SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Antonela Trbović

Torzijske grupe eliptičkih krivulja nad kvadratnim poljima

Zagreb, 2016.

Ovaj rad izrađen je na Zavodu za algebru i osnove matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta, pod vodstvom prof. dr. sc. Filipa Najmana, i predan je na natječaj za dodjelu Rektorove nagrade u akademskoj godini 2015./2016.

Sadržaj

Poglavlje 1

Uvod

Diofantske jednadžbe (tj. polinomijalne jednadžbe) nad $\mathbb{Z}$, $\mathbb{Q}$ ili nekim drugim nama zanimljivim poljima (ili prstenima) proučavaju se još od stare Grčke. Zanimaju nas rješenja tih jednadžbi, odnosno postoje li uopće načini za određivanje postoje li rješenja takvih jednadžbi. Najpoznatiji takav problem je Fermatov zadnji teorem, koji nam govori kako ne postoje $a,b,c \in \mathbb{Z}$ strogo veći od 1 i $n \geq 3$ takvi da je

$$a^n + b^n = c^n.$$

Dokazao ga je Andrew Wiles 1994. godine, a ključnu ulogu u dokazu imale su eliptičke krivulje.

Za jednostavnije oblike diofantskih jednadžbi u dvije varijable, koje određuju krivulju genusa 0, problem određivanja rješenja je riješen. No, promatramo li kompliciraniji slučaj, tj. kubne diofantske jednadžbe u dvije varijable, one određuju krivulju genusa 1. To nas motivira da proučavamo eliptičke krivulje.

Imamo li eliptičku krivulju E definiranu nad poljem algebarskih brojeva $\mathbb{K}$, znamo (prema Mordell-Weilovom teoremu) da ona ima oblik $E \cong T \oplus \mathbb{Z}^r$, gdje je T podgrupa elemenata konačnog reda, a $r \geq 0$ neki cijeli broj. Prirodno se postavlja pitanje koje su njene moguće torzijske podgrupe. Odgovor na to pitanje je za eliptičke krivulje definirane nad $\mathbb{Q}$ dao Mazur 1978. godine. Kasnije je dokazan sličan rezultat za eliptičke krivulje definirane

nad kvadratnim poljima. No, taj rezultat nam ne govori ništa o tome koje torzijske grupe bismo mogli imati kada fiksiramo neko kvadratno polje. To je bila glavna motivacija za nastanak ovog rada.

Navedimo i pregled materijala izloženog u radu:
U 2. poglavlju smo definirali eliptičku krivulju, uveli teorijske osnove i naveli rezultate bitne za nastavak našeg rada. Definirali smo operaciju zbrajanja točaka na eliptičkoj krivulji i dokazali da uz tako definirano zbrajanje imamo Abelovu grupu (za koju još vijedi i da je konačnogenerirana). Iskazujemo Mordell-Weilov i Mazurov teorem. To su centralni teoremi potrebni za nastavak ovog rada.

U 3. poglavlju smo definirali redukciju modulo p i proste brojeve u kojima eliptička krivulja ima dobru, odnosno lošu redukciju te vrste loše redukcije. Također, iskazali smo dva teorema koja daju dobre ograde za broj točaka eliptičkih krivulja nad konačnim poljima. Analogon redukcije modulo p za Jacobijane nam je bitan kod traženja torzije Jacobijana koje koristimo u zadnjem poglavlju, kod traženja torzije eliptičkih krivulja nad fiksnim kvadratnim poljem.

U 4. poglavlju definiramo kvadratna polja i navodimo njihova osnovna svojstva. Definiramo i proste brojeve koji se cijepaju, inertni su ili su razgranati. Oni će nam biti bitni kod traženja konačnih polja u koja se ulaže torzija Jacobijana hipereliptičke krivulje. Navodimo i konkretne primjere.

U 5. poglavlju definiramo Galoisove reprezentacije pridružene eliptičkim krivuljama i neka njihova osnovna svojstva. One su nam od posebnog značaja kada na eliptičkoj krivulji imamo točku reda n.

U 6. poglavlju definiramo djelidbene polinome pomoću kojih možemo odrediti postoje li točke nekog fiksnog reda na nekoj eliptičkoj krivulji.

U 7. poglavlju definiramo modularne krivulje i primijećujemo ključnu činjenicu da su točke na modularnoj krivulji zapravo klase izomorfizama s određenim torzijskim svojstvom. Sada se naš posao traženja grupa koje se mogu pojaviti kao torzijske podgrupe neke eliptičke krivulje nad fiksnim kvadratnim poljem svodi na određivanje broja točaka

na određenim modularnim krivuljama.

U 8. poglavlju navodimo neke bitne rezultate vezane uz hipereliptičke krivulje. To nam je bitno jer su neke od modularnih krivulja s kojima moramo raditi kod traženja torzije zapravo hipereliptičke. Sve ćemo to koristiti u zadnjem poglavlju.

9. poglavlje je zaključak našeg teorijskog pregleda u kojem iskazujemo i dokazujemo neka svojstva eliptičkih krivulja nad kvadratnim poljima koja će nam tehnički olakšati zaključivanje pojavljuju li se određene torzijske grupe nad fiksnim kvadratnim poljem ili ne.

U 10. i zadnjem poglavlju Fiksiramo neko kvadratno polje i opisujemo postupke određivanja mogućih torzijskih grupa eliptičkih krivulja nad njime. Navodimo i konkretne primjere, tj. za svaku od mogućih 26 grupa detaljno opisujemo postupak zaključivanja pojavljuje li se ona kao torzijska grupa neke eliptičke krivulje ili ne. Ovo cijelo poglavlje je ujedno i (originalni) doprinos ovog rada.

Imamo i dodatke, koje smo zbog preglednosti stavili na kraj, u njima su jednadžbe nekih eliptičkih i modularnih krivulja koje koristimo kroz cijeli rad te kodovi iz Magme, programa kojeg koristimo kako bismo došli do određenih rezultata u radu.

Poglavlje 2

Eliptičke krivulje

U ovom poglavlju definirat ćemo centralni objekt kojeg ćemo proučavati u radu te navesti neke osnovne definicije i rezultate koje ćemo koristiti u nastavku.

2.1 Osnovni pojmovi

Definicija 2.1. *Neka je* $\mathbb{K}$ *polje. Eliptička krivulja nad* $\mathbb{K}$ *je nesingularna projektivna kubna krivulja nad* $\mathbb{K}$ *s barem jednom (*$\mathbb{K}$*-racionalnom) točkom.*

Svaka takva krivulja nad poljem $\mathbb{K}$ ima (afinu) jednadžbu oblika:

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

s koeficijentima $a, b, ..., j$ iz polja $\mathbb{K}$.
Ta jednadžba se može biracionalnim transformacijama (racionalnim transformacijama čiji je inverz također racionalna transformacija) svesti na oblik

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

koji zovemo Weierstrassova forma.
Nadalje, ako je karakteristika $char(\mathbb{K}) \neq 2, 3$ (pa smijemo nadopunjavati na potpun kvadrat i potpun kub i dijeliti s 2 i 3 ako je potrebno), onda se afina jednadžba može zapisati

u obliku

$$y^2 = x^3 + ax + b,\ a,b \in \mathbb{K},$$

koji zovemo kratka Weierstrassova forma.

Neće nas zanimati eliptičke krivulje nad poljima karakteristike 2 ili 3 pa nadalje možemo zapisivati krivulje i u kratkoj Weierstrassovoj formi.

Uvjet nesingularnosti nam govori da kubni polinom $f(x) = x^3 + ax + b$ ne smije imati višestrukih nultočaka, tj. diskriminanta $-4a^3 - 27b^2$ polinoma f mora biti različita od nule.

Diskriminantu eliptičke krivulje E drfiniramo kao

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

Zaključujemo, E ima singularnu točku ako i samo ako vrijedi $\Delta(E) = 0$. Također, ako je E definirana nad potpoljem od $\mathbb{R}$, tada polinom $f(x) = x^3 + ax + b$ ima 1 ili 3 nultočke, ovisno o tome je li $\Delta(E) < 0$ ili $\Delta(E) > 0$.

Eliptičku krivulju definiranu nad poljem $\mathbb{K}$ zamišljamo kao skup svih točaka $(x,y) \in \mathbb{K} \times \mathbb{K}$ koje zadovoljavaju jednadžbu

$$E:\ y^2 = x^3 + ax + b,$$

gdje su $a,b \in \mathbb{K}$ i $-4a^3 - 27b^2 \neq 0$, zajedno s "točkom u beskonačnosti" O. Taj skup označavamo s $E(\mathbb{K})$.

Točka u beskonačnosti se prirodno pojavljuje ako zapišemo krivulju u projektivnim koordinatama i ima oblik $O = (0:1:0)$.

Eliptička krivulja E, zapisana u projektivnom obliku je zapravo

$$E:\ Y^2Z + a_1XYZ + a_3YZ^2 = X^2 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

odnosno

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

2.2 Zbrajanje točaka na eliptičkoj krivulji

U ovom poglavlju definirat ćemo operaciju (zbrajanje točaka) na eliptičkoj krivulji koju smo definirali u prethodnom poglavlju te ćemo vidjeti da je eliptička krivulja s tako definiranim zbrajanjem Abelova grupa. Kasnije će se pokazati da je ona konačnogenerirana pa ćemo prema strukturnom teoremu o konačnogeneriranim Abelovim grupama moći zaključiti nešto o strukturi grupe $E(\mathbb{K})$.

Uzmimo na kratko da je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva. Tada $E(\mathbb{R})$, bez točke u beskonačnosti, možemo prikazati kao podskup ravnine. Geometrijski ćemo definirati zbrajanje točaka na $E(\mathbb{R})$.

Navedimo prvo jedan koristan rezultat kojeg ćemo koristiti kasnije u definiciji zbrajanja točaka.

Teorem 2.2. ***(Bezout)*** *Dvije algebarske krivulje definirane nad poljem k stupnjeva m i n, koje nemaju zajedničku komponentu, sijeku se u $m \cdot n$ točaka (ako brojimo kratnost svake točke presjeka) nad algebarskim zatvorenjem $\overline{k}$ od k.*

Izabremo li dvije točke P i Q na eliptičkoj krivulji E, primjećujemo da postoji nekoliko mogućnosti za njihov međusoban odnos. Za svaki od tih slučajeva definirat ćemo zbroj te dvije točke, odnosno točku $P+Q$ na eliptičkoj krivulji.

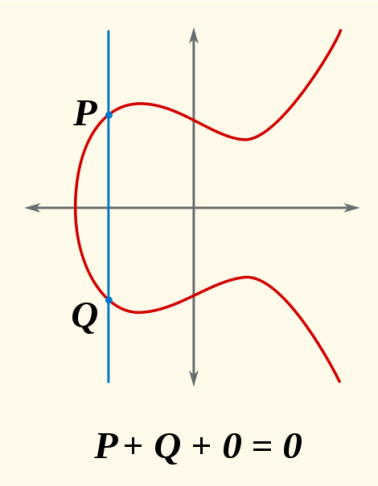
Prije svega, definiramo točku O kao neutral za zbrajanje. Nadalje, neka je $P+Q+R=O$ ako točke P, Q, i R leže na istom pravcu.

1. slučaj. Neka su $P,Q \in E(\mathbb{R})$ točke na eliptičkoj krivulji za koje vrijedi $P = -Q$, tj. $P = (x,y)$, $Q = (x,-y)$. Prebacimo se na kratko u projektivne koordinate. Tada je $P = (x:y:1)$, $Q = (x:-y:1)$ te je pravac p koji prolazi točkama P i Q skup svih točaka oblika

$$u(x:y:1) + v(x:-y:1),\ u,v \in \mathbb{R}.$$

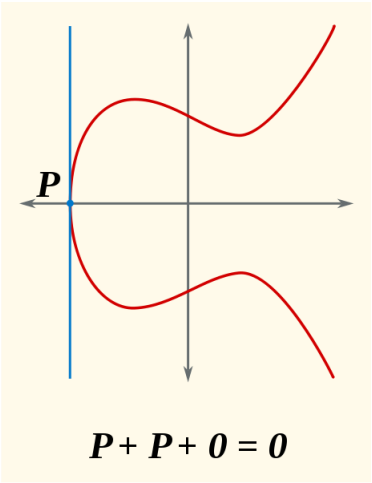
Za $u = -v = 1$ dobivamo točku $(0:2y:0) = (0:1:0)$ na pravcu, tj. pravac siječe točku u beskonačnosti.

Sada, definiramo da je $P+Q=O$, gdje je O točka u beskonačnosti.



Slika 2.1: 1. slučaj

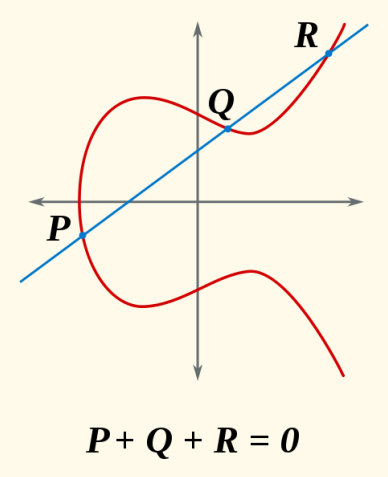
2. slučaj. Neka je $P=(x,0)$. Tada je pravac p tangenta na E u P, pa je $P+P+O=O$, tj. $2P=O$. Primijetimo da će P biti točka reda 2 u grupi čije zbrajanje upravo definiramo.



Slika 2.2: 2. slučaj

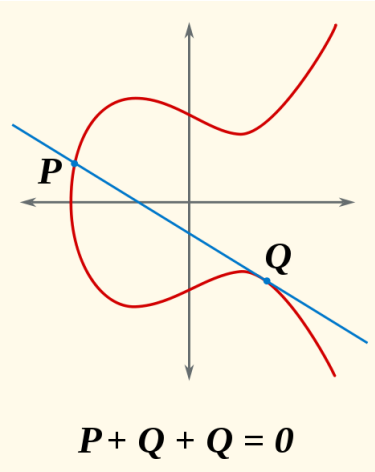
3. slučaj. Neka su $P,Q \in E(\mathbb{R})$ te neka pravac p kroz te dvije točke siječe svaku od tih točaka s multiplicitetom 1 (dakle, točke P i Q nisu točke infleksije i pravac p nije tangenta na eliptičku krivulju). Tada po Bezoutovom teoremu slijedi da pravac p siječe krivulju u nekoj trećoj točki, označimo ju s R. Ona mora biti iz $E(\mathbb{R})$, jer odgovarajuća

jednadžba pravca ima 2 rješenja nad $\mathbb{R}$ pa i tada i treće mora biti nad $\mathbb{R}$. Sada definiramo da je $P+Q=-R$, gdje je $-R$ točka na krivulji osnosimetrična točki R s obzirom na os x.



Slika 2.3: 3. slučaj

4. slučaj. Neka su $P,Q \in E(\mathbb{R})$ i neka pravac p kroz točke P i Q siječe jednu od točaka s multiplicitetom 2 (ne može više zbog Bezoutovog teorema). Tada definiramo $P+Q=-Q$.



Slika 2.4: 4. slučaj

5. slučaj. Ako je točka P točka infleksije, tj. pravac p siječe krivulju s multiplicitetom 3 (to je najveći multiplicitet kroz jednu točku zbog Bezoutovog teorema), tada je $P+P+$

$P = O$, tj. $P + P = -P$.

Ovaj geometrijski zakon može se opisati i eksplicitnim formulama za koordinate zbroja točaka. Pomoću tih formula kasnije možemo definirati i zbrajanje točaka na eliptičkoj krivulji nad proizvoljnim poljem $\mathbb{K}$. Spomenimo još da će u polju karakteristike 2 ili 3 sljedeće formule biti nešto drugačije, budući da krivulju ne možemo zapisati u kratkoj Weierstrassovoj formi, ali već smo rekli da nas takve krivulje neće zanimati.

Neka je

$$E: \ y^2 = x^3 + ax + b$$

elliptička krivulja i neka su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke na E. Tada je:

1. $-O = O$
2. $-P = (x_1, -y_1)$
3. $O + P = P$
4. Ako je $Q = -P$, tada je $P + Q = O$
5. Ako je $Q \neq -P$, tada je $P + Q = (x_3, y_3)$, gdje je

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

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

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & x_1 \neq x_2 \\ (3x_1^2 + a)/2y_1, & x_1 = x_2. \end{cases}$$

Sada vidimo da je $(E(\mathbb{K}), +)$ Abelova grupa. Postojanje inverza je očito, neutral u grupi je točka O, dok je dokaz asocijativnosti nešto (tehnički) kompliciraniji pa njega izostavljamo, ali može se naći u [19]. Zatvorenost na zbrajanje je također očita zbog činjenice da su formule za zbrajanje točaka racionalne funkcije.

2.3 Torzijska grupa

U prethodnom poglavlju došli smo do zaključka kako je eliptička krivulja $E(\mathbb{K})$ Abelova grupa. Sada, kako bismo bolje opisali tu grupu, navodimo bitan teorem kojeg je za eliptičke krivulje nad $\mathbb{Q}$ dokazao Mordell, a poopćio ga je Weil na Abelove mnogostrukosti nad poljima algebarskih brojeva.

Teorem 2.3. ***(Mordell-Weil)*** *Neka je E eliptička krivulja nad poljem algebarskih brojeva* $\mathbb{K}$. *Tada je* $E(\mathbb{K})$ *konačnogenerirana Abelova grupa.*

Dokaz izostavljamo jer je kompliciran te nije bitan za daljnje razumijevanje, a može se naći recimo u [15]. U poglavlju 8, gdje koristimo Mordell-Weilov teorem za Abelove mnogostrukosti ukratko dajemo ideju dokaza.

Iz Mordell-Weilovog teorema i strukturnog teorema o konačnogeneriranim Abelovim grupama zaključujemo da je $E(\mathbb{K})$ sljedećeg oblika:

$$E(\mathbb{K}) \cong E(\mathbb{K})_{tors} \oplus \mathbb{Z}^r,$$

gdje je $r \in \mathbb{Z}, r \geq 0$, rang eliptičke krivulje, a $E(\mathbb{K})_{tors}$ torzijska podgrupa od $E(\mathbb{K})$, tj podgrupa elemenata konačnog reda s obzirom na zbrajanje.
O rangu eliptičke krivulje nad $\mathbb{Q}$ se ne zna mnogo. Nije poznato može li biti proizvoljno velik i ne postoje algoritmi za računanje ranga eliptičkih krivulja. No, nas neće zanimati rang, već torzijska podgrupa. Za računanje torzije nad $\mathbb{Q}$ postoje algoritmi, koji su efikasni i u praksi. Navodimo još jedan teorem koji će nam pomoći da razumijemo kako mogu izgledati torzijske podgrupe eliptičke krivulje nad poljem racionalnih brojeva.

Teorem 2.4. ***(Mazur)*** *Neka je* $E(\mathbb{Q})$ *eliptička krivulja. Tada je torzijska grupa,* $E(\mathbb{Q})_{tors}$, *izomorfna jednoj od sljedećih 15 grupa:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,2,...,10,12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4.$$

No, situacija nije tako jednostavna uzmemo li za $\mathbb{K}$ neko "kompliciranije" polje. Nas će zanimati kvadratna polja, tj. polja oblika $\mathbb{Q}(\sqrt{d})$, gdje je $d \in \mathbb{Z}$ kvadratno slobodan.

Postoji sličan teorem koji govori koje su mogućnosti za torzijske podgrupe ako uzmemo u obzir sva moguća kvadratna polja. Problem nastaje kada pokušamo fiksirati neko kvadratno polje i vidjeti koje su moguće torzijske grupe eliptičkih krivulja definiranih nad tim poljem.

Postavlja se pitanje možemo li za fiksnu eliptičku krivulju nad $\mathbb{Q}$ lako odrediti koja je njena torzijska podgrupa. I taj problem je riješen i to sljedećim teoremom koji daje i algoritam za računanje torzije.

Teorem 2.5. ***(Lutz-Nagell)*** *Neka je*

$$E: \ y^2 = x^3 + ax + b, \ a, b \in \mathbb{Z},$$

te neka je $O \neq P \in E(\mathbb{Q})$ točka konačnog reda (torzijska točka). Tada vrijedi:
(1) $x(P), y(P) \in \mathbb{Z}$,
(2) $y(P) = 0$ *ili* $y(P)^2 | 4a^3 + 27b^2 = \dfrac{-\Delta(E)}{16}$.

Prethodni teorem nam zapravo govori da kod traženja torzijskih točaka fiksne eliptičke krivulje imamo samo konačno mnogo mogućnosti koje moramo provjeriti.

2.4 Preslikavanja između eliptičkih krivulja

U ovom poglavlju nam je cilj definirati izomorfizam između eliptičkih krivulja te reći pod kojim uvjetima su dvije krivulje izomorfne. Također, definirat ćemo stupanj preslikavanja eliptičkih krivulja pomoću kojeg ćemo dokazati zanimljivu činjenicu o broju torzijskih točaka reda m na eliptičkoj krivulji, koju ćemo koristiti u poglavlju o Galoisovim reprezentacijama eliptičkih krivulja.

Označimo sa $\mathbb{K}(x_1, ..., x_n)$ polje razlomaka od $\mathbb{K}[x_1, ...x_n]$. Tada svaku funkciju $f \in \mathbb{K}(x_1, ..., x_n) =: \mathbb{K}(\mathbb{A}^n)$ zovemo racionalnom funkcijom.

Ako imamo krivulju C definiranu nad poljem $\mathbb{K}$, i $f = \dfrac{g}{h} \in \mathbb{K}(\mathbb{A}^n)$ takvu da je $h \neq 0$ na $C(\mathbb{K})$, tada je restrikcija od f,

$$f : C \setminus \{h = 0\} \to \overline{\mathbb{K}}$$

racionalna funkcija na C. Skup svih racionalnih funkcija čini polje koje označavamo s $\mathbb{K}(C)$.

Definicija 2.6. *Neka su C i D krivulje definirane nad poljem* $\mathbb{K}$. *Racionalno preslikavanje nad* $\mathbb{K}$ $\phi : C \to D$ *je preslikavanje definirano racionalnim funkcijama* $\phi = (u,v),\ u,v \in \mathbb{K}(C)$, *takvima da u i v nisu obje 0. Drugim riječima,* $\phi(P) = (u(P),v(P))$, *za* $P \in C(\mathbb{K})$.

Definicija 2.7. *Kažemo da je preslikavanje* $\phi : C \to D$ *regularno u točki P ako postoji* $g \in \mathbb{K}(C)^*$ *takav da su ug i vg definirani u P. Ako je* ϕ *regularno na cijeloj krivulji C, tada kažemo da je* ϕ *morfizam.*

Definicija 2.8. *Ako je* $\phi : C \to D$ *morfizam takav da postoji morfizam* $\psi : D \to C$ *sa svojstvom* $\psi \circ \phi = id_C$ *i* $\phi \circ \psi = id_D$, *tada kažemo da je* ϕ *izomorfizam.*

Sada kada znamo što je izomorfizam, pogledajmo dvije eliptičke krivulje

$$E:\ y^2 = x^3 + ax + b,$$

$$E' : y^2 = x^3 + a'x + b'$$

u kratkoj Weierstrassovoj formi. Ako su one izomorfne, tada postoji zamjena varijabli

$$x_{E'} = u^2 x_E,$$

$$y_{E'} = u^3 y_E,$$

gdje je $u \in \mathbb{K}^*$. Dakle, zaključujemo da vrijedi:

$$E \cong E' \iff (u^3 y_E)^2 = (u^2 x_E)^3 + a'(u^2 x_E) + b' \iff a' = u^4 a, b' = u^6 b$$

$$\Delta(E') = -16(4(a')^3 + 27(b')^2) = u^{12}\Delta(E).$$

Ovu činjenicu ćemo koristiti u sljedećem poglavlju, kod redukcije eliptičkih krivulja.

Definicija 2.9. *Izogenija između dvije eliptičke krivulje je morfizam* $\phi : E \to E'$ *koji preslikava* $O \in E$ *u* $O' \in E'$.

Sada, za svaki $m \in \mathbb{Z}$ definiramo množenje s m,

$$[m] : E \to E$$

na sljedeći način:

Ako je $m > 0$, tada je

$$[m](P) = \underbrace{P + P + ... + P}_{\text{m puta}}$$

Ako je $m < 0$ tada je

$$[m](P) = [-m](-P).$$

Ako $m = 0$, tada je $[0](P) = O$.

Može se pokazati da je zbrajanje točaka na eliptičkoj krivulji,

$$+ : E \times E \to E,$$

$$(P_1, P_2) \mapsto P_1 + P_2$$

morfizam pa indukcijom lako slijedi da je i množenje s m također morfizam. Budući da množenje s m šalje točku O u O, vrijedi da je ono izogenija,

Sada ćemo definirati stupanj preslikavanja te ćemo odrediti stupanj upravo definirane izogenije.

Pogledajmo prvo dvije krivulje C i D te preslikavanje $\phi : C \to D$. Ako je a racionalna funkcija iz $\mathbb{K}(D)$, tada je $a \circ \phi$ racionalna funkcija iz $\mathbb{K}(C)$. Dakle, funkcija $\phi : C \to D$ inducira injektivni homomorfizam polja

$$\phi^* : \mathbb{K}(D) \to \mathbb{K}(C),$$

$$a \mapsto a \circ \phi = \phi^* a.$$

Definicija 2.10. *Stupanj preslikavanja $\phi : C \to D$ je $[\mathbb{K}(C) : \phi^* \mathbb{D}]$, ako je ϕ nekonstantno preslikavanje, a 0 ako je ϕ konstantno preslikavanje.*

Pogledajmo na sljedećem primjeru kako računamo stupanj nekog preslikavanja.

Primjer 2.11. Uzmimo dvije krivulje,

$$C: \ y^2 = x^3 + 1,$$

$$D: \ y = 0$$

te racionalno preslikavanje

$$\phi : C \to D,$$

$$\phi(x,y) = (x,0).$$

Ako je $a(x,0) = x$ racionalna funkcija na $\mathbb{K}(D)$, tada je

$$a \circ \phi(x,y) = \phi^* a(x,y) = x.$$

Dakle, $\phi^*\mathbb{K}(D) = \mathbb{K}(x)$ te je

$$[\mathbb{K}(C) : \phi^*\mathbb{K}(D)] = [\mathbb{K}(x, \sqrt{x^3+1}) : \mathbb{K}(x)] = 2.$$

Slijedi da je preslikavanje ϕ stupnja 2.

Označimo sada sa $E[m] = Ker[m]$, jezgru gore definirane izogenije, odnosno skup točaka reda m na eliptičkoj krivulji E.

Propozicija 2.12. *Neka je E eliptička krivulja i* $m \in \mathbb{Z}$, $m \neq 0$.
(1) Stupanj izogenije $[m] : E \to E$ *je* m^2.
(2) $\#E[m] = deg[m]$.
(3) Neka je $char(\mathbb{K}) = 0$ *ili* $p = char(\mathbb{Z}) > 0$ *i* $p \nmid m$, *tada je*

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

Dokaz. (1), (2): Ovaj dio nećemo dokazivati jer bismo morali uvoditi još pojmova koji nam neće biti od interesa u daljnjim razmatranjima.
(3): Iz (1) i (2) imamo

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

Slično, za svaki djelitelj d broja m imamo

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

Sada, ako zapišemo $E[m]$ kao produkt cikličkih grupa, jasno je da je jedina mogućnost

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

□

Poglavlje 3

Redukcija modulo p

U ovom poglavlju opisujemo redukciju eliptičkih krivulja modulo p. Ideja je da pomoću dobro poznatog homomorfizma $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $n \mapsto n(mod\ p)$, reduciramo krivulju modulo p tako da reduciramo modulo p njezine koeficijente. Naravno, neće uvijek biti moguće na taj način dobiti krivulju koja je i dalje eliptička, ali pokušat ćemo naći uvjete pod kojima to možemo učiniti.

Vidjet ćemo i da ovako definirana redukcija modulo p ima svoje primjene kod nalaženja torzijskih točaka eliptičke krivulje definirane nad poljem racionalnih brojeva, ali pokazat će se korisna i kasnije, u poglavlju 8, kada budemo htjeli opisati torzijsku podgrupu Jacobijana pridruženog nekoj hipereliptičkoj krivulji. Više o tome kasnije.

Definicija 3.1. *Neka je* $E:\ y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ *eliptička krivulja nad* $\mathbb{Q}$. *Kažemo da je to minimalni model ako su svi* $a_i \in \mathbb{Z}$ *i ako je* $|\Delta(E)|$ *minimalan u klasi izomorfizama od* E.

Definicija 3.2. *Neka je* $n \in \mathbb{Z}$ *i* $p \in \mathbb{N}$ *prost broj. Neka je* $n = p^k \cdot m$, $(p,m) = 1$. *Red elementa p u n definiramo kao* $\nu_p(n) = k$.

Propozicija 3.3. *Neka je*

$$E:\ y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,\ \in \mathbb{Z}$$

i neka je $0 \leq \nu_p(\Delta(E)) \leq 12$, *za sve proste brojeve p. Tada je E minimalni model.*

Dokaz. Neka je E' eliptička krivulja izomorfna eliptičkoj krivulji E. Tada iz poglavlja 2.4 zaključujemo da vrijedi $\Delta(E') = u^{12}\Delta(E)$, za neki $u \in \mathbb{Q}^*$. Budući da vrijedi $\nu_p(\Delta(E)) < 12$, za svaki prost broj p te $\nu_p(\Delta(E'))$ mora biti cjelobrojan, slijedi da je $u \in \mathbb{Z}^*$. Dakle, $|\Delta(E')| \geq |\Delta(E)|$. □

Promotrimo sada "redukciju modulo p", odnosno homomorfizam $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, gdje je $p \in \mathbb{N}$ prost broj.
Znamo (iz 2. poglavlja) da je svaka eliptička krivulja nad $\mathbb{Q}$ izomorfna nekoj eliptičkoj krivulji nad $\mathbb{Q}$ oblika $y^2 = x^3 + ax + b,\ a,b \in \mathbb{Q}$. Sasvim je jasno da eliminacijom nazivnika i jednostavnim supstitucijama možemo doći do izomorfne eliptičke krivulje oblika $y^2 = x^3 + ax + b,\ a,b \in \mathbb{Z}$.

Sada je ideja da iz eliptičke krivulje E dobijemo "reduciranu krivulju modulo p". Prvo navodimo formalnu definiciju redukcije koju opisujemo za eliptičke krivulje u kratkoj Weierstrassovoj formi. Jasno je kako je definicija redukcije sasvim analogna i kada imamo dugu Weierstrassovu formu. Ona nam ponekad treba kada reduciramo krivulju modulo p, za $p = 2,3$. Naravno, u tom slučaju su i formule za zbrajanje točaka nešto drugačije (i kompliciranije). Mi ih nećemo koristiti, ali mogu se naći u [15].
Nakon toga, imamo jednostavan primjer koji stoji iza motivacije za uvođenje minimalnog modela eliptičke krivulje.

Definicija 3.4. *Neka je E eliptička krivulja nad $\mathbb{Q}$ s minimalnim modelom*

$$E:\ y^2 = x^3 + ax + b,\ a,b \in \mathbb{Z}.$$

Definiramo $\overline{E}$ nad $\mathbb{F}_p$ kao

$$\overline{E}:\ y^2 = x^3 + \overline{a}x + \overline{b},$$

gdje su $\overline{a}$ i $\overline{b}$ slike od a i b s obzirom na redukciju modulo p, odnosno homomorfizam $\mathbb{Z} \to \mathbb{F}_p$. $\overline{E}$ zovemo redukcijom eliptičke krivulje E modulo p.

Primjer 3.5. Promotrimo krivulje

$$E_1:\ y^2 = x^3 + x + 1$$

$$E_2 : \ y^2 = x^3 + 81x + 729$$

Krivulje E_1 i E_2 su izomorfne nad $\mathbb{Q}$. Njihove redukcije modulo 3 su:

$$\overline{E_1} : \ y^2 = x^3 + x + 1$$

$$\overline{E_2} : \ y^2 = x^3.$$

Prva jednadžba je eliptička krivulja, ali druga nije (jer je singularna). Također, vrijedi:

$$\Delta(E_1) = 2^4 \cdot 31, \ \ \Delta(E_2) = 2^4 \cdot 3^{12} \cdot 31.$$

Dakle, da bismo reducirali eliptičku krivulju, treba izabrati minimalni model u klasi izomorfizama eliptičke krivulje nad $\mathbb{Q}$.

Napomena 3.6. Primijetimo da je $\overline{E}$ eliptička krivulja ako i samo ako vrijedi $\Delta(\overline{E}) \neq 0$ u $\mathbb{F}_p$, to jest ako i samo ako $p \nmid \Delta(E)$.

U sljedećoj definiciji uvodimo nazive za redukcije eliptičkih krivulja koje nam (ne) odgovaraju, odnosno za redukcije koje (ne) definiraju novu eliptičku krivulju nad konačnim poljem $\mathbb{F}_p$.

Definicija 3.7. *Neka je eliptička krivulja zadana modelom*

$$E : \ y^2 = f(x),$$

gdje je f polinom stupnja 3. Ako je s $\overline{E}$ definirana eliptička krivulja nad poljem $\mathbb{F}_p$, tada kažemo da E ima dobru redukciju modulo p. U protivnom, kažemo da E ima lošu redukciju modulo p.
Kod prostih brojeva s lošom redukcijom, kubni polinom f ima višestruki korijen modulo p. Ako polinom ima trostruki korijen, kažemo da E ima aditivnu redukciju, a ako polinom ima dvostruki korijen, onda kažemo da E ima multiplikativnu redukciju.
Nadalje, razlikujemo rascjepivu i nerascjepivu multiplikativnu redukciju. Multiplikativna redukcija je rascjepiva ako su koeficijenti smjera tangenata u singularnoj točki iz $\mathbb{F}_p$, a nerascjepiva inače.

Je li multiplikativna redukcija rascjepiva ili nerascjepiva u p, možemo odrediti jednostavno. Zapišemo li krivulju u obliku $y^2 = x^2(x+c)$, jednadžbe tangenti u singularnoj točki $(0,0)$ su $y = \pm\sqrt{c}x$ pa je multiplikativna redukcija rascjepiva ako i samo ako je c kvadrat u $\mathbb{F}_p$.

Napomena 3.8. Iz napomene 3.6 i činjenice da diskriminanta eliptičke krivulje ima samo konačno mnogo prostih faktora, zaključujemo da svaka eliptička krivulja ima lošu redukciju u samo konačno mnogo prostih brojeva p.

Napomena 3.9. U terminima nove definicije, ako eliptička krivulja E ima lošu redukciju za neki p, traženjem minimalnog modela nalazimo eliptičku krivulju izomorfnu s E, za koju je moguće da ima dobru redukciju u p, kao što smo zaključili nakon primjera 3.5.

U sljedećem primjeru ćemo naći proste brojeve p za danu eliptičku krivulju u kojima ona ima dobru, odnosno lošu redukciju, a za brojeve u kojima je redukcija loša, odredit ćemo i vrstu te loše redukcije.

Primjer 3.10. Promotrimo eliptičku krivulju nad $\mathbb{Q}$ zadanu jednadžbom

$$E:\ y^2 = x^3 + 6250x + 234375.$$

Diskriminanta eliptičke krivulje E je jednaka $\Delta(E) = -2^4 \cdot 5^{14} \cdot 13 \cdot 31$. Iz napomene (broj) zaključujemo da E ima dobru redukciju svugdje osim možda u 2, 5, 13 i 31. Također, jasno je da gornjom jednadžbom nije zadan minimalni model jer u diskriminanti imamo faktor 5^{12}.
Sada uvodimo supstituciju $x = 25x_1,\ y = 125y_1$ i dobivamo jednadžbu

$$E_1:\ y_1^2 = x_1^3 + 10x_1 + 15,$$

čija diskriminanta je jednaka $\Delta(E) = -2^4 \cdot 5^2 \cdot 13 \cdot 31$. Ovo je očito minimalni model (jer $v_p(\Delta(E_1)) < 12$, za svaki p) pa možemo vidjeti da je redukcija u brojevima 2, 5, 13 i 31 zaista loša.
Odredimo sada kakvu lošu redukciju krivulja ima u 31. Reducirana krivulja modulo 13 glasi

$$\overline{E}:\ y^2 = x^3 + 10x + 11.$$

Očita nultočka polinoma $\overline{f}(x) = x^3 + 10x + 11$ je $x = -1$. Nadalje, vrijedi

$$\overline{f}'(-1) = 0,\ \overline{f}''(-1) \neq 0.$$

To znači da je redukcija u 13 multiplikativna. Na kraju, $\overline{f}(x) = (x+1)^2(x+11)$, a supstitucijom $x \mapsto x-1$ dobivamo $\overline{f} = x^2(x+10)$. Sada, budući da je $10 \equiv 7^2 \pmod{13}$ slijedi da je redukcija u 13 rascjepiva.

Sada navodimo propoziciju iz koje možemo vidjeti kako pomoću redukcije mod p možemo naći torzijsku grupu eliptičke krivulje nad poljem racionalnih brojeva. Ipak, ovaj postupak nije algoritam, kao što je to bio Lutz-Nagellov teorem.

Propozicija 3.11. *Neka je E eliptička krivulja s dobrom redukcijom u p. Tada je redukcija modulo p injekcija na p-slobodnom dijelu torzije od $E(\mathbb{Q})$, tj. podgrupi točaka čiji red je relativno prost s p.*

Sada se postavlja pitanje koliko točaka uopće možemo imati na krivulji $E(\mathbb{F}_p)$. To će nam biti bitno kasnije, kod nalaženja broja torzijskih točaka na Jacobijanu hipereliptičke krivulje ili ako budemo htjeli odrediti jednadžbu eliptičke krivulje s nekim torzijama nad kadratnim poljem.

Pokušajmo sada odrediti točan broj točaka, odnosno $|E(\mathbb{F}_p)|$. Neka je

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

Prolazimo po svim točakama $x \in \mathbb{F}_{\mathbb{p}}$. Jasno je da za taj x na $E(\mathbb{F}_{\mathbb{p}})$ postoji 0 točaka ako $x^3 + ax + b$ nije kvadratni ostatak modulo p, 1 točka, ako je $x^3 + ax + b$ djeljivo s p te 2 točke ako je $x^3 + ax + b$ kvadratni ostatak modulo p i nije djeljiv s p. I još nam ostaje točka O, koja je uvijek torzijska točka. Dolazimo do zaključka:

$$|E(\mathbb{F}_p)| = 1 + \sum_{x=0}^{p-1} \Big(\frac{x^3 + ax + b}{p}\Big).$$

No, nekada nije potrebno znati točan broj točaka, već samo neku gornju ogradu. Tu su nam od koristi sljedeća dva teorema.

Teorem 3.12. ***(Hasse)*** *Neka je E eliptička krivulja nad konačnim poljem $\mathbb{F}_q$. Tada je*

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

Vrijedi i sljedeća generalizacija:

Teorem 3.13. ***(Hasse-Weil)*** *Neka je C nesingularna krivulja genusa g nad $\mathbb{F}_q$. Tada je*

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

Poglavlje 4

Kvadratna polja

Već smo rekli da će nas zanimati torzijske grupe eliptičkih krivulja nad kvadratnim poljima. Dakle potrebno je definirati kvadratna polja i navesti neka njihova osnovna svojstva. To činimo u ovom poglavlju.

Definicija 4.1. *Polje algebarskih brojeva* $\mathbb{K}$ *je proširenje od* $\mathbb{Q}$ *konačnog stupnja, to jest proširenje takvo da vrijedi* $[\mathbb{K} : \mathbb{Q}] < \infty$.

Definicija 4.2. *Kvadratno polje* $\mathbb{K}$ *je proširenje od* $\mathbb{Q}$ *stupnja 2.*

Svako polje algebarskih brojeva $\mathbb{K}$ se može generirati jednim elementom, tj. $\mathbb{K}$ je oblika

$$\mathbb{K} = \mathbb{Q}(\alpha) = \left\{ \sum_{i=0}^{n-1} c_i \alpha^i : c_i \in \mathbb{Q} \right\},$$

gdje je n stupanj od $\mathbb{K}$. No, za kvadratna polja možemo postići još i bolje, tj. možemo α prikazati kao korijen nekog kvadratno slobodnog elementa iz $\mathbb{Z}$.

Teorem 4.3. *Svako kvadratno polje* $\mathbb{K}$ *može se prikazati u obliku*

$$\mathbb{K} = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\},$$

gdje je $d \in \mathbb{Z}$ *kvadratno slobodan.*

Dokaz. Trebamo pokazati da je svako kvadratno polje, odnosno svako proširenje od $\mathbb{Q}$ stupnja 2 izomorfno s $\mathbb{Q}(\sqrt{d})$, gdje je $d \in \mathbb{Z}$ kvadratno slobodan.

Neka je $\alpha \in \mathbb{K}$ proizvoljan element s minimalnim polinomom (tj. normiranim polinomom najmanjeg stupnja koji poništava element) $f \in \mathbb{Q}[x]$ stupnja 2. Označimo

$$f(x) = x^2 + ax + b, \;\; a, b \in \mathbb{Q}.$$

Vrijedi

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2},$$

odnosno

$$(2\alpha + a)^2 = a^2 - 4b.$$

Dakle, u $\mathbb{K}$ postoji element $\beta = 2\alpha + a$ takav da je $\beta^2 = a^2 - 4b \in \mathbb{Q}$. Primijetimo da $a^2 - 4b$ nije kvadrat u $\mathbb{Q}$, inače $f(x)$ ne bi bio ireducibilan. Dakle, β je također element iz $\mathbb{K}$ s minimalnim polinomom stupnja 2. U slučaju da $a^2 - 4b$ nije kvadratno slobodan cijeli broj, zbog jedinstvene faktorizacije u $\mathbb{Z}$ postoji $c \in \mathbb{Q}$ takav da je $c^2(a^2 - 4b)$ kvadratno slobodan cijeli broj. Tada $c\beta$, koji je korijen kvadratno slobodnog cijelog broja, i dalje generira $\mathbb{K}$. □

Znamo da u $\mathbb{Z}$ postoji jedinstvena faktorizacija cijelih brojeva na ireducibilne faktore. No, u $\mathbb{Z}[\sqrt{d}]$ ta tvrdnja nije općenito istinita. Primjerice, vidimo da brojevi

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in \mathbb{Q}(\sqrt{-5})$$

i

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}) \in \mathbb{Q}(\sqrt{-3})$$

nemaju jedinstvenu faktorizaciju.

Zapravo, nemamo niti jedinstvenu faktorizaciju ideala u $\mathbb{Z}[\sqrt{d}]$. Neka je $a = (2, 1 + \sqrt{-3})$ ideal. Računamo

$$a^2 = (4, 2 + 2\sqrt{-3}, (1 + \sqrt{-3})^2) = (4, 2 + 2\sqrt{-3}, -2 + 2\sqrt{-3}) =$$

$$= (4, 2 + 2\sqrt{-3}) = (2)(2, 1 + \sqrt{-3}) = (2)a,$$

ali $a \neq (2)$, budući da $1 + \sqrt{-3} \notin (2)$. Dakle imamo $a \cdot a = (2)a$, što nije jedinstvena faktorizacija.

Sada definirano prsten u kojem ipak postoji nekakva jedinstvena faktorizacija.

Definicija 4.4. *Prsten cijelih brojeva $O_{\mathbb{K}}$ nekog polja algebarskih brojeva $\mathbb{K}$ je skup elemenata iz $\mathbb{K}$ čiji minimalni polinom ima cjelobrojne koeficijente.*

Prsteni cijelih brojeva polja algebarskih brojeva su Dedekindove domene, tj. postoji jedinstvena faktorizacija u proste ideale.

Neka je $\mathcal{P}$ prost ideal u $O_{\mathbb{K}}$. Tada postoji jedinstveni cijeli broj p takav da je $\mathcal{P}|(p) = pO_{\mathbb{K}}$. Kažemo da $\mathcal{P}$ leži iznad (p) te da (p) leži ispod $\mathcal{P}$. Kažemo da je stupanj proširenja $O_{\mathbb{K}}/\mathcal{P}$ od $\mathbb{F}_p$ stupanj inertnosti od p te da je najveća potencija od $\mathcal{P}$ koja dijeli (p) stupanj grananja od $\mathcal{P}$.

Neka je

$$(p) = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}$$

faktorizacija od (p) u $O_{\mathbb{K}}$, gdje je e_i stupanj grananja od $\mathcal{P}_i$. Neka je f_i stupanj inertnosti od $\mathcal{P}_i$ te neka je $\mathbb{K}$ polje stupnja n. Tada vrijedi

$$\sum_{i=1}^{k} e_i f_i = n.$$

Ako je $k = 1$, $e_1 = 1$ te $f_1 = n$, tada kažemo da je p inertan u $O_{\mathbb{K}}$. Ako je $e_i > 1$, za neki i, kažemo da je p razgranat u $O_{\mathbb{K}}$. Ako je $k = 1$, $e_1 = n$ te $f_1 = 1$, kažemo da je p potpuno razgranat. Ako je $k \geq 2$, kažemo da se p cijepa u $O_{\mathbb{K}}$. Ako je $k = n$, kažemo da se p potpuno cijepa u $O_{\mathbb{K}}$.

Napomena 4.5. *Ima samo konačno mnogo prostih brojeva koji su razgranati u $O_{\mathbb{K}}$. To su oni prosti brojevi p koji dijele diskriminantu $\Delta_{\mathbb{K}}$.*

Promotrimo sada faktorizaciju u kvadratnom polju $\mathbb{K} = \mathbb{Q}(\sqrt{d})$. Za kvadratna polja vrijedi

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} d, & d \equiv 1 (mod\ 4) \\ 4d, & \text{inače.} \end{cases}$$

Iz napomene 4.5 vidimo da su jedini prosti brojevi koji se granaju oni koji dijele d ako je $d \equiv 1 (mod\ 4)$ te 2 i oni koji dijele d ako je $d \equiv 2, 3 (mod\ 4)$.

Napomena 4.6. *U* $\mathbb{K}$ *se cijepaju oni prosti brojevi za koje* $x^2 - d$ *ima nultočke modulo p, što je ekvivalentno tome da je d kvadrat modulo p.*

Dakle, uzevši u obzir zadnje dvije napomene, imamo

$$p \text{ se cijepa ako i samo ako } \left(\frac{d}{p}\right) = 1,$$

$$p \text{ je inertan ako i samo ako } \left(\frac{d}{p}\right) = -1,$$

$$p \text{ je razgranat ako i samo ako } \left(\frac{d}{p}\right) = 0.$$

Vrijednost $\left(\frac{d}{p}\right)$ lako računamo pomoću $\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \pmod{p}$, za neparne proste brojeve p.

U sljedećem primjeru ćemo uzeti neko kvadratno polje i za prvih nekoliko prostih brojeva vidjeti jesu li oni razgranati, inertni ili se cijepaju. Na početku primjera ćemo koristiti i činjenicu da je

$$O_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \pmod{4} \\ \mathbb{Z}[\sqrt{d}], & \text{inače.} \end{cases}$$

Dokaz se može naći u [20].

Primjer 4.7. Neka je $\mathbb{K} = \mathbb{Q}(-5)$. Tada je $O_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}]$. Faktorizirajmo neke proste brojeve.

Uzmimo prvo $p = 2$. Tada je

$$x^2 + 5 \equiv (x+1)^2 \pmod{2}$$

pa je 2 razgranat u $O_{\mathbb{K}}$,

$$2O_{\mathbb{K}} = (2, \sqrt{-5}+1)^2.$$

Za $p = 3$, imamo

$$x^2 + 5 \equiv (x+1)(x+2) \pmod{3}$$

pa se 3 (potpuno) cijepa u $O_{\mathbb{K}}$,

$$3O_{\mathbb{K}} = (3, \sqrt{-5}+1)(3, \sqrt{-5}+2).$$

Za $p = 5$, imamo

$$x^2 + 5 \equiv x^2 \pmod 5$$

pa se i 5 grana u $O_{\mathbb{K}}$,

$$5O_{\mathbb{K}} = (5, \sqrt{-5})^2.$$

Primijetimo da su 2 i 5, zbog napomene 4.5, jedini prosti brojevi koji se granaju.
Nadalje, za $p = 7$, imamo

$$x^2 + 5 \equiv (x+3)(x+4) \pmod 7$$

pa se 7 (potpuno) cijepa,

$$7O_{\mathbb{K}} = (7, \sqrt{-5}+3)(7, \sqrt{-5}+4).$$

Poglavlje 5

Galoisove reprezentacije pridružene eliptičkim krivuljama

U ovom poglavlju će $\mathbb{K}$ biti polje karakteristike $char(\mathbb{K}) = 0$.

Definicija 5.1. *Neka je $\mathbb{K}$ polje te neka je $\overline{\mathbb{K}}$ njegovo algebarsko zatvorenje. Tada grupu $G_{\mathbb{K}} = Gal(\overline{\mathbb{K}}/\mathbb{K})$ svih automorfizama polja $\overline{\mathbb{K}}$ koji fiksiraju $\mathbb{K}$ (po točkama) zovemo apsolutna Galoisova grupa.*

Sada uvodimo definiciju u kojoj nam novo polje k ne mora biti karakteristike 0.

Definicija 5.2. *n-dimenzionalna reprezentacija grupe G je homomorfizam grupa*

$$\rho : G \to GL_n(k),$$

gdje je k neko polje.
Ako je $k \subset \mathbb{F}_p$, gdje je $\mathbb{F}_p$ konačno polje s p elemenata, tada ρ nazivamo mod p reprezentacijom.

Sada, uzmemo li u obzir prethodne dvije definicije, i stavimo $G = G_{\mathbb{K}}$, možemo promatrati reprezentaciju

$$\rho : G_{\mathbb{K}} \to GL_n(k),$$

koju zovemo n-dimenzionalna Galoisova reprezentacija.

Cilj ovog poglavlja nam je reći nešto više o Galoisovim reprezentacijama pridruženim eliptičkim krivuljama. To su *mod m* 2-dimenzionalne reprezentacije. Preciznije, to su monomorfizmi oblika

$$\rho_{E,m} : G_{\mathbb{K}} \to GL_2(\mathbb{Z}/m\mathbb{Z}).$$

Napomena 5.3. Neka je $\sigma \in G_{\mathbb{K}}$. Za svake dvije točke P i Q na eliptičkoj krivulji vrijedi

$$\sigma(P+Q) = \sigma(P) + \sigma(Q).$$

To je zato što je zbroj točaka na eliptičkoj krivulji dan racionalnim funkcijama sa svim koeficijentima iz polja $\mathbb{K}$, kao što smo mogli vidjeti u poglavlju 2.
Iz ovoga zaključujemo kako σ fiksira grupu $E[m]$, tj. skup svih elemenata iz pogrupe točaka reda m eliptičke krivulje E. Tako smo dobili endomorfizam (induciran sa σ) $E[m] \to E[m]$.
Pokažimo još da je preslikavanje σ injektivno. Neka su $P,Q \in E[m]$ za koje vrijedi $\sigma(P) = \sigma(Q)$, imamo: $O = \sigma(P) - \sigma(Q) = \sigma(P-Q)$ pa zaključujemo da je $P-Q = O$, odnosno $P = Q$.
Dakle, gore spomenuti endomorfizam je i automorfizam pa možemo promatrati i grupu $Aut(E[m])$.

Sada ćemo vidjeti na koji način su grupe $Aut(E[m])$ i $GL_2(\mathbb{Z}/m\mathbb{Z})$ povezane kada ih gledamo pod djelovanjem grupe $G_{\mathbb{K}}$.

Već smo vidjeli u propoziciji 2.12 da za cijeli broj $m \neq 0$ vrijedi

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

Ovdje m može biti proizvoljan cijeli broj $\neq 0$ baš zbog toga što promatramo polja karakteristike 0, no kada bismo imali polje karakteristike $char(\mathbb{K}) = k > 0$, m moramo uzeti kao cijeli broj $\neq 0$ koji je relativno prost s k.
Sada izaberimo bazu $\{P_1, P_2\}$ za $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. To znači da se svaki element iz

$E[m]$ može prikazati u obliku $a_1P_1 + a_2P_2$, gdje su $a_1, a_2 \in \mathbb{Z}$.

Neka je

$$\alpha_E : E(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$$

automorfizam eliptičke krivulje E. Tada iz napomene 5.3 vidimo da α_E preslikava $E[m]$ u $E[m]$, tj. imamo homomorfizam

$$\alpha_{E,m} : E[m] \to E[m].$$

Nadalje, postoje $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ takvi da je

$$\alpha_E(P_1) = aP_1 + cP_2,$$

$$\alpha_E(P_2) = bP_1 + dP_2.$$

Dakle, svaki homomorfizam $\alpha_{E,m} : E[m] \to E[m]$ je reprezentiran nekom 2×2 matricom $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}/m\mathbb{Z})$ pa imamo $Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$.

Napomena 5.4. Vidimo da smo na ovaj način dobili homomorfizam grupa

$$\rho_{E,m} : G_{\mathbb{K}} \to GL_2(\mathbb{Z}/m\mathbb{Z}),$$

$$\sigma \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Primijetimo još da je $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}/m\mathbb{Z})$ zbog toga što je α_E automorfizam, tj. ima inverz.

Napomena 5.5. Galoisovu reprezentaciju smo mogli definirati na još jedan način, kao

$$\rho_{E,m} : Gal(\mathbb{Q}(E[m])/\mathbb{Q}) \to GL_2(\mathbb{Z}/m\mathbb{Z}).$$

Motivacija za to je sljedeća:

$$Im(\rho_{E,m}) \cong \frac{Gal(\overline{\mathbb{Q}}/\mathbb{Q})}{Ker(\rho_{E,m})} \cong \frac{Gal(\overline{\mathbb{Q}}/\mathbb{Q})}{Gal(\overline{\mathbb{Q}}/\mathbb{Q}(E[m]))} \cong Gal(\mathbb{Q}(E[m])/\mathbb{Q}),$$

gdje je $\mathbb{Q}(E[m])$ najmanje polje koje sadrži sve elemente iz $E[m]$, tzv. m-to djelidbeno polje od E. Također, vrijedi da je ono Galoisovo nad $\mathbb{Q}$ pa je gornji izraz dobro definiran.

Sada ćemo vidjeti što se događa ako na eliptičkoj krivulji nad $\mathbb{Q}$ postoji neka točka reda m.

Dakle, neka je E eliptička krivulja nad $\mathbb{Q}$ i neka je P_1 točka na E reda m. Tada postoji P_2 takav da je $E[m] = \langle P_1, P_2 \rangle$. Kako svaki element iz $G_{\mathbb{Q}}$ fiksira P_1, vrijedi da je

$$\alpha_{E,m}(\sigma) = \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}, \text{ za svaki } \sigma \in G_{\mathbb{Q}}.$$

Ovu činjenicu ćemo koristiti u 10. poglavlju kada budemo dokazivali da se torzijske grupe spomenute u Mazurovom teoremu pojavljuju nad svim kvadratnim poljima.

Poglavlje 6

Djelidbeni polinomi

U ovom poglavlju definiramo tzv. djelidbene polinome koji će nam biti korisni u traženju torzijskih točaka fiksnog reda eliptičkih krivulja nad poljima algebarskih brojeva. Prvo ih definiramo i navodimo neka osnovna svojstva te primjerom pokazujemo kako s njima možemo računati.

Neka su $a, b \in \mathbb{Z}$ i neka je

$$E: \ y^2 = x^3 + ax + b$$

eliptička krivulja. Definiramo djelidbene polinome ψ_n na sljedeći način:

$\psi_0 = 0$,

$\psi_1 = 1$,

$\psi_2 = 2y$,

$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$,

$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$,

$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$, za $m \geq 2$,

$2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$, za $m \geq 3$.

Polinom ψ_n nazivamo $n-$tim djelidbenim polinomom.

Nadalje, definiramo i polinome

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$

$$4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-1}\psi_{m+1}^2.$$

U sljedećem teoremu navdimo neka osnovna svojstva djelidbenih polinoma:

Teorem 6.1. *Neka je $m \in \mathbb{N}$. Tada vrijedi:*
(1) *ψ_m, ϕ_m, $y^{-1}\omega_m$ za neparne m i $(2y)^{-1}\psi_m$, ϕ_m, ω_m za parni m su polinomi u $\mathbb{Z}[x,y^2]$. Supstitucijom $y^2 = x^3 + ax + b$ dobivamo polinome u $\mathbb{Z}[x]$.*
(2) *Ako gledamo ψ_m i ϕ_m kao polinome u $\mathbb{Z}[x]$, tada je*

$$\phi_m(x) = x^{m^2} + \textit{monomi nižeg stupnja},$$

$$\psi_m^2(x) = m^2 x^{m^2-1} + \textit{monomi nižeg stupnja}.$$

(3) *Ako je $P \in E(\mathbb{Q})$, tada je*

$$mP = \left(\frac{\phi_m(P)}{\psi_m^2(P)}, \frac{\omega_m(P)}{\psi_m^3(P)} \right).$$

Prva dva svojstva možemo dokazati indukcijom, a treće izravno [18], ali dokaz je tehnički kompliciran pa ga izostavljamo.

Primijetimo da je, za točku $P = (x,y)$, $mP = O$ ako i samo ako je $\psi_m(x) = 0$. Ova činjenica nam daje metodu pronalaženja x-koordinata točaka iz $E[m]$. Mogući kandidati su nultočke polinoma ψ_m, kojih prema teoremu 6.1 ima $\frac{m^2-1}{2}$.
No, ako je α nultočka polinoma $\psi_m(x)$ iz polja $\mathbb{K}$ to ne znači da postoji točka P takva da je $mP = O$, samo znači da postoji takva točka P s x-koordinatom iz $\mathbb{K}$. Želimo da i y-koordinata bude iz $\mathbb{K}$. Ako je $\alpha^3 + a\alpha + b$ kvadrat u $\mathbb{K}$, tada je i y-koordinata točke P iz $\mathbb{K}$.
Polinom ϕ_m je stupnja $\frac{m^2-1}{2}$ pa zaključujemo da je u najgorem slučaju x-koordinata od P definirana nad poljem stupnja $\frac{m^2-1}{2}$, a y-koordinata će biti definirana nad istim poljem ili nad proširenjem stupnja 2 od tog polja.

Iz sljedećeg primjera će biti jasno kako se točno koriste djelidbeni polinomi u postupku kojeg smo sada opisali.

Primjer 6.2. Neka je

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

eliptička krivulja definirana nad $\mathbb{Q}$. Nalazimo treći djelidbeni polinom pridružen toj eliptičkoj krivulji, on glasi

$$\psi_3(x) = 3 \cdot \left(x^4 + 2x^2 + 8x - \frac{1}{3} \right).$$

To je ireducibilan polinom nad $\mathbb{Q}$. Odmah zaključujemo kako eliptička krivulja E nema točaka reda 3 s koordinatama iz $\mathbb{Q}$. Također, ne postoje točke reda 3 na E niti nad jednim kvadratnim ili kubnim poljem.

Zanimljivo je i spomenuti kako se pomoću djelidbenih polinoma može dokazati i Lutz-Nagellov teorem iz poglavlja 2.3. Više o tome možemo naći u [18].

Poglavlje 7

Modularne krivulje

Cilj ovog poglavlja je definirati modularne krivulje koje će biti prostor parametara klasa izomorfizama eliptičkih krivulja s nekim svojstvom. Koristit ćemo ih u poglavlju 10 kod određivanja postoje li eliptičke krivulje s određenom torzijskom grupom nad zadanim (kvadratnim) poljem.

Definicija 7.1. *Modularna grupa $SL_2(\mathbb{Z})$ je*

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}, ad-bc = 1 \right\}.$$

Sada ćemo definirati i neke podgrupe ove modularne grupe.

Definicija 7.2. *Neka je $N \in \mathbb{N}$. Glavna kongruencijska podgrupa nivoa N je*

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Podgrupa Γ od $SL_2(\mathbb{Z})$ je kongruencijska podgrupa ako je $\Gamma(N) \leq \Gamma$, za neki $N \in \mathbb{N}$. Ako je N najmanji takav, kažemo da je Γ kongruencijska podgrupa nivoa N.

Navodimo i sljedeće dvije kongruencijske podgrupe:

Definicija 7.3.

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}.$$

Uočimo da vrijedi

$$\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq SL_2(\mathbb{Z}).$$

Neka je E eliptička krivulja. Tada joj možemo pridružiti rešetku Λ. Rešetka $\Lambda \subset \mathbb{C}$ je skup svih točaka oblika $w_1 m + w_2 n$, gdje su $m,n \in \mathbb{Z}$, $w_1, w_2 \in \mathbb{C}$ te su w_1 i w_2 linearno nezavisni nad $\mathbb{R}$.

Bez smanjenja općenitosti možemo uzeti da je svaka rešetka Λ oblika $\Lambda = \mathbb{Z} + \tau\mathbb{Z}, \tau \in \mathcal{H}$, gdje je

$$\mathcal{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}$$

gornja poluravnina.

Označimo

$$SL_2(\mathbb{Z})\backslash\mathcal{H} = \{SL_2(\mathbb{Z})\tau : \tau \in \mathcal{H}\}$$

Budući da za $\gamma \in SL_2(\mathbb{Z})$ vrijedi da su $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ i $\Lambda = \mathbb{Z} + \gamma(\tau)\mathbb{Z}$ iste rešetke, postoji izomorfizam između $SL_2(\mathbb{Z})\backslash\mathcal{H}$ i skupa eliptičkih krivulja nad $\mathbb{C}$ (do na izomorfizam). Kažemo da je $SL_2(\mathbb{Z})\backslash\mathcal{H}$ prostor parametara za eliptičke krivulje. Na sličan način grupe $\Gamma(N)$, $\Gamma_0(N)$ i $\Gamma_1(N)$ generiraju prostor parametara eliptičkih krivulja s nekim svojstvom.

Definicija 7.4. *Za kongruencijsku podgrupu* Γ *od* $SL_2(\mathbb{Z})$ *definiramo modularnu krivulju kao kvocijentni prostor orbita od* Γ*, to jest*

$$Y(\Gamma) = \Gamma \setminus \mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}.$$

Analogno definiramo modularne krivulje za $\Gamma_0(N)$, $\Gamma_1(N)$ i $\Gamma(N)$ na sljedeći način:

$$Y_0(N) = \Gamma_0(N) \setminus \mathcal{H},\ Y_1(N) = \Gamma_1(N) \setminus \mathcal{H},\ Y(N) = \Gamma(N) \setminus \mathcal{H}.$$

Nadalje, definiramo skupove klasa izomorfizama eliptičkih krivulja s nekim svojstvom te ćemo pokazati koja je veza tih skupova i upravo definiranih modularnih krivulja.

Definicija 7.5. $S_0(N) = \{[E,C] : E$ *eliptička krivulja,* C *je podgrupa reda* $N\}$.
$[E,C]$ *ovdje označava klasu izomorfizama.* (E,C) *i* (E',C') *su izomorfni ako postoji izomorfizam eliptičkih krivulja* $f : E \to E'$ *takav da je* $f(C) = C'$.

$S_1(N) = \{[E,Q] : E$ *eliptička krivulja,* Q *je točka reda* $N\}$.
$[E,Q]$ *ovdje označava klasu izomorfizama.* (E,Q) *i* (E',Q') *su izomorfni ako postoji izomorfizam eliptičkih krivulja* $f : E \to E'$ *takav da je* $f(Q) = Q'$.

$S(N) = \{[E,(P,Q)] : E$ *eliptička krivulja,* $\langle P,Q\rangle \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$,
$e_N(P,Q) = e^{2\pi i/N}\}$.
$[E,(P,Q)]$ *ovdje označava klasu izomorfizama.* $(E,(P,Q))$ *i* $(E',(P',Q'))$ *su izomorfni ako postoji izomorfizam eliptičkih krivulja* $f : E \to E'$ *takav da je* $f(P) = P'$ *i* $f(Q) = Q'$.

Označimo sada sa E_τ eliptičku krivulju dobivenu kao $E_\tau = \mathbb{C}/\Lambda_\tau$, $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$.

Teorem 7.6. *Neka je* $N \in \mathbb{N}$.
(1) Prostor parametara za $\Gamma_0(N)$ *je*

$$S_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau\rangle] : \tau \in \mathcal{H}\}.$$

Dvije točke $[E_\tau, \langle 1/N + \Lambda_\tau\rangle]$ *i* $[E_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle]$ *su jednake ako i samo ako je* $\Gamma_0(N)\tau = \Gamma_0(N)\tau'$. *Dakle, postoji bijekcija*

$$\phi_0 : S_0(N) \to Y_0(N),\ [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] \to \Gamma_0(N)\tau.$$

(2) Prostor parametara za $\Gamma_1(N)$ *je*

$$S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}.$$

Dvije točke $[E_\tau, 1/N+\Lambda_\tau]$ *i* $[E_{\tau'}, 1/N+\Lambda_{\tau'}]$ *su jednake ako i samo ako je* $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. *Dakle, postoji bijekcija*

$$\phi_1 : S_1(N) \to Y_1(N),\ [\mathbb{C}/\Lambda_\tau, 1/N+\Lambda_\tau] \to \Gamma_1(N)\tau.$$

(3) Prostor parametara za $\Gamma(N)$ *je*

$$S(N) = \{[E_\tau, (\tau/N+\Lambda_\tau, 1/N+\Lambda_\tau)] : \tau \in \mathcal{H}\}.$$

Dvije točke $[E_\tau, (\tau/N+\Lambda_\tau, 1/N+\Lambda_\tau)]$ *i* $[E_{\tau'}, (\tau'/N+\Lambda_{\tau'}, 1/N+\Lambda_{\tau'})]$ *su jednake ako i samo ako je* $\Gamma(N)\tau = \Gamma(N)\tau'$. *Dakle, postoji bijekcija*

$$\phi : S(N) \to Y(N),\ [\mathbb{C}/\Lambda_\tau, (\tau/N+\Lambda_\tau, 1/N+\Lambda_\tau)] \to \Gamma(N)\tau.$$

Dokaz gornjeg teorema se može naći u [11].
Primijetimo da ako stavimo $N = 1$, imamo $Y_0(1) = Y_1(1) = Y(1) = SL_2(\mathbb{Z})\backslash\mathcal{H}$ te svaka od ovih modularnih krivulja predstavlja skup klasa izomorfizama eliptičkih krivulja.
Nadalje, skupovi $Y(N)$, $Y_0(N)$ i $Y_1(N)$ nisu kompaktni, ali može ih se kompaktificirati. Uzmimo $\mathcal{H}^* = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$ te definirajmo $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$, za neku kongruencijsku grupu Γ. Sada je $X(\Gamma)$ jednak uniji od $\mathcal{H}$ i konačnom skupu klasa elemenata od $\mathbb{Q} \cup \{\infty\}$ koji se zovu kuspovi. Više o kuspovima i broju kuspova na modularnim krivuljama imamo u [4].
Točke u $S(N)$, $S_0(N)$ i $S_1(N)$, odnosno $Y(N)$, $Y_0(N)$ i $Y_1(N)$ određuju krivulje s nekom strukturom do na izomorfizam. Promatrajmo sada samo eliptičku krivulju. Za točke iz $S_0(N)$, K-racionalna točka definira eliptičku krivulju do na $\overline{K}$-izomorfizam, a za $S(N)$ i $S_1(N)$, eliptička krivulja je definirana do na K-izomorfizam.

Napomena 7.7. Modularne krivulje $X_1(11)$, $X_1(14)$ i $X_1(15)$ su jedine modularne krivulje oblika $X_1(N)$, $N \in \mathbb{N}$ koje su genusa 1. Te krivulje su eliptičke krivulje nad $\mathbb{Q}$.

Krivulje $X_1(13)$, $X_1(16)$ i $X_1(18)$ su jedine krivulje genusa 2, dakle hipereliptičke krivulje.

Uzmimo sada jednu modularnu krivulju i pokažimo kako izgledaju parovi eliptičke krivulje i točke reda N pridruženi određenoj točki te modularne krivulje. Pogledajmo primjer

za $N = 14$. Ostali se mogu naći u [13].

Primjer 7.8.

$$X_1(14): \ s^2 + st + s = t^3 - t.$$

Za svaku točku $(t,s) \in X_1(14)$ pogledat ćemo par (E_{14}, P) eliptičke krivulje E i točke $P \in E_{14}$ reda 14.

Ako je $P = (0,0)$ točka reda 14, tada eliptička krivulja E_{14} ima sljedeći oblik:

$$E_{14} = y^2 + axy + by = x^3 + bx^2,$$

gdje je

$$a = \frac{t^4 - st^3 + (2s-4)t^2 - st + 1}{(t+1)(t^3 - 2t^2 - t + 1)^2},$$

$$b = \frac{-t^7 + 2t^6 + (2s-1)t^5 + (-2s-1)t^4 + (-2s+2)t^3 + (3s-1)t^2 - st}{(t+1)^2(t^3 - 2t^2 - t + 1)^2}.$$

Poglavlje 8

Hipereliptičke krivulje

U ovom poglavlju će svako polje $\mathbb{K}$ biti savršeno, a svaka krivulja C (nad $\mathbb{K}$) će biti glatka, projektivna i ireducibilna.

Već smo spomenuli (u napomeni 7.7) kako su neke modularne krivulje hipereliptičke. Također smo spomenuli kako ćemo ih koristiti u poglavlju 10 pa nam je to motivacija da precizno definiramo pojam hipereliptičke krivulje te proučimo neka njena svojstva.

Definicija 8.1. *Hipereliptička krivulja je algebarska krivulja dana jednadžbom oblika* $y^2 = f(x)$, *gdje je* $f(x)$ *polinom stupnja* $n > 4$ *s* n *različitih korijena.*

Stupanj polinoma određuje genus krivulje; polinomi stupnja $2g+1$ i $2g+2$ određuju krivulju genusa g. Sve krivulje genusa 2 su hipereliptičke.

U nastavku ćemo definirati još nekoliko korisnih pojmova, koji će nam pomoći da razumijemo već spomenuti Jacobijan krivulje C, koji će u slučaju krivulja genusa 2 imati neka dobra svojstva.

Neka je $\mathbb{K}$ polje i C krivulja nad $\mathbb{K}$. Definiramo grupu Div_C kao slobodnu Abelovu grupu generiranu s $C(\overline{\mathbb{K}})$, skupom svih točaka od C definiranih nad algebarskim zatvorenjem $\overline{\mathbb{K}}$ od $\mathbb{K}$. Elemente te grupe zovemo divizori. Dakle, divizor D je $\mathbb{Z}$-linearna kombinacija točaka od C.

Grupa $Gal(\overline{\mathbb{K}}/\mathbb{K})$ djeluje na $C(\overline{\mathbb{K}})$ na uobičajeni način. To inducira djelovanje na grupu divizora Div_C. Divizore koji su invarijantni na to djelovanje zovemo $\mathbb{K}$-racionalnim divizorima. Podgrupu $\mathbb{K}$-racionalnih divizora označavamo s $Div_C(\mathbb{K})$.

Primjer 8.2. Neka je $C: \ y^2 = f(x)$ hipereliptička krivulja nad $\mathbb{K}$. Fiksirajmo $\xi \in \mathbb{K}$ i neka je $\eta \in \overline{\mathbb{K}}$ takav da je $\eta^2 = f(\xi)$. Tada je

$$D_\xi = (\xi, \eta) + (\xi, -\eta)$$

$\mathbb{K}$-racionalni divizor na C, to jest $D_\xi \in Div_C(\mathbb{K})$.

Nadalje, definiramo stupanj divizora kao sumu njegovih koeficijenata. Preciznije, ako imamo divizor

$$D = \sum_P n_P P,$$

tada je stupanj

$$deg(D) = \sum_P n_P \in \mathbb{Z}.$$

Ovime smo dobili homomorfizam $deg : Div_C \to \mathbb{Z}$. Njegova jezgra, u oznaci Div_C^0, je podgrupa divizora stupnja nula.

Ako je $f \in \overline{\mathbb{K}}(C)^\times$ racionalna funkcija na C, možemo joj pridružiti divizor

$$div(f) = \sum_P v_P(f) \cdot P \in Div_C,$$

gdje $v_P(f)$ označava red od f u točki P. Ako f u P ima pol, onda je $v_P(f)$ red pola, a ako f u P ima nultočku, onda je $v_P(f)$ kratnost te nultočke. Budući da svaka ne-nul funkcija na C ima konačno mnogo nultočki i polova, suma je konačna pa je divizor dobro definiran. Također, suma redova polova jednaka je sumi redova nultočaka.

Ovime smo dobili homomorfizam

$$div : \overline{\mathbb{K}}(C)^\times \to Div_C,$$

čiju sliku označavamo s $Princ_C$. Kojezgra od div je Picardova grupa,

$$Pic_C = Div_C / Princ_C.$$

Vrijedi: $Princ_C \subset Div_C^0$.

Sada pogledajmo restrikciju gornje funkcije deg,

$$deg : Pic_C \to \mathbb{Z}.$$

Ona ima jezgru

$$Pic_C^0 = Div_C^0 / Princ_C.$$

Definicija 8.3. *Kažemo da su dva divizora D i D' linearno ekvivalentni, i pišemo $D \sim D'$, ako imaju istu sliku u Picardovoj grupi Pic_C. Tu sliku divizora D označavamo s $[D]$, to je klasa ekvivalencije relacije $\sim$.*

Teorem 8.4. *Neka je C krivulja genusa g nad $\mathbb{K}$. Tada postoji Abelova mnogostrukost J genusa g nad $\mathbb{K}$ takva da postoji izomorfizam $Pic_C^0 \to J(\overline{\mathbb{K}})$.*

Mnogostrukost J iz iskaza teorema nazivamo Jacobijan od C.
Ako je C krivulja genusa 1, tada je J jednodimenzionalna Abelova mnogostrukost, dakle eliptička krivulja. Ako C ima $\mathbb{K}$-racionalnu točku (dakle C je eliptička krivulja), tada su J i C izomorfni. U protivnom, J i C ne mogu biti izomorfni, jer J uvijek ima $\mathbb{K}$-racionalnu točku (grupovni neutral).
Sada navodimo još jednu korisnu propoziciju.

Propozicija 8.5. *Neka je C krivulja nad $\mathbb{K}$ s genusom $g \geq 1$ i Jacobijanom J te neka je $[D_0]$ klasa $\mathbb{K}$-racionalnih divizora stupnja 1. Tada je*

$$i_{[D_0]} : C \to J,\ P \mapsto [P - D_0]$$

ulaganje.

Sada je ideja dobiti informacije o $C(\mathbb{Q})$ pomoću navedenog ulaganja u J. Preslikavanje i inducira bijekciju između $C(\mathbb{Q})$ i presjeka $J(\mathbb{Q})$ i $i(C)$. Pokušat ćemo pomoću informacija koje znamo o J i grupovnoj strukturi na J zaključiti nešto o $C(\mathbb{Q})$.

Znamo da je J Abelova mnogostrukost pa to znači da su $J(\mathbb{K})$ i $J(\overline{\mathbb{K}})$ Abelove grupe. Sljedeći teorem nam govori više o strukturi tih grupa.

Teorem 8.6. ***(Mordell-Weil)*** *Neka je $\mathbb{K} = \mathbb{Q}$ i neka je J Jacobian neke krivulje nad $\mathbb{K}$. Tada je Abelova grupa $J(\mathbb{K})$ konačnogenerirana.*

Iz strukturnog teorema za konačnogenerirane Abelove grupe možemo zaključiti da vrijedi sljedeće:

$$J(\mathbb{K}) \cong J(\mathbb{K})_{tors} \times \mathbb{Z}^r.$$

Dokaz ovog teorema je kompliciran pa detalje izostavljamo, navest ćemo samo ideju. Teorem se dokazuje u dva koraka, prvi je tzv. slabi Mordell-Weilov teorem u kojem dokazujemo da je $J(\mathbb{K})/mJ(\mathbb{K})$, za neki $m \geq 2$, konačna grupa. U drugom koraku dokazujemo da iz prvog koraka i činjenice da postoji funkcija visine na $J(\mathbb{K})$ slijedi da je grupa konačnogenerirana.

Recimo sada nešto i o torzijskoj grupi $J(\mathbb{Q})_{tors}$, gdje je J Jacobijan krivulje nad $\mathbb{Q}$.
Neka je p prost broj u kojemu krivulja C genusa g ima dobru redukciju, to jest kada zapišemo C kao jednadžbu s cjelobrojnim koeficijentima i reduciramo te koeficijente modulo p, opet ćemo dobiti neku krivulju $\overline{C}$ genusa g. Tada imamo (kanonsku) redukciju

$$C(\mathbb{Q}) \to \overline{C}(\mathbb{F}_p), \;\; P \mapsto \overline{P}.$$

Sada navodimo propoziciju koja nam pomaže razumjeti strukturu torzijske grupe Jacobijana od C.

Propozicija 8.7. *Uz gornje pretpostavke, p je također broj u kojemu J ima dobru redukciju. Redukcija $J(\mathbb{Q}) \to \overline{J}(\mathbb{F}_p)$ je homomorfizam grupa. Ako je $p \geq 3$, tada je restrikcija gornjeg homomorfizma na $J(\mathbb{Q})_{tors}$ injektivna. Nadalje, ako $P_0 \in C(\mathbb{Q})$ definira ulaganje*

$i_{P_0} : C \to J$, *onda sljedeći dijagram komutira:*

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{i_{P_0}} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ \overline{C}(\mathbb{F}_p) & \xrightarrow{i_{\overline{P}_0}} & \overline{J}(\mathbb{F}_p) \end{array}$$

Prethodna propozicija (čiji dokaz imamo u [16]) je koristan rezultat jer nam omogućuje da dobijemo gornju odgradu za $|J(\mathbb{Q})_{tors}|$ iz činjenice da $|J(\mathbb{Q})_{tors}|$ dijeli $|\overline{J}(\mathbb{F}_p)|$ za sve p u kojima je redukcija dobra. Donju ogradu možemo dobiti jednostavno traženjem torzijskih točaka.

Poglavlje 9

Eliptičke krivulje nad kvadratnim poljima

U ovom poglavlju ćemo iskazati nekoliko bitnih tvrdnji vezanih uz rang i torziju eliptičkih krivulja koje ćemo koristiti u sljedećem poglavlju.

Definicija 9.1. *Neka je E eliptička krivulja definirana nad poljem algebarskih brojeva $\mathbb{K}$. Twist od E je glatka krivulja C (nad $\mathbb{K}$) koja je izomorfna s E nad $\overline{\mathbb{K}}$.*

Dakle, ako je C (nad $\mathbb{K}$) twist od E (nad $\mathbb{K}$), tada postoji izomorfizam $\Phi : C \to E$, koji je definiran nad $\overline{\mathbb{K}}$.

Primjer 9.2. Neka je E eliptička krivulja nad $\mathbb{K}$ zadana Weierstrassovom jednadžbom

$$E: \ y^2 = f(x),$$

te neka je $\mathbb{K}(\sqrt{d})$ kvadratno proširenje od $\mathbb{K}$.
Tada je s jednadžbom

$$C: \ dy^2 = f(x)$$

dan jedan twist od E te je izomorfizam $\Phi : C \to E$ dan sa $\Phi(x,y) = (x, y\sqrt{d})$.
Ovakve twistove zovemo kvadratnim twistovima i označavamo ih s E^d.

Propozicija 9.3. *Neka je* $\mathbb{K}$ *polje algebarskih brojeva,* $\mathbb{L}$ *kvadratno proširenje od* $\mathbb{K}$*,* $\mathbb{L} = \mathbb{K}(\sqrt{d})$*, te E eliptička krivulja definirana nad* $\mathbb{K}$*. Tada je*

$$rk(E(\mathbb{L})) = rk(E(\mathbb{K})) + rk(E^d(\mathbb{K})),$$

gdje E^d *označava kvadratni twist.*

Dokaz. Neka je E eliptička krivulja u kratkoj Weierstrassovoj formi

$$E: \ y^2 = x^3 + ax + b$$

te neka je twist E^d zapisan u obliku

$$E^d: \ dy^2 = x^3 + ax + b,$$

gdje su $a, b \in \mathbb{K}$. Neka je σ generator od $Gal(\mathbb{L}/\mathbb{K})$. Prvo primijetimo da točke na $(x,y) \in E^d(\mathbb{K})$ odgovaraju točkama $(x, y\sqrt{d}) \in E(\mathbb{L})$, gdje su $x, y \in \mathbb{K}$.
Prvo dokazujemo da je

$$rk(E(\mathbb{L})) \geq rk(E(\mathbb{K})) + rk(E^d(\mathbb{K})).$$

Ako je $rk(E(\mathbb{L})) = 0$ ili $rk(E^d(\mathbb{K})) = 0$, onda smo gotovi. Ako E i E^d imaju pozitivan rang nad $\mathbb{K}$, tada trebamo dokazati da će dvije točke beskonačnog reda, od kojih jedna dolazi $E(\mathbb{K})$, a druga od $E^d(\mathbb{K})$, nužno biti nezavisne. Neka su $P_1 \in E(\mathbb{K})$ i $P_2 \in E^d(\mathbb{K})$ točke beskonačnog reda. Pretpostavimo suprotno, to jest da su linearno zavisne. Tada postoje $\alpha, \beta \in \mathbb{Z}$, ne oba jednaka nuli, takvi da vrijedi

$$\alpha P_1 + \beta P_2 = O.$$

Djelujemo sa σ na ovu jednadžbu te budući da je $\sigma P_2 = -P_2$, dobivamo

$$\alpha P_1 - \beta P_2 = O.$$

Zbrajajući ove dvije jednadžbe, dobivamo $\alpha = 0$ i $\beta = 0$, što je kontradikcija.
Sada dokazujemo da je

$$rk(E(\mathbb{L})) \leq rk(E(\mathbb{K})) + rk(E^d(\mathbb{K})).$$

Neka je

$$rk(E(\mathbb{K})) = r_1,\ rk(E^d(\mathbb{K})) = r_2,\ rk(E(\mathbb{L})) = r,$$

$$\langle P_1,...,P_{r_1}\rangle = E(\mathbb{K})/E(\mathbb{K})_{tors},$$

$$\langle P_{r_1+1},...,P_{r_1+r_2}\rangle = E^d(\mathbb{K})/E^d(\mathbb{K})_{tors},$$

$$\langle T_1,...,T_r\rangle = E(\mathbb{L})/E(\mathbb{L})_{tors}.$$

Pretpostavimo da je $P = (x_1 + x_2\sqrt{d}, y_1 + y_2\sqrt{d}) \in E(\mathbb{L})$ točka beskonačnog reda. Budući da je E definirana nad $\mathbb{K}$, zaključujemo da je $\sigma P \in E(\mathbb{L})$. Tada, direktnim računom, možemo provjeriti da je

$$P + \sigma P \in E(\mathbb{K}), P - \sigma P \in E^d(\mathbb{K}),$$

te je

$$2P \in E(\mathbb{K}) + E^d(\mathbb{K}).$$

Zaključujemo da je

$$\langle 2T_1,...,2T_r\rangle / E(\mathbb{L})_{tors}$$

podgrupa od

$$\langle P_1,...,P_{r_1+r_2}\rangle / E(\mathbb{L})_{tors}.$$

Dakle $\langle P_1,...,P_{r_1+r_2}\rangle$ je konačnog indeksa u $E(\mathbb{L})/E(\mathbb{L})_{tors}$, što dokazuje $rk(E(\mathbb{L})) \leq rk(E(\mathbb{K})) + rk(E^d(\mathbb{K}))$. □

Prethodna propozicija će nam biti bitna u slučaju kada je $\mathbb{K} = \mathbb{Q}$, a $\mathbb{L}$ je kvadratno proširenje od $\mathbb{Q}$, budući da je lakše izračunati rang eliptičke krivulje nad $\mathbb{Q}$, nego nad proširenjima od $\mathbb{Q}$.

Propozicija 9.4. *Neka je E eliptička krivulja nad $\mathbb{Q}$ i $\mathbb{L}$ kvadratno proširenje od $\mathbb{K}$, $\mathbb{L} = \mathbb{K}(\sqrt{d})$. Tada je*

$$E(\mathbb{L})_{(2')} \cong E(\mathbb{K})_{(2')} \oplus E^d(\mathbb{K})_{(2')},$$

gdje $E(\mathbb{L})_{(2')}$ podgrupa od $E(\mathbb{L})$ točaka neparnog reda.

Dokaz ove propozicije može se provesti analogno dokazu prethodne propozicije, ako točke beskonačnog reda zamijenimo točkama neparnog reda.

Propozicija 9.5. *Neka je $E/\mathbb{K}$ eliptička krivulja te neka $d \in \mathbb{K}$ nije kvadrat. Tada je*

$$E(\mathbb{K})[2] \cong E^d(\mathbb{K})[2].$$

Dokaz. Neka je

$$E:\ y^2 = x^3 + ax + b,$$

te neka je kvadratni twist zapisan kao

$$E^d:\ y^2 = x^3 + ad^2x + bd^3.$$

Sjetimo se da je $P \in E(\mathbb{K})$ točka reda 2 ako i samo ako je $y(P) = 0$, to jest $P = (t, 0)$, gdje je $t \in \mathbb{K}$ korijen od $x^3 + ax + b$. Međutim, t je korijen od $x^3 + ax + b$ ako i samo ako je td korijen od $x^3 + ad^2x + bd^3$. Dakle, broj nultočaka od $x^3 + ax + b$ i $x^3 + ad^2x + bd^3$ se poklapa, pa je

$$E(\mathbb{K})[2] = E^d(\mathbb{K})[2].$$

□

Sada ćemo iskazati teorem koji nam govori koje su moguće torzijske grupe eliptičkih krivulja nad kvadratnim poljima. Kada budemo fiksirali neko kvadratno polje i pitali se koje su moguće torzije nad njim, ovaj teorem će nam biti od koristi, budući da imamo samo određeni broj grupa koje moramo provjeriti.

Teorem 9.6. ***(Kamienny-Kenku-Momose)*** *Neka E varira po svim eliptičkim krivuljama nad svim kvadratnim poljima $\mathbb{K}$. Tada će $E(\mathbb{K})_{tors}$ biti jedna od sljedećih 26 grupa:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 1, ..., 16, 18,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1, ..., 6,$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1, 2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Još ćemo iskazati jedan teorem koji nam govori što možemo očekivati promatramo li neke određene torzijske grupe eliptičkih krivulja nad poljima algebarskih brojeva.

Teorem 9.7. *Neka je* $\mathbb{K}$ *polje algebarskih brojeva. Postoji konačno mnogo (do na izomorfizam) eliptičkih krivulja s torzijom* $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ *i* $\mathbb{Z}/18\mathbb{Z}$.

Dokaz slijedi izravno iz Faltingsovog teorema koji kaže da svaka krivulja genusa ≥ 2 ima samo konačno mnogo točaka nad bilo kojim poljem algebarskih brojeva i iz činjenice da su modularne krivulje pridružene ovim torzijskim grupama genusa 2.

Poglavlje 10

Torzijske grupe eliptičkih krivulja nad kvadratnim poljima

U ovom poglavlju opisat ćemo postupak nalaženja torzijske grupe eliptičkih krivulja nad fiksnim kvadratnim poljem.

Dakle, neka je od sada $\mathbb{K}$ neko fiksno kvadratno polje. U teoremu 9.6 smo vidjeli da postoji 26 mogućih torzijskih grupa eliptičkih krivulja nad $\mathbb{K}$. Za svaku od tih 26 grupa ćemo pokazati način na koji možemo zaključiti pojavljuje li se ona kao torzija nad $\mathbb{K}$ ili ne.

Usredotočimo se prvo na 15 mogućih torzijskih grupa za torziju $E(\mathbb{Q})_{tors}$ iz Mazurovog teorema (teorem 2.4). Preciznije, to su grupe

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,2,...,10,12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4.$$

Prvo što želimo je pokazati da se svaka od tih grupa mora pojavljivati kao torzija nad kvadratnim poljem $\mathbb{K}$. Štoviše, to su grupe koje će se pojavljivati beskonačno mnogo puta nad proizvoljnim kvadratnim poljem.

Dakle, zanima nas može li se dogoditi da svaka eliptička krivulja nad $\mathbb{K}$ koja ima točku

reda n ima i neku točku reda većeg od n. Naime, to bi značilo da niti jedna krivulja ne može imati torzijsku grupu $\mathbb{Z}/n\mathbb{Z}$, već to mora biti neka grupa s više elemenata.

Npr. pogledamo li sve krivulje s točkom reda 6 nad $\mathbb{K}$, neke od njih će imati torziju $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, ili neku od preostalih grupa iz teorema 9.6 koje sadrže točku reda 6. Mi zapravo želimo vidjeti da je preostala barem 1 krivulja (iako će se pokazati da ih je preostalo beskonačno mnogo) takva da ona ima torzijsku grupu $\mathbb{Z}/6\mathbb{Z}$.

To ćemo pokazati slično kao što je to u [6], [9] napravljeno za torziju nad $\mathbb{Q}$: iz dodatka A uzmemo opći oblik krivulje s točkom reda 6 i pogledajmo samo cjelobrojne vrijednosti parametra c takve da je $c \equiv \pm 2 \pmod 5$. Iz oblika diskriminante takve eliptičke krivulje E možemo vidjeti da u tim slučajevima broj 5 ne dijeli diskriminantu pa krivulja tada ima dobru redukciju u 5. Sada iz propozicije 3.11 zaključujemo da se 5-slobodni dio torzije ulaže u $E(\mathbb{F}_5)$. No, iz teorema 3.13 vidimo da $E(\mathbb{F}_5)$ ima najviše 10 točaka. Dakle, za vrijednosti c takve da je $c \equiv \pm 2 \pmod 5$ eliptička krivulja E ne može imati torzijsku grupu koja ima više od 10 elemenata. No, sve ostale grupe osim $\mathbb{Z}/6\mathbb{Z}$ koje mogu sadržavati točku reda 6 imaju strogo više od 10 elemenata. Dakle, našli smo beskonačno mnogo krivulja koje imaju torzijsku grupu $\mathbb{Z}/6\mathbb{Z}$.

Ovaj postupak nam daje i način kako da nađemo eliptičku krivulju nad $\mathbb{K}$ s određenom torzijskom grupom. U dodatku A nađemo opći oblik jednadžbe eliptičke krivulje sa željenom torzijskom grupom, i uvrstimo (u gornjem slučaju) $c \equiv \pm 2 \pmod 5$. Krivulja nad $\mathbb{K}$ koju smo dobili tada ima torzijsku grupu $\mathbb{Z}/6\mathbb{Z}$.

Ipak, primjećujemo da gornji postupak nije dobar u baš svim slučajevima. Uzmemo li točke manjeg reda (od 6) nećemo uvijek moći dobiti dovoljno dobru ogradu za broj elemenata u $E(\mathbb{F}_p)$ da bismo mogli zaključiti da se ta točka ne nalazi u nekoj grupi većeg reda.

Dakle, točkama manjeg reda moramo pristupiti drugačije.
Vidjeli smo već u 5. poglavlju da ako eliptička krivulja ima točku reda n nad $\mathbb{K}$, vrijedi

$$\alpha_{E,m}(\sigma) = \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}, \text{ za svaki } \sigma \in G_{\mathbb{K}}.$$

Označimo s $I = \{\alpha_{E,m}(\sigma) : \sigma \in G_{\mathbb{K}}\}$. Tada je

$$I \subseteq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \pmod{n} \right\} = \Gamma_1(n)$$

Ako je $X_I = \{E : \alpha_{E,m}(\sigma) \subseteq I\}$, tada je $X_1(n)$ možemo zapisati kao $X_{\Gamma_1(n)}$.

Uzmimo npr. $n = 4, 8$ i pogledajmo sljedeće skupove:

$$\Gamma_1(8) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \pmod{8} \right\},$$

$$\Gamma_1(4) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \pmod{4} \right\} =$$

$$= \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1,5 & * \\ 0,4 & * \end{bmatrix} \pmod{8} \right\}.$$

Očito je da vrijedi $\Gamma_1(4) \supseteq \Gamma_1(8)$ pa je i $X_1(4) \supseteq X_1(8)$, tj. postoji preslikavanje sa $X_1(8)$ u $X_1(4)$ takvo da $(E,P) \mapsto (E,2P)$. No, ako je $X_I \cong \mathbb{P}^1$, tj. u našem slučaju ako je $X_{\Gamma_1(n)} = X_1(n)$ genusa 0, onda vrijedi i više, tj. vrijedi jednakost do na skup mjere nula. Dokaz ove tvrdnje možemo naći u [22].

Ovo što smo upravo vidjeli nam govori da imamo beskonačno mnogo krivulja nad $\mathbb{K}$ s torzijama čije su odgovarajuće modularne krivulje genusa 0. Genuse modularnih krivulja oblika $X_1(m,n)$ možemo naći u [6]. No, sve krivulje koje sada promatramo, tj. one oblika $X_1(n)$, $n = 1, ..., 10, 12$ i $X_1(2,2n)$, $n = 1,2,3,4$, su genusa 0.
Dakle, uzmemo li bilo koju krivulju iz dodatka A sa željenom torzijskom grupom i uvrstimo u nju koeficijente iz polja $\mathbb{K}$, sigurno ćemo dobiti krivulju koja ima istu torzijsku grupu, jer je skup svih krivulja koje imaju veću torziju mjere nula.

Dakle, ovime smo dokazali da se svih 15 grupa iz Mazurovog teorema moraju pojaviti kao torzijska grupa neke eliptičke krivulje nad fiksnim kvadratnim poljem $\mathbb{K}$.

Pogledajmo sada grupe

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}, \ n = 1,2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Iz svojstava Weilovog sparivanja [19] slijedi da je $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subset E(\mathbb{K})$ samo ako vrijedi $\mathbb{Q}(\zeta_n) \subset \mathbb{K}$. Dakle, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} \subset E(\mathbb{K})$, $n = 1,2$, samo kada je $\mathbb{K} \supset \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ te $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subset E(\mathbb{K})$ samo kada je $\mathbb{K} \supset \mathbb{Q}(i)$. Štoviše, spomenute grupe su uz grupe iz Mazurovog teorema jedine koje se pojavljuju nad $\mathbb{Q}(\sqrt{-3})$ i $\mathbb{Q}(i)$ [10], [12].

Sada se možemo posvetiti ostalim grupama. Nešto je kompliciranije vidjeti pojavljuju li se ostale grupe iz teorema 9.6 kao torzija neke eliptičke krivulje nad fiksnim kvadratnim poljem $\mathbb{K}$.

Problem se svodi na određivanje imaju li odgovarajuće modularne krivulje (odnosno njihove kompaktifikacije) $\mathbb{K}-$racionalnu točku koja nije kusp. Uzmemo li modularnu krivulju $Y_1(m,n)$, njene $\mathbb{K}-$racionalne točke su klase izomorfizama uređenih trojki (E, P_m, P_n), gdje je E eliptička krivulja nad $\mathbb{K}$, a P_m i P_n torzijske točke koje generiraju podgrupu $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Vidimo da čim na kompaktifikaciji $X_1(m,n)$ nađemo $\mathbb{K}-$racionalnu točku koja nije kusp, imamo jednu eliptičku krivulju (do na izomorfizam) s torzijskom grupom $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Neke od odgovarajućih modularnih krivulja su eliptičke, a neke su hipereliptičke. Njihove jednadžbe i jednadžbe koje zadovoljavaju kuspovi na tim krivuljama možemo naći u dodatku B. U njemu se nalaze samo jednadžbe modularnih krivulja za koje nismo već dokazali da se pripadne torzijske grupe (ne) pojavljuju nad $\mathbb{K}$, a ostale imamo u [1] i [21].

Kuspova ima konačno mnogo (jer tražimo nultočke polinoma nekog stupnja n). Nađemo li k kuspova na modularnoj krivulji i k $\mathbb{K}-$racionalnih točaka, možemo zaključiti kako nema eliptičkih krivulja nad $\mathbb{K}$ s odgovarajućom torzijom. Ako nađemo strogo više od k $\mathbb{K}-$racionalnih točaka, tada imamo eliptičku krivulju.

To ćemo napraviti u ovisnosti o tome je li krivulja $X_1(m,n)$ eliptička ili hipereliptička. U napomeni 7.7 smo već rekli kako su krivulje $X_1(11)$, $X_1(14)$ i $X_1(15)$ (odnosno $X_1(1,11)$, $X_1(1,14)$ i $X_1(1,15)$) eliptičke, a $X_1(13)$, $X_1(16)$ i $X_1(18)$ (odnosno $X_1(1,13)$, $X_1(1,16)$

i $X_1(1,18)$) hipereliptičke. Krivulje $X_1(2,10)$ i $X_1(2,12)$ su također eliptičke.

Ako je $X_1(m,n)$ eliptička krivulja, prvi korak je računanje ranga. Njega možemo izračunati u programskom paketu Magma [2]. Ako je rang pozitivan, očito postoji beskonačno mnogo $\mathbb{K}-$racionalnih točaka pa zaključujemo da nad $\mathbb{K}$ postoji eliptička krivulja s torzijskom grupom $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Ako je rang 0, tada tražimo torzijsku grupu eliptičke krivulje $X_1(m,n)$ i provjeravamo jesu li sve torzijske točke kuspovi ili nisu.

Ako je $X_1(m,n)$ hipereliptička krivulja, korisno je promatrati Jacobijane tih krivulja, budući da same hipereliptičke krivulje nemaju strukturu grupe. Računamo rang Jacobijana te krivulje nad $\mathbb{K}$ u Magmi koristeći $2-$spust. Algoritam za 2-spust možemo naći u [17]. On je implementiran samo za Jacobijane definirane nad $\mathbb{Q}$, ali možemo koristiti činjenicu da je

$$rk(J(\mathbb{K})) = rk(J(\mathbb{Q})) + rk(J^d(\mathbb{Q}))$$

da dobijemo rang nad kvadratnim proširenjem $\mathbb{K} = \mathbb{Q}(\sqrt{d})$.

No, treba znati da 2-spust nije algoritam pa iako je u praksi često djelotvoran, nemamo garanciju da ćemo zaista dobiti traženi rang. Neke od tih slučajeva možemo riješiti metodom opisanom u [7].

Ako je rang jednak nuli, nastavljamo s računanjem torzijske grupe Jacobijana. U tome nam mogu pomoći činjenice da je

$$J(\mathbb{Q}(\sqrt{d}))_{(2')} = J(\mathbb{Q})_{(2')} \times J^d(\mathbb{Q})_{(2')}$$

te da se $J(\mathbb{Q}(\sqrt{d}))$ ulaže u $J(\mathbb{F}_p)$ za proste brojeve $p > 2$ koji se cijepaju u $\mathbb{Q}(\sqrt{d})$, odnosno u $J(\mathbb{F}_{p^2})$ za proste brojeve $p > 2$ koji su inertni u $\mathbb{Q}(\sqrt{d})$. Sve što sada treba je provjeriti dolazi li neka $\mathbb{K}-$racionalna točka na Jacobijanu od točke koja nije kusp.
Ako je rang pozitivan, problem postaje puno kompliciraniji te možemo probati primijeniti metodu iz [14].

Sada ćemo pokazati opisane metode na konkretnom primjeru. Izabrat ćemo neko kvadratno polje te ćemo provjeriti koje točno od 26 mogućih grupa se pojavljuju kao torzijske grupe eliptičkih krivulja nad tim poljem.

Fiksirajmo sada kvadratno polje $\mathbb{K} = \mathbb{Q}(\sqrt{13})$.

Kao što smo zaključili na početku poglavlja, grupe

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,2,...,10,12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4$$

(iz Mazurovog teorema) se pojavljuju kao torzijske grupe, a grupe

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1,2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

nisu moguće torzijske grupe nad ovim poljem.

Pogledajmo sada što se događa s ostalih 8 grupa. Prvo promatramo one grupe čije su pripadne modularne krivulje eliptičke krivulje.

Propozicija 10.1. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je $Y_1(11)(\mathbb{Q}(\sqrt{13}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(11)(\mathbb{Q}(\sqrt{13}))$ osim kuspova ima još beskonačno mnogo točaka. Budući da znamo da kuspova ima samo konačno mnogo, nije ih potrebno računati, već će biti dovoljno vidjeti da je rang $rk(X_1(11)(\mathbb{Q}(\sqrt{13})))$ pozitivan.

Za modularnu krivulju

$$X_1(11):\ y^2 - y = x^3 - x^2$$

pomoću koda $(C.1)$ iz dodatka C računamo rang nad $\mathbb{Q}(\sqrt{13})$. Program vraća donju i gornju ogradu za rang, koje su u ovom slučaju jednake 1. Dakle,

$$rk(X_1(11)(\mathbb{Q}(\sqrt{13}))) = 1.$$

Dobili smo i jedan generator grupe $X_1(11)(\mathbb{Q}(\sqrt{13}))$ (modulo torzijska podgrupa), tj.

točku beskonačnog reda. Ona je zapisana u projektivnim koordinatama i odgovara sljedećoj točki na krivulji:

$$\left(\frac{1}{9}(-2\sqrt{13}+5), \frac{1}{27}(-2\sqrt{13}+32)\right).$$

Zaključujemo da se na toj modularnoj krivulji (i kada oduzmemo broj kuspova) nalazi još beskonačno mnogo točaka. Svaka od tih točaka je uređeni par jedne eliptičke krivulje (do na izomorfizam) nad $\mathbb{Q}(\sqrt{13})$ zajedno s točkom reda 11 na toj eliptičkoj krivulji. □

Propozicija 10.2. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/14\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je

$$Y_1(14)(\mathbb{Q}(\sqrt{13})) = \emptyset,$$

tj. da se na modularnoj krivulji $X_1(14)(\mathbb{Q}(\sqrt{13}))$ nalaze samo kuspovi.
U dodatku B možemo naći modularnu krivulju $X_1(14)$ i jednadžbu koju zadovoljavaju $x-$koordinate njezinih kuspova. Ona glasi:

$$x(x-1)(x+1)(x^3-9x^2-x+1)(x^3-2x^2-x+1) = 0.$$

Dobijemo $x \in \{-1,0,1\}$ (to su sva rješenja gornje jednadžbe nad $\mathbb{Q}(\sqrt{13})$.) Uvrstimo li te točke u krivulju

$$X_1(14): \ y^2+xy+y = x^3-x,$$

zaključujemo da su kuspovi sljedeći:

$$X_1(14)(\mathbb{Q}(\sqrt{13}))\backslash Y_1(14)(\mathbb{Q}(\sqrt{13})) = \{O,(-1,0),(0,0),(0,-1),(1,0),(1,-2)\}.$$

Još je preostalo pokazati da krivulju $X_1(14)(\mathbb{Q}(\sqrt{13}))$ čini samo 6 točaka, tj.

$$X_1(14)(\mathbb{Q}(\sqrt{13})) \cong \mathbb{Z}/6\mathbb{Z}.$$

Kada to dobijemo, odmah slijedi da su sve točke na toj krivulji kuspovi, dakle ne postoje eliptičke krivulje nad $\mathbb{Q}(\sqrt{13})$ s torzijskom grupom $\mathbb{Z}/14\mathbb{Z}$.
Pomoću koda $(C.2)$ dobivamo željeni rezultat:

$$rk(X_1(14)(\mathbb{Q}(\sqrt{13}))) = 0,$$

$$X_1(14)(\mathbb{Q}(\sqrt{13}))_{tors} = \mathbb{Z}/6\mathbb{Z}.$$

□

Propozicija 10.3. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/15\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Slično kao u propoziciji 10.1, želimo pokazati kako je $Y_1(15)(\mathbb{Q}(\sqrt{13}))$ beskonačan skup, tj. da je rang $rk(X_1(15)(\mathbb{Q}(\sqrt{13})))$ pozitivan. U ovom slučaju to ćemo izračunati na malo drugačiji način. Pomoću koda $(C.3)$ možemo vidjeti da vrijedi:

$$rk(X_1(15)(\mathbb{Q})) = 0,$$

$$rk(X_1^{13}(15)(\mathbb{Q})) = 1,$$

gdje je $X_1^{13}(15)(\mathbb{Q})$ kvadratni twist od $X_1(15)(\mathbb{Q})$. Sada iz propozicije 9.1 slijedi da je

$$rk(X_1(15)(\mathbb{Q}(\sqrt{13})) = rk(X_1(15)(\mathbb{Q})) + rk(X_1^{13}(15)(\mathbb{Q})) = 0+1.$$

Dakle, dovoljno je bilo vidjeti da je rang kvadratnog twista $X_1^{13}(15)(\mathbb{Q})$ pozitivan da bismo zaključili kako postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$. Istim kodom tražimo i jedan generator grupe $X_1(15)(\mathbb{Q}(\sqrt{13})$. Dobivamo točku

$$\left(\frac{1}{2}(-\sqrt{13}+5), -\sqrt{13}+4\right).$$

□

Propozicija 10.4. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Cilj nam je zaključiti kako je $Y_1(2,10)(\mathbb{Q}(\sqrt{13}))$ beskonačan skup. Opet nije potrebno računati kuspove, već samo vidjeti je li rang $rk(X_1(2,10)(\mathbb{Q}(\sqrt{13})))$ pozitivan. Pomoću koda $(C.4)$ dobivamo upravo

$$rk(X_1(2,10)(\mathbb{Q}(\sqrt{13}))) = 1$$

te točku beskonačnog reda

$$\left(\frac{1}{2}(\sqrt{13}+3), -\sqrt{13}-3\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$. □

Propozicija 10.5. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Pomoću koda $(C.5)$ dobivamo da je

$$rk(X_1(2,12)(\mathbb{Q}(\sqrt{13}))) = 1$$

pa vidimo sa je skup $Y_1(2,12)(\mathbb{Q}(\sqrt{13}))$ beskonačan. Jedna točka beskonačnog reda dana je sa

$$\left(4, 2\sqrt{13}\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$. □

Nakon ovog niza propozicija vidimo da smo za kvadratno polje $\mathbb{Q}(\sqrt{13})$ provjerili postoji li nad njime eliptička krivulja s torzijskom grupom $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ takvom da je modularna krivulja $X_1(m,n)$ eliptička. To nam je bilo nešto lakše nego što će biti kada su modularne krivulje hipereliptičke. Ako pogledamo u dodatak B, vidimo da su jedine 3 preostale krivulje hipereliptičke. Prije nego što krenemo raditi s njima, navest ćemo još 2 korisna teorema.

Teorem 10.6. *Ako* $X_1(13)$ *ima točku koja nije kusp nad kvadratnim poljem* $\mathbb{Q}(\sqrt{d})$, *tada je:*

(1) $d > 0$;

(2) $d \equiv 1 \pmod 8$.

Teorem 10.7. *Ako $X_1(18)$ ima točku koja nije kusp nad kvadratnim poljem $\mathbb{Q}(\sqrt{d})$, $d \neq -3$, tada je:*
(1) $d > 0$;
(2) $d \equiv 1 \pmod 8$;
(3) $d \not\equiv 2 \pmod 3$.

Dokaze ovih teorema možemo naći u [8]. Pogledajmo sada što se događa s preostale 3 grupe, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ i $\mathbb{Z}/18\mathbb{Z}$. Iz teorema 9.7 zaključujemo kako možemo očekivati samo konačno mnogo eliptičkih krivulja s navedenim torzijskim grupama nad $\mathbb{Q}(\sqrt{13})$.

Propozicija 10.8. *Ne postoji eliptička krivulja s torzijom $\mathbb{Z}/13\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$.*

Dokaz. Vidimo da $d = 13 \not\equiv 1 \pmod 8$ pa prema teoremu 10.6 slijedi da je $X_1(13)(\mathbb{Q}(\sqrt{13})) = \{kuspovi\}$. Dakle, ne postoje eliptičke krivulje s torzijom $\mathbb{Z}/13\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$.
No, dokažimo ovu propoziciju na još jedan način, onako kako bismo ju dokazali da imamo d za koji vrijedi $d \equiv 1 \pmod 8$.
Označimo $J := J_1(13)$, Jacobijan od hipereliptičke krivulje $X_1(13)$. Pomoću koda $(C.6)$ računamo rang Jacobijana hipereliptičke krivulje nad $\mathbb{Q}$ i rang Jacobijana kvadratnog twista te hipereliptičke krivulje nad $\mathbb{Q}$,

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^{13}(\mathbb{Q})) = 0.$$

Sada zaključujemo da je

$$rk(J(\mathbb{Q}(\sqrt{13}))) = rk(J(\mathbb{Q})) + rk(J^{13}(\mathbb{Q})) = 0.$$

Dakle, moramo izračunati torzijsku grupu Jacobijana $J(\mathbb{Q}(\sqrt{13}))$ i vidjeti postoji li neka točka na Jacobijanu koja dolazi od točke koja nije kusp.

Izračunajmo sada kuspove na $X_1(13)$. Njihove $x-$koordinate zadovoljavaju

$$x(x-1)(x^3 - 4x^2 + x + 1) = 0.$$

Dobijemo da je $x \in \{0,1\}$. Uvrstimo te točke u krivulju

$$X_1(13): \ y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

i dobijemo da su kuspovi

$$X_1(13)(\mathbb{Q}(\sqrt{13}))\backslash Y_1(13)(\mathbb{Q}(\sqrt{13})) = \{\infty_+, \infty_-, (0,1), (0,-1), (1,-1), (1,1)\}.$$

Istim kodom računamo torzijsku grupu od $J(\mathbb{Q})$. Dobijemo

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Nadalje, dobivamo

$$J(\mathbb{Q})^{13}_{tors} \cong \{O\}.$$

Budući da vrijedi

$$J(\mathbb{Q}(\sqrt{13}))_{(2')} = J(\mathbb{Q})_{(2')} \times J(\mathbb{Q})^{13}_{(2')},$$

imamo

$$J(\mathbb{Q})_{(2')} \cong \mathbb{Z}/19\mathbb{Z},$$

gdje $J(\mathbb{Q})_{(2')}$ označava da se radi o 2-slobodnom dijelu torzije od $J(\mathbb{Q})$.

Sada, ako dokažemo da $J(\mathbb{Q}(\sqrt{13}))$ nema točaka reda 2, to će nam biti dovoljno da zaključimo da je $J(\mathbb{Q}(\sqrt{13}))_{tors} = \mathbb{Z}/19\mathbb{Z}$.

No, ako polinom

$$f(x) = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

nema nultočku nad poljem $\mathbb{Q}(\sqrt{13})$, tada ni $J(\mathbb{Q}(\sqrt{13}))$ nema točku reda 2. Zaista, polinom f nema nultočku nad $\mathbb{Q}(\sqrt{13})$, što znači da je

$$J(\mathbb{Q}(\sqrt{13}))_{tors} \cong J(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Još je preostalo provjeriti dolazi li koja točka s Jacobijana od neke točke na krivulji koja nije kusp. U Magmi tražimo spomenutih 19 točaka, kod vraća divizore u Mumfordovoj reprezentaciji [3], a iz njih dolazimo do točaka $\{\infty_+, \infty_-, (0,1), (0,-1), (1,-1), (1,1)\}$ na hipereliptičkoj krivulji. Primijećujemo da su sve točke kuspovi, što znači da ne postoji eliptička krivulja s torzijom $\mathbb{Z}/13\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$. □

Prije nego pokušamo vidjeti postoje li eliptičke krivulje s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$, recimo nešto o $L-$funkciji pridruženoj eliptičkim krivuljama i Birch-Swinnerton-Dyerovoj slutnji. To ćemo koristiti u propoziciji 10.13 kako bismo izračunali rang Jacobijana hipereliptičke krivulje.

Definicija 10.9. *Neka je E eliptička krivulja u minimalnom modelu i neka je Δ diskriminanta od E. Definiramo a_p na sljedeći način:*

$$a_p = \begin{cases} p+1-|E(\mathbb{F}_p)|, & \text{ako } p \nmid \Delta \\ 1, & \text{ako } E \text{ ima rascjepivu multiplikativnu redukciju u } p \\ -1, & \text{ako } E \text{ ima nerascjepivu multiplikativnu redukciju u } p \\ 0, & \text{ako } E \text{ ima aditivnu redukciju u } p. \end{cases}$$

$L-$funkcija eliptičke krivulje je dana sa

$$L_E(s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p \cdot p^{-s} + p^{1-2s}} \cdot \prod_{p \mid \Delta} \frac{1}{1 - a_p \cdot p^{-s}}.$$

Napomena 10.10. $L-$funkcija iz definicije 10.9 se može zapisati i kao

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Nas će zanimati vrijednost $L-$funkcije u točki $s = 1$.

Definicija 10.11. *Red nultočke $L-$funkcije L_E eliptičke krivulje E u točki $s = 1$ se naziva analitički rang od E.*

Rang koji smo definirali još u 2. poglavlju zovemo algebarski rang. Sljedeća slutnja nam govori nešto o (mogućoj) vezi algebarskog i analitičkog ranga.

Slutnja 10.12. ***(Birch-Swinnerton-Dyer)*** *Algebarski i analitički rang eliptičke krivulje E su jednaki.*

Primijetimo da slutnja povlači sljedeću činjenicu:

$$L_E(1) \neq 0 \iff rk(E) = 0.$$

Iako je ovo slutnja, ona vrijedi u slučajevima koji će nama trebati. U sljedećoj propoziciji, Magma nije efikasna za računanje ranga Jacobijana hipereliptičke krivulje $X_1(16)$ na standardni način pa ćemo umjesto toga vidjeti da je vrijednost $L-$funkcije u točki 1 različita od nule i na temelju toga zaključiti nešto o rangu.

Propozicija 10.13. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/16\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Već znamo da nas zanimaju rang Jacobijana hipereliptičke krivulje nad $\mathbb{Q}$ i rang Jacobijana kvadratnog twista te hipereliptičke krivulje nad $\mathbb{Q}$. Označimo $J := J_1(16)$, Jacobijan od hipereliptičke krivulje $X_1(16)$. Pomoću koda $(C.7)$ računamo

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^{13}(\mathbb{Q})) = 0.$$

Primijetimo da smo rang $rk(J^{13}(\mathbb{Q}))$ izračunali na standardni način, dok smo $rk(J(\mathbb{Q}))$ izračunali tako da smo provjerili da je analitički rang $L-$funkcije različit od nule. To je onda ekvivalentno tome da je $rk(J(\mathbb{Q}))$ jednak nuli. Dakle, vrijedi:

$$rk(J(\mathbb{Q}(\sqrt{13}))) = rk(J(\mathbb{Q})) + rk(J^{13}(\mathbb{Q})) = 0.$$

Budući da je ovaj rang nula, trebamo vidjeti koliko ima kuspova na modularnoj krivulji $X_1(16)$ i dolazi li koja točka iz torzijske grupe $J(\mathbb{Q}(\sqrt{13}))_{tors}$ od neke točke na modularnoj krivulji koja nije kusp.
$x-$koordinate kuspova moraju zadovoljavati

$$x(x-1)(x+1)(x^2-2x-1)(x^2+2x-1) = 0.$$

Slijedi da je

$$x \in \{-1, 0, 1\}.$$

Uvrštavanjem tih točaka u modularnu krivulju

$$X_1(16): \ y^2 = x(x^2+1)(x^2+2x-1)$$

dobijemo kuspove

$$X_1(16)(\mathbb{Q}(\sqrt{13}))\backslash Y_1(16)(\mathbb{Q}(\sqrt{13})) = \{O, (0,0), (1,2), (1,-2), (-1,2), (-1,-2)\}.$$

Nađimo sada torzijske podgrupe pomoću koda $(C.8)$. Imamo:

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

$$J^{13}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Pomoću izraza

$$J(\mathbb{Q}(\sqrt{13}))_{(2')} \cong J(\mathbb{Q})_{(2')} \times J^{13}(\mathbb{Q})_{(2')},$$

računamo:

$$J(\mathbb{Q}(\sqrt{13}))_{(2')} = \mathbb{Z}/5\mathbb{Z}.$$

U Magmi također imamo funkciju koja računa 2-torzijsku podgrupu od Jacobijana te je ona implementirana i za Jacobijane nad kvadratnim poljima. Istim kodom (C.8) vidimo da je 2-torzija od $J(\mathbb{Q}(\sqrt{13}))$ upravo grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dakle,

$$J(\mathbb{Q}(\sqrt{13})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

odnosno

$$J(\mathbb{Q}(\sqrt{13})) \cong J^{13}(\mathbb{Q})_{tors}.$$

U Magmi dobijemo 20 divizora u Mumfordovoj reprezentaciji koji predstavljaju sljedeće točke na hipereliptičkoj krivulji:

$$\{O, (0,0), (1,2), (1,-2), (-1,2), (-1,-2)\}.$$

Primjećujemo da su sve točke kuspovi, tj. ne postoji eliptička krivulja s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$. □

Propozicija 10.14. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/18\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Vidimo da $d = 13 \not\equiv 1 \pmod 8$ pa prema teoremu 10.7 slijedi da je $X_1(13) = \{kuspovi\}$. Dakle, ne postoje eliptičke krivulje s torzijom $\mathbb{Z}/18\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$.
Ipak, dokažimo ovu propoziciju na još jedan način.

Označimo $J := J_1(18)$, Jacobijan od hipereliptičke krivulje $X_1(18)$. Pomoću koda $(C.9)$ računamo rang Jacobijana hipereliptičke krivulje nad $\mathbb{Q}$ i rang Jacobijana kvadratnog twista te hipereliptičke krivulje nad $\mathbb{Q}$,

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^{13}(\mathbb{Q})) = 0.$$

Sada zaključujemo da je

$$rk(J(\mathbb{Q}(\sqrt{13}))) = rk(J(\mathbb{Q})) + rk(J^{13}(\mathbb{Q})) = 0.$$

Dakle, moramo izračunati torzijsku grupu Jacobijana $J(\mathbb{Q}(\sqrt{13}))$ i vidjeti postoji li neka točka na Jacobijanu koja dolazi od točke koja nije kusp.

Izračunajmo sada kuspove na $X_1(18)$. Njihove $x-$koordinate zadovoljavaju

$$x(x+1)(x^2+x+1)(x^2-3x-1) = 0.$$

Dobijemo da je

$$x \in \{0, -1, \frac{3+\sqrt{13}}{2}, \frac{3-\sqrt{13}}{2}\}.$$

Uvrstimo te točke u krivulju

$$X_1(18): \ y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

i dobijemo da su kuspovi

$$X_1(18)(\mathbb{Q}(\sqrt{13}))\backslash Y_1(18)(\mathbb{Q}(\sqrt{13})) = \{\infty_+, \infty_-, (0,1), (0,-1), (-1,1), (-1,-1)\}.$$

($y-$koordinate za točke $x = \frac{3 \pm \sqrt{13}}{2}$ nisu definirane nad $\mathbb{Q}(\sqrt{13})$.)

Istim kodom računamo torzijske grupe. Dobijemo

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/21\mathbb{Z},$$

$$J^{13}(\mathbb{Q})_{tors} \cong \{O\}.$$

Budući da vrijedi

$$J(\mathbb{Q}(\sqrt{13}))_{(2')} = J(\mathbb{Q})_{(2')} \times J^{13}(\mathbb{Q})_{(2')},$$

imamo

$$J(\mathbb{Q})_{(2')} \cong \mathbb{Z}/21\mathbb{Z}.$$

Sada, ako dokažemo da $J(\mathbb{Q}(\sqrt{13}))$ nema točaka reda 2, to će nam biti dovoljno da zaključimo da je $J(\mathbb{Q}(\sqrt{13}))_{tors} = \mathbb{Z}/21\mathbb{Z}$.

No, ako polinom

$$f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

nema nultočku nad poljem $\mathbb{Q}(\sqrt{13})$, tada ni $J(\mathbb{Q}(\sqrt{13}))$ nema točku reda 2. Zaista, polinom f nema nultočku nad $\mathbb{Q}(\sqrt{13})$, što znači da je

$$J(\mathbb{Q}(\sqrt{13}))_{tors} \cong J(\mathbb{Q})_{tors} \cong \mathbb{Z}/21\mathbb{Z}.$$

Još je preostalo provjeriti dolazi li koja točka s Jacobijana od neke točke na krivulji koja nije kusp. U Magmi tražimo spomenutu 21 točku, kod vraća divizore u Mumfordovoj reprezentaciji, a iz njih dolazimo do točaka $\{\infty_+, \infty_-, (0,1), (0,-1), (-1,1), (-1,-1)\}$ na hipereliptičkoj krivulji. Primijećujemo da su sve točke kuspovi, što znači da ne postoji eliptička krivulja s torzijom $\mathbb{Z}/18\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{13})$. □

Prošli smo kroz sve moguće torzijske grupe nad kvadratnim poljem $\mathbb{Q}(\sqrt{13})$ i dokazali sljedeći teorem:

Teorem 10.15. *Moguće torzijske grupe eliptičkih krivulja nad kvadratnim poljem* $\mathbb{Q}(\sqrt{13})$ *su:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 1, ..., 12, 15,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1, 2, 3, 4, 5, 6.$$

Fiksirajmo sada neko drugo kvadratno polje kvadratno polje, npr. $\mathbb{K} = \mathbb{Q}(\sqrt{11})$.

Za ovo kvadratno polje (kao i za svako drugo) znamo da se grupe

$$\mathbb{Z}/n\mathbb{Z},\ n = 1, 2, ..., 10, 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4$$

(iz Mazurovog teorema) pojavljuju kao torzijske grupe. Grupe

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1,2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

nisu moguće torzijske grupe nad ovim poljem.

Pogledajmo sada što se događa s ostalih 8 grupa. Prvo promatramo one grupe čije su pripadne modularne krivulje eliptičke krivulje.

Propozicija 10.16. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je $Y_1(11)(\mathbb{Q}(\sqrt{11}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(11)(\mathbb{Q}(\sqrt{11}))$ osim kuspova ima još beskonačno mnogo točaka. Budući da znamo da kuspova ima samo konačno mnogo, nije ih potrebno računati, već će biti dovoljno vidjeti da je rang $rk(X_1(11)(\mathbb{Q}(\sqrt{11})))$ pozitivan.

Za modularnu krivulju

$$X_1(11):\ y^2 - y = x^3 - x^2$$

u Magmi $(C.10)$ računamo rang $\mathbb{Q}(\sqrt{11})$. Program vraća donju i gornju ogradu za rang, koje su u ovom slučaju jednake 1. Dakle,

$$rk(X_1(11)(\mathbb{Q}(\sqrt{11}))) = 1.$$

Imamo i točku beskonačnog reda na $X_1(11)(\mathbb{Q}(\sqrt{11}))$:

$$\left(-\frac{1}{4}, \frac{1}{8}(\sqrt{11}+4)\right).$$

Zaključujemo da se na toj modularnoj krivulji (i kada oduzmemo broj kuspova) nalazi još beskonačno mnogo točaka. Svaka od tih točaka je uređeni par jedne eliptičke krivulje (do na izomorfizam) nad $\mathbb{Q}(\sqrt{11})$ zajedno s točkom reda 11 na toj eliptičkoj krivulji. □

Propozicija 10.17. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/14\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{13})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je

$$Y_1(14)(\mathbb{Q}(\sqrt{11})) = \emptyset,$$

tj. da se na modularnoj krivulji $X_1(14)(\mathbb{Q}(\sqrt{11}))$ nalaze samo kuspovi.
U dodatku B možemo naći modularnu krivulju $X_1(14)$. Jednadžba koju zadovoljavaju $x-$koordinate njezinih kuspova glasi:

$$x(x-1)(x+1)(x^3-9x^2-x+1)(x^3-2x^2-x+1) = 0.$$

Dobijemo $x \in \{-1,0,1\}$. Uvrstimo li te točke u krivulju

$$X_1(14): \ y^2+xy+y = x^3-x,$$

zaključujemo da su kuspovi sljedeći:

$$X_1(14)(\mathbb{Q}(\sqrt{11}))\backslash Y_1(14)(\mathbb{Q}(\sqrt{11})) = \{O,(-1,0),(0,0),(0,-1),(1,0),(1,-2)\}.$$

Još je preostalo pokazati da krivulju $X_1(14)(\mathbb{Q}(\sqrt{11}))$ čini samo 6 točaka, tj.

$$X_1(14)(\mathbb{Q}(\sqrt{11})) \cong \mathbb{Z}/6\mathbb{Z}.$$

Kada to dobijemo, odmah slijedi da su sve točke na toj krivulji kuspovi, dakle ne postoje eliptičke krivulje nad $\mathbb{Q}(\sqrt{11})$ s torzijskom grupom $\mathbb{Z}/14\mathbb{Z}$.
U Magmi $(C.11)$ dobivamo željeni rezultat:

$$rk(X_1(14)(\mathbb{Q}(\sqrt{11}))) = 0,$$

$$X_1(14)(\mathbb{Q}(\sqrt{11}))_{tors} = \mathbb{Z}/6\mathbb{Z}.$$

□

Propozicija 10.18. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/15\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Opet, želimo pokazati sa je $Y_1(15)(\mathbb{Q}(\sqrt{11}))$ beskonačan skup, tj. da je rang $rk(X_1(15)(\mathbb{Q}(\sqrt{11})))$ pozitivan. U Magmi $(C.12)$ računamo

$$rk(X_1(15)(\mathbb{Q}(\sqrt{11})) = 1.$$

Jedna točka beskonačnog reda je dana sa

$$\left(\frac{1}{1225}(1272\sqrt{11}+3168), \frac{1}{42875}(-125928\sqrt{11}-434907)\right).$$

Dakle, rang je pozitivan pa slično kao u propoziciji 10.16 zaključujemo do postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{11})$. □

Propozicija 10.19. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Cilj nam je zaključiti kako je $Y_1(2,10)(\mathbb{Q}(\sqrt{11}))$ beskonačan skup. Opet nije potrebno računati kuspove, već samo vidjeti je li rang $rk(X_1(2,10)(\mathbb{Q}(\sqrt{11})))$ pozitivan. Dobivamo upravo $(C.13)$

$$rk(X_1(2,10)(\mathbb{Q}(\sqrt{11}))) = 1.$$

Imamo i točku beskonačnog reda

$$\left(\frac{1}{1369}(132\sqrt{11}-1367), \frac{1}{50653}(-264\sqrt{11}+45181)\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{11})$. □

Propozicija 10.20. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Računamo $(C.14)$:

$$rk(X_1(2,12)(\mathbb{Q}(\sqrt{11}))) = 1$$

pa vidimo sa je skup $Y_1(2,12)(\mathbb{Q}(\sqrt{11}))$ beskonačan. Jedan generator od $X_1(2,12)(\mathbb{Q}(\sqrt{11}))$ dan je sa

$$\left(5\sqrt{11}+18, 30\sqrt{11}+101\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{11})$. □

Dakle, za naše novo polje, $\mathbb{Q}(\sqrt{11})$, smo provjerili postoji li nad njime eliptička krivulja s torzijskom grupom $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ takvom da je modularna krivulja $X_1(m,n)$ eliptička.

Pogledajmo sada preostale 3 grupe, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ i $\mathbb{Z}/18\mathbb{Z}$. Iz teorema 9.7 zaključujemo kako možemo očekivati samo konačno mnogo eliptičkih krivulja s navedenim torzijskim grupama nad $\mathbb{Q}(\sqrt{11})$.

Propozicija 10.21. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/13\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Budući da sada radimo s hipereliptičkom krivuljom $X_1(13)$, zanima nas kako izgledaju Jacobijan od $X_1(13)(\mathbb{Q})$ i Jacobijan od kvadratnog twista od $X_1(13)(\mathbb{Q})$. Označimo $J := J_1(13)$, Jacobijan od hipereliptičke krivulje $X_1(13)$. U Magmi $(C.15)$ računamo rangove spomenutih Jacobijana i dobijemo

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^{11}(\mathbb{Q})) = 0.$$

Sada zaključujemo da je

$$rk(J(\mathbb{Q}(\sqrt{11}))) = rk(J(\mathbb{Q})) + rk(J^{11}(\mathbb{Q})) = 0.$$

Dakle, moramo izračunati torzijsku grupu Jacobijana $J(\mathbb{Q}(\sqrt{11}))$ i vidjeti postoji li neka točka na Jacobijanu koja dolazi od točke koja nije kusp.

Izračunajmo sada kuspove na $X_1(13)(\mathbb{Q}(\sqrt{11}))$. Iz propozicije 10.8 znamo da su oni

$$X_1(13)(\mathbb{Q}(\sqrt{11}))\backslash Y_1(13)(\mathbb{Q}(\sqrt{11})) = \{\infty_+, \infty_-, (0,1), (0,-1), (1,-1), (1,1)\}.$$

(Ne postoje nikakvi dodatni kusovi koji su definirani nad $\mathbb{Q}(\sqrt{11})$, a nisu bili nad $\mathbb{Q}(\sqrt{13})$.)

Sada računamo torzijsku grupu od $J(\mathbb{Q})$. Dobijemo

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Nadalje, dobivamo

$$J^{11}(\mathbb{Q})_{tors} \cong \{O\}.$$

Budući da vrijedi

$$J(\mathbb{Q}(\sqrt{11}))_{(2')} = J(\mathbb{Q})_{(2')} \times J^{11}(\mathbb{Q})_{(2')},$$

imamo

$$J(\mathbb{Q})_{(2')} \cong \mathbb{Z}/19\mathbb{Z}.$$

Sada, ako dokažemo da $J(\mathbb{Q}(\sqrt{11}))$ nema točaka reda 2, to će nam biti dovoljno da zaključimo da je $J(\mathbb{Q}(\sqrt{11}))_{tors} = \mathbb{Z}/19\mathbb{Z}$.

No, polinom

$$f(x) = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

nema nultočku nad poljem $\mathbb{Q}(\sqrt{11})$ pa $J(\mathbb{Q}(\sqrt{11}))$ nema točku reda 2. Dakle,

$$J(\mathbb{Q}(\sqrt{11}))_{tors} \cong J(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Još je preostalo provjeriti dolazi li koja točka s Jacobijana od neke točke na krivulji koja nije kusp. U Magmi tražimo spomenutih 19 točaka, na Jacobijanu, a iz njih dolazimo do točaka $\{\infty_+, \infty_-, (0,1), (0,-1), (1,-1), (1,1)\}$ na hipereliptičkoj krivulji. Primijećujemo da su sve točke kuspovi, što znači da ne postoji eliptička krivulja s torzijom $\mathbb{Z}/13\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{11})$. □

Propozicija 10.22. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/16\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Zanimaju nas rang Jacobijana hipereliptičke krivulje nad $\mathbb{Q}$ i rang Jacobijana kvadratnog twista te hipereliptičke krivulje nad $\mathbb{Q}$. Računamo $(C.16)$

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^{11}(\mathbb{Q})) = 0.$$

Opet smo rang $rk(J^{11}(\mathbb{Q}))$ izračunali na standardni način, dok smo $rk(J(\mathbb{Q}))$ izračunali tako da smo provjerili da je analitički rang $L-$funkcije različit od nule. Dakle, vrijedi:

$$rk(J(\mathbb{Q}(\sqrt{11}))) = rk(J(\mathbb{Q})) + rk(J^{11}(\mathbb{Q})) = 0.$$

Budući da je ovaj rang nula, trebamo vidjeti koliko ima kuspova na modularnoj krivulji $X_1(16)$ i dolazi li koja točka iz torzijske grupe $J(\mathbb{Q}(\sqrt{11}))_{tors}$ od neke točke na modularnoj krivulji koja nije kusp.
U propoziciji 10.13 smo već vidjeli da su kuspovi

$$X_1(16)(\mathbb{Q}(\sqrt{11}))\backslash Y_1(16)(\mathbb{Q}(\sqrt{11})) = \{O,(0,0),(1,2),(1,-2),(-1,2),(-1,-2)\}.$$

Nađimo sada torzijske podgrupe. Računamo $(C.17)$:

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

$$J^{11}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Pomoću izraza

$$J(\mathbb{Q}(\sqrt{11}))_{(2')} \cong J(\mathbb{Q})_{(2')} \times J^{11}(\mathbb{Q})_{(2')},$$

računamo:

$$J(\mathbb{Q}(\sqrt{11}))_{(2')} = \mathbb{Z}/5\mathbb{Z}.$$

Vidimo i da je 2-torzija od $J(\mathbb{Q}(\sqrt{11}))$ jednaka $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dakle,

$$J(\mathbb{Q}(\sqrt{11})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

odnosno

$$J(\mathbb{Q}(\sqrt{11})) \cong J^{11}(\mathbb{Q})_{tors}.$$

U Magmi dobijemo 20 divizora u Mumfordovoj reprezentaciji koji predstavljaju sljedeće točke na hipereliptičkoj krivulji:

$$\{O,(0,0),(1,2),(1,-2),(-1,2),(-1,-2)\}.$$

Primjećujemo da su sve točke kuspovi, tj. ne postoji eliptička krivulja s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{11})$. □

Propozicija 10.23. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/18\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Već smo spomenuli kako 2-spust kojim Magma računa rang nije algoritam i nemamo garanciju da ćemo dobiti jednaku donju i gornju ogradu za rang. Upravo za Jacobijan kvadratnog twista s 11 modularne krivulje $X_1(18)$ ne možemo dobiti jednake ograde za rang.

Srećom, vrijedi da $d = 11 \not\equiv 1 \pmod 8$ pa prema teoremu 10.7 slijedi da je $X_1(18) = \{kuspovi\}$. Dakle, ne postoji eliptička krivulja s torzijom $\mathbb{Z}/18\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{11})$. □

Dakle, prošli smo kroz sve moguće torzijske grupe nad kvadratnim poljem $\mathbb{Q}(\sqrt{11})$ i dokazali sljedeći teorem:

Teorem 10.24. *Moguće torzijske grupe eliptičkih krivulja nad kvadratnim poljem* $\mathbb{Q}(\sqrt{11})$ *su:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,...,12,15,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4,5,6.$$

Neka je sada $\mathbb{K} = \mathbb{Q}(\sqrt{7})$. Napravit ćemo istu stvar kao i za prethodna dva primjera, samo malo manje detaljno. Svaku bitniju promjenu ćemo naglasiti.

Grupe

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,2,...,10,12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4$$

(iz Mazurovog teorema) se sigurno pojavljuju kao torzijske grupe. Grupe

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1,2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

nisu moguće torzijske grupe nad ovim poljem.

Pogledajmo sada što se događa s ostalih 8 grupa. Prvo promatramo one grupe čije su pripadne modularne krivulje eliptičke krivulje.

Propozicija 10.25. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je $Y_1(11)(\mathbb{Q}(\sqrt{7}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(11)(\mathbb{Q}(\sqrt{7}))$ osim kuspova ima još beskonačno mnogo točaka.

U Magmi $(C.18)$ računamo:

$$rk(X_1(11)(\mathbb{Q}(\sqrt{7}))) = 1.$$

Imamo i točku beskonačnog reda:

$$\left(2\sqrt{7}+5, -6\sqrt{7}-15\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/11\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{7})$. □

Propozicija 10.26. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/14\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Slično kao u prethodnoj propoziciji, trebamo vidjeti da je $Y_1(14)(\mathbb{Q}(\sqrt{7}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(14)(\mathbb{Q}(\sqrt{7}))$ osim kuspova ima još beskonačno mnogo točaka.

U Magmi $(C.19)$ računamo:

$$rk(X_1(14)(\mathbb{Q}(\sqrt{7}))) = 1,$$

a točka beskonačnog reda je

$$\left(\frac{1}{9}(2\sqrt{7}-1), \frac{1}{27}(-4\sqrt{7}+2)\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/14\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{7})$. □

Propozicija 10.27. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/15\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Opet, želimo pokazati sa je $Y_1(15)(\mathbb{Q}(\sqrt{7}))$ beskonačan skup, tj. da je rang $rk(X_1(15)(\mathbb{Q}(\sqrt{7})))$ pozitivan. U Magmi $(C.20)$ računamo

$$rk(X_1(15)(\mathbb{Q}(\sqrt{7})) = 1.$$

Točka beskonačnog reda je

$$\left(\frac{3}{4}, \frac{1}{8}(-4\sqrt{7}-7)\right).$$

Dakle, rang je pozitivan pa zaključujemo do postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{7})$. □

Propozicija 10.28. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je

$$Y_1(2,10)(\mathbb{Q}(\sqrt{7})) = \emptyset,$$

tj. da se na modularnoj krivulji $X_1(2,10)(\mathbb{Q}(\sqrt{7}))$ nalaze samo kuspovi.
Kuspovi su sljedeći:

$$X_1(2,10)(\mathbb{Q}(\sqrt{7}))\backslash Y_1(2,10)(\mathbb{Q}(\sqrt{7})) = \{O,(0,0),(1,1),(1,-1),(-1,1),(-1,-1)\}.$$

Još je preostalo pokazati da krivulju $X_1(2,10)(\mathbb{Q}(\sqrt{7}))$ čini samo 6 točaka, tj.

$$X_1(2,10)(\mathbb{Q}(\sqrt{7})) \cong \mathbb{Z}/6\mathbb{Z}.$$

Kada to dobijemo, odmah slijedi da su sve točke na toj krivulji kuspovi, dakle ne postoje eliptičke krivulje nad $\mathbb{Q}(\sqrt{7})$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.
U Magmi $(C.21)$ dobivamo željeni rezultat:

$$rk(X_1(2,10)(\mathbb{Q}(\sqrt{7}))) = 0,$$

$$X_1(2,10)(\mathbb{Q}(\sqrt{7}))_{tors} = \mathbb{Z}/6\mathbb{Z}.$$

□

Propozicija 10.29. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Radimo slično kao u prethodnoj propoziciji.

Kuspovi su sljedeći:

$$X_1(2,12)(\mathbb{Q}(\sqrt{7}))\backslash Y_1(2,12)(\mathbb{Q}(\sqrt{7})) = \{O,(0,0),(1,1),(1,-1)\}.$$

Još je preostalo pokazati da krivulju $X_1(2,12)(\mathbb{Q}(\sqrt{7}))$ čini samo 4 točke, tj.

$$X_1(2,12)(\mathbb{Q}(\sqrt{7})) \cong \mathbb{Z}/4\mathbb{Z}.$$

U Magmi $(C.22)$ dobivamo:

$$rk(X_1(2,12)(\mathbb{Q}(\sqrt{7}))) = 0,$$

$$X_1(2,12)(\mathbb{Q}(\sqrt{7}))_{tors} = \mathbb{Z}/4\mathbb{Z}.$$

Dakle, ne postoje eliptičke krivulje nad $\mathbb{Q}(\sqrt{7})$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

□

Pogledajmo sada grupe $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ i $\mathbb{Z}/18\mathbb{Z}$. Iz teorema 9.7 zaključujemo kako možemo očekivati samo konačno mnogo eliptičkih krivulja s navedenim torzijskim grupama nad $\mathbb{Q}(\sqrt{7})$.

Propozicija 10.30. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/13\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Vidimo da $d = 7 \not\equiv 1 \pmod 8$ pa prema teoremu 10.6 slijedi da je $X_1(13)(\mathbb{Q}(\sqrt{7})) = \{kuspovi\}$. Dakle, ne postoje eliptičke krivulje s torzijom $\mathbb{Z}/13\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{7})$. □

Propozicija 10.31. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/16\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{7})$.

Dokaz. Zanimaju nas rang Jacobijana hipereliptičke krivulje nad $\mathbb{Q}$ i rang Jacobijana kvadratnog twista te hipereliptičke krivulje nad $\mathbb{Q}$. Računamo $(C.23)$

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^7(\mathbb{Q})) = 0.$$

Dakle, vrijedi:

$$rk(J(\mathbb{Q}(\sqrt{7}))) = rk(J(\mathbb{Q})) + rk(J^7(\mathbb{Q})) = 0.$$

Budući da je ovaj rang nula, trebamo vidjeti koliko ima kuspova na modularnoj krivulji $X_1(16)$ i dolazi li koja točka iz torzijske grupe $J(\mathbb{Q}(\sqrt{7}))_{tors}$ od neke točke na modularnoj krivulji koja nije kusp. Kuspovi su

$$X_1(16)(\mathbb{Q}(\sqrt{7}))\backslash Y_1(16)(\mathbb{Q}(\sqrt{7})) = \{O,(0,0),(1,2),(1,-2),(-1,2),(-1,-2)\}.$$

Nađimo sada torzijske podgrupe. Računamo $(C.24)$:

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

$$J^7(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Pomoću izraza

$$J(\mathbb{Q}(\sqrt{7}))_{(2')} \cong J(\mathbb{Q})_{(2')} \times J^7(\mathbb{Q})_{(2')},$$

računamo:

$$J(\mathbb{Q}(\sqrt{7}))_{(2')} = \mathbb{Z}/5\mathbb{Z}.$$

Vidimo i da je 2-torzija od $J(\mathbb{Q}(\sqrt{7}))$ jednaka $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dakle,

$$J(\mathbb{Q}(\sqrt{7})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

odnosno

$$J(\mathbb{Q}(\sqrt{7})) \cong J^7(\mathbb{Q})_{tors}.$$

U Magmi dobijemo 20 divizora u Mumfordovoj reprezentaciji koji predstavljaju sljedeće točke na hipereliptičkoj krivulji:

$$\{O,(0,0),(1,2),(1,-2),(-1,2),(-1,-2)\}.$$

Primjećujemo da su sve točke kuspovi, tj. ne postoji eliptička krivulja s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{7})$. □

Propozicija 10.32. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/18\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{11})$.

Dokaz. Vrijedi da $d = 11 \not\equiv 1 \pmod 8$ pa prema teoremu 10.7 slijedi da je $X_1(18) = \{kuspovi\}$. Dakle, ne postoji eliptička krivulja s torzijom $\mathbb{Z}/18\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{7})$. □

Ovim nizom propozicija dokazali smo sljedeći teorem:

Teorem 10.33. *Moguće torzijske grupe eliptičkih krivulja nad kvadratnim poljem* $\mathbb{Q}(\sqrt{7})$ *su:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,...,12,14,15,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4.$$

I za kraj, uzmimo $\mathbb{K} = \mathbb{Q}(\sqrt{6})$.

Grupe

$$\mathbb{Z}/n\mathbb{Z},\ n = 1,2,...,10,12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4$$

(iz Mazurovog teorema) se sigurno pojavljuju kao torzijske grupe. Grupe

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1,2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

nisu moguće torzijske grupe nad ovim poljem.

Pogledajmo sada što se događa s ostalih 8 grupa. Prvo promatramo one grupe čije su pripadne modularne krivulje eliptičke krivulje.

Propozicija 10.34. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/11\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je $Y_1(11)(\mathbb{Q}(\sqrt{6}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(11)(\mathbb{Q}(\sqrt{6}))$ osim kuspova ima još beskonačno mnogo točaka.

U Magmi $(C.25)$ računamo:

$$rk(X_1(11)(\mathbb{Q}(\sqrt{6}))) = 1.$$

Točka beskonačnog reda je

$$\left(\frac{1}{6}, \frac{1}{36}(-7\sqrt{6}+18)\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/11\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Propozicija 10.35. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/14\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. Slično kao u prethodnoj propoziciji, trebamo vidjeti da je $Y_1(14)(\mathbb{Q}(\sqrt{6}))$ beskonačan skup, tj. da na modularnoj krivulji $X_1(14)(\mathbb{Q}(\sqrt{6}))$ osim kuspova ima još beskonačno mnogo točaka.

U Magmi $(C.26)$ računamo:

$$rk(X_1(14)(\mathbb{Q}(\sqrt{6}))) = 1.$$

Kod vraća i sljedeću točku beskonačnog reda:

$$\left(-\frac{1}{4}, \frac{1}{8}(-2\sqrt{6}-3)\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/14\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Propozicija 10.36. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/15\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. Da bismo ovo dokazali, trebamo vidjeti da je

$$Y_1(15)(\mathbb{Q}(\sqrt{6})) = \emptyset,$$

tj. da se na modularnoj krivulji $X_1(15)(\mathbb{Q}(\sqrt{6}))$ nalaze samo kuspovi.

Kuspovi su sljedeći:

$$X_1(15)(\mathbb{Q}(\sqrt{6}))\backslash Y_1(15)(\mathbb{Q}(\sqrt{6})) = \{O,(0,0),(-1,0),(0,-1)\}.$$

U Magmi $(C.27)$ dobivamo:

$$rk(X_1(15)(\mathbb{Q}(\sqrt{6}))) = 0,$$

$$X_1(15)(\mathbb{Q}(\sqrt{6}))_{tors} = \mathbb{Z}/6\mathbb{Z}.$$

Dakle, ne postoji eliptička krivulja s torzijom $\mathbb{Z}/15\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Propozicija 10.37. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. U Magmi $(C.28)$ računamo:

$$rk(X_1(2,10)(\mathbb{Q}(\sqrt{6}))) = 1.$$

Točka beskonačnog reda je:

$$\left(2\sqrt{6}+7, 8\sqrt{6}+23\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Propozicija 10.38. *Postoji beskonačno mnogo eliptičkih krivulja s torzijom* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. U Magmi $(C.29)$ računamo:

$$rk(X_1(2,12)(\mathbb{Q}(\sqrt{6}))) = 1.$$

Točka beskonačnog reda je:

$$\left(2\sqrt{6}+5, -6\sqrt{6}-15\right).$$

Dakle, postoji beskonačno mnogo eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Pogledajmo sada grupe, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ i $\mathbb{Z}/18\mathbb{Z}$. Već znamo da možemo očekivati samo konačno mnogo eliptičkih krivulja s navedenim torzijskim grupama nad $\mathbb{Q}(\sqrt{6})$.

Propozicija 10.39. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/13\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. Vidimo da $d = 6 \not\equiv 1 \pmod 8$ pa prema teoremu 10.6 slijedi da je $X_1(13)(\mathbb{Q}(\sqrt{6})) = \{kuspovi\}$. Dakle, ne postoje eliptičke krivulje s torzijom $\mathbb{Z}/13\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Propozicija 10.40. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/16\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. Zanimaju nas rang Jacobijana hipereliptičke krivulje nad $\mathbb{Q}$ i rang Jacobijana kvadratnog twista te hipereliptičke krivulje nad $\mathbb{Q}$. Računamo $(C.30)$

$$rk(J(\mathbb{Q})) = 0,$$

$$rk(J^6(\mathbb{Q})) = 0.$$

Dakle, vrijedi:

$$rk(J(\mathbb{Q}(\sqrt{6}))) = rk(J(\mathbb{Q})) + rk(J^6(\mathbb{Q})) = 0.$$

Budući da je ovaj rang nula, trebamo vidjeti koliko ima kuspova na modularnoj krivulji $X_1(16)$ i dolazi li koja točka iz torzijske grupe $J(\mathbb{Q}(\sqrt{6}))_{tors}$ od neke točke na modularnoj krivulji koja nije kusp. Kuspovi su

$$X_1(16)(\mathbb{Q}(\sqrt{6}))\backslash Y_1(16)(\mathbb{Q}(\sqrt{6})) = \{O,(0,0),(1,2),(1,-2),(-1,2),(-1,-2)\}.$$

Nađimo sada torzijske podgrupe. Računamo $(C.31)$:

$$J(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

$$J^6(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Pomoću izraza

$$J(\mathbb{Q}(\sqrt{6}))_{(2')} \cong J(\mathbb{Q})_{(2')} \times J^6(\mathbb{Q})_{(2')},$$

računamo:

$$J(\mathbb{Q}(\sqrt{6}))_{(2')} = \mathbb{Z}/5\mathbb{Z}.$$

Vidimo i da je 2-torzija od $J(\mathbb{Q}(\sqrt{6}))$ jednaka $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Dakle,

$$J(\mathbb{Q}(\sqrt{6})) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},$$

odnosno

$$J(\mathbb{Q}(\sqrt{6})) \cong J^6(\mathbb{Q})_{tors}.$$

U Magmi dobijemo 20 divizora u Mumfordovoj reprezentaciji koji predstavljaju sljedeće točke na hipereliptičkoj krivulji:

$$\{O, (0,0), (1,2), (1,-2), (-1,2), (-1,-2)\}.$$

Primjećujemo da su sve točke kuspovi, tj. ne postoji eliptička krivulja s torzijom $\mathbb{Z}/16\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Propozicija 10.41. *Ne postoji eliptička krivulja s torzijom* $\mathbb{Z}/18\mathbb{Z}$ *nad* $\mathbb{Q}(\sqrt{6})$.

Dokaz. Vrijedi da $d = 6 \not\equiv 1 \pmod 8$ pa prema teoremu 10.7 slijedi da je $X_1(18) = \{kuspovi\}$. Dakle, ne postoji eliptička krivulja s torzijom $\mathbb{Z}/18\mathbb{Z}$ nad $\mathbb{Q}(\sqrt{6})$. □

Završavamo sljedećim teoremom:

Teorem 10.42. *Moguće torzijske grupe eliptičkih krivulja nad kvadratnim poljem* $\mathbb{Q}(\sqrt{6})$ *su:*

$$\mathbb{Z}/n\mathbb{Z}, \ \ n = 1, ..., 12, 14,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \ \ n = 1, 2, 3, 4, 5, 6.$$

Dodatak A

Jednadžbe eliptičkih krivulja sa zadanom torzijskom grupom

Način na koji smo došli do ovih jednadžbi možemo naći u [5].

$\{O\}$:

$$y^2 = x^3 + ax^2 + bx + c$$

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^3$$

$\mathbb{Z}/2\mathbb{Z}$:

$$y^2 = x(x^2 + ax + b)$$

$$\Delta = a^2b^2 - 4b^3$$

$\mathbb{Z}/3\mathbb{Z}$:

$$y^2 + axy + by = x^3$$

$$\Delta = a^3b^3 - 27b^4$$

$\mathbb{Z}/4\mathbb{Z}$:

$$y^2 + (1-c)xy - by = x^3 - bx^2,\ c = 0$$

$$\Delta = b^2(1 + 16b)$$

$\mathbb{Z}/5\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2,\ b=c$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/6\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=c+c^2$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/7\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=d^3-d^2,\ c=d^2-d$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/8\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=(2d-1)(d-1),\ c=\frac{(2d-1)(d-1)}{d}$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/9\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=cd,\ c=fd-f,\ d=f(f-1)+1$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/10\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=cd,\ c=fd-f,\ d=\frac{f^2}{f-(f-1)^2}$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/12\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=cd,\ c=fd-f,\ d=m+r$$

$$f=\frac{m}{1-r},\ m=\frac{3r-3r^2-1}{r-1}$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$:

$$y=x(x+a)(x+b),\ a,b\neq 0,\ a\neq b$$

$$\Delta=a^2b+ab^2-4a^3b^3$$

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=d^2-\frac{1}{16},\ c=0$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=c+c^2,\ c=\frac{10-2(1-c)}{(1-c)^2-9}$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$:

$$y^2+(1-c)xy-by=x^3-bx^2$$

$$b=(2d-1)(d-1),\ c=\frac{(2d-1)(d-1)}{d}$$

$$d=\frac{(1-c)(8(1-c)+2)}{8(1-c)^2-1}$$

$$\Delta=(1-c)^4b^3-8(1-c)^2b^4-(1-c)^3b^3+36(1-c)b^4+16b^5-27b^4$$

Dodatak B

Jednadžbe modularnih krivulja i njihovih kuspova

$$X_1(11): \ y^2 - y = x^3 - x^2$$

$$x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0$$

$$X_1(13): \ y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

$$x(x-1)(x^3 - 4x^2 + x + 1) = 0$$

$$X_1(14): \ y^2 + xy + y = x^3 - x$$

$$x(x-1)(x+1)(x^3 - 9x^2 - x + 1)(x^3 - 2x^2 - x + 1) = 0$$

$$X_1(15): \ y^2 + xy + y = x^3 + x^2$$

$$x(x+1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^2 - 6x^2 + 2x + 1) = 0$$

$$X_1(16): \ y^2 = x(x^2+1)(x^2+2x-1)$$

$$x(x-1)(x+1)(x^2-2x-1)(x^2+2x-1) = 0$$

$$X_1(18): \ y^2 = x^6+2x^5+5x^4+10x^3+10x^2+4x+1$$

$$x(x+1)(x^2+x+1)(x^2-3x-1) = 0$$

$$X_1(2,10): \ y^2 = x^3+x^2-x$$

$$x(x-1)(x+1)(x^2+x-1)(x^2-4x-1) = 0$$

$$X_1(2,12): \ y^2 = x^3-x^2+x$$

$$x(x-1)(2x-1)(2x^2-x+1)(3x^2-3x-1)(6x^2-6x-1) = 0$$

Dodatak C

Kodovi u Magmi

(*C*.1)
```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,-1,0,0]);
K<w>:=NumberField(x^2-13);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/5
The 2-Selmer group has rank 1
New point of infinite order (x = 1/4)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/9*(-2*w + 5) : 1/27*(-2*w + 32) : 1) ]
[
    <2, [ 0, 0 ]>
```

```
]
```

(*C*.2)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,0,1,-1,0]);
K<w>:=NumberField(x^2-13);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 1
After 2-descent:
    0 <= Rank(E) <= 0
    Sha(E)[2] is trivial

[ 0, 0 ]
[]
[
    <2, [ 0, 0 ]>
]
```

(*C*.3)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,1,1,0,0]);
rank, gens, sha:=DescentInformation(E);
E2:=QuadraticTwist(E,13);
rank2, gens2, sha2:=DescentInformation(E2);
K<w>:=NumberField(x^2-13);
```

```
E3:=BaseChange(E,K);
DescentInformation(E3);
```

Kod vraća:

```
Torsion Subgroup = Z/4
Analytic rank = 0
     ==> Rank(E) = 0


Torsion Subgroup = Z/2
Analytic rank = 1
     ==> Rank(E) = 1
The 2-Selmer group has rank 2
New point of infinite order (x = 2031)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 100 on the 2-coverings.)


Torsion Subgroup = Z/4
The 2-Selmer group has rank 2
New point of infinite order (x = 1/2*(w + 5))
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/2*(-w + 5) : -w + 4 : 1) ]
[
```

```
    <2, [ 0, 0 ]>
]
```

(*C*.4)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,1,0,-1,0]);
K<w>:=NumberField(x^2-13);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 2
New point of infinite order (x = 1/9*(-w + 2))
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/2*(w + 3) : -w - 3 : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.5)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,0,1,0]);
K<w>:=NumberField(x^2-13);
```

```
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/4
The 2-Selmer group has rank 2
New point of infinite order (x = 1/4)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (4 : 2*w : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.6)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6-2*x^5+x^4-2*x^3+6*x^2-4*x+1);
J:=Jacobian(C);
RankBounds(J);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,13);
J2:=Jacobian(C2);
RankBounds(J2);
TorsionSubgroup(J2);
```

```
Points(J2:Bound:=100);
```

Kod vraća:

```
0 0
Abelian Group isomorphic to Z/19
Defined on 1 generator
Relations:
    19*P[1] = 0

Mapping from: Abelian Group isomorphic to Z/19
Defined on 1 generator
Relations:
    19*P[1] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (1, x^3 - x^2, 2), (1, -x^3 + x^2, 2),
(x^2, 2*x - 1,  2), (x^2,-2*x + 1, 2), (x^2 - 2*x +
1, x, 2), (x^2 - 2*x + 1, -x, 2), (x, x^3 - 1, 2),
(x, -x^3 + 1, 2), (x, x^3 + 1, 2), (x, -x^3 - 1, 2),
(x - 1, x^3 - 2, 2), (x - 1, -x^3 + 2, 2), (x - 1,
x^3, 2), (x - 1, -x^3, 2), (x^2 - x, 2*x - 1, 2),
(x^2 - x, -2*x + 1, 2), (x^2 - x, 1, 2), (x^2 - x,
-1, 2) @}

0 0
Abelian Group of order 1
Mapping from: Abelian Group of order 1 to JacHyp:
J2 given by a rule [no inverse]
{@ (1, 0, 0) @}
```

(*C*.7) `Q<x>:=PolynomialRing(Rationals());`

```
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=JOne(16);
L:=LSeries(J);
IsZeroAt(L,1);

tr, p:=NewModularHyperellipticCurve(ModularSymbols(J));
C1:=HyperellipticCurve(p);
C2:=QuadraticTwist(C1,13);
J2:=Jacobian(C2);
RankBounds(J2);
```

Kod vraća:

```
false
0 0
```

(*C*.8)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=Jacobian(C);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,13);
J2:=Jacobian(C2);
TorsionSubgroup(J2);
Points(J2:Bound:=100);

K<w>:=NumberField(x^2-13);
J3:=BaseChange(J,K);
TwoTorsionSubgroup(J3);
```

Kod vraća:

```
Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0

Mapping from: Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (x^2 + 2*x + 1, 2*x, 2), (x^2 + 2*x +
1, -2*x, 2), (x^2 - 2*x + 1, 4*x - 2, 2), (x^2 - 2*x
+ 1, -4*x + 2, 2), (x + 1, 2, 1), (x + 1, -2, 1), (x,
0, 1), (x - 1, 2, 1), (x - 1, -2, 1), (x^2 + 2*x - 1,
0, 2), (x^2 + x, 2*x, 2), (x^2 + x, -2*x, 2), (x^2 -
1, 2*x, 2), (x^2 - 1, -2*x, 2), (x^2 - 1, 2, 2), (x^2
- 1, -2, 2), (x^2 + 1, 0, 2), (x^2 - x, 2*x, 2), (x^2
- x, -2*x, 2) @}

Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0

Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
```

```
    2*P[2] = 0 to JacHyp: J2 given by a rule [no inverse]
{@ (1, 0, 0), (x, 0, 1), (x^2 + 2*x - 1, 0, 2),
(x^2 + 1, 0, 2) @}

        Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0 to JacHyp: J3 given by a rule [no inverse]
```

(*C*.9)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6+2*x^5+5*x^4+10*x^3+10*x^2+4*x+1);
J:=Jacobian(C);
RankBounds(J);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,13);
J2:=Jacobian(C2);
RankBounds(J2);
TorsionSubgroup(J2);
Points(J2:Bound:=100);
```

Kod vraća:

```
0 0
Abelian Group isomorphic to Z/21
Defined on 1 generator
Relations:
    21*P[1] = 0

Mapping from: Abelian Group isomorphic to Z/21
Defined on 1 generator
Relations:
    21*P[1] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (1, x^3 + x^2, 2), (1, -x^3 - x^2, 2),
(x^2 + 2*x + 1, x, 2), (x^2 + 2*x + 1, -x, 2), (x^2,
2*x + 1, 2), (x^2, -2*x - 1, 2), (x + 1, x^3, 2),
(x + 1, -x^3, 2), (x + 1, x^3 + 2, 2), (x + 1, -x^3
- 2, 2), (x, x^3 - 1, 2), (x, -x^3 + 1, 2), (x, x^3
+ 1, 2), (x, -x^3 - 1, 2), (x^2 + x, 2*x + 1, 2),
(x^2 + x, -2*x - 1, 2), (x^2 + x, 1, 2), (x^2 + x,
-1, 2), (x^2 + x + 1, x - 1, 2), (x^2 + x + 1, -x
+ 1, 2) @}

0 0
Abelian Group of order 1

Mapping from: Abelian Group of order 1 to JacHyp:
J2 given by a rule [no inverse]
{@ (1, 0, 0) @}
```

(*C*.10)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,-1,0,0]);
```

```
K<w>:=NumberField(x^2-11);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/5
The 2-Selmer group has rank 1
New point of infinite order (x = 1/25*(2*w + 13))
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (-1/4 : 1/8*(w + 4) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.11)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,0,1,-1,0]);
K<w>:=NumberField(x^2-11);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 3
After 2-descent:
```

```
        0 <= Rank(E) <= 2
        Sha(E)[2] <= (Z/2)^2
    (Searched up to height 16 on the 2-coverings.)
    The Cassels-Tate pairing on Sel(2,E)/E[2] is
        [0 1]
        [1 0]
    After using Cassels-Tate:
        0 <= Rank(E) <= 0
        (Z/2)^2 <= Sha(E)[4] <= (Z/2)^2


    [ 0, 0 ]
    []
    [
        <2, [ 2, 2 ]>,
        <4, [ 0, 0 ]>
    ]
```

(*C*.12)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,1,1,0,0]);
rank, gens, sha:=DescentInformation(E);
E2:=QuadraticTwist(E,11);
rank2, gens2, sha2:=DescentInformation(E2);
K<w>:=NumberField(x^2-11);
E3:=BaseChange(E,K);
DescentInformation(E3);
```

Kod vraća:

```
Torsion Subgroup = Z/4
```

```
Analytic rank = 0
     ==> Rank(E) = 0


Torsion Subgroup = Z/2
Analytic rank = 1
     ==> Rank(E) = 1
The 2-Selmer group has rank 2
New point of infinite order (x = 25)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 100 on the 2-coverings.)


Torsion Subgroup = Z/4
The 2-Selmer group has rank 2
New point of infinite order (x = 1/1225*(1272*w + 3168))
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/1225*(1272*w + 3168) :
1/42875*(-125928*w - 434907) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.13)
```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,1,0,-1,0]);
K<w>:=NumberField(x^2-11);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 2
New point of infinite order (x = 1/1369*(132*w - 1367))
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/1369*(132*w - 1367) : 1/50653*(-264*w - 45181) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.14)
```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,0,1,0]);
K<w>:=NumberField(x^2-11);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/4
The 2-Selmer group has rank 2
New point of infinite order (x = 5*w + 18)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (5*w + 18 : 30*w + 101 : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.15)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6-2*x^5+x^4-2*x^3+6*x^2-4*x+1);
J:=Jacobian(C);
RankBounds(J);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,11);
J2:=Jacobian(C2);
RankBounds(J2);
TorsionSubgroup(J2);
Points(J2:Bound:=100);
```

Kod vraća:

```
0 0
```

```
Abelian Group isomorphic to Z/19
Defined on 1 generator
Relations:
    19*P[1] = 0
Mapping from: Abelian Group isomorphic to Z/19
Defined on 1 generator
Relations:
    19*P[1] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (1, x^3 - x^2, 2), (1, -x^3 + x^2, 2),
(x^2, 2*x - 1, 2), (x^2, -2*x + 1, 2), (x^2 - 2*x +
1, x, 2), (x^2 - 2*x + 1, -x, 2), (x, x^3 - 1, 2),
(x, -x^3 + 1, 2), (x, x^3 + 1, 2), (x, -x^3 - 1, 2),
(x - 1, x^3 - 2, 2), (x - 1, -x^3 + 2, 2), (x - 1,
x^3, 2), (x - 1, -x^3, 2), (x^2 - x, 2*x - 1, 2),
(x^2 - x, -2*x + 1, 2), (x^2 - x, 1, 2), (x^2 - x, -1,
2) @}
0 0
Abelian Group of order 1
Mapping from: Abelian Group of order 1 to JacHyp:
J2 given by arule [no inverse]
{@ (1, 0, 0) @}
```

(*C*.16)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=JOne(16);
L:=LSeries(J);
IsZeroAt(L,1);

tr, p:=NewModularHyperellipticCurve(ModularSymbols(J));
```

```
C1:=HyperellipticCurve(p);
C2:=QuadraticTwist(C1,11);
J2:=Jacobian(C2);
RankBounds(J2);
```

Kod vraća:

```
false
0 0
```

(*C*.17)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=Jacobian(C);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,11);
J2:=Jacobian(C2);
TorsionSubgroup(J2);
Points(J2:Bound:=100);

K<w>:=NumberField(x^2-11);
J3:=BaseChange(J,K);
TwoTorsionSubgroup(J3);
```

Kod vraća:

```
Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
```

```
    10*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (x^2 + 2*x + 1, 2*x, 2), (x^2 + 2*x +
1, -2*x, 2), (x^2 - 2*x + 1, 4*x - 2, 2), (x^2 - 2*x
+ 1, -4*x + 2, 2), (x + 1, 2, 1), (x + 1, -2, 1), (x,
0, 1), (x - 1, 2, 1), (x - 1, -2, 1), (x^2 + 2*x - 1,
0, 2), (x^2 + x, 2*x, 2), (x^2 + x, -2*x, 2), (x^2 -
1, 2*x, 2), (x^2 - 1, -2*x, 2), (x^2 - 1, 2, 2), (x^2
- 1, -2, 2), (x^2 + 1, 0, 2), (x^2 - x, 2*x, 2), (x^2
- x, -2*x, 2) @}
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0 to JacHyp: J2 given by a rule [no inverse]
{@ (1, 0, 0), (x, 0, 1), (x^2 + 2*x - 1, 0, 2), (x^2
+ 1, 0, 2) @}
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0
```

```
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0 to JacHyp: J3 given by a rule [no inverse]
```

(*C*.18)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,-1,0,0]);
K<w>:=NumberField(x^2-7);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/5
The 2-Selmer group has rank 1
New point of infinite order (x = 1/9*(-2*w + 8))
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (2*w + 5 : -6*w - 15 : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.19)

```
Q<x>:=PolynomialRing(Rationals());
```

```
E:=EllipticCurve([1,0,1,-1,0]);
K<w>:=NumberField(x^2-7);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 2
New point of infinite order (x = 3)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/9*(2*w - 1) : 1/27*(-4*w + 2) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.20)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,1,1,0,0]);
rank, gens, sha:=DescentInformation(E);
E2:=QuadraticTwist(E,7);
rank2, gens2, sha2:=DescentInformation(E2);
K<w>:=NumberField(x^2-7);
E3:=BaseChange(E,K);
DescentInformation(E3);
```

Kod vraća:

```
Torsion Subgroup = Z/4
Analytic rank = 0
     ==> Rank(E) = 0


Torsion Subgroup = Z/2
Analytic rank = 1
     ==> Rank(E) = 1
The 2-Selmer group has rank 2
New point of infinite order (x = -3)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 100 on the 2-coverings.)


Torsion Subgroup = Z/4
The 2-Selmer group has rank 2
New point of infinite order (x = 3/4)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (3/4 : 1/8*(-4*w - 7) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.21)
```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,1,0,-1,0]);
K<w>:=NumberField(x^2-7);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 1
After 2-descent:
    0 <= Rank(E) <= 0
    Sha(E)[2] is trivial

[ 0, 0 ]
[]
[
    <2, [ 0, 0 ]>
]
```

(*C*.22)
```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,0,1,0]);
K<w>:=NumberField(x^2-7);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/4
```

```
The 2-Selmer group has rank 1
After 2-descent:
    0 <= Rank(E) <= 0
    Sha(E)[2] is trivial

[ 0, 0 ]
[]
[
    <2, [ 0, 0 ]>
]
```

(*C*.23)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=JOne(16);
L:=LSeries(J);
IsZeroAt(L,1);

tr, p:=NewModularHyperellipticCurve(ModularSymbols(J));
C1:=HyperellipticCurve(p);
C2:=QuadraticTwist(C1,7);
J2:=Jacobian(C2);
RankBounds(J2);
```

Kod vraća:

```
false
0 0
```

(*C*.24)
```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=Jacobian(C);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,7);
J2:=Jacobian(C2);
TorsionSubgroup(J2);
Points(J2:Bound:=100);

K<w>:=NumberField(x^2-7);
J3:=BaseChange(J,K);
TwoTorsionSubgroup(J3);
```

Kod vraća:

```
Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (x^2 + 2*x + 1, 2*x, 2), (x^2 + 2*x + 1,
-2*x, 2), (x^2 - 2*x + 1, 4*x - 2, 2), (x^2 - 2*x + 1,
-4*x + 2, 2), (x + 1, 2, 1), (x + 1, -2, 1), (x, 0, 1),
(x - 1, 2, 1), (x - 1, -2, 1), (x^2 + 2*x - 1, 0, 2),
(x^2 + x, 2*x, 2), (x^2 + x, -2*x, 2), (x^2 - 1, 2*x,
```

```
2), (x^2 − 1, −2∗x, 2), (x^2 − 1, 2, 2), (x^2 − 1, −2,
2), (x^2 + 1, 0, 2), (x^2 − x, 2∗x, 2), (x^2 − x, −2∗x,
2) @}
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2∗P[1] = 0
    2∗P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2∗P[1] = 0
    2∗P[2] = 0 to JacHyp: J2 given by a rule [no inverse]
{@ (1, 0, 0), (x, 0, 1), (x^2 + 2∗x − 1, 0, 2), (x^2
+ 1, 0, 2) @}
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2∗P[1] = 0
    2∗P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2∗P[1] = 0
    2∗P[2] = 0 to JacHyp: J3 given by a rule [no inverse]
```

(*C*.25)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,−1,−1,0,0]);
K<w>:=NumberField(x^2−6);
```

```
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/5
The 2-Selmer group has rank 1
New point of infinite order (x = 7*w + 18)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (1/6 : 1/36*(-7*w + 18) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.26)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,0,1,-1,0]);
K<w>:=NumberField(x^2-6);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 2
New point of infinite order (x = 1/25*(-8*w - 3))
After 2-descent:
```

```
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (-1/4 : 1/8*(-2*w - 3) : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.27)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,1,1,0,0]);
rank, gens, sha:=DescentInformation(E);
E2:=QuadraticTwist(E,6);
rank2, gens2, sha2:=DescentInformation(E2);
K<w>:=NumberField(x^2-6);
E3:=BaseChange(E,K);
DescentInformation(E3);
```

Kod vraća:

```
Torsion Subgroup = Z/4
Analytic rank = 0
    ==> Rank(E) = 0


Torsion Subgroup = Z/2
Analytic rank = 0
    ==> Rank(E) = 0
```

```
Torsion Subgroup = Z/4
The 2-Selmer group has rank 1
After 2-descent:
    0 <= Rank(E) <= 0
    Sha(E)[2] is trivial

[ 0, 0 ]
[]
[
    <2, [ 0, 0 ]>
]
```

(*C*.28)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,1,0,-1,0]);
K<w>:=NumberField(x^2-6);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/6
The 2-Selmer group has rank 2
New point of infinite order (x = -2*w + 7)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
```

```
[ (2*w + 7 : 8*w + 23 : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.29)

```
Q<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,0,1,0]);
K<w>:=NumberField(x^2-6);
E2:=BaseChange(E,K);
DescentInformation(E2);
```

Kod vraća:

```
Torsion Subgroup = Z/4
The 2-Selmer group has rank 2
New point of infinite order (x = -2*w + 5)
After 2-descent:
    1 <= Rank(E) <= 1
    Sha(E)[2] is trivial
(Searched up to height 16 on the 2-coverings.)

[ 1, 1 ]
[ (2*w + 5 : -6*w - 15 : 1) ]
[
    <2, [ 0, 0 ]>
]
```

(*C*.30)

```
Q<x>:=PolynomialRing(Rationals());
```

```
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=JOne(16);
L:=LSeries(J);
IsZeroAt(L,1);

tr, p:=NewModularHyperellipticCurve(ModularSymbols(J));
C1:=HyperellipticCurve(p);
C2:=QuadraticTwist(C1,6);
J2:=Jacobian(C2);
RankBounds(J2);
```

Kod vraća:

```
false
0 0
```

(*C*.31)

```
Q<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J:=Jacobian(C);
TorsionSubgroup(J);
Points(J:Bound:=100);

C2:=QuadraticTwist(C,6);
J2:=Jacobian(C2);
TorsionSubgroup(J2);
Points(J2:Bound:=100);

K<w>:=NumberField(x^2-6);
J3:=BaseChange(J,K);
TwoTorsionSubgroup(J3);
```

Kod vraća:

```
Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/10
Defined on 2 generators
Relations:
    2*P[1] = 0
    10*P[2] = 0 to JacHyp: J given by a rule [no inverse]
{@ (1, 0, 0), (x^2 + 2*x + 1, 2*x, 2), (x^2 + 2*x +
1, -2*x, 2), (x^2 - 2*x + 1, 4*x - 2, 2), (x^2 - 2*x
+ 1, -4*x + 2, 2), (x + 1, 2, 1), (x + 1, -2, 1), (x,
0, 1), (x - 1, 2, 1), (x - 1, -2, 1), (x^2 + 2*x - 1,
0, 2), (x^2 + x, 2*x, 2), (x^2 + x, -2*x, 2), (x^2 -
1, 2*x, 2), (x^2 - 1, -2*x, 2), (x^2 - 1, 2, 2), (x^2
- 1, -2, 2), (x^2 + 1, 0, 2), (x^2 - x, 2*x, 2), (x^2
- x, -2*x, 2) @}
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0 to JacHyp: J2 given by a rule [no inverse]
{@ (1, 0, 0), (x, 0, 1), (x^2 + 2*x - 1, 0, 2), (x^2
+ 1, 0, 2) @}
```

```
Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0
Mapping from: Abelian Group isomorphic to Z/2 + Z/2
Defined on 2 generators
Relations:
    2*P[1] = 0
    2*P[2] = 0 to JacHyp: J3 given by a rule [no inverse]
```

Bibliografija

[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. 79 (2010), 2371–2386.

[2] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[3] H. Cohen, G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)*, Chapman and Hall/CRC; 1 edition, 2005.

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

[5] A. Dujella, *Algoritmi za eliptičke krivulje* (skripta kolegija na doktorskom studiju 2008./2009., PMF — Matematički odsjek, dostupno na https://web.math.pmf.unizg.hr/ duje/elipticke/algelip.pdf), 2013.

[6] D. Jeon, C. H. Kim, A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta. Arith. 133.3 (2004), 291-301.

[7] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta. Arith. 152 (2012), 291-305.

[8] D. Krumm, *Quadratic Points on Modular Curves*, doktorska disertacija, Athens, Georgia, 2013.

[9] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976), 193–237.

[10] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory 130 (2010), 1964-1968.

[11] F. Najman, *Eliptičke krivulje nad poljima algebarskih brojeva* (skripta kolegija na doktorskom studiju 2013., PMF — Matematički odsjek, dostupno na https://web.math.pmf.unizg.hr/ fnajman/elipticke.pdf), 2013.

[12] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math. J. Okayama Univ. 53 (2011), 75-82.

[13] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. 144 (2010), 17–52.

[14] S. Siksek, *Explicit Chabauty over Number Fields*, Algebra & Number Theory 7, issue 4, (2013) 765-793.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag New York, 2009.

[16] M. Stoll, *Rational Points on Curves*, Journal de Théorie des Nombres de Bordeaux 23 (2011) , 257-277.

[17] M. Stoll, *Implementing 2-descent on Jacobians of hyperelliptic curves of genus two, II*, Acta Arith. 98 (2001), 245–277.

[18] M. Ulas, *On torsion points on an elliptic curves via division polynomials*, Universitatis Iagellonicae Acta Mathematica 43 (2005), 103-108.

[19] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman and Hall/CRC; second edition (2008).

[20] T. Weston, *Algebraic Number Theory*, dostupno na http://people.math.umass.edu/ weston/cn/notes.pdf

[21] Y. Yang, *Defining equations of modular curves*, Advances in Mathematics 204 (2006) 481–508.

[22] D. J. Zywina, *On the possible images of the mod l representations associated to elliptic curves over* $\mathbb{Q}$, arXiv:1508.07660 [math.NT] (2015).

Sažetak

Antonela Trbović

Torzijske grupe eliptičkih krivulja nad kvadratnim poljima

Mazur je 1978. godine dokazao kojih se točno 15 grupa pojavljuju kao torzijska podgrupa kada prolazimo po svim eliptičkim krivuljama definiranim nad poljem racionalnih brojeva. 1990-ih godina dokazan je sličan rezultat za kvadratna polja, koji nam govori koje se sve grupe mogu pojaviti kao torzijska podgrupa eliptičke krivulje ako prolazimo po svim kvadratnim poljima.

No, taj rezultat nam ne govori ništa o tome na koje grupe možemo naići nad fiksnim kvadratnim poljem. U ovom radu opisujemo metode kojima možemo odrediti koje se sve grupe pojavljuju kao torzijske podgrupe eliptičkih krivulja ako fiksiramo neko kvadratno polje. Navodimo i konkretan primjer kroz kojeg detaljno rješavamo i određene probleme na koje možemo naići kod provođenja opisanih metoda.

U radu se navode i sve potrebne definicije i rezultati vezani uz eliptičke krivulje, hipereliptičke krivulje i modularne krivulje koje koristimo kod traženja mogućih torzijskih grupa nad fiksnim kvadratnim poljem. Cijela teorijska pozadina popraćena je konkrenim primjerima, a do nekih rezultata dolazimo uz pomoć programskog paketa Magma, što je jasno naznačeno u tekstu i u jednom od dodataka ovom radu.

Ključne riječi: Torzijska grupa, Eliptičke krivulje, Kvadratna polja.

Summary

Antonela Trbović

Torsion groups of elliptic curves over quadratic fields

In 1978., Mazur proved exactly which groups appear as a torsion subgroup if we go through all elliptic curves defined over the field of rational numbers. In the 1990s, a similar result was proved for quadratic fields, that tells us which groups can appear as a torsion subgroup of an elliptic curve if the field varies through all quadratic fields.

That result tells us nothing about possible torsion subgroups if we fix a quadratic field. In this paper we describe methods that we can use to determine all possible groups that can appear as torsion subgroups of elliptic curves if we fix a quadratic field. We also have an example in which we solve some of the problems that can appear while conducting the described methods.

Furthermore, we mention all the necessary definitions and results related to elliptic curves, hyperelliptic curves and modular curves that we use while determining possible torsion groups over the fixed quadratic field. All theoretical material is accompanied with concrete examples. Also, in this paper we use Magma, a computer algebra system, which helps us to get some necessary results. Places in the text in which we use Magma are clearly marked and also mentioned in one of the appendices.

Key words: Torsion group, Elliptic Curves, Quadratic fields.