Torzija eliptičkih krivulja nad beskonačnim Abelovim proširenjima

Krijan, Ivan

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Ivan Krijan

Torzija eliptičkih krivulja nad beskonačnim Abelovim proširenjima od $\mathbb{Q}$

DOKTORSKI RAD

Mentor:

izv. prof. dr. sc. Filip Najman

Zagreb, 2020.

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Ivan Krijan

Torsion groups of elliptic curves over infinite Abelian extensions of $\mathbb{Q}$

DOCTORAL DISSERTATION

Supervisor:

izv. prof. dr. sc. Filip Najman

Zagreb, 2020.

ZAHVALA

Hvala mojoj supruzi *Ani* i sinu *Filipu* na beskrajnoj podršci i razumijevanju. Ovaj rad posvećen je upravo vama!

Hvala mentoru izv. prof. dr. sc. Filipu Najmanu na odabiru odlične teme i neizmjernoj pomoći oko stvaranja ovog rada. Svim članovima Seminara za teoriju brojeva i algebru hvala na veoma ugodnim matematičkim druženjima. Antoneli, Borni i Tomislavu zahvaljujem na brojnim konstruktivnim diskusijama i poučnim te korisnim savjetima!

Posebno hvala svima koji su ovaj rad detaljno pročitali. Pri tome su ukazali na nemali broj sitnih i onih manje sitnih grešaka. To su doc. dr. sc. Nikola Adžaga, akademik prof. dr. sc. Andrej Dujella, izv. prof. dr. sc. Zrinka Franušić i izv. prof. dr. sc. Matija Kazalicki. Učinili ste ovaj rad uistinu boljim!

Hvala svim članovima Seminara za unitarne reprezentacije i automorfne forme kojeg sam pohodio neko vrijeme. Posebno hvala prijatelju i najboljem kolegi dr. sc. Petru Bakiću na predivnih 5 godina dijeljenja ureda.

Ovaj rad je nastao uz podršku Znanstvenog centra izvrsnosti *QuantiXLie*, projekt koji sufinanciraju Republika Hrvatska i Europska unija kroz Europski regionalni razvojni fond - kompetitivnost i kohezija. Grant KK.01.1.1.01.0004

SAŽETAK

Za eliptičku krivulju $E/\mathbb{Q}$ i za svaki prost broj p najprije određujemo sve moguće torzijske grupe $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$, gdje je $\mathbb{Q}_{\infty,p}$ jedinstveno $\mathbb{Z}_p$-proširenje od $\mathbb{Q}$, tj. jedinstveno Galoisovo proširenje od $\mathbb{Q}$ takvo da je $\text{Gal}\,(\mathbb{Q}_{\infty,p}/\mathbb{Q}) \simeq \mathbb{Z}_p$. Za eliptičku krivulju $E/\mathbb{Q}$ i prost broj p vrijedi:

- Ako je $p \geq 5$, onda je $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$.
- Ako je $p = 3$, onda je grupa $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ izomorfna nekoj od grupa iz Mazurovog teorema ili nekoj od grupa $\mathbb{Z}/21\mathbb{Z}$ i $\mathbb{Z}/27\mathbb{Z}$.
- Ako je $p = 2$, onda je grupa $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$ izomorfna nekoj od grupa iz Mazurovog teorema.

Treba biti oprezan, u slučajevima $p = 2$ i $p = 3$ ne vrijedi nužno da je $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$. Na ovo pitanje također dajemo detaljan odgovor te nalazimo primjere za sve moguće slučajeva rasta torzije $\mathbb{Q} \to \mathbb{Q}_{\infty,p}$, gdje je $p \in \{2,3\}$.

Promatramo također i torziju nad kompozitumom svih $\mathbb{Z}_p$-proširenja od $\mathbb{Q}$. Neka je

$$\mathscr{K}_{\geq 5} = \prod_{p \geq 5 \text{ prost}} \mathbb{Q}_{\infty,p} \qquad \text{te} \qquad \mathscr{K} = \prod_{p \text{ prost}} \mathbb{Q}_{\infty,p}.$$

Dokazali smo da za eliptičku krivulju $E/\mathbb{Q}$ vrijedi da je $E(\mathscr{K}_{\geq 5})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ te da je $E(\mathscr{K})_{\text{tors}}$ izomorfno nekoj od grupa iz Mazurovog teorema ili nekoj od grupa $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$ i $\mathbb{Z}/27\mathbb{Z}$.

Na kraju navodimo neke rezultate o ponašanju torzije eliptičke krivulje $E/\mathbb{Q}$ nad poljima

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{k=1}^{\infty} \mathbb{Q}(\mu_{p^k}), \qquad \text{gdje je} \quad \mu_n = \{\omega \in \mathbb{C} \,:\, \omega^n = 1\}.$$

Preciznije, dokazan je sljedeći rezultat za eliptičke krivulje $E/\mathbb{Q}$:

$$E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}, \quad E(\mathbb{Q}(\mu_{3^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}}$$

$$\text{te} \qquad E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_p))_{\text{tors}}, \quad \text{za svaki prost broj } p \geq 5.$$

Ključne riječi: eliptička krivulja, Iwasawina teorija, $\mathbb{Z}_p$-proširenje, torzija, rast torzije, ciklotomsko proširenje

SUMMARY

We determine, for an elliptic curve $E/\mathbb{Q}$ and for all prime numbers p, all the possible torsion groups $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$, where $\mathbb{Q}_{\infty,p}$ is the $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

For a prime number p, denote by $\mathbb{Q}_{\infty,p}$ the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and for a positive integer n, denote by $\mathbb{Q}_{n,p}$ the n^{th} layer of $\mathbb{Q}_{\infty,p}$, i.e. the unique subfield of $\mathbb{Q}_{\infty,p}$ such that $\text{Gal}\,(\mathbb{Q}_{n,p}/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Let, as always, $\mu_n = \{\omega \in \mathbb{C} \,:\, \omega^n = 1\}$ be the set of all n^{th} roots of unity. We also define

$$\mu_{p^\infty} = \bigcup_{k\in\mathbb{N}} \mu_{p^k}.$$

Note that $\mathbb{Q}(\mu_{p^k}) = \mathbb{Q}(\zeta_{p^k})$, where ζ_n is n^{th} primitive root of unity.

Recall that the $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is the unique Galois extension $\mathbb{Q}_{\infty,p}$ of $\mathbb{Q}$ such that

$$\text{Gal}\,(\mathbb{Q}_{\infty,p}/\mathbb{Q}) \simeq \mathbb{Z}_p,$$

where $\mathbb{Z}_p$ is the additive group of the p-adic integers and is constructed as follows:

Let

$$G = \text{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \varprojlim_n \text{Gal}\left(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}\right) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Here we know that $G = \Delta \times \Gamma$, where $\Gamma \simeq \mathbb{Z}_p$ and $\Delta \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ for $p \geq 3$ and $\Delta \simeq \mathbb{Z}/2\mathbb{Z}$ (generated by complex conjugation) for $p = 2$, so we define

$$\mathbb{Q}_{\infty,p} := \mathbb{Q}(\mu_{p^\infty})^\Delta.$$

We also see that every layer is uniquely determined by (for $p \geq 3$)

$$\mathbb{Q}_{n,p} = \mathbb{Q}(\mu_{p^{n+1}}) \cap \mathbb{Q}_{\infty,p},$$

so for $p \geq 3$ it is the unique subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$. More details and proofs of these facts about $\mathbb{Z}_p$-extensions and Iwasawa theory can be found in [56, Chapter 13].

Summary

Iwasawa theory for elliptic curves (see [19]) studies elliptic curves in $\mathbb{Z}_p$-extensions, in particular the growth of the rank and n-Selmer groups in the layers of the $\mathbb{Z}_p$-extensions.

In this paper we completely solve the problem of determining how the torsion of an elliptic curve defined over $\mathbb{Q}$ grows in the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$. These results, interesting in their own right, might also find applications in other problems in Iwasawa theory for elliptic curves and in general. For example, to show that elliptic curves over $\mathbb{Q}_{\infty,p}$ are modular for all p, Thorne [55] needed to show that $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$ for two particular elliptic curves. In this work we did that thing in general case.

Our results are the following:

Let $E/\mathbb{Q}$ be an elliptic curve. Let $p \geq 5$ be a prime number. Then

$$E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}.$$

Group $E(\mathbb{Q}_{\infty,2})_{\text{tors}}$ is isomorphic to exactly one of the following groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \leq N \leq 10, \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad 1 \leq N \leq 4, \end{aligned}$$

and for each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq G$.

Group $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ is isomorphic to exactly one of the following groups:

$$\begin{aligned} \mathbb{Z}/N\mathbb{Z}, &\qquad 1 \leq N \leq 10, \text{ or } N = 12, 21 \text{ or } 27, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, &\qquad 1 \leq N \leq 4. \end{aligned}$$

and for each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq G$.

By Mazur's theorem we see that

$$\{E(\mathbb{Q}_{\infty,2})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} = \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\},$$
$$\{E(\mathbb{Q}_{\infty,3})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} = \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ elliptic curve}\} \cup \{\mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}.$$

However, given a specific $E/\mathbb{Q}$ it is not necessarily the case that $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$. Indeed there are many elliptic curves for which torsion grows from $\mathbb{Q}$ to $\mathbb{Q}_{\infty,p}$, and we investigate this question further in Section 3.6. Specifically, for each prime p we find for which groups G there exists infinitely many j-invariants j such that there exists an elliptic curve $E/\mathbb{Q}$ with $j(E) = j$ and such that $E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}} \simeq G$.

Furthermore, after we understood the behaviour of the torsion of elliptic curve $E/\mathbb{Q}$ over the field $\mathbb{Q}_{\infty,p}$, we tried to find out what will happen if we look at the compositum of all of those fields. We answered that question completely too.

Let

$$\mathscr{K}_{\geq 5} = \prod_{p\geq 5 \text{ prime}} \mathbb{Q}_{\infty,p}$$

and let

$$\mathscr{K} = \prod_{p \text{ prime}} \mathbb{Q}_{\infty,p}.$$

We proved that for an elliptic curve $E/\mathbb{Q}$ it holds that

$$E(\mathscr{K}_{\geq 5})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$$

and also that $E(\mathscr{K})_{\text{tors}}$ is isomorphic to one of the following groups

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ or } n \in \{12, 13, 21, 27\},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

For each group G from the list above there exists an $E/\mathbb{Q}$ such that $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq G$.

At the end, in chapter 5 we state some results about the behaviour of the torsion of elliptic curve $E/\mathbb{Q}$ over the fields

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{k=1}^{\infty} \mathbb{Q}(\mu_{p^k}).$$

More precisely, we prove the following result

Let $E/\mathbb{Q}$ be an elliptic curve, then for a prime number $p \geq 5$ it holds that

$$E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_p))_{\text{tors}}.$$

Furthermore

$$E(\mathbb{Q}(\mu_{3^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}} \qquad \text{and} \qquad E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}.$$

In chapter 6 we exhibit all `magma` [2] codes that we used for computations.

Keywords: elliptic curve, Iwasawa theory, $\mathbb{Z}_p$-extension, torsion, torsion growth, cyclotomic extension

SADRŽAJ

Uvod **1**

Predgovor 4

1 Teorijska pozadina **5**

1.1 Galoisove reprezentacije pridružene eliptičkim krivuljama 5

1.2 Djelidbeni polinomi 11

1.3 Modularne krivulje 13

1.4 Kvadratni twist 19

2 $\mathbb{Z}_p$-proširenje **20**

2.1 Što je to $\mathbb{Z}_p$-proširenje? 20

2.2 $\mathbb{Z}_p$-proširenje od $\mathbb{Q}$ 23

3 Torzija nad $\mathbb{Z}_p$-proširenjem od $\mathbb{Q}$ **25**

3.1 Poznati i pomoćni rezultati 25

3.2 Rezultati 30

3.3 Dokaz teorema 3.2.1 32

3.4 Dokaz teorema 3.2.2 35

3.5 Dokaz teorema 3.2.3 40

3.6 Rast torzije 45

4 Torzija nad kompozitumom svih $\mathbb{Z}_p$-proširenja od $\mathbb{Q}$ **57**

4.1 Rezultati 58

4.2 Dokaz teorema 4.1.1 59

4.3 Dokaz teorema 4.1.2 61

5 Torzija nad $\mathbb{Q}(\mu_{p^\infty})$ **69**

5.1 Rezultati 70

5.2 Dokaz teorema 5.1.1 71

5.3 Neke posljedice 81

6 Korišteni magma kôdovi **83**

Zaključak **94**

Bibliografija **96**

Životopis **102**

UVOD

Eliptička krivulja je glavni objekt promatranja u ovom radu. Preciznije, promatrat ćemo eliptičke krivulje definirane nad poljem racionalnih brojeva.

Definicija. ***Eliptička krivulja*** *nad* $\mathbb{Q}$ *je glatka, projektivna krivulja genusa* 1 *sa specifiranom racionalnom točkom, koju ćemo označiti s* 0.

Za precizno izloženu teoriju eliptičkih krivulja, svakako se treba konzultirati s [42,44,53]. U ovom uvodu ćemo u kratkim crtama izložiti osnovne definicije i svojstva koja su nam od bitnog interesa. U cijelom radu "eliptička krivulja $E/\mathbb{Q}$" nam znači da je E eliptička krivulja koja je definirana nad $\mathbb{Q}$. Kako ćemo cijelo vrijeme biti nad poljem $\mathbb{Q}$ i nad njegovim proširenjima, $E/\mathbb{Q}$ uvijek možemo zapisati u kratkoj Weierstrassovoj formi:

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

gdje su a i b racionalni brojevi. Napomenimo da je ovo krivulja zapisana u afinim koordinatama. Zapravo je riječ o krivulji

$$y^2 z = x^3 + axz^2 + bz^3$$

u projektivnim koordinatama. Specificirana točka koju smo spomenuli u definiciji i koju označavamo s 0 je zapravo točka $(0:1:0)$ i nju zamišljamo kao točku u beskonačnosti.

Za polje algebarskih brojeva $\mathbb{K}$, označimo s $E(\mathbb{K})$ skup točaka eliptičke krivulje $E/\mathbb{Q}$ čije su koordinate elementi polja $\mathbb{K}$, tj. točke koje su definirane nad $\mathbb{K}$. Kako je $E/\mathbb{Q}$ eliptička krivulja, taj skup uvijek ima barem jedan element, točku 0. Nadalje, skup $E(K)$ uz prirodno definirano zbrajanje točaka na eliptičkoj krivulji čini Abelovu grupu. Sama definicija zbrajanja (te više o tome) može se naći u već spomenutim izvorima [42, 44, 53].

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

Dakle, vrijedi da je

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

gdje je r nenegativni cijeli broj koji zovemo **rang** eliptičke krivulje $E/\mathbb{K}$. Grupa $E(\mathbb{K})_{\text{tors}}$ je **torzijska podgrupa** eliptičke krivulje $E/\mathbb{K}$, preciznije, to je podgrupa elemenata konačnog reda u $E(\mathbb{K})$.

Upravo je torzijska podgrupa $E(\mathbb{K})_{\text{tors}}$ ono što ćemo detaljno proučavati u ovom radu, za neka specifična polja $\mathbb{K}$. Napomenimo da ćemo grupu $E(\mathbb{K})_{\text{tors}}$ često nazivati "torzija eliptičke krivulje $E/\mathbb{Q}$ nad $\mathbb{K}$". Mazur [37] je 1978. dokazao idući teorem koji nam opisuje sve moguće torzije eliptičke krivulje $E/\mathbb{Q}$ nad poljem $\mathbb{Q}$.

Teorem (Mazur)**.** *Neka je $E/\mathbb{Q}$ eliptička krivulja. Grupa $E(\mathbb{Q})_{tors}$ je izomorfna točno jednoj od sljedećih* 15 *grupa:*

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ ili } n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

U idućem poglavlju ćemo definirati jedno specifično proširenje polja $\mathbb{Q}$, riječ je o $\mathbb{Z}_p$-proširenju od $\mathbb{Q}$. Takvo proširenje ćemo označiti s $\mathbb{Q}_{\infty,p}$. U ovom radu osobito zanimanje posvećujemo sljedećem pitanju:

Kakav je odnos grupa $E(\mathbb{Q})_{\text{tors}}$ i $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$?

Na to pitanje dajemo potpuni odgovor, tj. točno određujemo sve moguće torzije nad $\mathbb{Q}_{\infty,p}$ te točno određujemo kada je $E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q}_{\infty,p})_{\text{tors}}$, a kada ipak imamo rast torzije. "Rast torzije" nam znači da je

$$E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}}.$$

Nakon što smo riješili taj problem, riješit ćemo i problem ponašanja torzije nad poljem koje je jednako kompozitumu svih $\mathbb{Z}_p$-proširenja.

Neka su a i b racionalni brojevi i neka je

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

eliptička krivulja. **Diskriminanta** eliptičke krivulje E je veličina

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

Krivulja E je eliptička ako i samo ako je $\Delta(E) \neq 0$. Nadalje, ***j*-invarijanta** eliptičke krivulje E je veličina

$$j(E) = 1728 \cdot \frac{(-4a)^3}{\Delta(E)}.$$

Eliptičke krivulje $E/\mathbb{Q}$ i $E'/\mathbb{Q}$ su izomorfne nad $\overline{\mathbb{Q}}$ (algebarskim zatvaračem od $\mathbb{Q}$) ako i samo ako je $j(E) = j(E')$.

Definicija. ***Izogenija*** *između dvije eliptičke krivulje je morfizam $\phi : E \to E'$ koji preslikava $0 \in E$ u $0' \in E'$.*

Primijetimo da ovdje moramo znati što je morfizam. Racionalno preslikavanje $\phi : E \to E'$ je *morfizam* ako je definirano na cijeloj eliptičkoj krivulji E. Za više detalja svakako pogledati [53, Chapter I §3, Chapter 2 §1-2]. Tu možemo naći i što je točno **stupanj** izogenije.

Glavni primjer izogenije je $[n] : E \to E$,

$$[n]P = nP = \underbrace{P + P + \cdots + P}_{n \text{ puta}}.$$

Bitno je napomenuti i da je ovo primjer izogenije stupnja n. Za većinu naših potreba, ovo je sve što treba znati o stupnju izogenije.

Za prirodni broj n ćemo s $E(\mathbb{K})[n]$ označiti skup, tj. grupu, svih točaka $P \in E(\mathbb{K})$ takvih da je $[n]P = 0$. Vrijedi da je

$$E(\overline{\mathbb{Q}})[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Naglasimo da smo u ovom uvodnom dijelu samo ukratko opisali neke od bitnijih objekata koje u radu proučavamo. Pri tome nismo ulazili u detalje kako bismo izbjegli da uvod postane nezgrapan i prevelik. Svi preskočeni detalji i pojašnjenja, kao što smo već spominjali, mogu se potražiti u [42, 44, 53].

Često ćemo eliptičku krivulju označiti pripadajućom *Cremoninom oznakom*[1]. Na primjer, eliptička krivulja 11a3 je krivulja

$$y^2 + y = x^3 - x,$$

kao što možemo i vidjeti na [54].

[1] pogledati https://johncremona.github.io/ecdata/ i https://www.lmfdb.org/knowledge/show/ec.q.cremona_label

PREDGOVOR

Kako bismo odgovorili na probleme koje smo si zadali potrebne su nam neke "opće poznate" činjenice o eliptičkim krivuljama. Točno tome služi poglavlje 1. Teorijska pozadina. Kratko i jasno, bez ulaženja u detalje izlažemo teorijsku pozadinu svega što će nam biti potrebno.

Poglavlje 2. $\mathbb{Z}_p$-proširenje služi preciznom definiranju samog $\mathbb{Z}_p$-proširenja. Također, izložen je dokaz činjenice da skup racionalnih brojeva ima jedinstveno $\mathbb{Z}_p$-proširenje, tzv. ciklotomsko $\mathbb{Z}_p$-proširenje.

M. Chou, H. B. Daniels i F. Najman su skupa s I.K. napisali članak [6] na osnovu kojega je nastala većina poglavlja 3. Torzija nad $\mathbb{Z}_p$-proširenjem od $\mathbb{Q}$. U tom poglavlju su najprije izloženi poznati rezultati na koje se oslanjamo. Prvenstveno istaknimo članak [17] (E. González-Jiménez i F. Najman) iz kojega su (između ostalog) istaknuti teoremi 3.1.7 i 3.1.8. To je svojevrsna motivacija na kojoj počiva gotovo sve napravljeno u ovom radu. Naime, prirodno se nametnulo pitanje možemo li reći nešto više o rastu torzije ako znamo više detalja o samom polju algebarskih brojeva osim samo njegovog stupnja nad $\mathbb{Q}$. Pokazalo se da možemo!

Nije potrebno naglašavati da se poglavlje 4. Torzija nad kompozitumom svih $\mathbb{Z}_p$-proširenja od $\mathbb{Q}$ nametnulo samo od sebe. Naime, nakon što znamo kako se ponaša torzija nad svakim $\mathbb{Z}_p$-proširenjem, zašto ne bismo pokušali saznati kako se ponaša nad kompozitumom svih $\mathbb{Z}_p$-proširenja? Upravo smo na to pitanje u ovom poglavlju i odgovorili.

Sjetimo li se konstrukcije samog $\mathbb{Z}_p$-proširenja (sekcija 2.1. Što je to $\mathbb{Z}_p$-proširenje?) vidimo da bitnu (zapravo glavnu) ulogu ima polje

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{k=1}^{\infty} \mathbb{Q}(\mu_{p^k}) = \bigcup_{k=1}^{\infty} \mathbb{Q}(\zeta_{p^k}),$$

gdje je ζ_n primitivni n-ti korijen iz 1, p je prost broj te $\mu_n = \{\omega \in \mathbb{C} \ : \ \omega^n = 1\}$. Zanima nas što možemo reći o rastu torzije nad tim poljem. U poglavlju 5. Torzija nad $\mathbb{Q}(\mu_{p^\infty})$ dokazujemo jedan vrlo koristan rezultat — sav rast torzije se dogodi već u prvim slojevima proširenja.

Svi korišteni `magma` [2] kôdovi nalaze se u poglavlju 6. Korišteni magma kôdovi.

Valja napomenuti da će rezultati poglavlja 4 i 5 u skorije vrijeme biti objavljeni u članku [21] koji je u nastajanju (suradnja s T. Gužvićem). Također, postoji prirodan nastavak istraživanja rasta torzije koji se posebno oslanja na rezultate iz poglavlja 5. Članak [22] će sadržavati upravo te rezultate koji su u nastajanju (suradnja s T. Gužvićem i B. Vukorepom).

1. TEORIJSKA POZADINA

Cilj ovog poglavlja je prikaz osnovnih metoda i rezultata koje ćemo u ovom radu opetovano koristiti. Sve što ćemo navesti su standardni rezultati vezani uz teoriju eliptičkih krivulja i za više detalja i dublju analizu dobro je pogledati [42, 44, 53]. Većina napisanog u ovom poglavlju se oslanja upravo na tu literaturu. Također, korisno je pogledati u bilješke s predavanja Samira Sikseka, [51].

1.1. GALOISOVE REPREZENTACIJE PRIDRUŽENE ELIPTIČKIM KRIVULJAMA

Neka je $E/\mathbb{Q}$ eliptička krivulja. Želimo što bolje razumjeti kako Galoisova grupa $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ djeluje na grupu $E[n]$, za prirodni broj n. Kao što ćemo vidjeti tokom ovog rada, analiza tog djelovanja nam može puno reći o samoj grupi $E[n]$. Kako bismo se mogli upustiti u tu analizu, najprije je potrebno znati što je to djelovanje grupe, a i neke osnovne rezultate vezane uz isto.

Definicija. *Neka je G grupa i X skup. Tada je (desno)* ***djelovanje grupe*** *G na X funkcija*

$$X \times G \to X$$
$$(g, x) \to x^g$$

takva da vrijedi

- *(asocijativnost) $x^{gh} = (x^g)^h$, za sve $x \in X$ i sve $g, h \in G$,*
- *$x^e = x$, za svaki $x \in X$, gdje je e jedinica u G.*

Npr. trivijalni primjer djelovanja grupe je taj da grupa G djeluje na samu sebe množenjem. Grupa svih permutacija skupa $\{1, 2, \ldots, n\}$, koju označavamo sa S_n, kanonski djeluje na skup

$\{1,2,\ldots,n\}$. Ako je $\mathbb{K}/\mathbb{F}$ Galoisovo proširenje polja algebarskih brojeva, onda Galoisova grupa $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ djeluje na $\mathbb{K}$.

Mi želimo razumjeti djelovanje grupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ na $E[n]$. Primijetimo da su koordinate svih točaka u $E[n]$ elementi nekih polja algebarskih brojeva. Najmanje polje nad kojim su definirane sve točke iz $E[n]$ (tj. najmanje polje koje sadrži koordinate svih tih točaka) označavamo s $\mathbb{Q}(E[n])$ i nazivamo ***n*-to djelidbeno polje od** E. Promotrimo kanonski homomorfizam

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Gal}\left(\mathbb{Q}(E[n])/\mathbb{Q}\right).$$

Jezgra tog homomorfizma je $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[n])\right)$. Primijetimo da svaki $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[n])\right)$ fiksira polje $\mathbb{Q}(E[n])$, a to znači i da fiksira sve točke u $E[n]$. Dakle, vidimo da je za svaki $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ dovoljno znati kako on djeluje na $\mathbb{Q}(E[n])$.

Potpuno ista razmatranja vrijede ukoliko umjesto baznog poja $\mathbb{Q}$ promatramo bilo koje polje algebarskih brojeva kao bazno. Preciznije, neka je $\mathbb{K}$ polje algebarskih brojeva i $E/\mathbb{K}$ eliptička krivulja. Želimo razumjeti kako $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ djeluje na $E[n]$, a za to je nužno i dovoljno razumjeti kako $\mathrm{Gal}\left(\mathbb{K}(E[n])/\mathbb{K}\right)$ djeluje na $E[n]$.

Sada navodimo osnovne definicije i činjenice vezane uz djelovanje grupa.

Definicija. *Neka grupa G djeluje na skup X i neka je $x \in X$. **Orbita** elementa x je skup svih elemenata iz X u koje se x može preslikati djelovanjem elemenata $g \in G$. Orbitu elementa x označavamo s Gx, dakle*

$$Gx = \{x^g \ : \ g \in G\}.$$

Definicija. *Neka grupa G djeluje na skup X i neka su $g \in G$ te $x \in X$ takvi da je $x^g = x$. U tom slučaju kažemo da je x fiksna točka od g, odnosno da g fiksira x. Za svaki $x \in X$ definiramo **stabilizatorsku podgrupu od** x (ili izotropsku grupu, ili samo stabilizator) kao skup svih elemenata grupe G koji fiksiraju x,*

$$G_x = \{g \in G \ : \ x^g = x\}.$$

Lako se pokaže da je G_x uistinu podgrupa od G. Koristeći Lagrangeov teorem lako se dokazuje

Teorem (o orbiti i stabilizatoru)**.** *Neka je G konačna grupa te X konačan i neprazan skup. Tada je*

$$|Gx| = [G : G_x] = \frac{|G|}{|G_x|}.$$

Primijetimo da je "biti u istoj orbiti" relacija ekvivalencija, dakle, na ovaj način dobivamo particiju skupa X.

Definicija. *Neka je G grupa i X skup. Ako djelovanje grupe G na X ima samo jednu orbitu, tj. ako je $Gx = X$, za svaki $x \in X$, onda kažemo da grupa G djeluje* ***tranzitivno*** *na skup X.*

Kažemo da grupa G djeluje ***vjerno*** *na skup X ako za svaki $g \in G$ različit od e (jedinica u G) postoji $x \in X$ takav da je $x^g \neq x$. Ekvivalentno, ako je $g \in G$ takav da je $x^g = x$, za svaki $x \in X$, onda je $g = e$ (jedinica u G).*

Nas će zanimati činjenice o $E[n]$, npr. koja su minimalna polja definicije elemenata iz $E[n]$. Za to nam je potreban pojam reprezentacije grupa.

Definicija. ***Reprezentacija grupe*** *G na vektorskom prostoru V je preslikavanje grupa*

$$\rho : G \to \mathrm{GL}(V), \quad \textit{takvo da je} \quad \rho(g_1 g_2) = \rho(g_1)\rho(g_2),$$

za sve $g_1, g_2 \in G$. Drugim riječima, to je homomorfizam grupa.

Neka je $E/\mathbb{Q}$ eliptička krivulja. Znamo da je $E[n] \simeq \mathbb{Z}/nZ \oplus \mathbb{Z}/n\mathbb{Z}$ te da $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ djeluje na $E[n]$, tj. automorfizam je od $E[n]$. Dakle, dobivamo preslikavanje

$$\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Na ovaj način smo dobili homomorfizam grupa $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ i $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Sjetimo se da umjesto grupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ možemo promatrati grupu $\mathrm{Gal}\left(\mathbb{Q}(E[n])/\mathbb{Q}\right)$ i ništa se neće promijeniti, to ćemo često prešutno i koristiti.

Definicija. *Upravo opisani homorfizam grupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ (tj. grupe $\mathrm{Gal}\left(\mathbb{Q}(E[n])/\mathbb{Q}\right)$) i grupe $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ nazivamo* ***mod n Galoisova reprezentacija*** *eliptičke krivulje E, inducirana s $E[n]$, za prirodni broj n. Tu reprezentaciju označavamo s $\overline{\rho}_n$, ukoliko nije skroz jasno o kojoj eliptičkoj krivulji E je riječ (a uglavnom hoće biti), onda je uobičajena oznaka $\overline{\rho}_{n,E}$.*

Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je n prirodni broj. Neka je $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(E[n])/\mathbb{Q}\right)$. Neka točke P_1 i P_2 čine bazu za $E[n]$. Tada postoje $\alpha, \beta, \gamma, \delta \in \mathbb{Z}/n\mathbb{Z}$ takvi da je

$$P_1^\sigma = \alpha P_1 + \beta P_2 \quad \text{i} \quad P_2^\sigma = \gamma P_1 + \delta P_2,$$

pri čemu je

$$\overline{\rho}_n(\sigma) = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Činjenica da je $\overline{\rho}_n(\sigma)$ invertibilna matrica slijedi iz činjenice da je σ automorfizam, tj. ima inverz.

Sliku Galoisove mod n reprezentacije u $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (nakon odabira neke fiksne baze za $E[n]$) označavamo s $G_{\mathbb{K}}(n)$ (ili $G_{\mathbb{K},E}(n)$ ukoliko je potrebno istaknuti o kojoj eliptičkoj krivulji $E/\mathbb{Q}$ je riječ). Sjetimo se da kao bazno polje možemo promatrati bilo koje polje algebarskih brojeva $\mathbb{K}$. To ćemo često i činiti kako bismo došli do korisnih informacija o strukturi grupe $G_{\mathbb{K}}(n)$, upravo radi toga u indeksu navodimo o kojem je baznom polju riječ. Preciznije,

$$G_{\mathbb{K}}(n) = \{\overline{\rho}_n(\sigma) \ : \ \sigma \in \mathrm{Gal}\,(\mathbb{K}(E[n])/\mathbb{K})\}.$$

Lema 1.1.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Neka je n prirodan broj i neka je ζ bilo koji n-ti korijen iz jedinice. Tada za svaki $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})$ vrijedi*

$$\sigma(\zeta) = \zeta^{\det \overline{\rho}_n(\sigma)}.$$

Prije samog dokaza ove leme, navedimo osnovno o Weilovom sparivanju, koje nam je potrebno za dokaz. U [53, Chapter III, §8] mogu se naći detalji oko same konstrukcije Weilovog sparivanja kao i dokazi svih potrebnih činjenica. Ovdje ćemo navesti o čemu je točno riječ i koja točno svojstva ima to sparivanje. Dakle, bitno nam je da postoji i da ima svojstva koja ima.

Neka je μ_n skup svih n-tih korijena iz jedinice, tj.

$$\mu_n = \{\omega \in \mathbb{C} \ : \ \omega^n = 1\}.$$

Neka je $\mathbb{K}$ polje algebarskih brojeva i neka je $E/\mathbb{K}$ eliptička krivulja te neka je n prirodni broj. Tada postoji **Weilovo sparivanje**

$$e_n \colon E[n] \times E[n] \to \mu_n$$

koje zadovoljava sljedeća svojstva.

- *Bilinearno je.* Za sve $S, S_1, S_2, T, T_1, T_2 \in E[n]$ je

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2).$$

- *Alternirajuće je.* Za svaki $T \in E[n]$ je

$$e_n(T, T) = 1.$$

  Ekvivalentno, za sve $S, T \in E[n]$ je $e_n(S, T)^{-1} = e_n(T, S)$.

- *Nedegenerirano je.* Ako je $T \in E[n]$ takav da je

$$e_n(S,T) = 1, \quad \text{za sve } S \in E[n],$$

onda je $T = 0$.

- *Galois invarijantno je.* Za sve $S,T \in E[n]$ i za sve $\sigma \in \mathrm{Gal}\left(\mathbb{K}(E[n])/\mathbb{K}\right)$ vrijedi

$$(e_n(S,T))^\sigma = e_n(S^\sigma, T^\sigma).$$

- *Kompatibilno je.* Za svaki prirodni broj m i za sve $S \in E[nm]$ te $T \in E[n]$ vrijedi

$$e_{nm}(S,T) = e_n(mS,T).$$

Sada smo spremni za dokaz leme 1.1.1.

Dokaz leme 1.1.1. Neka je $\{P,Q\}$ baza za $E[n]$ i neka je $e_n(P,Q) = \zeta_n$, gdje je ζ_n n-ti primitivni korijen iz jedinice, a e_n upravo spomenuto Weilovo sparivanje.

Kako je ζ_n primitivni n-ti korijen iz jedinice, znamo da postoji prirodan broj m takav da je $\zeta = \zeta_n^m$. Nadalje, $\det\colon \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ je homomorfizam grupa, stoga je dovoljno pokazati da je $\sigma(\zeta_n) = \zeta_n^{\det \overline{\rho}_n(\sigma)}$.

Neka su $a,b,c,d \in (\mathbb{Z}/n\mathbb{Z})^\times$ takvi da je

$$P^\sigma = aP + bQ \qquad \text{i} \qquad Q^\sigma = cP + dQ.$$

Koristeći svojstva Weilovog sparivanja računamo:

$$\begin{aligned}\sigma(\zeta_n) = \sigma(e_n(P,Q)) &= e_n(P^\sigma, Q^\sigma) = e_n(aP+bQ, cP+dQ)\\ &= e_n(P,P)^{ac} e_n(P,Q)^{ad} e_n(Q,P)^{bc} e_n(Q,Q)^{bd}\\ &= 1^{ac} \cdot \zeta_n^{ad} \cdot \zeta_n^{-bc} \cdot 1^{bd} = \zeta_n^{\det \overline{\rho}_n(\sigma)}.\end{aligned}$$

■

Propozicija 1.1.2. *Neka je $E/\mathbb{K}$ eliptička krivulja, gdje je $\mathbb{K}$ polje algebarskih brojeva. Neka je n prirodan broj i neka je ζ_n n-ti primitivni korijen iz jedinice. Tada je*

$$\det G_{\mathbb{K}}(n) \simeq \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{K} \cap \mathbb{Q}(\zeta_n)\right).$$

Napomena. $\det G_{\mathbb{K}}(n) = \left\{\det \overline{\rho}_n(\sigma) : \sigma \in \mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)\right\}$.

Dokaz. Svaki $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ jedinstveno je određen svojim djelovanjem na ζ_n. Preciznije, za svaki $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ postoji $\sigma_a \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ takav da je $\sigma_a(\zeta_n) = \zeta_n^a$ i obratno, za svaki $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ postoji $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ takav da je $\sigma = \sigma_a$. Neka je g kanonski izomorfizam

$$g\colon (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q}),$$
$$g(a) = \sigma_a.$$

Neka je sada $f\colon \mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right) \to \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ definirana s

$$f = g \circ \det \circ \overline{\rho}_n.$$

Znamo da je $\det G_{\mathbb{K}}(n) \leq (\mathbb{Z}/n\mathbb{Z})^\times$, zato je $f\left(\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)\right) \leq \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, a to po Galoisovoj teoriji, znači da je $f\left(\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)\right) = \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{K}')$, za neko potpolje $\mathbb{K}' \subseteq \mathbb{Q}(\zeta_n)$.

Iz prethodne leme 1.1.1 slijedi da je preslikavanje f zapravo restrikcija koja $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ šalje u $\sigma\big|_{\mathbb{Q}(\zeta_n)} = \sigma_{\det\overline{\rho}_n(\sigma)}$.

Konačno, slijedi da se $f\left(\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)\right)$ sastoji od točno onih σ_a koji fiksiraju $\mathbb{K} \cap \mathbb{Q}(\zeta_n)$, čime je dokazano da je $\mathbb{K}' = \mathbb{K} \cap \mathbb{Q}(\zeta_n)$. ■

Također, bit će nam potrebno poznavanje Tateovog modula, za detalje je najbolje pogledati [53, Chapter III, §7].

Definicija. *Neka je $E/\mathbb{K}$ eliptička krivulja i neka je ℓ prost broj.* ***Tateov modul*** *(ℓ-adski) pridružen eliptičkoj krivulji E je grupa*

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

gdje inverzni limes promatramo kroz prirodna preslikavanja

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Definicija. *Neka je $E/\mathbb{K}$ eliptička krivulja i neka je ℓ prost broj. Eliptičkoj krivulji E pridružujemo* ***ℓ-adsku Galoisovu reprezentaciju***

$$\rho_\ell\colon \mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right) \to \mathrm{Aut}(T_\ell(E))$$

induciranu djelovanjem grupe $\mathrm{Gal}\left(\overline{\mathbb{K}}/\mathbb{K}\right)$ *na Tateov modul $T_\ell(E)$.*

U više navrata će nam se pokazati korisnim rezultat [20, Theorem 2], stoga ga radi potpunosti i navodimo.

Teorem 1.1.3. *Broj* $[\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : \mathrm{Img}(\rho_5)]$ *nije djeljiv s* 25.

1.2. DJELIDBENI POLINOMI

Djelidbeni polinomi nam pružaju eksplicitni način baratanja s torzijskim točkama eliptičke krivulje. Iako daju manje informacija od Galoisovih reprezentacija, često će nam biti korisni.

Neka je $E/\mathbb{Q}$ eliptička krivulja zadana jednadžbom

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

i neka je

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^3 + 4a_6, \quad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Gledamo dugu Weierstrassovu formu radi pune općenitosti, iako bismo nad poljem $\mathbb{Q}$ (zapravo nad bilo kojim poljem karakteristike različite od 2 i 3) sve mogli izložiti koristeći kratku Weierstrassovu formu.

Za svaki prirodni broj m definiramo **djelidbeni polinom** $\psi_m \in \mathbb{Q}[x,y]$:

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4 &= \psi_2 \cdot (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)),
\end{aligned}$$

te dalje rekurzivno

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, && \text{za } m \geq 2,\\
\psi_{2m} &= (\psi_2)^{-1}(\psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2), && \text{za } m \geq 3.
\end{aligned}$$

Lako se vidi da je ψ_{2m} uistinu polinom za prirodni broj m. Naime, dovoljno je primijetiti da je polinom ψ_{2m} djeljiv polinomom ψ_2, za svaki prirodni broj m (indukcija).

Nadalje, za prirodni broj $m \geq 2$, definiramo polinome

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= (4y)^{-1}(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Lako se pokaže sljedeće:

- Ako je $m \geq 3$ neparan prirodni broj, onda su polinomi ψ_m, ϕ_m i $y^{-1}\omega_m$ zapravo polinomi u varijablama x i $(2y+a_1x+a_3)^2$.

- Slično, ako je m paran prirodni broj, vrijedi da su polinomi $(2y+a_1x+a_3)^{-1}\psi_m$, ϕ_m i ω_m također polinomi u varijablama x i $(2y+a_1x+a_3)^2$.

Dakle, zamijenimo li $(2y+a_1x+a_3)^2$ s $4x^3+b_2x^2+2b^4x+b_6$, vidimo da je svaki od tih polinoma zapravo polinom u varijabli x. Tako ćemo ih i promatrati.

Sljedeću činjenicu navodimo bez dokaza. Dokaz je potpuno tehnički i za detalje je zgodno pogledati u [42, 44, 53].

Propozicija. *Neka je $P=(x,y)$ točka na eliptičkoj krivulji E s jednadžbom (1.1). Neka je $n \geq 2$ prirodni broj, tada je*

$$nP = \left(\frac{\phi_n(x,y)}{\psi_n^2(x,y)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)} \right).$$

Nadalje, primijetimo da su nultočke djelidbenog polinoma ψ_n zapravo x-koordinate točaka iz $E[n]$. Štoviše, sve x-koordinate točaka iz $E[n]$, osim točke 0, su nultočke polinoma ψ_n.

Treba biti oprezan, ne odgovara svaka nultočka polinoma ψ_n x-koordinati točke reda n, već x-koordinati točke P takve da je $nP=0$, to ne znači da je P reda n. Ukoliko želimo, za prost broj p, naći x-koordinate točaka reda p^{m+1} (za neki prirodni broj m), to će biti upravo nultočke polinoma $\dfrac{\psi_{p^{m+1}}}{\psi_{p^m}}$.

Komentirajmo još sljedeće. Ako ψ_n ima nultočku nad nekim poljem algebarskih brojeva $\mathbb{K}$, to ne znači nužno da nad tim poljem eliptička krivulja E ima točku P takvu da je $nP=0$. Naime, ne mora nužno i y koordinata biti definirana nad $\mathbb{K}$. No, ono što znamo je da će sigurno biti definirana nad nekim kvadratnim proširenjem od $\mathbb{K}$.

Poznato je da se djelidbeni polinomi eliptičkih krivulja s istim j-invarijantama podudaraju do na multiplikativnu konstantu. Preciznije, neka su $E/\mathbb{K}$ i $E'/\mathbb{K}$ eliptičke krivulje nad poljem algebarskih brojeva $\mathbb{K}$ te neka je n prirodni broj. Neka su ψ_n i ψ_n', redom n-ti djelidbeni polinomi eliptičkih krivulja E i E'. Tada postoji broj $0 \neq d \in \mathbb{K}$ takav da je $\psi_n' = d\psi_n$.

To zapravo znači da je skup nultočaka polinoma ψ_n' isti kao skup nultočaka polinoma ψ_n. Ovu činjenicu ćemo često koristiti bez da se posebno referiramo na nju. Naime, iz nekog (uglavnom torzijskog) svojstva eliptičke krivulje $E/\mathbb{K}$ ponekad možemo zaključiti koja je (jedna ili njih konačno mnogo) mogućnost za $j(E)$. U tom trenutku možemo odabrati proizvoljnu eliptičku krivulju $E'/\mathbb{K}$ takvu da je $j(E')=j(E)$ i na taj način odrediti skup nultočaka bilo kojeg djelidbenog polinoma eliptičke krivulje E.

1.3. MODULARNE KRIVULJE

U ovoj sekciji slijedimo [12, Chapter 1]. Navest ćemo osnovno o *modularnim krivuljama* koje će istovremeno biti kvocijent gornje poluravnine po nekoj matričnoj grupi i *prostor parametara* klasa izomorfizama eliptičkih krivulja skupa s nekim (torzijskim) svojstvom.

Modularna grupa je grupa

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

Riemannova sfera je skup kompleksnih brojeva proširen s "točkom u beskonačnosti", tj.

$$\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}.$$

Svaki element modularne grupe možemo promatrati kao automorfizam Riemannove sfere na sljedeći način: neka je $\tau \in \hat{\mathbb{C}}$, tada je

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau+b}{c\tau+d}.$$

Komentirajmo što se zbiva s točkom ∞:

$$\text{ako je } c \neq 0, \text{ onda} \quad -\frac{d}{c} \to \infty \to \frac{a}{c},$$
$$\text{ako je } c = 0, \text{ onda} \quad \infty \to \infty.$$

Modularna grupa je generirana matricama

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{i} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

To znači da se sve transformacije Riemannove sfere definirane elementima iz modularne grupe mogu dobiti kompozicijama funkcija

$$\tau \to \tau+1 \quad \text{i} \quad \tau \to -\frac{1}{\tau}.$$

Gornja poluravnina je skup kompleksnih brojeva čiji je imaginarni dio pozitivan, tj.

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

Neka je $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, primijetimo da je

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2},$$

dakle modularna grupa šalje gornju poluravninu u gornju poluravninu.

Definicija. *Neka je N prirodni broj.* ***Glavna kongruencijska podgrupa nivoa*** *N je grupa*

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

Primijetimo da bismo glavnu kongruencijsku podgrupu mogli definirati i kao jezgru kanonske "redukcije modulo n"

$$\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Definicija. *Podgrupa Γ od $\mathrm{SL}_2(\mathbb{Z})$ je* ***kongruencijska podgrupa*** *ako postoji prirodni broj N takav da je $\Gamma(N) \leq \Gamma$. Nivo kongruencijske podgrupe Γ je najmanji prirodni broj N takav da je $\Gamma(N) \leq \Gamma$.*

Primijetimo da je, za svaki prirodni broj N, glavna kongruencijska podgrupa $\Gamma(N)$ konačnog indeksa u grupi $\mathrm{SL}_2(\mathbb{Z})$, što znači da je svaka kongruencijska podgrupa također konačnog indeksa u $\mathrm{SL}_2(\mathbb{Z})$.

Osim glavne kongruencijske podgrupe, bit će nam važne i sljedeće dvije kongruencijske podgrupe.

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

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

Primijetimo da je

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

Definicija. ***Rešetka*** *$\Lambda \subset \mathbb{C}$ je diskretna podgrupa ranga 2, tj.*

$$\Lambda = \mathbb{Z}\lambda_1 + \mathbb{Z}\lambda_2,$$

gdje su λ_1 i λ_2 kompleksni brojevi linearno nezavisni nad $\mathbb{R}$.

Primijetimo da je baza $\{\lambda_1, \lambda_2\}$ jedinstvena do na $\mathrm{GL}_2(\mathbb{Z})$.

Napomenimo da više detalja o eliptičkim krivuljama $E/\mathbb{C}$ možemo naći u [53, Chapter VI]. Bez dokaza navodimo idući teorem koji nam je bitan za daljnja razmatranja.

Teorem. *Neka je $E/\mathbb{C}$ eliptička krivulja, tada postoji rešetka $\Lambda \subset \mathbb{C}$ takva da je*

$$E \simeq \mathbb{C}/\Lambda.$$

Radi gornjih opservacija znamo da svakoj eliptičkoj krivulji $E/\mathbb{C}$ možemo pridružiti rešetku $\Lambda \subset \mathbb{C}$ i to takvu da je

$$\Lambda = \mathbb{Z} + \tau\mathbb{Z},$$

gdje je $\tau \in \mathscr{H}$. Primijetimo da za svaki $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ vrijedi da su Λ i $\mathbb{Z} + \gamma(\tau)\mathbb{Z}$ iste rešetke (zapravo vrijedi i obrat). Vidimo da zapravo možemo poistovjetiti sve elemente $\tau_1, \tau_2 \in \mathscr{H}$ za koje postoji $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ takva da je $\gamma(\tau_1) = \tau_2$. Preciznije, promatramo kvocijent

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathscr{H} = \{\mathrm{SL}_2(\mathbb{Z})\tau \ : \ \tau \in \mathscr{H}\}.$$

Dakle, dobili smo bijekciju među skupovima

$$\{\text{eliptičke krivulje nad } \mathbb{C} \text{ do na izomorfizam}\} \qquad \longleftrightarrow \qquad \mathrm{SL}_2(\mathbb{Z})\backslash\mathscr{H}.$$

Kažemo da je $\mathrm{SL}_2(\mathbb{Z})\backslash\mathscr{H}$ **prostor parametara** za eliptičke krivulje. Vidjet ćemo da na sličan način grupe $\Gamma(N)$, $\Gamma_0(N)$ i $\Gamma_1(N)$ generiraju prostor parametara eliptičkih krivulja s nekim (torzijskim) svojstvom.

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

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

Objasnimo najprije pojmove vezane uz eliptičke krivulje definirane nad poljem kompleksnih brojeva Kasnije ćemo objasniti što se događa nad poljima algebarskih brojeva. Uvedimo najprije notaciju

$$[E, \text{objekt na } E],$$

gdje je E eliptička krivulja. Tom notacijom označavamo klasu izomorfizma eliptičkih krivulja i pripadajućih objekata. Vrste objekata koje promatramo su sljedeće.

- Podgrupa grupe točaka na E reda N, za neki prirodni broj N, u oznaci C. Ekvivalentno, jezgra N-izogenije. Reći ćemo da su parovi (E,C) i (E',C') izomorfni (oba pripadaju klasi $[E,C]$) ako postoji izomorfizam eliptičkih krivulja $f\colon E \to E'$ takav da je $f(C) = C'$.

- Točka $P \in E$ reda N, za neki prirodni broj N. Reći ćemo da su parovi (E,P) i (E,P') izomorfni (oba pripadaju klasi $[E,P]$) ako postoji izomorfizam eliptičkih krivulja $f\colon E \to E'$ takav da je $f(P) = P'$.

- Uređeni par (P,Q) točaka na E takvih da je

$$\langle P,Q\rangle \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \quad \text{i} \quad e_N(P,Q) = e^{\frac{2\pi i}{N}},$$

  gdje je N prirodni broj, a e_N Weilovo sparivanje (pogledati na stranicu 8). Reći ćemo da su parovi $(E,(P,Q))$ i $(E',(P',Q'))$ izomorfni (tj. da pripadaju istoj klasi $[E,(P,Q)]$) ako postoji izomorfizam eliptičkih krivulja $f\colon E \to E'$ takav da je $f(P) = P'$ i $f(Q) = Q'$.

Sada definiramo sljedeće skupove (E je eliptička krivulja, a N prirodni broj):

$$\begin{aligned}
S_0(N) &= \{[E,C] \ : \ C \text{ je podgrupa grupe točaka na } E \text{ reda } N\},\\
S_1(N) &= \{[E,P] \ : \ P \text{ je točka reda } N \text{ na } E\},\\
S(N) &= \left\{[E,(P,Q)] \ : \ P,Q \in E, \quad \langle P,Q\rangle \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}, \quad e_N(P,Q) = e^{\frac{2\pi i}{N}}\right\}.
\end{aligned}$$

Nadalje, označimo modularne krivulje za (tj. kvocijentne prostore orbita od) $\Gamma_0(N)$, $\Gamma_1(N)$ i $\Gamma(N)$ sa

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

Također, napomenimo da, za $\tau \in \mathscr{H}$, sa E_τ označavamo pripadajuću klasu izomorfizama eliptičkih krivulja $\mathbb{C}/\Lambda_\tau$, gdje je $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$.

Sada smo spremni iskazati važan teorem koji nam govori što točno parametrizira svaka od spomenutih modularnih krivulja.

Teorem. *Neka je N prirodni broj.*

(a) Skup $Y_0(N) = \Gamma_0(N)\backslash\mathscr{H}$ je prostor parametara za

$$S_0(N) = \left\{\left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right] \ : \ \tau \in \mathscr{H}\right\}.$$

Dvije točke $\left[E_\tau, \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle\right]$ i $\left[E_{\tau'}, \left\langle \frac{1}{N} + \Lambda_{\tau'} \right\rangle\right]$ su jednake ako i samo ako je

$$\Gamma_0(N)\tau = \Gamma_0(N)\tau'.$$

Dakle, postoji bijekcija

$$\begin{aligned} S_0(N) &\xrightarrow{\sim} Y_0(N), \\ \left[E_\tau, \left\langle \tfrac{1}{N} + \Lambda_\tau \right\rangle\right] &\to \Gamma_0(N)\tau. \end{aligned}$$

(b) Skup $Y_1(N) = \Gamma_1(N)\backslash\mathscr{H}$ *je prostor parametara za*

$$S_1(N) = \left\{ \left[E_\tau, \frac{1}{N} + \Lambda_\tau \right] \ : \ \tau \in \mathscr{H} \right\}.$$

Dvije točke $\left[E_\tau, \frac{1}{N} + \Lambda_\tau\right]$ *i* $\left[E_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right]$ *su jednake ako i samo ako je*

$$\Gamma_1(N)\tau = \Gamma_1(N)\tau'.$$

Dakle, postoji bijekcija

$$\begin{aligned} S_1(N) &\xrightarrow{\sim} Y_1(N), \\ \left[E_\tau, \tfrac{1}{N} + \Lambda_\tau\right] &\to \Gamma_1(N)\tau. \end{aligned}$$

(c) Skup $Y(N) = \Gamma(N)\backslash\mathscr{H}$ *je prostor parametara za*

$$S(N) = \left\{ \left[E_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau \right) \right] \ : \ \tau \in \mathscr{H} \right\}.$$

Dvije točke $\left[E_\tau, \left(\frac{\tau}{N} + \Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right)\right]$ *i* $\left[E_{\tau'}, \left(\frac{\tau'}{N} + \Lambda_{\tau'}, \frac{1}{N} + \Lambda_{\tau'}\right)\right]$ *su jednake ako i samo ako je*

$$\Gamma(N)\tau = \Gamma(N)\tau'.$$

Dakle, postoji bijekcija

$$\begin{aligned} S(N) &\xrightarrow{\sim} Y(N), \\ \left[E_\tau, \left(\tfrac{\tau}{N} + \Lambda_\tau, \tfrac{1}{N} + \Lambda_\tau\right)\right] &\to \Gamma(N)\tau. \end{aligned}$$

Primijetimo da ako specijaliziramo $N = 1$, dobivamo da je

$$Y_0(1) = Y_1(1) = Y(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathscr{H}$$

te svaka od ovih modularnih krivulja u tom slučaju predstavlja naprosto skup klasa izomorfizama eliptičkih krivulja (nad $\mathbb{C}$).

Skupovi $Y_0(N)$, $Y_1(N)$ i $Y(N)$ nisu kompaktni. Kako bismo ih kompaktificirali najprije definiramo

$$\mathscr{H}^* = \mathscr{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Sada, za kongruencijsku podgrupu Γ definirajmo

$$X(\Gamma) = \Gamma\backslash\mathscr{H}^*.$$

Dakle, $X(\Gamma)$ jednak je uniji skupa $Y(\Gamma)$ i konačnog skupa klasa elemenata iz $\mathbb{Q} \cup \{\infty\}$ koji se zovu kaspovi.

Može se pokazati da $X_0(N)$, $X_1(N)$ i $X(N)$ imaju strukturu Riemannove plohe te da su i algebarske krivulje. Iz toga slijedi da su i $Y_0(N)$, $Y_1(N)$ te $Y(N)$ algebarske krivulje. Štoviše, $Y_0(N)$ i $Y_1(N)$ se mogu definirati nad $\mathbb{Q}$, dok se $Y(N)$ može definirati nad $\mathbb{Q}(\zeta_N)$, gdje je ζ_N primitivni N-ti korijen iz 1. Više detalja o ovoj temi, kao i same dokaze moguće je pronaći u [12, Chapter 2]

Napomena. *Točke u $S_0(N)$, $S_1(N)$ i $S(N)$ određuju krivulje skupa s nekom strukturom "do na izomorfizam". Ako zanemarimo na trenutak tu strukturu i promatramo samo eliptičku krivulju, nameće se prirodno pitanje – nad kojim poljem je taj izomorfizam definiran? Odgovor je sljedeći.*

- *Točka na $S_0(N)$ koja je $\mathbb{K}$-racionalna definira eliptičku krivulju E do na $\overline{\mathbb{K}}$-izomorfizam.*
- *Točka na $S_1(N)$, odnosno točka na $S(N)$ koja je $\mathbb{K}$-racionalna definira eliptičku krivulju E do na $\mathbb{K}$-izomorfizam.*

Prostor parametara $S_0(N)$ je primjer *grubog* prostora parametara koji razaznaje elemente do na izomorfizam nad algebarskih zatvorenjem. Prostori parametara $S_1(N)$ (za $N \geq 5$) i $S(N)$ (za $N \geq 3$) su primjeri *finih* prostora parametara koji razaznaju elemente do na izomorfizam definiran nad tim poljem.

Spomenimo još sljedeći pojam: **Jakobijan** modularne (tj. bilo koje algebarske) krivulje. Nećemo ulaziti u detalje (koji se mogu naći u npr. [51, Chapter 5]). Zapravo nam je jedino bitno znati da za svaku modularnu (tj. za bilo koju algebarsku) krivulju X postoji Abelova mnogostrukost J_X s nekim lijepim svojstvima.

Naime, ako je $\mathbb{K}$ polje algebarskih brojeva, onda je grupa $\mathbb{K}$-racionalnih točaka na X u funkcijskom odnosu s grupom $\mathbb{K}$-racionalnih točaka na J_X. Dodatno, grupa $J_X(\mathbb{K})$ je konačno generirana Abelova grupa. Na ovaj način možemo proučavajući Jakobijan krivulje saznati neke iznimno vrijedne informacije o samoj krivulji. Na nekoliko mjesta u ovom radu upravo to i radimo. Pogledati npr. dokaze leme 3.4.3.

1.4. KVADRATNI TWIST

U ovoj sekciji u jako kratkim crtama želimo prikazati što je to kvadratni twist eliptičke krivulje. Također, istaknut ćemo neka svojstva koja ćemo tokom rada koristiti bez da se posebno referiramo na njih. Naime, ti rezultati se smatraju "opće poznatima". Za detalje svakako pogledati [53, Chapter X, §5].

Neka je $E/\mathbb{Q}$ eliptička krivulja s Weierstrassovom jednadžbom

$$y^2 = f(x),$$

te neka je d kvadratno slobodan cijeli broj. **Kvadratni twist** eliptičke krivulje E za d, koji ćemo označiti s $E^{(d)}$ je eliptička krivulju s jednadžbom

$$dy^2 = f(x).$$

Neka je $E/\mathbb{Q}$ eliptička krivulja, neka je d kvadratno slobodan cijeli broj i neka je n neparni prirodni broj. Nadalje, neka je $\mathbb{K}$ polje algebarskih brojeva koje ne sadrži $\sqrt{d}$, tada je

$$E(\mathbb{K}(\sqrt{d}))[n] \simeq E(\mathbb{K})[n] \oplus E^{(d)}(\mathbb{K})[n].$$

Nadalje, vrijedi i (pogledati npr. u [1])

$$\mathrm{rk}(E(\mathbb{K}(\sqrt{d}))) = \mathrm{rk}(E(\mathbb{K})) + \mathrm{rk}(E^{(d)}(\mathbb{K})).$$

2. $\mathbb{Z}_p$-PROŠIRENJE

2.1. ŠTO JE TO $\mathbb{Z}_p$-PROŠIRENJE?

Ono što će se u ovom radu proučavati je $\mathbb{Z}_p$-proširenje polja racionalnih brojeva. Točnije, zanima nas ponašanje torzijske grupe nad $\mathbb{Z}_p$-proširenjima od $\mathbb{Q}$ eliptičkih krivulja definiranih nad $\mathbb{Q}$. No prije ikakvog govora o tome, potrebno je saznati što je to $\mathbb{Z}_p$-proširenje od $\mathbb{Q}$. Radi potpunosti to i izlažemo u ovom poglavlju.

Definicija. *Neka je $\mathbb{F}$ polje algebarskih brojeva i neka je p prost broj. Beskonačno Galoisovo proširenje $\mathbb{F}_\infty/\mathbb{F}$ naziva se $\mathbb{Z}_p$-proširenje ako je topološka grupa $\mathrm{Gal}\,(\mathbb{F}_\infty/\mathbb{F})$ izomorfna aditivnoj grupi p-adskih cijelih brojeva, $\mathbb{Z}_p$.*

Ovdje podrazumijevamo poznavanje pojmova kao što su polje algebarskih brojeva, beskonačno Galoisovo proširenje, topološka grupa, p-adski cijeli brojevi. Osnovno o svemu navedenom može se naći u [44].

Objasnimo, ukratko, o kojoj je točno topologiji riječ na grupi $G = \mathrm{Gal}\,(\mathbb{F}_\infty/\mathbb{F})$. Naime, to će nam biti bitno jer smo onda u stanju, koristeći fundamentalni teorem beskonačne Galoisove teorije, odrediti sva međupolja proširenja $\mathbb{F}_\infty/\mathbb{F}$.

Na grupi G promatramo prirodnu topologiju, koja se zove *Krullova topologija* (više o tome može se naći u [49]), a definirana je na sljedeći način. Definiramo kolekciju skupova u G koji čine bazu otvorenih skupova oko 1 (tj. oko trivijalnog automorfizma):

$$\{\mathrm{Gal}\,(\mathbb{F}_\infty/\mathbb{K}) \ : \ \mathbb{K} \text{ polje takvo da je } \mathbb{F}_\infty \supset \mathbb{K} \supseteq \mathbb{F} \text{ i } [\mathbb{K}:\mathbb{F}] < \infty\}.$$

Odnosno, skup $U \subseteq G$ je u bazi otvorenih skupova oko 1 ako i samo ako postoji međupolje $\mathbb{F}_\infty \supset \mathbb{K} \supseteq \mathbb{F}$ takvo da je stupanj $[\mathbb{K}:\mathbb{F}]$ konačan i za sve $\sigma \in U$ vrijedi da je $\sigma\big|_{\mathbb{K}} = 1\big|_{\mathbb{K}}$.

Ono što nam je sada potrebno je tzv. fundamentalni teorem beskonačne Galoisove teorije, više detalja o njemu može se naći u npr. [38].

Postoji bijekcija (analogon one u konačnoj Galoisovoj teoriji) između skupova

$$\{\text{zatvorene podgrupe od } \mathrm{Gal}\,(\mathbb{F}_\infty/\mathbb{F})\} \qquad \longleftrightarrow \qquad \{\text{međupolja proširenja } \mathbb{F}_\infty/\mathbb{F}\}\,.$$

Zatvorena podgrupa H odgovara međupolju kojeg fiksiraju automorfizmi sadržani u H i obratno.

Kako je $\mathrm{Gal}\,(\mathbb{F}_\infty/\mathbb{F}) \simeq \mathbb{Z}_p$ i kako su sve zatvorene podgrupe (osim trivijalne) od $\mathbb{Z}_p$ oblika $p^n\mathbb{Z}_p$ (za prirodan broj n), zaključujemo da sva međupolja proširenja $\mathbb{F}_\infty/\mathbb{F}$ formiraju toranj

$$\mathbb{F} = \mathbb{F}_0 \subset \mathbb{F}_1 \subset \mathbb{F}_2 \subset \mathbb{F}_3 \subset \ldots \subset \mathbb{F}_\infty.$$

Ovdje je, za svaki prirodni broj n, $\mathbb{F}_n$ jedinstveno polje stupnja p^n nad $\mathbb{F}$, sadržano u $\mathbb{F}_\infty$. To međupolje nazivamo n-tim *slojem* $\mathbb{Z}_p$-proširenja $\mathbb{F}_\infty/\mathbb{F}$.

Kao što ćemo vidjeti u nastavku, svako polje algebarskih brojeva ima barem jedno $\mathbb{Z}_p$-proširenje, tzv. *ciklotomsko* $\mathbb{Z}_p$-proširenje. Neka je $\mathbb{F}$ polje koje je sadržano u $\mathbb{Q}^{\mathrm{ab}}$, tj. u maksimalnom Abelovom proširenju od $\mathbb{Q}$, onda je poznato da je ciklotomsko proširenje polja $\mathbb{F}$ jedino $\mathbb{Z}_p$-proširenje tog polja. Ako je $\mathbb{F}$ totalno realno polje, koje nije nužno sadržano u $\mathbb{Q}^{\mathrm{ab}}$, onda Leopoldtova slutnja [34] govori da je i u tom slučaju istina da je ciklotomsko proširenje polja $\mathbb{F}$ jedino $\mathbb{Z}_p$-proširenje tog polja, no, to je i dalje otvoren problem. Ukoliko polje $\mathbb{F}$ nije totalno realno, onda je poznato da postoji beskonačno mnogo različitih $\mathbb{Z}_p$-proširenja polja $\mathbb{F}$.

U nastavku opisujemo konstrukciju spomenutog ciklotomskog proširenja. Neka je, za prirodni broj n:

$$\mu_n = \{\omega \in \mathbb{C} \,:\, \omega^n = 1\},$$

skup svih n-tih korijena iz jedinice. Nadalje, neka je

$$\mu_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mu_{p^n},$$

skup svih $\omega \in \mathbb{C}$ za koje postoji neki prirodni broj n takav da je $\omega^{p^n} = 1$. Primijetimo da je

$$\mathbb{Q}(\mu_{p^n}) = \mathbb{Q}(\zeta_{p^n}) \quad \text{i} \quad \mathbb{Q}(\mu_{p^\infty}) = \prod_{n\in\mathbb{N}} \mathbb{Q}(\zeta_{p^n}),$$

gdje je sa ζ_n standardno označen n-ti primitivni korijen iz 1.

Znamo da za svaki prost broj $\boxed{p \geq 3}$ i za svaki prirodni broj n vrijedi da je

$$\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times \simeq (\mathbb{Z}/(p-1)\,\mathbb{Z}) \oplus \left(\mathbb{Z}/p^{n-1}\mathbb{Z}\right).$$

Dakle, zaključujemo da je

$$\mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}\,(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq \varprojlim_n \left((\mathbb{Z}/p^n\mathbb{Z})^\times\right) \simeq \Delta_p \oplus \mathbb{Z}_p,$$

gdje je $\Delta_p \subseteq \mathrm{Gal}\,(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ i $\Delta_p \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

Sada naprosto definiramo da je

$$\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^{\Delta_p}.$$

Za općenito polje algebarskih brojeva $\mathbb{F}$ definiramo $\mathbb{F}_\infty = \mathbb{F}\mathbb{Q}_\infty$, vidimo da je $\mathrm{Gal}\,(\mathbb{F}_\infty/\mathbb{F}) \simeq \mathbb{Z}_p$, tj. ovo proširenje uistinu jest $\mathbb{Z}_p$-proširenje.

Primijetimo da smo ovime zapravo odredili i svaki sloj konstruiranog $\mathbb{Z}_p$-proširenja. Naime, vrijedi da je

$$\mathbb{Q}_n = \mathbb{Q}_\infty \cap \mathbb{Q}(\mu_{p^{n+1}}).$$

U slučaju $p = 2$ je naprosto $\mathbb{Q}_n = \mathbb{Q}\left(\cos\left(\frac{\pi}{2^{n+1}}\right)\right)$ te $\mathbb{Q}_\infty = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n$. Ovdje je zgodno primijetiti da je zapravo

$$\mathbb{Q}_n = \mathbb{Q}\left(\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}\right),$$

gdje se $\sqrt{\ }$ pojavljuje n puta.

Više detalja o općenitim $\mathbb{Z}_p$-proširenjima i Iwasawinoj teoriji može se naći u [56].

Napomenimo još da je, za $p \geq 3$,

$$\mathbb{Q}_n = \mathbb{Q}(\mu_{p^{n+1}})^+,$$

što je maksimalno realno potpolje od $\mathbb{Q}(\mu_{p^{n+1}})$. Također, za $p = 2$ vrijedi da je

$$\mathbb{Q}_n = \mathbb{Q}(\mu_{2^{n+2}})^+.$$

2.2. $\mathbb{Z}_p$-PROŠIRENJE OD $\mathbb{Q}$

Kao što će uskoro biti pokazano (Teorem 2.2.1), spomenuto ciklotomsko $\mathbb{Z}_p$-proširenje je jedino $\mathbb{Z}_p$-proširenje od $\mathbb{Q}$. Uvedimo oznake:

- $\mathbb{Q}_{\infty,p}$ je ciklotomsko $\mathbb{Z}_p$-proširenje od $\mathbb{Q}$,
- $\mathbb{Q}_{n,p}$ je n-ti sloj proširenja $\mathbb{Q}_{\infty,p}/\mathbb{Q}$, tj. imamo

$$\mathbb{Q} = \mathbb{Q}_{0,p} \subset \mathbb{Q}_{1,p} \subset \mathbb{Q}_{2,p} \subset \cdots \subset \mathbb{Q}_{\infty,p}.$$

Prisjetimo se da je $[\mathbb{Q}_{n,p} : \mathbb{Q}] = p^n$ te da je

$$\mathbb{Q}_{\infty,p} = \mathbb{Q}(\mu_{p^\infty})^{\Delta_p} \quad \text{i} \quad \mathbb{Q}_{n,p} = \mathbb{Q}(\mu_{p^{n+1}}) \cap \mathbb{Q}_{\infty,p},$$

za prost broj $p \geq 3$ i

$$\mathbb{Q}_{n,2} = \mathbb{Q}\left(\underbrace{\sqrt{2+\sqrt{2+\cdots+\sqrt{2}}}}_{n \text{ pojavljivanja } \sqrt{\ }}\right) \quad \text{te} \quad \mathbb{Q}_{\infty,2} = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_{n,2}.$$

Teorem 2.2.1. *Neka je p prost broj i $\mathbb{K}$ polje koje je $\mathbb{Z}_p$-proširenje polja $\mathbb{Q}$. Tada je*

$$\mathbb{K} = \mathbb{Q}_{\infty,p}.$$

Dakle, ovaj teorem govori da je ciklotomsko $\mathbb{Z}_p$-proširenje jedino $\mathbb{Z}_p$-proširenje polja racionalnih brojeva.

Dokaz. U ovom dokazu ćemo koristiti uobičajene oznake, tj. sa $\mathbb{Z}_q^+$ ćemo označiti aditivnu grupu q-adskih cijelih brojeva, dok ćemo sa $\mathbb{Z}_q^\times$ označiti multiplikativnu grupu invertibilnih q-adskih cijelih brojeva. Neka je μ_∞ skup svih korijena iz jedinice. Kronecker - Weberov teorem (pogledati u [33, str. 210, Corollary 3.]) govori da se svako Abelovo proširenje polja $\mathbb{Q}$ nalazi u $\mathbb{Q}(\mu_\infty)$. Kako je $\mathbb{K}/\mathbb{Q}$ Abelovo proširenje, zaključujemo da je $\mathbb{K} \subseteq \mathbb{Q}(\mu_\infty)$. Nadalje, znamo da je (opet pogledati u [33, §10])

$$\mathrm{Gal}\,(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \simeq \prod_{q \text{ prost}} \mathbb{Z}_q^\times = \hat{\mathbb{Z}}^\times.$$

Zaključujemo da je $\mathbb{Z}_p^+ \simeq \mathrm{Gal}\,(\mathbb{K}/\mathbb{Q})$ kvocijent od $\hat{\mathbb{Z}}^\times$. Poznato je da grupa $\mathbb{Z}_p^+$ nema torzije (vidjeti u [18]) pa zaključujemo da jezgra kanonskog homomorfizma

$$\mathrm{Gal}\,(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \to \mathrm{Gal}\,(\mathbb{K}/\mathbb{Q})$$

sadrži $(\hat{\mathbb{Z}}^\times)_{\text{tors}}$, što zapravo znači da je $\text{Gal}\,(\mathbb{K}/\mathbb{Q})$ kvocijent od

$$\hat{\mathbb{Z}}^\times/(\hat{\mathbb{Z}}^\times)_{\text{tors}} = \prod_{q \text{ prost}} \mathbb{Z}_q^\times/(\mathbb{Z}_q^\times)_{\text{tors}} = (1+4\mathbb{Z}_2^\times) \times \prod_{q\neq 2 \text{ prost}} (1+q\mathbb{Z}_q^\times).$$

Ovdje smo koristili činjenicu da je

$$\mathbb{Z}_q^\times \simeq \mu_{q-1} \times (1+q\mathbb{Z}_q^\times), \quad \text{za } q \neq 2 \qquad \text{i} \qquad \mathbb{Z}_2^\times \simeq \{\pm 1\} \times (1+4\mathbb{Z}_2^\times),$$

gdje je μ_{q-1} multiplikativna grupa $(q-1)$-vih korijena iz jedinice u $\mathbb{Z}_q$. Nadalje, vrijedi da je $1+q\mathbb{Z}_q^\times \simeq \mathbb{Z}_q^+$, za sve proste brojeve $q \geq 3$ te da je $1+4\mathbb{Z}_2^\times \simeq \mathbb{Z}_2^+$. U grupama $\mathbb{Z}_q^+$ nema torzije, stoga je $(\mathbb{Z}_q^\times)_{\text{tors}} = \mu_{q-1}$, za sve proste brojeve $q \geq 3$ te $(\mathbb{Z}_2^\times)_{\text{tors}} = \{\pm 1\}$.

Puno više detalja vezanih uz teoriju q-adskih cijelih brojeva može se naći u [18, §3].

Neka je n prirodan broj te neka je $\mathbb{K}_n$ jedinstveno polje stupnja p^n nad $\mathbb{Q}$ koje je sadržano u $\mathbb{K}$, tj. $\mathbb{K}_n$ je n-ti sloj proširenja $\mathbb{K}/\mathbb{Q}$. Po definiciji $\mathbb{Z}_p$-proširenja je $\text{Gal}\,(\mathbb{K}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Kako je $\text{Gal}\,(\mathbb{K}/\mathbb{Q})$ kvocijent od $\hat{\mathbb{Z}}^\times/(\hat{\mathbb{Z}}^\times)_{\text{tors}}$, zaključujemo da je i $\text{Gal}\,(\mathbb{K}_n/\mathbb{Q})$ kvocijent od $\hat{\mathbb{Z}}^\times/(\hat{\mathbb{Z}}^\times)_{\text{tors}}$. Pretpostavimo nadalje da je $p > 2$. Grupa $\text{Gal}\,(\mathbb{K}_n/\mathbb{Q})$ je konačna i reda je p^n, stoga je polje $\mathbb{K}_n$ fiksirano s

$$\begin{aligned}(\hat{\mathbb{Z}}^\times/(\hat{\mathbb{Z}}^\times)_{\text{tors}})^{p^n} &= (1+4\mathbb{Z}_2^\times)^{p^n} \times \prod_{q\neq 2 \text{ prost}} (1+q\mathbb{Z}_q^\times)^{p^n} \\ &= (1+p^{n+1}\mathbb{Z}_p^\times) \times (1+4\mathbb{Z}_2^\times) \times \prod_{q\neq 2, q \text{ prost}} (1+q\mathbb{Z}_q^\times).\end{aligned}$$

Zato je polje $\mathbb{K} = \bigcup_{n\in\mathbb{N}} \mathbb{K}_n$ fiksirano s

$$\bigcap_{n\in\mathbb{N}} (\hat{\mathbb{Z}}^\times/(\hat{\mathbb{Z}}^\times)_{\text{tors}})^{p^n} = (1+4\mathbb{Z}_2^\times) \times \prod_{q\neq 2, p \text{ prost}} (1+q\mathbb{Z}_q^\times) = \text{Gal}\,(\mathbb{Q}(\mu_\infty)/\mathbb{Q}(\mu_{p^\infty})^{\mu_{p-1}}).$$

Zaključujemo da je $\mathbb{K} \subseteq \mathbb{Q}(\mu_{p^\infty})^{\mu_{p-1}} = \mathbb{Q}_{\infty,p}$, ali $\mathbb{K}$ je $\mathbb{Z}_p$-proširenje od $\mathbb{Q}$, stoga mora biti $\mathbb{K} = \mathbb{Q}_{\infty,p}$. Dokaz u slučaju $p = 2$ je analogan. ■

3. TORZIJA NAD $\mathbb{Z}_p$-PROŠIRENJEM OD $\mathbb{Q}$

Jedan od glavnih rezultata ovog rada je potpuno rješenje problema rasta torzije eliptičke krivulje definirane nad $\mathbb{Q}$ u $\mathbb{Z}_p$-proširenjima od $\mathbb{Q}$. M. Chou, H. B. Daniels i F. Najman su skupa s I.K. napisali članak [6] u kojem su također izloženi navedeni rezultati.

3.1. POZNATI I POMOĆNI REZULTATI

Sljedeća propozicija je direktna posljedica Weilovog sparivanja, dokaz se može naći u [53, Ch. III, Cor. 8.1.1].

Propozicija 3.1.1. *Neka je $\mathbb{L} \subseteq \overline{\mathbb{Q}}$, $E/\mathbb{L}$ eliptička krivulja i n prirodan broj. Ako je $E[n]$ sadržano u $E(\mathbb{L})$, onda je n-to ciklotomsko polje $\mathbb{Q}(\zeta_n)$ sadržano u $\mathbb{L}$.*

Ono što će nam biti od koristi je sljedeći direktni korolar prethodne propozicije.

Korolar 3.1.2. *Neka su p i $q > 2$ prosti brojevi. Tada je*

$$E(\mathbb{Q}_{\infty,p})[q] \simeq \{0\} \quad ili \quad \mathbb{Z}/q\mathbb{Z}.$$

Napomena 3.1.3. *Ovo zapravo znači da $E[q^n] \not\subseteq E(\mathbb{Q}_{\infty,p})$, za svaki prost broj $q > 2$ i za svaki prirodan broj n. Nadalje, vrijedi i da $E[2^{n+1}] \not\subseteq E(\mathbb{Q}_{\infty,p})$, za svaki prirodan broj n. Uz analogan dokaz.*

Dokaz. Jedini korijeni iz jedinice sadržani u $\mathbb{Q}_{\infty,p}$ su -1 i 1, stoga se $\mathbb{Q}(\zeta_q)$ ne nalazi u $\mathbb{Q}_{\infty,p}$, rezultat sada slijedi iz prethodne propozicije 3.1.1. ■

Kažemo da eliptička krivulja $E/\mathbb{Q}$ ima racionalnu n-izogeniju ako postoji eliptička krivulja $E'/\mathbb{Q}$ takva da postoji izogenija $f\colon E \to E'$ stupnja n definirana također nad $\mathbb{Q}$.

Lema 3.1.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $\mathbb{F}$ Galoisovo proširenje od $\mathbb{Q}$. Neka je p prost broj i neka je k najveći cijeli broj za koji je $E[p^k] \subseteq E(\mathbb{F})$. Ako $E(\mathbb{F})_{tors}$ sadrži*

podgrupu izomorfnu sa $\mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^j\mathbb{Z}$, gdje je $j \geq k$ prirodan broj, onda E ima racionalnu p^{j-k}-izogeniju.

Dokaz. Riječ je o rezultatu [9, Lemma 4.6], gdje se može vidjeti i dokaz. ■

Navedimo i jedan od klasičnih Mazurovih i Kenkuovih rezultata koji možemo naći u [27–30, 37].

Teorem 3.1.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja s racionalnom n-izogenijom, tada je*

$$n \leq 19 \quad ili \quad n \in \{21, 25, 27, 37, 43, 67, 163\}.$$

Korolar 3.1.6. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je p prost broj. Ako $E(\mathbb{Q}_{\infty,p})_{tors}$ sadrži točku reda q^n, za neki prost broj q i prirodan broj n, onda je*

$$q^n \in \{2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 25, 27, 32, 37, 43, 67, 163\}.$$

Dokaz. Neka je najprije $q = 2$. Iz napomene 3.1.3 vidimo da $E[4] \nsubseteq E(\mathbb{Q}_{\infty,p})$. Dakle, uz oznake kao u lemi 3.1.4 zaključujemo da je $k \leq 1$, što znači da E ima racionalnu 2^{n-1}-izogeniju. Konačno, koristeći teorem 3.1.5 vidimo da su jedine mogućnosti za 2^n upravo $2, 4, 8, 16, 32$.

Ako je $q \geq 3$, onda po korolaru 3.1.2 znamo da $E[q] \nsubseteq E(\mathbb{Q}_{\infty,p})$ pa prema lemi 3.1.4 zaključujemo da E ima racionalnu q^n-izogeniju. Rezultat sada slijedi iz teorema 3.1.5. ■

Sljedeća dva bitna teorema su rezultati [17, Theorem 5.8 i Theorem 7.2].

Teorem 3.1.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je p prost broj te P točka reda p na E. Tada*

- *ako je $p \leq 13$ ili $p = 37$, onda su jedini mogući slučajevi za $[\mathbb{Q}(P) : \mathbb{Q}]$, od kojih se svi pojavljuju:*

p	$[\mathbb{Q}(P) : \mathbb{Q}]$
2	$1, 2, 3$
3	$1, 2, 3, 4, 6, 8$
5	$1, 2, 4, 5, 8, 10, 16, 20, 24$
7	$1, 2, 3, 6, 7, 9, 12, 14, 18, 21, 24, 36, 42, 48$
11	$5, 10, 20, 40, 55, 80, 100, 110, 120$
13	$3, 4, 6, 12, 24, 39, 48, 52, 72, 78, 96, 144, 156, 168$
37	$12, 36, 72, 444, 1296, 1332, 1368$

- *ako je $p > 13$ i $p \neq 37$, onda se idući slučajevi za $[\mathbb{Q}(P) : \mathbb{Q}]$ pojavljuju:*

  1. $p^2 - 1$, *za sve p,*
  2. 8, 16, 32, 136, 256, 272, 288, *za $p = 17$,*
  3. $\frac{p-1}{2}$, $p-1$, $\frac{p(p-1)}{2}$, $p(p-1)$, *ako je $p \in \{19, 43, 67, 163\}$,*
  4. $2(p-1)$, $(p-1)^2$, *ako je $p \equiv 1 \pmod 3$ ili $\left(\frac{-D}{p}\right) = 1$, za neki $D \in \{1, 2, 7, 11, 19, 43, 67, 163\}$,*
  5. $\frac{(p-1)^2}{3}$, $\frac{2(p-1)^2}{3}$, *ako je $p \equiv 4, 7 \pmod 9$,*
  6. $\frac{p^2-1}{3}$, $\frac{2(p^2-1)}{3}$, *ako je $p \equiv 2, 5 \pmod 9$,*

- *ako $p \not\equiv 8 \pmod 9$, onda su jedine mogućnosti one navedene u prve dvije točke. Ako je $p \equiv 8 \pmod 9$, onda postoje još samo dvije mogućnosti za $[\mathbb{Q}(P) : \mathbb{Q}]$:*

$$\frac{p^2-1}{3}, \qquad \frac{2(p^2-1)}{3}.$$

Nije poznato pojavljuju li se ili ne, no poznato je da nema drugih mogućnosti.

Teorem 3.1.8. *Neka je p najmanji prosti djelitelj prirodnog broja d i neka je $\mathbb{K}/\mathbb{Q}$ proširenje polja stupnja d. Tada*

- *ako je $p \geq 11$, onda je $E(\mathbb{K})_{tors} = E(\mathbb{Q})_{tors}$,*
- *ako je $p = 7$, onda je $E(\mathbb{K})[q^\infty] = E(\mathbb{Q})[q^\infty]$, za sve proste brojeve q različite od 7,*
- *ako je $p = 5$, onda je $E(\mathbb{K})[q^\infty] = E(\mathbb{Q})[q^\infty]$, za sve proste brojeve q različite od 5, 7 i 11,*
- *ako je $p = 3$, onda je $E(\mathbb{K})[q^\infty] = E(\mathbb{Q})[q^\infty]$, za sve proste brojeve q različite od 2, 3, 5, 7, 11, 13, 19, 43, 67 i 163.*

Iduća lema nam je korisna budući da njome efikasno eliminiramo nemali broj slučajeva.

Lema 3.1.9. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je p prost broj. Neka je $q \neq 2$ prost broj takav da $p \nmid q - 1$. Nadalje, neka je $\mathbb{K}/\mathbb{Q}$ cikličko proširenje polja stupnja p i neka je $P \in E$ točka reda q. Ako je $P \in E(\mathbb{K})$, onda je $P \in E(\mathbb{Q})$.*

Dokaz. Pretpostavimo li da je $\mathbb{Q}(\zeta_q) \subseteq \mathbb{K}$, onda $q - 1 = [\mathbb{Q}(\zeta_q) : \mathbb{Q}] \mid [\mathbb{K} : \mathbb{Q}] = p$, a kako je $q \neq 2$ to znači da je $q - 1 = p$. Međutim, to je kontradikcija budući da $p \nmid q - 1$. Stoga, po korolaru 3.1.2 slijedi da je $E(\mathbb{K})[q] \simeq \mathbb{Z}/q\mathbb{Z}$.

Pretpostavimo da $P \notin E(\mathbb{Q})$, to znači da postoji $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ takav da $P^\sigma \neq P$, odnosno da postoji $a \in \{2,3,\ldots,q-1\}$, takav da je $P^\sigma = aP$. Kako je $[\mathbb{K}:\mathbb{Q}] = p$, znamo da je $\sigma^p = 1$, stoga je

$$P = P^{\sigma^p} = a^p P,$$

što znači da je $a^p \equiv 1 \pmod{q}$. No, takav $a \in \{2,3,\ldots,q-1\}$ postoji ako i samo ako $p \mid q-1$, što je kontradikcija. ■

Iduća lema i njen korolar nam brzo i efikasno odgovaraju na pitanje u kojem sloju $\mathbb{Z}_p$-proširenja se točka reda n nalazi, ako uopće postoji.

Lema 3.1.10. *Neka je $E/\mathbb{Q}$ eliptička krivulja i $P \in E$ točka reda n takva da je $\mathbb{Q}(P)/\mathbb{Q}$ Galoisovo proširenje. Ako je $E(\mathbb{Q}(P))[n] \simeq \mathbb{Z}/n\mathbb{Z}$, onda je $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ izomorfno nekoj podgrupi od $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Dokaz. Proširenje $\mathbb{Q}(P)/P$ je Galoisovo što znači da za svaki $\sigma \in \mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ vrijedi da je red točke P^σ također jednak n. To znači da za svaki $\sigma \in \mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ postoji $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ takav da je $P^\sigma = aP$. Konačno, kako je djelovanje grupe $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ na $\langle P \rangle$ vjerno, zaključujemo da je $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ izomorfno nekoj podgrupi od $(\mathbb{Z}/n\mathbb{Z})^\times$. ■

Napomena 3.1.11. *Za prirodni broj n, $\phi(n)$ je broj prirodnih brojeva manjih od n i relativno prostih s n (tj. broj elemenata grupe $(\mathbb{Z}/n\mathbb{Z})^\times$). Nadalje, za prost broj p i prirodni broj k, $v_p(k)$ je najveća potencija broja p koja dijeli broj k.*

Korolar 3.1.12. *Neka je $n > 1$ neparan prirodni broj. Neka je $E/\mathbb{Q}$ eliptička krivulja i $P \in E$ točka reda n takva da je $\mathbb{Q}(P) \subseteq \mathbb{Q}_{\infty,p}$. Tada je $\mathbb{Q}(P) \subseteq \mathbb{Q}_{m,p}$, gdje je $m = v_p(\phi(n))$.*

Dokaz. Iz propozicije 3.1.1 zaključujemo da $E[n] \nsubseteq E(\mathbb{Q}_{\infty,p})$, stoga je $E(\mathbb{Q}(P))[n] \simeq \mathbb{Z}/n\mathbb{Z}$, primjenom leme 3.1.10 zaključujemo da je $\mathrm{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ izomorfno nekoj podgrupi grupe $(\mathbb{Z}/n\mathbb{Z})^\times$ koja ima $\phi(n)$ elemenata. Kako znamo da je $\mathbb{Q}(P) \subseteq \mathbb{Q}_{\infty,p}$, zaključujemo da je stupanj proširenja $\mathbb{Q}(P)/\mathbb{Q}$ oblika p^k te za taj prirodni broj k vrijedi $k \leq v_p(\phi(n))$. Konačno, preostaje se sjetiti činjenice da je stupanj proširenja $\mathbb{Q}_{m,p}/\mathbb{Q}$ jednak p^m. ■

Idući korisni alat je [17, Proposition 4.6], ali s malo jačim pretpostavkama koje su dostatne za naše potrebe.

Propozicija 3.1.13. *Neka je $E/\mathbb{F}$ eliptička krivulja, gdje je $\mathbb{F}$ polje algebarskih brojeva. Nadalje, neka je p prost broj, n prirodan broj i $P \in E$ točka reda p^{n+1} takva da $E(\mathbb{F}(pP))$ ne sadrži točke reda p^{n+1}. Ako je proširenje $\mathbb{F}(P)/\mathbb{F}(pP)$ Galoisovo, onda je $[\mathbb{F}(P):\mathbb{F}(pP)] \in \{p, p^2\}$.*

Dokaz. Neka je $Q = pP$, promotrimo jednadžbu

$$pX = Q. \tag{3.1}$$

Ono što nas zanima su mogućnosti za $[\mathbb{F}(P) : \mathbb{F}(Q)]$, gdje je P rješenje od (3.1). Taj stupanj je jednak duljini orbite od točke P pri djelovanju grupe $G = \mathrm{Gal}(\mathbb{F}(P)/\mathbb{F}(pP))$ na rješenja jednadžbe (3.1).

Očito je da su sva rješenja jednadžbe (3.1) u bijekciji s $E(\mathbb{F}(P))[p]$. Sva rješenja, dakle njih p^2 se pri djelovanju grupe G raspadaju na orbite uz uvjet da ako je točka P definirana nad nekim poljem, da su onda i svi višekratnici od P također definirani nad tim istim poljem. To znači da se sva rješenja jednadžbe (3.1) nalaze u orbitama jednakih duljina. Pretpostavimo da imamo m orbita i da su sve duljine d. Tada znamo da je

$$d \cdot x \in \{p, p^2\}.$$

Konačno, to znači da je $d \in \{p, p^2\}$, čime smo gotovi. ■

3.2. REZULTATI

Sada ćemo navesti rezultate iz kojih saznajemo sve moguće torzije eliptičkih krivulja $E/\mathbb{Q}$ nad poljima $\mathbb{Q}_{\infty,p}$. Preciznije, vidjet ćemo da za proste brojeve $p \geq 5$ nad poljima $\mathbb{Q}_{\infty,p}$ torzija uopće ne raste. Nad poljima $\mathbb{Q}_{\infty,3}$ i $\mathbb{Q}_{\infty,2}$ torzija može rasti, ali točno otkrivamo sve moguće grupe u koje može narasti.

Teorem 3.2.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja i $p \geq 5$ prost broj, tada je*

$$E(\mathbb{Q}_{\infty,p})_{tors} = E(\mathbb{Q})_{tors}.$$

Teorem 3.2.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je $E(\mathbb{Q}_{\infty,3})_{tors}$ izomorfno nekoj od idućih grupa*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad 1 \leq n \leq 10 \text{ ili } n \in \{12, 21, 27\}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, &\quad 1 \leq n \leq 4. \end{aligned} \tag{∞_3}$$

Za svaku grupu G s liste (∞_3), postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq G$.

Teorem 3.2.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je $E(\mathbb{Q}_{\infty,2})_{tors}$ izomorfno nekoj od idućih grupa*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad 1 \leq n \leq 10 \text{ ili } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, &\quad 1 \leq n \leq 4. \end{aligned} \tag{∞_2}$$

Za svaku grupu G s liste (∞_2), postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq G$.

Poznati Mazurov teorem [37, Theorem 2] govori da je, za eliptičku krivulju $E/\mathbb{Q}$, $E(\mathbb{Q})_{\text{tors}}$ izomorfno jednoj od grupa

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad 1 \leq n \leq 10 \text{ ili } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, &\quad 1 \leq n \leq 4. \end{aligned}$$

Stoga vidimo da je

$$\begin{aligned} \{E(\mathbb{Q}_{\infty,3})_{\text{tors}} : E/\mathbb{Q} \text{ e.k.}\} &= \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ e.k.}\} \cup \{\mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\}, \\ \{E(\mathbb{Q}_{\infty,2})_{\text{tors}} : E/\mathbb{Q} \text{ e.k.}\} &= \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ e.k.}\}, \end{aligned}$$

pri čemu e.k. znači eliptička krivulja.

Valja napomenuti da u slučajevima $p = 2$ i $p = 3$ ne vrijedi da je $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, za općenitu eliptičku krivulju $E/\mathbb{Q}$. Točnije, postoje mnoge eliptičke krivulje $E/\mathbb{Q}$ kod kojih torzija raste s $\mathbb{Q}$ na $\mathbb{Q}_{\infty,p}$. U sekciji 3.6, za $p = 2$ i $p = 3$, nalazimo za koje grupe G postoji beskonačno mnogo j-invarijanti j takvih da postoji eliptička krivulja $E/\mathbb{Q}$ s j-invarijantom j takva da je

$$E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}} \simeq G.$$

3.3. DOKAZ TEOREMA 3.2.1

Neka je $p \geq 11$ prost broj i $E/\mathbb{Q}$ eliptička krivulja. Po teoremu 3.1.8 vidimo da je

$$E(\mathbb{Q}_{n,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}},$$

za svaki prirodni broj n. Stoga je $E(\mathbb{Q}_{\infty,p})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$, čime je teorem 3.2.1 dokazan za svaki prost broj $p \geq 11$. Preostaje dokazati da je

$$E(\mathbb{Q}_{\infty,7})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}} \qquad \text{i} \qquad E(\mathbb{Q}_{\infty,5})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}},$$

što je i dokazano teoremima 3.3.1 i 3.3.2.

Teorem 3.3.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,7})_{tors} = E(\mathbb{Q})_{tors}.$$

Dokaz. Teorem 3.1.8 nam kaže da je

$$E(\mathbb{Q}_{n,7})[q^\infty] = E(\mathbb{Q})[q^\infty],$$

za svaki prost broj $q \neq 7$ i za svaki prirodni broj n. Stoga je $E(\mathbb{Q}_{\infty,7})[q^\infty] = E(\mathbb{Q})[q^\infty]$, za svaki prost broj $q \neq 7$ pa preostaje pokazati da je

$$E(\mathbb{Q}_{\infty,7})[7^\infty] = E(\mathbb{Q})[7^\infty].$$

Po korolaru 3.1.6 zaključujemo da nema 49-torzije u $E(\mathbb{Q}_{\infty,7})$ pa preostaje pokazati da je $E(\mathbb{Q}_{\infty,7})[7] = E(\mathbb{Q})[7]$.

Neka je $P \in E(\mathbb{Q}_{\infty,7})$ točka reda 7. Iz teorema 3.1.7 slijedi da je točka P definirana nad poljem stupnja najviše $48 = 7^2 - 1$. Stoga zaključujemo da je $P \in E(\mathbb{Q}_{1,7})$. Konačno, lema 3.1.9 sada govori da je $P \in E(\mathbb{Q})$ te smo time gotovi. ■

Teorem 3.3.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,5})_{tors} = E(\mathbb{Q})_{tors}.$$

Kako bismo dokazali ovaj teorem, imajući na umu teorem 3.1.8, vidimo da je dovoljno pokazati da je $E(\mathbb{Q}_{\infty,5})[q^\infty] = E(\mathbb{Q})[q^\infty]$, za $q = 11, 7, 5$. Svi argumenti potrebni za to nalaze se u sljedećih nekoliko rezultata.

Lema 3.3.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,5})[11^\infty] = \{0\}.$$

Dokaz. Iz korolara 3.1.6 slijedi da nema 121-torzije u $E(\mathbb{Q}_{\infty,5})$, stoga treba pokazati da je $E(\mathbb{Q}_{\infty,5})[11] = \{0\}$.

Pretpostavimo da postoji točka $P \in E(\mathbb{Q}_{\infty,5})$ koja je reda 11. Iz teorema 3.1.7 tada slijedi da je $P \in E(\mathbb{Q}_{1,5})$. Modularna krivulja $X_1(11)$ je eliptička krivulja

$$y^2 + y = x^3 - x^2.$$

Ovaj model možemo naći u npr. [47]. Također, riječ je zapravo o eliptičkoj krivulji 11a3 s [54]. Koristeći programski alat `magma` [2] lako računamo (kôd 1.m) da krivulja $X_1(11)$ ima rang jednak 0 i torziju jednaku $\mathbb{Z}/5\mathbb{Z}$ nad $\mathbb{Q}_{1,5}$. No, $X_1(11)$ ima torziju jednaku $\mathbb{Z}/5\mathbb{Z}$ i nad $\mathbb{Q}$, a znamo da nad $\mathbb{Q}$ ne postoji točka reda 11. Dakle, sve torzijske točke su kaspovi, stoga ne postoji eliptička krivulja nad $\mathbb{Q}$ koja ima 11-torziju nad $\mathbb{Q}_{1,5}$. ■

Lema 3.3.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,5})[7^\infty] = E(\mathbb{Q})[7^\infty].$$

Dokaz. Zbog korolara 3.1.6 znamo da ne postoji 49-torzija u $E(\mathbb{Q}_{\infty,5})$, zato je dovoljno pokazati da je $E(\mathbb{Q}_{\infty,5})[7] = E(\mathbb{Q})[7]$. Neka je $P \in E(\mathbb{Q}_{\infty,5})$ točka reda 7, pretpostavimo da $P \notin E(\mathbb{Q})$. No, iz teorema 3.1.7 slijedi da $5 \nmid [\mathbb{Q}(P) : \mathbb{Q}]$, što je kontradikcija. ■

Lema 3.3.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,5})[5^\infty] = E(\mathbb{Q})[5^\infty].$$

Dokaz. U $E(\mathbb{Q}_{\infty,5})$ nema 125-torzije po korolaru 3.1.6. Nadalje, pretpostavimo da je $P \in E(\mathbb{Q}_{\infty,5})$ točka reda 5. Po teoremu 3.1.7 znamo da je tada $P \in E(\mathbb{Q}_{1,5})$, a sada nam lema 3.1.9 govori da je $P \in E(\mathbb{Q})$. Stoga, preostaje dokazati da je $E(\mathbb{Q}_{\infty,5})[25] = E(\mathbb{Q})[25]$.

Ako pretpostavimo da postoji točka $P \in E$ reda 25 takva da je $P \in E(\mathbb{Q}_{\infty,5})$, znamo da $P \notin E(\mathbb{Q})$. Točka $5P$ je tada točka reda 5 pa analogno prethodnom zaključujemo da je $5P \in E(\mathbb{Q})$. Nadalje, iz korolara 3.1.12 slijedi da je $P \in E(\mathbb{Q}_{1,5})$. Lema 3.1.4 nam govori da E ima racionalnu 25-izogeniju, to znači da grupa $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ djeluje na $\langle P \rangle$, odnosno da za svaki $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ postoji $a \in (\mathbb{Z}/25\mathbb{Z})^\times$ takav da je $P^\sigma = aP$. Neka je $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, kako je $5P \in E(\mathbb{Q})$, vrijedi

$$5P = (5P)^\sigma = 5P^\sigma = 5aP,$$

odnosno $5(a-1)P=0$. Točka P je reda 25, stoga je nužno $a \equiv 1 \pmod 5$. Zaključujemo da je $G_{\mathbb{Q}}(25)$ oblika

$$\left\{ \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} : a \in 1+5\mathbb{Z}/25\mathbb{Z} \right\}.$$

Nadalje, znamo da je $[\mathbb{Q}(\zeta_{25}) : \mathbb{Q}_{1,5}] = 4$, što znači da je $\left|\mathrm{Gal}\left(\mathbb{Q}(\zeta_{25})/\mathbb{Q}_{1,5}\right)\right| = 4$. Sada iz propozicije 1.1.2 zaključujemo da je $\det G_{\mathbb{Q}_{1,5}}(25)$ izomorfno jedinstvenoj podgrupi reda 4 grupe $(\mathbb{Z}/25\mathbb{Z})^\times$, koja je jednaka $\langle 7 \rangle = \{7,-1,-7,1\}$. Sjetimo se još da $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}_{1,5}\right)$ fiksira točku P, stoga je

$$G_{\mathbb{Q}_{1,5}}(25) \leq \left\{ \begin{pmatrix} 1 & * \\ 0 & b \end{pmatrix} : b \in \{7,-1,-7,1\} \right\}.$$

Vrijedi da je $[G_{\mathbb{Q}}(25) : G_{\mathbb{Q}_{1,5}}(25)] = 5$, a znamo i da $P \notin E(\mathbb{Q})$, iz svega toga zaključujemo da je

$$G_{\mathbb{Q}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in 1+5\mathbb{Z}/25\mathbb{Z},\ b \in \{7,-1,-7,1\} \right\}.$$

Konačno, računamo

$$25 \mid 600 \mid [\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_{\mathbb{Q}}(25)] \mid [\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : \mathrm{Img}(\rho_{5,E})],$$

što je kontradikcija s teoremom 1.1.3. ■

Dokaz teorema 3.3.2. Teorem 3.1.8 nam kaže da je

$$E(\mathbb{Q}_{n,5})[q^\infty] = E(\mathbb{Q})[q^\infty],$$

za svaki prost broj $q \neq 5,7,11$ i za svaki prirodni broj n. Stoga je $E(\mathbb{Q}_{\infty,5})[q^\infty] = E(\mathbb{Q})[q^\infty]$, za svaki prost broj $q \neq 5,7,11$ pa preostaje pokazati da je

$$E(\mathbb{Q}_{\infty,5})[q^\infty] = E(\mathbb{Q})[q^\infty],$$

za $q = 5,7,11$, a to slijedi iz lema 3.3.5, 3.3.4 i 3.3.3. ■

3.4. DOKAZ TEOREMA 3.2.2

Ključni sastojci dokaza su sljedeći tehnički rezultati.

Lema 3.4.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,3})[q^\infty] = \{0\} = E(\mathbb{Q})[q^\infty],$$

za sve proste brojeve q različite od 2, 3, 5, 7, 13 i 19.

Dokaz. Slijedi direktno iz teorema 3.1.7 i iz jednostavne činjenice da brojevi $p-1$ i p^2-1 nisu potencije broja 3 niti za koji neparni prost broj p. Naime, brojevi $p-1$ i p^2-1 su parni. ■

Lema 3.4.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada $E(\mathbb{Q}_{\infty,3})$ ne sadrži točku reda 19.*

Dokaz. Pretpostavimo da je $P \in E(\mathbb{Q}_{\infty,3})$ točka reda 19. Po korolaru 3.1.12 zaključujemo da je točka P definirana nad $\mathbb{Q}_{2,3}$. Eliptička krivulja E mora imati racionalnu 19-izogeniju (lema 3.1.4). To znači (pogledati u [36, str. 301, Table 4] ili u [52, Appendix A, §3]) da je

$$j(E) = -2^{15} \cdot 3^3.$$

Koristeći programski alat `magma` [2] provjerimo (kôd 2.m) da 19. djelidbeni polinom eliptičkih krivulja s tom j-invarijantom nema nultočaka nad poljem $\mathbb{Q}_{2,3}$, stoga je nemoguće da $E(\mathbb{Q}_{\infty,3})$ sadrži točku reda 19. ■

Lema 3.4.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada $E(\mathbb{Q}_{\infty,3})$ ne sadrži točku reda 13.*

Dokaz. Pretpostavimo da je $P \in E(\mathbb{Q}_{\infty,3})$ točka reda 13. Po korolaru 3.1.12 zaključujemo da je točka P definirana nad $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$, tj. nad maksimalnim realnim potpoljem od $\mathbb{Q}(\zeta_9)$. Kao što možemo vidjeti u [25, str. 3], modularna krivulja $X_1(13)$ je krivulja genusa 2 sa sljedećom formulom (na [54] možemo naći još jedan model te krivulje: 169.a.169.1):

$$y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1.$$

Koristeći programski alat `magma` [2] računamo (kôd 3.m) da je rang Jakobijana $J_1(13)$ ove krivulje nad poljem $\mathbb{Q}(\zeta_9)^+$ jednak 0. Nadalje, gledajući redukciju modulo 11 i 19 zaključujemo da je

$$J_1(13)(\mathbb{Q}(\zeta_9)^+)_{\text{tors}} \simeq \mathbb{Z}/19\mathbb{Z},$$

također računamo i da je $J_1(13)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/19\mathbb{Z}$. Nakon toga lako računamo da je $X_1(13)(\mathbb{Q}) = X_1(13)(\mathbb{Q}(\zeta_9)^+)$. Naime, nađemo neke točke na $X_1(13)(\mathbb{Q}(\zeta_9)^+)$, pomoću njih možemo generirati svih 19 točaka iz $J_1(13)(\mathbb{Q}(\zeta_9)^+)_{\text{tors}}$ te na kraju provjerimo da svih tih 19 točaka odgovara upravo nađenim točkama na $X_1(13)(\mathbb{Q}(\zeta_9)^+)$. Time smo našli sve točke na $X_1(13)(\mathbb{Q}(\zeta_9)^+)$. Istim postupkom nađemo i sve točke na $X_1(13)(\mathbb{Q})$. Znamo da $E/\mathbb{Q}$ nema točaka reda 13 nad $\mathbb{Q}$, stoga su sve točke na $X_1(13)(\mathbb{Q}) = X_1(13)(\mathbb{Q}(\zeta_9)^+)$ kaspovi pa zaključujemo da $E/\mathbb{Q}$ nema točaka reda 13 niti nad $\mathbb{Q}(\zeta_9)^+$. ■

Lema 3.4.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada je*

$$E(\mathbb{Q}_{\infty,3})[5^\infty] = E(\mathbb{Q})[5^\infty].$$

Dokaz. Iz teorema 3.1.7 vidimo da ako je $E(\mathbb{Q})[5] = \{0\}$, da je onda i $E(\mathbb{Q}_{\infty,3})[5] = \{0\}$, naime, točka reda 5 ne može biti definirana nad proširenjem stupnja 3^n. Ako je pak $E(\mathbb{Q})[5] \neq \{0\}$, onda iz propozicije 3.1.13 slijedi da je $E(\mathbb{Q}_{\infty,3})[5^\infty] = E(\mathbb{Q})[5^\infty]$. Napomenimo još da znamo da puna 5-torzija nije sadržana u $E(\mathbb{Q}_{\infty,3})$, budući da $\mathbb{Q}_{\infty,3}$ ne sadrži ζ_5, peti primitivni korijen iz jedinice. ■

Lema 3.4.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Ako $E(\mathbb{Q}_{\infty,3})$ sadrži točku reda 7, onda je*

$$E(\mathbb{Q}_{\infty,3})_{tors} \simeq G, \quad \textit{gdje je} \quad G \in \{\mathbb{Z}/7\mathbb{Z},\ \mathbb{Z}/21\mathbb{Z}\}.$$

Dokaz. Neka je $P \in E(\mathbb{Q}_{\infty,3})$ točka reda 7. Po korolaru 3.1.12 znamo da je točka P definirana nad $\mathbb{Q}_{1,3}$. Po korolaru 3.1.6 znamo da je tada $E(\mathbb{Q}_{\infty,3})[7^\infty] \simeq \mathbb{Z}/7\mathbb{Z}$, budući da E ne može imati 49-torziju.

Pretpostavimo da $E(\mathbb{Q}_{\infty,3})$ sadrži i točku reda 5. Tada $E(\mathbb{Q}_{\infty,3})$ sadrži točku reda 35, a to onda znači da E ima racionalnu 35-izogeniju, što je kontradikcija s teoremom 3.1.5.

Nadalje, pretpostavimo da $E(\mathbb{Q}_{\infty,3})$ sadrži točku reda 2. Ona je tada definirana nad $\mathbb{Q}_{1,3}$ (teorem 3.1.7). Zaključujemo da $E(\mathbb{Q}_{1,3})$ sadrži točku reda 14. Modularna krivulja $X_1(14)$ je eliptička krivulja (na [54] je nalazimo: 14.a5):

$$y^2 + xy + y = x^3 - x.$$

Sada lako računamo (`magma` [2] kôd 4.m) da je $X_1(14)(\mathbb{Q}_{1,3}) = X_1(14)(\mathbb{Q})$. ■

Lema 3.4.6. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Ako je $E(\mathbb{Q})[2^\infty] \subsetneq E(\mathbb{Q}_{\infty,3})[2^\infty]$, onda je*

$$E(\mathbb{Q}_{\infty,3})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Dokaz. Po rezultatu [41, Lemma 1] vidimo da ako je $E(\mathbb{Q})[2] \neq \{0\}$, da je onda $E(\mathbb{Q})[2^\infty] = E(\mathbb{Q}_{\infty,3})[2^\infty]$, stoga imamo da je $E(\mathbb{Q})[2] = \{0\}$. Nadalje, iz istog rezultata slijedi da je tada cijela 2-torzija $E(\mathbb{Q}_{\infty,3})[2^\infty]$ definirana nad poljem koje sadrži točku reda 2, tj. nad $\mathbb{Q}_{1,3}$. Dakle, treba pokazati da ako je $\{0\} = E(\mathbb{Q})[2] \subsetneq E(\mathbb{Q}_{\infty,3})[2]$, da je onda $E(\mathbb{Q}_{1,3})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Međutim, ta činjenica slijedi direktno iz rezultata [45, Proposition 9], stoga je uistinu

$$E(\mathbb{Q}_{\infty,3})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \qquad \blacksquare$$

Lema 3.4.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada $E(\mathbb{Q}_{\infty,3})$ ne sadrži točku reda* 18.

Dokaz. Pretpostavimo li da $E(\mathbb{Q}_{\infty,3})$ sadrži točku P reda 18, po korolaru 3.1.12 znamo da je točka $2P$ definirana nad $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$, tj. nad maksimalnim realnim potpoljem polja $\mathbb{Q}(\zeta_9)$. Znamo da je i točka $9P$ (koja je reda 2) nužno definirana također nad tim poljem. Dakle, točka $P = 9P - 4 \cdot (2P)$ mora biti definirana nad $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$. Ono što ćemo sada napraviti je, koristeći programski alat `magma` [2], dokazati da se $X_1(18)(\mathbb{Q}(\zeta_9)^+)$ sastoji samo od kaspova. Za to koristimo kôd 5.m.

U [46, str. 20] nalazimo model (na [54] nalazimo još jedan model ove krivulje: 324.a.648.1) za modularnu krivulju $X_1(18)$, to je krivulja genusa 2:

$$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

Najprije računamo da je rang Jakobijana $J_1(18)(\mathbb{Q}(\zeta_9)^+)$ jednak 0. Nadalje, koristeći teorem [51, Theorem 37] (preciznije, pogledati [26, Appendix]) zaključujemo da je torzija krivulje $J_1(18)(\mathbb{Q}(\zeta_9)^+)$ podgrupa grupe $\mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}$. Naime, promotrimo redukciju modulo 17 na konačno polje $\mathbb{F}_{17}$ (17 je najmanji prost broj koji se potpuno cijepa u prstenu cijelih polja $\mathbb{Q}(\zeta_9)^+$, tj. takav da mu je stupanj inercije jednak 3), a tamo lako računamo gornju ogradu torzijske grupe, koja je upravo $\mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}$.

U $X_1(18)(\mathbb{Q}(\zeta_9)^+)$ nalazimo 12 točaka te vidimo da te točke generiraju barem $147 = 7 \cdot 21$ točaka na $J_1(18)(\mathbb{Q}(\zeta_9)^+)$. Dakle, zaključujemo da je

$$\mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z} \leq J_1(18)(\mathbb{Q}(\zeta_9)^+)_{\text{tors}} \leq \mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}.$$

Računamo

$$J_1(18)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/21\mathbb{Z},$$
$$J_1(18)(\mathbb{Q}(\zeta_3))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z},$$
$$J_1(18)(\mathbb{Q}(\zeta_9))_{\text{tors}} \leq \mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}.$$

Znamo da je

$$\mathbb{Q}(\zeta_9) = \mathbb{Q}(\zeta_3)\mathbb{Q}(\zeta_9)^+ \quad \text{i} \quad \mathbb{Q}(\zeta_3) \cap \mathbb{Q}(\zeta_9)^+ = \mathbb{Q}.$$

Dakle, svi ne-racionalni elementi od $J_1(18)(\mathbb{Q}(\zeta_9))[3]$ su definirani nad $\mathbb{Q}(\zeta_3)$. Stoga je

$$J_1(18)(\mathbb{Q}(\zeta_9)^+) \simeq \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}.$$

Dakle, znamo sve točke na $J_1(18)(\mathbb{Q}(\zeta_9)^+)$, pogledamo li točke na $X_1(18)(\mathbb{Q}(\zeta_9)^+)$ koje njima odgovaraju vidimo da je to onih istih 12 točaka koje smo našli. Preostaje vidjeti da su one kaspovi. U [46, str. 20] možemo naći rezultat koji govori da su x koordinate kaspova na $X_1(18)(\overline{\mathbb{Q}})$ (s modelom koji koristimo) nultočke polinoma

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

Lako vidimo da su x-koordinate svih točaka na $X_1(18)(\mathbb{Q}(\zeta_9)^+)$ nultočke toga polinoma čime smo gotovi. ■

Dokaz teorema 3.2.2. Imajući na umu sve prethodne rezultate, tj. leme 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6 i 3.4.7, zaključujemo da jedino još moramo proučiti eventualni rast 3-torzije i utvrditi kada se isti može dogoditi.

Lema 3.1.9 nam odmah govori da ako je $E(\mathbb{Q}_{\infty,3}) \neq \{0\}$, da je onda i $E(\mathbb{Q})[3] \neq \{0\}$.

Pretpostavimo najprije da $E(\mathbb{Q}_{\infty,3})$ sadrži točku P reda 27. Iz korolara 3.1.12 slijedi da je točka P definirana nad poljem $\mathbb{Q}_{2,3}$. Nadalje, eliptička krivulja E u ovom slučaju mora imati racionalnu 27-izogeniju, stoga je (pogledati u [36, str. 301, Table 4] ili u [52, Appendix A, §3])

$$j(E) = -2^{15} \cdot 3 \cdot 53.$$

Sada ćemo koristiti činjenicu da eliptičke krivulje s istom j-invarijantom imaju iste (do na multiplikativnu konstantu) djelidbene polinome. Neka je E' neka eliptička krivulja s tom j-invarijantom, npr. 27a2:

$$y^2 + y = x^3 - 270x - 1708.$$

Koristeći programski alat `magma` [2] i to kôd 6.m, faktoriziramo polinom $\frac{\psi_{27}}{\psi_9}$ (ovdje je ψ_n n-ti djelidbeni polinom od E') i uočimo da taj polinom ima nultočke nad poljem $\mathbb{Q}_{2,3}$. To znači da postoji kvadratni twist (nad $\mathbb{Q}_{2,3}$) E'^{δ} od E', za neki $\delta \in \mathbb{Q}_{2,3}^*/(\mathbb{Q}_{2,3}^*)^2$ takav da $E'^{\delta}(\mathbb{Q}_{2,3})$ sadrži točku reda 27. Preostaje provjeriti možemo li naći δ takav da je krivulja E'^{δ} definirana nad $\mathbb{Q}$. To je ekvivalentno tome da postoje $a \in \mathbb{Q}_{2,3}^*$ i $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ takvi da je $\delta \cdot a^2 = d$. Odnosno da je kvadratni twist za δ izomorfan kvadratnom twistu za d. Neka je α neka nultočka polinoma

$\frac{\psi_{27}}{\psi_9}$ nad poljem $\mathbb{Q}_{2,3}$. Računamo i nalazimo da je norma diskriminante kvadratne jednadžbe $y^2+y=\alpha^3-270\alpha-1708$ jednaka 3^{49}. Stoga su jedini kvadratni twistovi koje ima smisla promatrati za $d=3$ i $d=-3$. Nalazimo da eliptička krivulja E^{-3}, što je zapravo 27a4, uistinu ima točku reda 27 nad $\mathbb{Q}_{2,3}$. Primijetimo da iz ove diskusije zapravo slijedi da je to jedina eliptička krivulja definirana nad $\mathbb{Q}$ s točkom reda 27 nad poljem $\mathbb{Q}_{\infty,3}$. Konačno, za tu krivulju imamo da je njena torzija nad $\mathbb{Q}_{\infty,3}$ izomorfna grupi $\mathbb{Z}/27\mathbb{Z}$, budući da bi bilo koja veća torzija bila u kontradikciji s teoremom 3.1.5.

Ako je $E/\mathbb{Q}$ eliptička krivulja takva da je $E(\mathbb{Q}_{\infty,3})[3^\infty]\simeq\mathbb{Z}/9\mathbb{Z}$, onda je nemoguće da postoji točka reda q za bilo koji prost broj $q>3$, jer bi to značilo da E ima racionalnu $9q$-izogeniju, što je nemoguće po teoremu 3.1.5. Također, nemoguće je da $E(\mathbb{Q}_{\infty,3})$ ima 2-torziju, budući da bi to značilo da nad $E(\mathbb{Q}_{1,3})$ ima $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}$ torziju što je u kontradikciji s rezultatom [45, Theorem 1]. Dakle, nužno je $E(\mathbb{Q}_{\infty,3})_{\text{tors}}\simeq\mathbb{Z}/9\mathbb{Z}$.

Konačno, iz svega do sada dokazanog zaključujemo da ako je $E(\mathbb{Q}_{\infty,3})[3^\infty]\simeq\mathbb{Z}/3\mathbb{Z}$, da je onda $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ izomorfno nekoj od grupa

$$\mathbb{Z}/3\mathbb{Z},\quad \mathbb{Z}/6\mathbb{Z},\quad \mathbb{Z}/12\mathbb{Z},\quad \mathbb{Z}/21\mathbb{Z},\quad \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},$$

čime je dokaz priveden kraju. ■

3.5. DOKAZ TEOREMA 3.2.3

Svi sastojci dokaza, kao i za prethodni rezultat, nalaze se u sljedećih nekoliko tehničkih rezultata.

Lema 3.5.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,2})[q^\infty] = \{0\} = E(\mathbb{Q})[q^\infty],$$

za sve proste brojeve q različite od 2, 3, 5, 7, 13 i 17.

Dokaz. Slijedi direktno iz teorema 3.1.7 i sljedećih jednostavnih činjenica.

- Primjetimo da je $\gcd(p-1, p+1) = 2$ te da je $p+1 > p-1 \geq 4$, za svaki prost broj $p > 3$. Stoga $p^2 - 1 = (p-1)(p+1)$ nije potencija broja 2, ni za koji prost broj $p > 3$.
- Za proste brojeve $p \in \{19, 43, 67, 163\}$ vidimo da $p-1$ nije potencija broja 2.
- Ako je p prost broj i $p-1$ potencija broja 2, onda je p oblika $2^{2^l}+1$, tj. p je Fermatov prost broj. Ako je $p > 17$, onda je p jednak barem 257 (3, 5, 17 i 257 su prva četiri Fermatova prosta broja). No, iz korolara 3.1.6 tada slijedi da $E(\mathbb{Q}_{\infty,2})$ nema točku reda $p > 17$.
- Primijetimo da je broj $\dfrac{(p-1)^2}{3}$ djeljiv s 3 za svaki prost broj $p \equiv 4, 7 \pmod 9$, stoga ne može biti potencija broja 2.
- Neka je $p \equiv 2, 5 \pmod 9$ prost broj koji je veći od 13, to znači da je $p = 3k-1$, za neki prirodan broj $k \geq 8$. No, tada je $\dfrac{p^2-1}{3} = (3k-2)\cdot k$, što ne može biti potencija broja 2, budući da je $\gcd(3k-2, k) \leq 2$.
- Ako je $p \equiv 8 \pmod 9$ prost broj, onda je broj $\dfrac{p^2-1}{3}$ djeljiv s 3 pa ne može biti potencija broja 2. ■

Lema 3.5.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada $E(\mathbb{Q}_{\infty,2})$ ne sadrži točku reda 17.*

Dokaz. Pretpostavimo da je $P \in E(\mathbb{Q}_{\infty,2})$ točka reda 17. Po korolaru 3.1.12 i teoremu 3.1.7 slijedi da je $\mathbb{Q}(P) = \mathbb{Q}_{3,2}$ ili $\mathbb{Q}(P) = \mathbb{Q}_{4,2}$. Nadalje, iz leme 3.1.4 zaključujemo da tada E ima

racionalnu 17-izogeniju. To znači (pogledati u [36, str. 301, Table 4] ili u [52, Appendix A, §3]) da je

$$j(E) = \frac{-17^2 \cdot 101^3}{2}, \quad \text{što je istina za eliptičku krivulju 14450p1}$$

ili

$$j(E) = \frac{-17 \cdot 373^3}{2^{17}}, \quad \text{što je istina za eliptičku krivulju 14450p2.}$$

Sada, za obje uočene j-invarijante, koristeći programski alat `magma` [2] faktoriziramo (kôd 7.m) 17. djelidbeni polinom. Preciznije, tražimo mu faktore stupnja ≤ 16. Za obje navedene j-invarijante dobijemo da pripadajući polinomi nemaju nultočaka nad poljem $\mathbb{Q}_{4,2}$. Dakle, $E(\mathbb{Q}_{\infty,2})$ uistinu ne sadrži točku reda 17. ■

Lema 3.5.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada $E(\mathbb{Q}_{\infty,2})$ ne sadrži točku reda 13.*

Dokaz. Pretpostavimo da je $P \in E(\mathbb{Q}_{\infty,2})$ točka reda 13. Po teoremu 3.1.7 slijedi da je

$$\mathbb{Q}(P) = \mathbb{Q}_{2,2} = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right).$$

No, to onda znači da E ili kvadratni twist od E ima 13-torziju nad $\mathbb{Q}(\sqrt{2})$, što je kontradikcija s rezultatom [25, Theorem 3]. Naime, taj rezultat nam govori (između ostalog) sljedeće. Ako je $E/\mathbb{Q}$ eliptička krivulja i d prirodni broj takav da $E(\mathbb{Q}(\sqrt{d}))$ sadrži točku reda 13, onda je $d \geq 7$. ■

Lema 3.5.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Ako $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 7, onda je*

$$E(\mathbb{Q}_{\infty,2})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}.$$

Dokaz. Iz korolara 3.1.2 znamo da je $E(\mathbb{Q}_{\infty,2})[7]$ ili trivijalna grupa ili izomorfna grupi $\mathbb{Z}/7\mathbb{Z}$. Stoga (imajući na umu prethodne rezultate) preostaje dokazati da $E(\mathbb{Q}_{\infty,2})$ ne sadrži točku reda 49, 2, 3 ili 5, ukoliko sadrži točku reda 7. Korolar 3.1.6 odmah eliminira točke reda 49.

Pretpostavimo da je $P \in E(\mathbb{Q}_{\infty,2})$ točka reda 7, iz korolara 3.1.12 znamo da je tada $\mathbb{Q}(P) \subseteq \mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$. No, to onda znači da $E(\mathbb{Q})$ ili kvadratni twist $E^2(\mathbb{Q})$ sadrži točku reda 7. Ukoliko $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 2, onda točku reda 2 sadrži i $E(\mathbb{Q})$ i $E^{(2)}(\mathbb{Q})$. Što znači da neka od $E(\mathbb{Q})$ i $E^{(2)}(\mathbb{Q})$ sadrži točku 14, što je kontradikcija s Mazurovim teoremom, [37, Theorem 2].

Pretpostavimo da $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 3. Po korolaru 3.1.12 ta je točka definirana nad $\mathbb{Q}_{1,2}$, što onda znači da $E(\mathbb{Q}_{1,2})$ sadrži točku reda 21, što je kontradikcija s rezultatima iz [24] i [31, str. 126].

Konačno, pretpostavimo da $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 5, to onda znači da $E/\mathbb{Q}$ ima racionalnu 35-izogeniju, što je kontradikcija s teoremom 3.1.5. ■

Lema 3.5.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Ako $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 5, onda je*

$$E(\mathbb{Q}_{\infty,2})_{tors} \simeq G, \quad \textit{gdje je} \quad G \in \{\mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z}\}.$$

Dokaz. Iz korolara 3.1.2 znamo da je $E(\mathbb{Q}_{\infty,2})[5]$ ili trivijalna grupa ili izomorfna grupi $\mathbb{Z}/5\mathbb{Z}$. Stoga (imajući na umu prethodne rezultate) moramo dokazati da $E(\mathbb{Q}_{\infty,2})$ ne sadrži točku reda 25 ili 3, ukoliko sadrži točku reda 5. Ukoliko $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 25, prema korolaru 3.1.12 ta je točka definirana nad $\mathbb{Q}_{2,2} = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$. No, to onda znači da E ili kvadratni twist od E ima 25-torziju nad $\mathbb{Q}(\sqrt{2})$, što je kontradikcija s rezultatima iz [24] i [31, str. 126]. Također, možemo pogledati i [25, Theorem 1].

Ukoliko $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 15, onda su i točka reda 5 i točka reda 3 po korolaru 3.1.12 sadržane u $E(\mathbb{Q}_{2,2})$, što znači da je i ta točka reda 15 sadržana u $E(\mathbb{Q}_{2,2})$. U [25, str. 3] nalazimo da je $X_1(15)$ eliptička krivulja

$$y^2 + (x+1)y = x^3 + x^2,$$

odnosno eliptička krivulja 15a8 na [54]. Vidimo da je $X_1(15)(\mathbb{Q})$ ranga 0 i da je $X_1(15)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. Koristeći programski alat `magma` [2] sada lako računamo (kôd 8.m) da je $X_1(15)(\mathbb{Q}) = X_1(15)(\mathbb{Q}_{2,2})$, stoga ne postoji točka reda 15 u $E(\mathbb{Q}_{\infty,2})$.

Preostaje dokazati da ako $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 5 i točku reda 2, da je onda

$$E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/10\mathbb{Z}.$$

Odmah vidimo da $E(\mathbb{Q}_{\infty,2})$ ne sadrži točku reda 4 pošto tada eliptička krivulja E ima racionalnu 20-izogeniju, što je u kontradikciji s teoremom 3.1.5. Dakle, preostaje još jedino isključiti opciju $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Pretpostavimo da je $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. Po teoremu 3.1.7 znamo da je $E[2]$ definirano nad $\mathbb{Q}_{1,2}$. Primijetimo da je

$$E(\mathbb{Q}_{2,2})[5] \simeq \mathbb{Z}/5\mathbb{Z} \quad \text{i} \quad E(\mathbb{Q}_{2,2})[5] \simeq E(\mathbb{Q}_{1,2})[5] \oplus E^{\delta}(\mathbb{Q}_{1,2})[5],$$

za neki kvadratni twist (nad $\mathbb{Q}_{1,2}$) E^{δ} od E. Kako kvadratni twist ne mijenja 2-torziju, zaključujemo da je $E(\mathbb{Q}_{1,2}) \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ ili $E^{\delta}(\mathbb{Q}_{1,2}) \supseteq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. U [25, str. 4] nalazimo da je $X_1(2,10)$ eliptička krivulja

$$y^2 = x^3 + x^2 - x,$$

odnosno 20a2 na [54], gdje vidimo da je $X_1(2,10)(\mathbb{Q})$ ranga 0 i da je $X_1(2,10)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. Koristeći programski alat `magma` [2] računamo (kôd 9.m) da je $X_1(2,10)(\mathbb{Q}(\sqrt{2})) = X_1(2,10)(\mathbb{Q})$ te zaključujemo da ne postoji eliptička krivulja nad $\mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$ sa $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ torzijom. ■

Lema 3.5.6. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Ako $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 9, onda je*

$$E(\mathbb{Q}_{\infty,2})_{tors} \simeq \mathbb{Z}/9\mathbb{Z}.$$

Dokaz. Iz korolara 3.1.2 znamo da je $E(\mathbb{Q}_{\infty,2})[9]$ ili trivijalna grupa ili izomorfna grupi $\mathbb{Z}/9\mathbb{Z}$. Stoga (imajući na umu prethodne rezultate) moramo dokazati da $E(\mathbb{Q}_{\infty,2})$ ne sadrži točku reda 27, ni točku reda 2, ukoliko sadrži točku reda 9.

Pretpostavimo da $E(\mathbb{Q}_{\infty,2})$ sadrži točku P reda 27. Točka $3P$ je tada točka reda 9 i ona je, po korolaru 3.1.12, sadržana u $E(\mathbb{Q}_{1,2})$. Po rezultatima iz [24] i [31, str. 126] znamo da $E(\mathbb{Q}_{1,2})$ ne sadrži točku reda 27. No, iz propozicije 3.1.13 vidimo da je tada $[\mathbb{Q}(P) : \mathbb{Q}_{1,2}] \in \{3,9\}$, što je nemoguće.

Pretpostavimo da $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 2. Po teoremu 3.1.7 i po korolaru 3.1.12 i točka reda 2 i točka reda 9 su definirane nad poljem $\mathbb{Q}_{1,2}$. Ovo pak znači da $E(\mathbb{Q}_{1,2})$ sadrži točku reda 18. No, to je kontradikcija s rezultatom [45, Theorem 2] koji (između ostalog) govori da ne postoji eliptička krivulja definirana nad $\mathbb{Q}$ s točkom reda 18 nad kvadratnim proširenjem od $\mathbb{Q}$. ■

Lema 3.5.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Ako $E(\mathbb{Q}_{\infty,2})$ sadrži točku reda 12, onda je*

$$E(\mathbb{Q}_{\infty,2})_{tors} \simeq \mathbb{Z}/12\mathbb{Z}.$$

Dokaz. Budući da znamo sve prethodne rezultate, dovoljno je pokazati da $E(\mathbb{Q}_{\infty,2})$ ne sadrži punu 2-torziju i da ne sadrži točku reda 24. Rezultat [5, Theorem 1.2] nam govori da eliptička krivulja $E/\mathbb{Q}$ ne sadrži točku reda 24 nad maksimalnim Abelovim proširenjem $\mathbb{Q}^{\text{ab}}$ od $\mathbb{Q}$. Kako je $\mathbb{Q}_{\infty,2} \subset \mathbb{Q}^{\text{ab}}$, zaključujemo da $E(\mathbb{Q}_{\infty,2})$ uistinu ne sadrži točku reda 24.

Jedina preostala mogućnost je da je $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ pa pretpostavimo da je to slučaj. Neka je $E(\mathbb{Q}_{\infty,2})_{\text{tors}} = \langle Q, P \rangle$, gdje je P točka reda 12, a Q točka reda 2. Koristeći teorem 3.1.7 zaključujemo da je točka Q (reda 2) definirana nad poljem $\mathbb{Q}_{1,2}$, a koristeći korolar 3.1.12 zaključujemo da je točka $4P$ (reda 3) također definirana nad poljem $\mathbb{Q}_{1,2}$.

Primijetimo da je $2E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \langle 2P \rangle \simeq \mathbb{Z}/6\mathbb{Z}$, što znači da je $(2P)^\sigma = 2aP$, za neki $a \in \{1,3,5\}$, za svaki $\sigma \in \text{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. To nadalje znači da je $(6P)^\sigma = 6P$, tj. točka $6P$ je definirana

nad $\mathbb{Q}$. Sada iz [17, Proposition 4.8] zaključujemo da je točka $3P$ definirana nad poljem kojemu je Galoisova grupa izomorfna $\mathbb{Z}/2\mathbb{Z}$, tj. nad poljem $\mathbb{Q}_{1,2}$.

To sve skupa znači da je zapravo $E(\mathbb{Q}_{1,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, što je kontradikcija s rezultatom [25, Theorem 10]. ■

Teorem 3.5.8. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}_{\infty,2})[2^\infty] \leq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Dokaz. Riječ je o rezultatu [14, Theorem 1]. ■

Dokaz teorema 3.2.3. Iz lema 3.5.1, 3.5.2 i 3.5.3 odmah zaključujemo da je

$$E(\mathbb{Q}_{\infty,2})[q^\infty] = \{0\} = E(\mathbb{Q})[q^\infty],$$

za sve proste brojeve q različite od 2, 3, 5 i 7. Konačno, leme 3.5.4, 3.5.5, 3.5.6, 3.5.7 te teorem 3.5.8 nam pokazuju da su jedine moguće torzije upravo one iz Mazurovog teorema, [37]. ■

3.6. RAST TORZIJE

Imajući na umu teorem 3.2.1 vidimo da je torzija svake eliptičke krivulje $E/\mathbb{Q}$ jednaka nad poljem $\mathbb{Q}$ i nad poljem $\mathbb{Q}_{\infty,p}$, za svaki prost broj $p > 3$. Kao što smo već napomenuli, u slučajevima $p = 2$ i $p = 3$ postoje eliptičke krivulje $E/\mathbb{Q}$ takve da je $E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}}$. U nastavku ove sekcije dajemo primjere takvih eliptičkih krivulja te određujemo u kojim slučajevima postoji beskonačno mnogo različitih j-invarijanti takvih da postoji eliptička krivulja $E/\mathbb{Q}$ s tom j-invarijantom takva da je $E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}} = G$, gdje je G neka od grupa koja se može pojaviti kao $E(\mathbb{Q}_{\infty,p})_{\text{tors}}$.

Teorem 3.6.1. *Neka je G neka od grupa*

$$\mathbb{Z}/n\mathbb{Z}, \quad 3 \leq n \leq 10 \text{ ili } n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

Tada postoji beskonačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ s različitim j-invarijantama takvih da je

$$E(\mathbb{Q})_{tors} \subsetneq E(\mathbb{Q}_{\infty,2})_{tors} \simeq G.$$

Napomena 3.6.2. *Primijetimo da se ovdje nalaze sve grupe iz teorema 3.2.3, tj. iz Mazurovog teorema [37, Theorem 1], osim trivijalne i grupe $\mathbb{Z}/2\mathbb{Z}$. Naime, ako je $E(\mathbb{Q}_{\infty,2})_{tors}$ trivijalna, jasno je da je i $E(\mathbb{Q})_{tors}$ trivijalna grupa. Nadalje, ako $E(\mathbb{Q}_{\infty,2})$ ima točku reda 2, onda ju ima i $E(\mathbb{Q})$ (npr. 3.1.12), stoga je i slučaj $E(\mathbb{Q})_{tors} \subsetneq E(\mathbb{Q}_{\infty,2})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}$ nemoguć.*

Dokaz. Pretpostavimo najprije da je $n = 2k+1$, za neki $k \in \{1,2,3,4\}$, tj. n je neparan prirodan broj između 3 i 10. Neka je $G = \mathbb{Z}/n\mathbb{Z}$. Tada postoji beskonačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ s različitim j-invarijantama takvih da je $E(\mathbb{Q})_{\text{tors}} \simeq G$. Pogledati prvu stranicu (tablicu na njoj) u [37]. Nadalje, eliptičke krivulje $E/\mathbb{Q}$ takve da je $E(\mathbb{Q})_{\text{tors}} \simeq G$ pojavljuju se u 1-parametarskoj familiji (pogledati npr. u [32, 35, 46]) te generički nemaju dodatnih izogenija. Stoga po Hilbertovom teoremu o ireducibilnosti, izvan "tankog" skupa svaka krivulja u familiji nema dodatnih racionalnih izogenija. Za više detalja o tankim skupovima i Hilbertovom teoremu o ireducibilnosti pogledati [50, §9]. Dakle, za svaku takvu eliptičku krivulju $E/\mathbb{Q}$, njen će kvadratni twist E^2 imati trivijalnu torziju nad $\mathbb{Q}$, zato što za neparni n vrijedi

$$E(\mathbb{Q}(\sqrt{2}))[n] \simeq E(\mathbb{Q})[n] \oplus E^2(\mathbb{Q})[n].$$

Nadalje, polje $\mathbb{Q}(\sqrt{2})$ ne zadrži niti jedan ζ_m, za $m > 2$, a to skupa s činjenicom da je n neparan i uz svojstva Weilovog sparivanja rezultira time da je $E^2(\mathbb{Q})[n] \simeq \{0\}$. Nadalje, krivulje E i E^2 su izomorfne nad $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}_{\infty,2}$ pa slijedi da je $E^2(\mathbb{Q}_{\infty,2})[n] \simeq G$. Primijetimo još da torzija ne može rasti dodatno zato što E pa time ni E^2 nema dodatnih racionalnih izogenija, stoga je uistinu $E^2(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq G$.

Neka je sada $n = 2k$, gdje je $k \in \{2,3,4,5,6\}$, tj. n je paran prirodan broj između 3 i 12. Kao i prije, znamo da postoji beskonačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ s različitim j-invarijantama takvih da je $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/n\mathbb{Z}$ i koje nemaju dodatnih racionalnih izogenija. Sada je, analogno kao i prije

$$E^2(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z},$$
$$E^2(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/n\mathbb{Z} \text{ ili } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Za $n = 10$ i $n = 12$ jedina je mogućnost da je $E^2(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/n\mathbb{Z}$ (teorem 3.2.3) pa smo u tim slučajevima gotovi. Ukoliko je $n \in \{4,6,8\}$ onda su obje navedene mogućnosti za $E^2(\mathbb{Q}_{\infty,2})_{\text{tors}}$ uistinu moguće, ovisno o tome kako izgleda diskriminanta eliptičke krivulje E.

U [32, 35, 46] možemo naći parametrizaciju 1-parametarske familije eliptičkih krivulja čija je torzija nad $\mathbb{Q}$ izomorfna grupi $\mathbb{Z}/n\mathbb{Z}$ za $n \in \{4,6,8\}$. Koristimo programski alat `magma` [2] (kôd 10.m), opišimo što i kako u slučaju $n = 4$. Isto radimo i za $n = 6$ te $n = 8$. Neki model eliptičkih krivulja E_t takvih da je $E_t(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z}$ dan je formulom

$$E_t \ : \ y^2 + xy - ty = x^3 - tx^2,$$

gdje je t proizvoljan racionalan broj različit od 0 i $\dfrac{-1}{16}$. Diskriminanta ove krivulje je oblika $\Delta_t = (16t+1)\square$. Krivulja

$$C \ : \ 16t + 1 = 2s^2$$

je krivulja genusa 0 koja ima barem jednu racionalnu točku, npr. $(t,s) = \left(\dfrac{1}{16}, 1\right)$. To znači da ih ima beskonačno. Odnosno, postoji beskonačno mnogo racionalnih brojeva t takvih da je $\Delta_t = 2\square$ i vidimo da je u tom slučaju $E^2(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

Analogno, promatrajući krivulju $16t + 1 = -s^2$ zaključimo da postoji beskonačno mnogo racionalnih brojeva t takvih da je $\Delta_t = -\square$ te u tom slučaju vrijedi $E^2(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/n\mathbb{Z}$.

Preostaje vidjeti što se događa u slučaju $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Definiramo familiju eliptičkih krivulja, za $t \in \mathbb{Q} \setminus \{0\}$:

$$E_t \quad \dots \quad y^2 = x^3 - \frac{4}{2t^2-1}x^2 - \frac{4}{2t^2-1}x.$$

Za tu familiju vrijedi da je $E_t(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$ i $\mathbb{Q}(E_t[2]) = \mathbb{Q}(\sqrt{2})$, što je provjereno koristeći programski alat `magma` [2], kôd 11.m. Te krivulje generički nemaju dodatnih racionalnih izogenija, stoga je za beskonačno mnogo njih

$$E_t(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}. \qquad \blacksquare$$

U tablici 3.1 (ispod) navodimo primjere eliptičkih krivulja $E/\mathbb{Q}$ za sve moguće slučajeve rasta iz prethodnog teorema 3.6.1.

Cremonina oznaka	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,2})_{\text{tors}}$
704d1	$\{0\}$	$\mathbb{Z}/3\mathbb{Z}$
24a6	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$
704a1	$\{0\}$	$\mathbb{Z}/5\mathbb{Z}$
320c1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$
832f	$\{0\}$	$\mathbb{Z}/7\mathbb{Z}$
24a3	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$
1728j3	$\{0\}$	$\mathbb{Z}/9\mathbb{Z}$
768b1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/10\mathbb{Z}$
30a5	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$
14a5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
24a2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
14a2	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
32a4	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

Tablica 3.1: Eliptičke krivulje s rastom torzije $\mathbb{Q} \to \mathbb{Q}_{\infty,2}$, [54]

U nastavku proučavamo rast torzije eliptičke krivulje $E/\mathbb{Q}$ nad poljem $\mathbb{Q}_{\infty,3}$. Imajući na umu teorem 3.2.2 i njegov dokaz, tj. sekciju 3.4, zaključujemo činjenice iz sljedeće napomene.

Napomena 3.6.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja, ako je $E(\mathbb{Q}_{\infty,3})_{\text{tors}}$ izomorfna nekoj od grupa*

$$\{0\}, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/5\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/10\mathbb{Z}, \quad \mathbb{Z}/12\mathbb{Z},$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z},$$

onda je $E(\mathbb{Q})_{tors} = E(\mathbb{Q}_{\infty,3})_{tors}$. Dakle, u tim slučajevima nema rasta torzije nad poljem $\mathbb{Q}_{\infty,3}$.

U tablici (3.2) navodimo primjere eliptičkih krivulja $E/\mathbb{Q}$ za sve moguće slučajeve rasta nad poljem $\mathbb{Q}_{\infty,3}$.

Lako se vidi da krivulje $X_0(21)$ i $X_0(27)$ imaju konačno mnogo racionalnih točaka, stoga postoji samo konačno mnogo različitih j-invarijanti takvih da postoji eliptička krivulja $E/\mathbb{Q}$ s danom j-invarijantom i rastom torzije $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$ (slučaj I u tablici 3.2):

$$\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/21\mathbb{Z}, \qquad \text{odnosno} \qquad \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/27\mathbb{Z}.$$

Za preostala 2 slučaja rasta torzije nad poljem $\mathbb{Q}_{\infty,3}$ (tj. za slučajeve II i III iz tablice 3.2) u nastavku dokazujemo da postoji beskonačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ s međusobno različitim j-invarijantama za koje se taj rast događa.

slučaj	Cremonina oznaka	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathbb{Q}_{\infty,3})_{\text{tors}}$
I	162b1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/21\mathbb{Z}$
	27a4	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/27\mathbb{Z}$
II	324a2	$\{0\}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
	324a1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
III	162b2	$\{0\}$	$\mathbb{Z}/7\mathbb{Z}$
	27a3	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$

Tablica 3.2: Eliptičke krivulje s rastom torzije $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$, [54]

Navodimo najprije jedan tehnički rezultat koji nam je potreban, a pomoću kojeg računamo konduktor kubičnog polja u terminima njegovog definirajućeg polinoma.

U idućem tehničkom teoremu potrebno je znati što je to **konduktor** polja algebarskh brojeva. Za općenitu definiciju i za detalje o konduktorima pogledati u [33, Chapter X]. Preciznije, ono što je nama potrebno je sljedeće:

Neka je $\mathbb{K}$ konačno Abelovo proširenje od $\mathbb{Q}$. Prema Kronecker - Weberovom teoremu znamo da postoji prirodni broj n takav da je $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, gdje je ζ_n primitivni n-ti korijen iz jedinice. Najmanji takav prirodni broj n naziva se *konduktor* polja $\mathbb{K}$.

Teorem 3.6.4. *Neka je $\mathbb{K}$ polje takvo da je $[\mathbb{K} : \mathbb{Q}] = 3$ i $\text{Gal}(\mathbb{K}/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. Tada vrijedi sljedeće*

- *$\mathbb{K} = \mathbb{Q}(\alpha)$, pri čemu je α nultočka polinoma*

$$x^3 + Ax + B,$$

gdje su A i B cijeli brojevi takvi da, ako za cijeli broj R vrijedi

$$R^2 \mid A \quad i \quad R^3 \mid B, \quad \text{onda je} \quad |R| = 1.$$

- *Konduktor $\mathfrak{f}(\mathbb{K})$ polja $\mathbb{K}$ dan je formulom*

$$\mathfrak{f}(\mathbb{K}) = 3^{\ell} \cdot \prod_{\substack{\text{prost broj } p \\ p \equiv 1 \pmod 3 \\ p \mid A \text{ i } p \mid B}} p,$$

gdje je

$$\ell = \begin{cases} 0, & \text{ako} \quad 3 \nmid A \quad \text{ili} \quad 3 \parallel A \text{ i } 3 \nmid B \text{ te } 3^3 \mid C, \\ 2, & \text{ako} \quad 3^2 \parallel A \text{ i } 3^2 \parallel B \quad \text{ili} \quad 3 \parallel A \text{ i } 3 \nmid B \text{ te } 3^2 \parallel C, \end{cases}$$

pri čemu je C drugi korijen diskriminante polja $\mathbb{K}$.

Dokaz. Riječ je centralnom rezultatu iz članka [23]. Napomenimo samo da su dva navedena slučaja za broj ℓ uistinu jedina dva (tj. četiri) slučaja koja se mogu dogoditi. ■

Iduća lema nam je ključni sastojak konstrukcije beskonačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ s međusobno različitim j-invarijantama za koje imamo rast torzije u slučaju II u tablici 3.2, tj. rast $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$:

$$\{0\} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \quad \text{odnosno} \quad \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Lema 3.6.5. *Neka je p prost broj takav da je $p \equiv 1 \pmod 3$ te neka je $k \in \{2,3\}$. Tada postoje relativno prosti cijeli brojevi u i v takvi da je*

$$u^2 + 27v^2 = 4 \cdot 3^k \cdot p^3.$$

Dokaz. Fiksirajmo prost broj p takav da je $p \equiv 1 \pmod 3$ i broj $k \in \{2,3\}$.

Neka je $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$, tada je

$$u^2 + 27v^2 = \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(u + 3v\sqrt{-3}).$$

Dakle, zapravo želimo pokazati da se u $\mathbb{K}$ nalazi element oblika $u + 3v\sqrt{-3}$ norme $4 \cdot 3^k \cdot p^3$, gdje su u i v relativno prosti cijeli brojevi.

Primijetimo da je (za $k \in \{2,3\}$)

$$4 \cdot 3^k = \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(3^{k-1} + 3\sqrt{-3}).$$

Dakle, imajući na umu da je norma multiplikativna, preostaje pokazati da se u $\mathbb{K}$ nalazi element oblika $u+3v\sqrt{-3}$ norme p^3, gdje su u i v relativno prosti cijeli brojevi.

Prsten cijelih brojeva u $\mathbb{Q}(\sqrt{-3})$ su zapravo Eisensteinovi cijeli brojevi, tj. jednak je $\mathbb{Z}[\zeta_3]$. Kako je $p \equiv 1 \pmod 3$, znamo da se prost broj p cijepa u polju $\mathbb{K}$, tj.

$$p = \mathfrak{p}\overline{\mathfrak{p}} = (a+b\zeta_3)(a+b\zeta_3^2),$$

za neke cijele brojeve a i b. Imamo da je $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}) = p$, stoga tvrdimo da je $\mathfrak{p}^3$ traženi element. Preostaje vidjeti da postoje relativno prosti cijeli brojevi u i v takvi da je $\mathfrak{p}^3 = (u+3v\sqrt{-3})$. Vrijedi da je

$$\mathfrak{p}^3 = (a+b\zeta_3)^3 = (a^3+b^3-3ab^2+3ab(a-b)\zeta_3).$$

Kako je $\mathfrak{p}$ prost, zaključujemo da su a i b relativno prosti. To znači i da su $a^3+b^3-3ab^2$ i $3ab(a-b)$ relativno prosti. Konačno, preostaje primijetiti da je broj $ab(a-b)$ paran, čime je dokaz priveden kraju. ■

Teorem 3.6.6. *Postoji beskonačno mnogo racionalnih brojeva j takvih da postoji eliptička krivulja $E/\mathbb{Q}$ s j-invarijantom j takva da je*

$$E(\mathbb{Q})_{tors} \simeq \{0\} \qquad i \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Također, postoji beskonačno mnogo $j \in \mathbb{Q}$ takvih da postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $j(E) = j$ te

$$E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z} \qquad i \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Prije samog dokaza samo napomenimo da ovaj teorem zapravo tvrdi da u slučaju II iz tablice 3.2 uistinu postoji beskonačno mnogo eliptičkih krivulja s međusobno različitim j-invarijantama za koje se taj rast događa.

Dokaz. Želimo pokazati da postoji beskonačno mnogo eliptičkih krivulja $E'/\mathbb{Q}$ (s međusobno različitim j-invarijantama) takvih da je

$$E'(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \qquad \text{i} \qquad E'(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

To zapravo znači da E' ima racionalnu 3-izogeniju i diskriminantu koja je jednaka kvadratu nekog racionalnog broja. Dakle, E' odgovara nekoj racionalnoj točki na $X_0(3)$ pa je zato

$$j(E') = \frac{(r+27)(r+3)^3}{r},$$

za neki racionalni broj $r \in \mathbb{Q} \setminus \{0\} = \mathbb{Q}^*$. Model neke eliptičke krivulje s tom j-invarijantom je dan s

$$E_r \quad \dots \quad y^2 = f_r(x),$$

gdje je

$$f_r(x) = x^3 + \frac{-27(r+3)^3(r+27)}{(r^2+18r-27)^2}x + \frac{54(r+3)^3(r+27)}{(r^2+18r-27)^2}.$$

Izračunamo li diskriminantu ovog modela za eliptičku krivulju E_r vidimo da je ona kvadrat racionalnog broja ako i samo ako je r kvadrat racionalnog broja. Dakle, za $r \in (\mathbb{Q}^*)^2$ je

$$\mathrm{Gal}\,(\mathbb{Q}(E_r[2])/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \qquad \text{i} \qquad \mathbb{Q}(E_r[2]) = \mathbb{Q}(f_r).$$

Ono što nas zanima je kada je $\mathbb{Q}(f_r) = \mathbb{Q}_{1,3}$. No, to će vrijediti onda i samo onda kada je konduktor polja $\mathbb{Q}(f_r)$ potencija broja 3.

Zamjenom varijabli

$$x \cdot \frac{r^2+18r-27}{r+3} \to x$$

vidimo da je $\mathbb{Q}(f_r) = \mathbb{Q}(x^3 + A_r x + B_r)$, gdje je

$$A_r = -27(r+3)(r+27) \qquad \text{i} \qquad B_r = 54(r+27)(r^2+18r-27).$$

Znamo da je $r \in (\mathbb{Q}^*)^2$ pa postoje relativno prosti cijeli brojevi u i v takvi da je $r = \frac{u^2}{v^2}$, sada vidimo da je $\mathbb{Q}(f_r) = \mathbb{Q}(x^3 + A_{u,v}x + B_{u,v})$, gdje je

$$A_{u,v} = -27(u^2+3v^2)(u^2+27v^2) \qquad \text{i} \qquad B_{u,v} = 54(u^4+18u^2v^2-27v^4)(u^2+27v^2).$$

Iz teorema 3.6.4 sada znamo da će konduktor polja $\mathbb{Q}(f_r)$ biti potencija broja 3 ako i samo ako je $\gcd(A_{u,v}, B_{u,v})$ djeljiv samo brojem 3, prostim brojevima p takvima da je $p \equiv 2 \pmod 3$ te kubovima prirodnih brojeva, budući da kubove možemo zanemariti jednostavnom zamjenom varijabli. Primijetimo da je

$$u^4 + 18u^2v^2 - 27v^4 = (u^2-9v^2)(u^2+3v^2) + 24u^2v^2,$$

pretpostavimo da prost broj $p \neq 2,3$ dijeli brojeve u^2+3v^2 i $u^4+18u^2v^2-27v^4$, to znači da p dijeli u^2+3v^2 i $24u^2v^2$. Kako je $p \neq 2,3$ zaključujemo da $p \mid u^2v^2$, a kako $p \mid u^2+3v^2$ i $p \neq 3$ zaključujemo da $p \mid u$ i $p \mid v$, što je kontradikcija budući da su u i v relativno prosti cijeli brojevi. Dakle, vrijedi da je

$$\gcd(A_{u,v}, B_{u,v}) = 2^a \cdot 3^b \cdot (u^2+27v^2),$$

za neke nenegativne cijele brojeve a i b.

Koristeći lemu 3.6.5 vidimo da za proizvoljan prost broj $p \equiv 1 \pmod 3$ možemo odabrati cijele brojeve u i v takve da je

$$\gcd(A_{u,v}, B_{u,v}) = 2^{a+2} \cdot 3^{b+k} \cdot p^3,$$

gdje su a i b nenegativni cijeli brojevi i $k \in \{2,3\}$. U tom slučaju je, po teoremu 3.6.4, konduktor polja $\mathbb{Q}(E_r[2])$ potencija broja 3 te je stoga $\mathbb{Q}(E_r[2]) = \mathbb{Q}_{1,3}$.

Konačno, kako je $p \equiv 1 \pmod 3$ proizvoljan vidimo da za svaki takav p dobijemo drukčiji $r = \dfrac{u}{v}$. Odnosno, osigurali smo beskonačno mnogo različitih j-invarijanti. Nadalje, po konstrukciji, krivulja E_r je definirana nad $\mathbb{Q}$ i ima racionalnu 3-izogeniju. Stoga postoji kvadratni twist od E_r koji ima točku reda 3 nad $\mathbb{Q}$. Preostaje primijetiti da kvadratni twist ne mijenja polje definicije točaka reda 2, stoga ovaj twist ima upravo rast koji želimo. ■

Za kraj ove sekcije dokazujemo još postojanje beskonačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ s međusobno različitim j-invarijantama za koje imamo rast torzije u slučaju III iz tablice 3.2, tj. rast $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$:

$$\{0\} \to \mathbb{Z}/7\mathbb{Z} \qquad \text{i} \qquad \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}.$$

Kao i za slučaj II, najprije navodimo sljedeću tehničku lemu. Ideja je generalno ista kao i za slučaj II, no sami detalji su ipak nešto drugačiji.

Lema 3.6.7. *Neka je $f(x,y)$ binarna kvadratna forma s diskriminantnom -27. Tada za svaki prost broj $p \equiv 1 \pmod 3$ postoje relativno prosti cijeli brojevi x i y takvi da je*

$$f(x,y) = 3^3 \cdot p^3.$$

Dokaz. Binarna kvadratna forma $f(x,y)$ ima diskriminantu -27, stoga postoji zamjena varijabli matricom iz $\mathrm{SL}_2(\mathbb{Z})$ tako da je

$$f(x,y) \sim u^2 + uv + 7v^2.$$

Preciznije, forme $f(x,y)$ i $u^2+uv+7v^2$ su ekvivalentne, što znači da postoji $M \in \mathrm{SL}_2(\mathbb{Z})$ takva da

$$\begin{bmatrix} u \\ v \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix} \implies f(x,y) = u^2 + uv + 7v^2.$$

Također, vrijedi da zamjena varijabli matricom iz $\mathrm{SL}_2(\mathbb{Z})$ čuva najveću zajedničku mjeru, tj. za $M \in \mathrm{SL}_2(\mathbb{Z})$ je

$$\begin{bmatrix} u \\ v \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix} \implies \gcd(x,y) = \gcd(u,v).$$

Stoga je dovoljno pokazati da za svaki prost broj $p \equiv 1 \pmod 3$ postoje relativno prosti brojevi u i v takvi da je

$$u^2 + uv + 7v^2 = 3^3 \cdot p^3.$$

Fiksirajmo nadalje neki prost broj $p \equiv 1 \pmod 3$. Kao i u dokazu leme 3.6.5, promatrajmo polje $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Prsten cijelih u tom polju su Eisensteinovi cijeli brojevi $\mathbb{Z}[\zeta_3]$. Ovdje podrazumijevamo da je $\zeta_3 = \dfrac{-1+\sqrt{-3}}{2}$. Primijetimo da je

$$u^2 + uv + 7v^2 = \mathrm{N}_{\mathbb{K}/\mathbb{Q}}(u + 3v\zeta_3),$$

stoga moramo pokazati da u $\mathbb{K}$ postoji element oblika $u + 3v\zeta_3$ norme $3^3 \cdot p^3$, gdje su u i v relativno prosti cijeli brojevi.

Prost broj p se cijepa u polju $\mathbb{K}$, što znači da postoje cijeli brojevi x i y takvi da je

$$p = \mathfrak{p}\overline{\mathfrak{p}} = (x + y\zeta_3)(x + y\zeta_3^2).$$

Vrijedi da je $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}) = p$, stoga tvrdimo da je $\mathfrak{p}^3$ traženi element. Preostaje vidjeti da postoje relativno prosti cijeli brojevi a i b takvi da je $\mathfrak{p}^3 = (a + 3b\sqrt{-3})$. Računamo

$$\mathfrak{p}^3 = (x + y\zeta_3)^3 = (x^3 + y^3 - 3xy^2 + 3xy(x-y)\zeta_3).$$

Kako je $\mathfrak{p}$ prost, zaključujemo da su x i y relativno prosti. To znači i da su $x^3 + y^3 - 3xy^2$ te $3xy(x-y)$ relativno prosti. Preostaje primijetiti da je broj $xy(x-y)$ paran.

Nadalje, primijetimo da je $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\sqrt{-3}) = 3$, stoga je $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(3\sqrt{-3}) = 3^3$. Lako se vidi da je $(3\sqrt{-3}) = (3 + 3 \cdot 2 \cdot \zeta_3)$ pa je

$$\mathfrak{p}^3(3\sqrt{-3}) = (3(a-6b) + 3 \cdot (2a-3b) \cdot \zeta_3)\,.$$

Preostaje vidjeti da su brojevi $3(a-6b)$ i $2a-3b$ relativno prosti. Pretpostavimo najprije da je $q \neq 3$ prost broj takav da $q \mid 3(a-6b)$ i $q \mid 2a-3b$. To znači da $q \mid a-6b$, tj.

$$q \mid (2a-3b) - 2(a-6b) = 9b,$$

odnosno $q \mid b$, a to onda znači da $q \mid (a-6b) + 6b = a$, što je kontradikcija jer su a i b relativno prosti. Primijetimo da $3 \mid 3(a-6b)$ i $3 \mid 2a-3b$ ako i samo ako $3 \mid a$. Dakle, preostaje vidjeti da $3 \nmid a$. Sjetimo se da je

$$a = x^3 + y^3 - 3xy^2,$$

gdje su x i y relativno prosti cijeli brojevi takvi da je $x^2 - xy + y^2 = p \equiv 1 \pmod 3$. Sada je

$$a \equiv x^3 + y^3 = (x+y)(x^2 - xy + y^2) \equiv x + y \pmod 3.$$

No, $x+y \equiv 0 \pmod 3$ znači da je $y \equiv -x \pmod 3$, tj. $x^2 - xy + y^2 \equiv 3x^2 \equiv 0 \pmod 3$, što je kontradikcija. ■

Iduća dva teorema napokon dovršavaju i slučaj III iz tablice 3.2.

Teorem 3.6.8. *Postoji beskonačno mnogo racionalnih brojeva j takvih da postoji eliptička krivulja $E/\mathbb{Q}$ s j-invarijantom j takva da je*

$$E(\mathbb{Q})_{tors} \simeq \{0\} \qquad i \qquad E(\mathbb{Q}_{\infty,3})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}.$$

Dokaz. Želimo pokazati da postoji beskonačno mnogo eliptičkih krivulja $E'/\mathbb{Q}$ (s međusobno različitim j-invarijantama) takvih da je $E'(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/7\mathbb{Z}$. To znači da E' ima racionalnu 7-izogeniju, što znači da E' odgovara nekoj racionalnoj točki na $X_0(7)$ pa je

$$j(E') = \frac{(r^2+13r+49)(r^2+5r+1)^3}{r},$$

za neki racionalni broj $r \neq 0$. Model za neku eliptičku krivulju s tom j-invarijantom je dan s

$$E_r \quad \dots \quad y^2 = f_r(x),$$

gdje je

$$f_r(x) = x^3 + \frac{-27(r^2+5r+1)^3(r^2+13r+49)}{(r^4+14r^3+63r^2+70r-7)^2}x + \frac{54(r^2+5r+1)^3(r^2+13r+49)}{(r^4+14r^3+63r^2+17r-7)^2}.$$

Računamo 7. djelidbeni polinom eliptičke krivulje E_r i uočimo da je on jednak umnošku dva ireducibilna polinoma, jednog stupnja 3 i drugog stupnja 21. Ireducibilni polinom stupnja 3 označimo s $f_{r,3}$. Želimo odrediti racionalne brojeve r za koje je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}_{1,3}$. Zamjenom varijabli postižemo da je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}(x^3 + A_r x + B_r)$, gdje je

$$A_r = -3(r^2+13r+49) \qquad \text{i} \qquad B_r = -(2r+13)(r^2+13r+49).$$

Kako je $r \neq 0$ racionalan broj, postoje relativno prosti cijeli brojevi u i v takvi da je $r = \frac{u}{v}$. Sada vidimo da je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}(x^3 + A_{u,v}x + B_{u,v})$, gdje je

$$A_{u,v} = -3(u^2+13uv+49v^2) \qquad \text{i} \qquad B_{u,v} = -(2u+13v)(u^2+13uv+49v^2).$$

Kao i u dokazu teorema 3.6.6, vrijedit će da je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}_{1,3}$ ako i samo ako je konduktor polja $\mathbb{Q}(f_{r,3})$ jednak potenciji broja 3. To će, po teoremu 3.6.4, vrijediti onda kada je $\gcd(A_{u,v}, B_{u,v})$ djeljiv samo brojem 3, prostim brojevima p takvima da je $p \equiv 2 \pmod 3$ te kubovima prirodnih brojeva, budući da, zamjenom varijabli, kubove možemo zanemariti.

Primijetimo da je

$$\gcd(A_{u,v}, B_{u,v}) = 3^a \cdot (u^2 + 13uv + 49v^2),$$

za neki $a \in \{0,1\}$. Vidimo da je diskriminanta binarne kvadratne forme $u^2 + 13uv + 49v^2$ jednaka -27. To znači da po lemi 3.6.7, za svaki prost broj $p \equiv 1 \pmod 3$, možemo naći relativno proste cijele brojeve u i v takve da je

$$\gcd(A_{u,v}, B_{u,v}) = 3^{a+3} \cdot p^3.$$

U tom slučaju je, po teoremu 3.6.4, konduktor polja $\mathbb{Q}(f_{r,3})$ potencija broja 3 te je stoga $\mathbb{Q}(f_{r,3}) = \mathbb{Q}_{1,3}$.

Konačno, proizvoljnost prostog broja $p \equiv 1 \pmod 3$ nam osigurava beskonačno mnogo različitih j-invarijanti. Nadalje, po konstrukciji, krivulja E_r je definirana nad $\mathbb{Q}$ i ima racionalnu 7-izogeniju. Stoga postoji kvadratni twist od E_r koji nema točku reda 7 nad $\mathbb{Q}$, a ima nad $\mathbb{Q}_{\infty,3}$. Ovime smo gotovi. ■

Teorem 3.6.9. *Postoji beskonačno mnogo $j \in \mathbb{Q}$ takvih da postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $j(E) = j$ te*

$$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \qquad i \qquad E(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/9\mathbb{Z}.$$

Dokaz. Želimo pokazati da postoji beskonačno mnogo eliptičkih krivulja $E'/\mathbb{Q}$ (s međusobno različitim j-invarijantama) takvih da je

$$E'(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \qquad \text{i} \qquad E'(\mathbb{Q}_{\infty,3})_{\text{tors}} \simeq \mathbb{Z}/9\mathbb{Z}.$$

To znači da E' ima točku reda 3 definiranu nad $\mathbb{Q}$ te da ima racionalnu 9-izogeniju čija jezgra sadrži tu točku reda 3. U [8, Table 6] nalazimo generički model za eliptičku krivulju s tim svojstvom:

$$E_r \quad \dots \quad y^2 = f_r(x),$$

gdje je

$$f_r(x) = x^3 - 27r^5(r^3-24)^5 x + 54r^6(r^3-24)^6(r^6 - 36r^3 + 216),$$

za neki $r \in \mathbb{Q}$. Računamo 9. djelidbeni polinom eliptičke krivulje E_r i uočimo da on ima jedan ireducibilni faktor stupnja 3. Označimo taj polinom s $f_{r,3}$. Želimo odrediti racionalne brojeve r za koje je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}_{1,3}$. Zamjenom varijabli postižemo da je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}(x^3 + A_r x + B_r)$, gdje je

$$A_r = -432(r^2 + 3r + 9) \qquad \text{i} \qquad B_r = -1728(2r+3)(r^2+3r+9).$$

Kako je $r \neq 0$ racionalan broj, postoje relativno prosti cijeli brojevi u i v takvi da je $r = \frac{u}{v}$. Sada vidimo da je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}(x^3 + A_{u,v}x + B_{u,v})$, gdje je

$$A_{u,v} = -432(u^2 + 3uv + 9v^2) \qquad \text{i} \qquad B_{u,v} = -1728(2u + 3v)(u^2 + 3uv + 9v^2).$$

Kao i u dokazu teorema 3.6.6, vrijedit će da je $\mathbb{Q}(f_{r,3}) = \mathbb{Q}_{1,3}$ ako i samo ako je konduktor polja $\mathbb{Q}(f_{r,3})$ jednak potenciji broja 3. To će, po teoremu 3.6.4, vrijediti onda kada je $\gcd(A_{u,v}, B_{u,v})$ djeljiv samo brojem 3, prostim brojevima p takvima da je $p \equiv 2 \pmod 3$ te kubovima prirodnih brojeva, budući da, zamjenom varijabli, kubove možemo zanemariti.

Primijetimo da je

$$\gcd(A_{u,v}, B_{u,v}) = 2^4 \cdot 3^3 \cdot (u^2 + 3uv + 9v^2).$$

Vidimo da je diskriminanta binarne kvadratne forme $u^2 + 3uv + 9v^2$ jednaka -27. To znači da po lemi 3.6.7, za svaki prost broj $p \equiv 1 \pmod 3$, možemo naći relativno proste cijele brojeve u i v takve da je

$$\gcd(A_{u,v}, B_{u,v}) = 2^4 \cdot 3^6 \cdot p^3.$$

U tom slučaju je, po teoremu 3.6.4, konduktor polja $\mathbb{Q}(f_{r,3})$ potencija broja 3 te je stoga $\mathbb{Q}(f_{r,3}) = \mathbb{Q}_{1,3}$.

Konačno, kako je $p \equiv 1 \pmod 3$ proizvolljan vidimo da za svaki takav p dobijemo drukčiji $r = \frac{u}{v}$. Odnosno, osigurali smo beskonačno mnogo različitih j-invarijanti. Nadalje, po konstrukciji, krivulja E_r je definirana nad $\mathbb{Q}$, ima točku reda 3 definiranu nad $\mathbb{Q}$ i ima racionalnu 9-izogeniju. Pokazali smo da je točka reda 9 definirana nad $\mathbb{Q}_{1,3}$ te smo time gotovi. ■

4. TORZIJA NAD KOMPOZITUMOM SVIH $\mathbb{Z}_p$-PROŠIRENJA OD $\mathbb{Q}$

U ovom poglavlju želimo vidjeti kako se ponaša torzija eliptičke krivulje $E/\mathbb{Q}$ nad kompozitumom svih $\mathbb{Z}_p$-proširenja od $\mathbb{Q}$.

Neka je $\mathscr{K}_{\geq 5}$ kompozitum svih $\mathbb{Z}_p$-proširenja od $\mathbb{Q}$, za $p \geq 5$, tj.

$$\mathscr{K}_{\geq 5} = \prod_{p \geq 5 \text{ prost}} \mathbb{Q}_{\infty,p}$$

te neka je $\mathscr{K}$ kompozitum svih $\mathbb{Z}_p$-proširenja od $\mathbb{Q}$, tj.

$$\mathscr{K} = \prod_{p \text{ prost}} \mathbb{Q}_{\infty,p}.$$

Za proste brojeve $p \neq q$ vrijedi da je $\mathbb{Q}_{\infty,p} \cap \mathbb{Q}_{\infty,q} = \mathbb{Q}$ te nam standardni rezultat (beskonačne) Galoisove teorije nam govori da je stoga $\mathrm{Gal}\left(\mathbb{Q}_{\infty,p}\mathbb{Q}_{\infty,q}/\mathbb{Q}\right) \simeq \mathbb{Z}_p \times \mathbb{Z}_q$. Dakle, vrijedi da je

$$\mathrm{Gal}\left(\mathscr{K}_{\geq 5}/\mathbb{Q}\right) \simeq \prod_{p \geq 5 \text{ prost}} \mathbb{Z}_p$$

i

$$\mathrm{Gal}\left(\mathscr{K}/\mathbb{Q}\right) \simeq \prod_{p \text{ prost}} \mathbb{Z}_p.$$

Ova opservacija nam je korisna zato što svako međupolje $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathscr{K}$ možemo točno odrediti ukoliko znamo koliko je $[\mathbb{F} : \mathbb{Q}]$.

Time ćemo se i služiti bez posebnog isticanja. Na primjer, ako je $\mathbb{F}$ polje sadržano u $\mathscr{K}$ za kojeg znamo da je $[\mathbb{F} : \mathbb{Q}] = 60 = 2^2 \cdot 3 \cdot 5$, onda znamo da je

$$\mathbb{F} = \mathbb{Q}_{2,2}\mathbb{Q}_{1,3}\mathbb{Q}_{1,5}.$$

4.1. REZULTATI

Sljedeća dva teorema nam govore da se torzija eliptičke krivulje $E/\mathbb{Q}$ nikako ne mijenja kada ju promatramo nad poljem $\mathscr{K}_{\geq 5}$, no ukoliko istu promotrimo nad poljem $\mathscr{K}$ onda se zbivaju iste stvari kao nad $\mathbb{Z}_3$ i $\mathbb{Z}_2$ proširenjima od $\mathbb{Q}$.

Teorem 4.1.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathscr{K}_{\geq 5})_{tors} = E(\mathbb{Q})_{tors}.$$

Teorem 4.1.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je $E(\mathscr{K})_{\text{tors}}$ izomorfno nekoj od idućih grupa*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z}, &\quad 1 \leq n \leq 10 \text{ ili } n \in \{12,13,21,27\}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, &\quad 1 \leq n \leq 4. \end{aligned}$$

Za svaku grupu G s gornje liste, postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $E(\mathscr{K})_{\text{tors}} \simeq G$.

Primijetimo da je

$$\{E(\mathscr{K})_{\text{tors}} : E/\mathbb{Q} \text{ e.k.}\} = \{E(\mathbb{Q})_{\text{tors}} : E/\mathbb{Q} \text{ e.k.}\} \cup \{\mathbb{Z}/13\mathbb{Z}, \mathbb{Z}/21\mathbb{Z}, \mathbb{Z}/27\mathbb{Z}\},$$

pri čemu e.k. znači eliptička krivulja. Nadalje, postoje mnoge eliptičke krivulje $E/\mathbb{Q}$ kod kojih torzija raste s $\mathbb{Q}$ na $\mathscr{K}$. U prethodnoj sekciji 3.6, za $p = 2$ i $p = 3$, nalazimo za koje grupe G postoji beskonačno mnogo j-invarijanti j takvih da postoji eliptička krivulja $E/\mathbb{Q}$ s j-invarijantom j takva da je

$$E(\mathbb{Q})_{\text{tors}} \subsetneq E(\mathbb{Q}_{\infty,p})_{\text{tors}} \simeq G.$$

Isti primjeri vrijede i za rast $\mathbb{Q} \to \mathscr{K}$. Na kraju dokaza teorema 4.1.2, točnije u lemi 4.3.10 pokazujemo da postoje eliptičke krivulje $E/\mathbb{Q}$ takve da je $E(\mathscr{K})_{\text{tors}} \simeq \mathbb{Z}/13\mathbb{Z}$.

4.2. DOKAZ TEOREMA 4.1.1

Kao što smo već konstatirali, znamo da je $\mathrm{Gal}(\mathscr{K}_{\geq 5}/\mathbb{Q}) \simeq \prod_{p\geq 5 \text{ prost}} \mathbb{Z}_p$. Stoga vidimo da vrijedi sljedeće:

Neka je $\mathbb{F}$ bilo koje konačno proširenje polja $\mathbb{Q}$ sadržano u $\mathscr{K}_{\geq 5}$ i neka je $[\mathbb{F}:\mathbb{Q}] = d$. Ako je p najmanji prosti djeljitelj broja d, onda je $p \geq 5$. Bilo koja točka iz $E(\mathscr{K}_{\geq 5})_{\text{tors}}$ definirana je nad nekim konačnim proširenjem od $\mathbb{Q}$, tj. mora biti definirana nad nekim od spomenutih međupolja $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathscr{K}_{\geq 5}$ koja su konačnog reda nad $\mathbb{Q}$. Iskoristimo li teorem 3.1.8 vidimo da je

$$E(\mathscr{K}_{\geq 5})[q^\infty] = E(\mathbb{Q})[q^\infty],$$

za sve proste brojeve q različite od 5, 7 i 11. Stoga preostaje dokazati da je

$$E(\mathscr{K}_{\geq 5})[5^\infty] = E(\mathbb{Q})[5^\infty], \qquad E(\mathscr{K}_{\geq 5})[7^\infty] = E(\mathbb{Q})[7^\infty] \qquad \text{i} \qquad E(\mathscr{K}_{\geq 5})[11^\infty] = E(\mathbb{Q})[11^\infty],$$

što i dokazujemo u iduće tri leme.

Prije samog iskaza i dokaza tih lema, napomenimo da korolar 3.1.6 vrijedi za polje $\mathscr{K}_{\geq 5}$ potpuno analogno kao i za sva polja $\mathbb{Q}_{\infty,p}$. Naime, dovoljno je primijetiti da je $\mathscr{K}_{\geq 5}$ cikličko proširenje od $\mathbb{Q}$, a time i sva međupolja (konačnog stupnja nad $\mathbb{Q}$) tog proširenja. Nadalje, jedini korijeni iz 1 sadržani u $\mathscr{K}_{\geq 5}$ su ± 1, stoga imamo sve argumente potrebne da bismo potpuno analogno dokazali korolar 3.1.6 u slučaju polja $\mathscr{K}_{\geq 5}$. Preciznije, vrijedi sljedeće

Korolar 4.2.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je p prost broj. Ako $E(\mathscr{K}_{\geq 5})_{tors}$ sadrži točku reda q^n, za neki prost broj q i prirodan broj n, onda je*

$$q^n \in \{2,3,4,5,7,8,9,11,13,16,17,19,25,27,32,37,43,67,163\}.$$

Lema 4.2.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathscr{K}_{\geq 5})[5^\infty] = E(\mathbb{Q})[5^\infty].$$

Dokaz. Uz 4.2.1, vidimo da dokaz ide potpuno analogno kao dokaz leme 3.3.5. ■

Lema 4.2.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathscr{K}_{\geq 5})[7^\infty] = E(\mathbb{Q})[7^\infty].$$

Dokaz. Najprije, koristeći korolar 4.2.1 zaključujemo da nema točaka reda 49 u $E(\mathscr{K}_{\geq 5})$, stoga preostaje pokazati da je $E(\mathscr{K}_{\geq 5})[7] = E(\mathbb{Q})[7]$. Pogledamo li teorem 3.1.7 vidimo da je jedina mogućnost da je $P \in E(\mathbb{Q}_{1,7})$, gdje je $P \in E(\mathscr{K}_{\geq 5})$ točka reda 7. No, sada potpuno analogno kao u teoremu 3.3.1 zaključimo da je $P \in E(\mathbb{Q})$ i gotovi smo. ■

Prije samog dokaza činjenice da je $E(\mathscr{K}_{\geq 5})[11^\infty] = E(\mathbb{Q})[11^\infty]$ iskažimo i dokažimo jedan tehnički korolar leme 3.1.10 koji će nam biti koristan i u dokazu teorema 4.1.2.

Korolar 4.2.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja te neka je $P \in E$ točka reda n. Ako E ima racionalnu n-izogeniju čiju jezgru generira točka P, onda $[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(n)$.*

Napomena. *Ovaj korolar ćemo opetovano koristiti skupa s lemom 3.1.4. Preciznije, pogledamo li dokaz te leme, tj. dokaz [9, Lemma 4.6] vidimo da će u našoj situaciji uvijek vrijediti sljedeće. Ako je $P \in E(\mathbb{K})$ točka reda n, onda je grupa $\langle P \rangle$ invarijantna pod djelovanjem opće Galoisove grupe* $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$*, tj. točka P generira jezgru racionalne n-izogenije.*

Dokaz. Slijedi direktno iz spomenute leme 3.1.10. Naime, grupa $(\mathbb{Z}/n\mathbb{Z})^\times$ ima upravo $\phi(n)$ elemenata. ■

Lema 4.2.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathscr{K}_{\geq 5})[11^\infty] = \{0\}.$$

Dokaz. Najprije, koristeći korolar 3.1.6, zaključujemo da $E(\mathscr{K}_{\geq 5})$ ne sadrži točku reda 121, stoga preostaje dokazati da je $E(\mathscr{K}_{\geq 5})[11] = \{0\}$. Pretpostavimo da je $P \in E(\mathscr{K}_{\geq 5})$ točka reda 11. Iskoristimo li teorem 3.1.7 skupa s činjenicom da je $\mathbb{Q} \subseteq \mathbb{Q}(P) \subseteq \mathscr{K}_{\geq 5}$, zaključujemo da je $[\mathbb{Q}(P) : \mathbb{Q}] \in \{5, 55\}$. Koristeći korolar 4.2.4 zaključujemo da je $[\mathbb{Q}(P) : \mathbb{Q}] = 5$. No, to znači da je $\mathbb{Q}(P) = \mathbb{Q}_{1,5}$ te dokaz dovršavamo analogno dokazu leme 3.3.3. ■

4.3. DOKAZ TEOREMA 4.1.2

Ovdje ćemo imati nešto više posla. Naime, "igra" sa stupnjevima proširenja kao u dokazu prethodnog teorema 4.1.1 nam ovdje ne pomaže pošto međupolja $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathscr{K}$ koja su konačnog stupnja nad $\mathbb{Q}$, mogu biti proizvoljnog stupnja.

Najprije ćemo, radi potpunosti, navesti glavni rezultat iz članka [5, Theorem 1.2.] čiji je autor Michael Chou:

Teorem 4.3.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja te neka je $\mathbb{Q}^{ab}$ maksimalno Abelovo proširenje od $\mathbb{Q}$. Grupa $E(\mathbb{Q}^{ab})_{\text{tors}}$ je izomorfna nekoj od idućih grupa*

$$\begin{aligned}
\mathbb{Z}/N_1\mathbb{Z}, &\qquad N_1 = 1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163,\\
\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2N_2\mathbb{Z}, &\qquad N_2 = 1,2,3,4,5,6,7,8,9,\\
\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3N_3\mathbb{Z}, &\qquad N_3 = 1,3,\\
\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4N_4\mathbb{Z}, &\qquad N_4 = 1,2,3,4,\\
\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}, &\\
\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}, &\\
\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}. &
\end{aligned}$$

Za svaku grupu G s gornje liste, postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $E(\mathbb{Q}^{ab})_{\text{tors}} \simeq G$.

Primijetimo da za polje $\mathscr{K}$ vrijedi analogon korolara 3.1.2, tj. znamo da $E(\mathscr{K})$ ne sadrži punu $\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$ torziju, ni za koji prirodni broj $n > 2$. Koristeći tu činjenicu skupa s činjenicom da je $\mathscr{K} \subseteq \mathbb{Q}^{\text{ab}}$ i gornji teorem 4.3.1, zaključujemo da je grupa $E(\mathscr{K})_{\text{tors}}$ izomorfna nekoj od idućih grupa

$$\begin{aligned}
\mathbb{Z}/n\mathbb{Z}, &\quad 1 \leq n \leq 19 \text{ ili } n \in \{21,25,27,37,43,67,163\},\\
\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2n\mathbb{Z}, &\quad 1 \leq n \leq 9.
\end{aligned}$$

Sada vidimo da, kako bismo dokazali teorem 4.1.2, moramo pokazati da $E(\mathscr{K})_{\text{tors}}$ ne sadrži točke reda

$$11,\ 14,\ 15,\ 16,\ 17,\ 18,\ 19,\ 25,\ 37,\ 43,\ 67,\ 163$$

te da ako $E(\mathscr{K})_{\text{tors}}$ sadrži točku reda 10, odnosno točku reda 12, da je $E(\mathscr{K})_{\text{tors}} \simeq \mathbb{Z}/10\mathbb{Z}$, odnosno $E(\mathscr{K})_{\text{tors}} \simeq \mathbb{Z}/12\mathbb{Z}$. To i dokazujemo sljedećim lemama. Na kraju, u lemi 4.3.10 pokazujemo da postoje $E/\mathbb{Q}$ koje sadrže točku reda 13 definiranu nad poljem $\mathscr{K}$.

Lema 4.3.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $p \in \{11,19,37,43,67,163\}$, tada je*

$$E(\mathscr{K})[p] = \{0\}.$$

Dokaz. Pretpostavimo da je $P \in E(\mathscr{K})$ točka reda p. Koristeći lemu 3.1.4 tada znamo da E ima racionalnu p-izogeniju s jezgrom $\langle P \rangle$. Korolar 4.2.4 nam tada govori da

$$[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(p) = p - 1.$$

Radi rezultata iz članka [36, str 301. Table 4] znamo da ako E ima racionalnu p-izogeniju onda ima samo nekoliko mogućnosti za j-invarijantu od E. Sve te mogućnosti su navedene u idućoj tablici.

p	j-invarijanta	Cremonina oznaka
11	$-11 \cdot 131^3$	121a1
	-2^{15}	121b1
	-11^2	121c1
19	$-2^{15} \cdot 3^3$	361a1
37	$-7 \cdot 11^3$	1225h1
	$-7 \cdot 137^3 \cdot 2083^3$	1225h2
43	$-2^{18} \cdot 3^3 \cdot 5^3$	1849a1
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489a1
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569a1

Tablica 4.1: Primjer eliptičkih krivulja sa zadanom j-invarijantom, [54]

Koristeći programski alat `magma` [2] lako računamo (kôd 12.m) p-ti djelidbeni polinom krivulja iz tablice 4.1. Kako je $[\mathbb{Q}(P) : \mathbb{Q}] \leq p-1$, tražimo ireducibilne faktore tih polinoma koji su stupnja $\leq p-1$ te lako vidimo da oni nemaju nultočaka nad $\mathscr{K}$. Naime, ireducibilni (nad $\mathbb{Q}$) polinom stupnja d sve nultočke ima nad poljem algebarskih brojeva stupnja također d. Međutim, polje stupnja d nad $\mathbb{Q}$ sadržano u $\mathscr{K}$ je jedinstveno i koristeći programski alat `magma` [2] ga jednostavno nalazimo. Preostaje provjeriti da uočeni polinom nema nultočaka nad tim poljem. Time dolazimo do kontradikcije s pretpostavkom da $E(\mathscr{K})$ sadrži točku reda p i dovršavamo dokaz u svim slučajevima osim u slučaju $p = 163$. Naime, u slučajevima $p < 163$ spomenuti algoritam se na računalu izvrši skoro pa trenutačno. U slučaju $p = 163$ moramo biti malo oprezniji. Kao što vidimo u tablici 4.2, jedini ireducibilni faktor 163. djelidbenog polinoma čiji je

stupanj ≤ 162 ima stupanj 81, nazovimo taj polinom φ. Ukoliko pretpostavimo da $E(\mathscr{K})$ sadrži točku reda 163, onda znamo da njena x koordinata mora biti definirana nad poljem stupnja 81, tj. nad $\mathbb{Q}_{4,3}$. No, $\mathbb{Q}_{4,3}/\mathbb{Q}$ je Galoisovo proširenje pa znamo da se φ razlaže na ireducibilne faktore (njih tri stupnja 27) nad poljem $\mathbb{Q}_{1,3} = \mathbb{Q}(\zeta_9)^+$. Međutim, koristeći programski alat `magma` [2] (kôd 13.m) vidimo da to nije istina, tj. polinom φ je ireducibilan i nad poljem $\mathbb{Q}(\zeta_9)^+$, što je kontradikcija. ■

p	Eliptička krivulja	$\deg \psi_p$	ireducibilni faktori stupnja $\leq p-1$
11	121a1	60	jedan stupnja 5
	121b1	60	jedan stupnja 5
	121c1	60	jedan stupnja 5
19	361a1	180	jedan stupnja 9
37	1225h1	684	tri stupnja 6
	1225h2	684	jedan stupnja 18
43	1849a1	924	jedan stupnja 21
67	4489a1	2244	jedan stupnja 33
163	26569a1	13284	jedan stupnja 81

Tablica 4.2: Stupnjevi ireducibilnih faktora stupnja $\leq p-1$

Prije dokaza iduće leme, navedimo jedan tehnički rezultat [17, Proposition 4.6].

Propozicija 4.3.3. *Neka je E eliptička krivulja nad poljem algebarskih brojeva $\mathbb{F}$. Neka je p prost broj te $n \in \mathbb{N}$ i $P \in E(\overline{\mathbb{F}})$ točka reda p^{n+1}. Tada $[\mathbb{F}(P) : \mathbb{F}(pP)]$ dijeli p^2 ili $(p-1)p$.*

Lema 4.3.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada $E(\mathscr{K})$ ne sadrži točku reda 16.*

Dokaz. Pretpostavimo da je $P \in E(\mathscr{K})$ točka reda 16. Iz leme 3.1.4 zaključujemo da E ima racionalnu 2-izogeniju. Naime, iz svega što nam je do sada poznato znamo da je $E(\mathscr{K})_{\text{tors}}$ izomorfna podgrupi od $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$. Dakle, E uistinu ima racionalnu 2-izogeniju. Koristeći [51, Theorem 4] zaključujemo da je

$$[\mathbb{Q}(E[2]) : \mathbb{Q}] = |G_{E,\mathbb{Q}}(2)| \leq |B(2)| = 2.$$

Točka $8P$ je točka reda 2 pa je radi upravo pokazanog $[\mathbb{Q}(8P) : \mathbb{Q}] \in \{1,2\}$. Sada koristimo propoziciju 4.3.3 i dobivamo

$$[\mathbb{Q}(P) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(P) : \mathbb{Q}(2P)]}_{\in\{1,2,4\}} \underbrace{[\mathbb{Q}(2P) : \mathbb{Q}(4P)]}_{\in\{1,2,4\}} \underbrace{[\mathbb{Q}(4P) : \mathbb{Q}(8P)]}_{\in\{1,2,4\}} \underbrace{[\mathbb{Q}(8P) : \mathbb{Q}]}_{\in\{1,2\}},$$

tj. $[\mathbb{Q}(P):\mathbb{Q}]$ je potencija broja 2, što znači da je točka P definirana nad $\mathbb{Q}_{\infty,2}$, a to je kontradikcija s teoremom 3.2.3. ■

Lema 4.3.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada $E(\mathscr{K})$ ne sadrži točku reda $n \in \{15,17\}$.*

Dokaz. Pretpostavimo da je $P \in E(\mathscr{K})$ točka reda n. Znamo da tada E ima racionalnu n-izogeniju (lema 3.1.4). Koristeći korolar 4.2.4 zaključujemo da

$$[\mathbb{Q}(P):\mathbb{Q}] \mid \phi(n).$$

Međutim, znamo da je $\phi(15) = 8$ i $\phi(17) = 16$, što znači da je točka P definirana nad $\mathbb{Q}_{\infty,2}$, što je kontradikcija s teoremom 3.2.3. ■

Lema 4.3.6. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada $E(\mathscr{K})$ ne sadrži točku reda $n \in \{14,18\}$.*

Dokaz. Primijetimo da je $n = 2k$, gdje je $k \in \{7,9\}$. Pretpostavimo li da $E(\mathscr{K})$ sadrži točku reda n, zaključujemo da $E(\mathscr{K})$ sadrži točku reda k, označimo tu točku s P_k. Koristeći lemu 3.1.4, a zatim i korolar 4.2.4 zaključujemo da

$$[\mathbb{Q}(P_k):\mathbb{Q}] \mid \phi(k) = 6.$$

To znači da je P_k definirana nad proširenjem stupnja najviše 6, tj. ta točka je definirana nad poljem $\mathbb{Q}_{1,2}\mathbb{Q}_{1,3}$. Koristeći npr. [43, Corollary 4.] znamo da je

$$E(\mathbb{Q}_{1,2}\mathbb{Q}_{1,3})[k] \simeq E(\mathbb{Q}_{1,3})[k] \oplus E^2(\mathbb{Q}_{1,3})[k],$$

gdje je E^2 kvadratni twist eliptičke krivulje E za 2. Znamo da je E^2 eliptička krivulja definirana također nad $\mathbb{Q}$. Nadalje, znamo da kvadratni twist ne utječe na 2-torziju, a kako je kP točka reda 2, znamo da E i E^2 imaju barem jednu točku reda 2 definiranu nad $\mathbb{Q}_{1,3}$. To znači da postoji eliptička krivulja definirana nad $\mathbb{Q}$ (dakle, E ili E^2) koja nad $\mathbb{Q}_{1,3}$ ima točku reda k i točku reda 2, tj. točku reda $2k$, a to je kontradikcija s teoremom 3.2.2. ■

Lema 4.3.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada $E(\mathscr{K})$ ne sadrži točku reda 25.*

Dokaz. Pretpostavimo da je $P \in E(\mathscr{K})$ točka reda 25. Koristeći lemu 3.1.4 zaključujemo da E ima racionalnu 25-izogeniju, što znači da $\mathrm{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q})$ djeluje na $\langle P\rangle$, odnosno da za svaki $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(E[25])/\mathbb{Q})$ postoji $a \in (\mathbb{Z}/25\mathbb{Z})^\times$ takav da je $P^\sigma = aP$. Koristeći korolar 4.2.4 zaključujemo da $[\mathbb{Q}(P):\mathbb{Q}] \mid \phi(25) = 20$. Nadalje, točka $5P$ je točka reda 5 i za nju na isti način zaključujemo da $[\mathbb{Q}(5P):\mathbb{Q}] \mid \phi(5) = 4$. Dakle, imamo da je

$$\mathbb{Q}(P) \subseteq \mathbb{Q}_{2,2}\mathbb{Q}_{1,5} \qquad \text{i} \qquad \mathbb{Q}(5P) \subseteq \mathbb{Q}_{2,2}.$$

Svaki $\sigma \in \mathrm{Gal}\left(\mathbb{Q}(E[25])/\mathbb{Q}_{2,2}\right)$ fiksira točku $5P$, stoga zaključujemo da je $G_{\mathbb{Q}_{2,2}}(25)$ oblika

$$\left\{ \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} : a \in 1+5\mathbb{Z}/25\mathbb{Z} \right\}.$$

Nadalje, znamo da je $[\mathbb{Q}(\zeta_{25}) : \mathbb{Q}_{1,5}] = 4$, što znači da je $\left|\mathrm{Gal}\left(\mathbb{Q}(\zeta_{25})/\mathbb{Q}_{1,5}\right)\right| = 4$. Sada iz propozicije 1.1.2 zaključujemo da je $\det G_{\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}}(25)$ izomorfno jedinstvenoj podgrupi reda 4 grupe $(\mathbb{Z}/25\mathbb{Z})^\times$, koja je jednaka $\langle 7 \rangle = \{7,-1,-7,1\}$. Sjetimo se još da $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}\right)$ fiksira točku P, stoga je

$$G_{\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}}(25) \leq \left\{ \begin{pmatrix} 1 & * \\ 0 & b \end{pmatrix} : b \in \{7,-1,-7,1\} \right\}.$$

Uočimo da $\mathrm{Gal}\left(\mathbb{Q}(E[25])/\mathbb{Q}_{2,2}\right)$ ne fiksira točku P (teorem 3.2.3) i da je

$$[G_{\mathbb{Q}_{2,2}}(25) : G_{\mathbb{Q}_{2,2}\mathbb{Q}_{1,5}}(25)] = [\mathbb{Q}_{2,2}\mathbb{Q}_{1,5} : \mathbb{Q}_{2,2}] = 5,$$

zato je

$$G_{\mathbb{Q}_{2,2}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in 1+5\mathbb{Z}/25\mathbb{Z},\ b \in \{7,-1,-7,1\} \right\}.$$

Vrijedi $[G_{\mathbb{Q}}(25) : G_{\mathbb{Q}_{2,2}}(25)] = [\mathbb{Q}_{2,2} : \mathbb{Q}] = 4$ te

$$[(\mathbb{Z}/25\mathbb{Z})^\times : 1+5\mathbb{Z}/25\mathbb{Z}] = 4 \qquad \text{i} \qquad [(\mathbb{Z}/25\mathbb{Z})^\times : \langle 7 \rangle] = 5.$$

Iz svega toga zaključujemo da je

$$G_{\mathbb{Q}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in (\mathbb{Z}/25\mathbb{Z})^\times,\ b \in \{7,-1,-7,1\} \right\}.$$

Konačno, računamo

$$25 \mid 150 \mid [\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_{\mathbb{Q}}(25)] \mid [\mathrm{Aut}_{\mathbb{Z}_5}(T_5(E)) : \mathrm{Img}(\rho_{5,E})],$$

što je kontradikcija s teoremom 1.1.3. ■

Lema 4.3.8. *Neka je $E/\mathbb{Q}$ eliptička krivulja takva da $E(\mathscr{K})$ sadrži točku reda 10, onda je*

$$E(\mathscr{K})_{\mathrm{tors}} \simeq \mathbb{Z}/10\mathbb{Z}.$$

Dokaz. Jedina druga mogućnost za $E(\mathscr{K})_{\mathrm{tors}}$ je $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ pa nju moramo eliminirati. Pretpostavimo stoga da je $E(\mathscr{K})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Cijela 2-torzija od E je definirana nad $\mathscr{K}$, što je Galoisovo proširenje od $\mathbb{Q}$, stoga zaključujemo da je $G_{\mathbb{Q}}(2)$ unutar $\mathrm{GL}_2(\mathbb{F}_2)$ konjugirano nekoj od grupa

$$G_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}, G_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}, G_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

U slučaju kada je $G_{\mathbb{Q}}(2) \sim G_1$ ili $G_{\mathbb{Q}}(2) \sim G_2$, odmah zaključujemo da je cijela 2-torzija od E definirana nad kvadratnim proširenjem, tj. nad $\mathbb{Q}_{1,2}$. Nadalje, koristeći lemu 3.1.4 i korolar 4.2.4 zaključujemo da su točke reda 5 na E definirane nad $\mathbb{Q}$, $\mathbb{Q}_{1,2}$ ili nad $\mathbb{Q}_{2,2}$. Dakle, dolazimo do toga da $E(\mathbb{Q}_{\infty,2})_{\mathrm{tors}}$ sadrži $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, što je kontradikcija s teoremom 3.2.3.

Preostaje promotriti slučaj kada je $G_{\mathbb{Q}}(2) \sim G_3$. Koristeći [17, Theorem 3.6.] zaključujemo da E nema kompleksno množenje. Nadalje, koristeći [57, Theorem 1.1.] zaključujemo da postoji racionalan broj u takav da je

$$j(E) = u^2 + 1728.$$

Lema 3.1.4 nam govori da E ima racionalnu 5-izogeniju, što znači da je $G_{\mathbb{Q}}(5)$ unutar $\mathrm{GL}_2(\mathbb{F}_5)$ konjugirano nekoj podgrupi grupe

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_5^{\times}, b \in \mathbb{F}_5 \right\}.$$

Koristeći [57, Theorem 1.4.] zaključujemo da postoji racionalan broj $v \neq 0$ takav da je

$$j(E) = \frac{5^2(v^2+10v+5)^3}{v^5}.$$

Dakle, dobivamo jednadžbu krivulje

$$C \ : \ 25(v^2+10v+5)^3 - u^2v^5 - 1728v^5 = 0.$$

Koristeći programski alat `magma` [2] (kôd 14.m) i kôdove koje su Enrique González-Jiménez i Filip Najman koristili u [17] (pogotovo u dokazu Leme 8.15.) vidimo da je ta krivulja birac-ionalno ekvivalentna eliptičkoj krivulji s Cremoninom oznakom 20a3. Kao što možemo vidjeti na [54], ta krivulja ima samo dvije racionalne točke. Dakle, C ima najviše dvije racionalne točke. Projektivno zatvorenje krivulje C je krivulja

$$x^2y^5 - 25y^6z + 978y^5z^2 - 7875y^4z^3 - 32500y^3z^4 - 39375y^2z^5 - 18750yz^6 - 3125z^7 = 0.$$

To je eliptička krivulja koja nad $\mathbb{Q}$ ima rang jednak 0 i torziju izomorfnu grupi $\mathbb{Z}/2\mathbb{Z}$. Jedine dvije racionalne točke na toj krivulji su $(0:1:0)$ i $(1:0:0)$. Međutim, te točke ne odgovaraju racionalnim točkama na krivulji C (zato što su to točke "u beskonačnosti"), što je kontradikcija.

■

Napomenimo da činjenica da ne postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $G_{\mathbb{Q}}(2) \sim G_3$ i da je $G_{\mathbb{Q}}(5)$ unutar $\mathrm{GL}_2(\mathbb{F}_5)$ konjugirano nekoj podgrupi grupe

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_5^{\times}, b \in \mathbb{F}_5 \right\}$$

slijedi i iz rezultata [39, Theorem C - (1)]. Međutim, onda bismo se još posebno morali pozabaviti eliptičkim krivuljama $E/\mathbb{Q}$ koje imaju kompleksno množenje.

Lema 4.3.9. *Neka je $E/\mathbb{Q}$ eliptička krivulja takva da $E(\mathscr{K})$ sadrži točku reda 12, onda je*

$$E(\mathscr{K})_{\text{tors}} \simeq \mathbb{Z}/12\mathbb{Z}.$$

Dokaz. Jedina druga mogućnost za $E(\mathscr{K})_{\text{tors}}$ je $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ pa nju moramo eliminirati. Pretpostavimo stoga da je $E(\mathscr{K})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

Iz leme 3.1.4 znamo da E ima racionalnu 2-izogeniju, a to znači da je $G_{\mathbb{Q}}(2) \sim G_1$ ili je $G_{\mathbb{Q}}(2) \sim G_2$ unutar $\mathrm{GL}_2(\mathbb{F}_2)$ (ovdje su G_1 i G_2 kao u dokazu prethodne leme 4.3.8). Zaključujemo stoga da je cijela 2-torzija definirana nad $\mathbb{Q}_{\infty,2}$.

Opet, radi leme 3.1.4 znamo da E ima racionalnu 3-izogeniju, što znači da je točka reda 3 definirana nad proširenjem stupnja najviše 2, tj. definirana je nad poljem $\mathbb{Q}_{\infty,2}$. Koristeći propoziciju 4.3.3 zaključujemo i da je točka reda 4 definirana nad $\mathbb{Q}_{\infty,2}$.

Dakle, dolazimo do toga da je $E(\mathbb{Q}_{\infty,2})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, što je kontradikcija s teoremom 3.2.3. ■

Lema 4.3.10. *Postoje eliptičke krivulje $E/\mathbb{Q}$ takve da je*

$$E(\mathbb{Q})_{tors} = \{0\} \qquad i \qquad E(\mathscr{K})_{tors} \simeq \mathbb{Z}/13\mathbb{Z}.$$

Dokaz. Pretpostavimo da je $P \in E(\mathscr{K})$ točka reda 13. Znamo da $P \notin E(\mathbb{Q})$, također znamo da je tada $E(\mathscr{K})_{\text{tors}} \simeq \mathbb{Z}/13\mathbb{Z}$, što vidimo iz [5, Theorem 1.2.]. Dakle, ukoliko nađemo $E/\mathbb{Q}$ koja ima točku reda 13 nad poljem $\mathscr{K}$ — gotovi smo. To upravo i činimo koristeći programski alat `magma` [2] (kôd 15.m). Nalazimo da u bazi [54] postoje dvije eliptičke krivulje definirane nad $\mathbb{Q}$ s ovim svojstvom, to su:

$$\begin{aligned} &20736\text{c}1 : \quad y^2 = x^3 + 6x + 8, \\ &20736\text{d}1 : \quad y^2 = x^3 + 24x + 64. \end{aligned}$$ ■

Napomena. *Modularna krivulja $X_1(13)$ je hipereliptička krivulja genusa 2 (pogledati npr. 169.a.169.1). Nadalje, ako neka eliptička krivulja $E/\mathbb{Q}$ ima točku P reda 13 definiranu nad poljem $\mathscr{K}$, onda znamo da ta eliptička krivulja ima racionalnu 13-izogeniju čiju jezgru generira točka P. No, koristeći korolar 4.2.4 to znači da je $[\mathbb{Q}(P):\mathbb{Q}] \mid \phi(13) = 12$. Dakle, točka P je sigurno definirana nad poljem $\mathbb{Q}_{2,2}\mathbb{Q}_{1,3}$. Koristeći Faltingsov teorem (pogledati [13]) zaključujemo da $X_1(13)(\mathbb{Q}_{2,2}\mathbb{Q}_{1,3})$ sadrži konačno mnogo točaka. Drugim riječima, postoji samo konačno mnogo eliptičkih krivulja $E/\mathbb{Q}$ koje sadrže točku reda 13 nad poljem $\mathscr{K}$.*

5. TORZIJA NAD $\mathbb{Q}(\mu_{p^\infty})$

U ovom poglavlju proučavamo kako se ponaša torzija eliptičkih krivulja $E/\mathbb{Q}$ nad poljem

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{k=1}^{\infty} \mathbb{Q}(\mu_{p^k}) = \bigcup_{k=1}^{\infty} \mathbb{Q}(\zeta_{p^k}),$$

gdje je ζ_n primitivni n-ti korijen iz 1, p je prost broj te

$$\mu_n = \{\omega \in \mathbb{C} \,:\, \omega^n = 1\}.$$

Sva ova polja su sadržana u maksimalnom Abelovom proširenju od $\mathbb{Q}$:

$$\mathbb{Q}^{\text{ab}} = \prod_{p \text{ prost}} \mathbb{Q}(\mu_{p^\infty}).$$

Koristeći već navedeni teorem [5, Theorem 1.2.] znamo da za eliptičku krivulju $E/\mathbb{Q}$ vrijedi da je, za svaki prost broj p, $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}}$ izomorfno nekoj podgrupi neke od idućih grupa

$$\begin{aligned}
\mathbb{Z}/N_1\mathbb{Z}, &\qquad N_1 = 1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163,\\
\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2N_2\mathbb{Z}, &\qquad N_2 = 1,2,3,4,5,6,7,8,9,\\
\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3N_3\mathbb{Z}, &\qquad N_3 = 1,3,\\
\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4N_4\mathbb{Z}, &\qquad N_4 = 1,2,3,4,\\
\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}, &\\
\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}, &\\
\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}. &
\end{aligned}$$

Ono što je cilj napraviti je odrediti koje su točno grupe uopće moguće za koji prost broj p. Time se i bavimo u narednoj sekciji.

Kako ćemo se često pozivati na ovu listu grupa, označimo s **T** skup svih podgrupa grupa s gornje liste. Često ćemo reći da znamo da se $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}}$ nalazi u **T**, pri tome mislimo da je $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}}$ izomorfno nekoj od grupa iz skupa **T**.

5.1. REZULTATI

Kako bismo proučili torziju eliptičke krivulje $E/\mathbb{Q}$ nad poljem $\mathbb{Q}(\mu_{p^\infty})$, zapravo ne moramo "ići daleko", sljedeći teorem nam upravo to i govori.

Teorem 5.1.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada za prost broj $p \geq 5$ vrijedi*

$$E(\mathbb{Q}(\mu_{p^\infty}))_{tors} = E(\mathbb{Q}(\mu_p))_{tors}.$$

Nadalje je

$$E(\mathbb{Q}(\mu_{3^\infty}))_{tors} = E(\mathbb{Q}(\mu_{3^3}))_{tors} \qquad i \qquad E(\mathbb{Q}(\mu_{2^\infty}))_{tors} = E(\mathbb{Q}(\mu_{2^4}))_{tors}.$$

Napomena. *Gornja situacija je "najbolja moguća". Naime, ako je $E = 27a4$ (Cremonina oznaka s [54]), onda je*

$$E(\mathbb{Q}(\mu_{3^2}))_{tors} = \mathbb{Z}/9\mathbb{Z} \subsetneq \mathbb{Z}/27\mathbb{Z} = E(\mathbb{Q}(\mu_{3^3}))_{tors}.$$

Nadalje, ako je $E = 32a4$ (Cremonina oznaka s [54]), onda je

$$E(\mathbb{Q}(\mu_{2^3}))_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \subsetneq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} = E(\mathbb{Q}(\mu_{2^4}))_{tors}.$$

5.2. DOKAZ TEOREMA 5.1.1

Kako bismo dokazali ovaj teorem, trebat će nam nekoliko poznatih rezultata i nekoliko tehničkih činjenica te stoga najprije to i navodimo. Sam dokaz ovog teorema je sadržan u nizu lema koje slijede.

Najprije, sjetimo se klasičnog Mazurovog (i Kenkuovog) teorema o izogenijama (Teorem 3.1.5, možemo ga naći u [27–30, 37]). Ako eliptička krivulja $E/\mathbb{Q}$ ima racionalnu n-izogeniju, onda n mora biti neki od brojeva iz tablice. Trebat će nam $\phi(n)$ od tih brojeva pa ih stoga i navodimo.

n	2	3	4	5	6	7	8	9	10	$\boxed{11}$	12	13	14	15	16
$\phi(n)$	1	2	2	2^2	2	$2\cdot 3$	2^2	$2\cdot 3$	2^2	$2\cdot 5$	2^2	$2^2\cdot 3$	$2\cdot 3$	2^3	2^3

n	$\boxed{17}$	18	19	21	$\boxed{25}$	27	37	$\boxed{43}$	$\boxed{67}$	$\boxed{163}$
$\phi(n)$	2^4	$2\cdot 3$	$2\cdot 3^2$	$2^2\cdot 3$	$2^2\cdot 5$	$2\cdot 3^2$	$2^2\cdot 3^2$	$2\cdot 3\cdot 7$	$2\cdot 3\cdot 11$	$2\cdot 3^4$

Tablica 5.1: Moguće racionalne n-izogenije s vrijednostima $\phi(n)$

Brojevi n koji se nalaze u $\boxed{\ }$ su istaknuti pošto ćemo se sa svakim od njih morati posebno pozabavit. Uskoro će biti jasno zašto.

Promotrimo sada rezultat [15, Theorem 1.1]:

Teorem 5.2.1. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $n \geq 2$ prirodan broj.*

Ako je $\mathbb{Q}(E[n]) = \mathbb{Q}(\mu_n)$, onda je $n \in \{2,3,4,5\}$. Nadalje, ako je proširenje $\mathbb{Q}(E[n])/\mathbb{Q}$ Abelovo, onda je $n \in \{2,3,4,5,6,8\}$ te vrijedi da je grupa $G = \mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})$ izomorfna nekoj od idućih grupa:

n	2	3	4	5	6	8
G	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

Sjetimo se da za prost broj $p \geq 3$ i prirodni broj k vrijedi da je

$$\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^k})/\mathbb{Q}\right) \simeq \mathbb{Z}/(p-1)p^{k-1}\mathbb{Z}. \tag{gal}$$

Koristeći tu činjenicu direktno dobivamo sljedeći korolar.

Korolar 5.2.2. *Neka je $E/\mathbb{Q}$ eliptička krivulja. Neka je $p \geq 3$ prost broj i neka je $n \geq 2$ prirodni broj. Ako je $\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{p^\infty})$, onda je $n \in \{2,3,4,5\}$ te vrijedi da je grupa $G = \mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})$ izomorfna nekoj od idućih grupa:*

n	2	3	4	5
G	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$

Dokaz. Kako je $\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{p^\infty})$ zaključujemo da je proširenje $\mathbb{Q}(E[n])/\mathbb{Q}$ Abelovo. Koristeći prethodni teorem 5.2.1 skupa s opservacijom za $\mathrm{Gal}\left(\mathbb{Q}(\mu_{p^k})/\mathbb{Q}\right)$, (gal) dokaz je gotov. ■

Sada direktno slijedi i sljedeći korolar.

Korolar 5.2.3. *Neka je $E/\mathbb{Q}$ eliptička krivulja, neka je $p \geq 3$ prost broj i neka je $n \geq 2$ prirodan broj. Ako je $\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{p^\infty})$, onda je $n \in \{2,3,4,5\}$ te vrijedi*

$$\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{3^2}),\ \text{za } p = 3 \quad i \quad \mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_p),\ \text{za } p \geq 5.$$

Nadalje, sjetimo se također da vrijedi sljedeće:

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_2)/\mathbb{Q}) \simeq \{0\}, \quad \mathrm{Gal}\,(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{te} \quad \mathrm{Gal}\,(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z},$$

za svaki prirodni broj $k > 2$. Koristeći teorem 5.2.1 odmah dobivamo korolar:

Korolar 5.2.4. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $n \geq 2$ prirodni broj. Ako je $\mathbb{Q}(E[n]) \subseteq \mathbb{Q}(\mu_{2^\infty})$, onda je $n \in \{2,3,4,5,6\}$ te vrijedi da je grupa $G = \mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})$ izomorfna nekoj od idućih grupa:*

n	2	3	4	5	6
G	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$(\mathbb{Z}/2\mathbb{Z})^2$

Iduća propozicija je rezultat iz [17, Proposition 4.8], tu propoziciju koristimo kako bismo se preciznije pozabavili s 2-torzijom.

Propozicija 5.2.5. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $P \in E(\overline{\mathbb{Q}})$ točka reda 2^{n+1}, za neki prirodan broj n. Tada*

$$[\mathbb{Q}(P) : \mathbb{Q}(2P)] \mid 4.$$

Nadalje, vrijedi da je $\mathrm{Gal}\,(\mathbb{Q}(P)/\mathbb{Q}(2P))$ *izomorfno nekoj od iduće* 3 *grupe:*

$$\{0\}, \qquad \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \qquad D_4,$$

gdje je D_4 diedralna grupa reda 8.

Korolar 5.2.6. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $P \in E(\mathbb{Q}(\mu_{p^\infty}))$ točka reda 2^n, za neki prirodan broj n i prost broj $p \geq 3$. Tada je*

$$\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^3}), \text{ za } p = 3 \quad i \quad \mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_p), \text{ za } p \geq 5.$$

Dokaz. Točka $2^{n-1}P$ je točka reda 2 pa znamo da je $[\mathbb{Q}(2^{n-1}P) : \mathbb{Q}] \in \{1,2,3\}$. Iterativnom primjenom propozicije 5.2.5 zaključujemo da je $[\mathbb{Q}(P) : \mathbb{Q}(2^{n-1}P)] = 2^a$, za neki $a \in \{0,1,2,\ldots,2n-2\}$, iz čega slijedi da je $[\mathbb{Q}(P) : \mathbb{Q}] = 2^a 3^b$, za neke $a \in \{0,1,2,\ldots,2n-1\}$, $b \in \{0,1\}$, čime je tvrdnja pokazana. ■

Lema 5.2.7. *Neka je $E/\mathbb{Q}$ eliptička krivulja i neka je $p \geq 13$ prost broj, tada je*

$$E(\mathbb{Q}(\mu_{p^\infty}))_{tors} = E(\mathbb{Q}(\mu_p))_{tors}.$$

Dokaz. Neka je najprije q prost broj različit od 2 i od p. Znamo da $\mathbb{Q}(\mu_{p^\infty})$ ne sadrži ζ_q pa iz propozicije 3.1.1 zaključujemo da $E(\mathbb{Q}(\mu_{p^\infty}))$ ne sadrži $E[q]$. Pretpostavimo da je n prirodan broj takav da $E(\mathbb{Q}(\mu_{p^\infty}))$ sadrži točku P koja je reda q^n, lema 3.1.4 nam tada govori da E ima racionalnu q^n-izogeniju. Iz korolara 4.2.4 zaključujemo da $[\mathbb{Q}(P) : \mathbb{Q}] \mid \phi(q^n)$. Pogledamo li u tablicu 5.1 vidimo da mora biti $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_p)$.

Ukoliko je $q = 2$, iz korolara 5.2.6 zaključujemo da su točke reda 2^n iz $E(\mathbb{Q}(\mu_{p^\infty}))_{\text{tors}}$ definirane nad $\mathbb{Q}(\mu_p)$. Na kraju, iz korolara 5.2.3 zaključujemo da $E(\mathbb{Q}(\mu_{p^\infty}))$ ne sadrži $E[p]$ pa za točku $P \in E(\mathbb{Q}(\mu_{p^\infty}))$ reda p^n vrijede isti argumenti kao za točku reda q^n. ■

Napomena. *U sljedećim lemama koje će rješavati slučajeve $p = 11$, $p = 7$, $p = 5$ i $p = 3$ ćemo provoditi suštinski isti postupak kao za $p = 13$. Dodatne "probleme" će stvarati istaknuti brojevi iz tablice 5.1. Njima ćemo se posebno pozabaviti.*

Lema 5.2.8. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}(\mu_{11^\infty}))_{tors} = E(\mathbb{Q}(\mu_{11}))_{tors}.$$

Dokaz. Primijetimo da ovdje vrijede potpuno analogni argumenti kao u dokazu prethodne leme 5.2.7, uz iznimku potencijalne točke $P \in E(\mathbb{Q}(\mu_{11^\infty}))$ koja je reda 67 (pogledati tablicu 5.1). U tom slučaju E ima racionalnu 67-izogeniju (pogledati skup **T** sa stranice 69), što znači da je (rezultati iz članka [36, str. 301, Table 4.]) $j(E) = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$. Iz dokaza leme 4.3.2 znamo da 67. djelidbeni polinom eliptičkih krivulja $E/\mathbb{Q}$ s ovom j-invarijantom ima jedan ireducibilni faktor stupnja ≤ 66 i taj faktor je stupnja 33, nazovimo ga φ. Međutim, polje $\mathbb{Q}(\mu_{11^\infty})$ ne sadrži potpolje stupnja 33 pa φ sigurno nema nultočaka nad tim poljem, čime smo gotovi. ■

Lema 5.2.9. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}(\mu_{7^\infty}))_{tors} = E(\mathbb{Q}(\mu_7))_{tors}.$$

Dokaz. Jedini potencijalni problem (svi ostali argumenti opet idu analogno) je postojanje točke $P \in E(\mathbb{Q}(\mu_{7^\infty}))$ koja je reda 43 (pogledati tablicu 5.1). U tom slučaju E ima racionalnu 43-izogeniju (pogledati skup **T** sa stranice 69), što znači da je (rezultati iz članka [36, str. 301, Table 4.]) $j(E) = -2^{18} \cdot 3^3 \cdot 5^3$. Iz dokaza leme 4.3.2 znamo da 43. djelidbeni polinom eliptičkih krivulja $E/\mathbb{Q}$ s ovom j-invarijantom ima jedan ireducibilni faktor stupnja ≤ 42 i taj faktor je stupnja 21, nazovimo ga φ. Međutim, polje $\mathbb{Q}(\mu_{7^\infty})$ ne sadrži potpolje stupnja 21 pa φ sigurno nema nultočaka nad tim poljem, čime smo gotovi. ■

Lema 5.2.10. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}(\mu_{5^\infty}))_{tors} = E(\mathbb{Q}(\mu_5))_{tors}.$$

Dokaz. Ovdje se potencijalno pojavljuje nekoliko problema. Prvi je mogućnost pojavljivanja $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ torzije. No, to je riješeno korolarom 5.2.3. Promotrimo skup **T** sa stranice 69 i vidimo da ako $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}} \supseteq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, da je onda $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. Nadalje, kao što vidimo u tablici 5.1 postoje još dva potencijalna problema, to su točke reda 11 i 25. Ako $E(\mathbb{Q}(\mu_{5^\infty}))$ sadrži točku reda 11, onda je cijela torzija $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}}$ jednaka upravo $\mathbb{Z}/11\mathbb{Z}$ (pogledati skup **T** sa stranice 69) pa E ima racionalnu 11-izogeniju. Pogledamo li tablicu 4.2 vidimo da 11. djelidbeni polinom eliptičkih krivulja $E/\mathbb{Q}$ koje imaju racionalnu 11-izogeniju uvijek ima samo jedan ireducibilni faktor stupnja ≤ 10 i taj faktor je stupnja 5. Međutim, u dokazu leme 4.3.2 smo pokazali da niti jedan od tih faktora stupnja 5 nema nultočaka nad jedinstvenim potpoljem polja $\mathbb{Q}(\mu_{5^\infty})$ stupnja 5 nad $\mathbb{Q}$, tj. nad poljem $\mathbb{Q}_{1,5}$. Preostaje nam riješiti točku reda 25. Pretpostavimo da je $P \in E(\mathbb{Q}(\mu_{5^\infty}))$ točka reda 25, vidimo da je u tom slučaju jedina mogućnost da je $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}} \simeq \mathbb{Z}/25\mathbb{Z}$ (skup **T** sa stranice 69) pa znamo da E ima

racionalnu 25-izogeniju. To pak znači da je $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{25})$. Pretpostavimo da $\mathbb{Q}(P) \nsubseteq \mathbb{Q}(\mu_5)$, u suprotnom smo gotovi. Analognim razmišljanjem zaključujemo da je $\mathbb{Q}(5P) \subseteq \mathbb{Q}(\mu_5)$ (imajući na umu da je $E(\mathbb{Q}(\mu_{5^\infty}))_{\text{tors}} \simeq \mathbb{Z}/25\mathbb{Z}$). Svaki $\sigma \in \text{Gal}\left(\mathbb{Q}(E[25])/\mathbb{Q}(\mu_5)\right)$ fiksira točku $5P$, stoga zaključujemo da je $G_{\mathbb{Q}(\mu_5)}(25)$ oblika

$$\left\{ \begin{pmatrix} a & * \\ 0 & * \end{pmatrix} : a \in 1+5\mathbb{Z}/25\mathbb{Z} \right\}.$$

Koristeći propoziciju 1.1.2 zaključujemo da je $\det G_{\mathbb{Q}(\mu_{25})}(25) \simeq \{1\}$. Sjetimo se još da grupa $\text{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{25})\right)$ fiksira točku P, stoga je

$$G_{\mathbb{Q}(\mu_{25})}(25) \leq \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}.$$

Uočimo da $\text{Gal}\left(\mathbb{Q}(E[25])/\mathbb{Q}(\mu_5)\right)$ ne fiksira točku P (pretpostavka) i da je

$$[G_{\mathbb{Q}(\mu_5)}(25) : G_{\mathbb{Q}(\mu_{25})}(25)] = [\mathbb{Q}(\mu_{25}) : \mathbb{Q}(\mu_5)] = 5,$$

zato je

$$G_{\mathbb{Q}(\mu_5)}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & 1 \end{pmatrix} : a \in 1+5\mathbb{Z}/25\mathbb{Z} \right\}.$$

Vrijedi $[G_{\mathbb{Q}}(25) : G_{\mathbb{Q}(\mu_5)}(25)] = [\mathbb{Q}(\mu_5) : \mathbb{Q}] = 4$ te

$$[(\mathbb{Z}/25\mathbb{Z})^\times : 1+5\mathbb{Z}/25\mathbb{Z}] = 4 \qquad \text{i} \qquad [\langle 7 \rangle : \{1\}] = 4.$$

Iz svega toga zaključujemo da je

$$G_{\mathbb{Q}}(25) \leq \left\{ \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} : a \in (\mathbb{Z}/25\mathbb{Z})^\times,\ b \in \{7,-1,-7,1\} \right\}.$$

Konačno, računamo

$$25 \mid 150 \mid [\text{GL}_2(\mathbb{Z}/25\mathbb{Z}) : G_{\mathbb{Q}}(25)] \mid [\text{Aut}_{\mathbb{Z}_5}(T_5(E)) : \text{Img}(\rho_{5,E})],$$

što je kontradikcija s teoremom 1.1.3. ■

Lema 5.2.11. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}(\mu_{3^\infty}))_{tors} = E(\mathbb{Q}(\mu_{3^3}))_{tors}.$$

Dokaz. Ako je $q \neq 3$ prost broj i n prirodan broj takvi da $E(\mathbb{Q}(\mu_{3^\infty}))$ sadrži točku P reda q^n, onda potpuno analogno kao i u dokazima prethodnih lema znamo da je $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^3})$, osim eventualno u slučaju $q = 163$ i $n = 1$ (pogledati tablicu 5.1). Pretpostavimo stoga da je $P \in E(\mathbb{Q}(\mu_{3^\infty}))$ točka reda 163. Znamo da je tada jedina mogućnost da je $E(\mathbb{Q}(\mu_{3^\infty}))_{\text{tors}} \simeq \mathbb{Z}/163\mathbb{Z}$, a to znači da E ima racionalnu 163-izogeniju. Što nadalje znači da je nužno $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{3^5})$ jer iz korolara 4.2.4 slijedi da $[\mathbb{Q}(P) : \mathbb{Q}] \mid 162$. Pogledamo li dokaz leme 4.3.2, tj. tablicu 4.2 vidimo da 163. djelidbeni polinom od E ima samo jedan faktor stupnja ≤ 162 i taj faktor ima stupanj 81, nazovimo ga φ. To znači da polinom φ ima nultočke u polju $\mathbb{Q}(\mu_{3^5})$. Preciznije, mora imati nultočke u polju stupnja 81 nad $\mathbb{Q}$ koje je sadržano u $\mathbb{Q}(\mu_{3^5})$, takvo polje je jedinstveno i to je upravo $\mathbb{Q}_{4,3}$. No, upravo u dokazu leme 4.3.2 smo pokazali da to nije istina čime dolazimo do kontradikcije i zaključka da $E(\mathbb{Q}(\mu_{3^\infty}))$ ne može sadržavati točku reda 163.

Preostaje vidjeti što je s točkama reda 3^n. Proučimo li skup **T** sa stranice 69 vidimo da je $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty]$ izomorfno točno jednoj od sljedećih grupa:

$$\mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/9\mathbb{Z}, \quad \mathbb{Z}/27\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.$$

Ukoliko je $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty] \simeq \mathbb{Z}/3^n\mathbb{Z}$, za neki $n \in \{1,2,3\}$, onda znamo da E ima racionalnu 3^n-izogeniju pa tvrdnja odmah slijedi pogledamo li tablicu 5.1.

Slučaj kada je $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ je riješen korolarom 5.2.3.

Preostaje nam promotriti situaciju kada je $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$. Neka je P točka reda 3 i neka je Q točka reda 9 te neka je $\{P,Q\}$ baza za $E(\mathbb{Q}(\mu_{3^\infty}))[3^\infty]$. Iz teorema 5.2.1 znamo da je $\mathbb{Q}(P) = \mathbb{Q}(3Q) = \mathbb{Q}(\mu_3)$. Koristeći propoziciju 3.1.13 zaključujemo da je

$$[\mathbb{Q}(Q) : \mathbb{Q}(3Q)] \in \{1,2,3,6,9\},$$

čime smo pokazali da je nužno $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\mu_{3^3})$. ■

Prije samog dokaza činjenice da je $E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}$, navodimo dva tehnička rezultata koja su nam potrebna.

Lema 5.2.12. *Neka je $E/\mathbb{Q}$ eliptička krivulja takva da $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, tada*

$$E(\mathbb{Q}(\mu_{2^4}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Dokaz. Neka su P i Q točke na $E(\mathbb{Q}(\mu_{2^\infty}))$ koje čine bazu za $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ te neka je P točka reda 4 i Q točka reda 8. Trebamo pokazati da je $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\zeta_{2^4})$. Iz korolara 5.2.4 zaključujemo da je $\mathbb{Q}(P,2Q) \subseteq \mathbb{Q}(\zeta_{2^3})$, a zatim primjenom propozicije 5.2.5

vidimo da je $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\zeta_{25})$. M. Derickx i A. V. Sutherland su u [11] izložili metodu za pronalazak modela za neke modularne krivulje $X_1(m,mn)$. Kompletna lista nalazi se na `http://math.mit.edu/~drew/X1mn.html`. Nalazimo da je $X_1(4,8)$ zapravo eliptička krivulja 32a2 (podaci s [54]):

$$E' \ : \ y^2 = x^3 - x.$$

Pokažimo da je $\mathrm{rk}(E'(\mathbb{Q}(\mu_{2^5}))) = \mathrm{rk}(E'(\mathbb{Q}(\mu_{2^4}))) = 0$ i da je $E'(\mathbb{Q}(\mu_{2^5}))_{\mathrm{tors}} = E'(\mathbb{Q}(\mu_{2^4}))_{\mathrm{tors}}$. To i radimo koristeći programski alat `magma` [2] (kôd 16.m). Iskoristimo li činjenicu da je (pogledati stranicu 19)

$$\mathrm{rk}(E'(\mathbb{Q}(\mu_{2^5}))) = \mathrm{rk}(E'(\mathbb{Q}_{3,2})) + \mathrm{rk}(E'^{(-1)}(\mathbb{Q}_{3,2}))$$

lako računamo da je rang od E' nad $\mathbb{Q}(\mu_{2^5})$ uistinu jednak 0. ■

Većina eliptičkih krivulja E (čak i nad poljem $\mathbb{C}$) zadovoljava da je $\mathrm{End}(E) \simeq \mathbb{Z}$. To znači da su svi endomorfizmi od E jedino množenja s m, gdje je m cijeli broj. Za eliptičku krivulju koja ima endomorfizam koji nije množenje s m za neki cijeli broj m kažemo da ima **kompleksno množenje**. Za detalje svakako pogledati [52, Chapter II].

Lema 5.2.13. *Neka je $E/\mathbb{Q}$ eliptička krivulja koja ima kompleksno množenje. Tada E ne sadrži točku reda* 16 *definiranu nad* $(\mathbb{Q}(\mu_{2^\infty}))$.

Dokaz. Pretpostavimo da $E(\mathbb{Q}(\mu_{2^\infty}))$ sadrži točku P reda 16, pogledamo li skup **T** sa stranice 69 vidimo da je tada $E(\mathbb{Q}(\mu_{2^\infty}))_{\mathrm{tors}}$ izomorfno nekoj od grupa

$$\mathbb{Z}/16\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

U slučaju grupe $\mathbb{Z}/16\mathbb{Z}$, pogledamo li tablicu 5.1 vidimo da je $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^4})$. U slučaju grupe $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, znamo da je točka $2P$ generator jezgre racionalne 8-izogenije pa je $\mathbb{Q}(2P) \subseteq \mathbb{Q}(\mu_{2^3})$. Koristeći propoziciju 5.2.5 zaključujemo da je tada $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^5})$. Konačno, ako je u pitanju grupa $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, onda je $4P$ generator jezgre 4-izogenije pa je $\mathbb{Q}(4P) \subseteq \mathbb{Q}(\mu_{2^2})$ i onda posljedično $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^6})$. Odnosno, u svakom slučaju je točka reda 16 definirana nad poljem $\mathbb{Q}(\mu_{2^6})$.

E ima kompleksno množenje pa je j-invarijanta od E jednaka jednom od idućih 13 brojeva (tu činjenicu možemo naći u [52, Appendix A §3][1]):

$$-262537412640768000, \ -147197952000, \ -884736000, \ -12288000, \ -884736,$$

[1] može se pogledati i na `https://wstein.org/`, tj. u tablicu `https://wstein.org/Tables/cmj.html`

$$-32768,\ -3375,\ 0,\ 1728,\ 8000,\ 54000,\ 287496,\ 16581375.$$

Sada koristeći programski alat `magma` [2] (kôd 17.m) nalazimo da za eliptičke krivulje s tim j-invarijantama, polinom $\frac{\psi_{16}}{\psi_8}$ (ovdje je, kao i uvijek, n-ti djelidbeni polinom od E označen s ψ_n) nema nultočaka nad poljem $\mathbb{Q}(\mu_{2^6})$, čime dokaz privodimo kraju. ■

Lema 5.2.14. *Neka je $E/\mathbb{Q}$ eliptička krivulja takva da je $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$. Tada je*

$$E(\mathbb{Q}(\mu_{2^4}))[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

Dokaz. Neka su P i Q točke na $E(\mathbb{Q}(\mu_{2^\infty}))$ koje čine bazu za $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ torziju i neka je P točka reda 2 te Q točka reda 16. Trebamo pokazati da je $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\zeta_{2^4})$. Pogledamo li dokaz leme 3.1.4 (točnije, dokaz od [9, Lemma 4.6]) vidimo da je točka $2Q$ generator jezgre racionalne 8-izogenije, što znači da je točka $2Q$ definirana nad poljem stupnja najviše 4 nad $\mathbb{Q}$. Sada koristeći propoziciju 5.2.5 vidimo da je točka Q definirana nad proširenjem stupnja najviše 16 nad $\mathbb{Q}$. Dakle, vidimo da je nužno $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\zeta_{2^5})$. Ono što ćemo sada pokazati je sljedeća tvrdnja:

$$\text{Ako je } [\mathbb{Q}(P,Q) : \mathbb{Q}] \geq 16, \text{ onda } \mathbb{Q}(P,Q) \text{ nije sadržano u } \mathbb{Q}(\mu_{2^\infty}).$$

Naime, to onda znači da ako je $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\mu_{2^\infty})$, onda je nužno $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\mu_{2^4})$, što i želimo pokazati.

Iz prethodne leme 5.2.13 slijedi da eliptička krivulja E nema kompleksno množenje. E. González-Jiménez i F. Najman su u dokazu [17, Lemma 8.15.] koristili `magma` [2] kôd[2] koji će i nama ovdje biti od koristi. Naime, za sve moguće 2-adske Galoisove reprezentacije eliptičke krivulje E nalazimo koje su sve mogućnosti za $\mathrm{Gal}\,(\mathbb{Q}(P,Q)/\mathbb{Q})$, uz uvjet da je $[\mathbb{Q}(P,Q) : \mathbb{Q}] \geq 16$. Napomenimo da nam je ključna baza podataka 2primary_Ss.txt koju su E. González-Jiménez i Á. Lozano-Robledo generirali u [16] za potrebe dokaza Corollary 3.3. i Corollary 3.4. Svi popratni `magma` [2] kôdovi dostupni su online[3]. Ta baza je nastala na osnovu baze koju su J. Rouse i D. Zureick-Brown generirali za potrebe članka [48], također se svi popratni `magma` [2] kôdovi mogu naći online[4].

[2] `http://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/growth/lem8_16a.txt`

[3] `http://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/pprimary/pprimary.html`

[4] `http://users.wfu.edu/rouseja/2adic/`

Konačno, koristeći programski alat `magma` [2] (kôd 18.m) nalazimo da za polje $\mathbb{K}$ takvo da je $\mathbb{Q}(P,Q) = \mathbb{K}$ i $[\mathbb{K} : \mathbb{Q}] \geq 16$ vrijedi da je $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}$. Sjetimo se opet činjenice da vrijedi: $\mathrm{Gal}(\mathbb{Q}(\zeta_2)/\mathbb{Q}) \simeq \{0\}$, $\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ te $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{k-2}\mathbb{Z}$, za svaki prirodni broj $k > 2$. To znači da polje $\mathbb{K}$ nije sadržano u $\mathbb{Q}(\mu_{2^\infty})$, čime smo dokaz priveli kraju. ■

Lema 5.2.15. *Neka je $E/\mathbb{Q}$ eliptička krivulja takva da je $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$. Tada je*

$$E(\mathbb{Q}(\mu_{2^4}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}.$$

Dokaz. Provodimo ga analogno kao dokaz prethodne leme 5.2.14, uz minimalne modifikacije.

Ako su P reda 4 i Q reda 16 točke u $E(\mathbb{Q}(\mu_{2^\infty}))$ koje čine bazu za $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ torziju, onda je $4Q$ generator jezgre 4-izogenije pa je $\mathbb{Q}(4Q)$ stupnja najviše 2 nad $\mathbb{Q}$. Iz toga onda zaključujemo da je $\mathbb{Q}(P,Q)$ stupnja najviše 32 nad $\mathbb{Q}$, tj. nužno je $\mathbb{Q}(P,Q) \subseteq \mathbb{Q}(\mu_{2^6})$. Sada opet pokazujemo analognu tvrdnju kao u dokazu leme 5.2.14:

$$\text{Ako je } [\mathbb{Q}(P,Q) : \mathbb{Q}] \geq 16, \text{ onda } \mathbb{Q}(P,Q) \text{ nije sadržano u } \mathbb{Q}(\mu_{2^\infty}).$$

Koristeći analogni `magma` [2] kôd 18.m (jedina bitna razlika je sama torzijska grupa), računamo da ako je $\mathbb{K} = \mathbb{Q}(P,Q)$ i $[\mathbb{K} : \mathbb{Q}] \geq 16$, onda je $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ izomorfno jednoj od grupa

$$(\mathbb{Z}/2\mathbb{Z})^4, \quad (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}, \quad (\mathbb{Z}/2\mathbb{Z})^5, \quad (\mathbb{Z}/2\mathbb{Z})^3 \oplus \mathbb{Z}/4\mathbb{Z}.$$

Zaključujemo da polje $\mathbb{K}$ nije sadržano u $\mathbb{Q}(\mu_{2^\infty})$ čime smo gotovi. ■

Konačno, sljedeća lema dovršava dokaz teorema 5.1.1.

Lema 5.2.16. *Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je*

$$E(\mathbb{Q}(\mu_{2^\infty}))_{tors} = E(\mathbb{Q}(\mu_{2^4}))_{tors}.$$

Dokaz. Ako je $q > 2$ prost broj i n prirodan broj takvi da $E(\mathbb{Q}(\mu_{2^\infty}))$ sadrži točku P reda q^n, onda potpuno analogno kao i u dokazima prethodnih lema znamo da je $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^4})$, osim eventualno u slučaju $q = 17$ i $n = 1$ (pogledati tablicu 5.1). Neka je $P \in E(\mathbb{Q}(\mu_{2^\infty}))$ točka reda 17. Znamo da je tada jedina mogućnost da je $E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} \simeq \mathbb{Z}/17\mathbb{Z}$, a to znači da E ima racionalnu 17-izogeniju. Što nadalje znači da je nužno $\mathbb{Q}(P) \subseteq \mathbb{Q}(\mu_{2^5})$. Pogledamo li u [36, str.

301, Table 4] ili u [52, Appendix A, §3], vidimo da je

$$j(E) = \frac{-17^2 \cdot 101^3}{2}, \quad \text{što je istina za eliptičku krivulju 14450p1}$$

ili

$$j(E) = \frac{-17 \cdot 373^3}{2^{17}}, \quad \text{što je istina za eliptičku krivulju 14450p2.}$$

Sada, za obje uočene j-invarijante, koristeći programski alat `magma` [2] faktoriziramo 17. djelidbeni polinom (kôd 19.m). Preciznije, tražimo mu faktore stupnja ≤ 16. Za obje navedene j-invarijante dobijemo da pripadajući polinomi nemaju nultočaka nad poljem $\mathbb{Q}(\mu_{2^5})$. Dakle, $E(\mathbb{Q}(\mu_{2^\infty}))$ ne može sadržavati točku reda 17.

Preostaje vidjeti što je s točkama reda 2^n. Proučimo li skup **T** sa stranice 69 vidimo da je $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty]$ izomorfno točno jednoj od sljedećih grupa:

$$\begin{aligned}
&\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/16\mathbb{Z},\\
&\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z},\\
&\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z},\\
&\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}.
\end{aligned}$$

Ukoliko je $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/2^n\mathbb{Z}$, za neki $n \in \{1,2,3,4\}$, onda znamo da E ima racionalnu 2^n-izogeniju pa tvrdnja odmah slijedi pogledamo li tablicu 5.1.

Znamo da je $\mathrm{Gal}\,(\mathbb{Q}(\zeta_2)/\mathbb{Q}) \simeq \{0\}$, $\mathrm{Gal}\,(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ te

$$\mathrm{Gal}\,(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2^{k-2}\mathbb{Z},$$

za svaki prirodni broj $k > 2$. Koristeći korolar 5.2.4 sada zaključujemo da je torzija $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$ nemoguća. Nadalje, iz istog korolara zaključujemo da tvrdnja leme vrijedi u slučaju torzije $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, odnosno torzije $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$.

U lemi 5.2.12 je pokazano da ako je $E(\mathbb{Q}(\mu_{2^\infty}))[2^\infty] \simeq \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$, onda je ta torzija definirana nad poljem $\mathbb{Q}(\mu_{2^4})$. Također, ista stvar je pokazana i za torzije $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$ i $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$ u lemama 5.2.14 i 5.2.15.

Preostaje još pitanje torzija $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$. Pretpostavimo da točke P i Q čine bazu te torzije, tj. P je reda 2, a Q je reda $2k$, za $k \in \{2,4\}$. Točka $2Q$ je tada generator jezgre k-izogenije i znamo da je ona definirana nad poljem stupnja najviše 2 nad $\mathbb{Q}$. To znači da je točka Q definirana nad poljem stupnja najviše $2 \cdot 4 = 8$ nad $\mathbb{Q}$, tj. nad poljem $\mathbb{Q}(\mu_{2^4})$. Ovime je dokaz leme, ali i teorema 5.1.1 priveden kraju. ■

5.3. NEKE POSLJEDICE

Neka je $E/\mathbb{Q}$ eliptička krivulja. Poznate su sve mogućnosti za torziju od E nad poljima $\mathbb{Q}(\mu_n)$, za $n \in \{2,3,4,7,8,11\}$. Sve ih navodimo navodimo u tablici 5.2, bez dokaza. Nadalje, za torziju nad $\mathbb{Q}(\mu_5)$ znamo da imamo samo 3 mogućnosti, ali za 2 još nismo sigurni postižu li se.

Sada vidimo da je direktna posljedica teorema 5.1.1 ta da zapravo znamo torziju nad $\mathbb{Q}(\mu_{7^\infty})$ i $\mathbb{Q}(\mu_{11^\infty})$.

Idući korak je pokušati odrediti sve moguće torzije eliptičkih krivulja $E/\mathbb{Q}$ nad poljima $\mathbb{Q}(\mu_{16})$ te $\mathbb{Q}(\mu_9)$, a zatim i nad $\mathbb{Q}(\mu_{27})$ te ćemo time znati torzije nad $\mathbb{Q}(\mu_{2^\infty})$ i nad $\mathbb{Q}(\mu_{3^\infty})$. Također, potrebno je naći primjer ili isključiti preostale dvije torzije u slučaju polja $\mathbb{Q}(\mu_5)$.

I.K. će u suradnji s T. Gužvićem i B. Vukorepom to i pokušati napraviti u skorije vrijeme te rezultate objaviti u [22].

Navedimo sada te već poznate rezultate. Kako je $\mu_2 = \{\pm 1\}$ znamo da $E(\mathbb{Q}(\mu_2))_{\text{tors}}$ može biti samo neka od grupa iz Mazurovog teorema [37, Theorem 2]:

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ ili } n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

Naravno, svaka od tih grupa se postiže. U nastavku nećemo spominjati ove grupe iz Mazurovog teorema već samo one dodatne koje se pojavljuju. Za svaku ćemo navesti i primjer eliptičke krivulje $E/\mathbb{Q}$ za koju se postiže.

- Za $n \in \{3,4\}$ rezultate nalazimo u [40, Theorem 1]. Dovoljno je primijetiti da je $\mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$ te $\mathbb{Q}(\mu_4) = \mathbb{Q}(i)$.
- Rezultat za $n = 5$ nalazimo u [3, Theorem 5]. Napominjemo, za grupe $\mathbb{Z}/15\mathbb{Z}$ i $\mathbb{Z}/16\mathbb{Z}$ znamo da se pojavljuju kod eliptičkih krivulja $E/\mathbb{Q}(\mu_5)$. Preostaje vidjeti postoji li eliptička krivulja $E/\mathbb{Q}$ za koju se pojavljuju te grupe.
- Rezultate za $n \in \{7,8,11\}$ je dokazao Borna Vukorepa i oni će biti objavljeni u [22].

U idućoj tablici 5.2 navodimo sve moguće torzijske grupe nad spomenutim poljima. Naravno, kao što smo napomenuli, ispuštamo grupe iz Mazurovog teorema. Prvi stupac tablice je polje nad kojim promatramo torziju. U drugom stupcu su navedene sve grupe (osim onih iz Mazurovog teorema) koje se mogu pojaviti kao torzija eliptičke krivulje $E/\mathbb{Q}$ nad tim poljem.

U zadnjem (trećem) stupcu dajemo primjer eliptičke krivulje $E/\mathbb{Q}$ koja ima odgovarajuću torziju nad promatranim poljem. Primjere krivulja navodimo s njihovim Cremoninim oznakama s [54]. Simbol **?** označava da još ne znamo postoji li $E/\mathbb{Q}$ s tom torzijom nad promatranim poljem.

polje	torzijska grupa	primjer $E/\mathbb{Q}$
$\mathbb{Q}(\mu_3)$	$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$	27a3
	$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$	14a2
$\mathbb{Q}(\mu_4)$	$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	15a1
$\mathbb{Q}(\mu_5)$	$\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$	550k2
	$\mathbb{Z}/15\mathbb{Z}$	**?**
	$\mathbb{Z}/16\mathbb{Z}$	**?**
$\mathbb{Q}(\mu_7)$	$\mathbb{Z}/13\mathbb{Z}$	147c1
	$\mathbb{Z}/14\mathbb{Z}$	49a4
	$\mathbb{Z}/18\mathbb{Z}$	14a6
	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$	49a1
	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z}$	14a4
$\mathbb{Q}(\mu_8)$	$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	15a1
	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$	2112bd2
$\mathbb{Q}(\mu_{11})$	$\mathbb{Z}/11\mathbb{Z}$	121b1
	$\mathbb{Z}/25\mathbb{Z}$	11a3
	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$	10230bg2

Tablica 5.2: Sve moguće torzije (bez onih iz Mazurovog teorema) od $E/\mathbb{Q}$ nad $\mathbb{Q}(\mu_n)$.

6. KORIŠTENI MAGMA KÔDOVI

U ovom poglavlju navodimo sve magma [2] kôdove koje smo koristili u ovom radu. Koristili smo verziju V2.24-7. Radna stanica je Fujitsu Celsius M770[1] s procesorom Intel® Xeon® W-2133 @ 3.60 GHz[2] i sa 64 GB RAM-a.

1.m ⇝ 3.3.3

Oprez! Naredbi u retku 5 treba neko vrijeme da se izvrši.

```
1  E := EllipticCurve([0, -1, 1, 0, 0]);
2  DescentInformation(E);
3  K := Subfields(CyclotomicField(25),5)[1][1];
4  E1 := BaseChange(E,K);
5  DescentInformation(E1);
```

2.m ⇝ 3.4.2

```
1  E := EllipticCurve("361a1");
2  P := DivisionPolynomial(E,19);
3  K := Subfields(CyclotomicField(27),9)[1][1];
4  HasRoot(P,K);
```

3.m ⇝ 3.4.3

Ovdje ćemo također koristiti pomoćnu funkciju Check iz 5.m.

```
1  Q<x> := PolynomialRing(Rationals());
2  C := HyperellipticCurve(x^6 - 2*x^5 + x^4 - 2*x^3 + 6*x^2 - 4*x + 1);
3  K := Subfields(CyclotomicField(9),3)[1][1];
4  C1 := ChangeRing(C, K);
```

[1] https://www.fujitsu.com/fts/products/computing/pc/workstations/celsius-m770/

[2] https://ark.intel.com/content/www/us/en/ark/products/125040/intel-xeon-w-2133-processor-8-25m-cache-3-60-ghz.html

```
RankBound(Jacobian(C1));
Discriminant(C1);
Factorization(177209344);
O := RingOfIntegers(K);
Factorization(11*O);
AbelianGroup(Jacobian(ChangeRing(C1,GF(11^3))));
Factorization(19*O);
AbelianGroup(Jacobian(ChangeRing(C1,GF(19))));
AbelianGroup(Jacobian(ChangeRing(C,GF(3))));
pts := Points(C1 : Bound := 10);
P1 := pts[1] - pts[4];
P2 := pts[2] - pts[5];
Check(C1, pts, P1, P2);
pts := Points(C : Bound := 10);
P1 := pts[1] - pts[4];
P2 := pts[2] - pts[5];
Check(C, pts, P1, P2);
```

4.m ⇝ 3.4.5

```
Q<x> := PolynomialRing(Rationals());
E := EllipticCurve(x^3 - x, x + 1);
K := Subfields(CyclotomicField(9),3)[1][1];
E := ChangeRing(E, K);
DescentInformation(E);
```

5.m ⇝ 3.4.7

Najprije navodimo pomoćnu funkciju `Check` koju koristimo. Ona za danu hipereliptičku krivulju `C` i skup točaka na njoj `pts` provjerava jesu li to sve točke na `C` (pod uvjetom da znamo da su `pts` sve točke na Jakobijanu od `C`).

```
Check := function(C, pts, P1, P2)
   print #pts;
   S := {};
   for i := 1 to 50 do
      for j := 1 to 50 do
         S := S join {i*P1 + j*P2};
         end for;
      end for;
```

```
9     pts1 := PointsAtInfinity(C);
10    for P in S do
11       p := Roots(P[1]);
12       for i := 1 to #p do
13          pts1 := pts1 join Points(C, p[i][1]);
14          end for;
15       end for;
16    return #S, (pts eq pts1);
17 end function;
```

Iduća je pomoćna funkcija `Find` koja nam nalazi gornju i donju ogradu na torziju Jakobijana krivulje `C` nad poljem `K`. Napomenimo da retci `13` i `14` ovise o samoj krivulji `C`. Tj. moraju se "pogoditi" vrijednosti koje će uspjeti pogoditi sve točke na Jakobijanu. Također, ovu funkciju koristimo samo i isključivo radi manjeg obujma samog kôda pa nas ne smeta ovo "gubljenje općenitosti".

```
1  Find := function(C, K)
2     o := RingOfIntegers(K);
3     q := Degree(K);
4     for p := 5 to 100 do
5        if IsPrime(p) then
6           if #Factorization(p*o) eq q then
7              print AbelianGroup(Jacobian(ChangeRing(C,GF(p))));
8              break;
9              end if;
10          end if;
11       end for;
12    pts := Points(C : Bound := 10);
13    P1 := pts[3] - pts[7];
14    P2 := pts[5] - pts[10];
15    return Check(C, pts, P1, P2);
16 end function;
```

```
1  Q<x> := PolynomialRing(Rationals());
2  C := HyperellipticCurve(x^6 + 2*x^5 + 5*x^4 + 10*x^3 + 10*x^2 + 4*x + 1);
3  K := Subfields(CyclotomicField(9),3)[1][1];
4  C1 := ChangeRing(C, K);
5  RankBound(Jacobian(C1));
6  Find(C1, K);
```

```
pts := PointsAtInfinity(C1);
for p in Roots(x*(x + 1)*(x^2 + x + 1)*(x^3 - 3*x - 1), K) do
   pts := pts join Points(C1,p[1]);
   end for;
#pts;
K := CyclotomicField(3);
Find(ChangeRing(C, K), K);
K := CyclotomicField(9);
Find(ChangeRing(C, K), K);
```

6.m ⇝ Dokaz teorema 3.2.2

```
E := EllipticCurve("27a2");
K := Subfields(CyclotomicField(27),9)[1][1];
f := DivisionPolynomial(E, 27) div DivisionPolynomial(E, 9);
f := Factorization(f : DegreeLimit := 9);
f;
r := Roots(f[1][1], K);
a := r[1][1];
_<y> := PolynomialRing(K);
Norm(Discriminant(y^2 + y - (a^3 - 270*a - 1708)));
Factorization(23929932923061752959008 3);
E1 := QuadraticTwist(E,3);
TorsionSubgroup(ChangeRing(E1,K));
E1 := QuadraticTwist(E,-3);
TorsionSubgroup(ChangeRing(E1,K));
```

7.m ⇝ 3.5.2

```
Q<x> := PolynomialRing(Rationals());
K:=NumberField(x^16-16*x^14+104*x^12-352*x^10+660*x^8-672*x^6+336*x^4-64*x^2+2);
f := function(E, K)
   r := Factorization(DivisionPolynomial(E,17) : DegreeLimit := 16);
   for p in r do if HasRoot(p[1], K) then return true; end if; end for;
   return false;
end function;
f(EllipticCurve("14450p1"), K);
f(EllipticCurve("14450p2"), K);
```

8.m ⇝ 3.5.5

```
1  Q<x> := PolynomialRing(Rationals());
2  E := EllipticCurve(x^3 + x^2, x + 1);
3  K := NumberField(x^4 - 4*x^2 + 2);
4  E := ChangeRing(E, K);
5  DescentInformation(E);
```

9.m ⇝ 3.5.5

```
1  Q<x> := PolynomialRing(Rationals());
2  E := EllipticCurve(x^3 + x^2 - x);
3  K := NumberField(x^2 - 2);
4  E := ChangeRing(E, K);
5  DescentInformation(E);
```

10.m ⇝ 3.6.1

```
1  F<t> := FunctionField(Rationals());
2  a := <0, t, (2*t-1)*(t-1)/t>;
3  b := <t, t^2 + t, (2*t-1)*(t-1)>;
4  for i := 1 to 3 do
5     E := EllipticCurve([1-a[i],-b[i],-b[i],0,0]);
6     g, m := TorsionSubgroup(E);
7     g;
8     Discriminant(E);
9  end for;
10 A<t,s> := AffineSpace(Rationals(),2);
11 a := <16*t + 1, (9*t+1)*(t+1), 2*(t^2 - t + 1/8)>;
12 for i := 1 to 3 do
13    C := ProjectiveClosure(Curve(A,a[i] - 2*s^2));
14    Genus(C);
15    #Points(C : Bound := 100);
16    C := ProjectiveClosure(Curve(A,a[i] + s^2));
17    Genus(C);
18    #Points(C : Bound := 100);
19 end for;
```

11.m ⇝ 3.6.1

```
1  F<t> := FunctionField(Rationals());
2  E := EllipticCurve([0,4/(1-2*t^2),0,4/(1-2*t^2),0]);
```

```
3  TorsionSubgroup(E);
4  Discriminant(E);
```

12.m ⇝ 4.3.2

```
1  Q<x> := PolynomialRing(Rationals());
2  label := <"121a1", "121b1", "121c1", "361a1",
3       "1225h1", "1225h2", "1849a1", "4489a1">;
4  prime := <11, 11, 11, 19, 37, 37, 43, 67>;
5  S := [];
6  for i := 1 to 8 do
7     E := EllipticCurve(label[i]);
8     p := prime[i];
9     T := Factorization(DivisionPolynomial(E,p) : DegreeLimit := p-1);
10    S := Append(S, T);
11    printf "Case E = %o:\n", label[i];
12    for p in S[i] do
13       Degree(p[1]);
14    end for;
15 end for;
16 function f(K, S, label, l, r)
17    for i := l to r do
18       printf "Case E = %o:\n", label[i];
19       for p in S[i] do
20          HasRoot(p[1], K);
21       end for;
22    end for;
23    return "done!";
24 end function;
25 //11
26 K := Subfields(CyclotomicField(25),5)[1][1];
27 f(K, S, label, 1, 3);
28 //19
29 K := Subfields(CyclotomicField(81),9)[1][1];
30 f(K, S, label, 4,4);
31 //37, deg = 6
32 F := Subfields(CyclotomicField(9),3)[1][1];
33 K := Compositum(F, NumberField(x^2 - 2));
34 f(K, S, label, 5, 5);
```

```
35  //37, deg = 18
36  F := Subfields(CyclotomicField(81),9)[1][1];
37  K := Compositum(F, NumberField(x^2 - 2));
38  f(K, S, label, 6, 6);
39  //43
40  F := Subfields(CyclotomicField(49),7)[1][1];
41  K := Subfields(CyclotomicField(9),3)[1][1];
42  K := Compositum(K, F);
43  f(K, S, label, 7, 7);
44  //67
45  F := Subfields(CyclotomicField(121),11)[1][1];
46  K := Subfields(CyclotomicField(9),3)[1][1];
47  K := Compositum(K, F);
48  f(K, S, label, 8, 8);
```

13.m ⇝ 4.3.2

Napomenimo da naredbi u retku 2 treba nešto više od sat vremena kako bi se izvršila.

```
1  E := EllipticCurve("26569a1");
2  S := Factorization(DivisionPolynomial(E,163) : DegreeLimit := 162);
3  for p in S do
4     Degree(p[1]);
5     end for;
6  K := Subfields(CyclotomicField(9),3)[1][1];
7  p := ChangeRing(S[1][1],K);
8  IsIrreducible(p);
```

14.m ⇝ 4.3.8

```
1  A<u, v> := AffineSpace(Rationals(),2);
2  C := ProjectiveClosure(Curve(A,25*(v^2+10*v+5)^3-u^2*v^5-1728*v^5));
3  IsSingular(C);
4  DescentInformation(EllipticCurve(C,SingularPoints(C)[1]));
5  Points(C : Bound := 10);
```

15.m ⇝ 4.3.10

Ovdje je skup `data` iz retka 19 skup svih eliptičkih krivulja definiranih nad $\mathbb{Q}$ s [54] koje dopuštaju 13-izogeniju nad $\mathbb{Q}$.

```
Q<x> := PolynomialRing(Rationals());
K := Subfields(CyclotomicField(9),3)[1][1];
K := Compositum(K, NumberField(x^4 - 4*x^2 + 2));
f := function(K, E)
   p := DivisionPolynomial(E, 13);
   fact := Factorization(p : DegreeLimit := 12);
   E := ChangeRing(E, K);
   for p in fact do
      r := Roots(p[1], K);
      for i in r do
         if #Points(E, i[1]) gt 0 then
            return true;
            end if;
         end for;
      end for;
   return false;
end function;
S := {};
for d in data do
   if f(K, EllipticCurve(d)) then
      S := S join {CremonaReference(EllipticCurve(d))};
   end if;
end for;
S;
```

16.m ⇝ 5.2.12

```
Q<x> := PolynomialRing(Rationals());
K := NumberField(x^8 - 8*x^6 + 20*x^4 - 16*x^2 + 2);
F := CyclotomicField(16);
L := CyclotomicField(32);
E := EllipticCurve("32a2");
TorsionSubgroup(ChangeRing(E,F));
TorsionSubgroup(ChangeRing(E,L));
RankBound(ChangeRing(E,K));
RankBound(ChangeRing(QuadraticTwist(E,-1),K));
```

17.m ⇝ 5.2.13

```
Q<x> := PolynomialRing(Rationals());
```

```
J := [0, 54000, -12288000, 1728, 287496, -3375, 16581375, 8000, -32768,
   -884736, -884736000, -147197952000, -262537412640768000];
K := CyclotomicField(64);
for j in J do
   E := EllipticCurveWithjInvariant(j);
   p := DivisionPolynomial(E, 16) div DivisionPolynomial(E, 8);
   fact := Factorization(p : DegreeLimit := 32);
   printf "j = %o, #fact = %o\n", j, #fact;
   for i := 1 to #fact do
      printf "%o : %o\n", i, HasRoot(fact[i][1], K);
   end for;
end for;
```

18.m ⇝ 5.2.14

Kao što smo napomenuli u samom dokazu leme 5.2.14, ovdje koristimo funkciju koju su napisali E. González-Jiménez i F. Najman za potrebe dokaza [17, Lemma 8.15.]. Njihov kôd može se naći na `http://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/growth/growth.html`, riječ je o funkciji `Cuenta` u lem8_16a.txt. Funkcija `Cuenta` za danu grupu G (koja je moguća 2-adska slika eliptičke krivulje $E/\mathbb{Q}$) i prirodne brojeve N, s i d vraća sve moguće Galoisove grupe koje odgovaraju poljima $\mathbb{K}$ takvima da je $E(K)[2^\infty] \simeq \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^N\mathbb{Z}$ i da $[\mathbb{K} : \mathbb{Q}]$ dijeli d. Kako bismo prošli po svim mogućim grupama G koristimo bazu `RZB` koja se može naći u datoteci 2primary_Ss.txt na stranici `http://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/pprimary/pprimary.html`. Tu datoteku su generirali E. González-Jiménez i Á. Lozano-Robledo za članak [16]. Oni su pak koristili [48] i njihove (J. Rouse i D. Zureick-Brown) baze koje se mogu naći na `http://users.wfu.edu/rouseja/2adic/`.

```
function aux_Id(m,s)
   if [Integers(2^s)!t : t in Eltseq(m)] eq [1,0,0,1]
      then return true;
      else return false;
   end if;
end function;
load "2primary_Ss.txt";
function Cuenta(G,N,s,d)
   M := Characteristic(BaseRing(G));
```

```
10    GG := sub<GL(2,Integers(2^N)) | Generators(G),
11       [[1,M,0,1],[1,0,M,1],[1+M,0,0,1],[1,0,0,1+M]]>;
12    Odds := [[i,j] : i in [0..2^N-1], j in [0..2^N-1] | IsOdd(i) or IsOdd(j)];
13    L := {};
14    V := RSpace(GG);
15    S := [];
16    for v in Odds do
17       Hv := Stabiliser(GG, V!v);
18       Hvmod2s := [m : m in Hv | aux_Id(m,s)];
19       HHv := sub<GL(2,Integers(2^N)) | Hvmod2s>;
20       ord_s := #Hvmod2s;
21       hv := Integers()!(Order(GG)/ord_s);
22       if IsDivisibleBy(d,hv) then
23          Kv := quo<GG | Core(GG,HHv)>;
24          Gal := GroupName(Kv);
25          if IsAbelian(Kv) eq true and Order(Kv) ge 16 then
26             L := L join {Gal};
27          end if;
28       end if;
29       end for;
30    return L;
31 end function;
32 S := {};
33 for rzb in RZB do
34    if rzb[3][2][4] le 16 then
35       G := sub<GL(2,Integers(rzb[2])) | {m : m in rzb[4]}>;
36    S := S join Cuenta(G,4,1,16);
37    end if;
38 end for;
39 S;
```

19.m ⇝ 5.2.16

```
1  Q<x> := PolynomialRing(Rationals());
2  K := CyclotomicField(32);
3  f := function(E, K)
4     r := Factorization(DivisionPolynomial(E,17) : DegreeLimit := 16);
5     for p in r do if HasRoot(p[1], K) then return true; end if; end for;
6     return false;
```

```
7  end function;
8  f(EllipticCurve("14450p1"), K);
9  f(EllipticCurve("14450p2"), K);
```

ZAKLJUČAK

U radu je potpuno riješeno pitanje rasta torzije eliptičkih krivulja $E/\mathbb{Q}$ nad poljima $\mathbb{Q}_{\infty,p}$, kao i nad kompozitumu svih tih polja. Preciznije, ako je $E/\mathbb{Q}$ eliptička krivulja, onda znamo da je

$$E(\mathscr{K}_{\geq 5})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}},$$

gdje je

$$\mathscr{K}_{\geq 5} = \prod_{p\geq 5 \text{ prost}} \mathbb{Q}_{\infty,p}.$$

Za $\mathscr{K} = \prod_{p \text{ prost}} \mathbb{Q}_{\infty,p}$ smo pokazali da je $E(\mathscr{K})_{\text{tors}}$ izomorfno nekoj od idućih grupa

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ ili } n \in \{12, 13, 21, 27\},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

Pri čemu znamo da za svaku grupu G s gornje liste, postoji eliptička krivulja $E/\mathbb{Q}$ takva da je $E(\mathscr{K})_{\text{tors}} \simeq G$.

Zgodno je primijetiti da se sav "rast torzije" događa upravo na kompozitumu polja $\mathbb{Q}_{\infty,2}$ i $\mathbb{Q}_{\infty,3}$. Štoviše, sve se događa "najdalje" nad poljem

$$\mathbb{Q}_{2,2}\mathbb{Q}_{2,3}.$$

Osim rasta koji smo imali za $\mathbb{Q} \to \mathbb{Q}_{\infty,2}$ i $\mathbb{Q} \to \mathbb{Q}_{\infty,3}$, ovdje se pojavio još jedan izniman slučaj rasta $\mathbb{Q} \to \mathbb{Q}_{2,2}\mathbb{Q}_{1,3}$, gdje imamo rast torzije

$$\{0\} \to \mathbb{Z}/13\mathbb{Z}.$$

Radi potpunosti i preglednosti, u sljedećoj tablici 6.1 navodimo primjere eliptičkih krivulja $E/\mathbb{Q}$ za svaki mogući rast torzije $\mathbb{Q} \to \mathscr{K}$.

Prvi stupac je Cremonina oznaka eliptičke krivulje, drugi stupac je njena torzija nad $\mathbb{Q}$, treći stupac je njena torzija nad $\mathscr{K}$, a četvrti stupac je polje najmanjeg stupnja nad $\mathbb{Q}$ sadržano u $\mathscr{K}$, označimo ga s $\mathbb{F}$, nad kojim je ta torzija definirana.

Cremonina oznaka	$E(\mathbb{Q})_{\text{tors}}$	$E(\mathscr{K})_{\text{tors}}$	$\mathbb{F}$
704d1	$\{0\}$	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Q}_{1,2}$
24a6	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}_{1,2}$
704a1	$\{0\}$	$\mathbb{Z}/5\mathbb{Z}$	$\mathbb{Q}_{1,2}$
320c1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}_{1,2}$
832f	$\{0\}$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Q}_{1,2}$
24a3	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Q}_{1,2}$
1728j3	$\{0\}$	$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Q}_{1,2}$
768b1	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/10\mathbb{Z}$	$\mathbb{Q}_{2,2}$
30a5	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z}$	$\mathbb{Q}_{1,2}$
14a5	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}_{1,2}$
24a2	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}_{1,2}$
14a2	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}_{1,2}$
32a4	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Q}_{1,2}$
32a4	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$	$\mathbb{Q}_{2,2}$
162b1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/21\mathbb{Z}$	$\mathbb{Q}_{1,3}$
27a4	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/27\mathbb{Z}$	$\mathbb{Q}_{2,3}$
324a2	$\{0\}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Q}_{1,3}$
324a1	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Q}_{1,3}$
162b2	$\{0\}$	$\mathbb{Z}/7\mathbb{Z}$	$\mathbb{Q}_{1,3}$
27a3	$\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/9\mathbb{Z}$	$\mathbb{Q}_{1,3}$
20736c1	$\{0\}$	$\mathbb{Z}/13\mathbb{Z}$	$\mathbb{Q}_{2,2}\mathbb{Q}_{1,3}$

Tablica 6.1: Skupna tablica rasta torzije

Na kraju smo pokazali da je za torziju nad $\mathbb{Q}(\mu_{p^\infty})$ dovoljno znati torziju nad $\mathbb{Q}(\mu_p)$, za svaki prost broj $p \geq 5$. Nadalje, vrijedi i da je

$$E(\mathbb{Q}(\mu_{3^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{3^3}))_{\text{tors}} \qquad \text{te} \qquad E(\mathbb{Q}(\mu_{2^\infty}))_{\text{tors}} = E(\mathbb{Q}(\mu_{2^4}))_{\text{tors}}.$$

Rezultati iz poglavlja 4 i 5 će u skorije vrijeme biti objavljeni u članku [21] koji je u nastajanju, u suradnji s Tomislavom Gužvićem. Nakon ovog rada pokušati ćemo reći nešto o torziji nad $\mathbb{Q}(\mu_p)$, za neke konkretne vrijednosti broja p. To će biti napravljeno u suradnji s Tomislavom Gužvićem i Bornom Vukorepom te u nekom trenutku objavljeno u članku [22].

BIBLIOGRAFIJA

[1] B. J. Birch i H. P. F. Swinnerton-Dyer: *Elliptic curves and modular functions*. U B. J. Birch i W. Kuyk (urednici): *Modular Functions of One Variable IV*, svezak 476 iz *Lecture Notes in Mathematics*, stranice 2–32. Springer, Berlin, Heidelberg, 1975. https://doi.org/10.1007/BFb0097581. ↑ 19.

[2] W. Bosma, J. Cannon i C. Playoust: *The magma algebra system. i. the user language*. J. Symbolic Comput., 24(3-4):235–265, 1997, ISSN 0747-7171. http://dx.doi.org/10.1006/jsco.1996.0125. ↑ v, 4, 33, 35, 36, 37, 38, 41, 42, 43, 46, 47, 62, 63, 66, 67, 77, 78, 79, 80, 83.

[3] P. Bruin i F. Najman: *A criterion to rule out torsion groups for elliptic curves over number fields*. Res. Number Theory, 2(3), 2016. https://doi.org/10.1007/s40993-015-0031-5. ↑ 81.

[4] M. Chou: *Torsion of rational elliptic curves over quartic galois number fields*. J. Number Theory, 160:603–628, 2016. https://doi.org/10.1016/j.jnt.2015.09.013.

[5] M. Chou: *Torsion of rational elliptic curves over the maximal abelian extension of* $\mathbb{Q}$. Pacific J. Math., 302(2):481–509, 2019. https://doi.org/10.2140/pjm.2019.302.481. ↑ 43, 61, 67, 69.

[6] M. Chou, H. B. Daniels, I. Krijan i F. Najman: *Torsion groups of elliptic curves over the* $\mathbb{Z}_p$*-extensions of* $\mathbb{Q}$. https://arxiv.org/abs/1808.05243, Submitted. ↑ 4, 25.

[7] P. L. Clark, P. Corn, A. Rice i J. Stankewicz: *Computation on elliptic curves with complex multiplication*. LMS J. Comput. Math., 17:509–535, 2014. https://doi.org/10.1112/S1461157014000072.

[8] H. B. Daniels, M. Derickx i J. Hatley: *Groups of generalized g-type and applications to torsion subgroups of rational elliptic curves over infinite extesions of* $\mathbb{Q}$. Trans. London Math. Soc., 6:22–52, 2019. https://doi.org/10.1112/tlm3.12018. ↑ 55.

[9] H. B. Daniels, Á. Lozano-Robledo, F. Najman i A. V. Sutherland: *Torsion points on rational elliptic curves over the compositum of all cubic fields*. Math. Comp., 87:425–458, 2018. https://doi.org/10.1090/mcom/3213. ↑ 26, 60, 78.

[10] M. Derickx i F. Najman: *Torsion of elliptic curves over cyclic cubic fields*. Math. Comp., 88:2443–2459, 2019. https://doi.org/10.1090/mcom/3408.

[11] M. Derickx i A. V. Sutherland: *Torsion subgroups of elliptic curves over quintic and sextic number fields*. Proc. Amer. Math. Soc., 145:4233–4245, 2017. https://doi.org/10.1090/proc/13605. ↑ 77.

[12] F. Diamond i J. Shurman: *A First Course in Modular Forms*, svezak 228 iz *Graduate Texts in Mathematics*. Springer-Verlag New York, 1. izdanje, 2005. https://doi.org/10.1007/978-0-387-27226-9. ↑ 13, 18.

[13] G. Faltings: *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math., 73:349–366, 1983. http://eudml.org/doc/143051. ↑ 68.

[14] Y. Fujita: *The* 2*-primary torsion on elliptic curves in the* $\mathbb{Z}_p$*-extensions of* $\mathbb{Q}$. Manuscripta Math., 118:339–360, 2005. https://doi.org/10.1007/s00229-005-0596-8. ↑ 44.

[15] E. González-Jiménez i Á. Lozano-Robledo: *Elliptic curves with abelian division fields*. Math. Z., 283:835—-859, 2016. https://doi.org/10.1007/s00209-016-1623-z. ↑ 71.

[16] E. González-Jiménez i Á. Lozano-Robledo: *On the minimal degree of definition of p-primary torsion subgroups of elliptic curves*. Math. Res. Lett., 24:1067–1096, 2017. https://dx.doi.org/10.4310/MRL.2017.v24.n4.a7. ↑ 78, 91.

[17] E. González-Jiménez i F. Najman: *Growth of torsion groups of elliptic curves upon base change*. Math. Comp., 89:1457–1485, 2020. https://doi.org/10.1090/mcom/3478. ↑ 4, 26, 28, 44, 63, 66, 72, 78, 91.

[18] F. Q. Gouvêa: *p-adic Numbers*. Universitext. Springer-Verlag Berlin Heidelberg, 2. izdanje, 1997. https://doi.org/10.1007/978-3-642-59058-0. ↑ 23, 24.

[19] R. Greenberg: *Iwasawa theory for elliptic curves*. U C. Viola (urednik): *Arithmetic Theory of Elliptic Curves*, svezak 1716 iz *Lecture Notes in Mathematics*, stranice 51–144. Springer, Berlin, Heidelberg, 1999. https://doi.org/10.1007/BFb0093453. ↑ iv.

[20] R. Greenberg: *The image of galois representations attached to elliptic curves with an isogeny*. Amer. J. Math., 134(5):1167–1196, 2012. https://doi.org/10.1353/ajm.2012.0040. ↑ 10.

[21] T. Gužvić i I. Krijan: *Torsion groups of elliptic curves over some infinite abelian extensions of* $\mathbb{Q}$. In preparation. ↑ 4, 95.

[22] T. Gužvić, I. Krijan i B. Vukorepa: *Torsion groups of elliptic curves over* $\mathbb{Q}(\mu_{p^\infty})$. In preparation. ↑ 4, 81, 95.

[23] J. G. Huard, B. K. Spearman i K. S. Williams: *A short proof of the formula for the conductor of an abelian cubic field*. Norske Vid. Selsk. Skr., 2:3–8, 1994. https://people.math.carleton.ca/~williams/papers/pdf/184.pdf. ↑ 49.

[24] S. Kamienny: *Torsion points on elliptic curves and q-coefficients of modular forms*. Invent. Math., 109:221–229, 1992. https://doi.org/10.1007/BF01232025. ↑ 41, 42, 43.

[25] S. Kamienny i F. Najman: *Torsion groups of elliptic curves over quadratic fields*. Acta Arith., 152:291–305, 2012. https://doi.org/10.4064/aa152-3-5. ↑ 35, 41, 42, 44.

[26] N. M. Katz: *Galois properties of torsion points on abelian varieties*. Invent. Math., 62:481–502, 1980. https://doi.org/10.1007/BF01394256. ↑ 37.

[27] M. A. Kenku: *The modular curve* $x_0(39)$ *and rational isogeny*. Math. Proc. Cambridge Philos. Soc., 85:21–23, 1979. https://doi.org/10.1017/S0305004100055444. ↑ 26, 71.

[28] M. A. Kenku: *The modular curve* $x_0(169)$ *and rational isogeny*. J. London Math. Soc., s2-22:239–244, 1980. https://doi.org/10.1112/jlms/s2-22.2.239, Corrigendum: https://doi.org/10.1112/jlms/s2-23.3.428-s. ↑ 26, 71.

[29] M. A. Kenku: *The modular curves $x_0(65)$ and $x_0(91)$ and rational isogeny*. Math. Proc. Cambridge Philos. Soc., 87:15–20, 1980. https://doi.org/10.1017/S0305004100056462. ↑ 26, 71.

[30] M. A. Kenku: *The modular curve $x_0(125)$, $x_1(25)$ and $x_1(49)$*. J. London Math. Soc., s2-23:415–427, 1981. https://doi.org/10.1112/jlms/s2-23.3.415. ↑ 26, 71.

[31] M. A. Kenku i F. Momose: *Torsion points on elliptic curves defined over quadratic fields*. Nagoya Math. J., 109:125–149, 1988. https://doi.org/10.1017/S0027763000002816. ↑ 41, 42, 43.

[32] D. S. Kubert: *Universal bounds on the torsion of elliptic curves*. Compos. Math., 38(1):121–128, 1979. http://www.numdam.org/item/CM_1979__38_1_121_0. ↑ 45, 46.

[33] S. Lang: *Algebraic Number Theory*, svezak 110 iz *Graduate Texts in Mathematics*. Springer-Verlag New York, 2. izdanje, 1994. https://doi.org/10.1007/978-1-4612-0853-2. ↑ 23, 48.

[34] H. W. Leopoldt: *Zur Arithmetik in abelschen Zahlkörpern*. J. Reine Angew. Math., 209:54–71, 1962. http://eudml.org/doc/150514. ↑ 21.

[35] Á. Lozano-Robledo: *Elliptic Curves, Modular Forms, and Their L-functions*, svezak 58 iz *Student mathematical library*. American Mathematical Soc., 2011. https://bookstore.ams.org/stml-58. ↑ 45, 46.

[36] Á Lozano-Robledo: *On the field of definition of p-torsion points on elliptic curves over the rationals*. Math. Ann., 357:279–305, 2013. https://doi.org/10.1007/s00208-013-0906-5. ↑ 35, 38, 41, 62, 74, 79.

[37] B. Mazur: *Rational isogenies of prime degree*. Invent. Math., 44:129–162, 1978. https://doi.org/10.1007/BF01390348. ↑ 2, 26, 30, 41, 44, 45, 71, 81.

[38] J. S. Milne: *Fields and galois theory*, 2018. https://www.jmilne.org/math/CourseNotes/FT.pdf, Course Notes version 4.60. ↑ 20.

[39] J. S. Morrow: *Composite images of galois for elliptic curves over* **Q** *and entanglement fields*. Math. Comp., 88:2389–2421, 2019. https://doi.org/10.1090/mcom/3426. ↑ 67.

[40] F. Najman: *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*. J. Number Theory, 130:1964–1968, 2010. https://doi.org/10.1016/j.jnt.2009.12.008. ↑ 81.

[41] F. Najman: *Torsion of elliptic curves over cubic fields*. J. Number Theory, 132:26–36, 2012. https://doi.org/10.1016/j.jnt.2011.06.013. ↑ 37.

[42] F. Najman: *Eliptičke krivulje nad poljima algebarskih brojeva*, 2013. https://web.math.pmf.unizg.hr/~fnajman/elipticke.pdf, Bilješke s predavanja. ↑ 1, 3, 5, 12.

[43] F. Najman: *The number of twists with large torsion of an elliptic curve*. Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM, 109:535–547, 2015. https://doi.org/10.1007/s13398-014-0199-x. ↑ 64.

[44] F. Najman: *Aritmetička geometrija*, 2016. https://web.math.pmf.unizg.hr/~fnajman/ag.pdf, Bilješke s predavanja. ↑ 1, 3, 5, 12, 20.

[45] F. Najman: *Torsion of rational elliptic curves over cubic fields and sporadic points on* $x_1(n)$. Math. Res. Lett., 23(1):245–272, 2016. https://dx.doi.org/10.4310/MRL.2016.v23.n1.a12. ↑ 37, 39, 43.

[46] F. P. Rabarison: *Structure de torsion des courbes elliptiques sur les corps quadratiques*. Acta Arith., 144 :17–52, 2010. http://eudml.org/doc/279559. ↑ 37, 38, 45, 46.

[47] M. A. Reichert: *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*. Math. Comp., 46(174):637–658, 1986. https://doi.org/10.2307/2008003. ↑ 33.

[48] J. Rouse i D. Zureick-Brown: *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of galois*. Res. Number Theory, 1(12), 2015. https://doi.org/10.1007/s40993-015-0013-7. ↑ 78, 91.

[49] J. P. Serre: *Galois Cohomology*. Springer Monographs in Mathematics. Springer-Verlag Berlin Heidelberg, 1. izdanje, 1997. https://doi.org/10.1007/978-3-642-59141-9. ↑ 20.

[50] J. P. Serre: *Lectures on the Mordell-Weil Theorem*, svezak 15 iz *Aspects of Mathematics*. Vieweg+Teubner Verlag, 3. izdanje, 1997. https://doi.org/10.1007/978-3-663-10632-6. ↑ 45.

[51] S. Siksek: *Explicit methods for modular curves*, 2019. https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf, Lecture notes. ↑ 5, 18, 37, 63.

[52] J. H. Silverman: *Advanced Topics in the Arithmetic of Elliptic Curves*, svezak 151 iz *Graduate Texts in Mathematics*. Springer-Verlag New York, 1. izdanje, 1994. https://doi.org/10.1007/978-1-4612-0851-8. ↑ 35, 38, 41, 77, 80.

[53] J. H. Silverman: *The Arithmetic of Elliptic Curves*, svezak 106 iz *Graduate Texts in Mathematics*. Springer-Verlag New York, 2. izdanje, 2009. https://doi.org/10.1007/978-0-387-09494-6. ↑ 1, 3, 5, 8, 10, 12, 14, 19, 25.

[54] The LMFDB Collaboration: *The l-functions and modular forms database*, 2019. http://www.lmfdb.org, [Online; accessed 30 October 2019]. ↑ 3, 33, 35, 36, 37, 42, 43, 47, 48, 62, 66, 67, 70, 77, 82, 89.

[55] J. A. Thorne: *Elliptic curves over $\mathbb{Q}_\infty$ are modular*. J. Eur. Math. Soc. (JEMS), 21, 2019. https://doi.org/10.4171/JEMS/877. ↑ iv.

[56] L. C. Washington: *Introduction to Cyclotomic Fields*, svezak 83 iz *Graduate Texts in Mathematics*. Springer-Verlag New York, 2. izdanje, 1997. https://doi.org/10.1007/978-1-4612-1934-7. ↑ iii, 22.

[57] D. Zywina: *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*. https://arxiv.org/pdf/1508.07660.pdf, Submitted. ↑ 66.

Životopis

Ivan Krijan rođen je 04.10.1989. u Slavonskom Brodu. Godine 2008. započeo je svoj studij na Sveučilištu u Zagrebu, gdje je studirao matematiku na Prirodoslovno matematičkom fakultetu (i stekao titulu B. Sc. 2011. godine). Diplomirao je summa cum laude s temom "Reprezentacije klasičnih konačnih grupa" (2013). Tijekom diplomskog studija nagrađen je Dekanovom nagradom za najboljeg studenta i Rektorovom nagradom za rad “Multipliciteti presjeka ravninskih krivulja”. Nakon stjecanja diplome, počeo je raditi kao asistent na Matematičkom odsjeku Prirodoslovno matematičkog fakulteta Sveučilišta u Zagrebu i upisao je zajednički sveučilišni poslijediplomski doktorski studij Matematika Sveučilišta u Zagrebu, Splitu, Rijeci i Osijeku (nositelj studija: Prirodoslovno-matematički fakultet – Matematički odsjek). Glavno polje njegovog istraživanja su eliptičke krivulje.

Godine 2016. stupa u brak sa suprugom Anom, a 2018. postaje ponosni otac sina Filipa.

Aktivno se bavi popularizacijom znanosti i matematike i član je Državnog povjerenstva za natjecanja iz matematike.

IZJAVA O IZVORNOSTI RADA

Ja, *Ivan Krijan*, asistent i doktorand na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu,

prebivalište: *Slavka Batušića 13, 10090 Zagreb, Hrvatska*,

JMBAG: *1191213860*,

matični broj doktoranda: *I-422/13*,

matični broj znanstvenika: *347336*,

ovim putem izjavljujem pod materijalnom i kaznenom odgovornošću da je moj *doktorski rad* pod naslovom: *Torzija eliptičkih krivulja nad beskonačnim Abelovim proširenjima od* $\mathbb{Q}$ (na engleskom: *Torsion groups of elliptic curves over infinite Abelian extensions of* $\mathbb{Q}$), isključivo moje autorsko djelo, koje je u potpunosti samostalno napisano uz naznaku izvora drugih autora i dokumenata korištenih u radu.

U Zagrebu, *20. travnja 2020.*

Ivan Krijan