka* $(0, 0)$ *reda* 5. *Dakle, modularna krivulja* $X_1(5)$ *se može zadati jednadžbom* $u = v + 1$ *pri čemu točka* $(v + 1, v)$ *parametrizira klasu* $[E_{v+1,v}, (0, 0)]$.

Odmah vidimo da je genus krivulje $X_1(5)$ *jednak* 0. *Također, kako je* j*-invarijanta krivulje* $E_{v+1,v}$ *dana formulom [12]*

$$j = \frac{(v^4 + 12v^3 + 14v^2 - 12v + 1)^3}{-v^5(v^2 + 11v - 1)},$$

možemo zaključiti da su 4 *kaspa krivulje* $X_1(5)$ *elementi skupa*

$$\left\{(v+1,v) : v = \infty, 0, \frac{11 \pm 5\sqrt{5}}{2}\right\}.$$

Primjer 2.0.11. *Slično kao u slučaju* $N = 5$*, u slučaju* $N = 11$ *može se pokazati da je krivulja* $X_1(11)$ *dana jednadžbom* $y^2 - y = x^3 - x$ *pri čemu točka* $(s,t) \in X_1(11)(K)$ *parametrizira klasu* $[E_{s,t}, (0,0)]$ *gdje je krivulja* $E_{s,t}$ *dana jednadžbom*

$$E_{s,t} : Y^2 + (st + t - s^2)XY + s(s-1)(s-t)t^2Y = X^3 + s(s-1)(s-t)X^2.$$

Genus krivulje $X_1(11)$ *je jednak* 1*, a* $X_1(11)(\mathbb{Q})$ *sadrži samo* 5 *točaka. Preciznije, vrijedi [12]*

$$X_1(11) = \{\mathcal{O}, (0,0), (0,1), (1,0), (1,1)\} \cong \mathbb{Z}/5\mathbb{Z}.$$

Te racionalne točke čine 5 *od* 10 *kaspova krivulje* $X_1(11)$ *što znači da ne postoji eliptička krivulja nad* $\mathbb{Q}$ *koja sadrži racionalnu točku reda* 11*.*

Preostali kaspovi su definirani nad ciklotomskim poljem $\mathbb{Q}(\omega_{11})$ *i dani su jednadžbama [12]*

$$t^5 - 18t^4 + 35t^3 - 16t^2 - 2t + 1 = 0, s = \frac{-3t^4 + 52t^3 - 74t^2 + 17t + 10}{11}.$$

Iz prethodnih teorema i primjera vidimo da brojne tvrdnje vezane za eliptičke krivulje možemo dokazati promatrajući samo jednu, modularnu krivulju. To nam pokazuje i sljedeća primjena Mazurova teorema za krivulju $X_1(N)$.

Teorem 2.0.12 (Mazur)**.** *Neka je* N *prirodan broj takav da je genus* $X_1(N)$ *veći od* 0 *(tj.* $N = 11$ *ili* $N \geq 13$*). Tada* $X_1(N)(\mathbb{Q})$ *sadrži samo kaspove.*

Dokaz. Dokaz se može naći u [9]. □

Korolar 2.0.13. *Neka je* $N = 11$ *ili* $N \geq 13$ *prirodan broj. Tada ne postoji eliptička krivulja nad* $\mathbb{Q}$ *koja sadrži* $\mathbb{Q}$*-racionalnu točku reda* N*.*

Dokaz. Kad bi postojao takav par (E, P), tada bi po teoremu 2.0.8 krivulja $X_1(N)(\mathbb{Q})$ sadržavala točku koja nije kasp. Međutim, to nije moguće po Mazurovom teoremu. □

Poglavlje 3

Mazurov teorem za krivulju $X_0(N)$

Neka je N prirodan broj. Primjeri eliptičkih krivulja nad $\mathbb{Q}$ za koje postoji ciklička N-izogenija nad $\mathbb{Q}$ su poznati za sljedeće vrijednosti N:

N	g	v	N	g	v	N	g	v
$\leq$10	0	∞	11	1	3	27	1	1
12	0	∞	14	1	2	37	2	2
13	0	∞	15	1	4	43	3	1
16	0	∞	17	1	2	67	5	1
18	0	∞	19	1	1	163	13	1
25	0	∞	21	1	4			

Tablica 3.1: Vrijednosti N za koje su poznate nekaspidalne točke na $X_0(N)(\mathbb{Q})$ (tablica preuzeta iz [10])

U tablici g označava genus krivulje $X_0(N)$, a v broj nekaspidalnih točaka na $X_0(N)(\mathbb{Q})$.

Mazurov teorem kaže da, u slučaju kad je N prost, krivulja $X_0(N)(\mathbb{Q})$ sadrži samo kaspove osim u slučajevima iz ove tablice. Ekvivalentno, ne postoji eliptička krivulja nad $\mathbb{Q}$ koja ima N-izogeniju nad $\mathbb{Q}$ za N prost osim u gornjim slučajevima.

Prije samog dokaza dokazat ćemo neke pomoćne rezultate.

3.1 Redukcija mod p

Redukcija mod p je vrlo važan pojam u teoriji eliptičkih krivulja. Ovdje podrazumijevamo da je čitatelj upoznat s pojmovima dobre te loše multiplikativne i aditivne redukcije mod p (definicije se mogu naći npr. u [3]).

Neka je K polje, R prsten cijelih u K i M maksimalni ideal u R. Tada za eliptičke krivulje nad K možemo definirati redukciju mod M na sličan način kao redukcije mod p. U slučaju kada je K lokalno polje, ideal M je jedinstven pa možemo govoriti o redukciji nad K.

Definicija 3.1.1. *Neka je E eliptička krivulja nad lokalnim poljem K. Kažemo da E ima potencijalno dobru redukciju nad K ako postoji konačno proširenje K'/K t.d. E ima dobru redukciju nad K'. Analogno se definira potencijalno multiplikativna redukcija.*

U ovoj definiciji smo spomenuli redukciju nad K'. To ima smisla jer je K' kao konačno proširenje lokalnog polja K također lokalno polje.

Htjeli bismo definirati potencijalno dobru i potencijalno multiplikativnu redukciju mod p za eliptičke krivulje nad $\mathbb{Q}$. Međutim, $\mathbb{Q}$ nije lokalno polje pa to ne možemo napraviti odmah. Zato ćemo sada definirati polje p-adskih brojeva koje će nam to omogućiti.

Definicija 3.1.2. *Neka je p prost broj. Prsten cijelih p-adskih brojeva $\mathbb{Z}_p$ je skup*

$$\{(a_1, a_2, \ldots) : a_n \in \mathbb{Z}/p^n\mathbb{Z}, a_{n+1} \equiv a_n \pmod{p^n}\}.$$

Operacije zbrajanja i množenja se definiraju po točkama. Nije teško provjeriti da je $\mathbb{Z}_p$ integralna domena pa možemo definirati polje p-adskih brojeva $\mathbb{Q}_p$ kao polje razlomaka $\mathbb{Z}_p$.

Cijeli p-adski broj $(a_0, a_1, \ldots) \in \mathbb{Z}_p$ je invertibilan ako i samo ako $a_0 \neq 0$ pa zaključujemo da je $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

Prsten $\mathbb{Z}_p$ je karakteristike 0 te se prsten cijelih brojeva $\mathbb{Z}$ prirodno ulaže u $\mathbb{Z}_p$ t.d. $k \to (\overline{k}, \overline{k}, \ldots)$. To znači da se i $\mathbb{Q}$ prirodno ulaže u $\mathbb{Q}_p$ na sljedeći način:

$$\frac{k_1}{k_2} \to \frac{(\overline{k_1}, \overline{k_1}, \ldots)}{(\overline{k_2}, \overline{k_2}, \ldots)}$$

pa svaku eliptičku krivulju nad $\mathbb{Q}$ možemo shvatiti kao eliptičku krivulju nad $\mathbb{Q}_p$.

Lako se provjeri da su svi ne-nul ideali u $\mathbb{Z}_p$ oblika (p^n) (dokaz se može naći u [11]). To znači da je $\mathbb{Z}_p$ domena glavnih ideala te da je jedinstveni maksimalni ideal jednak (p) pa je $\mathbb{Q}_p$ lokalno polje.

Dakle, preko polja p-adskih brojeva možemo definirati pojmove potencijalno dobre i potencijalno multiplikativne redukcije mod p za krivulje nad $\mathbb{Q}$. Štoviše, za krivulju E nad $\mathbb{Q}$, tip redukcije mod p (dobra, multiplikativna, aditivna) se poklapa s tipom redukcije nad $\mathbb{Q}_p$.

Propozicija 3.1.3. *Neka je K lokalno polje i E eliptička krivulja nad K.*

(a) Neka je K'/K konačno proširenje. Ako E ima dobru ili multiplikativnu redukciju nad K, tada ima istu redukciju nad K'.

(b) Postoji konačno proširenje K'/K t.d. E ima dobru ili multiplikativnu redukciju nad K.

(c) E ima potencijalno dobru redukciju ako i samo ako je $j(E) \in R$, gdje je R skup cijelih brojeva u K.

Dokaz. Dokaz se može naći u [13, Propozicija VII.5.4, Propozicija VII.5.5]. □

Gornja propozicija nam kaže da svaka krivulja ima ili potencijalno dobru ili potencijalno multiplikativnu redukciju te da koji od ta dva tipa redukcije ima ne ovisi o proširenju K'.

Također, iz (c) dijela prethodne propozicije dobivamo da je za točku $[(E, C_N)] \in X_0(N)(\mathbb{Q})$ tip redukcije (potencijalno dobra ili potencijalno multiplikativna) isti za svaku krivulju E iz klase (naime, sve te krivulje imaju istu j-invarijantu).

Odsada nadalje ćemo, osim ako drugačije ne naznačimo, pod tipom redukcije eliptičke krivulje E nad poljem K smatrati potencijalno dobru i potencijalno multiplikativnu redukciju.

Bez dokaza navodimo sljedeću važnu propoziciju.

Propozicija 3.1.4. *Neka su E i E' eliptičke krivulje nad lokalnim poljem K i $\phi : E \to E'$ izogenija. Tada te krivulje imaju isti tip redukcije nad K.*

Sad ćemo definirati Atkin-Lehnerove involucije koje će nam biti potrebne za dokaz propozicije na kraju ovog odjeljka.

Definicija 3.1.5. *Preslikavanje $\omega_N : X_0(N) \to X_0(N)$, $\omega_N(\Gamma_0(N)\tau) = \Gamma_0(N)\frac{-1}{N\tau}$ se zove Atkin-Lehnerova involucija.*

Da bi ova definicija bila dobra, treba provjeriti da je ovo preslikavanje dobro definirano. Prvo primijetimo da je $\dfrac{-1}{N\tau} = \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} \tau$. Ako je $A = \begin{bmatrix} a & b \\ cN & d \end{bmatrix} \in \Gamma_0(N)$, tada vrijedi

$$\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} A \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}^{-1} = \frac{1}{N} \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} \begin{bmatrix} a & b \\ cN & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix} =$$

$$= \begin{bmatrix} d & -c \\ -bN & a \end{bmatrix} \in \Gamma_0(N).$$

To znači da za svaku matricu $A \in \Gamma_0(N)$ postoji matrica $B \in \Gamma_0(N)$ za koju vrijedi $\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} A = B \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}$ iz čega slijedi

$$\omega_N(\Gamma_0(N)A\tau) = \Gamma_0(N) \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} A\tau = \Gamma_0(N) \begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix} \tau = \omega_N(\Gamma_0(N)\tau).$$

Ovaj račun pokazuje da je preslikavanje ω_N zaista dobro definirano. Lako se vidi da je $\omega_N \circ \omega_N = \mathrm{id}_{X_0(N)}$ pa je to stvarno involucija. Nadalje, iz definicije izravno slijedi $\omega_N(\Gamma_0(N)0) = \Gamma_0(N)\infty$ i $\omega_N(\Gamma_0(N)\infty) = \Gamma_0(N)0$ što znači da ω_N preslikava jedan kasp grupe $\Gamma_0(N)$ u drugi.

Involuciju ω_N smo definirali preko djelovanja na poluravnini. Naravno da nas zanima i kako djeluje na klasama $[(E, C_N)]$. Prisjetimo se da smo u prvom poglavlju rekli da postoji krivulja E' i izogenija $\phi : E \to E'$ t.d. je $\ker \phi = C_N$. Jedna takva krivulja je E/C_N koja sadrži podgrupu $E[N]/C_N$.

Primijetimo da je $E[N]/C_N$ ciklička (jer je $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$) i Galois-invarijantna (jer je $E[N]$ Galois-invarijantna). Može se pokazati da involucija klasu $[(E, C_N)]$ šalje u klasu $[(E/C_N, E[N]/C_N)]$.

Također, može se pokazati i da je Atkin-Lehnerova involucija racionalno preslikavanje, što implicira da komutira s redukcijom mod p, tj. nije važno u kojem poretku radimo te operacije.

Da se involucija dobro ponaša s obzirom na redukcije vidimo i iz sljedeće propozicije.

Propozicija 3.1.6. *Neka je $x = [(E, C_N)] \in X_0(N)(\mathbb{Q})$ i $\omega_N(x) = [(E', C'_N)] \in X_0(N)(\mathbb{Q})$. Tada krivulje E i E' imaju isti tip redukcije mod p za svaki prosti broj p.*

Dokaz. Postoji izogenija $\phi : E \to E'$ t.d. $\ker \phi = C_N$. Kako su E i E' izogene, prema propoziciji 3.1.4 imaju isti tip redukcije mod p (stavimo da je $K = \mathbb{F}_p$). □

Sad smo spremni za glavnu propoziciju ovog odjeljka.

Propozicija 3.1.7. *Neka je $N = 11$ ili $N \geq 17$ prost broj. Tada svaka eliptička krivulja nad $\mathbb{Q}$ koja posjeduje $\mathbb{Q}$-racionalnu cikličku podgrupu reda N ima potencijalno dobru redukciju mod p za sve $p \notin \{2, N\}$ proste brojeve.*

Dokaz. Pretpostavimo suprotno, tj. neka je E eliptička krivulja nad $\mathbb{Q}$ i C_N $\mathbb{Q}$-racionalna ciklička podgrupa reda N te neka E ima potencijalno multiplikativnu redukciju za neki $p \notin \{2, N\}$ prost broj.

Neka je $x = [(E, C_N)] \in X_0(N)(\mathbb{Q})$. Tada se x redukcijom mod p reducira u kasp. Kako $X_0(N)(\mathbb{F}_p)$ ima točno 2 kaspa, možemo bez smanjenja općenitosti uzeti da se x reducira u $\infty_{\mathbb{F}_p}$. Naime, ako se x reducira u drugi kasp, umjesto x možemo

promatrati $w_N(x) = [(E', C'_N)]$. Tada prema propoziciji E' također ima potencijalno multiplikativnu redukciju u p, a kako involucija preslikava jedan kasp u drugi te komutira s redukcijom, $w_N(x)$ se reducira u $\infty_{\mathbb{F}_p}$.

Međutim, sad možemo iskoristiti [12, Poglavlje 7, Propozicija 0.1] koja kaže da je za svaki prosti broj N takav da je genus krivulje $X_0(N)$ veći od 0 (tj. $N = 11$ ili $N \geq 17$) $X_0(N)(\mathbb{Q}) \cap \mathrm{Res}_p(\infty) = \{\infty\}$, pri čemu je

$$\mathrm{Res}_p(x) = \{x' \in X_0(N)(\mathbb{Q}_p) : x' \equiv x \pmod{p}\}$$

p-adski disk ostataka mod p.

To znači da je jedina točka na $X_0(N)(\mathbb{Q})$ koja se reducira u $\infty_{\mathbb{F}_p}$ upravo ∞. Kako je ∞ kasp, a x po definiciji nije, dobili smo kontradikciju s pretpostavkom da takva krivulja E postoji. □

Napomena 3.1.8. *Nismo iskazali propoziciju iz [12] koju smo koristili jer se u iskazu i dokazu te propozicije javljaju pojmovi jakobijana i formalne imerzije koji nam više neće biti potrebni u dokazu Mazurovog teorema.*

Napomena 3.1.9. *Tvrdnja iz prethodne propozicije vrijedi i kad je $p = N$, međutim tada je dokaz puno kompliciraniji jer redukcija mod N u točki ∞ ne mora biti injektivna.*

3.2 Galoisove reprezentacije i karakter izogenije

U ovom odjeljku ćemo se upoznati s nekim primjerima Galoisovih reprezentacija eliptičkih krivulja i njihovim svojstvima. Pri od tih primjera je karakter izogenije. Da bismo ga mogli definirati, na početku ovog odjeljka napravit ćemo kratku digresiju i uvesti neke pojmove iz algebre.

Definicija 3.2.1. *Neka je G grupa. Tada za g, $h \in G$ element $g^{-1}h^{-1}gh$ zovemo komutator elemenata g i h te ga označavamo $[g, h]$.*

Podgrupu grupe G generiranu svim komutatorima u G zovemo komutatorska podgrupa grupe G i označavamo ju $[G, G]$ ili G'.

Kvocijentnu grupu G/G' zovemo abelijaniziranom grupom grupe G i označavamo ju G^{ab} ili G_{ab}.

Ako su aG' i bG' elementi G/G', tada vrijedi $aG'bG' = abG' = ba(a^{-1}b^{-1}ab)G' = baG' = bG'aG'$ što znači da je abelijanizirana grupa stvarno Abelova.

Vratimo se sad na eliptičke krivulje. Neka je kao i prije E krivulja definirana nad K s cikličkom G_K-invarijantnom podgrupom C_N reda N. Ubuduće ćemo to kraće pisati ovako: par (E, C_N) je definiran nad K.

Promotrimo preslikavanje $r' : G_K \to \mathrm{Aut}(C_N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, $\sigma \to n$ pri čemu je n takav da je $\sigma(Q) = nQ$ za sve $Q \in C_N$. Ovo preslikavanje je dobro definirano jer je C_N Galois-invarijantna (pa za svaku točku Q postoji n) i ciklička (pa je taj n isti za sve $Q \in C_N$) te je σ automorfizam pa je $n \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Osim toga, iz definicije izravno slijedi $r'(\sigma\circ\tau) = r'(\tau\circ\sigma)$ pa zaključujemo da vrijedi $r'(a \circ b \circ a^{-1} \circ b^{-1}) = 1$ za sve a,$b \in G_K$, tj. r' trivijalno djeluje na komutatorima. To znači da možemo definirati kvocijentno preslikavanje na abelijaniziranoj Galoisovoj grupi G_K^{ab}.

Definicija 3.2.2. *Preslikavanje $r : G_K^{ab} \to (\mathbb{Z}/N\mathbb{Z})^\times$ definirano na gore opisan način je karakter izogenije para (E, C_N).*

Slično kao karakter izogenije može se definirati i mod N ciklotomski karakter, još jedan primjer Galoisove reprezentacije eliptičkih krivulja.

Definicija 3.2.3. *Neka je $\omega_N = e^{\frac{2\pi i}{N}}$ primitivni N-ti korijen iz jedinice i neka je $\sigma \in G_\mathbb{Q}$. Kako je $\sigma(\omega_N)$ opet N-ti korijen iz jedinice i σ automorfizam, postoji $n \in (\mathbb{Z}/N\mathbb{Z})^\times$ takav da je $\sigma(\omega_N) = \omega_N^n$.*

Preslikavanje $\chi_N : G_\mathbb{Q} \to (\mathbb{Z}/N\mathbb{Z})^\times$, $\sigma \to n$ na gore opisan način je mod N ciklotomski karakter. Za općenito polje $\mathbb{Q} \subset K$ ciklotomski karakter se definira kao restrikcija χ_N na G_K.

Lako se vidi da je $\chi_N^{\phi(N)} = 1$, gdje je ϕ Eulerova funkcija. Naime, za svaki $n \in (\mathbb{Z}/N\mathbb{Z})^\times$ vrijedi $n^{\phi(N)} = 1$ jer grupa $(\mathbb{Z}/N\mathbb{Z})^\times$ ima točno $\phi(N)$ elemenata.

Prisjetimo se da je grupa $E[N]$ oblika $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ i Galois-invarijatna. To nam omogućuje da definiramo mod N Galoisovu reprezentaciju krivulje E, treći primjer Galoisove reprezentacije eliptičkih krivulja.

Definicija 3.2.4. *Preslikavanje $\overline{\rho}_{E,N} : G_K \to \mathrm{Aut}(E[N])$, koje svakom $\sigma \in G_K$ pridružuje $\sigma|_{E[N]}$ zove se mod N Galoisova reprezentacija krivulje E.*

Ako odaberemo bazu $E[N]$, tada $\overline{\rho}_{E,N}$ možemo na prirodan način poistovjetiti s preslikavanjem $\overline{\rho}_{E,N} : G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Napomena 3.2.5. *Promjenom baze $E[N]$ slika $\overline{\rho}_{E,N}$ se konjugira matricom prelaska. Međutim, vrijednost $\det(\overline{\rho}_{E,N})$ se ne mijenja pa se može definirati neovisno o izboru baze.*

Sljedeća vrlo bitna propozicija jednostavno povezuje mod N Galoisovu reprezentaciju i mod N ciklotomski karakter. Za dokaz te propozicije će nam trebati Weilovo sparivanje. Nećemo duboko ulaziti u teoriju vezanu uz njega, već ćemo samo izreći neka njegova osnovna svojstva.

Neka je $m \in \mathbb{N}$ i E eliptička krivulja nad K. Tada postoji Weilovo sparivanje $e_m : E[m] \times E[m] \to \mu_m$ (μ_m je skup m-tih korijena jedinice) i za njega vrijede sljedeća svojstva:

$$\begin{aligned} e_m(S_1 + S_2, T) &= e_m(S_1, T)e_m(S_2, T), \\ e_m(S, T_1 + T_2) &= e_m(S, T_1)e_m(S, T_2), \\ e_m(T, T) &= 1, \\ e_m(S, T) &= e_m(T, S)^{-1}, \\ e_m(S, T) &= 1, \forall S \in E[m] \implies T = 0, \\ e_m(S, T)^\sigma &= e_m(S^\sigma, T^\sigma), \forall \sigma \in G_K. \end{aligned}$$

Prva dva svojstva kažu da je Weilovo sparivanje bilinearno, treće i četvrto da je alternirajuće, peto da je nedegenerirano, a posljednje da je Galois-invarijantno. Dokazi ovih tvrdnji i opširnija teorija Weilovog sparivanja mogu se naći u [13, Poglavlje III.8].

Propozicija 3.2.6. $\det(\overline{\rho}_{E,N}) = \chi_N$

Dokaz. Neka je $\omega_N = e^{\frac{2\pi i}{N}}$. Zbog nedegeneriranosti Weilovog sparivanja postoji $\{S, T\}$ baza $E[N]$ t.d. je $e_N(S, T) = \omega_N$. Uzmimo neki $\sigma \in G_K$ i neka je

$$\overline{\rho}_{E,N}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

odnosno $S^\sigma = aS + cT$, $T^\sigma = bS + dT$. Sada računamo:

$$\begin{aligned} \omega_N^{\chi_N(\sigma)} = \omega_N^\sigma = (e_N(S, T))^\sigma = e_N(S^\sigma, T^\sigma) = e_N(aS + cT, bS + dT) = \\ = e_N(S, S)^{ac} e_N(S, T)^{ad} e_N(T, S)^{bc} e_N(T, T)^{cd} = e_N(S, T)^{ad-bc} = \omega_N^{ad-bc}. \end{aligned}$$

Prva jednakost slijedi izravno iz definicije χ_N, u trećoj smo koristili Galoisovu invarijantnost, u petoj bilinearnost, a u šestoj da je Weilovo sparivanje alternirajuće.

Dakle, dobili smo da je $\chi_N(\sigma) = ad - bc = \det(\overline{\rho}_{E,N})(\sigma)$. Kako to vrijedi za svaki $\sigma \in G_K$, slijedi tvrdnja propozicije. □

Sada ćemo definirati inercijske podgrupe pomoću kojih ćemo moći povezati karakter izogenije i mod N ciklotomski karakter. Prije definicije napomenimo samo da pod pojmom prosti ideal u polju mislimo na prosti ideal u prstenu cijelih brojeva tog polja (npr, prsten cijelih brojeva $\mathbb{Q}$ je $\mathbb{Z}$).

Definicija 3.2.7. *Neka je λ prost ideal u K i μ prost ideal u $\overline{K}$ koji leži nad λ (ovo zapravo znači $\lambda \subset \mu$). Inercijska podgrupa $I_\mu \subset G_K$ je skup svih Galoisovih preslikavanja σ za koje vrijedi $\sigma(a) \equiv a \pmod{\mu}$ za sve $a \in \overline{K} \cap \mathbb{A}$ ($\overline{K} \cap \mathbb{A}$ je prsten cijelih u $\overline{K}$), tj. koja djeluju trivijalno na polju ostataka $(\overline{K} \cap \mathbb{A})/\mu$.*

Ako je μ' neki drugi prosti ideal u $\overline{K}$ koji leži nad λ, poznati teorem iz algebarske teorije brojeva nam kaže da tada postoji $\tau \in G_K$ za koji vrijedi $\tau(\mu) = \mu'$. Sljedeća lema kaže da iz toga slijedi da su pripadne inercijske podgrupe konjugirane.

Lema 3.2.8. *Neka je λ prost ideal u K i μ,μ' prosti ideali u $\overline{K}$ koji leže nad λ. Tada postoji $\tau \in G_K$ za koji vrijedi $\tau I_\mu \tau^{-1} = I_{\mu'}$, odnosno I_μ i $I_{\mu'}$ su konjugirane.*

Dokaz. Neka je $\tau \in G_K$ takav da vrijedi $\tau(\mu) = \mu'$. Iz činjenice da je $\sigma(a) - a \in \mu$ za sve $a \in \overline{K} \cap \mathbb{A}$ zaključujemo sljedeće:

$$\begin{aligned} &\tau(\sigma(a)) - \tau(a) \in \mu', \forall a \in \overline{K} \cap \mathbb{A} \\ \implies &\tau(\sigma(\tau^{-1}(\tau(a)))) - \tau(a) \in \mu', \forall a \in \overline{K} \cap \mathbb{A} \\ \implies &\tau(\sigma(\tau^{-1}(b))) - b \in \mu', \forall b \in \overline{K} \cap \mathbb{A}. \end{aligned}$$

U zadnjem koraku smo koristili činjenicu iz algebarske teorije brojeva da svako Galoisovo preslikavanje šalje cijele algebarske brojeve u cijele algebarske brojeve.

Zadnja jednakost zapravo znači da je $\tau \circ \sigma \circ \tau^{-1} \in I_{\mu'}$ pa smo dobili $\tau I_\mu \tau^{-1} \subset I_{\mu'}$. Analognim računom se dobije $\tau^{-1} I_{\mu'} \tau \subset I_\mu$ što znači da je $\tau I_\mu \tau^{-1} = I_{\mu'}$ čime je tvrdnja leme dokazana. □

Pomoću inercijskih podgrupa ćemo definirati pojam razgranatosti karaktera.

Definicija 3.2.9. *Neka je $\rho : G_K \to (\mathbb{Z}/N\mathbb{Z})^\times$ homomorfizam i neka je λ prosti ideal u K. Kažemo da je ρ nerazgranat u λ ako za svaki prosti ideal μ u $\overline{K}$ koji leži nad λ ρ trivijalno djeluje na I_μ, tj. $\rho(I_\mu) = 1$.*

Napomena 3.2.10. *Da se dokaže razgranatost, dovoljno je provjeriti jedan prosti ideal μ. Naime, pretpostavimo da je $\rho(I_\mu) = 1$ i neka je μ' drugi prosti ideal koji leži nad λ. Po prethodnoj lemi postoji $\tau \in G_K$ t.d. $I_{\mu'} = \tau I_\mu \tau^{-1}$ pa dobivamo*

$$\rho(I_{\mu'}) = \rho(\tau I_\mu \tau^{-1}) = \rho(\tau)\rho(I_\mu)\rho(\tau^{-1}) = \rho(\tau)\rho(\tau^{-1}) = 1.$$

Primjer 3.2.11. *Za N prost broj i $\lambda \neq (N)$ prost ideal u K ciklotomski karakter χ_N (odnosno njegova restrikcija na G_K) je nerazgranat u λ.*

Naime, uzmimo neki μ prosti ideal u $\overline{K}$ koji leži nad λ. Kako je N-ti korijen iz jedinice ω_N cijeli algebarski broj, po definiciji inercije vrijedi $\omega_N^\sigma \equiv \omega_N \pmod{\mu}$ za sve $\sigma \in I_\mu$. Također, vrijedi i sljedeća jednakost:

$$N = (1 - \omega_N)(1 - \omega_N^2) \dots (1 - \omega_N^{N-1}).$$

Kad bi za neki σ vrijedilo $\omega_N^\sigma \neq \omega_N$, tada bismo zbog prethodne jednakosti i invertibilnosti ω_N imali $\omega_N^\sigma - \omega_N \mid N$ pa bi vrijedilo $N \in \mu$. Kako je $\mu \cap K = \lambda$ (važan rezultat

iz algebarske teorije brojeva), iz toga bi slijedilo $N \in \lambda \implies (N) \subset \lambda$. *Međutim, kako su* (N) *i* λ *prosti ideali u* K, *zaključujemo da su jednaki što nije moguće po pretpostavci.*

Dakle, jedina je mogućnost $\omega_N^\sigma = \omega_N$ *za sve* $\sigma \in I_\mu$ *pa zaključujemo* $\chi_N(I_\mu) = 1$. *Prethodna napomena nam sada govori da je* χ_N *nerazgranat u* λ.

Za kraj ovog odjeljka bez dokaza ćemo navesti propoziciju koja daje vezu karaktera izogenije r i ciklotomskog karaktera χ_N. U dokaz nećemo ulaziti jer zahtjeva dobro poznavanje teorije klasa polja koja izlazi van okvira ovog rada.

Prije same propozicije ćemo navesti oznake koje ćemo odsada nadalje koristiti (oznake preuzete iz [10]).

$$\boxed{\begin{aligned} &N \geq 5, \text{prost broj},\\ &m = \frac{N-1}{2},\\ &n = \text{brojnik skraćenog razlomka } \left(\frac{N-1}{12}\right),\\ &t = \frac{m}{n}. \end{aligned}}$$

Propozicija 3.2.12. *Neka je par* (E, C_N) *definiran nad* $\mathbb{Q}$ *pri čemu* E *ima potencijalno dobru redukciju mod* N. *Tada se pripadni karakter izogenije* r *može faktorizirati u obliku* $r = \alpha \cdot \chi_N^k$ *pri čemu je* $\alpha^{2t} = 1$ *i* k *poprima jednu od sljedećih vrijednosti mod* m*:*

$$\begin{aligned} k &\equiv 0, 1 \pmod{m},\\ k &\equiv \frac{1}{2} \pmod{m},\\ k &\equiv \frac{1}{3}, \frac{2}{3} \pmod{m}. \end{aligned}$$

Posljednja dva slučaja su moguća samo ako $2 \nmid m$ *i* $3 \nmid m$, *respektivno.*

Također, α *i* k *iz faktorizacije su jedinstveni u smislu da, ako je* $r = \alpha' \cdot \chi_N^{k'}$ *neka druga faktorizacija, tada je* $\alpha = \alpha'$ *i* $k \equiv k' \pmod{N-1}$.

3.3 Frobeniusov trag

Ovaj odjeljak ćemo započeti s Hasseovim teoremom koji daje ograde na broj točaka na eliptičkoj krivulji nad konačnim poljem.

Teorem 3.3.1 (Hasse)**.** *Neka je p prost broj, $q = p^r$ i E eliptička krivulja nad $\mathbb{F}_q$ (konačno polje s q elemenata). Ako sa $\#E(\mathbb{F}_q)$ označimo broj $\mathbb{F}_q$-racionalnih točaka na E, tada vrijedi sljedeća nejednakost:*

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

Hasseov teorem je, osim što je sam po sebi vrlo važan, u uskoj vezi s pojmom Frobeniusovog traga. Prije nego što definiramo trag, definirat ćemo što je q-Frobeniusov endomorfizam.

Definicija 3.3.2. *Neka je E eliptička krivulja nad $\mathbb{F}_q$ zadana Weierstrassovom jednadžbom*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Tada je $\phi_q : E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$, $(x, y) \to (x^q, y^q)$ q-Frobeniusov endomorfizam.

Iz definicije nije odmah jasno da je preslikavanje ϕ_q $E(\overline{\mathbb{F}_q})$-zatvoreno pa ćemo to sada provjeriti.

Dakle, neka je $(x, y) \in E(\overline{\mathbb{F}_q})$. Kako je multiplikativna grupa svakog konačnog polja ciklička, svaki element $\mathbb{F}_q$ (uključujući i 0) je (multiplikativnog) reda $q-1$ te je stoga $a_i^q = a_i, \forall i$. Također, polje $\mathbb{F}_q$ je karakteristike p (što znači da je $px = 0, \forall x \in \mathbb{F}_q$) pa imamo

$$y^{2q} + a_1x^qy^q + a_3y^q = y^{2q} + (a_1xy)^q + (a_3y)^q = (y^2 + a_1xy + a_3y)^q =$$

$$= (x^3 + a_2x^2 + a_4x + a_6)^q = x^{3q} + (a_2x^2)^q + (a_4x)^q + a_6^q = x^{3q} + a_2x^{2q} + a_4x^q + a_6$$

te je stoga $(x^q, y^q) \in E(\overline{\mathbb{F}_q})$. Pri potenciranju s q međučlanovi su se pokratili jer su pripadni binomni koeficijenti djeljivi s p, a $pa_i = 0, \forall i$.

Primijetimo također da ako je $(x, y) \in E(\mathbb{F}_q)$, tada vrijedi $(x^q, y^q) = (x, y)$. Stoga su sve $\mathbb{F}_q$-racionalne točke E fiksne točke endomorfizma.

Napomena 3.3.3. *Valja razlikovati q-Frobeniusov endomorfizam od Frobeniusovog automorfizma. Frobeniusov automorfizam je zadan na $\mathbb{F}_q$ na sljedeći način:*

$$\phi : \mathbb{F}_q \to \mathbb{F}_q, x \to x^p.$$

To je stvarno automorfizam jer je $\phi^n(x) = x^{p^n} = x^q = x, \forall x \in \mathbb{F}_p$.

Sada ćemo definirati i Frobeniusov trag.

Definicija 3.3.4. *Neka je E eliptička krivulja nad $\mathbb{F}_q$. Tada je $a_q = q + 1 - \#E(\mathbb{F}_q)$ Frobeniusov trag krivulje E nad $\mathbb{F}_q$.*

Odmah vidimo da po Hasseovom teoremu slijedi $|a_q| \leq 2\sqrt{q}$.

Iz definicije nije odmah jasno u kakvoj su vezi q-Frobeniusov automorfizam i Frobeniusov trag. Sljedeći teorem će nam dati tu vezu.

Teorem 3.3.5. *Neka je E eliptička krivulja nad $\mathbb{F}_q$.*

(a) Ako su $\alpha, \beta \in \mathbb{C}$ nultočke polinoma $T^2 - a_q T + q$, tada su one kompleksno konjugirane i vrijedi $|\alpha| = |\beta| = \sqrt{q}$ te za svaki $n \in \mathbb{N}$ vrijedi

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n.$$

(b) q-Frobeniusov endomorfizam zadovoljava jednakost

$$\phi_q \circ \phi_q - [a_q] \circ \phi_q + [q] = 0.$$

Dokaz. Dokaz se može naći u [13, Teorem 2.3.1]. □

Neka $a(\mathbb{F}_{q^n}/\mathbb{F}_q)$ označava bilo koji cijeli broj koji je Frobeniusov trag nad $\mathbb{F}_{q^n}$ neke eliptičke krivulje definirane nad $\mathbb{F}_q$. Ako je $n = 1$, pišemo $a(\mathbb{F}_q) = a(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

Primjer 3.3.6. *Može se provjeriti da vrijedi [13]*

$$a(\mathbb{F}_{2^{12}}/\mathbb{F}_2) \in \{128, -128, -47\},$$

$$a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) \in \{658, 1358, -1458\}.$$

Korištenjem teorije klasa polja uz pomoć formula iz prethodnog teorema može se dokazati sljedeća propozicija koju također navodimo bez dokaza.

Propozicija 3.3.7. *Neka je par (E, C_N) definiran nad $\mathbb{Q}$ pri čemu E ima potencijalno dobru redukciju mod p i mod N te neka je $r = \alpha \cdot \chi^k$ pripadni karakter izogenije. Tada vrijede sljedeće dvije tvrdnje:*

(a) Postoje $a \in a(\mathbb{F}_p)$ i $\Theta \in (\mathbb{Z}/N\mathbb{Z})^\times$ takvi da je $\Theta^{2t} = 1$ i $\Theta p^k + \Theta^{-1} p^{1-k} \equiv a \pmod{N}$.

(b) Postoji $a \in a(\mathbb{F}_{p^{12}}/\mathbb{F}_p)$ takav da je $p^{12k} + p^{12-12k} \equiv a \pmod{N}$.

Napomena 3.3.8. *Θ iz prethodne propozicije je određen s α iz faktorizacije karaktera izogenije $r = \alpha \cdot \chi_N^k$. Kako nam način na koji je Θ dobiven nije bitan za dokaz Mazurovog teorema, propoziciju smo iskazali na ovako pojednostavljen način. Dokaz propozicije i postupak dobivanja Θ mogu se naći u [10, Poglavlje 6].*

3.4 Dokaz Mazurovog teorema

Sad smo napokon spremni dokazati Mazurov teorem za krivulju $X_0(N)$. Prije samog teorema dokazat ćemo dvije pomoćne leme te navesti nekoliko teorema iz algebarske teorije brojeva koje ćemo koristiti u dokazu.

Lema 3.4.1. *Neka par (E, C_N) definiran nad K ima karakter izogenije $r = \alpha \cdot \chi_N^k$. Tada par $(E/C_N, E[N]/C_N)$ koji se dobije djelovanjem Atkin-Lehnerove involucije ima karakter izogenije $r' = \alpha^{-1} \cdot \chi_n^{1-k}$.*

Dokaz. Neka je P neki generator grupe C_N, odnosno $C_N = (P)$. Uzmimo $Q \in E[N]$ t.d. je $\{P, Q\}$ baza $E[M]$. Tada je $E[N]/C_N = (Q + C_N)$.

Neka je $\sigma \in G_K$ i neka je, uz odabranu bazu $\{P, Q\}$, djelovanje $\overline{\rho}_{E,N}$ na σ dano na sljedeći način:

$$\overline{\rho}_{E,N}(\sigma) = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}.$$

Odavde lako vidimo da vrijedi $P^\sigma = aP$ i $Q^\sigma = bP + dQ$. Zato dobivamo $(Q + C_N)^\sigma = d(Q + C_N)$ pa možemo zaključiti da je $r(\sigma) = a$ i $r'(\sigma) = d$

Kako je $ad = \det(\overline{\rho}_{E,N})(\sigma) = \chi_N(\sigma)$, slijedi da je $rr' = \chi_n$, odnosno da je $r' = \chi_n r = \alpha^{-1}\chi_N^{1-k}$ čime je tvrdnja leme dokazana. □

Lema 3.4.2. *Neka je K polje algebarskih brojeva, R prsten cijelih u K i $I \neq 0$ ideal u R. Tada I dijeli ideal $(N(I))$ ($N(I)$ je norma ideala I).*

Dokaz. Označimo $m = N(I) = |R/I|$. Poznata je činjenica da je R Dedekindova domena, što znači da I dijeli (m) ako i samo ako je $(m) \subset I \iff m \in I$.

Kako je $|R/I| = m$, svaki element R/I je reda koji dijeli m. To znači da je $m + I = m(1 + I) = I \implies m \in I$ čime je tvrdnja leme dokazana. □

Teorem 3.4.3 (Baker-Heegner-Stark)**.** *Neka je $d \in \mathbb{N}$. Tada je $\mathbb{Q}(\sqrt{-d})$ domena glavnih ideala ako i samo ako je $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.*

Teorem 3.4.4 (Minkowski)**.** *Neka je K polje algebarskih brojeva i $n = [K : \mathbb{Q}]$ stupanj proširenja. Neka r_1 označava broj realnih, a $2r_2 = n - r_1$ broj kompleksnih ulaganja K u $\mathbb{C}$ te neka je D diskriminanta polja K.*

Tada svaka klasa u grupi klasa ideala polja K sadrži ideal norme ne veće od

$$M_K = \sqrt{|D|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}.$$

Broj M_K je ograda Minkowskog za polje K.

Teorem 3.4.5 (Dedekind)**.** *Neka je $k \in \mathbb{Z}$ i R prsten cijelih u polju $\mathbb{Q}(\sqrt{k})$.*

(a) Ako $p \mid k$, tada je $(p) = \left(p, \sqrt{k}\right)^2$.

(b) Ako $2 \nmid k$, tada je

$$(2) = \begin{cases} \left(2, 1+\sqrt{k}\right)^2 & \text{ako je } k \equiv -1 \pmod 4, \\ \left(2, \frac{1+\sqrt{k}}{2}\right)\left(2, \frac{1-\sqrt{k}}{2}\right) & \text{ako je } k \equiv 1 \pmod 8, \\ \text{prost} & \text{ako je } k \equiv 5 \pmod 8. \end{cases}$$

(c) Ako $2 \neq p \mid k$, tada je

$$(p) = \begin{cases} \left(p, n+\sqrt{k}\right)\left(p, n-\sqrt{k}\right) & \text{ako je } k \equiv n^2 \pmod p, \\ \text{prost} & \text{ako je } \left(\frac{k}{p}\right) = -1. \end{cases}$$

Teorem 3.4.6 (Mazur)**.** *Neka je N prost broj takav da je genus krivulje $X_0(N)$ veći od 0 (tj. $N = 11$ ili $N \geq 17$). Tada $X_0(N)(\mathbb{Q})$ ne sadrži nijednu nekaspidalnu $\mathbb{Q}$-racionalnu točku osim u slučajevima iz tablice 3.1.*

Dokaz. Tvrdnja teorema je ekvivalentna tvrdnji da za gore navedene N ne postoji eliptička krivulja nad $\mathbb{Q}$ koja sadrži cikličku $G_{\mathbb{Q}}$-invarijantnu podgrupu reda N.

Pretpostavimo suprotno, neka je (E, C_N) jedan takav par. Kako su uvjeti iz propozicije 3.1.7 ispunjeni, zaključujemo da E ima potencijalno dobru redukciju mod p za sve $p > 2$ proste brojeve.

Neka je $r = \alpha \cdot \chi_N^k$ karakter izogenije para (E, C_N). Primjenom propozicije 3.2.12 i, ako je potrebno, leme 3.4.1, možemo pretpostaviti $k \equiv 0, \frac{1}{3}, \frac{1}{2} \pmod m$. Štoviše, možemo pretpostaviti i jaču tvrdnju da je $k \equiv 0 \pmod{N-1}$, $3k \equiv 1 \pmod{N-1}$ ili $2k \equiv 1 + m \pmod{N-1}$ [10]. Promotrimo svaki od tih slučajeva.

- $k \equiv 0 \pmod{N-1}$

  Primjenom propozicije 3.3.7 za $p = 3$ dobivamo

  $$1 + 3^{12} \equiv 3^{12k} + 3^{12-12k} \equiv 658, -1358, 1458 \pmod N.$$

  Jedini prosti brojevi N za koje je to moguće su $N = 2, 3, 5, 7, 13, 19, 37, 97$. Ponovnom primjenom propozicije 3.3.7 za $p = 5$ dobivamo

  $$1 + 5^{12} \equiv 5^{12k} + 5^{12-12k} \equiv a(\mathbb{F}_{5^{12}}/\mathbb{F}_5) \pmod N.$$

Može se pokazati da su jedini prosti brojevi N za koje je to moguće $N = 2, 3, 5, 7, 13, 17, 31, 37, 61, 157, 229$ [10].

Zaključujemo da N mora biti element skupa

$$\{2, 3, 5, 7, 13, 19, 37, 97\} \cap \{2, 3, 5, 7, 13, 17, 31, 37, 61, 157, 229\} =$$

$$= \{2, 3, 5, 7, 13, 37\}.$$

Dakle, u ovom slučaju jedini mogući prosti broj N za koji je genus krivulje $X_0(N)$ veći od 0 je $N = 37$, a on se nalazi u tablici.

- $3k \equiv 1 \pmod{N-1}$

  Primjenom propozicije 3.3.7 za $p = 3$ dobivamo

  $$3^4 + 3^8 \equiv 3^{12k} + 3^{12-12k} \equiv 658, -1358, 1458 \pmod{N}.$$

  Jedini prosti brojevi N za koje je to moguće su $N = 2, 3, 5, 11, 17$. Dakle, u ovom slučaju jedini mogući prosti brojevi N za koje je genus krivulje $X_0(N)$ veći od 0 su $N = 11$ i $N = 17$, a oni se nalaze u tablici.

- $2k \equiv 1 + m \pmod{N-1}$

  Kako je $2k \equiv 1 \pmod{m}$, zaključujemo da je m neparan pa je $N \equiv -1 \pmod{4}$. To znači da je $t = 1$ ili $t = 3$.

  Pretpostavimo da za neki prosti broj $2 < p < \frac{N}{4}$ vrijedi $\left(\frac{p}{N}\right) = 1$. To po definiciji Legendreovog simbola znači da je $p^m = p^{\frac{N-1}{2}} \equiv 1 \pmod{N}$, stoga vrijedi $p^k \equiv p^{1-k} \pmod{N}$. Primjenom propozicije 3.3.7 dobivamo

  $$p^k(\Theta + \Theta^{-1}) \equiv p^k\Theta + p^{1-k}\Theta^{-1} \equiv a(\mathbb{F}_p) \pmod{N}.$$

  Iz propozicije 3.3.7 također dobivamo $\Theta^6 = 1$ što znači da je $\Theta^3 = \pm 1$.

  Ako $\Theta \neq \pm 1$, tada vrijedi $\Theta + \Theta^{-1} = \pm 1$ pa je $p^k \equiv \pm a(\mathbb{F}_p) \pmod{N} \implies p \equiv p^{2k} \equiv a(\mathbb{F}_p)^2 \pmod{N}$. Po Hasseovom teoremu je $a(\mathbb{F}_p)^2 \leq 4p < N$ pa zaključujemo $a(\mathbb{F}_p)^2 = p$ što je nemoguće jer je p prost broj.

  Ako $\Theta = \pm 1$, tada vrijedi $2p^k \equiv \pm a(\mathbb{F}_p) \pmod{N} \implies 4p \equiv 4p^{2k} \equiv a(\mathbb{F}_p)^2 \pmod{N}$. Ponovno, po Hasseovom teoremu je $a(\mathbb{F}_p)^2 \leq 4p < N$ pa zaključujemo $a(\mathbb{F}_p)^2 = 4p$ što je nemoguće jer je p prost broj.

  Dakle, u oba slučaja smo dobili kontradikciju što znači da za svaki prosti broj $2 < p < \frac{N}{4}$ vrijedi $\left(\frac{p}{N}\right) = -1$. Iz Dedekindovog teorema sada slijedi da je za

svaki prosti broj $2 < p < \frac{N}{4}$ ideal (p) prost. Dokažimo da iz toga slijedi da su svi ideali u $\mathbb{Q}(\sqrt{-N})$ neparne norme manje od $\frac{N}{4}$ glavni.

Neka je I ideal u $\mathbb{Q}(\sqrt{-N})$ neparne norme $m = N(I) < \frac{N}{4}$. Po lemi 3.4.2 znamo da vrijedi $I \mid (m) = (p_1)^{\alpha_1} \dots (p_k)^{\alpha_k}$ pri čemu je $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ rastav na proste faktore. Iz prethodne diskusije znamo da su svi ideali (p_i) prosti pa zaključujemo da je $I = (p_1)^{\beta_1} \dots (p_k)^{\beta_k}$ i stoga glavni ideal.

Dokažimo sad da je i (2) prost ideal u $\mathbb{Q}(\sqrt{-N})$. Pretpostavimo da nije prost. Iz Dedekindovog teorema i uvjeta $N \equiv -1 \pmod 4$ dobivamo da tada mora vrijediti $N \equiv -1 \pmod 8 \implies N \equiv -1, 7 \pmod{16}$.

Prvo pretpostavimo da je $N \equiv -1 \pmod{16}$. Neka je $\alpha = \frac{3+\sqrt{-N}}{2}$. Lako se vidi da je $N(\alpha) = \frac{9+N}{4}$ što je broj oblika $4k + 2$. Kako norma prostog ideala može biti jedino potencija prostog broja (jer je za prosti ideal P R/P konačno polje), zaključujemo da postoji faktorizacija $(\alpha) = PI$, gdje je P prosti ideal norme 2, a I ideal neparne norme.

Kako I ima neparnu normu $\frac{N+9}{8} < \frac{N}{4}$ (pretpostavili smo $N \geq 11$), dokazali smo da je glavni. Iz toga slijedi i da je P glavni. Dakle, postoji $\beta \in R$ t.d. $P = (\beta)$ i $N(\beta) = 2$. Međutim, lako se vidi da u $\mathbb{Q}(\sqrt{-N})$ ne postoji element norme 2 pa smo dobili kontradikciju.

U slučaju kada je $N \equiv 7 \pmod{16}$, uzimanjem $\alpha = \frac{1+\sqrt{-N}}{2}$ na analogan način dobivamo kontradikciju.

Dakle, pretpostavka da (2) nije prost u $\mathbb{Q}(\sqrt{-N})$ vodi na kontradikciju, stoga je to prost ideal. Sada na isti način kao prije možemo dokazati da su svi ideali u $\mathbb{Q}(\sqrt{-N})$ norme manje od $\frac{N}{4}$ glavni. Dokažimo da iz toga slijedi da je R domena glavnih ideala.

Lako se vidi da je $\mathbb{Q}(\sqrt{-N})$ kvadratno proširenje $\mathbb{Q}$, tj. da je stupanj proširenja 2 te da je diskriminanta jednaka $-N$. Također, ne postoje realna ulaganja $\mathbb{Q}(\sqrt{-N})$ u C pa je $r_1 = 0$, $r_2 = 1$. Sad primjenom teorema Minkowskog možemo dobiti da u svakoj klasi ideala postoji ideal norme manje ili jednake $\sqrt{N}\frac{2}{\pi} < \frac{N}{4}$ (jer je $n \geq 11$). Međutim, dokazali smo da je svaki takav ideal glavni pa je svaka klasa zapravo klasa glavnih ideala, odnosno R je domena glavnih ideala.

Baker-Heegner-Starkov teorem nam sada kaže da su jedine mogućnosti $N = 11, 19, 43, 67, 163$, a sve se one nalaze u tablici.

□

Bibliografija

[1] F. Diamond, J. Im, *Modular forms and modular curves*, dostupno na: `https://www.math.wisc.edu/~boston/Diamond-Im-Modular_forms_and_modular_curves.pdf`

[2] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Springer-Verlag New York, 2005.

[3] A. Dujella, *Eliptičke krivulje u kriptografiji*, dostupno na: `https://web.math.pmf.unizg.hr/~duje/elkript/elkripto2.pdf`

[4] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

[5] M. A. Kenku, *The modular curve* $X_0(39)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), no. 1, 21-23

[6] M. A. Kenku, *The modular curves* $X_0(65)$ *and* $X_0(91)$ *and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), no. 1, 15-20

[7] M. A. Kenku, *The modular curve* $X_0(169)$ *and rational isogeny*, J. London Math. Soc. (2) **22** (1980), no. 2, 239-244

[8] M. A. Kenku, *The modular curves* $X_0(125)$*,* $X_0(25)$ *and* $X_0(49)$, J. London Math. Soc. (2) **23** (1981), no. 3, 415-427

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1978), 33-186, dostupno na: `http://www.numdam.org/article/PMIHES_1977__47__33_0.pdf`

[10] B. Mazur, *Rational Isogenies of Prime Degree*, Invent. Math. **44** (1978), 129-162

[11] F. Najman, *Aritmetička geometrija*, dostupno na: `https://web.math.pmf.unizg.hr/~fnajman/ag.pdf`

[12] S. Siksek, *Explicit Arithmetic of Modular Curves*, dostupno na: `https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf`

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag New York; 2nd edition, 2009.

Sažetak

U ovom radu bavili smo se izogenijama eliptičkih krivulja. Prvo smo definirali eliptičke krivulje i operaciju zbrajanja, a zatim se posvetili izogenijama. Nakon uvodnih definicija i primjera naveli smo i dokazali neka njihova osnovna svojstva.

Nakon toga prešli smo na modularne krivulje. Definirali smo modularne krivulje $X_0(N)$ i $X_1(N)$ preko kongruencijskih podgrupa modularne grupe $\mathrm{SL}_2(\mathbb{Z})$. Zatim smo iskazali tvrdnju da su to algebarske krivulje definirane nad $\mathbb{Q}$, a nakon toga smo dokazali teoreme koji daju vezu točaka na modularnoj krivulji i eliptičkih krivulja. Također smo dali primjere kako se modularne krivulje mogu koristiti u dokazivanju tvrdnji za eliptičke krivulje.

Onda smo krenuli na Mazurov teorem. Naveli smo slučajeve u kojima krivulja $X_0(N)$ ima racionalne nekaspidalne točke i rekli da teorem kaže da su to svi slučajevi kad je N prost, a nakon toga smo počeli obrađivati pojmove i razultate potrebne za dokaz teorema. Koristeći polje p-adskih brojeva $\mathbb{Q}_p$ uveli smo pojmove potencijalno dobre i potencijalno multiplikativne redukcije i, uz pomoć Atkin-Lehnerove involucije, kojoj smo također posvetili malo vremena, dokazali važnu pomoćnu tvrdnju. Zatim smo definirali karakter izogenije, ciklotomski karakter i mod N-Galoisove reprezentacije eliptičkih krivulja. Pokazali smo neke veze između tih pojmova i iskazali rezultat o faktorizaciji karaktera izogenije. Iza toga smo definirali Frobeniusov trag, naveli neka njegova svojstva i iskazali vezu s karakterom izogenije. Naposlijetku, uz pomoć rezultata iz ovog rada te nekoliko teorema iz algebarske teorije brojeva dokazali smo Mazurov teorem.

Summary

In this thesis we considered isogenies of elliptic curves. We first defined elliptic curves and the addition operation, after which we turned to isogenies. After some introductory definitions and examples, we stated and proved some of their basic properties.

After that, we considered modular curves. We defined modular curves $X_0(N)$ and $X_1(N)$ using the congruence subgroups of the modular group $\mathrm{SL}_2(\mathbb{Z})$. Then we stated the fact that these are algebraic curves defined over $\mathbb{Q}$ and proved the theorems that give the connection between points on a modular curve and elliptic curves. We also gave examples of how modular curves can be used to prove statements about elliptic curves.

Then we moved on to Mazur's theorem. We listed the cases when the curve $X_0(N)$ has rational non-cuspidal points and mentioned that the theorem says that these are all the cases when N is a prime number. After that, we started considering notions and results needed for the proof of the theorem. Using the field of p-adic numbers $\mathbb{Q}_p$ we introduced the notions of potential good and potential multiplicative reduction and, using the Atkin-Lehner involution, which we also considered for a while, proved an important auxiliary statement. We then defined the isogeny character, the cyclotomic character and mod N-Galois representations of elliptic curves. We proved some connections between these notions and stated a result about the factorization of the isogeny character. Next, we defined the trace of Frobenius, stated its basic properties and linked it with the isogeny character. Finally, using the results from this paper and several algebraic number theory theorems we proved Mazur's theorem.

Životopis

Petar Orlić rođen je 11.7.1998. u Zagrebu gdje je pohađao Osnovnu školu Josipa Račića i XV. Gimnaziju. Za vrijeme osnovnoškolskog i srednjoškolskog obrazovanja sudjelovao je na brojnim natjecanjima iz matematike i drugih znanosti. Na 56. Međunarodnoj matematičkoj olimpijadi u Tajlandu osvojio je srebrnu, a na 57. Međunarodnoj matematičkoj olimpijadi u Hong Kongu brončanu medalju.

Na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu 2016. godine upisao je Preddiplomski sveučilišni studij Matematika, a 2019. Diplomski sveučilišni studij Teorijska matematika.

Tijekom studija držao je demonstrature iz više kolegija i sudjelovao na studentskim natjecanjima iz matematike. Na međunarodnim matematičkim natjecanjima IMC 2017. i IMC. 2018. osvojio je prvu nagradu za što je 2019. godine dobio Posebno priznanje rektora, a na Međunarodnom matematičkom natjecanju Vojtěch Jarník 2018. osvojio je drugo mjesto. 2021. godine dobio je Dekanovu nagradu za izuzetan uspjeh u studiju.