Mordell-Weilove grupe i izogenije familija eliptičkih krivulja

Mikić, Miljen

Sveučilište u Zagrebu

PRIRODOSLOVNO - MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Miljen Mikić

Mordell-Weilove grupe i izogenije familija eliptičkih krivulja

DOKTORSKI RAD

Zagreb, 2014.

University of Zagreb

FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Miljen Mikić

Mordell-Weil groups and isogenies of the families of elliptic curves

DOCTORAL THESIS

Zagreb, 2014

Sveučilište u Zagrebu

PRIRODOSLOVNO - MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Miljen Mikić

Mordell-Weilove grupe i izogenije familija eliptičkih krivulja

DOKTORSKI RAD

Mentori:
prof.dr.sc. Andrej Dujella
doc.dr.sc. Filip Najman

Zagreb, 2014.

University of Zagreb

FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS

Miljen Mikić

Mordell-Weil groups and isogenies of the families of elliptic curves

DOCTORAL THESIS

Supervisors:
prof.dr.sc. Andrej Dujella
doc.dr.sc. Filip Najman

Zagreb, 2014

Zahvala

Izrada ove disertacije bila je zahtjevno, ali zanimljivo putovanje. Dozvolite mi da se zahvalim suputnicima: prije svega mojoj obitelji, a najviše supruzi Rozariji, što su imali strpljenja za vrijeme koje sam proveo zatvoren u sobi s olovkom, papirima i računalom. Hvala i kolegama iz Hrvatskog Telekoma d.d. te Asseca SEE d.d. na razumijevanju jer ponekad nije bilo jednostavno uskladiti predavanja, ispite i istraživanje s poslom koji zahtijeva puno radno vrijeme.

Na kraju, zahvaljujem se svim članovima Seminara za teoriju brojeva i algebru, članovima povjerenstva za ocjenu disertacije, a posebno sjajnim mentorima prof.dr.sc. Andreju Dujelli i doc.dr.sc. Filipu Najmanu na svim savjetima, podršci i vremenu kojeg su uložili i tako mi pomogli da ovo putovanje uspješno privedemo kraju.

Sadržaj

Uvod

Eliptička krivulja je glatka projektivna algebarska krivulja genusa 1 s jednom definiranom točkom. Eliptičke krivulje su bitan dio brojnih važnih matematičkih rezultata u posljednjih stotinu godina. Primjerice, Teorem o modularnosti spada među najvažnije matematičke rezultate 20. stoljeća te kao najpoznatiju primjenu (nakon čak 358 godina neuspješnih pokušaja) daje dokaz Velikog Fermatovog teorema koji glasi:

Ne postoje prirodni brojevi x, y, z takvi da je $x^n = y^n + z^n$, gdje je $n > 2$ prirodan broj.

Nadalje, čuvena Birch-Swinnerton-Dyer slutnja [65] o rangu eliptičkih krivulja jedan je od sedam tzv. „Milenijskih problema" za čije je rješavanje Clay Mathematics Institute ponudio milijun dolara po svakom problemu.

Iako su dio teorije brojeva, grane koja povijesno spada u „čistu" matematiku, eliptičke krivulje su se pojavom kriptografije pokazale kao izuzetno korisne i u primjeni. Eliptičke krivulje nad konačnim poljima igraju važnu ulogu u kriptografiji javnog ključa, pogotovo kad treba postići istu sigurnost s manjim ključem. Naime, pokazuje se [46] da kriptosustavi koji se baziraju na eliptičkim krivuljama pružaju istu sigurnost kao RSA kriptosustav uz čak 7 puta manju duljinu ključa. Kad prostor za spremanje ključa nije velik (npr. „pametne kartice") to može biti od osobitog značaja. Interesantno je spomenuti da je čak i američka National Security Agency propisala da se sve razmjene ključeva u elektroničkoj korespondenciji američke Vlade kao i digitalno potpisivanje dokumenata moraju obavljati isključivo korištenjem Elliptic Curve Cryptography [57]. Osim u kriptografiji, eliptičke krivulje koriste se i u nekima od najbržih algoritama za faktorizaciju cijelih brojeva [45] i dokazivanje prostosti [1].

Za cijele brojeve n i m, $D(n)$-m-torka definira se kao skup od m cijelih brojeva različitih od nule, takvih da je umnožak svaka dva broja iz tog skupa uvećan za n potpun kvadrat. Jedno od najzanimljivijih pitanja vezanih uz $D(n)$-m-torke jest: koliko veliki ti skupovi mogu biti? Pokazuje se da je taj problem usko povezan s određivanjem torzijske grupe i ranga pripadajućih eliptičkih krivulja. Veličina ranga je posebno interesantna jer postoji slutnja da broj cjelobrojnih točaka na eliptičkoj krivulji E u Weierstrassovom obliku eksponencijalno raste s rangom od $E(\mathbb{Q})$.

Starogrčki matematičar Diofant pronašao je $D(256)$-četvorku $\{1, 33, 68, 105\}$, dok je prvu $D(1)$-četvorku, skup $\{1, 3, 8, 120\}$, pronašao Fermat [9, 10]. Dakle, problem najveće moguće veličine $D(n)$-m-torke je vrlo star problem, a o njegovoj težini i zanimljivosti svjedoči činjenica da su i brojni suvremeni matematičari ostavili velik trag u ovom području. Jedan od najvažnijih neriješenih problema vezan uz $D(n)$-m-torke jest slutnja da ne postoji $D(1)$-petorka. Mi ćemo proučavati problem proširenja $D(n^2)$-trojki na $D(n^2)$-četvorke i promatrati rang i moguće oblike torzijskih grupa eliptičkih krivulja koje nastaju tim postupkom. Najvažnije rezultate o torzijskim grupama dokazat ćemo za eliptičke krivulje dobivene iz $D(4)$-trojki. Mazur je u svom članku [47] pobrojao 15 mogućih torzijskih grupa eliptičkih krivulja nad $\mathbb{Q}$, a mi ćemo dokazati da su u ovom slučaju moguće samo dvije. Taj dio radnje temelji se na članku [26].

Nadalje, promatrat ćemo familije $D(1)$-trojki (Diofantovih trojki) oblika $\{k-1, k+1, c_l(k)\}$, gdje za $k \geq 2$ i $l \in \mathbb{N}$, definiramo niz $\{c_l(k)\}$ kao:

$$c_l(k) = \frac{(k + \sqrt{k^2-1})^{2l+1} + (k - \sqrt{k^2-1})^{2l+1} - 2k}{2(k^2-1)}.$$

Dujella je bio prvi koji se bavio tim familijama i on je uspio u slučaju $l = 1$ pronaći sve cjelobrojne točke za krivulje ranga 1, te za određene potfamilije krivulja ranga 2 i 3. Osim njega, ovim familijama i pridruženim problemima bavili su se i Pethő, Najman, Bugeuad, Mignotte i Fujita. Najman je pokazao da torzijska grupa krivulja induciranih trojkama oblika $\{k-1, k+1, c_3(k)\}$ može biti ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, ali je ostalo otvoreno pitanje može li se potonja ikad pojaviti. U našem radu ćemo eliminirati tu mogućnost. Kao logičan idući korak, dokazat ćemo isto i za slučaj $\{k-1, k+1, c_4(k)\}$. Taj rezultat kasnije ćemo proširiti na sve familije krivulja dobivenih iz Diofantovih trojki oblika $\{k-1, k+1, c_l(k)\}$, takve da l daje ostatak 1 ili 2 pri dijeljenju s 4. O rangu krivulja dobivenih iz Diofantovih trojki oblika $\{k-1, k+1, c_l(k)\}$ dosad se iz radova Najmana, Dujelle i Pethőa zna da je rang veći ili jednak 2 u slučajevima $l = 2, 3$, odnosno $k = 2$. Mi ćemo ovaj rezultat proširiti na sve familije eliptičkih krivulja dobivenih iz Diofantovih trojki oblika $\{k-1, k+1, c_l(k)\}$ gdje je $l \geq 2$. Ovaj dio radnje temelji se na rezultatima iz članka [48]. Osim familije $\{k-1, k+1, c_l(k)\}$, dokazat ćemo i određene rezultate o torzijskoj grupi eliptičkih krivulja koje dobijemo iz familije Diofantovih trojki oblika $\{a, b, a+b+2r\}$, gdje je $ab+1 = r^2$.

Konačno, odredit ćemo broj eliptičkih krivulja s cikličkom izogenijom stupnja n nad raznim kvartičnim poljima. Najman, Kamienny i drugi bavili su se određivanjem broja eliptičkih krivulja s unaprijed određenom torzijom, i tu ima dosta rezultata nad raznim poljima algebarskih brojeva. Do većine rezultata došlo se promatranjem tzv. modularnih

krivulja, pa ćemo i mi primijeniti sličan pristup. Iskoristit ćemo rezultate Yanga, koji je našao modele od $X_0(n)$, gdje je $X_0(n)$ modularna krivulja dobivena kompaktifikacijom modularne krivulje $Y_0(n)$, tj. dodavanjem kaspova. Mazur je u svom radu odredio stupnjeve izogenija nad poljem racionalnih brojeva, a mi ćemo se koncentrirati na kvartična polja. Promatranjem torzije i ranga Najman je pronašao kvadratna polja nad kojima krivulje $X_0(n)$ za razne n-ove imaju i dalje konačno mnogo točaka, ali više nego u racionalnom slučaju. Mi ćemo na temelju toga dokazati da postoji beskonačno mnogo kvartičnih polja takvih da isto vrijedi, čime ujedno dokazujemo i da postoji beskonačno mnogo kvartičnih polja nad kojima ima konačno mnogo eliptičkih krivulja s cikličkom izogenijom stupnja n.

Ciljevi i hipoteze istraživanja

Ciljevi ovog istraživanja su:

- pronaći moguće oblike torzijskih grupa za eliptičke krivulje dobivene proširivanjem $D(4)$-trojki na $D(4)$-četvorke
- odrediti Mordell-Weilove grupe eliptičkih krivulja induciranih familijama Diofantovih trojki oblika $\{k-1, k+1, c_l(k)\}$
- prebrojati koliko ima eliptičkih krivulja s cikličkom izogenijom stupnja n nad raznim kvartičnim poljima

Hipoteze koje ćemo provjeriti su da eliptičke krivulje dobivene iz $D(4)$-trojki mogu imati samo jednu od torzijskih grupa: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, te da je za velik broj vrijednosti od k i l, torzijska grupa eliptičkih krivulja dobivenih iz Diofantovih trojki oblika $\{k-1, k+1, c_l(k)\}$ jednaka $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i njihov rang je barem 2.

Doprinosi doktorskog rada

Slutnja je da je jedina moguća torzijska grupa eliptičkih krivulja dobivenih iz Diofantovih trojki $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i ovaj rad potvrđuje tu slutnju za familije Diofantovih trojki te pruža metode za daljnje istraživanje tog problema. Nadalje, dosadašnji rezultati o rangu familija eliptičkih krivulja koji su dobiveni za pojedine specijalne slučajeve ovdje su bitno prošireni. Naposljetku, dok se o torzijskim grupama eliptičkih krivulja nad raznim poljima algebarskih brojeva puno zna, za izogenije to nije slučaj te dobiveni rezultati iz ove disertacije predstavljaju dobar temelj za daljnji napredak u tom području.

Pregled doktorskog rada po poglavljima

Prvo poglavlje naslovljeno „$D(n^2)$-trojke i inducirane eliptičke krivulje" započinje s definicijama i pregledom najvažnijih rezultata koji su dosad otkriveni u ovom području.

Nakon toga promatraju se $D(n^2)$-trojke i prezentiraju rezultati o Mordell-Weilovoj grupi induciranih eliptičkih krivulja, dobiveni za ovaj općeniti slučaj. Glavni dio poglavlja su rezultati o torzijskoj grupi eliptičkih krivulja induciranih $D(4)$-trojkama.

U drugom poglavlju koje se zove „Familije Diofantovih trojki i inducirane eliptičke krivulje" najviše se bavimo familijama Diofantovih trojki oblika $\{k-1, k+1, c_l(k)\}$ te prezentiramo teoreme o Mordell-Weilovoj grupi eliptičkih krivulja pridruženih familijama takvih Diofantovih trojki. Poglavlje zaključujemo rezultatima o torzijskoj grupi krivulja dobivenih iz jedne druge familije Diofantovih trojki: $\{a, b, a+b+2r\}$.

Treće, posljednje poglavlje s naslovom „Eliptičke krivulje s cikličkom izogenijom stupnja n" prvo daje kratki uvod u modularne krivulje i prikazuje najvažnije dosadašnje rezultate. Nakon toga slijedi niz novih rezultata o rangu modularnih krivulja $X_0(n)$, što za posljedicu daje nalaženje kvartičnih polja nad kojima ima više krivulja s cikličkom izogenijom stupnja n nego u racionalnom slučaju, ali i dalje konačno mnogo.

Disertacija završava bibliografijom, sažetkom i životopisom autora.

Poglavlje 1

$D(n^2)$-trojke i inducirane eliptičke krivulje

1.1 Uvod i pregled poznatih rezultata

1.1.1 Eliptičke krivulje

Neka je $\mathbb{K}$ polje.

Definicija 1.1. Eliptička krivulja nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja s barem jednom ($\mathbb{K}$-racionalnom) točkom.

Eliptička krivulja ima afinu jednadžbu koja se biracionalnim transformacijama može svesti na oblik

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

kojeg nazivamo Weierstrassova forma. Ovaj oblik može se dodatno pojednostaviti ako je karakteristika od $\mathbb{K}$ različita od 2 i 3, tada nadopunjavanjem na potpun kvadrat i potpun kub tu jednadžbu transformiramo u oblik

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

kojeg nazivamo kratka Weierstrassova forma. Uvjet nesingularnosti je da pripadni polinom $f(x) = x^3 + ax + b$ nema višestrukih nultočki, odnosno da je diskriminanta $-4a^3 - 27b^2$ različita od nule. Skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koji zadovoljavaju jednadžbu

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

gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$ zajedno s točkom u beskonačnosti $\mathcal{O}$ označavamo s $E(\mathbb{K})$. Taj skup točaka eliptičke krivulje E nad poljem $\mathbb{K}$ čini abelovu grupu uz operaciju zbrajanja koju definiramo na sljedeći način. Neka je $P = (x_1, y_1),\ Q = (x_2, y_2)$, onda je:

1) -$\mathcal{O} = \mathcal{O}$;

2) $-P = (x_1, -y_1)$;

3) $\mathcal{O} + P = P$;

4) ako je $Q = -P$, onda je $P + Q = \mathcal{O}$;

5) ako je $Q \neq -P$, onda je $P + Q = (x_3, y_3)$, gdje je

$$x_3 = \lambda^2 - x_1 - x_2, \;\; y_3 = -y_1 + \lambda(x_1 - x_3),$$

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

U ovom radu najviše ćemo se baviti eliptičkim krivuljama nad poljem $\mathbb{Q}$. Najvažnija činjenica o njima jest Mordell-Weilov teorem:

Teorem 1.1. *(Mordell-Weil) Grupa $E(\mathbb{Q})$ je konačno generirana abelova grupa.*

To znači da postoji konačan skup racionalnih točaka P_1, P_2, ..., P_k (generatora) na E iz kojih se sve ostale racionalne točke na E mogu dobiti povlačeći sekante i tangente. Budući da je svaka konačno generirana abelova grupa izomorfna produktu cikličkih grupa, dobivamo sljedeći korolar:

Korolar 1.2. $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$.

Drugim riječima, grupa $E(\mathbb{Q})$ je produkt torzijske grupe i r ($r \geq 0$) kopija beskonačne cikličke grupe. Podgrupu $E(\mathbb{Q})_{tors}$ od $E(\mathbb{Q})$ čine sve točke konačnog reda i nju nazivamo torzijska grupa od E. Nenegativni cijeli broj r naziva se rang od E i označava se s $\text{rank}(E(\mathbb{Q}))$. Korolar 1.2 nam zapravo kaže da postoji r racionalnih točaka P_1, P_2, ..., P_r beskonačnog reda na krivulji E takvih da se svaka racionalna točka P na E može prikazati kao linearna kombinacija

$$P = T + m_1P_1 + m_2P_2 + ... + m_rP_r,$$

gdje je T neka točka konačnog reda, a $m_1, m_2, ..., m_r$ su cijeli brojevi. U disertaciji se prvenstveno bavimo pitanjima koje sve vrijednosti mogu poprimiti $E(\mathbb{Q})_{tors}$ i $\text{rank}(E(\mathbb{Q}))$ za određene familije eliptičkih krivulja, te kako ih izračunati. U općenitom slučaju, određivanje ranga znatno je teže od određivanja torzijske grupe. Spomenimo i vrlo važan Mazurov rezultat [47] iz 1978. koji karakterizira sve moguće torzijske grupe eliptičkih krivulja nad $\mathbb{Q}$. To su:

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

Različiti oblici iste eliptičke krivulje nad $\mathbb{Q}$ su međusobno izomorfni, tj. transformacije krivulje čuvaju grupovni zakon. Tu činjenicu ćemo iskoristiti pri računanju Mordell-Weilove grupe tako što ćemo krivulju koju promatramo svesti u oblik koji je pogodniji za njeno računanje, a da se pri tome ta grupa ne promijeni. Ukoliko želimo utvrditi ima li na krivulji točaka reda $2k$, gdje je $k \geq 2$, sljedeća propozicija nam je izuzetno korisna:

Propozicija 1.3. ([**43, 4.2, str.85**]) *Neka je E eliptička krivulja nad poljem $\mathbb{K}$ karakteristike različite od 2 i 3. Neka je*

$$E : y^2 = (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha, \beta, \gamma \in \mathbb{K}.$$

Za točku $Q = (x_2, y_2) \in E(\mathbb{K})$ postoji točka $P = (x_1, y_1) \in E(\mathbb{K})$ takva da je $Q = 2P$ ako i samo ako su $x_2 - \alpha$, $x_2 - \beta$, $x_2 - \gamma$ potpuni kvadrati u $\mathbb{K}$.

Spomenimo i da cjelobrojne točke na eliptičkoj krivulji za razliku od racionalnih nemaju uređenu strukturu. Nadalje, dok racionalnih točaka može biti beskonačno u slučaju pozitivnog ranga, cjelobrojnih može biti samo konačno o čemu govori Siegelov teorem. Za određivanje cjelobrojnih točaka obično se koriste eliptički logaritmi i Thueove jednadžbe, iako postoje i druge metode, npr. pomoću Pellovskih jednadžbi [**53**]. Istaknimo i da između cjelobrojnih točaka i točaka konačnog reda postoji zanimljiva veza:

Teorem 1.4. *(Lutz-Nagell) Neka je E eliptička krivulja zadana jednadžbom $y^2 = f(x) = x^3 + ax^2 + bx + c$, gdje su $a, b, c \in \mathbb{Z}$. Ako je $P = (x_1, y_1)$ točka konačnog reda u $E(\mathbb{Q})$, tada su $x_1, y_1 \in \mathbb{Z}$.*

Dok nam Lutz-Nagellov teorem kaže da je svaka točka konačnog reda na eliptičkoj krivulji ujedno i cjelobrojna, postoji i vrlo važna slutnja koja povezuje cjelobrojne točke s rangom. Naime, sluti se (vidi [**61, Conjecture 3.5, str. 250**]) da broj cjelobrojnih točaka na krivulji E u Weierstrassovom obliku raste eksponencijalno s rangom od $E(\mathbb{Q})$.

1.1.2 $D(n)$-m-torke

Definirajmo sada formalno $D(n)$-m-torke; njih i njihovu vezu s eliptičkim krivuljama proučavat ćemo i u ovom i u idućem poglavlju.

Definicija 1.2. Neka je n zadani cijeli broj različit od nule. Skup $\{a_1, a_2, \ldots, a_m\}$ od m cijelih brojeva različitih od nule nazivamo $D(n)$-m-torka (ili Diofantova m-torka sa svojstvom $D(n)$) ako je $a_i a_j + n$ potpun kvadrat za sve $1 \leq i < j \leq m$.

Kao što smo spomenuli u uvodu, jedno od najzanimljivijih pitanja vezanih uz $D(n)$-m-torke jest kolika je najveća vrijednost od m za pojedini n. $D(n)$-trojki ima beskonačno mnogo za svaki cijeli broj n, to su, primjerice, trojke $\{a, b, a+b+2r\}$, gdje je $ab + n = r^2$. Euler je prvi pronašao beskonačnu familiju $D(1)$-četvorki, $\{a, b, a+b+2r, 4r(a+r)(b+r)\}$.

Međutim, ne postoje $D(n)$-četvorke za svaki cijeli broj n, primjer su svi n-ovi takvi da je $n \equiv 2 \pmod 4$, što su nezavisno jedni od drugih 1985. dokazali Brown [4], Gupta i Singh [36] te Mohanty i Ramasamy [51]. Za većinu preostalih n-ova odgovor je 1993. dao Dujella [11] koji je dokazao ako $n \not\equiv 2 \pmod 4$ i $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, onda postoji barem jedna $D(n)$-četvorka. Što se petorki tiče, najvažnija slutnja jest da ne postoji $D(1)$-petorka. Ono što sigurno danas znamo jest da ih ima najviše konačno mnogo i to je 2004. dokazao također Dujella [22]. S druge strane, postoje $D(256)$-petorka i $D(-255)$-petorka [12, 14]. $D(2985984)$-šestorku pronašao je Gibbs 1999. [35]. Možemo se pitati postoji li neki općeniti rezultat za m i n, a odgovor je potvrdan. Ako definiramo

$$M_n = \sup\{|S| : S \text{ ima svojstvo } D(n)\},$$

onda vrijedi [20, 21]

$$\begin{aligned} M_n &\leq 31, && \text{za } |n| \leq 400, \\ M_n &\leq 15.476 \log |n|, && \text{za } |n| > 400. \end{aligned}$$

U ovom poglavlju posebno će nas zanimati $D(4)$-slučaj pa slijedi pregled najvažnijih rezultata za taj slučaj. Mohanty i Ramasamy [52] su prvi dokazali da se $D(4)$-četvorka $\{1, 5, 12, 96\}$ ne može proširiti na $D(4)$-petorku. Kedlaya [38] je kasnije dokazao da ako je $\{1, 5, 12, d\}$ $D(4)$-četvorka, tada d mora biti 96. Dujella i Ramasamy [25] generalizirali su taj rezultat na parametarsku familiju $D(4)$-četvorki $\{F_{2k}, 5F_{2k}, 4F_{2k+2}, 4L_{2k}F_{4k+2}\}$ koje uključuju Fibonaccijeve i Lucasove brojeve. Ostale generalizacije na dvoparametarske familije $D(4)$-trojki mogu se pronaći u [33]. Budući da je Dujella [22] dokazao da ne postoji $D(1)$-šestorka i da postoji samo konačno mnogo $D(1)$-petorki, ti rezultati direktno impliciraju da ne postoji $D(4)$-osmorka i da postoji samo konačno mnogo $D(4)$-sedmorki. Ove rezultate bitno je popravio Filipin [30, 31] koji je dokazao da ne postoji $D(4)$-šestorka i da postoji samo konačno mnogo $D(4)$-petorki.

Neka je $\{a, b, c\}$ $D(n^2)$-trojka, tj. trojka za koju postoje nenegativni cijeli brojevi r, s, t tako da vrijedi

$$ab + n^2 = r^2, \quad bc + n^2 = s^2, \quad ac + n^2 = t^2. \tag{1.1}$$

Kako bismo proširili ovu trojku do četvorke, potrebno je riješiti sustav jednadžbi

$$ax + n^2 = \square, \quad bx + n^2 = \square, \quad cx + n^2 = \square, \tag{1.2}$$

gdje smo s $\square$ označili kvadrat, i tu oznaku ćemo nadalje upotrebljavati za kvadrat racionalnog broja. Međusobnim množenjem svih jednadžbi sustava (1.2), prirodno mu pridružimo

eliptičku krivulju

$$E : y^2 = (ax + n^2)(bx + n^2)(cx + n^2). \tag{1.3}$$

Za krivulju E kažemo da je inducirana, odnosno generirana $D(n^2)$-trojkom $\{a, b, c\}$. Jasno je da svako rješenje sustava (1.2) inducira cjelobrojnu točku na eliptičkoj krivulji E, a uz određene uvjete povezane s rangom i torzijskom grupom (za $D(1)$-slučaj vidi Propoziciju 2.1) vrijedi i obrat ove tvrdnje. Dakle, kako bismo riješili problem proširenja $D(n^2)$-trojke do četvorke (koji je ekvivalentan problemu proširenja racionalne Diofantove trojke do četvorke) od velike koristi nam je utvrditi torzijsku grupu i rang od (1.3).

Na E postoje 3 racionalne točke reda 2:

$$A = \left(-\frac{n^2}{a},\ 0\right),\ B = \left(-\frac{n^2}{b},\ 0\right),\ C = \left(-\frac{n^2}{c},\ 0\right),$$

te također očite racionalne točke

$$P = \left(0,\ n^3\right),\ S = \left(\frac{n^4}{abc},\ n^3\frac{rst}{abc}\right).$$

Nije očito, ali je lako provjeriti da je $S \in 2E(\mathbb{Q})$. Naime, $S = 2R$, gdje je

$$R = \left(n^2\frac{rs + rt + st + n^2}{abc}, n^3\frac{(r + s)(r + t)(s + t)}{abc}\right).$$

Transformacija koordinata

$$x \mapsto \frac{x}{abc},\ y \mapsto \frac{y}{abc},$$

primijenjena na krivulju E vodi na eliptičku krivulju

$$E' : y^2 = (x + n^2bc)(x + n^2ac)(x + n^2ab). \tag{1.4}$$

Kao što smo definirali E', tako uz pomoć navedene transformacije i točaka A, B, C, P, R, S na E možemo definirati i analogne točke A', B', C', P', R', S' na E' koje ćemo nadalje promatrati:

$$A' = \left(-n^2bc,\ 0\right),\ B' = \left(-n^2ac,\ 0\right),\ C' = \left(-n^2ab,\ 0\right), \tag{1.5}$$

$$\begin{aligned} P' &= \left(0,\ n^3abc\right),\ S' = \left(n^4,\ n^3rst\right), \\ R' &= \left(n^2(rs{+}rt + st + n^2),\ n^3(r + s)(r + t)(s + t)\right). \end{aligned} \tag{1.6}$$

Spomenimo i da se, zapisom E' u dugom Weierstrassovom obliku, dobivaju koeficijenti $a_1 = 0,\ \ a_2 = n^2(ab + ac + bc),\ \ a_3 = 0,\ a_4 = n^4abc(a + b + c)$ \ i $a_6 = n^6abc$. Njihovim

uvrštavanjem u formulu za diskriminantu

$$D = 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2$$

uz

$$b_2 = 4a_2,\ b_4 = 2a_4,\ b_6 = 4a_6,\ b_8 = 4a_2a_6 - a_4^2, \tag{1.7}$$

dobiva se

$$D = 288a_2a_4a_6 - 16a_2^2(4a_2a_6 - a_4^2) - 64a_4^3 - 432a_6^2,$$

što daljnjim raspisivanjem daje konačnu formulu

$$D = 16n^{12}a^2b^2c^2(a-b)^2(b-c)^2(a-c)^2.$$

Iz definicije Diofantove trojke znamo da a, b, c moraju svi biti međusobno različiti i različiti od nule, iz čega slijedi da diskriminanta induciranih eliptičkih krivulja nikad nije nula, odnosno takve krivulje nisu singularne.

1.2 Torzijska grupa i rang od E

Znamo da je $a \neq b \neq c \neq a$, pa stoga bez smanjenja općenitosti možemo pretpostaviti da je $a < b < c$. Osim $a < b < c$, pretpostavit ćemo nadalje u ovom poglavlju da su a, b, c pozitivni cijeli brojevi. Iduća dva rezultata bave se pitanjem torzijske grupe krivulja dobivenih na ovaj način.

Lema 1.5. *$A', B' \notin 2E'(\mathbb{Q})$.*

Dokaz. Ako je $A' \in 2E'(\mathbb{Q})$ tada Propozicija 1.3 povlači da je $c(a-b)$ kvadrat. Međutim, vrijedi $c(a-b) < 0$, pa to nije moguće. Slično, $B' \notin 2E'(\mathbb{Q})$. □

Teorem 1.6. *$E'(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ uz $k = 1, 2, 3$ ili 4.*

Dokaz. Prema Mazurovom teoremu [47] koji karakterizira sve moguće torzijske grupe eliptičkih krivulja nad $\mathbb{Q}$, i zbog činjenice da E' ima tri točke reda 2, jedine mogućnosti za $E'(\mathbb{Q})_{tors}$ su $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ uz $k = 1, 2, 3, 4$. □

Napomena 1.1. U određenim slučajevima ($n = 1, n = 2$, vidi Lemu 1.10) dokazat ćemo i da je $C' \notin 2E'(\mathbb{Q})$ što reducira mogućnosti za $E'(\mathbb{Q})_{tors}$ na $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Sljedeći rezultati donose uvjete pod kojima je rang ovakvih krivulja pozitivan.

Teorem 1.7. *Ako je $\gcd(n, t) = 1$, onda je $\operatorname{rank}(E(\mathbb{Q})) \geq 1$.*

Dokaz. Dovoljno je dokazati da je točka S' na $E'(\mathbb{Q})$ beskonačnog reda. Pretpostavimo suprotno, tj. da je S' konačnog reda. Tada i $S' + A'$ mora biti konačnog reda pa po Lutz-Nagellovom teoremu koordinate od $S' + A'$ moraju biti cijeli brojevi. Prva koordinata od

$S' + A'$ je

$$\left(n\frac{rs}{t}\right)^2 - n^4 + bcn^2.$$

Ako je ovaj broj cijeli, onda je i

$$\begin{aligned} n^2\frac{r^2s^2}{t^2} &= n^2\frac{a^2bc + n^2ab + n^2ac + n^4}{bc + n^2} \\ &= n^2\left(a^2 + \frac{n^2ab + n^2ac + n^4 - n^2a^2}{bc + n^2}\right) \\ &= n^2\left(a^2 + n^2\frac{ab + ac + n^2 - a^2}{bc + n^2}\right) \end{aligned}$$

također cijeli broj, pa iz toga i činjenice da je $\gcd(n, t) = 1$ slijedi da je $ab+ac+n^2-a^2 \geq bc + n^2$, ali to povlači $(b - a)(c - a) \leq 0$, što je kontradikcija. □

Teorem 1.8. *Ako su ispunjena oba uvjeta:*

$$\begin{aligned} &1)\ 3n^8 + 4n^6(ab + ac + bc) + 6n^4abc(a + b + c) + 12n^2(abc)^2 \\ &\qquad - (abc)^2(a^2 + b^2 + c^2 - 2ab - 2ac - 2bc) \neq 0 \\ &2)\ r \neq \sqrt[4]{ab(c - a)(c - b)} \end{aligned}$$

onda je $\operatorname{rank}(E(\mathbb{Q})) \geq 1$.

Dokaz. Uvjerimo se da su uvjeti navedeni u teoremu zapravo uvjeti uz koje je točka S' na $E'(\mathbb{Q})$ beskonačnog reda. Ako je S' konačnog reda, tada činjenica $S' = 2R'$ i Teorem 1.6 povlače da je S' reda 3 ili 4. S' će biti reda 3 ako i samo ako $x(2S') = x(-S') = x(S')$ te $y(2S') = y(-S')$, a reda 4 ako i samo ako $C' = 2S'$ što je ekvivalentno s $x(2S') = x(C')$ i $y(2S') = y(C') = 0$. Naime, točke reda 2 su A', B' i C', a iz Leme 1.5 slijedi da $A' \neq 2S'$ i $B' \neq 2S'$.

Slučaj $3S' = 0$:
Iz formule za zbrajanje točaka na eliptičkoj krivulji u (dugoj) Weierstrassovoj formi slijedi:

$$x(2S') = \lambda^2 + a_1\lambda - a_2 - 2x(S'),$$

pri čemu je

$$a_1 = a_3 = 0,$$

$$a_2 = n^2(ab + ac + bc),$$

$$a_4 = n^4abc(a + b + c),$$

$$\lambda = \frac{3x(S')^2 + 2a_2x(S') + a_4 - a_1y(S')}{2y(S') + a_1x(S') + a_3} = \frac{3n^5 + 2n^3(ab + ac + bc) + nabc(a + b + c)}{2rst}.$$

Možemo pretpostaviti $rst \neq 0$, jer je inače $2S' = 0$. Uvrštavanjem svega, uvjet $x(S') = x(2S')$ implicira:

$$\begin{aligned} &3n^4 + n^2(ab+ac+bc) \\ &= \frac{9n^{10} + 4n^6(ab+ac+bc)^2 + (nabc(a+b+c))^2 + 12n^8(ab+ac+bc)}{4r^2s^2t^2} \\ &\quad + \frac{6n^6abc(a+b+c) + 4n^4abc(ab+ac+bc)(a+b+c)}{4r^2s^2t^2} \end{aligned}$$

odakle dobijemo

$$\begin{aligned} &4\left((abc)^2 + n^2abc(a+b+c) + n^4(ab+ac+bc) + n^6\right)(3n^2+ab+ac+bc) \\ &= 9n^8 + 12n^6(ab+ac+bc) + n^4\left(6abc(a+b+c) + 4(ab+ac+bc)^2\right) \\ &\quad + 4n^2abc(ab+ac+bc)(a+b+c) + (abc(a+b+c))^2 \end{aligned}$$

a to je ekvivalentno s

$$\begin{aligned} &3n^8 + 4n^6(ab+ac+bc) + 6n^4abc(a+b+c) + 12n^2(abc)^2 \\ &\quad - (abc)^2(a^2+b^2+c^2-2ab-2ac-2bc) = 0 \end{aligned}$$

Slučaj $4S' = 0$:
Koristeći iste formule kao u prethodnom slučaju, uvjet $x(C') = x(2S')$ implicira:

$$\begin{aligned} &2n^4 + n^2(bc+ac) \\ &= \frac{9n^{10} + 4n^6(ab+ac+bc)^2 + (nabc(a+b+c))^2 + 12n^8(ab+ac+bc)}{4r^2s^2t^2} \\ &\quad + \frac{6n^6abc(a+b+c) + 4n^4abc(ab+ac+bc)(a+b+c)}{4r^2s^2t^2} \end{aligned}$$

iz čega slijedi

$$n^8 + 4n^6ab + 4n^4a^2b^2 + 2n^4abc(a+b-c) + 4n^2a^2b^2c(a+b-c) + (abc(c-a-b))^2 = 0 \Leftrightarrow$$

$$\left(n^2(n^2+2ab) - abc(c-a-b)\right)^2 = 0 \Leftrightarrow$$

$$n^2(n^2+2ab) = abc(c-a-b) \Leftrightarrow$$

$$(n^2+ab)^2 = ab\left(c(c-a-b)+ab\right) \Leftrightarrow$$

$$r = \sqrt[4]{ab(c(c-a-b)+ab)} = \sqrt[4]{ab(c-a)(c-b)}.$$

□

Napomena 1.2. Iako ih nije jednostavno pronaći, ipak postoje primjeri eliptičkih krivulja

dobivenih iz $D(n^2)$-trojki za koje uvjeti prethodnog teorema nisu ispunjeni, tako da ne vrijedi da je S' beskonačnog reda za sve eliptičke krivulje E' dobivene na ovaj način. Naime,

$$\{120954166577466779013665 13, 602151813375338421905 13,$$
$$468880296070263877341488\}$$

je $D(769323827663466408638916^2)$-trojka koja inducira eliptičku krivulju za koju je $3S' = 0$. Za nju smo uspjeli dobiti da je donja ograda za rang jednaka dva, a torzijska grupa je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Slično,

$$\{387124931772901992980738 3, 10186205699920341673214740 8,$$
$$217448139952121636379025175\}$$

je $D(52208405404435206419201940^2)$-trojka koja inducira krivulju za koju je $4S' = 0$. Ovdje je torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, a za rang smo programom **mwrank**[7] dobili ograde $0 \leq \text{rang} \leq 2$. Iako smo velik broj izračuna u ovoj disertaciji dobili programskim paketom PARI/GP [59], napomenimo da za posljednja dva primjera nismo mogli izračunati torzijsku grupu zbog nedovoljne preciznosti računanja. Stoga je u ovim slučajevima korišten programski paket Sage [63] koji je uspješno odradio tu zadaću.

Napomena 1.3. Pozitivni rang možemo dobiti promatranjem i drugih racionalnih točaka na E', no za S' imamo najmanji broj slučajeva te zgodne formule. Primjerice, da bi P' bila beskonačnog reda, ona ne smije biti ni reda 3, ni reda 4, ni reda 6, niti reda 8. Spomenimo da jednostavnije formule u ovom slučaju dobijemo za uvjet $3P' = 0$ jer iz $X(2P) = X(-P) = X(P)$ te $X(2P) = \dfrac{n^2}{4}(a+b+c)^2 - n^2(ab+ac+bc)$ imamo

$$c = (\sqrt{a} + \sqrt{b})^2.$$

I ovdje smo pronašli primjer krivulje za koju ta jednakost vrijedi, to je krivulja dobivena iz $D(466882678248651357^2)$-trojke

$$\{87079110228523204, 4450194713526565444,$$
$$5782294299084825600\}.$$

Ta krivulja ima torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, a za rang smo dobili ograde $1 \leq \text{rang} \leq 4$. Spomenimo i da je i u posljednjem primjeru iz Napomene 1.2 točka P' također konačnog reda.

Napomena 1.4. Ako dopustimo miješane predznake, onda nije toliko teško pronaći primjere krivulja u kojima je rang jednak nuli. Pronašli smo $D(n^2)$-trojke koje induciraju

eliptičke krivulje za koje je rang nula, a torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$: $D(144)$-trojke $\{-1, 63, 80\}$ i $\{-80, -63, 1\}$ te $D(784)$-trojke $\{-15, 48, 49\}$ i $\{-49, -48, 15\}$. U svim navedenim slučajevima je točka S' reda 3. Postoji također i $D(144)$-trojka $\{-9, 7, 16\}$ iz koje dobivamo eliptičku krivulju ranga nula i torzijske grupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. U svim spomenutim primjerima rang je određen korištenjem programa **mwrank**[7].

1.3 Torzijska grupa u $D(4)$ i $D(1)$-slučajevima

Neka je $\{a, b, c\}$ $D(4)$-trojka. Tada postoje nenegativni cijeli brojevi r, s, t takvi da je

$$ab + 4 = r^2,\ ac + 4 = s^2,\ bc + 4 = t^2. \tag{1.8}$$

Na isti način kao u prethodnom poglavlju (vidi formulu (1.4)), dolazimo do krivulje E':

$$E' : y^2 = (x + 4bc)(x + 4ac)(x + 4ab). \tag{1.9}$$

Teorem 1.6 daje nam moguće oblike torzijskih grupa ovih krivulja. Međutim, pokazalo se da se u $D(4)$-slučaju mogu dobiti i jači rezultati nego u općenitom, $D(n^2)$-slučaju. Dodatna motivacija za proučavanje torzijskih grupa eliptičkih krivulja dobivenih iz $D(4)$-trojki je nedostatak pronađen u dokazu od [**19, Lemma 1**] koji se bavi torzijskim grupama eliptičkih krivulja dobivenih iz $D(1)$-trojki. Naime, ako je $\{a', b', c'\}$ $D(1)$-trojka, onda je $\{2a', 2b', 2c'\}$ $D(4)$-trojka. Stoga, dokaz Leme 1.10 u ovom radu ujedno predstavlja i ispravan dokaz od [**19, Lemma 1**].

Iz definicija (1.5) i (1.6) dobivamo uvrštavanjem $n^2 = 4$ da na E' postoje tri racionalne točke reda 2:

$$A' = (-4bc,\ 0)\,,\ B' = (-4ac,\ 0)\,,\ C' = (-4ab,\ 0)\,,$$

te dodatne racionalne točke

$$P' = (0,\ 8abc)\,,\ R' = (4rs + 4rt + 4st + 16,\ 8(r + s)(r + t)(s + t))\,,\ S' = (16,\ 8rst)\,,$$

pri čemu vrijedi $S' = 2R'$.

U ovom odjeljku prvo ćemo promotriti jedan specijalni slučaj nakon čega bez smanjenja općenitosti možemo pretpostaviti da su a, b, c pozitivni cijeli brojevi takvi da je $a < b < c$. Budući da $\{-a, -b, -c\}$ inducira istu krivulju kao i $\{a, b, c\}$, problem se može pojaviti u slučaju miješanih predznaka. Lako se vidi da je jedina takva moguća $D(4)$-trojka $\{-1, 3, 4\}$ (kao i njoj ekvivalentna $\{-4, -3, 1\}$). Eliptička krivulja pridružena toj $D(4)$-trojci ima rang 0 i torzijsku grupu izomorfnu s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. U tom specijalnom slučaju je $B' \in 2E'(\mathbb{Q})$, odnosno preciznije $B' = 2P'$, pa je točka P' reda 4. Primijetimo da je u tom slučaju točka R' također reda 4, budući da je $R' = P' + A'$, i stoga $2R' = 2P'$.

Dakle, odsad nadalje možemo pretpostaviti da su a, b, c pozitivni cijeli brojevi takvi da $a < b < c$.

Lema 1.9. *Ako je* $\{a, b, c\}$ $D(4)$*-trojka, tada* $c = a + b + 2r$ *ili* $c > ab + a + b + 1 > ab$.

Dokaz. Prema [**20, Lemma 3**], postoji cijeli broj

$$e = 4(a + b + c) + 2(abc - rst) \tag{1.10}$$

i nenegativni cijeli brojevi x, y, z takvi da

$$ae + 16 = x^2, \tag{1.11}$$
$$be + 16 = y^2, \tag{1.12}$$
$$ce + 16 = z^2 \tag{1.13}$$

i $c = a + b + \frac{e}{4} + \frac{1}{8}(abe + rxy)$. Iz (1.13), slijedi da $e \geq 0$ (slučaj $e = -1$ implicira $c \leq 16$, ali jedine takve $D(4)$-trojke $\{1, 5, 12\}$ i $\{3, 4, 15\}$ ne zadovoljavaju (1.11) i (1.12)). Za $e = 0$ dobivamo $c = a + b + 2r$, dok za $e \geq 1$ imamo $c > \frac{1}{4}abe + a + b + \frac{e}{4}$. Promatranjem kongruencija modulo 8, lako možemo dokazati da su u svakoj $D(4)$-trojci $\{a, b, c\}$ najviše dva od cijelih brojeva a, b, c neparna (u suprotnom barem jedan od r^2, s^2 i t^2 ne daje ostatak 1 pri dijeljenju s 8), što povlači da je $abc - rst$ paran. Na temelju toga i (1.10) zaključujemo da $e \equiv 0 \pmod 4$. Slijedi $e \geq 4$ i konačno $c > ab + a + b + 1$. □

Napomena 1.5. Filipin (vidi [**32, Lemma 4**]) je promatranjem mogućih vrijednosti od c dokazao da je ili $c = a + b + 2r$ ili $c > \frac{1}{4}abe$. Lemu 1.9 možemo u tom kontekstu smatrati kao malo unaprijeđenje tog rezultata.

Napomena 1.6. Lema 1.9 povlači $c \geq a+b+2r$. Doista, nejednakost $ab+a+b+1 \geq a+b+2r$ je ekvivalentna s $(r-3)(r+1) \geq 0$, a to je zadovoljeno za sve $D(4)$-trojke s pozitivnim elementima.

Napomena 1.7. Lema 1.9 je oštra u smislu da nejednakost $c > ab$ ne može biti zamijenjena s $c > (1 + \varepsilon)ab$ za bilo koji fiksni $\varepsilon > 0$. Zaista, za cijeli broj $k \geq 3$, ako postavimo $a = k^2 - 4$, $b = k^2 + 2k - 3$, $c = k^4 + 2k^3 - 3k^2 - 4k$, tada je $\{a, b, c\}$ $D(4)$-trojka i $\lim_{k\to\infty} \frac{c}{ab} = 1$.

U idućoj lemi pokazat ćemo da E' ne može imati točku reda 4. Slijedimo strategiju iz dokaza analognog rezultata za $D(1)$-trojke [**19, Lemma 1**]. Valja napomenuti da smo u tom dokazu primijetili ozbiljni nedostatak. Naime, [**19, formula (7)**] bi trebala glasiti $(\beta^2 - 1)^2 = b(4c\beta^2 - a^2b - 2a(1 + \beta^2))$, umjesto $(\beta^2 - 1)^2 = b(4c - a^2b - 2a(1 + \beta^2))$, pa argumenti koji slijede nakon toga nisu točni u slučaju $\beta \neq 1$. Ovdje ćemo dokazati

općenitiji rezultat, ali ćemo istodobno (uzevši da su a, b, c parni) ispraviti i navedeni nedostatak koji smo pronašli u dokazu od [**19, Lemma 1**].

Lema 1.10. $A', B', C' \notin 2E'(\mathbb{Q})$.

Dokaz. Iz Leme 1.5 već znamo da vrijedi $A' \notin 2E'(\mathbb{Q})$, te $B' \notin 2E'(\mathbb{Q})$. Ako $C' \in 2E'(\mathbb{Q})$, tada je iz Propozicije 1.3

$$a(c-b) = X^2, \tag{1.14}$$
$$b(c-a) = Y^2, \tag{1.15}$$

za neke cijele brojeve X i Y.

Ako je $\{a, b, c\}$ $D(4)$-trojka gdje $a < b < c$, tada $c = a + b + 2r$ ili $c > ab + a + b + 1$ prema Lemi 1.9.

Pretpostavimo prvo da je $c = a + b + 2r$. Iz (1.14) i (1.15), dobivamo da je $a = kx^2$, $c - b = ky^2$, $b = lz^2$, $c - a = lu^2$, gdje su k, l, x, y, z, u prirodni brojevi. Imamo $c = kx^2 + lu^2 = ky^2 + lz^2$, a iz $c = a + b + 2r$ dobivamo

$$2r = k(y^2 - x^2) = l(u^2 - z^2). \tag{1.16}$$

Kvadriranjem (1.16), dobivamo

$$4r^2 = 16 + 4ab = 16 + 4klx^2z^2 = k^2(y^2 - x^2)^2 = l^2(u^2 - z^2)^2,$$

iz čega slijedi da je $k \in \{1, 2, 4\}$ te $l \in \{1, 2, 4\}$. S obzirom da kl nije potpun kvadrat (inače bi bilo $(2r)^2 = 16 + (2xz\sqrt{kl})^2$, a to povlači $2r = 5$), možemo uzeti bez smanjenja općenitosti $k = 1$, $l = 2$ ili $k = 2$, $l = 4$. Za $k = 1$, $l = 2$, imamo $4r^2 = 16 + 8x^2z^2$, što implicira $r^2 = 4 + 2x^2z^2$, iz čega zaključujemo da je r paran i da je xz paran. Dakle, $r^2 \equiv 4 \pmod 8$ i $r \equiv 2 \pmod 4$. Ali iz $2r = 2(u^2 - z^2)$ zaključujemo da je $u^2 - z^2 \equiv 2 \pmod 4$, a to je nemoguće. Ako je $k = 2$, $l = 4$, tada je $4r^2 = 16 + 32x^2z^2$, što povlači $r^2 = 4 + 8x^2z^2$, pa opet dobivamo $r^2 \equiv 4 \pmod 8$ i $r \equiv 2 \pmod 4$. Međutim, iz $2r = 2(y^2 - x^2)$ zaključujemo $y^2 - x^2 \equiv 2 \pmod 4$, a to je nemoguće.

Pretpostavimo sada $c > ab + a + b + 1 > ab$.

Zapišimo uvjete (1.14) i (1.15) u obliku

$$ac - ab = s^2 - r^2 = (s - \gamma)^2, \tag{1.17}$$
$$bc - ab = t^2 - r^2 = (t - \beta)^2, \tag{1.18}$$

gdje $0 < \gamma < s$, $0 < \beta < t$. Iz toga imamo

$$r^2 = 2s\gamma - \gamma^2 = 2t\beta - \beta^2. \tag{1.19}$$

Iz (1.19) dobivamo

$$4(bc+4)\beta^2 = (ab+4+\beta^2)^2,$$

iz čega je

$$(\beta^2-4)^2 = b(4c\beta^2 - a^2b - 2a(4+\beta^2)). \tag{1.20}$$

Iz (1.20) zaključujemo da je ili $\beta = 1$ ili $\beta = 2$ ili $\beta^2 \geq \sqrt{b}+4$.

Ako je $\beta = 1$, tada je

$$b(4c - a^2b - 10a) = 9, \tag{1.21}$$

što povlači $b \mid 9$, ali to je moguće samo za $b = 9$ (ne postoje $D(4)$-trojke s $b < 4$). To nam daje $a = 5$, ali (1.21) tada daje $c = 69$, a $\{5, 9, 69\}$ nije $D(4)$-trojka.

Ako je $\beta = 2$, tada iz (1.20) dobivamo da je

$$c = \frac{a^2b + 16a}{16}\,. \tag{1.22}$$

Sada je

$$s^2 = ac + 4 = \frac{1}{16}(a^3b + 16a^2 + 64) = \frac{1}{16}(a^2r^2 + 12a^2 + 64).$$

Dakle, $s^2 > \left(\frac{ar}{4}\right)^2$ i $s^2 < \left(\frac{ar+8}{4}\right)^2$. Prema tome, moramo promatrati nekoliko slučajeva:

1. $s^2 = \left(\frac{ar+n}{4}\right)^2$, gdje je n neparan. To je ekvivalentno s

$$2a(rn - 6a) = 64 - n^2. \tag{1.23}$$

   Lijeva strana od (1.23) je parna, a desna je neparna što je kontradikcija.

2. $s^2 = \left(\frac{ar+2}{4}\right)^2$, ili ekvivalentno $a(r-3a) = 15$. Slučaj $a \leq 3$ zajedno s (1.22) implicira $c < b$. Slučaj $a = 5$ daje trojku $\{5, 64, 105\}$ koja ne zadovoljava $c > ab$ (c je jednak $a+b+2r$), i $a = 15$ dovodi do jednadžbe $15b + 4 = 46^2$ koja nema cjelobrojnih rješenja.

3. $s^2 = \left(\frac{ar+4}{4}\right)^2$, ili ekvivalentno $a(2r-3a) = 12$. Zaključujemo da a mora biti paran pa dobivamo trojke: $\{2, 16, 6\}$ (uz $c < b$) i $\{6, 16, 42\}$ (uz $c = a+b+2r$), pa možemo eliminirati ovaj slučaj.

4. $s^2 = \left(\frac{ar+6}{4}\right)^2$ je ekvivalentno s $3a(r-a) = 7$, što je očito nemoguće.

Prema tome, možemo pretpostaviti da je $\beta^2 \geq \sqrt{b}+4$, što povlači

$$\beta > \max\{\sqrt[4]{b}, 2\} \tag{1.24}$$

Vrijedi

$$ab = t^2 - (t-\beta)^2 - 4, \tag{1.25}$$

a funkcija $f(x) = t^2 - (t-x)^2$ je rastuća za $0 < x < t$. Znamo da je $0 < \sqrt[4]{b} < \beta < t$, pa stoga imamo

$$ab = t^2 - (t-\beta)^2 - 4 > 2t\sqrt[4]{b} - \sqrt{b} - 4 > 2\sqrt{bc}\sqrt[4]{b} - \sqrt{b} - 4,$$

što povlači $ab > \sqrt{bc}\sqrt[4]{b}$, zbog $\sqrt{b}(\sqrt{c}\sqrt[4]{b} - 1) > 4$ (budući da $b \geq 4$ i $c \geq 12$, što slijedi iz činjenice da su $\{3, 4, 15\}$ i $\{1, 5, 12\}$ $D(4)$-trojke s najmanjim vrijednostima b i c respektivno). Ovo nadalje daje

$$c < a^2\sqrt{b}. \tag{1.26}$$

Koristit ćemo (1.10) kako bismo definirali cijeli broj d_- kao

$$d_- = \frac{e}{4} = a + b + c + \frac{abc - rst}{2}$$

Slijedi $d_- \neq 0$ (zbog $c \neq a + b + 2r$) i $\{a, b, c, d_-\}$ je $D(4)$-četvorka. Posebice,

$$\begin{aligned} ad_- + 4 &= a^2 + ab + ac + \frac{a^2bc - arst}{2} + 4 \\ &= \frac{1}{4}\left(4a^2 + 4ab + 4ac + 2a^2bc - 2arst + 16\right) \\ &= \frac{1}{4}\left((ab+4)(ac+4) - 2arst + a^2(bc+4)\right) \\ &= \left(\frac{rs - at}{2}\right)^2. \end{aligned} \tag{1.27}$$

Povrh toga,

$$c = a + b + d_- + \frac{1}{2}\Big(abd_- + \sqrt{(ab+4)(ad_-+4)(bd_-+4)}\Big) > abd_- \tag{1.28}$$

(vidi dokaz Leme 1.9). Uspoređujući ovo s (1.26), dobivamo

$$d_- < \frac{a}{\sqrt{b}}. \tag{1.29}$$

Dakle, imamo $d_- < a < b$ iz čega slijedi da je b najveći element u $D(4)$-trojci $\{a, b, d_-\}$. Prema tome, iz Napomene 1.6, $b \geq a + d_- + 2\sqrt{ad_- + 4}$, ili ekvivalentno

$$d_- \leq a + b - 2r. \tag{1.30}$$

Naime,

$$b \geq a + d_- + 2\sqrt{ad_- + 4} \Leftrightarrow$$

$$(b-a-d_-)^2 \geq 4ad_- + 16 \Leftrightarrow$$
$$(b+a-d_-)^2 \geq 4ab + 16 \Leftrightarrow$$
$$b+a-d_- \geq 2r.$$

Definirajmo također

$$c' = a+b+d_- + \frac{1}{2}\Big(abd_- - \sqrt{(ab+4)(ad_-+4)(bd_-+4)}\Big).$$

Zbog (1.30) imamo

$$\begin{aligned} cc' &= (a+b+d_- + \frac{1}{2}abd_-)^2 - \frac{1}{4}(ab+4)(ad_-+4)(bd_-+4) \\ &= (a+b+d_-)^2 - 4ab - 4ad_- - 4bd_- - 16 \\ &= (a+b-d_-)^2 - 4r^2 = (a+b+2r-d_-)(a+b-2r-d_-) \geq 0. \end{aligned}$$

Iz toga slijedi $c' \geq 0$, odnosno $a+b+d_- + \frac{1}{2}abd_- \geq \frac{1}{2}\sqrt{(ab+4)(ad_-+4)(bd_-+4)}$, iz čega zaključujemo

$$c < 2(a+b+d_- + \frac{1}{2}abd_-) < 4b + abd_- < 2abd_- \tag{1.31}$$

(ovdje koristimo nejednakost $ad_- > 4$ koja slijedi iz činjenice da je $\{a, d_-\}$ $D(4)$-par). Označimo $p = \dfrac{rs-at}{2}$. Tada je $p > 0$, te prema (1.27), imamo $ad_- + 4 = p^2$. Kako bismo procijenili veličinu p, također definirajmo $p' = \dfrac{rs+at}{2}$. Vrijedi

$$pp' = \frac{1}{4}(a^2bc + 4ac + 4ab + 16 - a^2bc - 4a^2) = a(b+c-a) + 4,$$

i

$$p = \frac{a(b+c-a)+4}{\frac{rs+at}{2}} < \frac{2a(c+b)}{2at} < \frac{c+b}{\sqrt{bc}} = \frac{\sqrt{c}}{\sqrt{b}} + \frac{\sqrt{b}}{\sqrt{c}}, \tag{1.32}$$

$$p > \frac{2(ac+4)}{2rs} = \frac{s}{r}.$$

Nadalje, imamo

$$\frac{\sqrt{c}}{\sqrt{b}} - \frac{s}{r} = \frac{r\sqrt{c} - s\sqrt{b}}{r\sqrt{b}} = \frac{4c-4b}{r\sqrt{b}(r\sqrt{c}+s\sqrt{b})} < \frac{4c}{2rsb} < \frac{2\sqrt{c}}{ab\sqrt{b}}$$

(jer je $a\sqrt{bc} < rs$, zbog $rs > at > a\sqrt{bc}$), i iz toga

$$p > \frac{\sqrt{c}}{\sqrt{b}} - \frac{2\sqrt{c}}{ab\sqrt{b}}. \tag{1.33}$$

Nejednakost (1.26) implicira $c < \frac{ab^2}{2}$, a to je ekvivalentno s

$$\frac{\sqrt{b}}{\sqrt{c}} > \frac{2\sqrt{c}}{ab\sqrt{b}}$$

što pak daje

$$p > \frac{\sqrt{c}}{\sqrt{b}} - \frac{\sqrt{b}}{\sqrt{c}}. \tag{1.34}$$

Uspoređujući obje ograde za p, dobivamo

$$\left| p - \frac{\sqrt{c}}{\sqrt{b}} \right| < \frac{\sqrt{b}}{\sqrt{c}}. \tag{1.35}$$

Definirajmo sada cijeli broj α kao

$$2d_-\beta = p + \alpha.$$

Pretpostavimo da je $\alpha = 0$. Tada (1.27) povlači $d_-(4\beta^2 d_- - a) = 4$, iz čega $d_- \in \{1, 2, 4\}$. Analiziramo tri slučaja:

1. $d_- = 1$, što povlači $2\beta = p$. Uz ovu pretpostavku, (1.18) daje

$$r^2 + \frac{p^2}{4} = tp, \tag{1.36}$$

dok c zadovoljava nejednakosti

$$ab < ab + a + b + 1 < c < ab + 2a + 2b + 2 < ab + 4b < 2ab \tag{1.37}$$

(vidi Lemu 1.9 i (1.31) s $d_- = 1$). Koristeći (1.32), (1.37) i nejednakost $\frac{b}{4c} < \frac{1}{4a}$ koja je ekvivalentna s $c > ab$, dobivamo da je lijeva strana od (1.36)

$$< ab + 4 + \frac{c^2 + 2bc + b^2}{4bc} < ab + 4 + \frac{a}{4} + 1 + \frac{1}{2} + \frac{1}{4a} < ab + \frac{a}{4} + 6.$$

S druge strane, iz (1.33) i (1.37) dobivamo da je desna strana od (1.36)

$$> \sqrt{bc}\left(\frac{\sqrt{c}}{\sqrt{b}} - \frac{2\sqrt{c}}{ab\sqrt{b}}\right) = c - \frac{2c}{ab} > ab + a + b + 1 - 4 = ab + a + b - 3.$$

Uspoređujući ove dvije ograde za (1.36), dobivamo

$$b + \frac{3}{4}a < 9,$$

ali to je u kontradikciji s $b \geq 12$ (b je najveći element u $D(4)$-trojci $\{d_-, a, b\}$).

Na sličan način rješavamo i preostala dva slučaja.

2. $d_- = 2$, što implicira $4\beta = p$, a to vodi do

$$\frac{b}{2} + \frac{3}{8}a < 8,$$

što je u kontradikciji s $b \geq 16$ ($D(4)$-trojka oblika $\{2, a, b\}$ s najmanjom vrijednosti b je $\{2, 6, 16\}$).

3. $d_- = 4$ je ekvivalentno s $8\beta = p$, što dovodi do

$$\frac{b}{4} + \frac{3}{16}a < 8,$$

ali jedina $D(4)$-trojka oblika $\{4, a, b\}$ s $b < 35$ je $\{4, 8, 24\}$, koja ne zadovoljava (1.29), pa i u ovom slučaju dobivamo kontradikciju.

Dakle, možemo pretpostaviti da je $\alpha \neq 0$. Ocijenit ćemo $2d_-t\beta$ i usporediti s c. Prvo ćemo dokazati

$$\beta^2 < \frac{a^2 b}{c}. \tag{1.38}$$

Naime, budući da je $\beta < t$, te da slučaj $\beta = t - 1$ daje $b(c - a) = 1$, što je nemoguće, zaključujemo da je $t \geq \beta + 2$. To povlači $t\beta \geq \beta^2 + 2\beta$, te $ab - t\beta \geq 2\beta - 4 > 0$ zbog (1.24) i (1.25). Dakle, dobivamo $t\beta < ab$, a ovo očito povlači (1.38).
Stoga,

$$0 < d_-\beta^2 < \frac{d_- a^2 b}{c} < a. \tag{1.39}$$

Iz $2t\beta = r^2 + \beta^2 > ab + 4$, dobivamo $2d_-t\beta > abd_- + 4d_-$. S druge strane, korištenjem (1.38) i (1.39) imamo

$$2d_-t\beta = d_-(r^2 + \beta^2) = d_-(ab + 4 + \beta^2) < abd_- + 4d_- + \frac{d_- a^2 b}{c} < abd_- + 4d_- + a.$$

Uspoređujući ove dvije ograde, slijedi

$$abd_- + 4d_- < 2d_-t\beta < abd_- + 4d_- + a. \tag{1.40}$$

Usporedbom (1.40) s (1.28) i (1.31), zaključujemo da je

$$|2d_-t\beta - c| < 4b. \tag{1.41}$$

Uspoređujući ogradu (1.35) za p s trivijalnom ogradom za α, a to je $|\alpha| \geq 1$, dobivamo

$$\left|2d_-\beta - \frac{\sqrt{c}}{\sqrt{b}}\right| = \left|p + \alpha - \frac{\sqrt{c}}{\sqrt{b}}\right| \geq 1 - \frac{\sqrt{b}}{\sqrt{c}}.$$

Nadalje, primijetimo da je $ad_- > 26$. Naime, jedini $D(4)$-parovi takvi da $ad_- \leq 26$ su

$$\{1,5\},\ \{1,12\},\ \{1,21\},\ \{2,6\},\ \{3,4\},\ \{3,7\}.$$

Iz prva tri para, uvažavajući (1.28) i (1.29), nalazimo trojke

$$\{5,12,96\},\{12,21,320\},\{12,96,1365\},\{21,32,780\},\{21,320,7392\}$$

koje ne zadovoljavaju (1.14) ni (1.15). Iz posljednja tri para ne možemo dobiti $D(4)$-trojku zbog (1.29).
Konačno, dobivamo

$$\begin{aligned}\left|2d_-t\beta - c\right| &= \left|2d_-t\beta - t\frac{\sqrt{c}}{\sqrt{b}} + t\frac{\sqrt{c}}{\sqrt{b}} - c\right| \geq t\left|2d_-\beta - \frac{\sqrt{c}}{\sqrt{b}}\right| - \left|t\frac{\sqrt{c}}{\sqrt{b}} - c\right| \\ &= t\left|2d_-\beta - \frac{\sqrt{c}}{\sqrt{b}}\right| - \left(t\frac{\sqrt{c}}{\sqrt{b}} - c\right) \geq t\left(1 - \frac{\sqrt{b}}{\sqrt{c}}\right) - \left(t\frac{\sqrt{c}}{\sqrt{b}} - c\right) \\ &= t\left(1 - \frac{\sqrt{b}}{\sqrt{c}}\right) - c\left(\sqrt{1+\frac{4}{bc}} - 1\right) > \sqrt{bc} - b - c\left(\sqrt{1+\frac{4}{bc}} - 1\right) \\ &> \sqrt{ab^2d_-} - b - \frac{2}{b} \geq b\Big(\sqrt{ad_-} - 1 - \frac{1}{72}\Big) > 4b\end{aligned}$$

što je u kontradikciji s (1.41). □

Teorem 1.11. *$E'(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Dokaz. Iz Teorema 1.6 znamo da su jedine mogućnosti za $E'(\mathbb{Q})_{tors}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ s $k = 1,2,3,4$. No, Lema 1.10 pokazuje da slučajevi $k = 2,4$ nisu mogući za eliptičku krivulju induciranu s $D(4)$-trojkom s pozitivnim elementima. □

Korolar 1.12. *Neka je $\{a,b,c\}$ $D(1)$-trojka. Tada je torzijska grupa eliptičke krivulje $y^2 = (ax+1)(bx+1)(cx+1)$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Napomena 1.8. Primijetimo da analogon Teorema 1.11 i Korolara 1.12 ne vrijedi za općenite $D(n^2)$-trojke i pripadne inducirane eliptičke krivulje

$$y^2 = (ax+n^2)(bx+n^2)(cx+n^2).$$

Primjerice, za $D(9)$-trojku $\{8,54,104\}$ torzijska grupa inducirane eliptičke krivulje je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Također, postoje primjeri s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, npr. za $D(52208405404435206419201940^2)$-trojku

$$\{387124931772901992980738 3, 10186205699920341673214740 8,$$
$$21744813995212163637902517 5\}$$

(postoje puno jednostavniji primjeri s miješanim predznacima, vidi npr. [**23**]).

Spomenimo također da ne znamo za nijedan primjer $D(1)$ ili $D(4)$-trojke koja inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Doista, poznato je da se ova torzijska grupa ne može pojaviti za određene familije $D(1)$-trojki (vidi [**16**, **18**, **19**, **54**]). Opet, postoje primjeri takvih krivulja za općenite $D(n^2)$-trojke. Primjerice, $D(294^2)$-trojka $\{32, 539, 1215\}$ inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Poglavlje 2

Familije Diofantovih trojki i inducirane eliptičke krivulje

2.1 Uvod

Dok smo u prethodnom poglavlju proučavali općenite $D(n^2)$-trojke i pridružene eliptičke krivulje (s naglaskom na $n = 2$), u ovom ćemo se koncentrirati na Diofantove trojke, tj. $D(1)$-trojke. Posebno će nas zanimati problem proširenja Diofantove trojke do četvorke za određene familije Diofantovih trojki te rezultati o Mordell-Weilovoj grupi induciranih eliptičkih krivulja.

Neka je $\{a, b, c\}$ Diofantova trojka, tj.

$$ab + 1 = r^2, \;\; ac + 1 = s^2, \;\; bc + 1 = t^2, \;\; r, s, t \in \mathbb{N}.$$

Već smo na nekoliko mjesta vidjeli da proširenje trojke $\{a, b, c\}$ do četvorke iziskuje nalaženje rješenja sustava jednadžbi

$$ax + 1 = \square, \;\; bx + 1 = \square, \;\; cx + 1 = \square. \tag{2.1}$$

Sustavu (2.1) pridružimo eliptičku krivulju

$$E : y^2 = (ax + 1)(bx + 1)(cx + 1).$$

E ima 3 očite racionalne točke reda 2:

$$A = \left(-\frac{1}{a}, 0\right), \;\; B = \left(-\frac{1}{b}, 0\right), \;\; C = \left(-\frac{1}{c}, 0\right),$$

te dvije dodatne racionalne točke:

$$P = (0, 1), \;\; S = \left(\frac{1}{abc}, \frac{rst}{abc}\right).$$

Točke P i S su u velikom broju slučajeva nezavisne i beskonačnog reda, što nam odmah

daje da je rank $E(\mathbb{Q}) \geq 2$ u takvim slučajevima.

Jasno je da svako rješenje sustava (2.1) inducira cjelobrojnu točku na eliptičkoj krivulji E. Obrat ove tvrdnje ovisi o Mordell-Weilovoj grupi od E nad $\mathbb{Q}$ i iskazan je u sljedećoj propoziciji:

Propozicija 2.1. ([**19, Proposition 1**],[**67**]) *X-koordinata točke $T \in E(\mathbb{Q})$ zadovoljava sustav (2.1) ako i samo ako je $T - P \in 2E(\mathbb{Q})$.*

Jasno je da, ako je P beskonačnog reda, onda i sustav (2.1) ima beskonačno mnogo rješenja, to su x-koordinate od $3P$, $5P$, $7P$... U prethodnom poglavlju vidjeli smo da postoji točka R takva da je $S = 2R$. U kontekstu Propozicije 2.1 to odmah daje da su $x(P + S)$ i $x(P - S)$ rješenja od (2.1). Ako definiramo brojeve d_- i d_+ kao

$$d_+ = a + b + c + 2abc + 2rst,$$

$$d_- = a + b + c + 2abc - 2rst,$$

može se pokazati da je $x(P+S) = d_-$ i $x(P-S) = d_+$. Inače, čuvena slutnja o nepostojanju Diofantove petorke u jačem obliku iskazuje se upravo preko d_- i d_+:

Slutnja 2.2. *Ako je $\{a, b, c, d\}$ Diofantova četvorka, onda je $d = d_-$ ili $d = d_+$.*

Istinitost prethodne slutnje povlači nepostojanje Diofantove petorke jer uz pretpostavku $a < b < c$ lako možemo dobiti $d_+d_- < c^2$, odnosno $d_- < c$. Slutnja je zasad provjerena za neke specifične Diofantove trojke [**2, 38, 64**], te za određene parametarske familije Diofantovih trojki [**13, 15**]. Dujella i Pethő su u [**17**] dokazali da se par $\{1, 3\}$ ne može proširiti do Diofantove petorke.

Dakle, veza između točaka na eliptičkoj krivulji i rješenja sustava (2.1) ovisi o Mordell-Weilovoj grupi od E nad $\mathbb{Q}$, odnosno o redovima određenih točaka. Stoga, kako bismo našli uvjete za proširenje Diofantovih trojki do četvorki, u ovom poglavlju promatrat ćemo rang i torzijsku grupu od eliptičke krivulje E inducirane s određenim familijama Diofantovih trojki. Osim što se eliptičke krivulje mogu koristiti za rješavanje problema proširenja Diofantovih trojki u četvorke (isti slučaj je i s proširivanjem četvorki u petorke, vidi [**19**]), spomenimo i da također postoji važna veza između eliptičkih krivulja i Diofantovih m-torki, ali u suprotnom smjeru. Naime, Diofantove trojke su se pokazale kao koristan alat u konstruiranju familija eliptičkih krivulja velikog ranga. Parametarsku familiju eliptičkih krivulja, induciranu s racionalnim Diofantovim trojkama i s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ te ranga 4 konstruirali su Dujella i Peral [**27**], i to je trenutni rekord za ovu torzijsku grupu.

U uvodu smo definirali za $k \geq 2$ i $l \in \mathbb{N}$, niz $\{c_l(k)\}$ kao:

$$c_l(k) = \frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1} - 2k}{2(k^2-1)}. \tag{2.2}$$

Ovdje ćemo dokazati da su $(k-1)c_l(k)+1$ i $(k+1)c_l(k)+1$ potpuni kvadrati, tj. $\{k-1, k+1, c_l(k)\}$ je Diofantova trojka. Definirajmo za $k \geq 2$ i $l \in \mathbb{N}$ nizove $\{s_l(k)\}$ i $\{t_l(k)\}$ kao:

$$s_l(k)^2 = (k-1)c_l(k)+1, \tag{2.3}$$
$$t_l(k)^2 = (k+1)c_l(k)+1. \tag{2.4}$$

Dokazat ćemo da su $s_l(k)$ i $t_l(k)$ zadani sa sljedećim eksplicitnim formulama:

$$s_l(k) = \frac{(k+\sqrt{k^2-1})^{l+1}(\sqrt{k+1}-\sqrt{k-1})}{2\sqrt{k+1}} + \frac{(k-\sqrt{k^2-1})^{l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k+1}}, \tag{2.5}$$

$$t_l(k) = \frac{(k+\sqrt{k^2-1})^{l+1}(\sqrt{k+1}-\sqrt{k-1})}{2\sqrt{k-1}} - \frac{(k-\sqrt{k^2-1})^{l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k-1}}. \tag{2.6}$$

Naime, iz (2.2) i (2.3) slijedi

$$s_l(k)^2 = \frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1} + 2}{2(k+1)}$$

$$= \left(\frac{(k+\sqrt{k^2-1})^{l+1}(\sqrt{k+1}-\sqrt{k-1}) + (k-\sqrt{k^2-1})^{l+1}(\sqrt{k+1}+\sqrt{k-1})}{2\sqrt{k+1}}\right)^2.$$

Formula (2.6) se dokaže na isti način. Uz eksplicitne formule, lako se može provjeriti da ovi nizovi zadovoljavaju sljedeće rekurzivne relacije:

$$s_l(k) = 2ks_{l-1}(k) - s_{l-2}(k), \tag{2.7}$$
$$t_l(k) = 2kt_{l-1}(k) - t_{l-2}(k). \tag{2.8}$$

Dakle, $s_l(k)$ i $t_l(k)$ su prirodni brojevi za sve $k \geq 2$ i $l \in \mathbb{N}$, što zajedno s (2.3) i (2.4) implicira da je $\{k-1, k+1, c_l(k)\}$ Diofantova trojka.

Prođimo sada detaljnije kroz dosadašnje rezultate o eliptičkim krivuljama dobivenim

na ovaj način. Dujella [16] je bio prvi koji je proučavao parametarsku familiju eliptičkih krivulja induciranih s Diofantovim trojkama $\{k-1, k+1, c_1(k)\}$. Sve cjelobrojne točke na eliptičkim krivuljama asociranim s takvim trojkama su nađene za krivulje ranga 1 i za određene potfamilije krivulja ranga 2 i 3. Dujella i Pethő [18] promatrali su specijalni slučaj $k = 2$, tj. trojke $\{1, 3, c_l(2)\}$, i pronašli su sve cjelobrojne točke u slučaju kad je ili rang odgovarajuće krivulje jednak 2, ili $l \leq 40$. Najman [54] je nastavio s proučavanjem familija krivulja induciranih s $\{k-1, k+1, c_l(k)\}$ i uspješno pronašao sve cjelobrojne točke na familijama induciranima s trojkama $\{k-1, k+1, c_2(k)\}$ i $\{k-1, k+1, c_3(k)\}$ pod pretpostavkom da je rang pripadne krivulje 2, ili $2 \leq k \leq 10000$. Postoje također rezultati o proširivosti Diofantovih trojki $\{k-1, k+1, c_l(k)\}$; u [5] i [34] dokazano je da ako je $\{k-1, k+1, c_l(k), d\}$ Diofantova četvorka, d mora biti ili $c_{l-1}(k)$ ili $c_{l+1}(k)$.

Ovo poglavlje dalje proširuje saznanja o familijama krivulja induciranim s trojkama $\{k-1, k+1, c_l(k)\}$, s naglaskom na njihovu torzijsku grupu i rang. U Korolaru 1.12 dokazali smo da ne postoje racionalne točke reda 4 na niti jednoj eliptičkoj krivulji induciranoj s Diofantovom trojkom. Drugim riječima, jedine moguće torzijske grupe od $E(\mathbb{Q})$ su $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Teorem 2.4 eliminira slučaj $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ koji je u [**54, Lemma 7**] ostao otvoren kod računanja oblika torzijske grupe za krivulje inducirane s $\{k-1, k+1, c_3(k)\}$. U Teoremu 2.5 dokazali smo isti rezultat za familiju induciranu s Diofantovim trojkama $\{k-1, k+1, c_4(k)\}$. Konačno, Teorem 2.6 proširuje taj rezultat na polovicu svih familija krivulja induciranih s trojkama $\{k-1, k+1, c_l(k)\}$, konkretno na one u kojima je $l \equiv 1$ ili $2 \pmod 4$. Pitanje ranga pokriveno je s Teoremom 2.18 u kojem smo dokazali da je rang svih eliptičkih krivulja induciranih s $\{k-1, k+1, c_l(k)\}$ uz $l \geq 2$ veći ili jednak 2.

U potpoglavlju 2.3.1 iskazali smo i dokazali uvjete uz koje je torzijska krivulja generiranih s Diofantovim trojkama oblika $\{a, b, a+b+2r\}$ izomorfna s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Kako bismo proširili Diofantovu trojku $\{k-1, k+1, c_l(k)\}$ do četvorke, moramo riješiti sustav jednadžbi

$$(k-1)x + 1 = \square, \quad (k+1)x + 1 = \square, \quad c_l(k)x + 1 = \square. \tag{2.9}$$

Sustavu (2.9) pridružimo eliptičku krivulju

$$E_l(k) : y^2 = ((k-1)x + 1)((k+1)x + 1)(c_l(k)x + 1).$$

2.2 Torzijska grupa od $E_l(k)$

Transformacija koordinata

$$x \mapsto \frac{x}{(k-1)(k+1)c_l(k)}, y \mapsto \frac{y}{(k-1)(k+1)c_l(k)}$$

primijenjena na krivulju $E_l(k)$ dovodi do eliptičke krivulje

$$E_l(k)' : y^2 = (x + (k-1)(k+1))(x + (k-1)c_l(k))(x + (k+1)c_l(k)). \tag{2.10}$$

Ovu krivulju dodatnom jednostavnom transformacijom možemo svesti na oblik $y^2 = x(x+M)(x+N)$, kojeg smo već vidjeli u Propoziciji 1.3. Taj oblik nam je izuzetno koristan zbog idućeg rezultata koji karakterizira torzijske grupe ovakvih eliptičkih krivulja, te uvjete pod kojima se pojedini oblici postižu:

Teorem 2.3. ([**58, Main Theorem 1**], [**44, Proposition 2**]) *Neka je E eliptička krivulja oblika*

$$y^2 = x(x+M)(x+N).$$

Torzijska podgrupa od $E(\mathbb{Q})$ jedinstveno je određena na sljedeći način:

- *Torzijska podgrupa od $E(\mathbb{Q})$ sadrži $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ako su M i N oba kvadrati, ili $-M$ i $N-M$ oba kvadrati, ili ako su $-N$ i $M-N$ oba kvadrati.*
- *Torzijska podgrupa od $E(\mathbb{Q})$ je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ako postoji cijeli broj d različit od nule takav da je $M = d^2u^4$ i $N = d^2v^4$, ili $M = -d^2v^4$ i $N = d^2(u^4 - v^4)$, ili $M = d^2(u^4 - v^4)$ i $N = -d^2v^4$, gdje je (u, v, w) Pitagorina trojka (tj. $u^2 + v^2 = w^2$).*
- *Torzijska podgrupa od $E(\mathbb{Q})$ je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ako postoje relativno prosti cijeli brojevi a, b i pozitivni cijeli broj d takvi da je $\frac{a}{b} \notin \{-2, -1, -\frac{1}{2}, 0, 1\}$, $M = d^2(a^4 + 2a^3b)$ i $N = d^2(b^4 + 2ab^3)$.*
- *U svim drugim slučajevima, torzijska podgrupa od $E(\mathbb{Q})$ je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Postoje tri racionalne točke na $E_l(k)'$ reda dva:

$$A' = \left(1 - k^2,\ 0\right),\ B' = \left((1-k)c_l(k),\ 0\right),\ C' = \left(-(k+1)c_l(k),\ 0\right).$$

Dokazat ćemo da su ovo jedine racionalne točke konačnog reda za $l = 3$, $l = 4$, te za sve l koji su oblika $l = 4m - 2$ i $l = 4m - 3$, pri čemu je $m \in \mathbb{N}$.

Na početku, pogledajmo prvih nekoliko članova od $\{c_l(k)\}$:

$$\begin{aligned} c_1(k) &= 4k, \\ c_2(k) &= 16k^3 - 4k, \\ c_3(k) &= 64k^5 - 48k^3 + 8k, \\ c_4(k) &= 256k^7 - 320k^5 + 112k^3 - 8k. \end{aligned}$$

Indukcijom po l, korištenjem identiteta

$$\begin{aligned} &\frac{(k+\sqrt{k^2-1})^{2l+5} + (k-\sqrt{k^2-1})^{2l+5} - 2k}{2(k^2-1)} \\ &= (4k^2-2)\frac{(k+\sqrt{k^2-1})^{2l+3} + (k-\sqrt{k^2-1})^{2l+3} - 2k}{2(k^2-1)} \\ &\quad - \frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1} - 2k}{2(k^2-1)} + 4k \end{aligned}$$

lako možemo provjeriti da članovi od $\{c_l(k)\}$ zadovoljavaju sljedeću rekurzivnu relaciju:

$$c_{l+2}(k) = (4k^2-2)c_{l+1}(k) - c_l(k) + 4k. \tag{2.11}$$

Teorem 2.4. *$E_3(k)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Dokaz. Stavljajući $l = 3$ u (2.10) dobiva se eliptička krivulja:

$$\begin{aligned} E_3(k)' : y^2 = &\left(x + (k-1)(k+1)\right)\left(x + (k-1)(64k^5 - 48k^3 + 8k)\right) \\ &\times \left(x + (k+1)(64k^5 - 48k^3 + 8k)\right). \end{aligned}$$

Uz jednostavnu transformaciju $x \mapsto x-(k-1)(k+1)$ dobivamo krivulju u željenom obliku $y^2 = x(x+M)(x+N)$:

$$E_3(k)'' : y^2 = x\left(x + (k-1)(64k^5 - 48k^3 + 7k - 1)\right)\left(x + (k+1)(64k^5 - 48k^3 + 7k + 1)\right).$$

Budući da je $\{k-1, k+1, 64k^5 - 48k^3 + 8k\}$ Diofantova trojka, iz Korolara 1.12 slijedi da su jedine moguće torzijske grupe od $E_3(k)''$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Dokazat ćemo da je potonji slučaj nemoguć. Pretpostavimo suprotno, tj. da je torzijska grupa izomorfna s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Prema Teoremu 2.3, postoje relativno prosti cijeli brojevi a, b i pozitivni cijeli broj d tako da:

$$M = d^2(a^4 + 2a^3b),$$

$$N = d^2(b^4 + 2ab^3)$$

i $\frac{a}{b} \notin \{-2, -1, -\frac{1}{2}, 0, 1\}$. Dakle, imamo:

$$M = (k-1)(64k^5 - 48k^3 + 7k - 1) = d^2(a^4 + 2a^3b), \tag{2.12}$$
$$N = (k+1)(64k^5 - 48k^3 + 7k + 1) = d^2(b^4 + 2ab^3). \tag{2.13}$$

Uočimo da

$$N + M = 128k^6 - 96k^4 + 14k^2 + 2, \tag{2.14}$$
$$N - M = 128k^5 - 96k^3 + 16k. \tag{2.15}$$

Definirajmo $m = \gcd(M, N)$. Dokazat ćemo da je $m = 2^a 3^b$, gdje su $a \leq 4, b \leq 1$ što će implicirati da $d^2 \in \{1, 4, 16\}$.
Očito, $m \mid N - M$, što je ekvivalentno s $m \mid 16k(8k^4 - 6k^2 + 1)$, a to daje

$$m \mid 16k(4k^2 - 1)(2k^2 - 1). \tag{2.16}$$

Neka je p bilo koji prosti djeljitelj od m. Iz (2.16), imamo sljedeće mogućnosti:

1. $p \mid k$

   Zbog (2.13), imamo:

   $$N = 64k^6 + 64k^5 - 48k^4 - 48k^3 + 7k^2 + 8k + 1 \equiv 1 \pmod{p},$$

   što je u kontradikciji s $N \equiv 0 \pmod{p}$.

2. $p \mid 2k^2 - 1$

   Imamo:

   $$14k^2 \equiv 7 \pmod{p},\ 96k^4 \equiv 24 \pmod{p},\ 128k^6 \equiv 16 \pmod{p}.$$

   Stoga, iz (2.14):

   $$N + M \equiv 16 - 24 + 7 + 2 \equiv 1 \pmod{p},$$

   što proturječi $N + M \equiv 0 \pmod{p}$.

3. $p \mid 16$

   U ovom slučaju očito je $p = 2$.

4. $p \mid 4k^2 - 1$

Promatrat ćemo jedino slučaj $p \mid 2k-1$ (slučaj $p \mid 2k+1$ je analogan). Imamo:

$$8k \equiv 4 \pmod{p},\ 8k^2 \equiv 2 \pmod{p},\ 48k^3 \equiv 6 \pmod{p},$$
$$48k^4 \equiv 3 \pmod{p},\ 64k^5 \equiv 2 \pmod{p},\ 64k^6 \equiv 1 \pmod{p}.$$

Stoga, ponovo iz (2.13):

$$N \equiv 1+2-3-6+(2-k^2)+4+1 \equiv 1-k^2 \pmod{p},$$

a znamo da je $N \equiv 0 \pmod{p}$, što povlači $1-k^2 \equiv 0 \pmod{p}$, a to je ekvivalentno s

$$4k^2 \equiv 4 \pmod{p}. \tag{2.17}$$

Kombinirajući (2.17) s $4k^2 \equiv 1 \pmod{p}$ dobiva se $p = 3$. Uočimo da je 1 najveća potencija od 3 sadržana u m zato što 3^n uz $n \geq 2$ ne može istovremeno dijeliti i $4k^2-1$ i $4k^2-4$. Dodatno, $p = 3$ ne može dijeliti $2k-1$ i $2k+1$ u isto vrijeme, a također ne dijeli ni ostale faktore od (2.16).

Stoga je očito da je $m = 2^a 3^b$, gdje su $a \leq 4, b \leq 1$ pa d^2 može biti jedan od $\{1, 4, 16\}$. Pokazat ćemo prvo da se slučaj $d^2 = 4$ ne može pojaviti. Naime, u tom slučaju sustav (2.12) i (2.13) postaje

$$64k^6 - 64k^5 - 48k^4 + 48k^3 + 7k^2 - 8k + 1 = 4(a^4 + 2a^3 b),$$

$$64k^6 + 64k^5 - 48k^4 - 48k^3 + 7k^2 + 8k + 1 = 4(b^4 + 2ab^3),$$

pa lijeve strane moraju biti djeljive s 4, a to je moguće samo ako $7k^2 + 1 \equiv 0 \pmod{4}$, što povlači $7k^2 + 1 \equiv 0 \pmod{8}$. Dakle, lijeve strane su djeljive s 8, pa i desne strane također moraju biti djeljive s 8, što je jedino moguće kad su i a i b parni. Međutim, a i b su relativno prosti pa je slučaj $d^2 = 4$ nemoguć. Za preostala dva slučaja uočimo da je $d^2 \equiv 1 \pmod{5}$. Iz toga, naš sustav implicira:

$$M = (k-1)(64k^5 - 48k^3 + 7k - 1) \equiv a^4 + 2a^3 b \pmod{5},$$

$$N = (k+1)(64k^5 - 48k^3 + 7k + 1) \equiv b^4 + 2ab^3 \pmod{5}.$$

Sada ćemo promatrati kongruencije modulo 5 i na temelju toga se uvjeriti da ovaj sustav nema rješenja u cijelim brojevima. Kada je $k \equiv 0$ ili 2 ili 3 $\pmod{5}$, lijeve strane ovog sustava su obje kongruentne ili 1 ili 2 modulo 5. U slučajevima $k \equiv 1$ ili 4 $\pmod{5}$, jedna od njih je kongruentna 0, a druga 3 modulo 5. Međutim, provjerom svih mogućih ostataka modulo 5 za a i b, lako utvrdimo da se nijedna od ovih kombinacija ne može pojaviti na desnim stranama ovog sustava. Dakle, ne postoje cjelobrojna rješenja. Kontradikcija. □

a mod 5	b mod 5	M mod 5	N mod 5
0	1	0	1
0	2	0	1
0	3	0	1
0	4	0	1
1	0	1	0
1	1	3	3
1	2	0	2
1	3	2	0
1	4	4	4
2	0	1	0
2	1	2	0
2	2	3	3
2	3	4	4
2	4	0	2
3	0	1	0
3	1	0	2
3	2	4	4
3	3	3	3
3	4	2	0
4	0	1	0
4	1	4	4
4	2	2	0
4	3	0	2
4	4	3	3

Tablica 2.1
Ostaci modulo 5 u slučaju $d^2 \equiv 1 \pmod 5$

Nadalje, dokazat ćemo isti rezultat za familiju $\{k-1, k+1, c_4(k)\}$.

Teorem 2.5. *$E_4(k)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Dokaz. Kao u prethodnom dokazu, pretpostavimo da je torzijska grupa izomorfna s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Sličnim zaključivanjem, dobivamo:

$$\begin{aligned} E_4(k)'' : y^2 = x\Big(x + (k-1)(256k^7 - 320k^5 + 112k^3 - 9k - 1)\Big) \\ \times \Big(x + (k+1)(256k^7 - 320k^5 + 112k^3 - 9k + 1)\Big) \end{aligned}$$

i

$$M = (k-1)(256k^7 - 320k^5 + 112k^3 - 9k - 1) = d^2(a^4 + 2a^3b), \tag{2.18}$$

$$N = (k+1)(256k^7 - 320k^5 + 112k^3 - 9k + 1) = d^2(b^4 + 2ab^3). \tag{2.19}$$

Ovdje ćemo promatrati kongruencije modulo 3. Očito, postoje tri moguća slučaja:

1. $k \equiv 2 \pmod 3$

   Lijeva strana od (2.18) je kongruentna 2 modulo 3 i lijeva strana od (2.19) je kongruentna 0 modulo 3. Stoga, desna strana od (2.19) mora također biti djeljiva s 3. To povlači jednu od sljedećih mogućnosti:

   1. $d \equiv 0 \pmod 3$
      Desna strana od (2.18) je djeljiva s 3, kontradikcija.
   2. $b \equiv 0 \pmod 3$
      Desna strana od (2.18) je kongruentna $d^2a^3(a+2b)$ modulo 3, što dalje daje $d^2a^3(a+2b) \equiv d^2a^4 \equiv (da^2)^2 \pmod 3$. Ovo je nemoguće budući da je desna strana od (2.18) kongruentna 2 modulo 3, a 2 nije kvadratni ostatak modulo 3.
   3. $a \equiv b \pmod 3$
      Desna strana od (2.18) je djeljiva s 3, kontradikcija.

2. $k \equiv 1 \pmod 3$

   Lijeva strana od (2.19) je kongruentna 2 modulo 3 i lijeva strana od (2.18) je kongruentna 0 modulo 3. Dakle, desna strana od (2.18) mora također biti djeljiva s 3. Ovaj slučaj je stoga analogan prethodnom, pa i ovdje imamo kontradikciju.

3. $k \equiv 0 \pmod 3$

   Lijeve strane i od (2.18) i od (2.19) su obje kongruentne 1 modulo 3. To implicira $d^2 \equiv 1 \pmod 3$ i $a^3(a+2b) \equiv b^3(b+2a) \equiv 1 \pmod 3$, što je nemoguće. Naime, ako je bilo koji od a i b djeljiv s 3, tada je barem jedan od prethodnih izraza djeljiv s 3. Ako a i b daju isti ostatak pri dijeljenju s 3, tada će faktori $(a+2b)$ i $(b+2a)$ biti djeljivi s 3. Dakle, jedina moguća preostala kombinacija jest da je jedan od a i b kongruentan 1 modulo 3, a drugi kongruentan 2 modulo 3. No, to ne zadovoljava zahtjev $a^3(a+2b) \equiv b^3(b+2a) \equiv 1 \pmod 3$.

□

Naredni rezultat je bitno općenitiji, naime pokriva sve eliptičke krivulje inducirane trojkama $\{k-1, k+1, c_l(k)\}$, gdje $l \equiv 1$ ili $2 \pmod 4$.

Teorem 2.6. *$E_l(k)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ za sve $l = 4m-2$ i $l = 4m-3$ gdje $m \in \mathbb{N}$.*

Dokaz. S obzirom da znamo egzaktne formule za $c_1(k)$ i $c_2(k)$, kombinirajmo ih s (2.11)

kako bismo dobili idući niz kongruencija modulo 8:

$$\begin{aligned} c_1(k) &\equiv 4k \pmod 8 \\ c_2(k) &\equiv 4k \pmod 8, \\ c_3(k) &\equiv 0 \pmod 8, \\ c_4(k) &\equiv 0 \pmod 8, \\ c_5(k) &\equiv 4k \pmod 8, \\ c_6(k) &\equiv 4k \pmod 8, \\ &\ldots \end{aligned}$$

Stoga, zaključujemo da

$$c_{4m-2}(k) \equiv c_{4m-3}(k) \equiv 4k \pmod 8, \tag{2.20}$$
$$c_{4m}(k) \equiv c_{4m-1}(k) \equiv 0 \pmod 8, \tag{2.21}$$

za $m \in \mathbb{N}$. Iz (2.10) uz transformaciju koordinata $x \mapsto x - (k-1)c_l(k)$ dobivamo iduću krivulju:

$$E_l(k)'' : y^2 = x\Big(x + (k-1)(k+1-c_l(k))\Big)\Big(x + 2c_l(k)\Big).$$

Jednako kao u dokazima prethodna dva teorema, pretpostavit ćemo suprotno, tj. da je torzijska grupa izomorfna s $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. To nam daje sustav jednadžbi:

$$M = (k-1)(k+1-c_l(k)) = d^2(a^4 + 2a^3b), \tag{2.22}$$
$$N = 2c_l(k) = d^2(b^4 + 2ab^3). \tag{2.23}$$

Iz (2.23) slijedi da je barem jedan od b, d paran.

1. b je paran i d je neparan

   Desna strana od (2.23) je djeljiva sa 16, pa lijeva strana također mora biti djeljiva sa 16, a to povlači da je k paran (vidi (2.20)). Tada, iz (2.22) slijedi da je a neparan. Zbrajanjem (2.22) i (2.23), dobivamo

   $$k^2 - 1 + (3-k)c_l(k) = d^2\left((a^2 + ab + b^2)^2 - 3a^2b^2\right). \tag{2.24}$$

   Budući da je d neparan, mora vrijediti $d^2 \equiv 1 \pmod 8$, što implicira da je desna strana od (2.24) kongruentna 1 ili 5 modulo 8. Na lijevoj strani imamo $c_l(k) \equiv 0 \pmod 8$, a k je paran, pa je lijeva strana kongruentna 3 ili 7 modulo 8, kontradikcija.

2. b je neparan i d je paran

Iz (2.22) slijedi da je k neparan. To znači da je lijeva strana od (2.23) djeljiva s 8, ali nije djeljiva sa 16. Ovo je pak u suprotnosti s desnom stranom koja je, ovisno o d, djeljiva ili s 4 ili sa 16.

3. Oba b i d su parna

Iz (2.22) slijedi da je k neparan, a iz (2.23) da je k paran što je očito nemoguće istovremeno.

□

Napomena 2.1. Za druge l, torzijska grupa i dalje može biti $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, iako nismo pronašli niti jedan primjer za potonju. Naime, dokaz koji smo predstavili ne vrijedi u situaciji kada je $l \equiv 0$ ili $3 \pmod 4$, zato jer tada imamo bezuvjetno $c_l(k) \equiv 0 \pmod 8$ pa stoga ne možemo eliminirati slučajeve 2. i 3. u dokazu kao što smo učinili kada je $l \equiv 1$ ili $2 \pmod 4$ i $c_l(k) \equiv 4k \pmod 8$.

2.3 Rang od $E_l(k)$

Pored točaka A', B', C', također postoje dvije dodatne racionalne točke na $E_l(k)'$:

$$P' = \Big(0,\ (k^2-1)c_l(k)\Big), \tag{2.25}$$

$$R' = \Big(s_l(k)t_l(k) + k(s_l(k)+t_l(k)) + 1,\ (s_l(k)+k)(t_l(k)+k)(s_l(k)+t_l(k))\Big). \tag{2.26}$$

Dokazat ćemo da su P' i R' nezavisne za sve $l \geq 2$, što zajedno s činjenicom da je $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ posljedično daje da je rang od $E_l(k)'$ nad $\mathbb{Q}$ veći ili jednak dva za sve $l \geq 2$.

Lema 2.7. $P', P'+A', P'+B', P'+C' \notin 2E_l(k)'(\mathbb{Q})$.

Dokaz. Imamo:

$$\begin{aligned} x(P') &= 0, \\ x(P'+A') &= c_l(k)^2 - 2kc_l(k), \\ x(P'+B') &= 2k+2-(k+1)c_l(k), \\ x(P'+C') &= -2k+2-(k-1)c_l(k). \end{aligned}$$

Ako je $P' \in 2E_l(k)'(\mathbb{Q})$, tada Propozicija 1.3 implicira da je k^2-1 kvadrat, što je nemoguće. Slično, ako je $P'+B' \in 2E_l(k)'(\mathbb{Q})$, tada je

$$x(P'+B') + k^2 - 1 = (k+1)(k+1-c_l(k)) = \square,$$

a ako je $P' + C' \in 2E_l(k)'(\mathbb{Q})$, onda je

$$x(P' + C') + k^2 - 1 = (k-1)(k-1-c_l(k)) = \square.$$

S obzirom da je $k \geq 2$ i $c_l(k) \geq c_1(k) = 4k$, oba izraza su negativna i zato ne mogu biti kvadrati. Konačno, ako je $P' + A' \in 2E_l(k)'(\mathbb{Q})$, onda je

$$x(P' + A') + k^2 - 1 = (c_l(k) - k)^2 - 1 = \square,$$

što je također nemoguće. □

Počevši s dokazom Leme 2.9, odsad nadalje trebat će nam sljedeći teorem kojeg su dokazali Mignotte i Pethő:

Teorem 2.8. ([50], *Théorème*) *Neka je a cijeli broj takav da $\Delta = a^2 - 4$ nije kvadrat cijelog broja. Definirajmo $\alpha = \dfrac{a + \sqrt{a^2-4}}{2}$ i $\beta = \dfrac{a - \sqrt{a^2-4}}{2}$, te promatrajmo Lucasove brojeve $u_n = u_n(a) = \dfrac{\alpha^l - \beta^l}{\alpha - \beta}$. Ako je $a \geq 4$ i $n > 3$, onda u_n nije ni kvadrat, ni dvostruki, ni trostruki, ni šesterostruki kvadrat cijelog broja, osim za $a = 338$ i $n = 4$.*

Lema 2.9. *$R', R' + A', R' + B', R' + C' \notin 2E_l(k)'(\mathbb{Q})$ za $l \geq 2$.*

Dokaz. Imamo:

$$\begin{aligned} x(R') &= s_l(k)t_l(k) + k(s_l(k) + t_l(k)) + 1, \\ x(R' + A') &= s_l(k)t_l(k) - k(s_l(k) + t_l(k)) + 1, \\ x(R' + B') &= (t_l(k) + k)(t_l(k) - s_l(k)) - (k+1)c_l(k), \\ x(R' + C') &= (s_l(k) + k)(s_l(k) - t_l(k)) - (k-1)c_l(k). \end{aligned}$$

Ako je $R' + B' \in 2E_l(k)'(\mathbb{Q})$, tada je

$$x(R' + B') + k^2 - 1 = (t_l(k) + k)(k - s_l(k)) = \square,$$

a ako je $R' + C' \in 2E_l(k)'(\mathbb{Q})$, tada je

$$x(R' + C') + k^2 - 1 = (s_l(k) + k)(k - t_l(k)) = \square.$$

Zbog $k \geq 2$, $s_l(k) \geq s_1(k) = 2k - 1$ i $t_l(k) \geq t_1(k) = 2k + 1$, oba izraza su negativna pa ne mogu biti kvadrati.

Ako je $R' \in 2E_l(k)'(\mathbb{Q})$, tada dobivamo idući sustav jednadžbi:

$$\begin{aligned}(s_l(k)+k)(t_l(k)+k) &= \square,\\ (s_l(k)+t_l(k))(s_l(k)+k) &= \square,\\ (s_l(k)+t_l(k))(t_l(k)+k) &= \square.\end{aligned}$$

Definirajmo

$$d = \gcd(s_l(k)+t_l(k),\ t_l(k)+k,\ s_l(k)+k),$$

tada

$$d \mid t_l(k)+k+s_l(k)+k-(s_l(k)+t_l(k)),$$

odnosno $d \mid 2k$. Ako $d \mid k$, onda također $d \mid s_l(k)$ i $d \mid t_l(k)$, ali iz (2.3) i (2.4) dobivamo $c_l(k) = \frac{1}{2}(t_l(k)-s_l(k))(t_l(k)+s_l(k))$, što povlači $d \mid c_l(k)$. Međutim, $d \mid c_l(k)$, $d \mid s_l(k)$ i (2.3) daju $d = 1$, pa je iz toga $d \in \{1,2\}$. Zapišimo

$$s_l(k)+k = dx\square,\ \ t_l(k)+k = dy\square,\ \ s_l(k)+t_l(k) = dz\square,$$

pri čemu su x, y, z kvadratno slobodni cijeli brojevi, takvi da je $\gcd(x,y,z) = 1$. Tada je

$$xy = \square,\ \ xz = \square,\ \ yz = \square,$$

iz čega dobivamo $x = y = z$. Zbog $\gcd(x,y,z) = 1$ slijedi $x = y = z = 1$, pa s obzirom na $d \in \{1,2\}$, to povlači

$$s_l(k)+k = \square,\ \ t_l(k)+k = \square,\ \ s_l(k)+t_l(k) = \square$$

ili

$$s_l(k)+k = 2\square,\ \ t_l(k)+k = 2\square,\ \ s_l(k)+t_l(k) = 2\square.$$

Definirajmo novi niz $\{a_l(k)\}$ kao $s_l(k)+t_l(k) = 2a_{l+1}(k)$. Zbog rekurzivnih relacija (2.7) i (2.8), slijedi da je

$$a_l(k) = 2ka_{l-1}(k) - a_{l-2}(k),\ a_0(k) = 0,\ a_1(k) = 1.$$

Lako je dokazati da je eksplicitna formula za niz $\{a_l(k)\}$ dana s

$$a_l(k) = \frac{(k+\sqrt{k^2-1})^l - (k-\sqrt{k^2-1})^l}{2\sqrt{k^2-1}}. \tag{2.27}$$

$a_l(k)$ je očito oblika $\dfrac{\alpha^l-\beta^l}{\alpha-\beta}$, gdje $\alpha = \dfrac{1}{2}\left(2k+\sqrt{(2k)^2-4}\right)$ i $\beta = \dfrac{1}{2}\left(2k-\sqrt{(2k)^2-4}\right)$. Zajedno s $k \geq 2$, to implicira da niz $\{a_l(k)\}$ zadovoljava uvjete Teorema 2.8, pa stoga

$a_l(k) = \square, 2\square, 3\square$ ili $6\square$ implicira $l < 4$. Slučajevi $l \in \{2, 3\}$ su provjereni u [54], pa zaključujemo da ako je $s_l(k)+t_l(k) = 2\square$ ili $s_l(k)+t_l(k) = \square$, tada je $l = 1$. U suprotnom, imamo kontradikciju s $R' \notin 2E_l(k)'(\mathbb{Q})$.
Ako je $R' + A' \in 2E_l(k)'(\mathbb{Q})$, imamo sljedeći sustav jednadžbi:

$$\begin{aligned}(s_l(k) - k)(t_l(k) - k) &= \square,\\ (s_l(k) + t_l(k))(s_l(k) - k) &= \square,\\ (s_l(k) + t_l(k))(t_l(k) - k) &= \square.\end{aligned}$$

Koristeći isto zaključivanje, slijedi da je $s_l(k) + t_l(k) = 2\square$ ili $s_l(k) + t_l(k) = \square$, što je jedino moguće za $l = 1$ pa slijedi $R' + A' \notin 2E_l(k)'(\mathbb{Q})$ za $l \geq 2$. □

Propozicija 2.10. $t_{2l}(k) - s_{2l}(k) = c_l(k) - c_{l-1}(k) = 2a_{2l}(k)$.

Dokaz. Iz (2.5) i (2.6) dobivamo da je $t_{2l}(k) - s_{2l}(k)$ jednako:

$$\begin{aligned}&\frac{(k+\sqrt{k^2-1})^{2l+1}(2k-2\sqrt{k^2-1}) + (k-\sqrt{k^2-1})^{2l+1}(-2k-2\sqrt{k^2-1})}{2\sqrt{k^2-1}}\\ =\ &\frac{(k+\sqrt{k^2-1})^{2l} - (k-\sqrt{k^2-1})^{2l}}{\sqrt{k^2-1}}.\end{aligned}$$

Zbog (2.27), to je jednako s $2a_{2l}(k)$. S druge strane, iz (2.2) računamo $c_l(k) - c_{l-1}(k)$:

$$\begin{aligned}&\frac{(k+\sqrt{k^2-1})^{2l+1} + (k-\sqrt{k^2-1})^{2l+1}}{2(k^2-1)}\\ &\quad - \frac{(k+\sqrt{k^2-1})^{2l-1} - (k-\sqrt{k^2-1})^{2l-1}}{2(k^2-1)}\\ =\ &\frac{(k+\sqrt{k^2-1})^{2l+1}\left(1-(k-\sqrt{k^2-1})^2\right)}{2(k^2-1)}\\ &\quad + \frac{(k-\sqrt{k^2-1})^{2l+1}\left(1-(k+\sqrt{k^2-1})^2\right)}{2(k^2-1)}\\ =\ &\frac{(k+\sqrt{k^2-1})^{2l+1}(k-\sqrt{k^2-1}) - (k-\sqrt{k^2-1})^{2l+1}(k+\sqrt{k^2-1})}{\sqrt{k^2-1}}\\ =\ &\frac{(k+\sqrt{k^2-1})^{2l} - (k-\sqrt{k^2-1})^{2l}}{\sqrt{k^2-1}}.\end{aligned}$$

□

Propozicija 2.11. $t_{2l}(k) + k = (k+1)\left(c_l(k) - \dfrac{c_l(k)+c_{l-1}(k)}{2k} + 1\right)$.

Dokaz. Računamo $-k+(k+1)\left(c_l(k)-\dfrac{c_l(k)+c_{l-1}(k)}{2k}+1\right)$:

$$\begin{aligned}
&-k+\frac{k+1}{2k}\left(c_l(k)(2k-1)-c_{l-1}(k)+2k\right)\\
&=\frac{4k-4k^2+\left(k+\sqrt{k^2-1}\right)^{2l+1}\left(2k-1-(k-\sqrt{k^2-1})^2\right)}{4k(k-1)}\\
&\quad+\frac{\left(k-\sqrt{k^2-1}\right)^{2l+1}\left(2k-1-(k+\sqrt{k^2-1})^2\right)}{4k(k-1)}+1\\
&=\frac{\left(k+\sqrt{k^2-1}\right)^{2l+1}\left(\sqrt{k+1}-\sqrt{k-1}\right)}{2\sqrt{k-1}}\\
&\quad-\frac{\left(k-\sqrt{k^2-1}\right)^{2l+1}\left(\sqrt{k+1}+\sqrt{k-1}\right)}{2\sqrt{k-1}}\\
&=t_{2l}(k).
\end{aligned}$$

□

Napomena 2.2. Oba kvocijenta na desnoj strani jednakosti u Propoziciji 2.11 su cijeli brojevi. Naime, iz prva dva elementa od $\{c_l(k)\}$ te iz formule (2.11) slijedi da je $c_l(k)$ djeljivo s $2k$ za sve k i l.

Sljedeća tri identiteta dokazujemo na sličan način prateći dokaz Propozicije 2.11:

Propozicija 2.12. $s_{2l}(k)-k=(k-1)\left(c_l(k)+\dfrac{c_l(k)+c_{l-1}(k)}{2k}-1\right).$

Propozicija 2.13. $s_{2l+1}(k)-k=(k-1)\left(\dfrac{c_{l+1}(k)+c_l(k)}{2k}+c_l(k)-1\right).$

Propozicija 2.14. $t_{2l+1}(k)-k=(k+1)\left(\dfrac{c_{l+1}(k)+c_l(k)}{2k}-c_l(k)-1\right).$

Iz Propozicija 2.13 i 2.14 dobivamo:

$$t_{2l+1}(k)-s_{2l+1}(k)=\frac{c_{l+1}(k)+c_l(k)}{k}-2kc_l(k)-2, \tag{2.28}$$

$$t_{2l+1}(k)+k=k-1+\frac{(k+1)\left(c_{l+1}(k)+(1-2k)c_l(k)\right)}{2k}, \tag{2.29}$$

$$s_{2l+1}(k)+k=k+1+\frac{(k-1)\left(c_{l+1}(k)+(1+2k)c_l(k)\right)}{2k}. \tag{2.30}$$

Kako bismo dokazali Lemu 2.17, osim prethodnih propozicija trebat ćemo još tri dodatna

niza, $\{d_l(k)\}$, $\{e_l(k)\}$ i $\{f_l(k)\}$, definirana na sljedeći način:

$$d_l(k) = \frac{c_l(k)}{k}(k-1)+1, \tag{2.31}$$

$$e_l(k) = \frac{c_l(k)}{k}(k+1)-1, \tag{2.32}$$

$$f_l(k) = \frac{c_l(k)}{2k}(k^2-1). \tag{2.33}$$

Iz (2.11), slijedi da je

$$d_{l+2}(k) = (4k^2-2)d_{l+1}(k) - d_l(k) + 4k - 4k^2, \tag{2.34}$$

$$e_{l+2}(k) = (4k^2-2)e_{l+1}(k) - e_l(k) + 4k + 4k^2, \tag{2.35}$$

$$f_{l+2}(k) = (4k^2-2)f_{l+1}(k) - f_l(k) + 2(k^2-1). \tag{2.36}$$

Dodatno, kao što Fibonaccijev niz zadovoljava čuveni Cassinijev identitet:

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n,\ F_n \text{ je } n\text{-ti Fibonaccijev broj;}$$

dokazali smo da također postoje četiri identiteta koja povezuju po dva uzastopna elementa od $\{c_l(k)\}$, $\{d_l(k)\}$, $\{e_l(k)\}$ i $\{f_l(k)\}$:

Propozicija 2.15.

$$d_{l+1}(k)^2 - (4k^2-2)d_{l+1}(k)d_l(k) + d_l(k)^2 + (4k^2-4k)(d_{l+1}(k)+d_l(k)) = 4(k-1)^2,$$
$$e_{l+1}(k)^2 - (4k^2-2)e_{l+1}(k)e_l(k) + e_l(k)^2 - (4k^2+4k)(e_{l+1}(k)+e_l(k)) = 4(k+1)^2,$$
$$c_{l+1}(k)^2 - (4k^2-2)c_{l+1}(k)c_l(k) + c_l(k)^2 - 4k(c_{l+1}(k)+c_l(k)) = 0,$$
$$f_{l+1}(k)^2 - (4k^2-2)f_{l+1}(k)f_l(k) + f_l(k)^2 - (2k^2-2)(c_{l+1}(k)+c_l(k)) = 0.$$

Dokaz. Dokazat ćemo samo prvi identitet indukcijom po l, ostali identiteti dokazuju se analogno. Imamo

$$d_1(k) = 4k-3,$$

$$d_2(k) = 16k^3 - 16k^2 - 4k + 5.$$

Dakle,

$$d_2(k)^2 - (4k^2-2)d_2(k)d_1(k) + d_1(k)^2 + (4k^2-4k)(d_2(k)+d_1(k)) = 4(k-1)^2,$$

što je i željeno. Pretpostavimo

$$d_{l+1}(k)^2 - (4k^2-2)d_{l+1}(k)d_l(k) + d_l(k)^2 + (4k^2-4k)(d_{l+1}(k)+d_l(k)) = 4(k-1)^2.$$

Iz (2.34) slijedi da je

$$\begin{aligned}
&d_{l+2}(k)^2 - (4k^2-2)d_{l+2}(k)d_{l+1}(k) + d_{l+1}(k)^2 \\
&\quad + (4k^2-4k)(d_{l+2}(k)+d_{l+1}(k)) \\
&= \left((4k^2-2)d_{l+1}(k) - d_l(k) + 4k - 4k^2\right)^2 + d_{l+1}(k)^2 + (4k^2-4k)d_{l+1}(k) \\
&\quad + \left((4k^2-2)d_{l+1}(k) - d_l(k) + 4k - 4k^2\right)\left(4k^2-4k-(4k^2-2)d_{l+1}(k)\right) \\
&= 4(k-1)^2.
\end{aligned}$$

□

Propozicija 2.16.

$$x(R'+P') + k^2 - 1 = (s_l(k)+k)(t_l(k)+k)(k^2-1)\square, \tag{2.37}$$

$$x(R'+P') + (k+1)c_l(k) = 2(k+1)(t_l(k)-s_l(k))(t_l(k)+k)\square, \tag{2.38}$$

$$x(R'+P') + (k-1)c_l(k) = 2(k-1)(t_l(k)-s_l(k))(s_l(k)+k)\square. \tag{2.39}$$

Dokaz. Dokažimo samo prvi identitet, ostala dva se dokazuju na isti način. Dokazat ćemo da je

$$\begin{aligned}
x(R'+P') + k^2 - 1 = (s_l(k)+k)(t_l(k)+k)(k^2-1) \\
\times \frac{(c_l(k)-t_l(k)-s_l(k))^2}{((s_l(k)+k)(t_l(k)+k)-(k^2-1))^2},
\end{aligned}$$

odnosno, ekvivalentno

$$x(R'+P') + k^2 - 1 = (s_l(k)+k)(t_l(k)+k)(k^2-1)\square.$$

Iz (2.3) i (2.4) dobivamo idući identitet:

$$\left(k^2-1\right)\left((c_l(k)-k)^2-1\right) = \left(s_l(k)^2-k^2\right)\left(t_l(k)^2-k^2\right). \tag{2.40}$$

Nadalje,

$$x(R'+P') = \lambda^2 + a_1\lambda - a_2 - x(R') - x(P'),$$

pri čemu je

$$a_1 = a_3 = 0,$$

$$a_2 = k^2 - 1 + 2kc_l(k),$$

$$a_4 = c_l(k)(k^2-1)(2k+c_l(k)),$$

$$a_6 = c_l(k)^2(k^2-1)^2,$$

$$\lambda = \frac{y(R') - y(P')}{x(R') - x(P')} = (\text{zbog } (2.25) \text{ i } (2.26))$$
$$= \frac{(s_l(k)+k)(t_l(k)+k)(s_l(k)+t_l(k)) - (k^2-1)c_l(k)}{(s_l(k)+k)(t_l(k)+k) - (k^2-1)}.$$

Uvrštavanjem svega uz zamjenu $x(R') = (s_l(k)+k)(t_l(k)+k) - (k^2-1)$ dobivamo da je $x(R'+P') + k^2 - 1$

$$= \frac{((s_l(k)+k)(t_l(k)+k)(s_l(k)+t_l(k)))^2 - 2c_l(k)(k^2-1)(s_l(k)+k)(t_l(k)+k)}{x(R')^2}$$
$$+ \frac{c_l(k)^2(k^2-1)^2 - 2kc_l(k)x(R')^2 - x(R')^3}{x(R')^2}$$
$$= \frac{(k^2-1)(s_l(k)+k)(t_l(k)+k)}{x(R')^2}\Bigg(-2c_l(k)(s_l(k)+t_l(k)) + 4kc_l(k) + 3(s_l(k)+k)(t_l(k)+k)$$
$$+ \frac{(s_l(k)+k)(t_l(k)+k)\left((s_l(k)+t_l(k))^2 - 2kc_l(k) - (s_l(k)+k)(t_l(k)+k)\right)}{k^2-1}$$
$$+ \frac{(k^2-1)(c_l(k)^2 - 2kc_l(k) + k^2 - 1)}{(s_l(k)+k)(t_l(k)+k)}\Bigg).$$

Korištenjem identiteta (2.40) i zamjenom $2kc_l(k) = s_l(k)^2 + t_l(k)^2 - 2$ dobivamo da je to jednako

$$\frac{(k^2-1)(s_l(k)+k)(t_l(k)+k)}{x(R')^2}\Bigg(\frac{(s_l(k)+k)(t_l(k)+k)((s_l(k)-k)(t_l(k)-k) - 2(k^2-1))}{k^2-1}$$
$$- 2c_l(k)(s_l(k)+t_l(k)) + 4kc_l(k) + 2(s_l(k)+k)(t_l(k)+k) + 2s_l(k)t_l(k) + 2k^2\Bigg).$$

Ponovnim korištenjem (2.40) i sređivanjem cijelog izraza dobivamo traženu tvrdnju. □

Lema 2.17. *$R'+P', R'+P'+A', R'+P'+B', R'+P'+C' \notin 2E_l(k)'(\mathbb{Q})$ za $l \geq 2$.*

Dokaz. $R'+P' \in 2E_l(k)'(\mathbb{Q})$ ako i samo ako $x(R'+P') + k^2 - 1 = \square$, $x(R'+P') + (k+1)c_l(k) = \square$ i $x(R'+P') + (k-1)c_l(k) = \square$. No, iz prethodne propozicije znamo da je

$$x(R'+P') + k^2 - 1 = (s_l(k)+k)(t_l(k)+k)(k^2-1)\square, \tag{2.41}$$
$$x(R'+P') + (k+1)c_l(k) = 2(k+1)(t_l(k)-s_l(k))(t_l(k)+k)\square, \tag{2.42}$$
$$x(R'+P') + (k-1)c_l(k) = 2(k-1)(t_l(k)-s_l(k))(s_l(k)+k)\square. \tag{2.43}$$

1. l je paran

Koristeći Propozicije 2.10 i 2.11, možemo zapisati (2.42) za parne l ($l = 2i$) kao

$$x(R'+P')+(k+1)c_{2i}(k)=2(c_i(k)-c_{i-1}(k))\left(c_i(k)-\frac{c_i(k)+c_{i-1}(k)}{2k}+1\right)\square. \quad (2.44)$$

Strategija dokaza ovog slučaja koja se prirodno nameće jest pokazati da desna strana od (2.44) ne može biti kvadrat niti za jedan prirodni broj i, što će implicirati da $R'+P'\notin 2E_l(k)'(\mathbb{Q})$ za sve parne l. Neka je

$$g=\gcd\left(c_i(k)-c_{i-1}(k),\ c_i(k)-\frac{c_i(k)+c_{i-1}(k)}{2k}+1\right).$$

Indukcijom možemo dokazati da je $\gcd(t_{2i}(k)+k,\ 2k)=1$, a to je ekvivalentno s $\gcd(g,2k)=1$. Iz toga slijedi

$$g\ \Big|\ \frac{c_i(k)-c_{i-1}(k)}{2k},\quad g\mid c_i(k)-\frac{c_i(k)+c_{i-1}(k)}{2k}+1,$$

što povlači

$$g\ \Big|\ \frac{c_i(k)}{k}(k-1)+1,\ g\ \Big|\ \frac{c_{i-1}(k)}{k}(k-1)+1.$$

Uz $d_l(k)$ definiran u (2.31), slijedi da $g\mid d_i(k)$, $g\mid d_{i-1}(k)$. Naš idući korak je utvrditi da je $g=1$. Ako kombiniramo prvi identitet iz Propozicije 2.15 s upravo dokazanim činjenicama $g\mid d_i(k)$ i $g\mid d_{i-1}(k)$, dobivamo da $g\mid 4(k-1)^2$. Formula (2.31) i činjenica da je $\gcd(g,2)=1$ dalje povlače $g=1$. Vrativši se na (2.42) i (2.44), sada možemo zaključiti da je $t_l(k)-s_l(k)=\square$ ili $t_l(k)-s_l(k)=2\square$, ali Propozicija 2.10 i Teorem 2.8 eliminiraju tu mogućnost, isto kao u dokazu Leme 2.9. Dakle, $R'+P'\notin 2E_l(k)'(\mathbb{Q})$ za sve parne l.

2. l je neparan i k je paran

Dokazat ćemo iz (2.42) i (2.43) da $t_l(k)+k$ i $s_l(k)+k$ oba moraju biti kvadrati. Kombiniranje tih činjenica s (2.41) će tada implicirati i da je k^2-1 kvadrat, što očito nije moguće. Zbog (2.29) i (2.30), formule (2.42) i (2.43) za neparne l ($l=2i+1$) možemo zapisati kao:

$$x(R'+P')+(k+1)c_{2i+1}(k)=2(k+1)\left(\frac{c_{i+1}(k)+c_i(k)}{k}-2kc_i(k)-2\right)$$
$$\times\left(k-1+\frac{(k+1)(c_{i+1}(k)+(1-2k)c_i(k))}{2k}\right), \quad (2.45)$$

$$x(R'+P')+(k-1)c_{2i+1}(k)=2(k-1)\left(\frac{c_{i+1}(k)+c_i(k)}{k}-2kc_i(k)-2\right)\times\left(k+1+\frac{(k-1)(c_{i+1}(k)+(1+2k)c_i(k))}{2k}\right). \quad (2.46)$$

Indukcijom možemo utvrditi iz definicije od $c_i(k)$ (vidi (2.2)) da je

$$\frac{(k+1)(c_{i+1}(k)+(1-2k)c_i(k))}{2k}$$

paran. Budući da je k također paran, slijedi da je $t_{2i+1}(k)+k$ neparno. Očito je da je $t_{2i+1}(k)+k\equiv 2 \pmod{k+1}$, stoga $\gcd(t_{2i+1}(k)+k,\ 2(k+1))=1$. Dokažimo sada da je i $\gcd(t_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k))=1$. Neka je

$$m=\gcd\left(\frac{c_{i+1}(k)+c_i(k)}{k}-2kc_i(k)-2,\ k-1+\frac{(k+1)(c_{i+1}(k)+(1-2k)c_i(k))}{2k}\right).$$

Tada je $\gcd(m,2k)=1$ zbog $m\mid t_{2i+1}(k)+k$ i $\gcd(t_{2i+1}(k)+k,\ k)=1$ (potonje induktivno slijedi iz definicije od $t_l(k)$). Nadalje,

$$m\mid (k^2-1)c_i(k)+2k,$$

što je ekvivalentno s

$$m\,\Big|\,\frac{(k^2-1)}{2k}c_i(k)+1.$$

Slično, dobivamo i

$$m\,\Big|\,\frac{(k^2-1)}{2k}c_{i+1}(k)+k^2.$$

Koristeći definiciju od $f_l(k)$ (vidi (2.33)), to povlači $m\mid f_l(k)+1$, $m\mid f_{l+1}(k)+k^2$. Propozicija 2.15 dalje daje $m\mid (k^2-1)^2$ što je, zbog definicije od $f_l(k)$ i činjenice da $m\mid f_l(k)$, moguće samo za $m=1$. Koristeći potpuno isto zaključivanje dobivamo

$$\gcd(s_{2i+1}(k)+k,\ 2(k-1))=1$$

i

$$\gcd(s_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k))=1.$$

Dakle, za parne k, oba $t_{2i+1}(k)+k$ i $s_{2i+1}(k)+k$ su kvadrati cijelih brojeva. Iz (2.41) slijedi da k^2-1 mora također biti kvadrat cijelog broja, a to je nemoguće.

3. l i k su neparni

Oba $t_{2i+1}(k)+k$ i $s_{2i+1}(k)+k$ su sada parni. Označimo

$$\begin{aligned} S = \{ &\gcd\left(t_{2i+1}(k)+k,\ 2(k+1)\right), \\ &\gcd\left(t_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k)\right), \\ &\gcd\left(s_{2i+1}(k)+k,\ 2(k-1)\right), \\ &\gcd\left(s_{2i+1}(k)+k,\ t_{2i+1}(k)-s_{2i+1}(k)\right)\}. \end{aligned}$$

Temeljem prethodnih opažanja, zaključujemo da svi elementi od S moraju biti potencije od 2. Ovisno o k i i, iz (2.20), (2.21), (2.28), (2.29) i (2.30) dobivamo sljedeće:

k	$t_{2i+1}(k)-s_{2i+1}(k)$	$t_{2i+1}(k)+k$	$s_{2i+1}(k)+k$
1	2	4	2
3	2	2	0
5	2	0	6
7	2	6	4

Tablica 2.2
Ostaci modulo 8 za $i \equiv 0$ ili 2 (mod 4)

k	$t_{2i+1}(k)-s_{2i+1}(k)$	$t_{2i+1}(k)+k$	$s_{2i+1}(k)+k$
1	6	0	2
3	6	2	4
5	6	4	6
7	6	6	0

Tablica 2.3
Ostaci modulo 8 za $i \equiv 1$ ili 3 (mod 4)

Iz tablica 2.2 i 2.3 slijedi da je $S = \{2, 4, 8\}$. Budući da desne strane i od (2.45) i od (2.46) moraju biti kvadrati, to povlači da je ili $t_{2i+1}(k)+k = 2\square$ i $s_{2i+1}(k)+k = 2\square$ ili $t_{2i+1}(k)+k = 2\square$ i $s_{2i+1}(k)+k = \square$ (ili obratno). Ako vrijedi $t_{2i+1}(k)+k = 2\square$ i $s_{2i+1}(k)+k = 2\square$, tada mora biti $k^2-1 = \square$, zato što desna strana od (2.41) mora biti kvadrat, a to nije moguće. S druge strane, ako vrijedi $t_{2i+1}(k)+k = 2\square$ i $s_{2i+1}(k)+k = \square$ (ili obratno), tada mora biti $k^2-1 = 2\square$, a to je moguće ako i samo ako $k-1 = \square$, $k+1 = 2\square$ ili $k-1 = 2\square$, $k+1 = \square$. Uvrstivši to natrag u (2.42) i (2.43) dobivamo da $t_l(k)-s_l(k) = \square$ ili $t_l(k)-s_l(k) = 2\square$ za sve neparne l. Zbog $t_l(k)-s_l(k) = 2a_l(k)$ (što se može dokazati kao u dokazu Propozicije 2.10) dolazimo do $a_l(k) = \square$ ili $a_l(k) = 2\square$ što ponovo eliminiramo pozivanjem na Teorem 2.8. Dakle, $R'+P' \notin 2E_l(k)'(\mathbb{Q})$ za sve $l \geq 2$.

Dalje, imamo

$$x(R'+P'+A')+(k^2-1)=(k^2-1)(t_l(k)-k)(s_l(k)-k)\square, \tag{2.47}$$

$$x(R'+P'+A')+(k+1)c_l(k)=2(k+1)(t_l(k)-s_l(k))(t_l(k)-k)\square, \tag{2.48}$$

$$x(R'+P'+A')+(k-1)c_l(k)=2(k-1)(t_l(k)-s_l(k))(s_l(k)-k)\square. \tag{2.49}$$

Vrijedi $R'+P'+A' \in 2E_l(k)'(\mathbb{Q})$ ako i samo ako su sve desne strane ovog sustava jednadžbi kvadrati. Ponovo, imat ćemo različite strategije ovisno o parnosti od l.

1. l je paran

   Propozicije 2.10 i 2.12 impliciraju da (2.49) za parne l ($l=2i$) postaje

   $$x(R'+P'+A')+(k-1)c_{2i}(k)=2\left(c_i(k)-c_{i-1}(k)\right)\left(c_i(k)+\frac{c_i(k)+c_{i-1}(k)}{2k}-1\right)\square. \tag{2.50}$$

   Prateći potpuno iste korake kao u dokazu $R'+P' \notin 2E_l(k)'(\mathbb{Q})$ za parne l, definirajmo

   $$h=\gcd\left(c_i(k)-c_{i-1}(k),\ c_i(k)+\frac{c_i(k)+c_{i-1}(k)}{2k}-1\right),$$

   tada

   $$h \mid \frac{c_i(k)}{k}(k+1)-1, \quad h \mid \frac{c_{i-1}(k)}{k}(k+1)-1.$$

   Uz $e_l(k)$ definiran u (2.32), slijedi da $h \mid e_i(k)$ i $h \mid e_{i-1}(k)$. Propozicija 2.15 povlači $h \mid 4(k+1)^2$, a to je nemoguće zbog same definicije od $e_i(k)$ i zato jer su svi $e_i(k)$ neparni. Dakle, $h=1$ i posljedično $t_l(k)-s_l(k)=\square$ ili $t_l(k)-s_l(k)=2\square$, a to smo prethodno već dokazali da je nemoguće.

2. l je neparan

   Iz Propozicija 2.13 i 2.14, jednadžba (2.47) za neparne l ($l=2i+1$) postaje:

   $$x(R'+P'+A')+(k^2-1)=\left(\frac{c_{i+1}(k)+(1-2k)c_i(k)-2k}{2k}\right)\times\left(\frac{c_{i+1}(k)+(1+2k)c_i(k)-2k}{2k}\right)\square.$$

   Neka je

   $$n=\gcd\left(\frac{c_{i+1}(k)+(1-2k)c_i(k)-2k}{2k},\ \frac{c_{i+1}(k)+(1+2k)c_i(k)-2k}{2k}\right).$$

Iz definicije od $c_l(k)$ jednostavno slijedi da

$$2k \mid \frac{c_{i+1}(k)+(1-2k)c_i(k)}{2k},\ 2k \mid \frac{c_{i+1}(k)+(1+2k)c_i(k)}{2k}.$$

Dakle, zaključujemo da su n i $2k$ relativno prosti. Nadalje, $n \mid c_{i+1}(k)+c_i(k)-2k$ i $n \mid 2c_i(k)$, a budući da je n neparan slijedi da $n \mid c_i(k)$. Štoviše, imamo $n \mid c_{i+1}(k)-2k$. Zbog $n \mid c_i(k)$ i Propozicije 2.15 slijedi da $n \mid c_{i+1}(k)(c_{i+1}(k)-4k)$, pa zaključujemo da $n \mid 4k^2$, a to je nemoguće za $n>1$ zato jer su n i $2k$ relativno prosti. Dakle,

$$\gcd\left(\frac{c_{i+1}(k)+(1-2k)c_i(k)-2k}{2k},\ \frac{c_{i+1}(k)+(1+2k)c_i(k)-2k}{2k}\right)=1,$$

pa zato oba ova broja moraju biti kvadrati cijelih brojeva. Ponovo iz Propozicija 2.13 i 2.14, jednadžbe (2.48) i (2.49) postaju:

$$\begin{aligned} x(R'+P'+A')+(k+1)c_{2i+1}(k) &= 2(t_{2i+1}(k)-s_{2i+1}(k)) \\ &\quad \times \left(\frac{c_{i+1}(k)+(1-2k)c_i(k)-2k}{2k}\right)\square, \\ x(R'+P'+A')+(k-1)c_{2i+1}(k) &= 2(t_{2i+1}(k)-s_{2i+1}(k)) \\ &\quad \times \left(\frac{c_{i+1}(k)+(1+2k)c_i(k)-2k}{2k}\right)\square. \end{aligned}$$

Zaključujemo da za neparne l vrijedi $t_l(k)-s_l(k)=2\square$, što implicira $a_l(k)=\square$, a to je nemoguće za $l\geq 2$ prema Teoremu 2.8. Iz toga slijedi da $R'+P'+A' \notin 2E_l(k)'(\mathbb{Q})$ za sve $l\geq 2$.

Konačno, imamo

$$x(R'+P'+B')+(k^2-1) = (k^2-1)(t_l(k)+k)(k-s_l(k))\square, \tag{2.51}$$
$$x(R'+P'+B')+(k+1)c_l(k) = 2(k+1)(t_l(k)+s_l(k))(t_l(k)+k)\square, \tag{2.52}$$
$$x(R'+P'+B')+(k-1)c_l(k) = 2(k-1)(t_l(k)+s_l(k))(k-s_l(k))\square. \tag{2.53}$$

i

$$x(R'+P'+C')+(k^2-1) = (k^2-1)(s_l(k)+k)(k-t_l(k))\square, \tag{2.54}$$
$$x(R'+P'+C')+(k+1)c_l(k) = 2(k+1)(t_l(k)+s_l(k))(t_l(k)-k)\square, \tag{2.55}$$
$$x(R'+P'+C')+(k-1)c_l(k) = 2(k-1)(t_l(k)+s_l(k))(s_l(k)+k)\square. \tag{2.56}$$

Desne strane od (2.51) i (2.54) su negativne pa ne mogu biti kvadrati, iz čega slijedi $R'+P'+B' \notin 2E_l(k)'(\mathbb{Q})$ i $R'+P'+C' \notin 2E_l(k)'(\mathbb{Q})$. □

Teorem 2.18. *Rang od $E_l(k)'$ nad $\mathbb{Q}$ je veći ili jednak dva za sve $l \geq 2$.*

Dokaz. Dokazat ćemo da P' i R' generiraju podgrupu ranga 2 u $E_l(k)'(\mathbb{Q})/E_l(k)'(\mathbb{Q})_{tors}$ za sve $l \geq 2$. Pretpostavimo suprotno, tada $aP' + bR' \in E_l(k)'(\mathbb{Q})_{tors}$ implicira da a i b ne mogu oba biti nula. Znamo da je $E_l(k)'(\mathbb{Q})_{tors}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Promotrimo prvo slučaj $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, tada je $E_l(k)'(\mathbb{Q})_{tors} = \{A', B', C', \mathcal{O}\}$. Neka je $aP' + bR' = T' \in E_l(k)'(\mathbb{Q})_{tors}$. Ako a i b nisu istovremeno parni, tada imamo jedan od sljedećih slučajeva: $P' + T' \in 2E_l(k)'(\mathbb{Q})$, $R' + T' \in 2E_l(k)'(\mathbb{Q})$, $P' + R' + T' \in 2E_l(k)'(\mathbb{Q})$. No, niti jedan od tih slučajeva nije moguć zbog Lema 2.7, 2.9 i 2.17. Dakle, i a i b moraju biti parni: $a = 2a_1, b = 2b_1$ i $2a_1P' + 2b_1R' \in E_l(k)'(\mathbb{Q})_{tors}$. Budući da su A', B', C' reda dva i stoga ne mogu biti oblika $2T'$, te $E_l(k)'(\mathbb{Q})_{tors} = \{A', B', C', \mathcal{O}\}$, slijedi da je $2a_1P' + 2b_1R' = \mathcal{O}$, pa $a_1P' + b_1R' \in E_l(k)'(\mathbb{Q})_{tors}$. Dakle, metoda beskonačnog spusta daje nam $a = b = 0$, što je kontradikcija.
Slučaj $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ se može riješiti na isti način kao i prethodni slučaj, zbog činjenice da svaka torzijska točka T' zadovoljava $T' \equiv \mathcal{O}, A', B'$ ili $C' \pmod{2E_l(k)'(\mathbb{Q})}$. □

Napomena 2.3. U Teoremu 2.18 postavili smo uvjete samo na l, dok je k fiksan i proizvoljan, odnosno implicitno pretpostavljamo uvjete koje smo naveli u definiciji niza $c_l(k)$ (vidi (2.2)), tj. $k \geq 2$.

2.3.1 Distribucija ranga

Prethodni teorem daje nam donju ogradu za rang eliptičkih krivulja induciranih familijama Diofantovih trojki $\{k-1, k+1, c_l(k)\}$, no interesantno je pogledati koje se doista vrijednosti pojavljuju za neke vrijednosti od k i l. Korištenjem programa **mwrank**[7] dobili smo egzaktne vrijednosti za rang za manje vrijednosti od k i l. Zanimljivo je da smo ovim postupkom uspjeli dobiti i jednu krivulju visokog ranga (6) u slučaju $k = 4$, $l = 5$. Tablice 2.4, 2.5 i 2.6 prikazuju dobivene rezultate. Valja primijetiti da rangovi dviju krivulja (označeni zvjezdicom) nisu egzaktno izračunati. U slučaju $l = 5, k = 28$ rang je ili 2 ili 4, dok je u slučaju $l = 9, k = 4$ rang jednak 4 ako je Birch-Swinnerton-Dyer slutnja [65] istinita, jer njena istinitost povlači istinitost Slutnje o parnosti koja daje ovaj rezultat o rangu.

k	rang
2	2
3	2
4	6
5	3
6	3
7	2
8	2
9	2

k	rang
10	4
11	3
12	2
13	2
14	2
15	3
16	2
17	3

k	rang
18	2
19	2
20	2
21	3
22	2
23	2
24	2
25	3

k	rang
26	2
27	2
28	2 ili 4*
29	3
30	2

Tablica 2.4
Rangovi u slučaju $l = 5$

k	rang
2	4
3	3
4	3
5	2
6	2
7	2
8	2

Tablica 2.5
Rangovi u slučaju $l = 7$

k	rang
2	3
3	3
4	4*
5	2
6	2
7	2
8	2

Tablica 2.6
Rangovi u slučaju $l = 9$

2.4 Torzijska grupa krivulja induciranih trojkama $\{a, b, a + b + 2r\}$

Poglavlje ćemo zaključiti nekim rezultatima o torzijskoj grupi eliptičkih krivulja generiranih familjama Diofantovih trojki oblika $\{a, b, a+b+2r\}$. Još je Euleru (a moguće već i Diofantu) bilo poznato da se svaki Diofantov par $\{a, b\}$ može jednostavnom konstrukcijom proširiti do Diofantove trojke: $c = a+b+2r$, pri čemu je $ab+1 = r^2$. Lako možemo provjeriti da točke P i R ovdje nisu nezavisne, budući da vrijedi $2P = -2R$. Ponovo nas zanima torzijska grupa eliptičkih krivulja dobivenih od Diofantovih trojki $\{a, b, a + b + 2r\}$. Iz Korolara 1.12 već znamo da su jedine moguće torzijske grupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Već uobičajenim postupkom iz Diofantove trojke $\{a, b, a + b + 2r\}$ dobivamo krivulju

$$C : y^2 = \Big(ax + 1\Big)\Big(bx + 1\Big)\Big((a + b + 2r)x + 1\Big).$$

Korištenjem zamjene varijabli:

$$y \mapsto \frac{y}{ab(a + b + 2r)}, x \mapsto \frac{x}{ab(a + b + 2r)}$$

tu krivulju transformiramo u:

$$C' : y^2 = \Big(x + b(a+b+2r)\Big)\Big(x + a(a+b+2r)\Big)\Big(x + ab\Big).$$

Uvjete za postojanje torzijske grupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ poznajemo iz Teorema 2.3; moraju postojati cijeli broj d te relativno prosti cijeli brojevi e i f takvi da je

$$a(a+2r) = d^2(e^4 + 2e^3 f), \tag{2.57}$$
$$b(b+2r) = d^2(f^4 + 2ef^3). \tag{2.58}$$

Teorem 2.19. *Ako je barem jedan od brojeva a, b neparan, onda je $C(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Dokaz. $C(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ako i samo ako sustav (2.57) i (2.58) ima cjelobrojnih rješenja. Kako bi ovaj sustav imao rješenja, uočimo prvo da d mora biti paran. U suprotnom je $d^2 \equiv 1 \pmod 4$; uvjerimo se da to nije moguće. Kako su e i f relativno prosti, ne mogu oba biti parna. Ako su oba neparna, tada su desne strane kongruentne 3 modulo 4, a ako je jedan od njih neparan a drugi paran, tada desne strane daju ostatak 1, odnosno 0 pri dijeljenju s 4. Međutim, lijeve strane ne mogu davati te ostatke pri dijeljenju s 4. Ako su i a i b neparni, onda je r paran, iz čega slijedi da su lijeve strane obje kongruentne 1 modulo 4. Ako je pak jedan od a, b paran, a drugi neparan, tada ovaj što je paran mora biti djeljiv s 4 (inače $r^2 \equiv 3 \pmod 4$), pa dobivamo da jedna lijeva strana daje ostatak 0, a druga 3 modulo 4, što se ne poklapa s onime što imamo na desnoj strani. Iz upravo dokazane parnosti od d odmah slijedi da i lijeve strane jednadžbi moraju biti parne, a to je moguće ako i samo ako su i a i b parni. Dakle, čim jedan od njih nije paran, sustav (2.57) i (2.58) nema cjelobrojnih rješenja i jedina moguća torzijska grupa je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Uočimo također da navedeni sustav ima rješenja samo ako vrijedi $4|d$. Kad bi d bio djeljiv samo s 2, a ne i s 4, tada bi barem jedna od desnih strana jednadžbi davala ostatak 4 pri dijeljenju s 8. No, to nije moguće jer ako $4|a$ ili $4|b$ onda je lijeva strana djeljiva s 8, a ako je $a \equiv 2 \pmod 4$ ili $b \equiv 2 \pmod 4$, zbog neparnosti od r opet dobivamo djeljivost lijeve strane s 8. □

Dodajmo u obje jednadžbe i s lijeve i s desne strane r^2 kako bismo slijeva dobili potpun kvadrat:

$$(a+r)^2 = r^2 + d^2(e^4 + 2e^3 f),$$
$$(b+r)^2 = r^2 + d^2(f^4 + 2ef^3).$$

Uz zamjene

$$m = e^4 + 2e^3 f,\ n = f^4 + 2ef^3 \tag{2.59}$$

sustav prelazi u:

$$r^2 + md^2 = (a + r)^2,$$

$$r^2 + nd^2 = (b + r)^2,$$

tj. dobili smo sustav jednadžbi poznat pod imenom Eulerove sukladne forme (*Euler's concordant forms*). Njihova cjelobrojna rješenja je Ono u svom članku [58] sveo na proučavanje eliptičkih krivulja oblika

$$E_{\mathbb{Q}}(m, n) : y^2 = x(x + m)(x + n)$$

i rezultate iz tog članka smo već iskoristili u ovom radu, npr. za dokazivanje da određeni oblici torzijskih grupa nisu mogući. U idućoj lemi ćemo ih dodatno iskoristiti.

Lema 2.20. *Nužni uvjet da bi vrijedilo* $C(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *jest da je je rang eliptičke krivulje* $y^2 = x(x + m)(x + n)$ *veći od nule.*

Dokaz. Iz [58, **Main Corollary 1**] dobivamo jedinstveno cjelobrojno rješenje Eulerovih sukladnih formi koje dolazi od torzijskih točaka od $E(\mathbb{Q})(m, n)$ gdje je $m = e^4+2e^3f,\ n = f^4 + 2ef^3$, a koje onda daje i torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ od $C(\mathbb{Q})$. To rješenje je:

$$r = ef,$$

$$d = 1,$$

$$a + r = e(e + f),$$

$$b + r = f(e + f).$$

Lako se vidi da ovo nije moguće. Teorem 2.19 eliminira $d = 1$, a vidimo i da mora biti $a = e^2,\ b = f^2$, što je nemoguće zbog $ab + 1 = r^2$. Stoga torzijske točke od $E(\mathbb{Q})(m, n)$ ne daju cjelobrojna rješenja Eulerovih formi, pa ako ih ima, rješenja jedino mogu doći od pozitivnog ranga. □

Napomena 2.4. Nismo pronašli niti jednu krivulju oblika $y^2 = x(x + m)(x + n)$ takvu da je rang veći od nule i da m i n zadovoljavaju sustav jednadžbi

$$r^2 + md^2 = (a + r)^2,$$

$$r^2 + nd^2 = (b + r)^2,$$

uz dodatni uvjet $ab + 1 = r^2$, tako da je slutnja da je $C(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Poglavlje 3

Eliptičke krivulje s cikličkom izogenijom stupnja n

3.1 Uvod

U ovom dijelu disertacije promatrat ćemo eliptičke krivulje s cikličkom izogenijom određenog stupnja, pa počnimo s definicijom izogenije.

Definicija 3.1. Izogenija između dvije eliptičke krivulje je konačni morfizam $\phi : E \to E'$ koji preslikava $\mathcal{O} \in E$ u $\mathcal{O}' \in E'$.

Propozicija 3.1. [61, **Theorem 4.8, Chapter III**] *Svaka izogenija je homomorfizam grupa.*

Definicija 3.2. Ciklička izogenija stupnja n ili n-izogenija je izogenija čija je jezgra ciklička grupa reda n.

Definicija 3.3. Ako $\phi : E \to E'$ ciklička izogenija stupnja $n \neq 0$, tada postoji jedinstvena izogenija $\psi : E' \to E$ takva da je $\phi\psi = [n]$, gdje je $[n]$ oznaka za množenje-s-n izogeniju. Izogeniju ψ nazivamo dualnom izogenijom.

Definicija 3.4. Za eliptičke krivulje E i E' kažemo da su izogene ako postoji izogenija iz E u E' (odnosno, ekvivalentno, iz E' u E).

Slijedi primjer jedne izogenije koju ćemo često upotrebljavati u ovom poglavlju:

Primjer 3.1. Eliptička krivulja E nad $\mathbb{Q}$ s jednadžbom

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

2-izogena je eliptičkoj krivulji E' nad $\mathbb{Q}$ s jednadžbom

$$y^2 = x^3 + a'x^2 + b'x,$$

gdje su $a' = -2a$ i $b' = a^2 - 4b$. Izogenija $\phi : E \to E'$ je definirana kao:

$$\phi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2-b)}{x^2}\right) & \text{, za } P = (x,y) \notin \{\mathcal{O}, (0,0)\} \\ \mathcal{O}' & \text{, inače.} \end{cases}$$

Analogno se definira $\psi : E' \to E$:

$$\psi(P') = \begin{cases} \left(\dfrac{y'^2}{4x'^2}, \dfrac{y'(x'^2-b')}{8x'^2}\right) & \text{, za } P' = (x',y') \notin \{\mathcal{O}', (0,0)\}, \\ \mathcal{O} & \text{, inače.} \end{cases}$$

Vrijedi $(\psi \circ \phi)(P) = 2P$ za sve $P \in E$ i $(\phi \circ \psi)(P') = 2P'$ za sve $P' \in E'$.

Iduće što želimo jest definirati modularne krivulje. Za to nam prvo treba definicija modularne grupe:

Definicija 3.5. Modularna grupa $\mathrm{SL}_2(\mathbb{Z})$ je

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

Modularnu grupu generiraju matrice

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ i } \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

a grupovna operacija je množenje matrica.

Definicija 3.6. Neka je N prirodan broj. Tada je glavna kongruencijska podgrupa nivoa N definirana kao

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

Definicija 3.7. Podgrupa Γ od $\mathrm{SL}_2(\mathbb{Z})$ je kongruencijska podgrupa ako je $\Gamma(N) \leq \Gamma$ za neki $N \in \mathbb{N}$. Neka je N najmanji takav; u tom slučaju kažemo da je Γ kongruencijska podgrupa nivoa N.

Sljedeće kongruencijske podgrupe su nam posebno zanimljive:

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

(gdje „*" označava „nije specificirano") i

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

Između ovih podgrupa vrijede odnosi:

$$\Gamma(N) \leq \Gamma_1(N) \leq \Gamma_0(N) \leq \mathrm{SL}_2(\mathbb{Z}).$$

Također, važna nam je i kongruencijska podgrupa koju definiramo prateći [42]

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

gdje je $N \geq 1$ i M je pozitivni djeljitelj od N.

Definicija 3.8. Gornja poluravnina je

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

Konačno, spremni smo definirati modularnu krivulju:

Definicija 3.9. Za kongruencijsku podgrupu Γ od $\mathrm{SL}_2(\mathbb{Z})$ definiramo modularnu krivulju kao kvocijentni prostor orbita od Γ, odnosno

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

Modularne krivulje za $\Gamma_0(N)$, $\Gamma_1(N)$ i $\Gamma(N)$ označavamo s

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

Važno je istaknuti da skupovi $Y(N)$, $Y_0(N)$ i $Y_1(N)$ nisu kompaktni (u kvocijentnoj topologiji), a s kompaktnima je puno lakše raditi. Stoga ih kompaktificiramo dodavanjem konačnog broja točaka koje nazivamo kaspovi (*cusps*). Formalno, definiramo $\mathcal{H}^* = \mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$ i $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$ za neku kongruencijsku grupu Γ. Dakle, $X(\Gamma)$ je unija od $\mathcal{H}$ i konačnog skupa klasa elemenata od $\mathbb{Q} \cup \{\infty\}$ (kaspova), pa možemo pisati $Y_0(N) = X_0(N)\backslash\{\text{kaspovi}\}$ i $Y_1(N) = X_1(N)\backslash\{\text{kaspovi}\}$.

Važnost modularnih krivulja $Y_0(N)$, $Y_1(N)$ i $Y_1(M,N)$ je u interpretaciji njihovih prostora parametara (*moduli space*). Naime, ako je K polje algebarskih brojeva, algebarska interpretacija od $Y_1(N)$ jest da je to modularna krivulja čije K-racionalne točke klasificiraju klase izomorfizama parova (E,P), gdje je E eliptička krivulja definirana nad K, a P je točka na $E(K)$ reda N. Slično, $Y_1(M,N)$ je modularna krivulja čije racionalne točke klasificiraju

klase izomorfizama trojki (E, P, R), gdje je E eliptička krivulja definirana nad K, a P i R su točke na $E(K)$ koje generiraju grupu izomorfnu s $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Uočimo da je $Y_1(1, N) = Y_1(N)$. Algebarska interpretacija od $Y_0(N)$ jest da je to modularna krivulja čije K-racionalne točke klasificiraju parove (E, f), gdje je E eliptička krivulja definirana nad K, a f je ciklička izogenija stupnja N definirana nad K iz E u neku drugu eliptičku krivulju E'. Sve navedene činjenice i pojmovi mogu se u [8] naći detaljnije obrađeni.

Definicija 3.10. Neka je E eliptička krivulja nad poljem algebarskih brojeva K. Zakret (*twist*) eliptičke krivulje E nad K je eliptička krivulja E' nad K koja je $\overline{K}$-izomorfna s E. Krivulju E' nazivamo kvadratni zakret ako je izomorfna s E nad nekim kvadratnim poljem. Ako je E zadana kao

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

te je $d \in K\backslash K^2, d \neq 0$, tada kvadratni zakret od E označavamo s $E^{(d)}$ i definiramo s jednadžbom

$$y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6.$$

Naš cilj je izbrojati koliko ima eliptičkih krivulja s cikličkom izogenijom stupnja n nad raznim kvartičnim poljima. Pri tome je bitno istaknuti da kad brojimo eliptičke krivulje nad K s cikličkom izogenijom stupnja n, brojimo do na $\overline{K}$-izomorfizam, jer ako $E(K)$ ima n-izogeniju, tada i svaki kvadratni zakret od E također ima n-izogeniju. Označimo dakle s $\#Y_0(n)(K)$ broj eliptičkih krivulja s cikličkom izogenijom stupnja n, do na $\overline{K}$-izomorfizam.

Svi mogući stupnjevi n-izogenija eliptičkih krivulja nad $\mathbb{Q}$, zajedno s brojem klasa $\overline{\mathbb{Q}}$-izomorfizama koje imaju n-izogeniju istog stupnja određeni su u radovima Mazura [47] i Kenkua [39, 40, 41]. Mi ćemo svoj cilj, brojanje eliptičkih krivulja s n-izogenijom nad određenim kvartičnim poljima, ostvariti tako što ćemo promatrati modularne krivulje $X_0(n)$ genusa 1. U [29] i [60, str.103] pobrojani su svi n-ovi za koje je $X_0(n)$ genusa 1, označimo taj skup sa S:

$$S = \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}.$$

Razlog zbog kojeg razmatramo samo n-ove za koje je $X_0(n)$ genusa 1 jest što je to jedini zanimljiv slučaj. Naime, ako je $X_0(n)$ genusa 0, onda je uz činjenice da $X_0(n)$ ima barem jedan racionalni kasp i da je broj kaspova konačan, $\#Y_0(n)(K) = \infty$ nad bilo kojim poljem. S druge strane, ako je $X_0(n)$ krivulja genusa ≥ 2, tada postoji samo konačno mnogo krivulja s cikličkom izogenijom stupnja n nad bilo kojim poljem K. To je izravna posljedica Faltingsovog teorema [28] jer $X_0(n)(K)$ ima samo konačno mnogo točaka (Faltings je inače, između ostalog i za taj rezultat, 1986. dobio Fieldsovu medalju). Kad je genus jednak 1 i $n \in S$, $\#Y_0(n)(K)$ može biti i konačan i beskonačan, a nas

zanimaju polja K nad kojima postoji pozitivan, ali konačan broj eliptičkih krivulja s cikličkom izogenijom stupnja n, te vrijedi $\#Y_0(n)(K) > \#Y_0(n)(\mathbb{Q})$. Da bi to vrijedilo, primijetimo da idući uvjeti moraju biti ispunjeni:

- $\text{rank}(X_0(n)(K)) = 0$.
- $\#X_0(n)(K)_{tors} > \#X_0(n)(\mathbb{Q})_{tors}$.

Za sve $n \in S$, $\#Y_0(n)(\mathbb{Q})$ je konačan (a u nekim slučajevima i nula). Naime, krivulje $X_0(n)$ imaju rang 0 nad $\mathbb{Q}$, što se može provjeriti npr. u Cremoninim tablicama [7], pa je stoga $\#Y_0(n)(\mathbb{Q})$ konačan za sve n-ove. Krivulja $Y_0(n)(\mathbb{Q})$ ima (vidi [47]) jednu točku za $n = 19, 27$, dvije točke za $n = 14, 17$, tri točke za $n = 11$, četiri točke za $n = 15, 21$, odnosno nema točaka za ostale slučajeve genusa 1.

Najman je [55] pokazao da, ako je K prostog stupnja (nad $\mathbb{Q}$), tada u svima, osim u konačno mnogo eksplicitno navedenih slučajeva, vrijedi da je ili $\#Y_0(n)(\mathbb{Q}) = \#Y_0(n)(K)$ ili $\#Y_0(n)(K) = \infty$. Isto je pokazano i za modularne krivulje $Y_1(n)$ genusa 1. S druge strane, u [56] je isti autor dokazao da postoji beskonačno mnogo kvartičnih polja K takvih da $\#Y_1(n)(\mathbb{Q}) \neq \#Y_1(n)(K) < \infty$. U ovoj disertaciji dokazat ćemo sličan rezultat za krivulje $Y_0(n)$, gdje je n takav da postoji kvadratno polje K takvo da $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$. Strategija koju ćemo koristiti je proširenje takvih kvadratnih polja u kvartična za odgovarajuće n-ove, osim za $n = 27$ za kojeg ne postoje točke reda 2 (u tom slučaju nalazimo sekstično polje). Sve takve n-ove, K-ove i odgovarajuće vrijednosti od $\#Y_0(n)(K)$ nalazimo u idućem teoremu:

Teorem 3.2. ([55, Theorem 3]) *Jedini parovi (n, K), gdje je $n \in S$ i K je polje prostog stupnja takvo da vrijedi $\#Y_0(n)(\mathbb{Q}) < \#Y_0(n)(K) < \infty$ su navedeni u tablici ispod. Polja algebarskih brojeva $K = \mathbb{Q}(\alpha)$ zadana su preko minimalnih polinoma f od α.*

n	f	$\#Y_0(n)(K)$
11	$x^3 - 13392x - 1080432$	8
14	$x^2 + 7$	8
14	$x^2 + 3$	14
15	$x^2 - 5$	12
15	$x^2 + 1$	12
19	$x^3 - 12096x - 544752$	4
20	$x^2 + 1$	6
21	$x^2 + 3$	12
27	$x^2 + 3$	3
27	$x^3 - 314928$	4
49	$x^2 + 7$	2

Mi ćemo dokazati da postoji beskonačno mnogo kvartičnih polja L, takvih da za n-ove iz Teorema 3.2 za koje je pripadno polje algebarskih brojeva K kvadratno (to su svi osim

11 i 19, te $n = 27$ za kojeg nalazimo sekstično polje) vrijedi $\#Y_0(n)(\mathbb{Q}) < \#Y_0(n)(L) < \infty$, te ćemo ih eksplicitno odrediti. Ta kvartična polja bit će bikvadratna polja dobivena proširivanjem kvadratnih polja K iz spomenutog teorema, tako da i dalje postoji samo konačno mnogo eliptičkih krivulja nad L s cikličkom izogenijom stupnja n. Lako se vidi da to postižemo ako i samo ako odgovarajuća modularna krivulja $X_0(n)$ i dalje ima rang 0 nad dobivenim bikvadratnim poljem. Naša strategija je pronaći beskonačnu familiju prostih brojeva p, takvih da za sva kvartična polja $\mathbb{Q}(\sqrt{d_1}, \sqrt{p})$, gdje su $K = \mathbb{Q}(\sqrt{d_1})$ polja iz Teorema 3.2, vrijedi

$$\operatorname{rank}(X_0(n)(\mathbb{Q}(\sqrt{d_1}, \sqrt{p}))) = 0.$$

U tom slučaju pronašli smo beskonačno mnogo kvartičnih polja nad kojima postoji konačan broj eliptičkih krivulja s cikličkom izogenijom stupnja n. Rang ćemo računati koristeći poznatu činjenicu [**61**]

$$\operatorname{rank}(E(L)) = \operatorname{rank}(E(K)) + \operatorname{rank}(E^{(d)}(K)),$$

gdje je $E^{(d)}$ kvadratni zakret eliptičke krivulje E za d, K je polje algebarskih brojeva, L je njegovo kvadratno proširenje ($L = K(\sqrt{d})$) i E je eliptička krivulja definirana nad K. Naime, ako ovo primijenimo na naš slučaj, dobivamo:

$$\begin{aligned}\operatorname{rank}(X_0(n)(\mathbb{Q}(\sqrt{d_1}, \sqrt{p}))) = \operatorname{rank}(X_0(n)(\mathbb{Q})) + \operatorname{rank}(X_0^{(d_1)}(n)(\mathbb{Q})) \\ + \operatorname{rank}(X_0^{(p)}(n)(\mathbb{Q})) + \operatorname{rank}(X_0^{(d_1 p)}(n)(\mathbb{Q})),\end{aligned} \tag{3.1}$$

pa je samo potrebno pronaći takve p za koje je

$$\operatorname{rank}(X_0^{(p)}(n)(\mathbb{Q})) = \operatorname{rank}(X_0^{(d_1 p)}(n)(\mathbb{Q})) = 0.$$

To ćemo učiniti metodom spusta s 2-izogenijama objašnjenom u idućem odjeljku.

3.2 Spust pomoću 2-izogenija

Računanje ranga eliptičke krivulje općenito je vrlo zahtjevan postupak, i nema garancije da će uspješno završiti. U slučaju da krivulja ima točku reda 2, onda je računanje obično lakše nego u općem slučaju i često se provodi metodom spusta pomoću 2-izogenija koju ćemo ovdje predstaviti, te koristiti za dokaze rezultata iz ovog poglavlja. Referiramo se na [**6**], [**24**] i [**37**], a formalniji pristup s više dokaza može se pronaći u [**61**].

Neka je E eliptička krivulja nad $\mathbb{Q}$ (možemo specijalizirati na $\mathbb{Q}$, jer ćemo spust raditi nad $\mathbb{Q}$) koja ima točku reda 2. Bez smanjenja općenitosti (uz eventualnu promjenu koordinata) možemo pretpostaviti da je točka reda 2 upravo točka $(0, 0)$, te da je E zadana jednadžbom

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

Nije teško krivulju iz općenitog oblika transformirati u ovaj oblik. Naime, ako je polazna krivulja bila zadana u dugom Weierstrassovom obliku, prvo pronađemo x_0, korijen kubnog polinoma $x^3 + b_2x^2 + 8b_4x + 16b_6$, te napravimo zamjenu $a = 3x_0 + b_2$, $b = (a + b_2)x_0 + 8b_4$ (prisjetimo se, b_2, b_4 i b_6 definirani su u (1.7)). U Primjeru 3.1 pokazali smo da E ima 2-izogenu krivulju E', te smo definirali preslikavanja $\phi : E \to E'$ i $\psi : E' \to E$. Definirajmo ovdje još i preslikavanje $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ kao

$$\alpha(P) = \begin{cases} 1 \cdot \mathbb{Q}^{*2} & , \text{za } P(x,y) = \mathcal{O}, \\ b \cdot \mathbb{Q}^{*2} & , \text{za } P(x,y) = (0,0), \\ x \cdot \mathbb{Q}^{*2} & , \text{za } P(x,y) \notin \{(0,0),\ \mathcal{O}\}. \end{cases}$$

Analogno definiramo i preslikavanje $\beta : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$. Očito je da je $\mathrm{Ker}(\phi) = \{(0,0),\ \mathcal{O}\}$ i $\mathrm{Ker}(\psi) = \{(0,0),\ \mathcal{O}\}$, a može se pokazati i da vrijedi $\mathrm{Im}(\phi)$=$\mathrm{Ker}(\beta)$ te $\mathrm{Im}(\psi)$=$\mathrm{Ker}(\alpha)$. Definiciju 3.2 u kojoj uvodimo pojam stupnja izogenije sada vidimo i na primjeru - preslikavanja ϕ i ψ su 2-izogenije jer im jezgre imaju po 2 elementa. Ta preslikavanja smo definirali jer su izravno povezana s rangom:

$$2^r = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|}{4}, \tag{3.2}$$

gdje je $r = \mathrm{rank}(E(\mathbb{Q}))$. Izogene krivulje imaju isti rang pa je i $r = \mathrm{rank}(E'(\mathbb{Q}))$, ali torzijske grupe ne moraju biti jednake. Ono što je sigurno zadovoljeno za njih jest $|E(\mathbb{Q})_{tors}| = 2^i |E'(\mathbb{Q})_{tors}|$, uz $i \in \{-1, 0, 1\}$.

Kako bismo izračunali rang korištenjem formule (3.2), moramo dobiti opis od $\mathrm{Im}(\alpha)$. Neka je $\widetilde{x}$ oznaka za klasu od x u $\mathbb{Q}^*/\mathbb{Q}^{*2}$, te neka je $(x, y) \in E(\mathbb{Q})$. Za $x = 0$ mora biti i $y = 0$ i $\alpha(x, y) = \widetilde{b}$. Za ostale x, može se pokazati (vidi npr. [6]) da se jednadžba eliptičke krivulje E jednostavno transformira u jednadžbu

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4 \tag{3.3}$$

koju nazivamo torzor, u kojoj su nepoznanice $M, N, e \in \mathbb{Z}$, $0 \neq M \neq e \neq 0$, te vrijedi $b_1b_2 = b$, pri čemu su i $b_1, b_2 \in \mathbb{Z}$. Također, uz tako definirane M, e i N, vrijedi

$$\alpha(x, y) = \frac{b_1M^2}{e^2} \cdot \mathbb{Q}^{*2} = \widetilde{b_1}.$$

Sada je jasno da se $\mathrm{Im}(\alpha)$ sastoji od $\widetilde{1}$, $\widetilde{b}$, te od svih $\widetilde{b_1}$ gdje je je b_1 djeljitelj broja b za kojeg jednadžba (3.3) uz $b_1b_2 = b$ ima rješenja $M, e, N \in \mathbb{Z}$, $0 \neq M \neq e \neq 0$. Primijetimo da (3.3) za $b_1 = 1$ i $b_1 = b$ uvijek ima očita rješenja $(M, e, N) = (1, 0, 1)$, odnosno $(M, e, N) = (0, 1, 1)$. Analogno opisujemo i $\mathrm{Im}(\beta)$.

Za primjenu ovog postupka važno je istaknuti da smijemo pretpostaviti da je $\gcd(M, e) = 1$, te da bez smanjenja općenitosti možemo promatrati samo one djeljitelje b_1 od b koji su kvadratno slobodni. Algoritam je sljedeći: za svaku faktorizaciju $b = b_1 b_2$, gdje je b_1 kvadratno slobodan cijeli broj, napišemo odgovarajući torzor i pokušamo odrediti ima li ta jednadžba netrivijalnih cjelobrojnih rješenja. Nemamo garancije da sa sigurnošću možemo to utvrditi, jer za ovakve jednadžbe ne mora vrijediti lokalno-globalni princip Hassea i Minkowskog. Svako pronađeno rješenje (M, e, N) inducira točku $\left(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3}\right)$ na krivulji E, pri čemu su oba razlomka do kraja skraćena. Ako s r_1 označimo broj faktorizacija za koje pripadna jednadžba (3.3) ima rješenja, te analogno definiramo r_2 za krivulju E', onda postoje nenegativni cijeli brojevi e_1 i e_2 takvi da je $r_1 = 2^{e_1}$, $r_2 = 2^{e_2}$ i vrijedi (vidi (3.2))

$$\operatorname{rank}(E(\mathbb{Q})) = e_1 + e_2 - 2. \tag{3.4}$$

Navedimo i da klase $b_1 \mathbb{Q}^{*2}$, takve da je (3.3) svuda lokalno rješiva (uključujući i u ∞) nazivamo ϕ-Selmerovom grupom koja odgovara 2-izogeniji ϕ i označavamo je sa $S_\psi(E)$. Na isti način definiramo ψ-Selmerovu grupu $S_\phi(E')$ koja odgovara 2-izogeniji ψ. Budući da ove grupe daju gornju ogradu za rang,

$$\operatorname{rank}(E(\mathbb{Q})) = \log_2(|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|) - 2 \leq \log_2(|S_\psi(E)| \cdot |S_\phi(E')|) - 2, \tag{3.5}$$

dobivamo formulu analognu formuli (3.4) za dokazivanje da je rang određene eliptičke krivulje jednak nuli.

3.3 Slučajevi $n = 14$ i $n = 15$

Teorem 3.3. *Neka je p prost broj koji zadovoljava $p \equiv 3 \pmod 8$ i $\left(\frac{7}{p}\right) = -1$. Tada je* $\operatorname{rank}(X_0^{(p)}(14)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-7p)}(14)(\mathbb{Q})) = 0$.

Dokaz. Iz [**56, Theorem 3**] i činjenice da su krivulje $X_0(14)$ i $X_1(14)$ izogene, izravno slijedi tvrdnja teorema (naime, izogene krivulje imaju isti rang). Izogenost krivulja $X_0(14)$ i $X_1(14)$ slijedi iz činjenice da uvijek uvijek postoji konačni morfizam $X_1(n) \to X_0(n)$. Uglavnom je $X_1(n)$ većeg genusa od $X_0(n)$, ali u slučaju $n = 14$ imamo da su obje krivulje genusa 1, pa taj morfizam mora biti izogenija eliptičkih krivulja nad $\mathbb{Q}$.

□

Korolar 3.4. *Postoji beskonačno mnogo prostih brojeva p takvih da za $K = \mathbb{Q}(\sqrt{-7}, \sqrt{p})$ vrijedi* $\operatorname{rank}(X_0(14)(K)) = 0$.

Dokaz. Uz korištenje formule (3.1), ovo je izravna posljedica Kineskog teorema o ostacima i Dirichletovog teorema o aritmetičkom nizu, primijenjenima na proste brojeve koji zadovoljavaju uvjete iz Teorema 3.3. □

Teorem 3.5. *Neka je p prost broj koji zadovoljava $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$ i $\left(\frac{p}{5}\right) = -1$. Tada je* $\operatorname{rank}(X_0^{(p)}(15)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-p)}(15)(\mathbb{Q})) = 0$.

Dokaz. Iz [66] dobivamo da je eksplicitni model od $X_0(15)$ zadan jednadžbom

$$y^2 + xy + y = x^3 + x^2 - 10x - 10. \tag{3.6}$$

Kako bismo dokazali teorem, koristit ćemo metodu spusta s 2-izogenijama. Dakle, moramo transformirati (3.6) iz Weierstrassovog oblika u oblik $y^2 = x^3 + ax^2 + bx$, prikladan za primjenu ove metode. Računamo $b_2 = a_1^2 + 4a_2 = 5, b_4 = a_1a_3 + 2a_4 = -19$ i $b_6 = a_3^2 + 4a_6 = -39$, pa je x_0 korijen od $x^3 + 5x^2 - 152x - 624 = 0$. Lako se provjeri da $x_0 = 12$ zadovoljava posljednju jednadžbu. Dakle, $a = 3x_0 + b_2 = 41$, $b = (a + b_2)x_0 + 8b_4 = 400$. Konačno, dobivamo sljedeće krivulje (označimo $E(n)$ umjesto $X_0^{(n)}(15)(\mathbb{Q})$ i s $E'(n)$ krivulju koja je 2-izogena s $E(n)$):

$$\begin{aligned} E(p) : y^2 &= x^3 + 41px^2 + 400p^2x, \\ E'(p) : y^2 &= x^3 - 82px^2 + 81p^2x, \\ E(-p) : y^2 &= x^3 - 41px^2 + 400p^2x, \\ E'(-p) : y^2 &= x^3 + 82px^2 + 81p^2x. \end{aligned}$$

Ideja dokaza je pronaći veličinu pridružene ψ-Selmerove grupe za krivulje $E(p)$ i $E(-p)$, odnosno veličinu ϕ-Selmerove grupe za krivulje $E'(p)$ i $E'(-p)$, iz čega ćemo posljedično izračunati i rang. Naime, ukoliko dobijemo da je umnožak redova odgovarajuće ψ-Selmerove i ϕ-Selmerove grupe jednak 4, tada izravno iz formule (3.5) slijedi i da je traženi rang jednak nuli.

1. $E(p) : y^2 = x^3 + 41px^2 + 400p^2x$

   Pogledat ćemo rješivost kvartike (torzora) $N^2 = b_1M^4 + 41pM^2e^2 + b_2e^4$ uz $b_1b_2 = 400p^2$, uzevši u obzir $\gcd(M, e) = 1$ i pretpostavljajući bez smanjenja općenitosti da je b_1 kvadratno slobodan. Dakle, $b_1 \in \{\pm 1,\ \pm 2,\ \pm 5,\ \pm 10,\ \pm p,\ \pm 2p,\ \pm 5p,\ \pm 10p\}$. Jedna očita vrijednost za koju postoji rješenje je $b_1 = 1$, ali i za $b_1 = -p$ također postoji rješenje; u ovom slučaju je naime $(M, e, N) = (5, 1, 0)$. Provjerit ćemo sada ostale moguće vrijednosti od b_1.

   1.1. $b_1 = -1$

   Torzor postaje $N^2 = -M^4 + 41pM^2e^2 - 400p^2e^4$. Redukcijom modulo 3 i uočavanjem da je $p \equiv 2 \pmod 3$, dobivamo $N^2 \equiv -M^4 + M^2e^2 - e^4 \equiv 2 \pmod 3$, a to nije kvadratni ostatak modulo 3. Dakle, $-1 \notin S_\psi(E(p))$.

1.2. $b_1 = 2$

Promatramo jednadžbu

$$N^2 = 2M^4 + 41pM^2e^2 + 200p^2e^4. \tag{3.7}$$

Kad je e paran i M neparan, desna strana od (3.7) je kongruentna 2 modulo 4, a to je u kontradikciji s lijevom stranom. Ako su oba M i e neparni, onda $N^2 \equiv 2 + p \equiv 7 \pmod 8$, a to nije moguće. Preostaje nam samo slučaj kada je M paran i e neparan. Tada je N također paran, pa možemo uzeti $M = 2t, N = 2N'$ i transformirati (3.7) u $N'^2 = 8t^4 + 41pt^2e^2 + 50p^2e^4$. Redukcijom modulo 4 dobivamo $N'^2 = pt^2 + 2p^2 \equiv 2, 3 \pmod 4$, ali to je nemoguće, pa $2 \notin S_\psi(E(p))$.

1.3. $b_1 = 2p$

Torzor je

$$N^2 = p(2M^4 + 41M^2e^2 + 200e^4). \tag{3.8}$$

Kada je e paran i M neparan, desna strana od (3.8) je kongruentna 2 modulo 4. Kad bi oba M i e bili neparni, desna strana je kongruentna $3p$ modulo 4, odnosno 3 modulo 4, a to nije kvadratni ostatak modulo 4. Ako je M paran i e neparan, možemo uzeti $M = 2t$, pa je tada $N^2 = p(32t^4 + 164t^2e^2 + 200e^4)$. Uzevši $N = 2N'$ i dijeljenjem obje strane s 4, dobivamo $N'^2 = p(8t^4 + 41t^2e^2 + 50e^4)$, što daje $N'^2 \equiv p(2 + t^2) \equiv 2, 6, 7 \pmod 8$, a to je nemoguće, što povlači $2p \notin S_\psi(E(p))$.

1.4. $b_1 = -5$

U ovom slučaju torzor je $N^2 = -5M^4 + 41pM^2e^2 - 80p^2e^4$. Ovdje ćemo promatrati kongruencije modulo 5 zato jer je desna strana kongruentna pM^2e^2 modulo 5. Budući da je lijeva strana kvadrat, te $\left(\frac{p}{5}\right) = -1$, jedine moguće opcije su ili $5|M$ ili $5|e$. U oba slučaja dobivamo kao posljedicu i $5|N$, pa je lijeva strana djeljiva ne samo s 5, već i s 25, te mora biti i desna. Ako $5|e$, onda zbog djeljivosti desne strane s 25 slijedi $5|M^4$, odnosno $5|M$, a to je nemoguće jer je $\gcd(M, e)$=1. Analogno dokazujemo i za slučaj $5|M$. Dakle, $-5 \notin S_\psi(E(p))$.

1.5. $b_1 = 5$

Torzor postaje $N^2 = 5M^4 + 41pM^2e^2 + 80p^2e^4$. Zaključujući na isti na način kao u slučaju $b_1 = -5$ i uzimajući u obzir da 5 nije kvadratni ostatak

modulo 25, dobivamo $5 \notin S_\psi(E(p))$.

1.6. $b_1 = 10$

Torzor je

$$N^2 = 10M^4 + 41pM^2e^2 + 40p^2e^4. \tag{3.9}$$

U ovom slučaju promatrat ćemo parnost od M i e. Kada je e paran, a M neparan, N^2 je kongruentan 2 modulo 4, a ako su oba neparna, onda $N^2 \equiv p + 2 \equiv 3 \pmod 4$. Preostaje nam samo analizirati slučaj kad je M paran i e neparan; pretpostavimo da je $M = 2t$. Jednadžba (3.9) postaje $N^2 = 160t^4 + 164pt^2e^2 + 40p^2e^4$. Uzimajući $N = 2N'$ i dijeljenjem obje strane s 4, dobivamo $N'^2 = 40t^4 + 41pt^2e^2 + 10p^2e^4$, što pak daje $N'^2 \equiv p(t^2 + 2p) \equiv 2, 3 \pmod 4$, a to je nemoguće. Stoga, $10 \notin S_\psi(E(p))$.

1.7. $b_1 = 10p$

Promatramo jednadžbu $N^2 = p(10M^4 + 41M^2e^2 + 40e^4)$. Zaključivanjem na isti način kao u slučaju $b_1 = 10$, dobivamo $N^2 \equiv 2p \equiv 2 \pmod 4$ za paran e i neparan M, odnosno $N^2 \equiv 3p \equiv 3 \pmod 4$ za oba e i M neparna. Uzimajući neparan e, $M = 2t$ te $N = 2N'$ dobivamo $N'^2 \equiv p(2 + t^2) \equiv 2, 3 \pmod 4$, što implicira $10p \notin S_\psi(E(p))$.

$S_\psi(E(p))$ je grupa, iz čega slijedi $p,\ -2p,\ -2,\ 5p,\ -5p,\ -10p,\ -10 \notin S_\psi(E(p))$. Naime, ako je primjerice $5p \in S_\psi(E(p))$, onda bismo zbog $-p \in S_\psi(E(p))$ imali $-p \cdot 5p = -5 \in S_\psi(E(p))$, a to smo već pokazali da ne vrijedi. Slijedi dakle $\#S_\psi(E(p)) = 2$.

2. $E'(p) : y^2 = x^3 - 82px^2 + 81p^2x$

Promatranjem torzora $N^2 = b_1M^4 - 82pM^2e^2 + b_2e^4$ uz $b_1b_2 = 81p^2$, jednostavno dobivamo da $b_1 = 1$ i $b_1 = p$ daju rješenja $(1, 0, 1)$ i $(1, 1, 0)$. Negativne vrijednosti za b_1 nisu moguće jer je u tom slučaju desna strana torzora negativna pa ne može biti kvadrat. Preostaje još samo jedan slučaj, $b_1 = 3$ (eliminacija tog slučaja automatski povlači i eliminaciju slučaja $b_1 = 3p$ zato jer je $S_\phi(E'(p))$ grupa). Reduciranjem torzora $N^2 = 3M^4 - 82pM^2e^2 + 27p^2e^4$ modulo p, dobivamo $N^2 \equiv 3M^4 \pmod p$. Zbog $p \equiv 2 \pmod 3$ i $p \equiv 1 \pmod 4$, iz zakona kvadratnog reciprociteta slijedi da $\left(\frac{3}{p}\right) = -1$, što implicira $p|M$ i $p|N$. Stavljanjem $M = pt$ i $N = pk$ jednakost postaje $k^2 = 3p^2t^4 - 82pt^2e^2 + 27e^4$, što još jednom redukcijom modulo p daje $k^2 \equiv 27e^4 \pmod p$. M i e su relativno prosti pa e ne može biti djeljiv s p, a 3 nije kvadratni ostatak modulo p. Dakle $3 \notin S_\phi(E'(p))$ i $3p \notin S_\phi(E'(p))$, što povlači $\#S_\phi(E'(p)) = 2$

i $\text{rank}(X_0^{(p)}(15)(\mathbb{Q})) = 0$.

3. $E(-p) : y^2 = x^3 - 41px^2 + 400p^2x$

Torzor je $N^2 = b_1M^4 - 41pM^2e^2 + b_2e^4$ uz $b_1b_2 = 400p^2$. Moguće vrijednosti od b_1 su $\{1, 2, 5, p, 2p, 5p, 10p, 10\}$ (za negativne vrijednosti desna strana je negativna). Osim $b_1 = 1$, $b_1 = p$ je također element od $S_\psi(E(-p))$, zato jer je u tom slučaju $(M, e, N) = (5, 1, 0)$ rješenje. Pokažimo da ostale vrijednosti od b_1 ne vode do rješenja.

3.1. $b_1 = 2$

Torzor je $N^2 = 2M^4 - 41pM^2e^2 + 200p^2e^4$. Kada je e paran i M neparan, onda $N^2 \equiv 2 \pmod 4$, a kad su oba M i e neparna, $N^2 \equiv 2 - p \equiv 5 \pmod 8$. Ako je e neparan, $M = 2t$ i $N = 2N'$ dobivamo $N'^2 \equiv 2p^2 - pt^2 \equiv 2, 5, 6 \pmod 8$, što povlači $2 \notin S_\psi(E(-p))$.

3.2. $b_1 = 5p$

Torzor je $N^2 = p(5M^4 - 41M^2e^2 + 80e^4)$. Redukcijom modulo 5 dobivamo $N^2 \equiv 4pM^2e^2 \pmod 5$, što povlači da je ili $5|M$ ili $5|e$. Naime, zbog $\left(\frac{p}{5}\right) = -1$ slijedi da je $\left(\frac{4p}{5}\right) = -1$. U oba slučaja dobivamo da je lijeva strana torzora djeljiva s 25, pa mora biti i desna, a to je moguće samo ako su oba M i e djeljivi s 5. Kontradikcija, $5p \notin S_\psi(E(-p))$.

3.3. $b_1 = 10$

Torzor je $N^2 = 10M^4 - 41pM^2e^2 + 40p^2e^4$. Redukcija modulo 4 i modulo 8 jednostavno eliminira slučajeve kad je e paran i M neparan, te kad su oba M i e neparna. Ako je e neparan, $M = 2t$ i $N = 2N'$, onda $N'^2 = 40t^4 - 41pt^2e^2 + 10p^2e^4 \equiv 2p^2 - pt^2 \equiv 2, 5, 6 \pmod 8$, iz čega je $10 \notin S_\psi(E(-p))$.

Vrijedi $2p,\ 5,\ 10p \notin S_\psi(E(-p))$, stoga $\#S_\psi(E(-p)) = 2$.

4. $E'(-p) : y^2 = x^3 + 82px^2 + 81p^2x$

Ispitat ćemo kvartiku $N^2 = b_1M^4 + 82pM^2e^2 + b_2e^4$ uz $b_1b_2 = 81p^2$. Vrijednost od b_1 može biti jedan od elemenata iz $\{\pm 1,\ \pm 3,\ \pm p,\ \pm 3p\}$, a za $b_1 = 1$ i $b_1 = -p$ postoje rješenja $(M, e, N) = (1, 0, 1)$ i $(M, e, N) = (1, 1, 0)$.

4.1. $b_1 = 3$

Torzor je $N^2 = 3M^4 + 82pM^2e^2 + 27p^2e^4$. Kombiniranjem redukcije modulo p i

činjenice $\left(\frac{3}{p}\right) = -1$ (do koje smo došli prilikom proučavanja ϕ-Selmerove grupe od $E'(p)$), dobivamo $p|M$ i $p|N$. Međutim, redukcijom torzora modulo p još jednom, to povlači $\left(\frac{3}{p}\right) = 1$, što je kontradikcija. Stoga, $3 \notin S_\phi(E'(-p))$.

4.2. $b_1 = -1$

Jednadžba koju promatramo $N^2 = -M^4 + 82pM^2e^2 - 81p^2e^4$. Kada je e paran i M neparan, $N^2 \equiv -M^4 \equiv 7 \pmod 8$, što nije moguće. Slično, kad je M paran i e neparan dobivamo $N^2 \equiv -p^2e^4 \equiv 7 \pmod 8$. Kad su oba neparna, možemo uzeti $M^2 = 8a+1, p = 8b+5$ i $e^2 = 8c+1$, pa torzor postaje $N^2 = -64a^2 + 9216abc + 1152ab + 5760ac + 704a - 69632b^2c^2 - 17408b^2c - 1088b^2 - 87040bc^2 - 20608bc - 1216b - 27200c^2 - 6080c - 336$. Promatranjem kongruencija modulo 64 imamo $N^2 \equiv 48 \pmod{64}$, a to je nemoguće, stoga $-1 \notin S_\phi(E'(-p))$.

4.3. $b_1 = 3p$

U ovom završnom slučaju, torzor je $N^2 = p(3M^4 + 82M^2e^2 + 27e^4)$. Slučajevi kad je M paran i e neparan (i obratno) daju $N^2 \equiv 7 \pmod 8$. Ako su oba M i e neparni, tada uvrštavanje $M^2 = 8a+1, e^2 = 8b+1$ daje $N^2 \equiv p\,(8 + 64(3a^2 + 2ab + a + 3b^2 + b)) \equiv 40 \pmod{64}$, što je nemoguće, pa $3p \notin S_\phi(E'(-p))$.

Ostale moguće vrijednosti od b_1 $(-3p,\ p,\ -3)$ također nisu u $S_\phi(E'(-p))$ zato jer je $S_\phi(E'(-p))$ grupa, stoga $\#S_\phi(E'(-p)) = 2$. S obzirom da je i $\#S_\psi(E(-p)) = 2$, zaključujemo da je $\operatorname{rank}(X_0^{(-p)}(15)(\mathbb{Q})) = 0$.

□

Da je idući korolar posljedica Teorema 3.5 dokazujemo jednako kao što smo dokazali da je Korolar 3.4 posljedica Teorema 3.3:

Korolar 3.6. *Postoji beskonačno mnogo prostih brojeva p takvih da za $K = \mathbb{Q}(i, \sqrt{p})$ vrijedi* $\operatorname{rank}(X_0(15)(K)) = 0$.

Dobili smo i jedan rezultat o modularnim krivuljama $X_1(n)$. Naime, sljedeći korolar je izravna posljedica Teorema 3.5 i činjenica da su $X_0(15)$ i $X_1(15)$ izogene:

Korolar 3.7. *Postoji beskonačno mnogo prostih brojeva p takvih da za $K = \mathbb{Q}(i, \sqrt{p})$ vrijedi* $\operatorname{rank}(X_1(15)(K)) = 0$.

3.4 Slučajevi $n = 20$, $n = 21$ i $n = 49$

U dokazima nekih od narednih teorema trebat će nam pojam kompleksnog množenja i činjenice povezane s krivuljama koje ga imaju.

Definicija 3.11. Prsten endomorfizama eliptičke krivulje E, oznaka $\mathrm{End}(E)$, sastoji se od svih izogenija s E na samu sebe.

Definicija 3.12. Eliptička krivulja ima kompleksno množenje ako joj je prsten endomorfizama veći od prstena cijelih brojeva $\mathbb{Z}$.

Promatrajući nad poljem karakteristike 0, prsten endomorfizama eliptičke krivulje E može biti ili $\mathbb{Z}$ (tada se sastoji od svih množenje-s-n izogenija $[n]$) ili red u kvadratnom imaginarnom polju K (tada E ima kompleksno množenje). Ono što je za nas bitno jest da ako eliptička krivulja ima kompleksno množenje, onda je izogena svom kvadratnom zakretu nad $\mathbb{Q}$, što posljedično daje da krivulje imaju isti rang. Naime, ako krivulja ima kompleksno množenje, to znači je da je izogena (nad algebarskim zatvorenjem od $\mathbb{Q}$) sama sa sobom kroz neku cikličku izogeniju (vidi npr. [**61, Chapter 2**]). Međutim, ova tvrdnja vrijedi samo nad poljem algebarskih brojeva koje sadrži K, odnosno dobivamo da je krivulja izogena svojem zakretu nad $\mathbb{Q}$, i to točno kvadratnom zakretu s d, gdje je d diskriminanta prstena s kojim krivulja ima kompleksno množenje. Poznato je (vidi npr. [**62, A §3**]) da postoji 13 klasa $\overline{\mathbb{Q}}$-izomorfizama, tj. j-invarijanti eliptičkih krivulja definiranih nad $\mathbb{Q}$ s kompleksnim množenjem. Tablica 3.1 daje predstavnika eliptičke krivulje nad $\mathbb{Q}$ za svaku od klasa, odnosno eliptičku krivulju s kompleksnim množenjem. U tablici D označava diskriminantu kvadratnog polja $\mathbb{Q}(\sqrt{D})$ u kojem se nalazi prsten endomorfizama, a f konduktor.

D	f	j-invarijanta	Kratka Weierstrassova forma
-3	1	0	$y^2 = x^3 + 16$
-3	2	$2 \cdot 30^3$	$y^2 = x^3 - 15x + 22$
-3	3	$-3 \cdot 160^3$	$y^2 = x^3 - 480x + 4048$
-4	1	12^3	$y^2 = x^3 + x$
-4	2	66^3	$y^2 = x^3 - 11x + 14$
-7	1	-15^3	$y^2 = x^3 - 2835x - 71442$
-7	2	255^3	$y^2 = x^3 - 595x + 5586$
-8	1	20^3	$y^2 = x^3 - 4320x + 96768$
-11	1	-2^{15}	$y^2 = x^3 - 9504x + 365904$
-19	1	-96^3	$y^2 = x^3 - 608x + 5776$
-43	1	-960^3	$y^2 = x^3 - 13760x + 621264$
-67	1	-5280^3	$y^2 = x^3 - 117920x + 15585808$
-163	1	-640320^3	$y^2 = x^3 - 34790720x + 78984748304$

Tablica 3.1
Klase izomorfizama eliptičkih krivulja definiranih nad $\mathbb{Q}$ s kompleksnim množenjem

Za praktičnu primjenu potrebno je dakle izračunati j-invarijantu zadane krivulje i provjeriti postoji li u Tablici 3.1 krivulja s istom vrijednošću j-invarijante. Zgodno je i upotrijebiti funkciju HasComplexMultiplication() iz programskog paketa Magma [3]. Napomenimo da isti paket ima još jednu izrazito korisnu funkciju koja odmah daje informaciju jesu li dvije krivulje izogene, IsIsogenous().

Teorem 3.8. *Neka je p prost broj koji zadovoljava $p \equiv 3 \pmod 4$ i $\left(\frac{p}{5}\right) = -1$. Tada je* $\operatorname{rank}(X_0^{(p)}(20)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-p)}(20)(\mathbb{Q})) = 0$.

Dokaz. Eksplicitni model od $X_0(20)$ je $y^2 = (x+1)(x^2+4)$ (vidi [66]), iz čega lako dobijemo krivulje koje treba analizirati:

$$E(p) : y^2 = x^3 - 2px^2 + 5p^2x, \tag{3.10}$$
$$E'(p) : y^2 = x^3 + px^2 - p^2x, \tag{3.11}$$
$$E(-p) : y^2 = x^3 + 2px^2 + 5p^2x, \tag{3.12}$$
$$E'(-p) : y^2 = x^3 - px^2 - p^2x. \tag{3.13}$$

Dobivene krivulje jednostavnim transformacijama sveli smo u oblik s jednostavnijim koeficijentima. Krivulju $E(p)$ smo u ovom obliku dobili zamjenom $x \mapsto x - 1$ nad eksplicitnim modelom. Nadalje, iz takvog $E(p)$ dobijemo $E'(p)$ koji originalno glasi

$$E'(p) : y^2 = x^3 + 4px^2 - 16p^2x, \tag{3.14}$$

ali ako na bilo koju krivulju oblika

$$y^2 = x^3 + ax^2 + bx$$

primijenimo jednostavnu supstituciju $x \mapsto xu^2$, $y \mapsto yu^3$ dobivamo izomorfnu krivulju u kojoj koeficijente transformiramo kao $a \mapsto au^2, b \mapsto bu^4$. Kako u ovom slučaju imamo $u = 2$, običnim dijeljenjem a i b iz (3.14) s 4, odnosno 16, dobivamo (3.11). Istu transformaciju učinimo i nad krivuljom $E'(-p)$.

1. $E(p) : y^2 = x^3 - 2px^2 + 5p^2x$

   Torzor je u ovom slučaju $N^2 = b_1M^4 - 8pM^2e^2 + b_2e^4$ gdje $b_1b_2 = 5p^2$. Očito je da $1, 5 \in S_\psi(E(p))$ te da negativne vrijednosti od b_1 impliciraju negativne vrijednosti desne strane torzora. Promatranjem ostataka pri dijeljenju s potencijama od 2 (slično kao u slučajevima 1.2. i 3.3. u dokazu Teorema 3.5) i uzimanjem u obzir pretpostavke $p \equiv 3 \pmod 4$, lako slijedi da $p \notin S_\psi(E(p))$. Kako je $S_\psi(E(p))$ grupa, $5p \notin S_\psi(E(p))$ također, stoga $\#S_\psi(E(p)) = 2$.

2. $E'(p) : y^2 = x^3 + px^2 - p^2x$

   Torzor je $N^2 = b_1M^4 + 16pM^2e^2 + b_2e^4$, $b_1b_2 = -p^2$. Za $b_1 = -1$ i $b_1 = 1$ torzor ima cjelobrojnih rješenja, a za ostale vrijednosti od b_1 nema. Naime, slučaj $b_1 = p$ je eliminiran redukcijom modulo 5 zato što $\left(\frac{p}{5}\right) = -1$, a $b_1 = -p$ eliminiramo činjenicom da je $S_\phi(E'(p))$ grupa, stoga $\#S_\phi(E'(p)) = 2$ i $\text{rank}(X_0^{(p)}(20)(\mathbb{Q})) = 0$.

3. $E(-p) : y^2 = x^3 + 2px^2 + 5p^2x$

   Torzor je $N^2 = b_1M^4 + 8pM^2e^2 + b_2e^4$, $b_1b_2 = 5p^2$, pa $1, 5 \in S_\psi(E(-p))$. Za negativne vrijednosti od b_1 desna strana je negativna pa ne može biti kvadrat, a slučaj $b_1 = p$ eliminiramo redukcijom po modulu potencije od 2. $S_\psi(E(-p))$ je grupa, stoga $\#S_\psi(E(-p)) = 2$.

4. $E'(-p) : y^2 = x^3 - px^2 - p^2x$

   Ovaj slučaj se riješi na isti način kao i (3.11), pa ćemo ga preskočiti. Slijedi da je $\text{rank}(X_0^{(-p)}(20)(\mathbb{Q})) = 0$, te je tvrdnja dokazana.

□

Iz Teorema 3.8 lako dokažemo idući korolar:

Korolar 3.9. *Postoji beskonačno mnogo prostih brojeva p takvih da za $K = \mathbb{Q}(i, \sqrt{p})$ vrijedi* $\text{rank}(X_0(20)(K)) = 0$.

Teorem 3.10. *Neka je p prost broj koji zadovoljava $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$, te $\left(\frac{p}{7}\right) = 1$. Tada je* $\text{rank}(X_0^{(p)}(21)(\mathbb{Q})) = \text{rank}(X_0^{(-3p)}(21)(\mathbb{Q})) = 0$.

Dokaz. Da bismo transformirali eksplicitni model od $X_0(21)$, $y^2 + xy = x^3 - 4x - 1$ (kojeg pronađemo u [**66**]), u oblik u kojem je $(0, 0)$ točka reda 2, potrebno je pronaći cjelobrojni korijen polinoma $x^3 + x^2 - 64x - 64$. Za razliku od ostalih dokaza teorema iz ovog poglavlja u kojima smo prilikom transformacije dobivali polinome sa samo jednim cjelobrojnim korijenom, ovaj polinom ima tri različita cjelobrojna korijena, pa smo odabrali $x_0 = 8$. Iz toga dobivamo krivulje:

$$\begin{aligned} E(p) : y^2 &= x^3 + 25px^2 + 144p^2x, \\ E'(p) : y^2 &= x^3 - 50px^2 + 49p^2x, \\ E(-3p) : y^2 &= x^3 - 75px^2 + 1296p^2x, \\ E'(-3p) : y^2 &= x^3 + 150px^2 + 441p^2x. \end{aligned}$$

1. $E(p) : y^2 = x^3 + 25px^2 + 144p^2x$

Kvartika koju ovdje promatramo je

$$N^2 = b_1M^4 + 25pM^2e^2 + b_2e^4.$$

Vidimo da su moguće vrijednosti od b_1 iz skupa $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm p, \pm 2p, \pm 3p, \pm 6p\}$. Očito, $b_1 = 1$ daje cjelobrojno rješenje, ali i vrijednost $b_1 = -p$ također daje cjelobrojno rješenje: $(M, e, N) = (4, 1, 0)$. Preostale slučajeve eliminiramo kako slijedi.

1.1. $b_1 = 2$

Torzor je $N^2 = 2M^4 + 25pM^2e^2 + 72p^2e^4$. Budući da je diskriminanta polinoma na desnoj strani potpun kvadrat, isti možemo faktorizirati kao

$$N^2 = (M^2 + 8pe^2)(2M^2 + 9pe^2). \tag{3.15}$$

Ako s a označimo najveći zajednički djeljitelj faktora na desnoj strani od (3.15), onda se množenjem prvog faktora s 2 i oduzimanjem drugog faktora lako vidi da je $a \in \{1, 7\}$ (prisjetimo se, M i e moraju biti relativno prosti pa a ne dijeli e, jer bi onda dijelio i M). Dakle, moguća su dva sustava jednadžbi:

$$\begin{aligned} M^2 + 8pe^2 &= \square, \\ 2M^2 + 9pe^2 &= \square, \end{aligned}$$

odnosno

$$\begin{aligned} M^2 + 8pe^2 &= 7\square, \\ 2M^2 + 9pe^2 &= 7\square. \end{aligned}$$

Uočimo da se redukcijom po modulu 3 oba sustava svode na isti, a uz $p \equiv 1 \pmod 3$ taj sustav lako eliminiramo. Naime, ako $3 \nmid M$, onda bi u drugoj jednadžbi 2 morao biti kvadratni ostatak po modulu 3, što očito nije istina. Ako pak $3|M$, onda $3 \nmid e$, pa u prvoj jednadžbi dobivamo da 2 mora biti kvadratni ostatak modulo 3, što također nije moguće. Zaključujemo $2 \notin S_\psi(E(p))$, a zbog grupoidnosti i činjenice $-p \in S_\psi(E(p))$, onda i $-2p \notin S_\psi(E(p))$.

1.2. $b_1 = 3$

Torzor je $N^2 = 3M^4 + 25pM^2e^2 + 48p^2e^4$. Ovaj slučaj eliminirat ćemo korištenjem $p \equiv 3 \pmod 4$ i promatranjem kongruencija po modulu potencije od 2. Ako su M i e oba neparni, tada je $N^2 \equiv 3 + p \equiv 2 \pmod 4$, što je nemoguće. Ako je e paran, a M neparan, onda je $N^2 \equiv 3 \pmod 4$, također nemoguće.

Preostaje slučaj kad je M paran, a e neparan. Ako označimo $M = 2t$, tada i N mora biti paran pa uzmemo $N = 2l$ i dobivamo $l^2 = 12t^2 + 25pt^2e^2 + 12p^2e^4$. Ako je t neparan, onda je $l^2 \equiv p \equiv 3 \pmod 4$, pa preostaje još gledati slučaj kad je t paran. Označimo $t = 2t'$, $l = 2l'$ (l također mora biti paran) i konačno dobivamo $l'^2 = 48t'^2 + 25pt'^2e^2 + 3p^2e^4$, odnosno $l'^2 \equiv 3(t'^2 + 1) \pmod 4$, što daje $l'^2 \equiv 2, 3 \pmod 4$, a nijedan od ta dva slučaja nije moguć. Dakle, $3 \notin S_\psi(E(p))$, a posljedično i $-3p \notin S_\psi(E(p))$.

1.3. $b_1 = 6$

Torzor je $N^2 = 6M^4 + 25pM^2e^2 + 24p^2e^4$, pa ga faktoriziramo kao

$$N^2 = (3M^2 + 8pe^2)(2M^2 + 3pe^2). \tag{3.16}$$

Slično kao u slučaju 1.1, ustanovimo da je najveći zajednički djeljitelj faktora na desnoj strani ili 1, ili p, ili 7, ili $7p$. Dobivamo sustave jednadžbi oblika

$$\begin{aligned} 3M^2 + 8pe^2 &= a\square, \\ 2M^2 + 3pe^2 &= a\square, \end{aligned}$$

gdje smo s a označili $\gcd(3M^2 + 8pe^2,\ 2M^2 + 3pe^2)$. Sva ova četiri sustava redukcijom po modulu 3 svode se na isti i uz $p \equiv 1 \pmod 3$ lako eliminiraju. Ako $3|M$, onda $3 \nmid e$, pa u prvoj jednadžbi dobivamo da 2 mora biti kvadratni ostatak pri dijeljenju s 3. Ako pak $3 \nmid M$, onda istu stvar zaključujemo u drugoj jednadžbi. Dakle, $6 \notin S_\psi(E(p))$, a iz toga i $-6p \notin S_\psi(E(p))$.

1.4. $b_1 = p$

Torzor je $N^2 = pM^4 + 25pM^2e^2 + 144pe^4$. Ovaj slučaj eliminiramo promatranjem kongruencija modulo potencije od 2, na identični način kao i slučaj 1.2. Dobivamo $p \notin S_\psi(E(p))$, a zbog grupoidnosti i $-1 \notin S_\psi(E(p))$.

1.5. $b_1 = 2p$

Torzor je $N^2 = 2pM^4 + 25pM^2e^2 + 72pe^4$, i faktoriziramo ga kao

$$N^2 = p(2M^2 + 9e^2)(M^2 + 8e^2). \tag{3.17}$$

Faktori na desnoj strani od (3.17) imaju najveći zajednički djeljitelj 1 ili 7, pa dobivamo sustave jednadžbi

$$2M^2 + 9e^2 = ap\square,$$

$$M^2 + 8e^2 = a\square,$$

odnosno

$$\begin{aligned} 2M^2 + 9e^2 &= a\square, \\ M^2 + 8e^2 &= ap\square, \end{aligned}$$

gdje je $a \in \{1, 7\}$. Svi ovi sustavi se redukcijom modulo 3, uz $p \equiv 1 \pmod 3$, svode na isti. Taj sustav lako eliminiramo promatranjem slučajeva $3 \nmid M$ (prva jednadžba), odnosno $3|M,\ 3 \nmid e$ (druga jednadžba). Dakle, $2p \notin S_\psi(E(p))$, pa je i $-2 \notin S_\psi(E(p))$.

1.6. $b_1 = 3p$

Torzor je $N^2 = 3pM^4 + 25pM^2e^2 + 48pe^4$. Ova jednadžba ekvivalentna je jednadžbi

$$(6M^2 + 25e^2)^2 - 49e^4 = 12p\square, \tag{3.18}$$

u kojoj ćemo promatrati ostatke pri dijeljenju sa 7. Iz pretpostavke $\left(\frac{p}{7}\right) = 1$ zaključujemo da je desna strana od (3.18) ili djeljiva sa 7 ili daje kvadratni neostatak pri dijeljenju sa 7. Međutim, na lijevoj strani redukcija modulo 7 ostavlja samo potpun kvadrat $(6M^2 + 25e^2)^2$, pa mora vrijediti

$$7 \mid 6M^2 + 25e^2. \tag{3.19}$$

Zapišimo torzor kao

$$N^2 = p(M^2 + 3e^2)(3M^2 + 16e^2).$$

Najveći zajednički djeljitelj faktora na desnoj strani može biti ili 1 ili 7. Iz (3.19) zaključujemo da $7|M^2 + 3e^2$ i $7|3M^2 + 16e^2$, pa je onda nužno $\gcd(M^2 + 3e^2,\ 3M^2 + 16e^2) = 7$. Iz toga dobivamo sustave jednadžbi

$$\begin{aligned} M^2 + 3e^2 &= 7p\square, \\ 3M^2 + 16e^2 &= 7\square, \end{aligned}$$

odnosno

$$\begin{aligned} M^2 + 3e^2 &= 7\square, \\ 3M^2 + 16e^2 &= 7p\square. \end{aligned}$$

Uz pretpostavku $p \equiv 3 \pmod 4$ oba sustava eliminiramo redukcijom modulo

potencije od 2. Ako je M paran, iz prve jednadžbe prvog sustava dobivamo da 3 mora biti kvadratni ostatak modulo 4, što je nemoguće. Ako je M neparan, onda je lijeva strana druge jednadžbe kongruentna 3 modulo 8, što je kontradikcija s desnom stranom. Pogledajmo sada drugi sustav. Ako je M neparan, onda iz druge jednadžbe drugog sustava dobivamo da 3 mora biti kvadratni ostatak modulo 4, što je nemoguće. Ako je M paran, onda e mora biti neparan. U slučaju kad je M djeljiv s 4, onda je lijeva strana prve jednadžbe kongruentna 3 modulo 8, što je kontradikcija s desnom stranom. Ako je pak M djeljiv s 2, ali ne i s 4, onda lijeva strana druge jednadžbe daje ostatak 12 pri dijeljenju sa 16, a desna strana ne može dati taj ostatak. Prema tome, $3p \notin S_\psi(E(p))$, te $-3 \notin S_\psi(E(p))$.

1.7. $b_1 = 6p$

Torzor je $N^2 = 6pM^4 + 25pM^2e^2 + 24pe^4$, i faktoriziramo ga kao

$$N^2 = p(3M^2 + 8e^2)(2M^2 + 3e^2).$$

Ovaj slučaj eliminiramo na isti način kao i slučaj 1.5., pa nećemo ponavljati dokaz. Dobiva se $6p \notin S_\psi(E(p))$, odnosno $-6 \notin S_\psi(E(p))$.

Analizom slučajeva 1.1. - 1.7. eliminirali smo sve preostale moguće vrijednosti od b_1. Dakle, $\#S_\psi(E(p)) = 2$.

2. $E'(p) : y^2 = x^3 - 50px^2 + 49p^2x$

Samo su četiri moguće vrijednosti od b_1 u ovom slučaju: $\{1, 7, p, 7p\}$. Za $b_1 = 1$ i $b_1 = p$ postoje rješenja $(1, 0, 1)$ i $(1, 1, 0)$, dok su slučajevi $b_1 = 7$ i $b_1 = 7p$ eliminirani redukcijom modulo 7 zbog $\left(\frac{p}{7}\right) = 1$. Zaključujemo da je $\#S_\phi(E'(p)) = 2$, te posljedično $\text{rank}(X_0^{(p)}(21)(\mathbb{Q})) = 0$.

3. $E(-3p) : y^2 = x^3 - 75px^2 + 1296p^2x$

Osim $b_1 = 1$, vrijednost $b_1 = 3p$ također daje cjelobrojno rješenje $(M, e, N) = (4, 1, 0)$ odgovarajućeg torzora. Negativne vrijednosti od b_1 odmah eliminiramo, pa nam preostaju slučajevi kad je $b_1 \in \{2, 3, 6, p, 2p, 6p\}$. Vrijednosti $b_1 = 2$ i $b_1 = 2p$ vode na kontradikciju promatranjem ostataka modulo 3, pri čemu nam za potonju vrijednost dodatno treba i pretpostavka $p \equiv 1 \pmod 3$. Slučaj $b_1 = 3$ eliminiramo redukcijom modulo potencije od 2. Budući da je $S_\psi(E(-3p))$ grupa, preostali slučajevi također ne daju cjelobrojna rješenja torzora. Dakle, $\#S_\psi(E(-3p)) = 2$.

4. $E'(-3p) : y^2 = x^3 + 150px^2 + 441p^2x$

Vrijednosti $b_1 = 1$ i $b_1 = -3p$ daju cjelobrojna rješenja pripadnog torzora, potonja $(M, e, N) = (1, 1, 0)$. Kada je $b_1 = -1$ ili $b_1 = -7$, dobivamo kontradikciju po modulu 3 za sve vrijednosti od p. Za $b_1 = -p$ i $b_1 = -7p$ dodatno koristimo uvjet $p \equiv 1 \pmod 3$. Vrijednost $b_1 = -3$ je eliminirana redukcijom modulo 32, a vrijednosti $b_1 = -21$ i $b_1 = -21p$ redukcijom modulo 7 i korištenjem pretpostavke $\left(\frac{p}{7}\right) = 1$. Svi ostali slučajevi eliminirani su činjenicom da je $S_\phi(E'(-3p))$ grupa, što povlači $\#S_\phi(E'(-3p)) = 2$ i konačno $\operatorname{rank}(X_0^{(-3p)}(21)(\mathbb{Q})) = 0$.

□

Kao i u ostalim slučajevima, Teorem 3.10 također implicira idući korolar:

Korolar 3.11. *Postoji beskonačno mnogo prostih brojeva p takvih da za $K = \mathbb{Q}(\sqrt{-3}, \sqrt{p})$,* $\operatorname{rank}(X_0(21)(K)) = 0$.

Teorem 3.12. *Neka je p prost broj koji zadovoljava $p \equiv 1 \pmod 4$, te $\left(\frac{p}{7}\right) = -1$. Tada je* $\operatorname{rank}(X_0^{(p)}(49)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-7p)}(49)(\mathbb{Q})) = 0$.

Dokaz. Eksplicitni model [66] od $X_0(49)$ je $y^2 + xy = x^3 - x^2 - 2x - 1$. Transformacijom u oblik pogodan za korištenje spusta s 2-izogenijama, dobivamo krivulje

$$\begin{aligned} E(p) : y^2 &= x^3 + 21px^2 + 112p^2x, \\ E'(p) : y^2 &= x^3 - 42px^2 - 7p^2x, \\ E(-7p) : y^2 &= x^3 - 147px^2 + 5488p^2x, \\ E'(-7p) : y^2 &= x^3 + 294px^2 - 343p^2x. \end{aligned}$$

Na ovom mjestu ćemo iskoristiti dosad navedeno o eliptičkim krivuljama koje imaju kompleksno množenje, kako bismo si olakšali račun. Naime, izračunom j-invarijante (koja je -3375) i usporedbom s vrijednostima j-invarijante krivulja iz Tablice 3.1 uočavamo da $E(p)$ ima kompleksno množenje s prstenom cijelih brojeva od $\mathbb{Q}(\sqrt{-7})$. Iz toga slijedi da su krivulje $E(p)$ i $E(-7p)$ izogene, pa ćemo provesti račun ranga samo za prvu od njih.

1. $E(p) : y^2 = x^3 + 21px^2 + 112p^2x$

   Pridruženi torzor ima očita cjelobrojna rješenja za $b_1 = 1$ i $b_1 = 7$. Vrijednosti $b_1 = p$ i $b_1 = 2p$ mogu se lako eliminirati korištenjem pretpostavke $\left(\frac{p}{7}\right) = -1$, a vrijednost $b_1 = 2$ korištenjem $p \equiv 1 \pmod 4$. Negativne vrijednosti od b_1 daju desnu stranu torzora negativnu, a sve ostale vrijednosti eliminirane su zbog grupoidnosti od $S_\psi(E(p))$. Dakle, $\#S_\psi(E(p)) = 2$.

2. $E'(p) : y^2 = x^3 - 42px^2 - 7p^2x$

Postoje cjelobrojna rješenja pridruženog torzora za vrijednosti $b_1 = 1$ i $b_1 = 7$, dok slučaj $b_1 = p$ ne daje cjelobrojna rješenja zbog $\left(\frac{p}{7}\right) = -1$. Nadalje, slučaj $b_1 = -p$ također nije moguć zbog $p \equiv 1 \pmod 4$. Zaključujemo da je $\#S_\phi(E'(p)) = 2$, te $\text{rank}(X_0^{(p)}(49)(\mathbb{Q})) = 0$.

Zbog $\text{rank}(X_0^{(p)}(49)(\mathbb{Q})) = 0$ i činjenice da su $E(p)$ i $E(-7p)$ izogene, vrijedi također i $\text{rank}(X_0^{(-7p)}(49)(\mathbb{Q})) = 0$. □

Korolar 3.13. *Postoji beskonačno mnogo prostih brojeva p takvih da je za $K = \mathbb{Q}(\sqrt{-7}, \sqrt{p})$,* $\text{rank}(X_0(49)(K)) = 0$.

Sumirajmo rezultate Korolara 3.4, 3.6, 3.9, 3.11 i 3.13. Pronašli smo beskonačno mnogo kvartičnih polja takvih da je rang odgovarajuće modularne krivulje nad tim poljem jednak nuli, što nam uz činjenicu da je torzijska grupa veća nego torzijska grupa nad $\mathbb{Q}$ posljedično daje da postoji konačno mnogo eliptičkih krivulja s n-izogenijom. Međutim, kako bismo pronašli točan broj takvih eliptičkih krivulja, prisjetimo se da se u Teoremu 3.2 samo broje točke na $Y_0(n)(K)$, dok mi u disertaciji brojimo eliptičke krivulje s cikličkim izogenijama stupnja n. Svaka točka na $Y_0(n)(K)$ odgovara paru (E, f), tako da treba pripaziti da smo u svim navedenim n-ovima doista dobili nove krivulje (a ne samo izogenije već postojećih krivulja). To ćemo učiniti računanjem j-invarijante svake od dobivenih krivulja uz pomoć programskog paketa Magma [3]. Slijedi primjer koda za $n = 49$:

```
C:=SmallModularCurve(49);
E1:=ChangeRing(C,QuadraticField(-7));//radimo nad poljem Q(Sqrt(-7))
TorsionSubgroup(E1);
g,m:=TorsionSubgroup(E1);
p:=m(g.1);
q:=m(g.2);
jInvariant(q,49);
jInvariant(p,49);
jInvariant(p+q,49);
```

Primjer računanja j-invarijanti eliptičkih krivulja dobivenih od $X_0(49)$

Tablice 3.2 i 3.3 prikazuju dobivene rezultate, s time da Tablica 3.2 zapravo predstavlja dopunu tablice iz Teorema 3.2.

n	$\#Y_0(n)(\mathbb{Q})$	K	$\#Y_0(n)(K)$	#kaspova	#krivulja s n-izogenijom nad K
14	2	$\mathbb{Q}(\sqrt{-7})$	8	4	6
15	4	$\mathbb{Q}(i)$	12	4	12
20	0	$\mathbb{Q}(i)$	6	6	2
21	4	$\mathbb{Q}(\sqrt{-3})$	12	4	7
49	0	$\mathbb{Q}(\sqrt{-7})$	2	2	2

Tablica 3.2
Broj različitih eliptičkih krivulja s n-izogenijom nad K

Primijetimo da u slučajevima $n = 15$ i $n = 49$ sve racionalne točke iz $Y_0(n)(K)$ daju različite eliptičke krivulje, dok u ostalim slučajevima imamo i međusobno izogenih krivulja. U svim slučajevima je broj točaka nad K veći nego nad $\mathbb{Q}$.

n	K	j-invarijante
14	$\mathbb{Q}(\sqrt{-7})$	$\left\{-3375, 16581375, \frac{-10529 \pm 16471\sqrt{-7}}{8}, \frac{56437681 \pm 1875341\sqrt{-7}}{32768}\right\}$
15	$\mathbb{Q}(i)$	$\left\{-\frac{25}{2}, -\frac{349938025}{8}, -\frac{121945}{32}, \frac{46969655}{32768}, \frac{-1971 \pm 86643i}{4}, \frac{-47709 \pm 15363i}{256}, \frac{19928133 \pm 13670181i}{8}, \frac{-62613 \pm 198261i}{2}\right\}$
20	$\mathbb{Q}(i)$	$\{1728, 287496\}$
21	$\mathbb{Q}(\sqrt{-3})$	$\left\{0, 54000, -12288000, \frac{3375}{2}, -\frac{140625}{8}, -\frac{189613868625}{128}, -\frac{1159088625}{2097152}\right\}$
49	$\mathbb{Q}(\sqrt{-7})$	$\left\{\frac{1306315496294666865 \pm 9115048720299375\sqrt{-7}}{1125899906842624}\right\}$

Tablica 3.3
j-invarijante eliptičkih krivulja dobivenih iz $X_0(n)(K)_{tors}$

Napomena 3.1. Postoji jedan slučaj iz [**55, Theorem 3**] koji nije obrađen u ovoj disertaciji, a to je $n = 27$. Naime, metoda spusta s 2-izogenijama koju ovdje koristimo ne može se primijeniti u tom slučaju zato jer se eksplicitni model od $X_0(27)$ ne može transformirati u oblik u kojem je $(0, 0)$ točka reda 2. Dodatno, kod $n = 27$ sve 3 točke na $Y_0(\mathbb{Q}(\sqrt{-3}))$ odgovaraju j-invarijanti -12288000. Dakle, nema više krivulja s 27-izogenijom nad $\mathbb{Q}(\sqrt{-3})$ nego što ima nad $\mathbb{Q}$, pa nam i s te strane slučaj $n = 27$ nije interesantan. Međutim, u članku [**49, Theorem 17**] obrađen je i taj slučaj te je dokazano da postoji beskonačno mnogo sekstičnih polja takvih da je $\#Y_0(n)(\mathbb{Q}) \neq \#Y_0(n)(K) < \infty$. To se dobije korištenjem činjenice da je $X_0(27)$ eliptička krivulja s j-invarijantom 0, te dokazom općenitog rezultata o rangovima takvih eliptičkih krivulja nad kubičnim proširenjima polja koja sadrže ζ_3,

gdje je ζ_3 primitivni treći korijen jedinice.

Napomena 3.2. Za $n = 36$, u [55] se dobije da su sve $\mathbb{Q}(\sqrt{-3})$-racionalne točke kaspovi, pa se zato taj slučaj ne pojavljuje u Teoremu 3.2. Međutim, metodama korištenim u ovom poglavlju dobijemo rezultate o zakretima eliptičke modularne krivulje $X_0(36) : y^2 = x^3 + 1$ s j-invarijantom 0, koji su zanimljivi sami po sebi:

Teorem 3.14. *Neka je p prost broj koji zadovoljava $p \equiv 2 \pmod 3$ i $p \equiv 1 \pmod 4$. Tada je* $\operatorname{rank}(X_0^{(p)}(36)(\mathbb{Q})) = \operatorname{rank}(X_0^{(-3p)}(36)(\mathbb{Q})) = 0$.

Dokaz. Krenuvši od eksplicitnog modela [66] od $X_0(36)$, $y^2 = x^3+1$, zamjenom $x \mapsto x-1$ dobivamo krivulje pogodne za primjenu metode spusta s 2-izogenijama:

$$\begin{aligned} E(p) : y^2 &= x^3 - 3px^2 + 3p^2x, \\ E'(p) : y^2 &= x^3 + 6px^2 - 3p^2x, \\ E(-3p) : y^2 &= x^3 + 9px^2 + 27p^2x, \\ E'(-3p) : y^2 &= x^3 - 18px^2 - 27p^2x. \end{aligned}$$

Uočavanjem da $E(p)$ i $E(-3p)$ imaju j-invarijantu 0, iz toga i Tablice 3.1 zaključujemo da imaju kompleksno množenje s prstenom cijelih brojeva od $\mathbb{Q}(\sqrt{-3})$. Posljedično dobivamo da su te dvije krivulje izogene, odnosno imaju isti rang. Stoga ćemo kod računanja ranga promatrati samo prvu od ove dvije krivulje, $E(p)$.

1. $E(p) : y^2 = x^3 - 3px^2 + 3p^2x$

   $b_1 = 1$ i $b_1 = 3$ su elementi od $S_\psi(E(p))$, a lako dokažemo da preostale vrijednosti od b_1 nisu. Da bismo eliminirali slučaj $b_1 = p$, još će nam trebati pretpostavka $p \equiv 2 \pmod 3$. Torzor je

   $$N^2 = pM^4 - 3pM^2e^2 + 3pe^4,$$

   pa ako $3 \nmid M$, onda je $N^2 \equiv p \equiv 2 \pmod 3$, što nije moguće. Ako pak $3|M$, onda i $3|N$, pa je lijeva strana torzora djeljiva s 9. To povlači da mora i desna strana biti djeljiva s 9, a to je moguće samo ako $3|e$, što je nemoguće jer su M i e relativno prosti. $S_\psi(E(p))$ je grupa pa ni za $b_1 = 3p$ pridruženi torzor ne može imati cjelobrojnih rješenja, što implicira $\#S_\psi(E(p)) = 2$.

2. $E'(p) : x^3 + 6px^2 - 3p^2x$

   Moguće vrijednosti od b_1 su $\{\pm 1, \pm 3, \pm p, \pm 3p\}$. Dokazat ćemo da nam samo $b_1 = 1$ i $b_1 = -3$ daju cjelobrojna rješenja pridružene kvartike. Naime, za $b_1 \in \{-1, p\}$ dobivamo kontradikciju promatranjem djeljivosti s 3 i 9 (kao i u prethodnom slučaju

za $b_1 = p$), pri čemu nam za eliminaciju $b_1 = p$ još dodatno treba i $p \equiv 2 \pmod 3$. Nadalje, $b_1 = -p$ nije moguće zbog činjenice $p \equiv 1 \pmod 4$. Naime, u tom slučaju torzor je

$$N^2 = -pM^4 + 6pM^2e^2 + 3pe^4,$$

pa ako je e paran, dobivamo da je lijeva strana kongruentna 3 modulo 4, što nije moguće. Istu kongruenciju na lijevoj strani dobivamo i ako je e neparan i M paran. Preostaje slučaj kad su oba M i e neparna. Tada je, zbog činjenice da četvrta potencija neparnog broja može dati samo ostatak 1 pri dijeljenju sa 16, $N^2 \equiv 2p(3M^2e^2 + 1) \equiv 8 \pmod{16}$, što je nemoguće i slijedi $-p \notin S_\phi(E'(p))$.
S obzirom da je $S_\phi(E'(p))$ grupa, i preostale mogućnosti za b_1 su eliminirane. Stoga, $\#S_\phi(E'(p)) = 2$ i $\operatorname{rank}(X_0^{(p)}(36)(\mathbb{Q})) = 0$.

Zbog izogenosti krivulja $E(p)$ i $E(-3p)$ dobivamo da je i $\operatorname{rank}(X_0^{(-3p)}(36)(\mathbb{Q})) = 0$. □

Bibliografija

[1] A. Atkin i F.Morain, *Elliptic curves and primality proving*, Math.Comp. **61** (1993), 29–68.

[2] A. Baker i H.Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2), **20** (1969), 129–137.

[3] W. Bosma, J. Cannon i C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., **24** (1997), 235–265.

[4] E. Brown, *Sets in which* $xy + k$ *is always a square*, Math. Comp. **45** (1985), 613–620.

[5] Y. Bugeaud, A. Dujella i M. Mignotte, *On the family of Diophantine triples* $\{k-1, k+1, 16k^3 - 4k\}$, Glasgow Math. J. **49** (2007), 333–344.

[6] I. Connell, Elliptic Curve Handbook, http://www.math.mcgill.ca/connell/public/ECH1/

[7] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997.

[8] F. Diamond i J. Shurman, A First Course in Modular Forms, Springer, 2005.

[9] L. E. Dickson, A history of the Theory of numbers, Vol. 2, Chelsea, New York, 1966., pp. 513–520.

[10] Diophantus of Alexandria, Arithmetics and the Book of Polygonal Numbers (I. G. Bashmakova, Ed.) , Nauka, 1974, (in Russian), pp. 103–104, 232.

[11] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[12] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.

[13] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.

[14] A. Dujella, *A problem of Diophantus and Pell numbers*, Application of Fibonacci Numbers, Vol. 7 (G. E. Bergum, A. N. Philippou, A. F. Horadam, eds.), Kluwer, Dordrecht, (1998), pp. 61–68.

[15] A. Dujella, *A proof of the Hoggatt-Bergum conjecture*, Proc. Amer. Math. Soc. **127** (1999), 1999–2005.

[16] A. Dujella, *A parametric family of elliptic curves*, Acta Arith. **94** (2000), 87–101.

[17] A. Dujella i A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2) **49** (1998), 291–306.

[18] A. Dujella i A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.

[19] A. Dujella, *Diophantine m-tuples and elliptic curves*, J. Theor. Nombres Bordeaux **13** (2001), 111–124.

[20] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.

[21] A. Dujella, *Bounds for the size of sets with the property $D(n)$*, Glas. Mat. Ser. III **39** (2004), 199–205.

[22] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[23] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), 3–18.

[24] A. Dujella, Algoritmi za eliptičke krivulje, http://web.math.pmf.unizg.hr/~duje/elipticke/algelip.pdf

[25] A. Dujella i A. M. S. Ramasamy, *Fibonacci numbers and sets with the property $D(4)$*, Simon Stevin **12** (2005), 401–412.

[26] A. Dujella i M. Mikić, *On the torsion group of elliptic curves induced by $D(4)$-triples*, An. Stiint. Univ. "Ovidius" Constanta Ser. Mat. **22** (2014), 79–90.

[27] A. Dujella i J.C. Peral, *High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples*, LMS J. Comput. Math. **17** (2014), 282–288.

[28] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366

[29] H. Fell, M. Newman i E. Ordman, *Tables of genera of groups of linear fractional transformations*, J. Res. Nat. Bur. Standards Sect. B **67B** (1963) 61–68.

[30] A. Filipin, *There does not exist a $D(4)$-sextuple*, J. Number Theory **128** (2008), 1555–1565.

[31] A. Filipin, *There are only finitely many $D(4)$-quintuples*, Rocky Mountain J. Math. **41** (2011), 1847–1859.

[32] A. Filipin, *An irregular $D(4)$-quadruple cannot be extended to a quintuple*, Acta Arith. **136** (2009), 167–176.

[33] A. Filipin, Bo He i A. Togbé, *On a family of two-parametric $D(4)$-triples*, Glas. Mat. Ser. III **47** (2012), 31–51.

[34] Y. Fujita, *The extensibility of Diophantine pairs $\{k-1, k+1\}$*, J. Number Theory **128** (2008), 322–353.

[35] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.

[36] H. Gupta i K. Singh, *On k-triad sequences*, Internat. J. Math. Math. Sci. **5** (1985), 799–804.

[37] I. Gusić, Uvod u aritmetiku eliptičkih krivulja, http://web.math.pmf.unizg.hr/~duje/aritmeliptkr.pdf

[38] K. S. Kedlaya, *Solving constrained Pell equations*, Math. Comp. **67** (1998), 833–842.

[39] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

[40] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244.

[41] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), 415–427.

[42] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[43] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.

[44] S. Kwon, *Torsion subgroups of elliptic curves over quadratic extensions*, J. Number Theory **62** (1997), 144–162.

[45] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math.(2), **126** (1987), 649–673.

[46] A. K. Lenstra i E. R. Verheul, *Selecting cryptographic key sizes*, J. Cryptology, **14** (2001), 255–293.

[47] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[48] M. Mikić, *On the Mordell-Weil group of elliptic curves induced by families of Diophantine triples*, Rocky Mountain J. Math., to appear.

[49] M. Mikić i F. Najman, *On the number of n-isogenies of elliptic curves over number fields*, Glas. Mat. Ser. III, to appear.

[50] M. Mignotte i A. Pethő, *Sur les carres dans certaines suites de Lucas*, J. Théor. Nombres Bordeaux **5** (1993), 333–341.

[51] S. P. Mohanty i A. M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. **23** (1985), 36–44.

[52] S. P. Mohanty i A. M. S. Ramasamy, *The characteristic number of two simultaneous Pell's equations and its applications*, Simon Stevin **59** (1985), 203–214.

[53] F. Najman, *Kompaktna reprezentacija cijelih kvadratnih brojeva i cjelobrojne točke na eliptičkim krivuljama*, doktorska disertacija, Sveučilište u Zagrebu, 2009.

[54] F. Najman, *Integer points on two families of elliptic curves*, Publ. Math. Debrecen **75** (2009), 401–418

[55] F. Najman, *On the number of elliptic curves with prescribed isogeny or torsion group over number fields of prime degree*, Glasgow Math. J, to appear.

[56] F. Najman, *Exceptional elliptic curves over quartic fields*, Int. J. Number Theory, **8** (2012), 1231–1246.

[57] NSA, "Suite B cryptography". http://www.nsa.gov/ia/programs/suiteb_cryptography/

[58] K. Ono, *Euler's concordant forms*, Acta Arith. **78** (1996), 101–123.

[59] The PARI Group, PARI/GP version `2.7.0`, 2014, Bordeaux, http://pari.math.u-bordeaux.fr/

[60] B. Schoeneberg, Elliptic Modular Functions, Springer-Verlag, NY, 1974.

[61] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[62] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer-Verlag, New York, 1994.

[63] W. A. Stein et al. Sage Mathematics Software (Version 5.4.1.), The Sage Development Team, 2012, http://www.sagemath.org

[64] M. Vellupillai, *The equations* $z^2 - 3y^2 = -2$ *and* $z^2 - 6x^2 = -5$, A Collection of Manuscripts Related to the Fibonacci Sequence, (V. E. Hoggatt, M. Bicknell-Johnson, eds.), The Fibonacci Association, Santa Clara, 1980, pp. 71–75.

[65] A. Wiles, *The Birch and Swinnerton-Dyer conjecture*, in the Millenium prize problems; American Mathematical Socitey pp. 31–44.

[66] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), 481–508.

[67] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen*, Jahresber. Deutsch. Math.-Verein **92** (1990), 58–76.

Sažetak

U ovom radu dokazano je da torzijska grupa eliptičkih krivulja induciranih $D(4)$-trojkama može biti ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Time je ujedno (kao specijalni slučaj) dobiveno i da torzijska grupa eliptičkih krivulja induciranih Diofantovim trojkama može biti jedna od navedenih. Promatrane su i familije eliptičkih krivulja generiranih Diofantovim trojkama oblika $\{k-1, k+1, c_l(k)\}$ te su određeni torzijska grupa i rang (a time i Mordell-Weilova grupa) koje mogu imati takve krivulje za veliki broj vrijednosti od k i l. Konačno, promatranjem modularnih krivulja $X_0(n)$ prebrojano je koliko ima eliptičkih krivulja s cikličkom izogenijom stupnja n nad raznim kvartičnim poljima.

Summary

In this work it is proved that the torsion group of elliptic curves induced by $D(4)$-triples can be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Therefore, as a special case it is proved that the torsion group of elliptic curves induced by Diophantine triples can be one of these two, as well. Families of elliptic curves induced by Diophantine triples of the form $\{k-1, k+1, c_l(k)\}$ are examined and the possible form of the torsion group and rank (i.e. Mordell-Weil group) of these curves is determined for the large number of values of k and l. Finally, by studying modular curves $X_0(n)$ the number of elliptic curves with cyclic isogeny of degree n over various quartic fields is found.

Životopis

Rođen sam 13.9.1984. u Rijeci gdje sam završio osnovnu i srednju školu. Tijekom cijelog školovanja postizao sam uspjehe na matematičkim natjecanjima, a najveći je bio plasman na Međunarodnu matematičku olimpijadu 2003. održanu u Japanu na kojoj sam osvojio pohvalu. Iste godine upisao sam Fakultet elektrotehnike i računarstva, na kojem sam diplomirao 2008. na studiju Računarstva s prosjekom ocjena 5.00. Pod vodstvom prof.dr.sc. Marina Goluba i doc.dr.sc. Stjepana Groša izradio sam diplomski rad „Ugradnja SNMP podrške u protokol za razmjenu ključeva". Tijekom studija za svaku akademsku godinu dobio sam priznanje dekana za najboljeg studenta godine, a uz diplomu i brončanu plaketu „Josip Lončar" za studenta generacije.

Akademske godine 2008./2009. upisao sam doktorski studij matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu, te od tada sudjelujem u radu Seminara za teoriju brojeva i algebru. 2008. godine sam se zaposlio u T-Mobile d.d., a od 2013. radim u Asseco SEE d.d. na poziciji razvojnog inženjera. Sudjelovao sam na stručnim i znanstvenim konferencijama (Mipro, Windays, JavaCro, Workshop on Number Theory and Algebra) na kojima sam održao prezentacije.

Znanstvenim istraživanjem bavim se pod vodstvom mentora prof.dr.sc. Andreja Dujelle i doc.dr.sc. Filipa Najmana. Objavljen mi je zajednički rad s prof.dr.sc. Andrejem Dujellom „On the torsion group of elliptic curves induced by D(4)-triples" u Analele Stiintifice ale Universitatii „Ovidius" Constanta Seria Matematica, dok su mi samostalni rad „On the Mordell-Weil group of elliptic curves induced by families of Diophantine triples" i zajednički rad s doc.dr.sc. Filipom Najmanom „On the number of n-isogenies of elliptic curves over number fields" prihvaćeni za objavu u Rocky Mountain Journal of Mathematics, odnosno u Glasniku Matematičkom.