Racionalne D(q)-m-torke

Dražić, Goran

Doctoral thesis / Disertacija

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:888094

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-02-20**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Goran Dražić

Racionalne $D(q)$-m-torke

DOKTORSKI RAD

Zagreb, 2021.

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Goran Dražić

Racionalne $D(q)$-m-torke

DOKTORSKI RAD

Mentor:

izv. prof. dr. sc. Matija Kazalicki

Zagreb, 2021.

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Goran Dražić

Rational $D(q)$-m-tuples

DOCTORAL DISSERTATION

Supervisor:

izv. prof. dr. sc. Matija Kazalicki

Zagreb, 2021.

ZAHVALA

Autor je tokom izrade ove disertacije suradnik na projektu Hrvatske zaklade za znanost "Diofantska geometrija i primjene" (HRZZ-1313) voditelja izv. prof. dr. sc. Matije Kazalickog.

Autor se posebno želi zahvaliti mentoru Matiji Kazalickom za uložen velik trud kroz zadnjih desetak godina, kao i svojoj djevojci Milani za potporu prilikom studiranja.

SAŽETAK

U radu se proučavaju racionalne $D(q)$-m-torke gdje je $m = 3, 4$ ili 5.

Prvo, parametriziramo racionalne $D(q)$-četvorke umnoška elemenata jednakog m pomoću točaka na eliptičkoj krivulji E_m definiranoj preko q, m. Za svaki racionalan q parametriziramo m takve da postoji četvorka umnoška elemenata m.

Potom konstruiramo nove familije racionalnih $D(q)$-petorki. Uz pretpostavku Slutnje o parnosti dokazujemo da za svaki kvadratno slobodan cijeli broj q koji se nalazi u jednoj od 99.5% klasa ostataka mod 394680 postoji beskonačno racionalnih $D(q)$-petorki.

Konačno, parametriziramo racionalne $D(q)$-trojke te koristimo tu parametrizaciju za rješavanje nekih problema.

Ključne riječi: Diofantove m-torke, Racionalne $D(q)$-m-torke, Eliptičke krivulje.

SUMMARY

This work studies rational $D(q)$-m-tuples, where $m = 3, 4$ or 5.

First, we parametrize rational $D(q)$-quadruples with product of elements equal to m using the elliptic curve E_m, defined via q, m. For each rational nonzero q we parametrize m, such that there exists a rational $D(q)$-quadruple with product of elements equal to m.

Then we construct new families of rational $D(q)$-quintuples. With the assumption of the Parity conjecture we prove that for each squarefree integer q in one of 99.5% of classes of residues mod 394680 there exists infinitely many rational $D(q)$-quintuples.

Finally, we parametrize all rational $D(q)$-triples for rational q which are not squares, and use this parametrization to solve problems.

The outline of the thesis is as follows. In the Introduction we define Diophantine m-tuples and give a historical overview of research in the field.

Chapter 1 ("Some basic results on elliptic curves") gives definitions and results from algebraic geometry and elliptic curves, which are used throughout the thesis.

In Chapter 2 ("Rational $D(q)$-quadruples") we describe rational $D(q)$-quadruples with product of elements equal to m. We parametrize all m, depending on q, for which there exists such a quadruple. For such pairs (q, m), we parametrize all such quadruples using triples of points on the elliptic curve E_m, whose equation depends on q and m.

In Chapter 3 ("Rational $D(q)$-quintuples") we construct families of rational $D(q)$-quintuples for squarefree integers q in specific classes of residues. With the assumption of the Parity conjecture we prove there are infinitely many $D(q)$-quintuples for squarefree integers q in 99.5% of classes of residues mod 394680.

In Chapter 4 ("Rational $D(q)$-triples") we parametrize rational $D(q)$-triples for each rational q which is not a square. We use this parametrization to solve problems.

In Chapter 5 ("Magma codes") we give explicit codes in the programming language Magma [4] used in the thesis.

Keywords: Diophatine m-tuples, Rational $D(q)$-m-tuples, Eliptic curves.

Acknowledgement

The author was supported by the Croatian Science Foundation under the project no. 1313 (HRZZ 1313) "Diophantine geometry and applications", led by associate professor Matija Kazalicki.

SADRŽAJ

UVOD

Diofantova m-torka je skup m cijelih brojeva, različitih od nule, sa svojstvom da je umnožak bilo koja dva različita elementa tog skupa uvećan za 1 potpun kvadrat. Takve skupove možemo prirodno poopćiti na sljedeći način: za neki racionalan q različit od nule, skup $\{a_1, a_2, \ldots, a_m\}$ racionalnih brojeva različitih od nule zovemo *racionalna $D(q)$-m-torka,* ako su brojevi $a_i a_j + q$ racionalni kvadrati za sve $1 \leq i < j \leq m$.

Diofantove m-torke proučavaju se od antičkih vremena. Prvi primjer (racionalne) Diofantove četvorke bio je skup

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\},$$

koji je otkrio starogrčki matematičar Diofant, po kome su i skupovi koje proučavamo nazvani. Fermat je pronašao prvu Diofantovu četvorku $\{1,3,8,120\}$. Euler je dokazao da postoji beskonačno cjelobrojnih $D(n)$-četvorki (vidi [27]), između ostalog, pronašao je i proširenje Fermatove četvorke do racionalne petorke

$$\left\{1,3,8,120,\frac{777480}{8288641}\right\},$$

a nedavno je Stoll [38] pokazao da je to proširenje jedinstveno.

Baker i Davenport [3] su 1969. pokazali da trojka $\{1,3,8\}$ ima jedinstveno proširenje do Diofantove četvorke, broj 120. Taj rezultat je potaknuo slutnju da ne postoji Diofantova petorka. Dujella [11] je 2004. dokazao da ne postoji Diofantova šestorka te da postoji najviše konačno mnogo Diofantovih petorki, a 2019. su cijelu slutnju dokazali He, Togbé i Ziegler [26].

Nije poznata gornja granica veličine racionalnih Diofantovih skupova, iako Langova slutnja o mnogostrukostima općeg tipa implicira da je broj članova racionalne Diofantove m-torke ograničen odozgo apsolutnom konstantom (vidi uvod [16]). Prvi primjer racionalne Diofantove šestorke pronašao je Gibbs [23] pomoću računala

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}.$$

Dujella, Kazalicki, Mikić i Szikszai [16] su 2017. dokazali da postoji beskonačno mnogo racionalnih Diofantovih šestorki. Piezas [32] je opazio kako neki primjeri Gibbsovih šestorki zadovoljavaju određen uzorak, što je inspiriralo Dujellu i Kazalickog da konstruiraju šestorke na nov način [14]. Dujella, Kazalicki i Petričević [19], [18] konstruirali su racionalne Diofantove šestorke s nazivnicima koji su kvadrati, odnosno šestorke koje sadrže dvije regularne četvorke i jednu regularnu petorku. Nije poznat niti jedan primjer racionalne Diofantove sedmorke.

Dujella [10] je dokazao da za svaki racionalan q postoji beskonačno mnogo racionalnih $D(q)$-četvorki te da za q oblika $3r^2$ postoji beskonačno mnogo racionalnih $D(q)$-petorki. Dujella i Fuchs [13] su pokazali da za beskonačno racionalnih kvadratno slobodnih brojeva q postoji beskonačno mnogo racionalnih $D(q)$-petorki. Posebno, uz pretpostavku Slutnje o parnosti, pokazali su da za sve kvadratno slobodne q u bar 497 klasa ostataka $\bmod 1320$ postoji beskonačno racionalnih $D(q)$-petorki. Nije poznat niti jedan primjer racionalne $D(q)$-šestorke gdje q nije potpun kvadrat.

Spomenimo i članke u kojima se autori bave parametrizacijama racionalnih $D(q)$-m-torki. Adžaga, Dujella, Kreso i Tadić [1] konstruirali su beskonačne familije cjelobrojnih Diofantovih trojki koje su $D(n)$ skupovi za još dva različita cijela broja n. Dujella, Kazalicki i Petričević [17] dokazali su postojanje beskonačnog broja različitih $D(n)$-petorki čiji su svi elementi potpuni kvadrati, gdje n nije fiksan broj. To su napravili tako što su neke takve petorke parametrizirali racionalnim točkama na određenoj plohi, potom su na plohi pronašli eliptičke krivulje pozitivnog ranga. Kazalicki i Naskrecki se u [28], između ostalog, bave parametrizacijama K-racionalnih Diofantovih trojki, gdje je K polje koje nema karatkeristiku jednaku dva. Otkrili su novu parametrizaciju racionalnih Diofantovih trojki koja je biracionalno ekvivalentna Lasićevoj parametrizaciji spomenutoj u dodatku istog članka. Još jedan primjer parametrizacije Diofantovih trojki spominje se u [12, §2]. Takve parametrizacije su dobra početna točka za konstrukcije većih Diofantovih skupova, kao i za konstrukcije eliptičkih krivulja velikog ranga [21].

Ova disertacija organizirana je na sljedeći način.

U Poglavlju 1 izlažemo osnovne definicije i pojmove potrebne u ostatku rada. Tu se nalazi kratki uvod u algebarsku geometriju pomoću kojeg prelazimo na osnovne rezultate o eliptičkim krivuljama, našem glavnom alatu u proučavanju $D(q)$-m-torki.

U Poglavlju 2 bavimo se racionalnim $D(q)$-četvorkama. Za racionalan q različit od nule, parametriziramo sve m takve da postoji racionalna $D(q)$-četvorka umnoška elemenata jednakog m, pritom dokazujući jači rezultat od Dujelle [10]. Za svaki par (q,m) za koji postoji racionalna

$D(q)$-četvorka, parametriziramo sve takve četvorke koristeći trojke točaka na eliptičkoj krivulji E_m koja je definirana pomoću q i m. Rezultati ovog poglavlja nalaze se u neobjavljenom članku [8].

U Poglavlju 3 konstruiramo racionalne $D(q)$-petorke na temelju Dujelline konstrukcije [9], prateći ideju Dujelle i Fuchsa [13]. Uz pretpostavku Slutnje o parnosti dokazujemo da za kvadratno slobodne $q \in \mathbb{N}$ u barem 295026 klasa ostataka $\bmod 394680$ te kvadratno slobodne $q \in -\mathbb{N}$ u barem 295435 klasa ostataka $\bmod 394680$ postoji beskonačno racionalnih $D(q)$-petorki. Budući da postoji 296010 klasa ostataka $\bmod 394680$ koje sadrže kvadratno slobodne brojeve, pokrivamo barem 99.5% svih klasa $\bmod 394680$. Iskazujemo slutnju da uz pretpostavku Slutnje o parnosti, za svaki racionalan q postoji beskonačno racionalnih $D(q)$-petorki. Rezultati ovog poglavlja nalaze se u članku [7].

U Poglavlju 4 smo uspjeli naći prvu parametrizaciju racionalnih $D(q)$-trojki, koristeći rad Kazalickog i Naskręckog [28]. Na dva smo načina parametrizirali racionalne $D(q)$-trojke koje su i $D(0)$-trojke te smo parametrizirali racionalne $D(q)$-četvorke koje sadrže regularnu trojku. Rezultati ovog poglavlja nalaze se u članku [6].

U Poglavlju 5 nalaze se kodovi za računalni program Magma. Naglašavamo veliku važnost računalnih programa u našem radu. Mnogi rezultati Poglavlja 2 i 3 naslućeni su korištenjem programa Magma [4]. Svi računi u kojima se spominju eliptičke krivulje također koriste Magmu kao osnovni alat.

1. NEKI OSNOVNI REZULTATI O ELIPTIČKIM KRIVULJAMA

U ovom poglavlju obraditi ćemo dio poznate teorije o eliptičkim krivuljama koja nam je potrebna u ostatku rada. Poglavlje dobrim dijelom prati razne dijelove knjige "The arithmetic of elliptic curves" Josepha Silvermana [37], djelomično prati skriptu Filipa Najmana koju je napisao u sklopu kolegija "Aritmetička geometrija" [31], a često se referencira na dokaze iz knjige "Algebraic geometry" Robina Hartshornea [25].

1.1. AFINE I PROJEKTIVNE MNOGOSTRUKOSTI

Eliptička krivulja je projektivna mnogostrukost genusa 1 s racionalnom točkom. Kako bi proučavali krivulje, moramo napraviti kratak uvod u algebarsku geometriju.

1.1.1. Afine mnogostrukosti

Neka je K savršeno polje, $\overline{K}$ njegov algebarski zatvarač, a $\mathrm{Gal}(\overline{K}/K)$ Galoisova grupa od $\overline{K}/K$.

Definicija 1.1.1. *Afini n-prostor (nad K)* je skup n-torki

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \ldots, x_n) \colon x_i \in \overline{K}\}.$$

Slično, *skup K-racionalnih točaka od* $\mathbb{A}^n$ je skup

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n \colon x_i \in K\}.$$

Galoisova grupa $\mathrm{Gal}(\overline{K}/K)$ djeluje na $\mathbb{A}^n$. Za $\sigma \in \mathrm{Gal}(\overline{K}/K)$ i $P \in \mathbb{A}^n$ imamo

$$P^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

Znamo da je $P \in \mathbb{A}^n(K)$ ako i samo ako je $P^\sigma = P$, za svaki $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Neka je $\overline{K}[X] = \overline{K}[X_1, \ldots, X_n]$ *prsten polinoma u n varijabli* s *poljem razlomaka* $\overline{K}(X)$ racionalnih funkcija na $\overline{K}$ (analogne definicije za K). Svakom idealu $I \subset \overline{K}[X]$ pridružujemo podskup od $\mathbb{A}^n$,

$$V_I = \{P \in \mathbb{A}^n \colon f(P) = 0 \text{ za svaku } f \in I\}.$$

Definicija 1.1.2. Bilo koji skup oblika V_I je *(afini) algebarski skup.* Ako je V neki algebarski skup, *ideal od* V je dan sa

$$I(V) = \{f \in \overline{K}[X] \colon f(P) = 0 \text{ za sve } P \in V\}.$$

Algebarski skup V je *definiran nad* K ako se njegov ideal $I(V)$ može generirati polinomima u $K[X]$, to označavamo sa V/K. Ako je V definiran nad K, onda je *skup K-racionalnih točaka od* V skup

$$V(K) = V \cap \mathbb{A}^n(K).$$

Definicija 1.1.3. Afini algebarski skup V zovemo *(afina) mnogostrukost* ako je $I(V)$ prost ideal u $\overline{K}[X]$. Za mnogostrukost V/K definiramo *afini koordinatni prsten od* V/K sa

$$K[V] = \frac{K[X]}{I(V/K)}.$$

Prsten $K[V]$ je integralna domena, njegovo polje razlomaka označavamo s $K(V)$ i zovemo *polje funkcija od* V/K. Slično definiramo i $\overline{K}[V]$ te $\overline{K}(V)$, ako zamijenimo K sa $\overline{K}$.

Ako je $f(X) \in \overline{K}[X]$ bilo koji polinom, onda $\mathrm{Gal}(\overline{K}/K)$ djeluje na f tako što djeluje na njegove koeficijente. Posebno, ako je V/K, onda $\mathrm{Gal}(\overline{K}/K)$ preslikava $I(V)$ u samog sebe pa imamo djelovanje $\mathrm{Gal}(\overline{K}/K)$ na $\overline{K}[V]$ te $\overline{K}(V)$. Može se provjeriti da su $K[V]$ te $K(V)$ podskupovi od $\overline{K}[V]$ te $\overline{K}(V)$ koje $\mathrm{Gal}(\overline{K}/K)$ fiksira. Djelovanje od $\sigma \in \mathrm{Gal}(\overline{K}/K)$ na f označavamo sa $f \mapsto f^\sigma$. Za svaku točku $P \in V$ vrijedi

$$(f(P))^\sigma = f^\sigma(P^\sigma).$$

Definicija 1.1.4. *Dimenzija mnogostrukosti* V, ili $\dim V$, je stupanj transcendentnosti od $\overline{K}(V)$ nad $\overline{K}$.

Definicija 1.1.5. Neka je V mnogostrukost, P neka točka na V te $f_1, \ldots, f_m \in \overline{K}[X]$ skup generatora za $I(V)$. Tada je V *glatka u* P (ili nesingularna u P) ako je rang $m \times n$ matrice

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \le i \le m, \\ 1 \le j \le n}}$$

jednak $n = \dim(V)$. Posebno, ako je V glatka u svakoj točki kažemo da je V *glatka.*

Za svaku točku $P \in V$ definiramo ideal M_P od $\overline{K}[V]$ sa

$$M_P = \{f \in \overline{K}[V] \colon f(P) = 0\}.$$

Ideal M_P je maksimalni ideal funkcija koje P poništava. Kvocijent M_P/M_P^2 je konačno dimenzionalni vektorski prostor nad $\overline{K}$.

Propozicija 1.1.6. Mnogostrukost V je glatka u točki $P \in V$ ako i samo ako je

$$\dim_{\overline{K}} M_P/M_P^2 = \dim V.$$

Dokaz. Vidi Hartshorne [25, I.5.1]. ■

Definicija 1.1.7. *Lokalni prsten od V u P,* koji označavamo $\overline{K}[V]_P$, je lokalizacija od $\overline{K}[V]$ u M_P. Funkciju $f \in \overline{K}[V]$ zovemo *regularnom u P* ako je $f \in \overline{K}[V]_P$.

1.1.2. Projektivne mnogostrukosti

Definicija 1.1.8. *Projektivni n-prostor nad K*, koji označavamo $\mathbb{P}^n$ ili $\mathbb{P}^n(\overline{K})$, je skup svih $(n+1)$-orki

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$$

takvih da je barem jedan od brojeva x_i različit od nule, modulo relacija ekvivalencije $\sim$, gdje je

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

ako postoji $\lambda \in \overline{K}^*$ takav da je $x_i = \lambda y_i$, za svaki i. Klasu ekvivalencije

$$\{(\lambda x_0, \ldots, \lambda x_n) \colon \lambda \in \overline{K}^*\}$$

označavamo $[x_0, \ldots, x_n]$. *Skup K-racionalnih točaka u $\mathbb{P}^n$* je skup

$$\mathbb{P}^n(K) = \{[x_0, \ldots, x_n] \in \mathbb{P}^n \colon \text{ svaki } x_i \in K\}.$$

Primijetimo da ako je $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(K)$, nije nužno da su $x_i \in K$, ali ako odaberemo neki j takav da je x_j različit od nule, onda su svi $x_i/x_j \in K$.

Definicija 1.1.9. Polinom $f \in \overline{K}[X] = \overline{K}[X_0, \ldots, X_n]$ je *homogen stupnja d* ako je

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n), \text{ za svaki } \lambda \in \overline{K}.$$

Ideal $I \subset \overline{K}[X]$ je *homogen* ako je generiran homogenim polinomima.

Za homogen polinom f i točku $P \in \mathbb{P}^n$ ima smisla pitati je li $f(P) = 0$, budući da je odgovor neovisan o izboru homogenih koordinata za P. Svakom homogenom idealu I pridružujemo podskup od $\mathbb{P}^n$ na sljedeći način:

$$V_I = \{P \in \mathbb{P}^n \colon f(P) = 0 \text{ za svaki homogeni } f \in I\}.$$

Definicija 1.1.10. *Projektivni algebarski skup* je bilo koji skup oblika V_I za homogen ideal I. Ako je V projektivni algebarski skup, *ideal od* V, koji označavamo sa $I(V)$, je ideal u $\overline{K}[X]$ generiran sa

$$\{f \in \overline{K}[X] \colon f \text{ je homogen te } f(P) = 0 \text{ za sve } P \in V\}.$$

Kažemo da je V *definiran nad* K, što označavamo V/K, ako se pripadajući ideal $I(V)$ može generirati homogenim polinomima u $K[X]$. Ako je V definiran nad K, onda je *skup K-racionalnih točaka od* V dan sa

$$V(K) = V \cap \mathbb{P}^n(K).$$

Kao i za afine prostore, vrijedi

$$V(K) = \{P \in V \colon P^\sigma = P \text{ za svaki } \sigma \in \mathrm{Gal}(\overline{K}/K)\}.$$

Definicija 1.1.11. *Projektivna mnogostrukost* je projektivni algebarski skup V čiji je homogen ideal $I(V)$ prost ideal u $\overline{K}[X]$.

Jasno je da $\mathbb{P}^n$ sadrži puno kopija $\mathbb{A}^n$. Na primjer, za svaki $0 \leq i \leq n$ postoji inkluzija $\phi_i \colon \mathbb{A}^n \to \mathbb{P}^n$ dana sa

$$(y_1, \ldots, y_n) \mapsto [y_1, y_2, \ldots, y_i, 1, y_{i+1}, \ldots, y_n].$$

Neka je H_i hiperravnina u $\mathbb{P}^n$ dana sa $x_i = 0$,

$$H_i = \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n \colon x_i = 0\},$$

a neka je U_i komplement od H_i,

$$U_i = \{P = [x_0, \ldots, x_n] \in \mathbb{P}^n \colon x_i \neq 0\} = \mathbb{P}^n \setminus H_i.$$

Postoji prirodna bijekcija $\phi_i^{-1} \colon U_i \to \mathbb{A}^n$,

$$[x_0, \ldots, x_n] \mapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Neka je V projektivan algebarski skup s homogenim idealom $I(V) \subset \overline{K}[X]$. Skup $\phi_i^{-1}(V \cap U_i)$, za svaki $i \in \{0,\ldots,n\}$, je afini algebarski skup, čiji je ideal $I\left(\phi_i^{-1}(V \cap U_i)\right) \subset \overline{K}[Y]$ dan sa

$$I\left(\phi_i^{-1}(V \cap U_i)\right) = \{f(Y_1,\ldots,Y_i,1,Y_{i+1},\ldots,Y_n)\colon f(X_0,\ldots,X_n) \in I(V)\}.$$

Oznaku $V \cap \mathbb{A}^n$ koristiti ćemo umjesto $\left(\phi_i^{-1}(V \cap U_i)\right)$, kada nam nije bitno o kojem se indeksu i radi, ili kada je jasno naznačeno o kojem se indeksu radi. Proces zamjene polinoma $f(X_0,\ldots,X_n)$ polinomom $\hat{f}_i(Y_1,\ldots,Y_n) = f(Y_1,\ldots,Y_i,1,Y_{i+1},\ldots,Y_n)$ zovemo *dehomogenizacija obzirom na* X_i. Taj proces možemo i obrnuti. Za bilo koji $f(Y) \in \overline{K}[Y]$, definiramo

$$\tilde{f}_i(X_0,\ldots,X_n) = X_i^d f\left(\frac{X_0}{X_i},\frac{X_1}{X_i},\ldots,\frac{X_{i-1}}{X_i},\frac{X_{i+1}}{X_i},\ldots,\frac{X_n}{X_i}\right),$$

gdje je $d = \deg(f)$ stupanj polinoma f. Kažemo da je $\tilde{f}_i$ *homogenizacija od* f *obzirom na* X_i.

Definicija 1.1.12. Neka je $V \subset \mathbb{A}^n$ afini algebarski skup čiji je ideal $I(V)$ i promatrajmo V kao podskup od $\mathbb{P}^n$ preko

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n.$$

Projektivno zatvorenje od V, označeno sa $\overline{V}$, je projektivni algebarski skup čiji je homogeni ideal $I(\overline{V})$ generiran sa

$$\{\tilde{f}_i(X)\colon f \in I(V)\}.$$

Propozicija 1.1.13. (a) Neka je V afina mnogostrukost. Tada je $\overline{V}$ projektivna mnogostrukost i vrijedi

$$V = \overline{V} \cap \mathbb{A}^n.$$

(b) Neka je V projektivna mnogostrukost. Tada je $V \cap \mathbb{A}^n$ afina mnogostrukost te vrijedi

$$V \cap \mathbb{A}^n = \emptyset \quad \text{ili} \quad V = \overline{V \cap \mathbb{A}^n}.$$

(c) Ako je afina (odnosno projektivna) mnogostrukost V definirana nad K, tada je i $\overline{V}$ (odnosno $V \cap \mathbb{A}^n$) definirana nad K.

Dokaz. Za (a) i (b) vidi Hartshorne [25, I.2.3]. (c) dio slijedi iz definicija. ■

Definicija 1.1.14. Neka je V/K projektivna mnogostrukost te neka je $\mathbb{A}^n \subset \mathbb{P}^n$ takav da $V \cap \mathbb{A}^n \neq \emptyset$. *Dimenzija od* V je dimenzija od $V \cap \mathbb{A}^n$. *Funkcijsko polje od* V, označeno sa $K(V)$, je funkcijsko polje od $V \cap \mathbb{A}^n$, slično vrijedi ako zamijenimo K sa $\overline{K}$.

Definicija 1.1.15. Neka je V projektivna mnogostrukost, $P \in V$ neka točka te neka je $\mathbb{A}^n \subset \mathbb{P}^n$ takav da je $P \in \mathbb{A}^n$. Tada je V *glatka u* P ako je $V \cap \mathbb{A}^n$ glatka u P. *Lokalni prsten od* V *u* P, označen sa $\overline{K}[V]_P$, je lokalni prsten od $V \cap \mathbb{A}^n$ u P. Funkcija $F \in \overline{K}(V)$ je *regularna (ili definirana) u* P ako je $F \in \overline{K}[V]_P$ te je tada ima smisla evaluirati u P.

1.1.3. Preslikavanja između mnogostrukosti

Definicija 1.1.16. Neka su V_1 i V_2 projektivne mnogostrukosti. *Racionalno preslikavanje iz* V_1 *u* V_2 je preslikavanje oblika

$$\phi : V_1 \to V_2, \quad \phi = [f_0, \ldots, f_n],$$

gdje su funkcije $f_i \in \overline{K}(V_1)$. Ako su V_1 i V_2 definirani nad K, onda $\mathrm{Gal}(\overline{K}/K)$ djeluje na ϕ na očit način,

$$\phi^\sigma(P) = [f_0^\sigma(P), \ldots, f_n^\sigma(P)].$$

Kažemo da je ϕ *definirano nad K,* ako postoji $\lambda \in \overline{K}^*$ takav da su $\lambda f_0, \ldots, \lambda f_n \in K(V_1)$.

Može se pokazati da je ϕ definirano nad K, ako i samo ako je $\phi = \phi^\sigma$, za svaki $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Racionalno preslikavanje $\phi : V_1 \to V_2$ nije nužno dobro definirano u svakoj točki u V_1. Nekad je moguće evaluirati $\phi(P)$ u nekim točkama $P \in V_1$ gdje neke f_i nisu regularne.

Definicija 1.1.17. Racionalno preslikavanje

$$\phi = [f_0, \ldots, f_n] : V_1 \to V_2$$

je *regularno* ili *definirano u* $P \in V_1$ ako postoji funkcija $g \in \overline{K}(V_1)$ takva da vrijedi

(i) svaka gf_i je regularna u P,

(ii) postoji neki i za koji $(gf_i)(P) \neq 0$.

Ako takva g postoji, onda vrijedi $\phi(P) = [(gf_0)(P), \ldots, (gf_0)(P)]$.

Racionalno preslikavanje koje je regularno u svakoj točki zovemo *morfizam.*

Definicija 1.1.18. Mnogostrukosti V_1 i V_2 su *biracionalno ekvivalentne* ako postoje racionalna preslikavanja $\phi : V_1 \to V_2$ te $\psi : V_2 \to V_1$, takva da su $\psi \circ \phi$ te $\phi \circ \psi$ identitete na V_1, odnosno, V_2. Posebno, ako su ϕ i ψ morfizmi, kažemo da su V_1 i V_2 *izomorfne.*

Kažemo da su V_1/K i V_2/K *biracionalno ekvivalentne nad K* (ili *izomorfne nad K*), ako su ϕ i ψ definirane nad K.

Primjer 1.1.19. Neka je V mnogostrukost zadana jednadžbom

$$V : Y^2Z = X^3 + X^2Z,$$

te promatrajmo racionalna preslikavanja

$$\psi\colon \mathbb{P}^1 \to V, \quad \psi = [(S^2-T^2)T, (S^2-T^2)S, T^3],$$
$$\phi\colon V \to \mathbb{P}^1, \quad \phi = [Y, X].$$

Preslikavanje ψ je morfizam, ali preslikavanje ϕ nije regularno u $P=[0,0,1]$. Nije slučajnost da je točka P singularna točka od V (vidi 1.2.5). Naglašavamo da iako su kompozicije $\phi\circ\psi$ i $\psi\circ\phi$ identitete svuda gdje su definirane, preslikavanja ϕ te ψ nisu izomorfizmi jer ϕ nije morfizam. Mnogostrukosti V i $\mathbb{P}^1$ su biracionalno ekvivalentne (nad $\mathbb{Q}$), ali nisu izomorfne.

1.2. ALGEBARSKE KRIVULJE

Krivulje su projektivne mnogostrukosti pa koristimo rezultate prethodnog poglavlja kako bismo nešto više rekli o njima.

1.2.1. Krivulje i preslikavanja među njima

Definicija 1.2.1. Krivulja C je projektivna mnogostrukost dimenzije jedan.

Propozicija 1.2.2. Neka je $P \in C$ glatka točka na krivulji C. Tada je $\overline{K}[C]_P$ prsten diskretne valuacije (domena glavnih ideala koja sadrži jedinstven maksimalni ideal, ali nije polje).

Dokaz. Iz Propozicije 1.1.6 znamo da je vektorski prostor M_P/M_P^2 jednodimenzionalan nad $\overline{K} = \overline{K}[C]_P/M_P$. Sada koristimo [2, Proposition 9.2]. ■

Valuacija iz prethodne propozicije dana je sa

$$\operatorname{ord}_P\colon \overline{K}[C]_P \to \mathbb{N}_0 \cup \{\infty\}, \quad \operatorname{ord}_P(f) = \sup\{d \in \mathbb{Z}\colon f \in M_P^d\}.$$

Koristeći $\operatorname{ord}_P(f/g) = \operatorname{ord}_P(f) - \operatorname{ord}_P(g)$, možemo proširiti ord_P na $\overline{K}(C)$,

$$\operatorname{ord}_P\colon \overline{K}(C)_P \to \mathbb{Z} \cup \{\infty\}.$$

Uniformizator za C u P je bilo koja funkcija $t \in \overline{K}(C)$ takva da je $\operatorname{ord}_P(t) = 1$, to jest, bilo koji generator ideala M_P.

Definicija 1.2.3. Neka su C i P kao gore te neka je $f \in \overline{K}(C)$. *Red od f u P* je $\operatorname{ord}_P(f)$. Ako je $\operatorname{ord}_P(f) > 0$, kažemo da se *$f$ poništava u P* ili da je P nultočka od f, a ako je $\operatorname{ord}_P(f) < 0$, kažemo da f ima *pol u P*. Ako je $\operatorname{ord}_P(f) \geq 0$, onda je f *regularna* ili *definirana u P* i možemo evaluirati $f(P)$. U suprotnom, f ima pol u P i pišemo $f(P) = \infty$.

Propozicija 1.2.4. Neka je C glatka krivulja te $f \in \overline{K}(C)$ takva da $f \neq 0$. Tada postoji samo konačno točaka na C u kojima f ima pol ili nultočku. Posebno, ako f nema polova onda je konstanta.

Dokaz. Hartshorne [25, I.6.5] nam daje konačnost broja polova. Promatrajući $1/f$ znamo da imamo i konačan broj nultočaka. Posljednju tvrdnju propozicije nam ponovo daje Harthshorne [25, I.3.4a] ■

Propozicija 1.2.5. Neka je C krivulja, $V \subset \mathbb{P}^n$ mnogostrukost, $P \in C$ glatka točka i $\phi : C \to V$ racionalno preslikavanje. Tada je ϕ regularno u P. Posebno, ako je C glatka, onda je ϕ morfizam.

Dokaz. Neka je $\phi = [f_0, \ldots, f_n]$, gdje su $f_i \in \overline{K}(C)$. Odaberimo uniformizator $t \in \overline{K}[C]$ za C u P. Neka je

$$k = \min_{0 \leq i \leq n} \operatorname{ord}_P(f_i).$$

Tada je

$$\operatorname{ord}_P\left(t^{-k} f_i\right) \geq 0 \text{ za svaki } i \quad \text{te} \quad \operatorname{ord}_P\left(t^{-k} f_j\right) = 0 \text{ za neki } j.$$

Svaka funkcija $t^{-k} f_i$ je regularna u P, a $t^{-k} f_j(P) \neq 0$ pa je ϕ regularna u P. ■

Neka su C_1/K te C_2/K krivulje i neka je $\phi : C_1 \to C_2$ nekonstantno racionalno preslikavanje definirano nad K. Operacija komponiranja sa ϕ inducira injekciju funkcijskih polja koja fiksira bazno polje K,

$$\phi^* : K(C_2) \to K(C_1), \quad \phi^* f \mapsto f \circ \phi.$$

Teorem 1.2.6. Neka je $\phi : C_1 \to C_2$ morfizam krivulja. Tada je ϕ konstantno ili surjektivno preslikavanje. Ako je ϕ nekonstantan morfizam definiran nad K gdje su obje krivulje C_1 i C_2 definirane nad K, onda je $K(C_1)$ konačno proširenje polja $\phi^*(K(C_2))$.

Dokaz. Vidi Hartshorne [25, II.6.8]. ■

Definicija 1.2.7. Neka je $\phi : C_1 \to C_2$ morfizam krivulja gdje su C_1, C_2 te ϕ definirani nad K. Ako je ϕ konstantno preslikavanje, kažemo da je *stupanj preslikavanja* ϕ jednak nula, inače kažemo da je ϕ *konačno preslikavanje* i definiramo *stupanj preslikavanja* ϕ sa

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

Definicija 1.2.8. Neka je $\phi : C_1 \to C_2$ nekonstantan morfizam glatkih krivulja i neka je $P \in C_1$. *Indeks grananja (ili stupanj grananja) od ϕ u P,* označen sa $e_\phi(P)$, je broj

$$e_\phi(P) = \operatorname{ord}_P\left(\phi^* t_{\phi(P)}\right),$$

gdje je $t_{\phi(P)} \in K(C_2)$ uniformizator u $\phi(P)$. Primijetimo da je $e_\phi(P) \geq 1$. Kažemo da je ϕ *nerazgranato u P* ako je $e_\phi(P) = 1$ (odnosno *razgranato u P* ako je $e_\phi(P) > 1$) te da je preslikavanje ϕ *nerazgranato*, ako je nerazgranato u svakoj točki na C_1.

Propozicija 1.2.9. Neka je $\phi\colon C_1 \to C_2$ nekonstantan morfizam glatkih krivulja. Tada je za svaki $Q \in C_2$

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$

Dokaz. Vidi Galbraith [22, 8.2.12]. ■

Korolar 1.2.10. Ako je $\phi\colon C_1 \to C_2$ morfizam glatkih krivulja stupnja d i $Q \in C_2(\overline{K})$, onda postoji najviše d točaka $P \in C_1(\overline{K})$ takvih da je $\phi(P) = Q$.

1.2.2. Divizori na krivulji

Divizore koristimo u odjeljku 2.2, kao i u iskazu Riemann-Rochovog teorema.

Definicija 1.2.11. *Grupa divizora krivulje C,* označena sa $\mathrm{Div}\,(C)$ je slobodna Abelova grupa generirana točkama na C. Ekvivalentno, divizor $D \in \mathrm{Div}\,(C)$ je formalna suma

$$D = \sum_{P \in C} n_P(P),$$

gdje su $n_P \in \mathbb{Z}$ i $n_P = 0$ za sve osim konačno mnogo $P \in C$. *Stupanj divizora D* jednak je

$$\deg D = \sum_{P \in C} n_P.$$

Divizori stupnja 0 tvore podgrupu od $\mathrm{Div}\,(C)$ koju označavamo sa

$$\mathrm{Div}^{\,0}(C) = \{D \in \mathrm{Div}\,(C)\colon \deg D = 0\}.$$

Ako je C/K, onda $\mathrm{Gal}(\overline{K}/K)$ djeluje na $\mathrm{Div}\,(C)$ te $\mathrm{Div}^{\,0}(C)$ na prirodan način,

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma).$$

Kažemo da je D *defniran nad K* ako je $D^\sigma = D$, za svaki $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Primijetimo da ako je $D = n_1(P_1) + \cdots + n_r(P_r)$ gdje su $n_i \neq 0$ i D je definiran nad K, nije nužno da su $P_i \in C(K)$. Dovoljno je da $\mathrm{Gal}(\overline{K}/K)$ permutira točke P_i na prikladan način.

Skup divizora definiranih nad K čini *grupu K-racionalnih divizora* označenu sa $\mathrm{Div}_K(C)$, te slično označavamo $\mathrm{Div}^{\,0}_K(C)$, *grupu K-racionalnih divizora stupnja nula.*

Pretpostavimo da je C glatka i neka je $f \in \overline{K}(C)^*$. Tada funkciji f pridružujemo divizor $\operatorname{div}(f)$ dan sa

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)(P).$$

Propozicija 1.2.4 nam kaže da je $\operatorname{div}(f)$ dobro definiran divizor. Ako je $\sigma \in \operatorname{Gal}(\overline{K}/K)$, lako se vidi da je

$$\operatorname{div}(f^\sigma) = (\operatorname{div}(f))^\sigma$$

te da $f \in K(C)$ povlači $\operatorname{div}(f) \in \operatorname{Div}_K(C)$.

Glavni divizor je divizor oblika $D = \operatorname{div}(f)$, za neki $f \in \overline{K}(C)^*$. Suma glavnih divizora $\operatorname{div}(f_1) + \operatorname{div}(f_2)$ je opet glavni divizor $\operatorname{div}(f_1 f_2)$. $\operatorname{Div}(1) = 0$ pa je preslikavanje $K(C)^* \to \operatorname{Div}_K(C)$ dano s $f \mapsto \operatorname{div} f$ homomorfizam, čija je slika *grupa glavnih K-racionalnih divizora,* označena sa $\operatorname{Gl}_K(C)$.

Definicija 1.2.12. Neka je C/K krivulja. Kvocijentna grupa

$$\operatorname{Pic}_K(C) = \operatorname{Div}_K(C)/\operatorname{Gl}_K(C),$$

naziva se *Picardova grupa od C* ili *grupa klasa divizora od C*. Divizori D_1 i D_2 su *linearno ekvivalentni,* označeno sa $D_1 \sim D_2$, ako je $D_1 - D_2 \in \operatorname{Gl}_K(C)$.

Propozicija 1.2.13. Neka je C glatka krivulja i $f \in \overline{K}(C)^*$. Tada je

(a) $\operatorname{div}(f) = 0$ ako i samo ako je $f \in \overline{K}^*$.

(b) $\deg(\operatorname{div}(f)) = 0$.

Dokaz. (a) Ako je $\operatorname{div}(f) = 0$ onda preslikavanje f nema pol pa je prema Propoziciji 1.2.4 konstantno. Obrat je jasan.

(b) Vidi Hartshorne [25, II.6.10].

■

Definicija 1.2.14. Neka je $\phi : C_1 \to C_2$ nekonstantni morfizam glatkih krivulja. *Preslikavanje povlačenja* ili *povlak* ϕ^* na divizorima je homomorfizam $\phi^* : \operatorname{Div}(C_2) \to \operatorname{Div}(C_1)$ definiran sa

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P),$$

gdje je (Q) divizor stupnja jedan točke $Q \in C_2(\overline{K})$. Djelovanje ϕ^* na proizvoljan divizor određeno je po linearnosti.

1.2.3. Diferencijali, genus i Riemann-Rochov teorem

Definicija 1.2.15. Neka je C krivulja. *Prostor (meromorfnih) diferencijalnih formi na C,* ili kraće, *diferencijala na C*, označen sa Ω_C, je $\overline{K}(C)$-vektorski prostor generiran simbolima oblika $\mathrm{d}x$ za $x \in \overline{K}(C)$, modulo sljedeće relacije:

1. $\mathrm{d}(x+y) = \mathrm{d}x + \mathrm{d}y$, za sve $x, y \in \overline{K}(C)$,
2. $\mathrm{d}(xy) = y\mathrm{d}x + x\mathrm{d}y$, za sve $x, y \in \overline{K}(C)$,
3. $\mathrm{d}a = 0$, za svaki $a \in \overline{K}$.

Propozicija 1.2.16. Neka je $P \in C$ točka na krivulji i neka je $t \in \overline{K}(C)$ uniformizator u P.

(a) Za svaki $\omega \in \Omega_C$ postoji jedinstvena funkcija $g \in \overline{K}(C)$, ovisna o ω i t, za koju vrijedi

$$\omega = g\mathrm{d}t.$$

Funkciju g označavamo sa $\omega/\mathrm{d}t$.

(b) Ako je $f \in \overline{K}(C)$ regularna u P, onda je i $\mathrm{d}f/\mathrm{d}t$ regularna u P.

(c) Neka je $\omega \in \Omega_C$ takav da $\omega \neq 0$. Vrijednost

$$\mathrm{ord}_P(\omega/\mathrm{d}t)$$

ovisi samo o ω i P, a neovisna je o izboru uniformizatora t. Tu vrijednost zovemo *red od* ω *u* P i označavamo sa $\mathrm{ord}_P(\omega)$. Vrijedi da je $\mathrm{ord}_P(\omega) = 0$, za sve osim konačno mnogo $P \in C$.

Dokaz. Vidi Silverman [37, II.4.3]. ■

Definicija 1.2.17. Neka je $\omega \in \Omega_C$ diferencijal različit od nule. *Divizor asociran sa* ω je

$$\mathrm{div}\,(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}\,(C).$$

Ako su $\omega_1, \omega_2 \in \Omega_C$ diferencijali različiti od nule, Propozicija 1.2.16 a) implicira da postoji $f \in \overline{K}(C)^*$ takva da je $\omega_1 = f\omega_2$. Shodno tome, vrijedi

$$\mathrm{div}\,(\omega_1) = \mathrm{div}\,(f) + \mathrm{div}\,(\omega_2)$$

pa sljedeća definicija ima smisla.

Definicija 1.2.18. Svaki divizor oblika $\operatorname{div}(\omega)$, gdje je $\omega \in \Omega_C$ zovemo *kanonski divizor*. *Klasa kanonskog divizora na C* je slika od $\operatorname{div}(\omega)$ u $\operatorname{Pic}(C)$.

Definicija 1.2.19. Divizor $D = \sum n_P(P)$ je *efektivan* ili *pozitivan*, označeno sa $D \geq 0$, ako je $n_P \geq 0$ za svaku $P \in C$.

Slično, za bilo koja dva divizora $D_1, D_2 \in \operatorname{Div}(C)$ pišemo $D_1 \geq D_2$ ako je divizor $D_1 - D_2$ efektivan.

Definicija 1.2.20. Divizoru D pridružujemo *Riemann-Rochov prostor* $\mathcal{L}(D)$, definiran sa

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^* \colon \operatorname{div}(f) \geq -D\} \cup \{0\}.$$

Skup $\mathcal{L}(D)$ je konačno dimenzionalan $\overline{K}$-vektorski prostor (vidi Silverman [37][II.5.2.b)] ili Najman [31][6.71, 6.74]) te označavamo njegovu dimenziju sa

$$l(D) = \dim_{\overline{K}} \mathcal{L}(D).$$

Teorem 1.2.21. Postoji $g \in \mathbb{N}_0$ takav da je

$$\deg D + 1 - l(D) \leq g,$$

za svaki $D \in \operatorname{Div}(C)$.

Dokaz. Vidi Najman [31][6.78]. ■

Definicija 1.2.22. Broj

$$g := \max\{\deg D - l(D) + 1 \colon\ D \in \operatorname{Div}(C)\}$$

zovemo *(geometrijski) genus krivulje C*.

Napomena 1.2.23. Postoji i aritmetički genus, ali se za glatke projektivne krivulje vrijednosti geometrijskog i aritmetičkog genusa podudaraju pa zato geometrijski genus jednostavno zovemo genus.

Teorem 1.2.24 (Riemann-Roch)**.** Neka je C glatka krivulja i K_C kanonski divizor na C. Za svaki divizor $D \in \operatorname{Div}(C)$ vrijedi

$$l(D) - l(K_C - D) = \deg D - g + 1.$$

Dokaz. Vidi Hartshorne [25][IV.1.3] ili Najman [31][§6]. ■

1.3. ELIPTIČKE KRIVULJE

Nakon uvoda u algebarsku geometriju, prelazimo na eliptičke krivulje te navodimo poznatu teoriju koju ćemo koristiti u ostatku rada.

Definicija 1.3.1. *Eliptička krivulja* je par $(E,\mathcal{O})$, gdje je E nesingularna krivulja genusa jedan, a $\mathcal{O}\in E$. (Najčešće samo pišemo E, dok se točka $\mathcal{O}$ podrazumijeva.) Kažemo da je E *definirana nad* K, označeno E/K, ako je E definirana nad K kao krivulja te ako je $\mathcal{O}\in E(K)$.

Sljedeća propozicija govori nam kako izgleda jednadžba eliptičke krivulje.

Propozicija 1.3.2. Neka je E/K eliptička krivulja.

(a) Postoje funkcije $x,y\in K(E)$ takve da je preslikavanje

$$\phi: E\to\mathbb{P}^2,\quad \phi=[x,y,1],$$

izomorfizam krivulje E/K na krivulju danu jednadžbom

$$C: Y^2+a_1XY+a_3Y=X^3+a_2X^2+a_4X+a_6 \tag{1.1}$$

s koeficijentima $a_1,\ldots,a_6\in K$ i pritom je $\phi(\mathcal{O})=[0,1,0]$. Funkcije x i y zovemo *(Weierstrassove) koordinatne funkcije,* a jednadžbu 1.1 *Weierstrassovom jednadžbom.*

(b) Svake dvije Weierstrassove jednadžbe za E oblika kao u (1.1) povezane su linearnim zamjenama varijabli oblika

$$X=u^2X'+r,\quad Y=u^3Y'+su^2X'+t,$$

gdje je $u\in K^*$, a r,s i $t\in K$.

(c) Svaka glatka krivulja C koja je zadana Weierstrassovom jednadžbom kao u (a) je eliptička krivulja nad K sa $\mathcal{O}=[0,1,0]$.

Dokaz. Vidi Silverman [37, III.3.1] ili Najman [31, Teorem 98]. Oba dokaza koriste Riemann-Rochov teorem. ■

Jednadžbu (1.1) najčešće možemo pojednostavniti. Ako polje $\overline{K}$ nije karakteristike 2, supstitucija

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

daje nam jednadžbu oblika

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

gdje su konstante b_i dane sa

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

Ujedno definiramo i konstante

$$b_8 = (b_2b_6 - b_4^2)/4, \quad c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Ako polje $\overline{K}$ nije karakteristike 2 niti 3, onda novom supstitucijom

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

možemo dobiti još jednostavniju jednadžbu za E oblika

$$E\colon y^2 = x^3 - 27c_4x - 54c_6.$$

Definiramo dvije bitne konstante vezane uz eliptičku krivulju.

Definicija 1.3.3. *Diskriminanta* Δ *Weierstrassove jednadžbe* te *j-invarijanta eliptičke krivulje* definirane su sa

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728}, \tag{1.2}$$

$$j = j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta} = \frac{c_4^3}{\Delta}. \tag{1.3}$$

Propozicija 1.3.4. Neka su krivulje E i E' dane Weierstrassovim jednadžbama oblika (1.1). Tada vrijedi

(a) (i) Krivulja E je nesingularna ako i samo ako je $\Delta \neq 0$.

(ii) Krivulja E je singularna i ima *čvor* ako i samo ako je $\Delta = 0$ te $c_4 \neq 0$. Postoje dvije različite tangente na krivulju E u čvoru.

(iii) Krivulja E je singularna i ima *kasp* ako i samo ako je $\Delta = 0$ te $c_4 = 0$. Postoji samo jedna tangenta u kaspu.

(b) Krivulje E i E' su izomorfne nad $\overline{K}$ ako i samo ako su im j-invarijante jednake.

(c) Neka je $j_0 \in \overline{K}$. Postoji E'' definirana nad poljem $K(j_0)$ takva da je $j(E'') = j_0$.

Dokaz. Vidi Silverman [37, III.1.4]. ■

Jedno od najbitnijih svojstava eliptičkih krivulja je to da možemo definirati zbrajanje točaka koje eliptičku krivulju čini grupom. Ako je E eliptička krivulja, onda se $E(\overline{K})$ kao podskup od $\mathbb{P}^2(\overline{K})$ sastoji od točaka $P=(x,y)$ koje zadovoljavaju Weierstrassovu jednadžbu te jedinstvene točke $\mathcal{O}=[0,1,0]$ u beskonačnosti. Svaki pravac $l\subset\mathbb{P}^2$ siječe krivulju E u točno tri točke, brojeći kratnost.

Definicija 1.3.5 (Zbrajanje na E)**.** Ako su P i $Q\in E$, neka je l pravac koji prolazi kroz P i Q (posebno, ako je $P=Q$, neka je l tangenta na E u P). Neka je R treća točka presjeka pravca l sa E i neka je l' pravac koji prolazi kroz R i $\mathcal{O}$. Tada l' siječe E u $R,\mathcal{O}$ i trećoj točki koju označavamo sa $P\bigoplus Q$.

Propozicija 1.3.6. Struktura $(E,\bigoplus)$ je Abelova grupa s neutralnim elementom $\mathcal{O}$. Posebno, pretpostavimo da je E definirana nad K i dana jednadžbom (1.1). Tada je skup *K-racionalnih točaka na krivulji* definiran sa

$$E(K)=\{(x,y)\in K^2\colon y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{\mathcal{O}\} \tag{1.4}$$

podgrupa od E.

Dokaz. Vidi Silverman [37, III.2.2]. ■

Napomena 1.3.7. Najteži dio dokaza da je $(E,\bigoplus)$ Abelova grupa je asocijativnost. U [37, III.3.4] je dokazano kako postoji bijekcija $\sigma\colon \mathrm{Pic}^0(E)\to E$ i kako se geometrijski grupovni zakon definiran na E te algebarski grupovni zakon naslijeđen od $\mathrm{Pic}^0(E)$ podudaraju. To dokazuje asocijativnost operacije $\bigoplus$ na više intuitivan način nego čisto računski kao na primjer Propozicija 1.3.8.

U nastavku, zbrajanje (ili oduzimanje) na E jednostavno označavamo sa $+$ (ili $-$). Posebno, za $m\in\mathbb{N}$ i $P\in E$ koristimo oznake

$$[m]P=\underbrace{P+\cdots+P}_{m\ \text{puta}},\quad [-m]P=-[m]P,\quad [0]P=\mathcal{O}.$$

Zbrajanje na E možemo opisati eksplicitnim jednadžbama.

Propozicija 1.3.8. Neka je E eliptička krivulja zadana jednadžbom (1.1).

(a) Neka je $P_0 = (x_0, y_0)$. Tada je

$$-P_0 = (x_0, -y_0 - a_1 x_0 - a_3).$$

(b) Pretpostavimo da je

$$P_1 + P_2 = P_3 \quad \text{gdje je} \quad P_i = (x_i, y_i) \in E, \text{ za } i = 1, 2, 3.$$

Ako je $x_1 = x_2$ i $y_1 + y_2 + a_1 x_2 + a_3 = 0$ onda je $P_1 + P_2 = \mathcal{O}$. Inače, definiramo brojeve λ i ν sljedećim formulama:

uvjet na x	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1 x_2 - x_1 y_2}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$	$\dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$

Tada je $y = \lambda x + \nu$ pravac koji prolazi kroz P_1 i P_2, a ako je $P_1 = P_2$, onda je tangenta na E u P_1.

(c) Uz notaciju kao u (b), točka $P_3 = P_1 + P_2$ ima koordinate

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Dokaz. Vidi Silverman [37, III.2.3]. ■

Teorem 1.3.9 (Mordell-Weil)**.** Neka je k konačno proširenje od $\mathbb{Q}$ te neka je $K = k$ ili $K = k(u)$, polje racionalnih funkcija nad k. Skup K-racionalnih točaka $E(K)$ je konačno generirana Abelova grupa.

Strukturni teorem za konačno generirane Abelove grupe nam kaže da je

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

gdje je $r \in \mathbb{N}_0$, a $E(K)_{\text{tors}}$ je grupa elemenata konačnog reda. Broj r zovemo *rang eliptičke krivulje* E, a podgrupu $E(K)_{\text{tors}}$ *torzijskom podgrupom.*

Napomena 1.3.10. Slučaj $K = \mathbb{Q}$ dokazao je Mordell, slučaj kada je K polje algebarskih brojeva dokazao je Weil, a slučaj $K = k(u)$ dokazao je Néron. Slučaj kada je K polje algebarskih brojeva je teorem [37, VIII.6.7], ali zapravo cijelo VIII. poglavlje vodi do tog dokaza. Za $K = k(u)$ vidi [36, III.6.1,III.6.2.2].

Definicija 1.3.11. Neka je E/K eliptička krivulja. Kažemo da su K-racionalne točke $P_1, \ldots, P_n \in E(K)$ *linearno zavisne nad* $\mathbb{Z}$ ako postoje $m_1, \ldots, m_n \in \mathbb{Z}$ takvi da je

$$[m_1]P_1 + \cdots + [m_n]P_n = T,$$

gdje je T torzijska točka, to jest, $T \in E(K)_{\text{tors}}$. U suprotnom kažemo da su točke $P_1, \ldots, P_n \in E(K)$ *linearno nezavisne nad* $\mathbb{Z}$.

Neka je $\mathbb{Q}(u)$ polje racionalnih funkcija nad $\mathbb{Q}$ u varijabli u i neka je $E/\mathbb{Q}(u)$ eliptička krivulja. Pretpostavimo da ne postoji eliptička krivulja $E_0/\mathbb{Q}$ zajedno s izomorfizmom krivulja $\phi : E \to E_0$ definiranim nad $\mathbb{Q}(u)$. Želimo definirati visinsku funkciju na $E(\mathbb{Q}(u))$.

Definicija 1.3.12. *Visina elementa* $f \in \mathbb{Q}(u)$ je stupanj pridruženog preslikavanja

$$h(f) = \deg(f : \mathbb{P}^1 \to \mathbb{P}^1).$$

Ako je f konstantna funkcija uzimamo da je $h(f) = 0$.

Neka je $E/\mathbb{Q}(u)$ eliptička krivulja zadana Weierstrassovom jednadžbom oblika (1.1). *Visinu točke* $P \in E(\mathbb{Q}(u))$ definiramo kao

$$h(P) = \begin{cases} 0, & \text{ako je } P = \mathcal{O}, \\ h(x), & \text{ako je } P = (x, y). \end{cases}$$

Teorem 1.3.13. (a) Za svaku točku $P \in E(\mathbb{Q}(u))$ postoji limes

$$\hat{h}(P) = \frac{1}{2} \lim_{n \to \infty} \frac{1}{4^n} h([2^n]P).$$

Vrijednost $\hat{h}(P)$ nazivamo *kanonska ili Néron-Tateova visina od P.*

(b) Preslikavanje $\hat{h}$ je kvadratna forma na $E(\mathbb{Q}(u))$. Drugim riječima, vrijedi $\hat{h}(P) = \hat{h}(-P)$ i *Néron-Tateovo sparivanje*

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}(u)) \times E(\mathbb{Q}(u)) \to \mathbb{R}, \text{ definirano sa}$$

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)$$

je bilinearno simetrično sparivanje. Preciznije, to je sparivanje za koje vrijedi

(i) $\langle P,Q\rangle = \langle Q,P\rangle$, za sve $P,Q \in E(\mathbb{Q}(u))$,

(ii) za sve P,Q i $R \in E(\mathbb{Q}(u))$ te m i $n \in \mathbb{Z}$ vrijedi

$$\langle P,[m]Q+[n]R\rangle = m\langle P,Q\rangle + n\langle P,R\rangle.$$

Néron-Tateovo sparivanje ima još jedno bitno svojstvo:

(iii) Neka je $P \in E(\mathbb{Q}(u))$. Tada je $\langle P,P\rangle \geq 0$ i posebno

$$\langle P,P\rangle = 0, \text{ ako i samo ako je } P \text{ torzijska točka.}$$

Dokaz. Vidi Silverman [36, III.4.3,III.§4]. ■

Definicija 1.3.14. Neka su $P_1,\ldots,P_r \in E(\mathbb{Q}(u))$. *Matrica eliptičke visine* pridružena točkama $\{P_i\}_{i=1}^r$ je

$$\mathcal{H} = \mathcal{H}(\{P_i\}_{i=1}^r) := (\langle P_i,P_j\rangle)_{\substack{1\leq i\leq r,\\ 1\leq j\leq r}}.$$

Determinantu matrice $\mathcal{H}$ zovemo *eliptički regulator* točaka $\{P_i\}_{i=1}^r$.

Korolar 1.3.15. Neka je $E/\mathbb{Q}(u)$ eliptička krivulja te neka su $P_1,\ldots,P_r \in E(\mathbb{Q}(u))$. Neka je $\mathcal{H}$ matrica eliptičke visine pridružena točkama $\{P_i\}_{i=1}^r$.

(i) Pretpostavimo da je $\det\mathcal{H} = 0$ i neka je $v = (n_1,\ldots,n_r) \in \mathrm{Ker}(\mathcal{H})$ takav da su $n_i \in \mathbb{Z}$. Tada su točke $\{P_i\}_{i=1}^r$ linearno zavisne i vrijedi

$$\sum_{i=1}^{r}[n_i]P_i = T, \text{ gdje je } T \text{ torzijska točka.}$$

(ii) Ako je $\det\mathcal{H} \neq 0$, onda su točke $\{P_i\}_{i=1}^r$ linearno nezavisne i rang Mordell-Weilove grupe od $E(\mathbb{Q}(u))$ je barem r.

Neka je sada $E/\mathbb{Q}$ krivulja zadana Weierstrassovom jednadžbom oblika (1.1). Kažemo da je model od $E/\mathbb{Q}$

$$E\colon y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6, \tag{1.5}$$

minimalan, ako su $a_i \in \mathbb{Z}$ te ako je $|\Delta(E)|$ minimalna u klasi izomorfizama od E.

Definicija 1.3.16. Neka je $E/\mathbb{Q}$ zadana minimalnim modelom (1.5) te neka je zadan prost broj p. Tada definiramo $\overline{E}/\mathbb{F}_p$, *redukciju* mod p *od* E sa

$$\overline{E}\colon y^2+\overline{a}_1xy+\overline{a}_3y = x^3+\overline{a}_2x^2+\overline{a}_4x+\overline{a}_6,$$

gdje su $\overline{a}_i \in \mathbb{F}_p$ takvi da je $\overline{a}_i = a_i \bmod p$.

Lako se vidi da je $\overline{E}/\mathbb{F}_p$ eliptička krivulja ako i samo ako nije singularna nad $\mathbb{F}_p$, što je istina ako i samo ako $p \nmid \Delta(E)$.

Definicija 1.3.17. Ako je redukcija mod p od E eliptička krivulja, kažemo da E ima *dobru redukciju u p.* Inače, ako E nema dobru redukciju u p, kažemo da E ima *lošu redukciju u p.* Ako je singularitet kasp, kažemo da E ima *aditivnu redukciju.* Ako je singularitet čvor kažemo da E ima *multiplikativnu redukciju.* Posebno, ako je čvor takav da su koeficijenti smjerova tangenti u čvoru u $\mathbb{F}_p$ različiti, kažemo da E ima *rascjepivu multiplikativnu redukciju,* a inače ima *nerascjepivu multiplikativnu redukciju*

Napomena 1.3.18. Diskriminanta $\Delta(E)$ ima samo konačno mnogo prostih faktora pa svaka eliptička krivulja E ima lošu redukciju u samo konačno mnogo prostih brojeva p.

L-funkcija eliptičke krivulje je funkcija koja nam daje globalne informacije o eliptičkoj krivulji iz lokalnih informacija.

Neka je $E/\mathbb{Q}$ zadana minimalnim modelom. Definiramo brojeve a_p na sljedeći način:

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

Definicija 1.3.19. *L-funkcija eliptičke krivulje* $E/\mathbb{Q}$ dana je sa

$$L_E(s) = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s} + p^{1-2s}} \prod_{p \mid \Delta(E)} \frac{1}{1 - a_p \cdot p^{-s}}. \tag{1.6}$$

Desna strana jednadžbe (1.6) može se razviti u red te vrijedi

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

Prirodno područje konvergencije ovog reda su svi kompleksni brojevi s čiji je realni dio veći od $3/2$, što slijedi iz Hasseovog teorema [37, V.1.1]. Jedna od posljedica Teorema o modularnosti je da postoji analitičko proširenje od $L_E(s)$ na cijelu kompleksnu ravninu $\mathbb{C}$. Posebno je bitna vrijednost $L_E(s)$ u $s = 1$.

Definicija 1.3.20. Red nultočke $L_E(s)$ u $s = 1$ naziva se *analitički rang od E*

Vrijednost koju smo definirali u Teoremu 1.3.9 naziva se i *algebarski rang od* $E/\mathbb{Q}$. Sljedeća slutnja (u najjednostavnijem obliku) je jedan od najvažnijih otvorenih matematičkih problema.

Slutnja 1.3.21 (Slutnja Bircha i Swinnerton-Dyera)**.** Neka je $E/\mathbb{Q}$ eliptička krivulja. Tada su njen algebarski i analitički rang jednaki.

Napomena 1.3.22. Zainteresiranog čitatelja upućujemo na [30, §18] te [29, §5].

2. RACIONALNE $D(q)$-ČETVORKE

U ovom poglavlju opisujemo racionalne $D(q)$-četvorke čiji je umnožak elemenata jednak m. Parametriziramo sve m, u ovisnosti o q, za koje takva četvorka postoji. Za svaki m za koji postoji racionalna $D(q)$-četvorka umnoška elemenata jednakog m, parametriziramo sve takve četvorke pomoću trojki točaka na eliptičkoj krivulji E_m, čija jednadžba ovisi o q i m.

2.1. VEZA ČETVORKI I ELIPTIČKIH KRIVULJA

Koristimo sličan pristup koji su imali Dujella i Kazalicki u [15], [14].

Neka je q racionalan broj različit od nule te neka je $\{a,b,c,d\}$ racionalna $D(q)$-četvorka, takva da je

$$ab+q=t_{12}^2, \quad ac+q=t_{13}^2, \quad ad+q=t_{14}^2,$$
$$bc+q=t_{23}^2, \quad bd+q=t_{24}^2, \quad cd+q=t_{34}^2.$$

Tada $(t_{12},t_{13},t_{14},t_{23},t_{24},t_{34},m=abcd)\in\mathbb{Q}^7$ određuje racionalnu točku na algebarskoj mnogostrukosti $\mathcal{C}$ definiranoj jednadžbama

$$(t_{12}^2-q)(t_{34}^2-q)=m,$$
$$(t_{13}^2-q)(t_{24}^2-q)=m,$$
$$(t_{14}^2-q)(t_{23}^2-q)=m.$$

Racionalne točke $(\pm t_{12},\pm t_{13},\pm t_{14},\pm t_{23},\pm t_{24},\pm t_{34},m)$ na $\mathcal{C}$ određivat će dvije racionalne $D(q)$-četvorke $\pm(a,b,c,d)$ $\left(\text{posebno, } a^2=\frac{(t_{12}^2-q)(t_{13}^2-q)}{t_{23}^2-q}\right)$ ako su a,b,c i d *racionalni*, *međusobno različiti* te *različiti od nule*.

Svaka točka $(t_{12},t_{13},t_{14},t_{23},t_{24},t_{34},m)$ na $\mathcal{C}$ daje nam tri točke $Q_1'=(t_{12},t_{34}),Q_2'=(t_{13},t_{24})$ i $Q_3'=(t_{14},t_{23})$ na krivulji

$$\mathcal{D}_m\colon (x^2-q)(y^2-q)=m.$$

Ako je $\mathcal{D}_m(\mathbb{Q}) = \emptyset$, tada ne postoji racionalna $D(q)$-četvorka s umnoškom elemenata jednakim m, zato pretpostavljamo da postoji točka $P_1 = (x_1, y_1) \in \mathcal{D}_m(\mathbb{Q})$. Zanimljiv je problem odrediti za koje m je skup $\mathcal{D}_m(\mathbb{Q})$ neprazan, ali mi se ne bavimo time nego jednostavno pretpostavljamo da je $\mathcal{D}_m(\mathbb{Q})$ neprazan.

Prvo ćemo riješiti jedan poseban slučaj.

Lema 2.1.1. Neka je $\{a,b,c,d\}$ racionalna $D(q)$-četvorka takva da je $abcd = q^2$. Tada je $q = q_1^2$, za neki $q_1 \in \mathbb{Q}$.

Dokaz. Neka je $ab+q = t_1^2$ te $cd+q = t_2^2$. Tada je

$$qt_1^2 = q(q+ab) = q^2+qab = abcd+qab = ab(cd+q) = abt_2^2$$

pa je broj abq potpun kvadrat. Slično zaključujemo da su brojevi acq te adq potpuni kvadrati. Tada je i njihov umnožak

$$\square = (abq)(acq)(adq) = (abcd)a^2q^3 = q^2a^2q^3 = (q^2a)^2q$$

potpun kvadrat pa q mora biti potpun kvadrat. ■

Propozicija 2.1.2. Neka je $\{a,b,c,d\}$ racionalna $D(q^2)$-četvorka takva da je $abcd = q^4$. Sve takve četvorke parametrizirane su sa

$$a = qxyz, \quad b = \frac{qx}{yz}, \quad c = \frac{qy}{xz}, \quad d = \frac{qz}{xy},$$

gdje su

$$x = \frac{t_1^2-1}{2t_1}, \quad y = \frac{t_2^2-1}{2t_2}, \quad z = \frac{t_3^2-1}{2t_3}$$

za racionalne brojeve t_1, t_2 i t_3 takve da je

$$t_i \notin \{-1,0,1\}, \quad t_it_j \neq \pm 1, \quad t_i \neq \pm t_j, \quad t_i \neq \pm\frac{t_j+1}{t_j-1}, \quad t_i \neq \pm\frac{t_j-1}{t_j+1}.$$

za sve $i, j \in \{1,2,3\}$, $i \neq j$.

Dokaz. Slično kao u dokazu prethodne leme imamo

$$ab(cd+q^2) = abcd+abq^2 = q^4+abq^2 = q^2(ab+q^2)$$

pa budući da su $cd+q^2$ te $ab+q^2$ kvadrati, broj ab također mora biti potpun kvadrat. Isto vrijedi i za brojeve ac te ad. Neka su $x, y, z \in \mathbb{Q}$ takvi da je

$$ab = (qx)^2, \quad ac = (qy)^2, \quad ad = (qz)^2.$$

Vrijedi

$$a^2q^4 = a^2(abcd) = (ab)(ac)(ad) = q^6x^2y^2z^2,$$

to jest

$$a = qxyz \quad \Longrightarrow \quad b = \frac{qx}{yz}, \quad c = \frac{qy}{xz}, \quad d = \frac{qz}{xy}.$$

Broj $ab+q^2 = q^2x^2+q^2 = q^2(x^2+1)$ mora biti potpun kvadrat pa je $x = \dfrac{t_1^2-1}{2t_1}$ za neki $t_1 \in \mathbb{Q}$. Ujedno je

$$cd+q^2 = \frac{q^2}{x^2}+q^2 = \frac{q^2}{x^2}(1+x^2) = \square.$$

Slično vidimo da mora biti

$$y = \frac{t_2^2-1}{2t_2}, \quad z = \frac{t_3^2-1}{2t_3},$$

za neke $t_2, t_3 \in \mathbb{Q}$.

Brojevi a,b,c,d moraju biti racionalni brojevi koji su različiti od nule pa je nužno je da je $xyz \neq 0$. Moraju biti i međusobno različiti, a iz tih uvjeta slijedi

$$xy \neq \pm 1, \quad xz \neq \pm 1, \quad yz \neq \pm 1, \quad x \neq \pm y, \quad x \neq \pm z, \quad y \neq \pm z.$$

Nadalje, vrijedi

$$0 \neq x \in \mathbb{Q} \quad \Longleftrightarrow \quad t_1 \notin \{-1,0,1\},$$

$$x \neq \pm y \quad \Longleftrightarrow \quad t_1 \neq \pm t_2 \quad \text{i} \quad t_1t_2 \neq \pm 1,$$

kao i

$$xy \neq \pm 1 \quad \Longleftrightarrow \quad t_1 \neq \pm\frac{t_2+1}{t_2-1} \quad \text{i} \quad t_1 \neq \pm\frac{t_2-1}{t_2+1}.$$

Analizirajući

$$0 \neq y \in \mathbb{Q}, \quad 0 \neq z \in \mathbb{Q}, \quad xz \neq \pm 1, \quad yz \neq \pm 1, \quad x \neq \pm z, \quad y \neq \pm z$$

Dobijemo i preostale uvjete na t_i navedene u iskazu propozicije. ■

Vratimo se natrag na općeniti slučaj. Budući da smo pretpostavili postojanje racionalne točke $P_1 = (x_1, y_1) \in \mathcal{D}_m$, krivulja $\mathcal{D}_m$ je biracionalno ekvivalentna krivulji

$$E_m \colon W^2 = T^3 + (4q^2-2m)T^2 + m^2T$$

preko preslikavanja $f \colon \mathcal{D}_m \to E_m$, koje je dano sa $(x,y) \mapsto (T,W)$, gdje je

$$T = (y_1^2-q)\frac{2x_1(y^2-q)x + (x_1^2+q)y^2 + x_1^2y_1^2 - 2x_1^2q - y_1^2q}{(y-y_1)^2},$$

$$W = 2T\,\frac{y_1x(q-y^2) + x_1y(q-y_1^2)}{y^2-y_1^2}.$$

Generički genus krivulje E_m je jedan, a biti će jednak nula jedino onda kada polinom

$$T^3+(4q^2-2m)T^2+m^2T=T(T^2+T(4q^2-2m)T+m^2)$$

ima dvostruku nultočku. Jedna mogućnost je da je 0 dvostruka nultočka, što povlači $m=0$, a druga je

$$(4q^2-2m)^2-4m^2=0 \quad \Longleftrightarrow \quad q^2(q^2-m)=0.$$

pa je u tom slučaju $m=q^2$.

Slučaj $m=0$ nam nije zanimljiv jer tada nemamo racionalne $D(q)$-četvorke čiji je umnožak jednak m (jedan od elemenata četvorke bi morao biti nula). Slučaj $m=q^2$ smo riješili pomoću Leme 2.1.1 i Propozicije 2.1.2 pa odsad nadalje pretpostavljamo da m nije jednak niti 0 niti q^2. Krivulja E_m je sada uvijek eliptička krivulja.

Koristeći Magmu [4] (kod u Odjeljku 5.1.1), izračunali smo da f preslikava $P_1=(x_1,y_1)$ u točku u beskonačnosti $\mathcal{O}\in E_m(\mathbb{Q})$, točku $(-y_1,x_1)$ u točku reda četiri, $R=(m,2mq)\in E_m(\mathbb{Q})$ te točku $(-x_1,y_1)$ u

$$S=\left(\frac{y_1^2(x_1^2-q)^2}{x_1^2},\frac{qy_1(x_1^2+y_1^2)(x_1^2-q)^2}{x_1^3}\right)\in E_m(\mathbb{Q}),$$

koja je generički beskonačnog reda.

Uspostavili smo vezu:

$$(a,b,c,d) \dashleftarrow\dashrightarrow \text{točka na } \mathcal{C}(\mathbb{Q}) \dashleftarrow\dashrightarrow (Q_1',Q_2',Q_3')\in\mathcal{D}_m(\mathbb{Q})^3.$$

Kako bi se iz neke trojke točaka na $\mathcal{D}_m(\mathbb{Q})$ zaista mogli vratiti u racionalnu $D(q)$-četvorku, moramo zadovoljiti uvjete koje smo naveli maloprije: brojevi a,b,c i d moraju biti racionalni, međusobno različiti te različiti od nule.

Lako se vidi da ako je jedan od njih racionalan da su i preostala tri (na primjer $b=\frac{t_{12}^2-q}{a}$) te da su različiti od nule čim je $m\neq 0$, jer je $m=abcd$.

Elementi četvorke (a,b,c,d) vezani uz trojku (Q_1',Q_2',Q_3') bit će međusobno različiti ako i samo ako se nikoje dvije od točaka (Q_1',Q_2',Q_3') ne mogu dobiti jedna iz druge zamjenom koordinata i/ili zamjenom predznaka neke od koordinata. Na primjer za $((t_{12},t_{34}),(-t_{34},t_{12}),(t_{14},t_{23}))$ imamo $a=d$. Ovaj uvjet na točke u $\mathcal{D}_m$ razumijemo i na točkama na krivulji E_m.

Ako je $P\in E_m\leftrightarrow(x,y)\in\mathcal{D}_m$, to jest, $f(x,y)=P$, onda je

$$S-P\leftrightarrow(-x,y), \quad P+R\leftrightarrow(-y,x). \tag{2.1}$$

Preslikavanja $P \mapsto S - P$ te $P \mapsto P + R$ generiraju grupu G automorfizama na E_m izomorfnu sa D_8, dihedralnom grupom reda 8. Grupa G inducira djelovanje na $E_m(\overline{\mathbb{Q}})$.

Da bi iz trojke $(Q_1, Q_2, Q_3) \in (E_m(\mathbb{Q}))^3$ dobili četvorku čiji su elementi različiti, orbite $G \cdot Q_1, G \cdot Q_2, G \cdot Q_3$ moraju biti disjunktne. To vrijedi jer je skup točaka u $\mathcal{D}_m$ koje odgovaraju skupu $G \cdot P$ točno $\{(\pm x, \pm y), (\pm y, \pm x)\}$.
Kažemo da takva trojka točaka na E_m zadovoljava *kriterij nedegeneriranosti.* Diskusiju o racionalnosti nastaviti ćemo u Odjeljku 2.3.

2.2. PRESLIKAVANJE g

Neka je $\overline{\mathcal{D}}_m$ projektivno zatvorenje krivulje $\mathcal{D}_m$ određeno jednadžbom

$$\overline{\mathcal{D}}_m \colon (X^2 - qZ^2)(Y^2 - qZ^2) = mZ^4.$$

Preslikavanje $f^{-1} \colon E_m \to \overline{\mathcal{D}}_m$ je racionalno preslikavanje, a budući da je E_m glatka krivulja, ono je morfizam [37, II.2.1]. Preslikavanje $x \circ f^{-1} : E_m \to \mathbb{A}^1$ dano sa

$$x \circ f^{-1}(P) = \frac{X \circ f^{-1}(P)}{Z \circ f^{-1}(P)},$$

ima pol u točkama P_0 za koje vrijedi $f^{-1}(P_0) = [1:0:0]$, a regularno je u svim ostalim točkama. To nije evidentno za točke P_2 takve da je $f^{-1}(P_2) = [0:1:0]$ pa pokažimo regularnost u takvim točkama. Neka je $t \in \overline{\mathbb{Q}}(E_m)$ uniformizator za E_m u P_2. Tada je $X \circ f^{-1} = t^{n_X} f_X$, $Y \circ f^{-1} = f_Y$, $Z \circ f^{-1} = t^{n_Z} f_Z$ za neke $f_X, f_Y, f_Z \in \overline{\mathbb{Q}}(E_m)$ koje P_2 ne poništava i prirodne brojeve n_X, n_Z. Iz jednadžbe krivulje $\overline{\mathcal{D}}_m$ slijedi

$$(t^{2n_X} \cdot (f_X)^2 - q \cdot t^{2n_Z} \cdot (f_Z)^2) \cdot ((f_Y)^2 - q \cdot t^{2n_Z} \cdot (f_Z)^2) = m \cdot t^{4n_Z} \cdot (f_Z)^4. \tag{2.2}$$

Neka je $M = \min\{2n_X, 2n_Z\}$. Nakon što podijelimo obje strane jednakosti (2.2) sa t^M, vidimo da P_2 i dalje poništava desnu stranu pa mora poništavati i lijevu. To će jedino biti moguće ako vrijedi $n_X = n_Z$. Zato vrijedi $x \circ f^{-1}(P_2) = \dfrac{f_X(P_2)}{f_Z(P_2)}$. Na sličan način vidimo da preslikavanje $y \circ f^{-1} \colon E_m \to \mathbb{A}^1$ dano sa

$$y \circ f^{-1}(P) = \frac{Y \circ f^{-1}(P)}{Z \circ f^{-1}(P)},$$

ima pol u svakoj točki P_2 za koju vrijedi $f^{-1}(P_2) = [0:1:0]$ i da je regularno u svim ostalim točkama (posebno, u svakoj točki P_0 za koju vrijedi $f^{-1}(P_0) = [1:0:0]$.)

Definiramo racionalno preslikavanje $g\colon E_m \to \mathbb{A}^1$ sa

$$g(P) = (x_1^2 - q) \cdot \left(\left(x \circ f^{-1}(P) \right)^2 - q \right).$$

Preslikavanje g ima polove u istim točkama kao i $x \circ f^{-1}$, a regularno je u ostalim točkama.

Preslikavanja f i g ovise o fiksnoj točki $P_1 \in \mathcal{D}_m(\mathbb{Q})$. U notaciji izostavljamo tu ovisnost i te funkcije zovemo f i g. Motivacija preslikavanja g je [14, 2.4, Proposition 4]. Dujella i Kazalicki u dokazu Propozicije 4 koriste 2-spust homomorfizam, mi ćemo u slične svrhe koristiti g. Analiziramo svojstva ovog preslikavanja.

Propozicija 2.2.1. Divizor preslikavanja g je

$$\operatorname{div} g = 2(S_1) + 2(S_2) - 2(R_1) - 2(R_2),$$

gdje su S_1, R_1, S_2, R_2 točke u $E_m(\mathbb{Q}(\sqrt{q}))$ s koordinatama

$$\begin{aligned}
S_1 &= (\ (y_1^2 - q)(x_1 - \sqrt{q})^2, \quad 2y_1\sqrt{q}\ (y_1^2 - q)(x_1 - \sqrt{q})^2\ ), \\
R_1 &= (\ (x_1^2 - q)(y_1 + \sqrt{q})^2, \quad 2x_1\sqrt{q}\ (x_1^2 - q)(y_1 + \sqrt{q})^2\ ), \\
S_2 &= (\ (y_1^2 - q)(x_1 + \sqrt{q})^2, \ -2y_1\sqrt{q}\ (y_1^2 - q)(x_1 + \sqrt{q})^2\ ), \\
R_2 &= (\ (x_1^2 - q)(y_1 + \sqrt{q})^2, \ -2x_1\sqrt{q}\ (x_1^2 - q)(y_1 - \sqrt{q})^2\ ).
\end{aligned}$$

Točke S_1, S_2, R_1 te R_2 zadovoljavaju sljedeće jednakosti:

$$\begin{aligned}
2S_1 = 2S_2 &= f(x_1, -y_1) = S + 2R, \\
2R_1 = 2R_2 &= f(-x_1, y_1) = S, \\
S_1 + R = R_1, \quad R_1 + R = S_2, \quad S_2 + R &= R_2, \quad R_2 + R = S_1.
\end{aligned}$$

Dokaz. Tražimo nultočke i polove preslikavanja g. Polovi preslikavanja g su isti kao i polovi preslikavanja $x \circ f^{-1}$. Kako bi našli nultočke od g, primijetimo da je

$$(x \circ f^{-1}(P))^2 - q = \frac{m}{(y \circ f^{-1}(P))^2 - q},$$

dakle samo trebamo saznati polove od $y \circ f^{-1}$.

Nultočke preslikavanja $x \circ f^{-1}$ su točke na E_m koje se preslikaju u točke na $\overline{\mathcal{D}}_m$ koje imaju x-koordinatu jednaku nula. Možemo ih jednostavno eksplicitno izračunati, ako je $x = 0$, onda je $y^2 = \frac{q^2 - m}{q}$. Označimo $K = \sqrt{\frac{q^2 - m}{q}}$. Znamo da $K \neq 0$ jer $m \neq q^2$.

Nultočke preslikavanja $x \circ f^{-1}$ su točke $f(0, K), f(0, -K) \in E_m(\overline{\mathbb{Q}})$ i one su različite jer $K \neq 0$. Budući da je $x \circ f^{-1}$ stupnja 2, obje nultočke su reda 1. Zaključujemo da $x \circ f^{-1}$ ima ili jedan dvostruki pol ili dva jednostruka pola.

Slično, nultočke preslikavanja $y \circ f^{-1}$ su točke $f(K,0), f(-K,0) \in E_m(\overline{\mathbb{Q}})$ i obje su nultočke reda 1. Zaključujemo da $y \circ f^{-1}$ ima ili jedan dvostruki pol ili dva jednostruka pola.

Pretpostavimo da se točka $P_0 \in E_m$ preslika u točku u beskonačnosti na $\overline{\mathcal{D}}_m$, to jest, u točku koja nije afina. Projektivno, to znači da je $Z \circ f^{-1}(P_0) = 0$ i da barem jedna od projektivnih koordinatnih funkcija $X \circ f^{-1}, Y \circ f^{-1}$ ima u točki P_0 vrijednost različitu od nule. Neka je to, bez smanjenja općenitosti, $X \circ f^{-1}$. Tada preslikavanje $x \circ f^{-1} = \dfrac{X \circ f^{-1}}{Z \circ f^{-1}}$ ima pol u točki P_0.

Neka je točka $P_0 \in E_m$ pol jedne od funkcija $x \circ f^{-1}, y \circ f^{-1}$. Niti jedna od točaka $f^{-1}(P_0)$, $f^{-1}(P_0+R), f^{-1}(P_0+2R), f^{-1}(P_0+3R)$ ne može biti afina točka na $\overline{\mathcal{D}}_m$ jer kada bi jedna od njih bila takva točka, onda bi sve bile, zbog (2.1). Naime, ako je $g_0 \in G$ i $A \in \mathcal{D}_m$ afina točka, onda je i $f^{-1} \circ g \circ f(A)$ opet afina točka. Zaključujemo da je svaka od točaka $P_0, P_0 + R, P_0 + 2R, P_0 + 3R$ pol jedne od funkcija $x \circ f^{-1}, y \circ f^{-1}$ te zajedno s prethodnim argumentima zaključujemo da preslikavanja $x \circ f^{-1}, y \circ f^{-1}$ oba imaju po dva jednostruka pola.

Slično kao maloprije, točke $f^{-1}(S-P_0), f^{-1}(S-P_0+R), f^{-1}(S-P_0+2R), f^{-1}(S-P_0+3R)$ nisu afine u $\overline{\mathcal{D}}_m$, jer bi onda i $f^{-1}(P_0)$ bila. Skupovi $\{P_0, P_0+R, P_0+2R, P_0+3R\}$ te $\{S-P_0, S-P_0+R, S-P_0+2R, S-P_0+3R\}$ moraju biti jednaki, inače bi preslikavanja $x \circ f^{-1}, y \circ f^{-1}$ imala više od četiri različita pola. To znači da svaki pol zadovoljava jednakost $2P_0 = S + kR$ za neki $k \in \{0,1,2,3\}$. Ekvivalentno, svaki pol P_0 je fiksna točka neke involucije i_k oblika $P \mapsto S - P + kR$. Svaka involucija i_k ima četiri fiksne točke na $E_m(\overline{\mathbb{Q}})$, jer se bilo koje dvije fiksne točke od i_k, recimo P' i P'', razlikuju za neki element iz $[2]$-torzije što vidimo iz

$$2(P'-P'') = 2P' - 2P'' = S - kR - (S - kR) = 0.$$

Involucija i_0, promatrana na $\overline{\mathcal{D}}_m$, šalje afinu točku $(x,y) = f^{-1}(P)$ u $(-x,y) = f^{-1}(S-P)$. Ona ima dvije afine fiksne točke koje na $\overline{\mathcal{D}}_m$ imaju x-koordinatu jednaku nula, kao i dvije fiksne točke koje nisu afine na $\overline{\mathcal{D}}_m$. Takve neafine točke su polovi preslikavanja $x \circ f^{-1}$ ili polovi preslikavanja $y \circ f^{-1}$. Koristeći računalni program Magma [4](kod u Odjeljku 5.1.2), računamo koordinate tih točaka te dolazimo do R_1 i R_2. Računski provjeravamo da su R_1 te R_2 polovi preslikavanja $x \circ f^{-1}$, odnosno polovi preslikavanja g.

Involucija i_2, promatrana na $\overline{\mathcal{D}}_m$, šalje afinu točku $(x,y) = f^{-1}(P)$ u $(x,-y) = f^{-1}(S-P+2R)$. Ona ima dvije afine fiksne točke koje na $\overline{\mathcal{D}}_m$ imaju y-koordinatu jednaku nula, kao i dvije fiksne točke koje nisu afine na $\overline{\mathcal{D}}_m$. Te neafine točke moraju biti polovi funkcije $y \circ f^{-1}$, odnosno nultočke funkcije g. Opet, koristeći Magmu, računamo koordinate te dolazimo do S_1 i S_2.

Budući da su polovi preslikavanja $x \circ f^{-1}$ reda 1, onda su polovi preslikavanja g reda 2. Isto vrijedi i za polove preslikavanja $y \circ f^{-1}$, shodno tome i za nultočke preslikavanja g.

■

Prilikom testiranja svojstava preslikavanja g pomoću računala, uočeno je zanimljivo i korisno svojstvo, g preslikava dvostruke točke iz $E_m(\mathbb{Q})$ u potpune kvadrate. To je motiviralo sljedeću propoziciju.

Propozicija 2.2.2. Postoji $h \in \mathbb{Q}(E_m)$ takvo da je $g \circ [2] = h^2$.

Dokaz. Neka je $\tilde{h} \in \overline{\mathbb{Q}}(E_m)$ takvo da je

$$\begin{aligned}\operatorname{div}\tilde{h} &= [2]^*((S_1)+(S_2)-(R_1)-(R_2)) \\ &= \sum_{T\in E_m[2]}(S_1'+T)+\sum_{T\in E_m[2]}(S_2'+T)-\sum_{T\in E_m[2]}(R_1'+T)-\sum_{T\in E_m[2]}(R_2'+T), \qquad (2.3)\end{aligned}$$

gdje su $S_i', R_i' \in E_m(\overline{\mathbb{Q}})$ neke točke takve da vrijedi $2S_i' = S_i, 2R_i' = R_i$, a $[2]^*$ je povlak (definiran u 1.2.14) množenja sa dva na krivulji E_m.

Takvo preslikavanje $\tilde{h}$ postoji zbog korolara [37, III.3.5] koji kaže da ako je E eliptička krivulja i $D = \sum n_P(P) \in \operatorname{Div}(E)$, onda je D glavni divizor ako i samo ako

$$\sum_{P\in E} n_P = 0 \quad \text{i} \quad \sum_{P\in E}[n_P]P = 0,$$

gdje je druga suma zbrajanje na E.

U našem slučaju je jasno da je prva suma jednaka nuli, a za drugu imamo

$$\sum_{T\in E_m[2]}(S_1'+T)+\sum_{T\in E_m[2]}(S_2'+T)-\sum_{T\in E_m[2]}(R_1'+T)-\sum_{T\in E_m[2]}(R_2'+T) = [4](S_1'+S_2'-R_1'-R_2')$$

$$= [2](S_1+S_2-R_1-R_2) = [2](S_1-R_2+S_2-R_1) \overset{(*)}{=} [2](R+R) = \mathcal{O},$$

gdje $(*)$ slijedi iz zadnjeg reda jednakosti u Propoziciji 2.2.1.

Jednostavan račun daje nam $\operatorname{div} g\circ[2] = \operatorname{div}\tilde{h}^2$, što povlači $C\tilde{h}^2 = g\circ[2]$ za neki $C \in \overline{\mathbb{Q}}$. Označimo $h := \tilde{h}\sqrt{C} \in \overline{\mathbb{Q}}(E_m)$ tako da vrijedi $h^2 = g\circ[2]$. Dokazati ćemo da je $h \in \mathbb{Q}(E_m)$.

Prvo ćemo pokazati da svaki $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutira nultočke i polove od $\tilde{h}$. Pogledajmo kako σ djeluje na S_1 i S_2. Budući da su S_1 i S_2 konjugati nad $\mathbb{Q}(\sqrt{q})$, jedine mogućnosti za S_1^σ su S_1 ili S_2. Ako je $S_1^\sigma = S_1$, tada mora biti $(S_1')^\sigma = S_1' + T$, za neki $T \in E_m[2]$, zato što je $2((S_1')^\sigma - S_1') = (2S_1')^\sigma - 2S_1' = S_1^\sigma - S_1 = \mathcal{O}$. Sada znamo da σ fiksira $\sum_{T\in E_m[2]}(S_1'+T)$. Uz pretpostavku da je $S_1^\sigma = S_1$, znamo da je ujedno i $S_2^\sigma = S_2$ pa σ također fiksira $\sum_{T\in E_m[2]}(S_2'+T)$.

Ako pak pretpostavimo da je $S_1^\sigma = S_2$, na sličan način možemo izvesti da je

$$\left(\sum_{T\in E_m[2]}(S_1'+T)\right)^\sigma = \sum_{T\in E_m[2]}(S_2'+T) \text{ te } \left(\sum_{T\in E_m[2]}(S_2'+T)\right)^\sigma = \sum_{T\in E_m[2]}(S_1'+T).$$

Slične izjave vrijede za R_1 i R_2 pa zaključujemo da je $\mathrm{div}(\tilde{h})$ definiran nad $\mathbb{Q}$. Preslikavanja h i $\tilde{h}$ imaju isti divizor pa je i $\mathrm{div}(h)$ definiran nad $\mathbb{Q}$. Sada koristimo drugu izjavu Teorema [22, 7.8.3]:

Teorem 2.2.3. Neka je C krivulja nad savršenim poljem k i neka je $f \in \overline{k}(C)$.

1. Ako je $\sigma(f) = f, \quad$ za svaki $\sigma \in \mathrm{Gal}(\overline{k}/k)$ onda je $f \in k(C)$.

2. Ako je $\mathrm{div}\,(f)$ definiran nad k onda je $f = ch$ za neki $c \in \overline{k}$ i $h \in k(C)$.

Iz druge tvrdnje Teorema 2.2.3 zaključujemo da je $h = c \cdot h'$ za neki $c \in \overline{\mathbb{Q}}$ i $h' \in \mathbb{Q}(E_m)$. Znamo da je $c^2(h')^2 = h^2 = g \circ [2]$ i da je $g \circ [2](\mathcal{O}) = (x_1^2 - q)^2$ racionalan kvadrat. Slijedi da je $c^2 = \frac{(x_1^2-q)^2}{h'(\mathcal{O})^2}$ također racionalan kvadrat pa je c racionalan. Konačno, imamo $h \in \mathbb{Q}(E_m)$. ■

Koristeći prethodne dvije propozicije dokazujemo da je $g \bmod (\mathbb{Q}^*)^2$ homomorfizam.

Teorem 2.2.4. Za sve $P, Q \in E_m(\mathbb{Q})$ vrijedi $g(P+Q) \equiv g(P)g(Q) \bmod (\mathbb{Q}^*)^2$.
Posebno, ako je $P \equiv Q \bmod 2E_m(\mathbb{Q})$, onda je $g(P) \equiv g(Q) \bmod (\mathbb{Q}^*)^2$.

Dokaz. Neka su $P', Q' \in E_m(\overline{\mathbb{Q}})$ takve da je $2P' = P$ i $2Q' = Q$. Želimo dokazati jednakost

$$\frac{\sigma(h(P'+Q'))}{h(P'+Q')} = \frac{\sigma(h(P'))}{h(P')}\frac{\sigma(h(Q'))}{h(Q')}$$

koja je ekvivalentna sa

$$\frac{h(P'+Q')}{h(P')h(Q')} = \frac{\sigma(h(P'+Q'))}{\sigma(h(Q'))\sigma(h(P'))} = \sigma\left(\frac{h(P'+Q')}{h(P')h(Q')}\right).$$

Neka je $T \in E_m[2]$ bilo koji element 2-torzije. Divizor preslikavanja h dan je sa (2.3), a lako se vidi da preslikavanje $X \mapsto h(X+T)$ ima isti divizor. Zato je divizor preslikavanja

$$X \mapsto \frac{h(X+T)}{h(X)}$$

nul divizor pa je po 1.2.13 a) navedeno preslikavanje konstantno.

Za $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ imamo $\sigma(P') - P' \in E_m[2], \sigma(Q') - Q' \in E_m[2]$ te $\sigma(P'+Q') - (P'+Q') \in E_m[2]$. Ovo vrijedi jer je $2P' = P \in E_m(\mathbb{Q})$ te $2Q' = Q \in E_m(\mathbb{Q})$. Prema Propoziciji 2.2.2, h je racionalna funkcija pa h i σ komutiraju, što koristimo u narednom računu. Vrijedi

$$\sigma(h(P'))h(P') = \frac{h(\sigma(P'))}{h(P')} = \frac{h(P'+(\sigma(P')-P'))}{h(P')} = \frac{h(X+(\sigma(P')-P'))}{h(X)}, \tag{2.4}$$

jer je $\sigma(P') - P' \in E_m[2]$. Slično

$$\frac{\sigma(h(Q'))}{h(Q')} = \frac{h(X+(\sigma(Q')-Q'))}{h(X)}, \quad \frac{\sigma(h(P'+Q'))}{h(P'+Q')} = \frac{h(X+(\sigma(P'+Q')-(P'+Q')))}{h(X)}.$$

Sada je

$$\begin{aligned}\frac{\sigma(h(P'+Q'))}{h(P'+Q')} &= \frac{h(X+(\sigma(P'+Q')-(P'+Q')))}{h(X)}\\ &= \frac{h(X+\sigma(P')-P'+(\sigma(Q')-Q')))}{h(X+\sigma(P')-P')}\frac{h(X+\sigma(P')-P')}{h(X)}\\ &\overset{(2.4)}{=} \frac{h(X+\sigma(P')-P'+(\sigma(Q')-Q')))}{h(X+\sigma(P')-P')}\frac{h(Y+\sigma(P')-P')}{h(Y)}\\ &= \frac{\sigma(h(Q'))}{h(Q')}\frac{\sigma(h(P'))}{h(P')}\end{aligned}$$

tako što uvrstimo $X = P'+Q'-\sigma(P')$ te $Y = P'$. Ovo vodi do

$$\frac{h(P'+Q')}{h(P')h(Q')} = \frac{\sigma(h(P'+Q'))}{\sigma(h(Q'))\sigma(h(P'))} = \sigma\left(\frac{h(P'+Q')}{h(P')h(Q')}\right)$$

za svaki $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Zaključujemo da je

$$\frac{h(P'+Q')}{h(P')h(Q')} \in \mathbb{Q} \implies h^2(P'+Q') \equiv h^2(P')h^2(Q') \mod (\mathbb{Q}^*)^2.$$

Konačno,

$$\begin{aligned}g(P+Q) = g\circ[2](P'+Q') = h^2(P'+Q') &\equiv h^2(P')h^2(Q') =\\ = g\circ[2](P')g\circ[2](Q') = g(P)g(Q) &\mod (\mathbb{Q}^*)^2.\end{aligned}$$

Druga tvrdnja teorema slijedi iz prve. Ako je $P = Q+2S_3$, za $S_3 \in E_m(\mathbb{Q})$, onda je

$$g(P) = g(Q+2S_3) \equiv g(Q)g(S_3)^2 \equiv g(Q) \mod (\mathbb{Q}^*)^2.$$

■

2.3. GLAVNI REZULTATI

Najveća prepreka konstrukcije racionalnih $D(q)$-četvorki pomoću točaka na E_m je racionalnost četvorke $\{a,b,c,d\}$. Teorem 2.2.4, nam daje uvjet na trojku točaka iz $E_m(\mathbb{Q})$, koji nam osigurava racionalnost četvorke $\{a,b,c,d\}$.

Teorem 2.3.1. Neka je $(x_1,y_1) \in \mathcal{D}_m(\mathbb{Q})$ točka pomoću koje je definirano preslikavanje $f\colon \mathcal{D}_m \to E_m$. Ako je $(Q_1,Q_2,Q_3) \in E_m(\mathbb{Q})^3$ trojka koja zadovoljava kriterij nedegeneriranosti, takva da je $(y_1^2-q)\cdot g(Q_1+Q_2+Q_3)$ kvadrat, onda su brojevi

$$a = \pm\left(\frac{1}{m}\frac{g(Q_1)}{(x_1^2-q)}\frac{g(Q_2)}{(x_1^2-q)}\frac{g(Q_3)}{(x_1^2-q)}\right)^{1/2},$$

$$b=\frac{g(Q_1)}{a(x_1^2-q)}, c=\frac{g(Q_2)}{a(x_1^2-q)}, d=\frac{g(Q_3)}{a(x_1^2-q)}$$

racionalni i čine racionalnu $D(q)$-četvorku takvu da je $abcd=m$.

Obratno, neka je $\{a,b,c,d\}$ racionalna $D(q)$-četvorka, takva da je $m=abcd$. Ako trojka $(Q_1,Q_2,Q_3)\in E_m(\mathbb{Q})^3$ odgovara četvorci $\{a,b,c,d\}$, onda je $(y_1^2-q)g(Q_1+Q_2+Q_3)$ kvadrat.

Dokaz. Pretpostavka teorema kaže da je $(y_1^2-q)g(Q_1+Q_2+Q_3)$ kvadrat. Sada imamo

$$\begin{aligned} a^2 &= \frac{g(Q_1)g(Q_2)g(Q_3)}{(x_1^2-q)^3 m} = \frac{g(Q_1)g(Q_2)g(Q_3)(y_1^2-q)}{(x_1^2-q)^4(y_1^2-q)^2} \\ &\equiv g(Q_1+Q_2+Q_3)(y_1^2-q) \mod (\mathbb{Q}^*)^2, \end{aligned}$$

gdje je ekvivalencija direktna posljedica Teorema 2.2.4.

Zaključujemo da je a racionalan, što povlači racionalnost od b,c i d. Budući da je $abcd=m\neq 0$, nijedan od brojeva a,b,c,d nije nula, a kriterij nedegeneriranosti trojke (Q_1,Q_2,Q_3) garantira da su a,b,c,d u parovima različiti.

Obratno, ako je $\{a,b,c,d\}$ racionalna $D(q)$-četvorka, njoj odgovara trojka $(Q_1,Q_2,Q_3)\in(E_m(\mathbb{Q}))^3$. Slično kao maloprije, vrijedi

$$\begin{aligned} g(Q_1+Q_2+Q_3)(y_1^2-q) &\equiv g(Q_1)g(Q_2)g(Q_3)(y_1^2-q) \equiv \\ &\equiv \frac{g(Q_1)g(Q_2)g(Q_3)(y_1^2-q)}{(x_1^2-q)^4(y_1^2-q)^2} = \frac{g(Q_1)g(Q_2)g(Q_3)}{(x_1^2-q)^3 m} = a^2 \mod (\mathbb{Q}^*)^2. \end{aligned}$$

■

Prirodno se nameće pitanje za koje m će postojati racionalna $D(q)$-četvorka s umnoškom elemenata jednakim m. Znamo parametrizirati sve m za koje postoje takve četvorke, ali nije dovoljno samo da je $D_m(\mathbb{Q})$ neprazan. Postoje primjeri parova brojeva (q,m), gdje je $D_m(\mathbb{Q})$ eliptička krivulja pozitivnog ranga, dakle beskonačan skup, ali ne postoje racionalne $D(q)$-četvorke umnoška elemenata jednakog m. Prvo dokazujemo jednu lemu.

Lema 2.3.2. Neka je $\{a,b,c,d\}$ racionalna $D(q)$-četvorka takva da je $abcd=m$. Postoji točka $(x_0,y_0)\in\mathcal{D}_m(\mathbb{Q})$, takva da je x_0^2-q potpun kvadrat.

Dokaz. Neka je $(Q_1,Q_2,Q_3)\in E_m(\mathbb{Q})^3$ trojka pridružena racionalnoj $D(q)$-četvorki $\{a,b,c,d\}$. Teorem 2.3.1 nam kaže da je $(y_1^2-q)g(Q_1+Q_2+Q_3)$ kvadrat.

Označimo sa $Q=Q_1+Q_2+Q_3$. Vrijedi

$$\begin{aligned} (y_1^2-q)g(Q) &= (y_1^2-q)(x_1^2-q)\left((x\circ f^{-1}(Q))^2-q\right) = m\cdot\left((x\circ f^{-1}(Q))^2-q\right) \\ &= m\cdot\frac{m}{(y\circ f^{-1}(Q))^2-q} = m^2\frac{1}{(y\circ f^{-1}(Q))^2-q}. \end{aligned}$$

Budući da je lijeva strana jednakosti kvadrat, zaključujemo da je $(y\circ f^{-1}(Q))^2-q$ također kvadrat. Neka je sada $(x_0,y_0):=f^{-1}(Q+R)$. Znamo da je

$$(y\circ f^{-1}(Q))^2-q \overset{(2.1)}{=} (x\circ f^{-1}(Q+R))^2-q=x_0^2-q,$$

i time je tvrdnja leme dokazana. ■

Sljedeći teorem parametrizira sve m za koje postoje tražene četvorke.

Teorem 2.3.3. Postoji racionalna $D(q)$-četvorka s umnoškom elemenata jednakim m ako i samo ako je

$$m=(t^2-q)\left(\frac{u^2-q}{2u}\right)^2,$$

za neke racionalne parametre (t,u).

Dokaz. Pretpostavimo da imamo racionalnu $D(q)$-četvorku umnoška elemenata jednakog m. Po Lemi 2.3.2 postoji točka $(x_0,y_0)\in\mathcal{D}_m(\mathbb{Q})$ takva da je x_0^2-q potpun kvadrat. Neka je $x_0^2-q=k^2$, tada vrijedi

$$q=x_0^2-k^2=(x_0-k)(x_0+k). \tag{2.5}$$

Označimo sa

$$u=x_0-k. \tag{2.6}$$

Sada, koristeći (2.5) i (2.6) slijedi

$$x_0+k=q/u \tag{2.7}$$

a zbrajajući (2.6) i (2.7) kako bi eliminirali k, dobijemo $x_0=\frac{q+u^2}{2u}$. Ako označimo $t=y_0$ imamo

$$m=(x_0^2-q)(y_0^2-q)=\left(\left(\frac{q+u^2}{2u}\right)^2-q\right)(t^2-q)=\left(\frac{q-u^2}{2u}\right)^2(t^2-q).$$

Obratno, pretpostavimo da je $m=\left(\frac{q-u^2}{2u}\right)^2(t^2-q)$ za neke racionalne (t,u). Označimo sa $y_1=t, x_1=\frac{q+u^2}{2u}$. Lako se provjeri da je $(x_1^2-q)(y_1^2-q)=m$ pa postoji točka $(x_1,y_1)\in\mathcal{D}_m(\mathbb{Q})$ takva da je $x_1^2-q=\left(\frac{u^2-q}{2u}\right)^2$ potpun kvadrat. Koristimo ovu točku $(x_1,y_1)=:P_1$ kako bi definirali preslikavanje $f:\mathcal{D}_m\to E_m$. Neka su $Q_1=R+S, Q_2=2S$ te $Q_3=3S$. Skupovi $G\cdot Q_i$ su disjunktni, a broj

$$\begin{aligned} g(Q_1+Q_2+Q_3)(y_1^2-q)&=g(R+6S)(y_1^2-q)\equiv g(R)(y_1^2-q)\\ &=\left((x_1^2-q)(y_1^2-q)\right)(y_1^2-q)=\left(\frac{u^2-q}{2u}\cdot(t^2-q)\right)^2 \mod(\mathbb{Q}^*)^2 \end{aligned}$$

je potpun kvadrat. Točke (Q_1, Q_2, Q_3) zadovoljavaju uvjete Teorema 2.3.1 što nam garantira postojanje racionalne $D(q)$-četvorke. ■

Napomena 2.3.4. Iz dokaza prehodnih teorema slijedi da je uvjet $m = \left(\frac{q-u^2}{2u}\right)^2 (t^2 - q)$ ekvivalentan tvrdnji da postoji točka $(x_0, y_0) \in \mathcal{D}_m(\mathbb{Q})$ takva da je $x_0^2 - q$ potpun kvadrat.

2.4. PRIMJERI

Postoje parovi racionalnih brojeva m, q takvi da je $m = (x_1^2 - q)(y_1^2 - q)$, to jest, $\mathcal{D}_m(\mathbb{Q}) \neq \emptyset$, ali da ne postoji racionalna $D(q)$-četvorka umnoška elemenata jednakog m.

Nužan uvjet koji trebamo provjeriti po Teoremu 2.3.1 je postoji li $T' \in E_m(\mathbb{Q})$ takva da je $g(T')(y_1^2 - q)$ kvadrat. Teorem 2.2.4 nam kaže da je tu tvrdnju dovoljno provjeriti na točkama $T \in E_m(\mathbb{Q})/2E_m(\mathbb{Q})$, a to je konačan skup. Ako za neke konkretne q, m znamo generatore grupe $E_m(\mathbb{Q})/2E_m(\mathbb{Q})$, onda možemo odrediti postoje li $D(q)$-četvorke umnoška elemenata jednakog m i parametrizirati ih pomoću točaka na $E_m(\mathbb{Q})$.

Korolar 2.4.1. Ne postoji racionalna $D(3)$-četvorka umnoška elemenata jednakog $m = 1012$.

Dokaz. Uz oznake $q = 3, x_1 = 5, y_1 = 7$, vrijedi

$$m = 1012 = (5^2 - 3)(7^2 - 3) = (x_1^2 - q)(y_1^2 - q).$$

Skup $\mathcal{D}_m(\mathbb{Q})$ je neprazan, krivulja $E_m(\mathbb{Q})$ je ranga 2 s torzijom $\mathbb{Z}/4\mathbb{Z}$ pa trebamo provjeriti osam točaka. Niti za jednu od osam točaka $T \in E_m(\mathbb{Q})/2E_m(\mathbb{Q})$ broj $g(T)(y_1^2 - q)$ nije kvadrat pa ne postoji racionalna $D(3)$-četvorka umnoška elemenata jednakog 1012. ■

Propozicija 2.4.2. Za svaki $t \in \mathbb{Q}$, postoji racionalna $D(-3)$-četvorka umnoška elemenata jednakog $m = 4(t^2 + 3)$.

Dokaz. Neka je $q = -3, x_1 = 1, y_1 = t$ te $m = 4(t^2 + 3)$. Točka S je beskonačnog reda u $E_m(\mathbb{Q}(t))$, a trojka $(Q_1, Q_2, Q_3) = (S + R, 2S, 3S)$ zadovoljava uvjete Teorema 1. Kod u Magmi (Odjeljak

5.1.3) nam daje familiju četvorki:

$$a = \frac{2\cdot(3+6t^2+7t^4)\cdot(27+162t^2+801t^4+1548t^6+1069t^8+306t^{10}+183t^{12})}{(3+t^2)\cdot(1+3t^2)\cdot(9+9t^2+19t^4+27t^6)\cdot(3+27t^2+33t^4+t^6)},$$
$$b = \frac{(3+t^2)^2\cdot(1+3t^2)\cdot(9+9t^2+19t^4+27t^6)\cdot(3+27t^2+33t^4+t^6)}{2\cdot(3+6t^2+7t^4)\cdot(27+162t^2+801t^4+1548t^6+1069t^8+306t^{10}+183t^{12})},$$
$$c = \frac{2\cdot(3+6t^2+7t^4)\cdot(3+27t^2+33t^4+t^6)\cdot(9+9t^2+19t^4+27t^6)}{(3+t^2)\cdot(1+3t^2)\cdot(27+162t^2+801t^4+1548t^6+1069t^8+306t^{10}+183t^{12})},$$
$$d = \frac{2\cdot(3+t^2)\cdot(1+3t^2)\cdot(27+162t^2+801t^4+1548t^6+1069t^8+306t^{10}+183t^{12})}{(3+6t^2+7t^4)\cdot(3+27t^2+33t^4+t^6)\cdot(9+9t^2+19t^4+27t^6)}.$$

■

Napomena 2.4.3. Označimo $x_1 = \frac{q+u^2}{2u}$ te $y_1 = t$ i definirajmo $m = (x_1^2-q)(y_1^2-q)$. Koristeći trojku točaka $(S+R, 2S, 3S)$ koja zadovoljava uvjete Teorema 2.3.1, možemo eksplicitno izračunati racionalnu $D(q)$-četvorku umnoška elemenata jednakog m (njeno postojanje je dokazano u Teoremu 2.3.3). Elementi te četvorke su racionalne funkcije stupnja 40 u tri varijable q,u,t i time preveliki za ispis.

3. RACIONALNE $D(q)$-PETORKE

U ovom poglavlju konstruiramo familije racionalnih $D(q)$-petorki, za neke specifične klase ostataka kvadratno slobodnih cijelih brojeva q. Naša ideja oslanja se na rad Dujelle i Fuchsa [13]. Oni su, uz pretpostavku Slutnje o parnosti, dokazali da za svaki kvadratno slobodan prirodan broj q u barem 497 klasa ostataka $\bmod 1320$ postoji beskonačno mnogo racionalnih $D(q)$-petorki. Ovdje proširujemo njihov rezultat na veću klasu ostataka.

3.1. PRETHODNI REZULTATI I KONSTRUKCIJE

Neka je q racionalan broj. Ako je $\{a_1, a_2, \ldots, a_n\}$ racionalna $D(q)$-n-torka, onda je za svaki $r \in \mathbb{Q}$ skup $\{ra_1, ra_2, \ldots, ra_n\}$ racionalna $D(qr^2)$-n-torka, jer je $(ra_1)(ra_2)+qr^2 = (a_1a_2+q)r^2$. Ako želimo pronaći sve racionalne $D(q)$-n-torke, dovoljno je pronaći sve racionalne $D(q')$-n-torke, gdje je q' kvadratno slobodan cijeli broj takav da je q'/q racionalan kvadrat.

Neka je $q(u)$ racionalna funkcija varijable u, koja nije identički jednaka nuli. Skup n različitih, ne identički jednakih nuli racionalnih funkcija $\{a_1(u), a_2(u), \ldots, a_n(u)\}$ zovemo $D(q(u))$-*n-torka s elementima iz* $\mathbb{Q}(u)$, ako vrijedi $a_i(u)a_j(u)+q(u) = h_{i,j}^2(u)$, $h_{i,j} \in \mathbb{Q}(u)$ za sve $1 \leq i < j \leq n$. Posebno, takve petorke ćemo kraće zvati $D(q(u))$-*petorke.*

Prateći Dujellu [9], želimo pronaći racionalne $D(q)$-petorke oblika (A,B,C,D,x^2) gdje je $q = \alpha \cdot x^2$, uz uvjet $\alpha, x \in \mathbb{Q}$. Dujella je krenuo od racionalnog $D(q)$-para $\{B,C\}$ za koji vrijedi $BC+\alpha x^2 = k^2$. Brojevi $A = B+C-2k$ i $D = B+C+2k$ proširuju par $\{B,C\}$ do regularnih $D(q)$-trojki. Četvorka $\{A,B,C,D\}$ je *skoro* racionalna $D(q)$-četvorka, uvjet koji nedostaje je $AD+\alpha x^2 = \square$. Kako bismo konstruirali racionalnu $D(q)$-petorku $\{A,B,C,D,x^2\}$, također mora vrijediti $Y \cdot x^2 + \alpha x^2 = (Y+\alpha)x^2 = \square$, za $Y = A,B,C$ te D.

Propozicija 3.1.1. Neka je $\{A,B,C,D,x^2\}$ racionalna $D(\alpha x^2)$-petorka koja zadovoljava

$$A+\alpha = a^2, B+\alpha = b^2, C+\alpha = c^2, D+\alpha = d^2, \tag{3.1}$$

$$BC+\alpha x^2=k^2,\quad A=B+C-2k,\quad D=B+C+2k. \tag{3.2}$$

Označimo $p=\frac{d+a}{2}, r=\frac{d-a}{2}$. Tada je

$$b^2=p^2+r^2-x^2+\frac{(p^2-x^2)(r^2-x^2)}{p^2+r^2-c^2-x^2}.$$

Dokaz. Oduzimanjem dvije desne jednadžbe iz (3.2) imamo

$$4k=D-A=(D+\alpha)-(A+\alpha)=d^2-a^2=(d-a)(d+a)=2r\cdot 2p.$$

Lako se vidi da je

$$k=pr,\quad a=p-r,\quad d=p+r. \tag{3.3}$$

Druga jednakost iz (3.2), koristeći (3.1) te (3.3) daje nam

$$(a^2-\alpha)=(b^2-\alpha)+(c^2-\alpha)-2k \quad\overset{(3.3)}{\Longrightarrow}\quad b^2+c^2=p^2+r^2+\alpha \tag{3.4}$$

Prva jednadžba iz (3.2) daje nam

$$k^2=(b^2-\alpha)(c^2-\alpha)+\alpha x^2.$$

Uvrštavamo $k=pr$ te manipuliramo pomoću (3.4) kako bismo dobili

$$4b^2c^2=4\cdot(p^2r^2+\alpha(p^2+r^2)-\alpha x^2).$$

Prethodna jednažba i (3.4) daju nam

$$(b^2-c^2)^2=(b^2+c^2)^2-4b^2c^2=(p^2+r^2+\alpha)^2-4\cdot(p^2r^2+\alpha(p^2+r^2)-\alpha x^2).$$

Još malo manipulacija vodi do

$$4(p^2-x^2)(r^2-x^2)=(\alpha-(p^2-x^2+r^2-x^2))^2-(b^2-c^2)^2.$$

Desna strana posljednje jednadžbe je razlika kvadrata. Označimo li

$$2v=\alpha-(p^2-x^2+r^2-x^2)-(b^2-c^2) \tag{3.5}$$

imamo

$$\frac{2(p^2-x^2)(r^2-x^2)}{v}=\alpha-(p^2-x^2+r^2-x^2)+(b^2-c^2). \tag{3.6}$$

Zbrajanje (3.5) i (3.6) te dijeljenje s dva vodi do

$$\alpha=v+\frac{(p^2-x^2)(r^2-x^2)}{v}+(p^2-x^2)+(r^2-x^2)=\frac{1}{v}(p^2-x^2+v)(r^2-x^2+v). \tag{3.7}$$

Oduzimanje (3.5) od (3.6) te dijeljenje s dva daje nam

$$b^2 - c^2 = \frac{1}{v}((p^2 - x^2)(r^2 - x^2) - v^2). \tag{3.8}$$

Eliminacijom varijable α iz (3.4) pomoću (3.7) slijedi

$$b^2 + c^2 = p^2 + r^2 + \frac{1}{v}(p^2 - x^2 + v)(r^2 - x^2 + v). \tag{3.9}$$

Konačno, zbrajanjem (3.8) i (3.9) te oduzimanjem (3.8) od (3.9) i dijeljenjem oba izraza brojem dva imamo

$$b^2 = p^2 + r^2 - x^2 + \frac{1}{v}(p^2 - x^2)(r^2 - x^2), \tag{3.10}$$

$$c^2 = p^2 + r^2 - x^2 - v. \tag{3.11}$$

Uvrštavajući v u (3.10) koristeći (3.11) dolazimo do

$$b^2 = p^2 + r^2 - x^2 + \frac{(p^2 - x^2)(r^2 - x^2)}{p^2 + r^2 - c^2 - x^2}. \tag{3.12}$$

■

Napomena 3.1.2. U dokazu prethodne propozicije nismo koristili činjenicu da je $AD + x^2$ potpun kvadrat.

Prethodna propozicija ima djelomični obrat, koji će nam omogućiti konstrukciju racionalnih $D(q)$-petorki.

Propozicija 3.1.3. Neka su $p, r, c, x, b \in \mathbb{Q}$ takvi da vrijedi

$$b^2 = p^2 + r^2 - x^2 + \frac{(p^2 - x^2)(r^2 - x^2)}{p^2 + r^2 - c^2 - x^2}.$$

Definirajmo

$$a = p - r, \quad d = p + r, \quad k = pr, \quad \alpha = \frac{(c^2 - r^2)(c^2 - p^2)}{c^2 + x^2 - p^2 - r^2},$$
$$A = a^2 - \alpha, \quad B = b^2 - \alpha, \quad C = c^2 - \alpha, \quad D = d^2 - \alpha.$$

Tada je $\{A, B, C, D, x^2\}$ racionalna $D(\alpha x^2)$-petorka ako vrijedi da su

(i) elementi petorke međusobno različiti,

(ii) nijedan element petorke niti α nije jednak nula,

(iii) $AD + \alpha x^2 = \square$.

Dokaz. Računskom provjerom vidi se da su brojevi $AB + \alpha x^2, AC + \alpha x^2, BC + \alpha x^2, BD + \alpha x^2$, $CD + \alpha x^2, Ax^2 + \alpha x^2, Bx^2 + \alpha x^2, Cx^2 + \alpha x^2, Dx^2 + \alpha x^2$ kvadrati. Ovo dokazuje propoziciju. ■

Glavni fokus su nam problemi s racionalnosti, konkretno, nalaženje racionalnih rješenja jednadžbi (3.13) i (3.14). Problem degeneričnosti rješavamo u dokazu Teorema 3.3.5.

3.2. SMANJIVANJE BROJA VARIJABLI

Kako bismo ovom metodom pronašli racionalne $D(q)$-petorke, trebamo naći racionalna rješenja jednadžbi

$$b^2 = p^2 + r^2 - x^2 + \frac{(p^2-x^2)(r^2-x^2)}{c^2+x^2-p^2-r^2} = p^2 + r^2 + \alpha - c^2, \tag{3.13}$$

$$z^2 = AD + \alpha x^2 = (p^2-r^2)^2 + \alpha(x^2 - 2(p^2+r^2) + \alpha), \tag{3.14}$$

gdje je α definiran formulom

$$\alpha = \frac{(c^2-r^2)(c^2-p^2)}{c^2+x^2-p^2-r^2}.$$

Primijetimo da su α, b^2 te z^2 homogene racionalne funkcije u varijablama p,r,c,x pa možemo uzeti $r=1$. Nakon toga, izrazi za α, b^2, z^2 pojednostavljuju se do

$$\alpha = \frac{(c^2-1)(c^2-p^2)}{c^2+x^2-p^2-1}, \tag{3.15}$$

$$b^2 = p^2 + 1 + \alpha - c^2, \tag{3.16}$$

$$z^2 = (p^2-1)^2 + \alpha(x^2 - 2(p^2+1) + \alpha). \tag{3.17}$$

Ne znamo pronaći sva rješenja jednadžbi (3.16), (3.17) pa želimo specijalizirati jednu od varijabli c,p,x pomoću preostale dvije. Pritom želimo imati što jednostavniji izraz za kvadratno slobodni dio broja α.

Definiramo mnogostrukosti S_1 i S_2 u $\mathbb{A}^3$ jednadžbama

$$S_1 \colon (c^2-1)(c^2-p^2) = 0, \quad S_2 \colon c^2+x^2-p^2-1 = 0.$$

Mnogostrukosti S_1 i S_2 su skupovi nultočaka brojnika i nazivnika od α. Ploha S_1 je unija četiri ravnine $c = \pm p$ te $c = \pm 1$, dok je ploha S_2 hiperboloid. Presjek $S_1 \cap S_2$ je unija osam pravaca

$$l_1, \ldots, l_4 \colon (c = \pm 1, x = \pm p), \quad l_5, \ldots, l_8 \colon (c = \pm p, x = \pm 1).$$

Heuristika u Sekciji 3 iz [17, Section 3, Lemma 5] kaže nam da bi dobra specijalizacija bila ploha niskog stupnja u varijablama c,p,x koja presijeca S_1 i S_2 točno u pravcima l_i. Logičan prvi izbor su ravnine koje sadrže dva pravca l_i. Jednadžbe takvih ravnina su $x = \pm 1 \pm c \pm p$ pa uzimamo $x = c + p + 1$ (promjena predznaka neće napraviti značajne promjene u specijalizaciji). U praksi, do ove specijalizacije došli smo istraživanjem $D(q(u))$-petorke (3.28), koju je pronašao Dujella.

Nakon specijalizacije $x = c + p + 1$, jednadžbe za α, b^2 te z^2 postaju

$$\alpha = \frac{1}{2}(c-p)(c-1), \tag{3.18}$$

$$b^2 = p^2 + \frac{1-c}{2}p - \frac{1}{2}(c^2+c) + 1, \tag{3.19}$$

$$z^2 = p^4 + \frac{c-1}{2}p^3 - \frac{5c^2+3}{4}p^2 + \frac{c^2-1}{2}p + \frac{3c^4-5c^2+2c+4}{4}. \tag{3.20}$$

Jednadžba (3.19) definira koniku u varijablama b, p s racionalnom točkom $(1, c)$. Postoji standardna tehnika pomoću koje možemo parametrizirati sve racionalne točke na (3.19). Promotrimo neki pravac koji prolazi kroz točku $(1, c)$. Druga presječna točka takvog pravca s konikom (3.19) imat će racionalne koordinate ako i samo ako je koeficijent smjera pravca racionalan. Svi pravci s racionalnim koeficijentom smjera koji prolaze kroz $(1, c)$ opisani su sa

$$b - 1 = u(p - c), \quad u \in \mathbb{Q}.$$

Uvrštavanjem b u (3.19) dobijemo kvadratnu jednadžbu u varijabli p čije je jedno rješenje $p_1 = c$, a drugo je

$$p_2 = \frac{u^2 c + c/2 + 1/2 - 2u}{u^2 - 1}.$$

Dobivamo parametrizaciju svih racionalnih rješenja jednadžbe (3.19),

$$p = \frac{u^2 c + c/2 + 1/2 - 2u}{u^2 - 1}, \quad b = \frac{u^2 - 3uc/2 - u/2 + 1}{u^2 - 1}, \quad u \in \mathbb{Q}. \tag{3.21}$$

Uvrštavanjem izraza za p iz (3.21) u (3.20), desna strana jednadžbe (3.20) postaje polinom stupnja četiri u varijabli c s koeficijentima u $\mathbb{Q}(u)$. Množenje obje strane sa $\left(\frac{(u^2-1)^2}{u^2-1/4}\right)^2$ vodi do

$$\mathcal{C}\colon z_1^2 = z^2 \cdot \left(\frac{(u^2-1)^2}{u^2-1/4}\right)^2 = f_4(u)c^4 + f_3(u)c^3 + f_2(u)c^2 + f_1(u)c + f_0(u), \tag{3.22}$$

gdje su $f_i(u)$ racionalne funkcije u varijabli u zadane sa

$$\begin{aligned}
f_4(u) &= u^4 + u^2 + 7,\\
f_3(u) &= -3 \cdot \frac{(u^3+3u-1)(2u^2+1)}{u^2-1/4},\\
f_2(u) &= \frac{-16u^8 + 16u^7 + 242u^6 - 76u^5 + 199u^4 - 166u^3 + 47u^2 + 10u - 13}{8 \cdot (u^2-1/4)^2},\\
f_1(u) &= 3 \cdot \frac{(u^3+3u^2+1/2)(u^4 - 11/2u^3 + 4u^2 - 3/2u + 1/2)}{(u^2-1/4)^2},\\
f_0(u) &= \frac{16u^8 + 16u^7 - 116u^6 + 40u^5 + 409u^4 - 308u^3 + 25u^2 - 20u + 19}{16(u^2-1/4)^2}.
\end{aligned} \tag{3.23}$$

Krivulja $\mathcal{C}$, definirana jednadžbom (3.22), biracionalno je ekvivalentna eliptičkoj krivulji nad $\mathbb{Q}(u)$ jer ima racionalnu točku $(c,z_1)=\left(1,\frac{4u(u-1)^2}{u^2-1/4}\right)$. Koristeći Magmu (kod u Odjeljku 5.2.1) računamo da je $\mathcal{C}$ biracionalna krivulji u Weierstrassovom obliku

$$\begin{aligned}E\colon y^2 =& x^3-27\cdot(256u^8+64u^7-1280u^6+1216u^5+3265u^4-2372u^3+310u^2-332u+169)x\\ &+54\cdot(4096u^{12}+1536u^{11}-30624u^{10}-18400u^9+74448u^8+125568u^7-59313u^6\\ &-165978u^5+154773u^4-40360u^3+5187u^2-6474u+2197).\end{aligned}\tag{3.24}$$

Točke

$$\begin{aligned}S_1 &= [48u^4+168u^3-9u^2-138u+39,-1944u^5-1944u^4+4374u^3+486u^2-972u],\\ S_2 &= \left[\frac{48u^6+588u^5+753u^4-1014u^3+24u^2-6u+39}{u^2+2u+1},\right.\\ &\quad\left.\frac{-5832u^8-25596u^7-6156u^6+48438u^5-8100u^4+324u^3-3240u^2+162u}{u^3+3u^2+3u+1}\right],\\ S_3 &= \left[\frac{48u^6+204u^5-855u^4+78u^3+2028u^2-1098u+27}{u^2-6u+9},\right.\\ &\quad\left.\frac{-5832u^8+21060u^7+972u^6-94446u^5+102384u^4+34020u^3-67392u^2+486u+8748}{u^3-9u^2+27u-27}\right],\\ S_4 &= [48u^4+492u^3+693u^2-84u-69,-5832u^5-19764u^4-15228u^3+3402u^2+2754u-324],\\ S_5 &= \left[\frac{48u^6+12u^5-291u^4+66u^3+600u^2+66u-69}{u^2+2u+1},\right.\\ &\quad\left.\frac{-1080u^8-2484u^7+6480u^6+17550u^5-1512u^4-18468u^3-3348u^2+2538u+324}{u^3+3u^2+3u+1}\right]\end{aligned}\tag{3.25}$$

su nezavisne točke Mordell-Weilove grupe $E(\mathbb{Q}(u))$. Koristili smo računalni program Magma [4] da dokažemo nezavisnost točaka S_i tako što smo provjerili da je eliptički regulator točaka $S_i, i\in\{1,\ldots,5\}$ različit od nule.

Svaka racionalna točka na E (Magma kod u Odjeljku 5.2.2) daje nam racionalnu točku $(c(u),z_1(u))$ na krivulji $\mathcal{C}$ (3.22). Uvrštavajući $c(u)$ u (3.21), imamo $b(u)$ te $p(u)$. Fiksiramo $r(u)=1$ te $x(u)=c(u)+p(u)+1$. Propozicija 3.1.3 daje nam racionalnu $D\left(\alpha(u)x(u)^2\right)$-petorku $\{A(u),B(u),C(u),D(u),x^2(u)\}$, pod uvjetom da nikoja dva elementa nisu međusobno jednaka, nijedan element nije jednak nuli te ako je $\alpha(u)\neq 0$. Uvjet $AD+\alpha x^2=\square$ ekvivalentan je postojanju rješenja jednadžbe (3.14), što smo ispunili nalaženjem racionalnih točaka na krivulji $\mathcal{C}$.

Fiksirajmo kvadratno slobodan $q \in \mathbb{Z}$ i pretpostavimo da je $\alpha(u_1)x(u_1)^2 = qs_1^2$ za neke racionalne u_1, s_1 takve da je $s_1 \neq 0$. Tada je $\{A(u_1)/s_1, B(u_1)/s_1, C(u_1)/s_1, D(u_1)/s_1, x^2(u_1)/s_1\}$ racionalna $D\left(\alpha(u_1)\cdot(x(u_1)/s_1)^2\right)$-petorka, to jest, racionalna $D(q)$-petorka. Dujella i Fuchs koristili su sljedeću ideju u [13]: ako postoji beskonačno racionalnih parova (u_1, s_1) takvih da vrijedi

$$\alpha(u_1) = q\left(\frac{s_1}{x(u_1)}\right)^2, \tag{3.26}$$

onda postoji i beskonačno racionalnih $D(q)$-petorki.

Neka je $P(u)$ kvadratno slobodan polinom takav da vrijedi

$$P(u) \equiv \alpha(u)x(u)^2 \mod (\mathbb{Q}(u)^*)^2. \tag{3.27}$$

Polinom $P(u)$ je jedinstveno određen do na množenje racionalnim kvadratom. Rješavanje jednadžbe (3.26) ekvivalentno je nalaženju racionalnog rješenja (u_1, s_1) jednadžbe

$$P(u) = qs^2. \tag{3.28}$$

Ako je stupanj polinoma $P(u)$ veći ili jednak od pet, onda jednadžba (3.28) određuje krivulju genusa barem dva (jer je P kvadratno slobodan pa nema dvostrukih nultočaka), a takva krivulja, po Faltingsovom teoremu, ima najviše konačno mnogo racionalnih točaka. To znači da se na ovaj način može doći do beskonačno rješenja (u_1, s_1) jednadžbe (3.28) jedino ako je stupanj polinoma $P(u)$ jednak $1, 2, 3$ ili 4.

Za svaku točku na E koja vodi do racionalne $D(\alpha(u)x(u)^2)$-petorke, računamo stupanj pripadajućeg polinoma $P(u)$. Koristili smo Magmu [4] kako bismo proveli račun za točke na E oblika $\sum_{i=1}^{5} k_i S_i$ gdje su $k_i \in \{-6, \ldots, 6\}$. Ovdje smo ograničeni računalnom moći, nije jasno kakve rezultate bismo dobili da smo provjeravali veće koeficijente k_i.

Nismo dobili nijedan polinom prvog ili drugog stupnja. Svaki polinom stupnja četiri kojeg smo dobili je bio reducibilan, neki su imali racionalnu nultočku, a neki su bili umožak dva ireducibilna kvadratna polinoma u $\mathbb{Q}[u]$. Dobili smo i neke polinome stupnja tri. Polinome stupnja tri i polinome stupnja četiri s racionalnom nultočkom zovemo *dobrim* polinomima. Njih posebno ističemo jer će svaka krivulja zadana jednadžbom (3.28) u varijablama u i s, gdje je $P(u)$ dobar polinom, biti eliptička krivulja. Za polinome stupnja tri ta tvrdnja je jasna, a dobri polinomi stupnja četiri imat će racionalnu točku takvu da je $s = 0$.

Pronašli smo osam točaka $Q_i \in E(\mathbb{Q}(u))$, $i \in \{1, \ldots, 8\}$, detalji u Tablici 3.2, takvih da svaka od njih određuje $D(q(u))$-petorku takvu da je polinom $P_{Q_i}(u)$, pridružen toj petorci, dobar.

Definiramo krivulje

$$E_q^{(i)}\colon P_{Q_i}(u) = qs^2,$$

za fiksan kvadratno slobodan $q \in \mathbb{Z}$ te $i \in \{1,\ldots,8\}$. Ako je $q = 1$, pišemo $E^{(i)}$ umjesto $E_1^{(i)}$.

Definicija 3.2.1. Pretpostavimo da je $q \in \mathbb{Q}$ različit od nule te nije potpun kvadrat i da je $E/\mathbb{Q}$ eliptička krivulja zadana jednadžbom

$$E\colon y^2 = P(x),$$

čija j-invarijanta nije jednaka 0 niti 1728. *Kvadratni q tvist krivulje E* je krivulja

$$E_q\colon qy^2 = P(x).$$

Krivulje E i E_q nisu izomorfne nad $\mathbb{Q}$, ali jesu nad $\mathbb{Q}(\sqrt{q})$.

Svaka krivulja $E_q^{(i)}$ je kvadratni q-tvist krivulje $E^{(i)}$.

Želimo pronaći racionalne točke na krivuljama $E_q^{(i)}$. Ako je rang krivulje $E_q^{(i)}$ pozitivan za bilo koji i, onda imamo beskonačno mnogo rješenja jednadžbe (3.28), a time i beskonačno mnogo racionalnih $D(q)$-petorki.

Za bilo koja dva različita dobra polinoma koji definiraju eliptičke krivulje s istom j-invarijantom, postoji $q_0 \in \mathbb{Z}$ takav da je kvadratni q_0-tvist jedne krivulje izomorfan nad $\mathbb{Q}$ s drugom krivuljom. Ovo je istina jer su j-invarijante svih krivulja $E^{(i)}$ različite od 0 te 1728 [37, Chapter X, Proposition 5.4]. Brojimo samo jednog predstavnika svake klase polinoma koji definiraju eliptičke krivulje s istom j-invarijatnom.

U Tablici 3.2 navedene su točke na E koje određuju $D(q(u))$-petorku takvu da je $P(u)$ dobar polinom, a svi njima pridruženi polinomi $P_{Q_i}(u)$ definiraju eliptičke krivulje $E^{(i)}$ koje imaju različite j-invarijante:

3.3. PREDZNAK ELIPTIČKE KRIVULJE

Neka je $E/\mathbb{Q}$ eliptička krivulja. *Predznak* eliptičke krivulje $W(E)$, definira se kao umnožak *lokalnih predznaka* $W_p(E) \in \{\pm 1\}$:

$$W(E) = \prod_{p \le \infty} W_p(E),$$

gdje je p konačno ili beskonačno mjesto od $\mathbb{Q}$. Lokalni predznaci imaju svojstvo da je $W_p(E) = 1$, za svako osim konačno mnogo mjesta p. Definicija lokalnih predznaka i njihova svojstva su

Tablica 3.1: Točke $Q_i \in E(\mathbb{Q}(u))$ s pridruženim polinomom $P_{Q_i}(u)$ koji određuje $E^{(i)}\colon y^2 = P_{Q_i}(u)$.

i	$Q_i \in E(\mathbb{Q}(u))$	$P_{Q_i}(u)$
1	$-4S_1-2S_2-2S_3+3S_4+5S_5$	$-1200u^3+1645u^2-410u-35$
2	$-4S_1-S_2-2S_3+2S_4+4S_5$	$-80u^4+148u^3-65u^2-12u+9$
3	$-3S_1-S_2-2S_3+S_4+4S_5$	$-28u^4-44u^3+157u^2-106u+21$
4	$-3S_1-S_2-S_3+2S_4+3S_5$	$112u^4-100u^3-93u^2+92u-11$
5	$-2S_1-S_2-2S_3+2S_4+4S_5$	$300u^3-65u^2+16u+1$
6	$-2S_1-2S_3+S_4+3S_5$	$4u^4-20u^3+13u^2+12u$
7	$-S_1-S_2-S_3+S_4+3S_5$	$-40u^3-19u^2+38u+21$
8	$-S_4+S_5$	$-144u^3+61u^2+94u-11$

detaljno objašnjena na primjer u [35]. Rohrlich u [34] daje eksplicitnu formulu za $W_p(E)$ kad p nije 2 ni 3 vezanu uz tip redukcije od E. Preostale slučajeve, kad je $p=2$ i $p=3$ je rješio Halberstad [24]. Rizzo [33] dao je potpun pregled rezultata na engleskom i pritom je uklonio neke uvjete minimalnosti iz tablica u [24].

Slutnja Bircha i Swinnerton-Dyera (1.3.21) implicira sljedeću slutnju:

Slutnja 3.3.1 (Slutnja o parnosti)**.** Neka je $E/\mathbb{Q}$ eliptička krivulja, tada je $(-1)^{\text{rang}E(\mathbb{Q})} = W(E)$.

Direktna posljedica prethodne slutnje je da je rang krivulje E pozitivan, kad god je $W(E) = -1$. U tom slučaju imamo beskonačno racionalnih točaka na E.

Za krivulju $E/\mathbb{Q}$ te cijeli broj t različit od nule, označimo sa E_t kvadratni tvist krivulje za t. Uvodimo malo nestandardnih oznaka iz [5].

Za cijeli broj β i prost broj p, sa $v_p(\beta)$ označavamo eksponent najveće potencije broja p koja dijeli β. Sa $\beta_{(p)}$ označavamo broj takav da vrijedi

$$\beta = \beta_{(p)} \cdot p^{v_p(\beta)}.$$

Slično, ako je $d = \prod p_i^{e_i}$, definiramo $\beta_{(d)}$ kao cijeli broj za koji vrijedi

$$\beta = \beta_{(d)} \cdot \prod_i p_i^{v_{p_i}(\beta)}.$$

U [5, Theorem 1.2 b)], Desjardins je dokazala da je funkcija

$$t \mapsto W(E_t)$$

periodična na kvadratno slobodnim cijelim brojevima t fiksnog predznaka, uz pretpostavku $j(E) \neq 0, 1728$. Želimo izračunati ove periode za krivulje $E^{(i)}$, kao i dati eksplicitne formule za predznak $W\left(E_t^{(i)}\right)$, koristeći [5] te tablice iz [33]. Naglašavamo da nijedna od krivulja $E^{(i)}$ nema j-invarijantu jednaku 0 ili 1728.

Teorem [5, Theorem 1.2 a)] nam daje eksplicitnu formulu za predznak tvista eliptičke krivulje čija j-invarijanta nije 0 ili 1728:

$$W(E_t) = -W_2(E_t) \cdot W_3(E_t) \cdot \left(\frac{-1}{|t_{(6\Delta)}|}\right) \cdot \left(\prod_{p|\Delta_{(6)}} W_p(E_t)\right), \tag{3.29}$$

gdje je $\left(\frac{\cdot}{\cdot}\right)$ Jacobijev simbol, a Δ diskriminanta krivulje E zadane u Weierstrassovom obliku.

Svaki faktor desne strane jednadžbe (3.29) periodičan je na kvadratno slobodnim t fiksnog predznaka. Ovo je posljedica svojstava Jacobijevog simbola i Leme [5, Lemma 3.2], koja kaže da je funkcija $t \mapsto W_p(E_t)$ periodična na kvadratno slobodnim t fiksnog predznaka za svaki prost p. Štoviše, lema dokazuje da za $p \geq 5$, period od $W_p(E_t)$ dijeli p^2, a za $p = 2$ ili 3, period je jednak p^{γ_p}, za neki $\gamma_p \in \mathbb{N}_0$. Za eksplicitne krivulje E možemo odrediti γ_p koristeći tablice iz [24] ili [33].

Sljedeći teorem detaljno opisuje svojstva krivulje $E^{(6)}$. Slična verzija Teorema 3.3.2 (sa sličnim dokazima) vrijedi za svaku od krivulja $E^{(i)}, i \in \{1, \ldots, 8\}$. Relevantni podaci za sve krivulje nalaze se u Tablicama 3.2 i 3.3.

Teorem 3.3.2. Krivulja $E^{(6)}$ ima Weierstrassov oblik $y^2 = x^3 - 24003x + 1296702$, konduktor $C = 30$, a diskriminanta ovog modela je $\Delta = 2^{14}3^{18}5^2$.

(a) Periodi funkcija $W_2(E_t^{(6)}), W_3(E_t^{(6)})$ i $W_5(E_t^{(6)})$ na kvadratno slobodnim t fiksnog predznaka su $8, 3$ i 5, respektivno. Period funkcije $\left(\frac{-1}{t_{(30)}}\right)$ na pozitivnim kvadratno slobodnim t je 24.

(b) Ako su $t > 0$, $t' < 0$, oba broja t i t' kvadratno slobodni i $t \equiv t' \pmod{120}$, onda je $\left(\frac{-1}{t_{(30)}}\right) = -\left(\frac{-1}{t'_{(30)}}\right)$. Posebno, $W(E_t^{(6)}) = -W(E_{t'}^{(6)})$.

(c) Period $W(E_t^{(6)}) = -W_2(E_t^{(6)})W_3(E_t^{(6)})W_5(E_t^{(6)})\left(\frac{-1}{t_{(30)}}\right)$ na kvadratno slobodnim t fiksnog predznaka je 120.

(d) Uz pretpostavku Slutnje o parnosti, ako je q pozitivan, kvadratno slobodan i u jednoj od 47 klasa ostataka $\pmod{120}$, onda je rang krivulje $E_q^{(6)}(\mathbb{Q})$ pozitivan.

Ako je q negativan, kvadratno slobodan i u jednoj od 43 klase $\pmod{120}$, onda je rang krivulje $E_q^{(6)}(\mathbb{Q})$ pozitivan.

Dokaz. (a) Neka je t pozitivan. Prvo dokazujemo $\left(\frac{-1}{t_{(30)}}\right) = \left(\frac{-1}{t_{(6)}}\right)$.

Ako $5 \nmid t$, tada očito vrijedi $t_{(30)} = t_{(6)}$ pa je $\left(\frac{-1}{t_{(30)}}\right) = \left(\frac{-1}{t_{(6)}}\right)$. Neka je sada $t = 5t'$, gdje $5 \nmid t'$, jer je t kvadratno slobodan. Vrijedi $\left(\frac{-1}{t_{(30)}}\right) = \left(\frac{-1}{t'_{(6)}}\right) = \left(\frac{-1}{t'_{(6)}}\right)\left(\frac{-1}{5}\right) = \left(\frac{-1}{(5t')_{(6)}}\right) = \left(\frac{-1}{t_{(6)}}\right)$.

Da bismo izračunali $\left(\frac{-1}{n}\right) = -1^{(n-1)/2}$, za neparan n, samo trebamo znati $n \bmod 4$. Stoga, kako bismo dokazali da je $\left(\frac{-1}{t_{(6)}}\right)$ periodično preslikavanje s periodom 24 (na kvadratno slobodnim t) provjeravamo nekoliko slučajeva.

Ako je $t = 6t'$, onda vrijedi $t_{(6)} = t'$ jer je t kvadratno slobodan. $\left(\frac{-1}{t'}\right)$ ima period 4 pa je ukupni period 24.

Slučajevi $t = 3t', t = 2t'$ i $t = t'$, gdje u svakom slučaju vrijedi $(t', 6) = 1$ se rješavaju na sličan način i u svakom od tih slučajeva period dijeli 24.

24 jer najmanji period jer $1 = \left(\frac{-1}{3_{(6)}}\right) \neq \left(\frac{-1}{(11)_{(6)}}\right) = -1$ te $1 = \left(\frac{-1}{2_{(6)}}\right) \neq \left(\frac{-1}{(14)_{(6)}}\right) = -1$.

Predznak $W_5(E_t)$ možemo izračunati koristeći [5, Prop 3.1]. Za našu krivulju, ako $5 \nmid t$, redukcija od E_t u 5 je tipa I_2, a ako $5|t$, redukcija je tipa I_2^*, izračunato pomoću Magme [4]. Zaključujemo

$$W_5(E_t) = \begin{cases} 1\ , & 5 \mid t \\ \left(\frac{t}{5}\right), & 5 \nmid t \end{cases}.$$

Kada je $p = 2$ ili 3, račun se komplicira. Prema [5, Prop 3.1], ili [33, 1.1] moramo pronaći najmanji vektor (a', b', c') s nenegativnim vrijednostima tako da vrijedi

$$(a', b', c') = (v_p(c_4), v_p(c_6), v_p(\Delta)) + k(4, 6, 12),$$

za neki $k \in \mathbb{Z}$, gdje su c_4, c_6, Δ uobičajene vrijednosti pridružene Weierstrassovoj jednadžbi eliptičke krivulje.

Za $p = 3$ i $t = 1$ imamo $(a', b', c') = (4, 6, 18) - 1 \cdot (4, 6, 12) = (0, 0, 6)$.

Tvistanje za $t \not\equiv 0 \pmod{3}$ ne mijenja (a', b', c'). Prema [33, Table II, 3. red] slijedi:

$t \equiv 1 \pmod 3 \Rightarrow (c_6)_{(3)} \equiv 2 \pmod 3$. Sada je $W_3(E_t) = -1$.

$t \equiv 2 \pmod 3 \Rightarrow (c_6)_{(3)} \equiv 1 \pmod 3$. Sada je $W_3(E_t) = 1$.

Tvistanje za $t \equiv 3,6 \pmod 9$ (primijetimo da je t kvadratno slobodan pa ne može biti $\equiv 0 \pmod 9$) u oba slučaja daje $(a',b',c') = (6,9,24) - 1(4,6,12) = (2,3,12)$. Prema [33, Table II, 13. red], imamo $W_3(E_t) = -1$. Ukratko,

$$W_3(E_t) = \begin{cases} -1, & t \equiv 0,1 \pmod 3 \\ 1, & t \equiv 2 \pmod 3 \end{cases}.$$

Ako je $p = 2$ i $t = 1$ imamo $(a',b',c') = (4,6,14) - 1(4,6,12) = (0,0,2)$. Tvistanje za neparan t ne mijenja (a',b',c'). Prema [33, Table III, redovi 2 i 9] vrijediti će $W_2(E_t) = 1$ ako i samo ako $(c_6)_{(2)} \equiv 3 \pmod 8$, što je istina točno onda kada je $t \equiv 1 \pmod 8$.

Tvistanje za $t \equiv 2,6 \pmod 8$ nam daje $(a',b',c') = (6,9,20) - 1(4,6,12) = (2,3,8)$. Prema [33, Table III, 17. red] imamo:

$t \equiv 2 \pmod 8 \Rightarrow (c_6)_{(2)} \equiv 3 \pmod 4$ pa je $W_2(E_t) = 1$, a za

$t \equiv 6 \pmod 8 \Rightarrow (c_6)_{(2)} \equiv 1 \pmod 4$ pa je $W_2(E_t) = -1$. Za $p = 2$ vrijedi

$$W_2(E_t) = \begin{cases} 1, & t \equiv 1,2 \pmod 8 \\ -1, & t \equiv 3,5,6,7 \pmod 8 \end{cases}.$$

Ovo dokazuje (a) dio teorema.

(b) $\left(\frac{-1}{t_{(30)}}\right) = -\left(\frac{-1}{-t'_{(30)}}\right) \Leftrightarrow \left(\frac{-1}{t_{(30)}}\right) \cdot \left(\frac{-1}{-t'_{(30)}}\right) = -1 \Leftrightarrow \left(\frac{-1}{-t_{(30)}t'_{(30)}}\right) = -1.$

$t_{(30)}$ i $t'_{(30)}$ su neparni brojevi, a budući da je $t \equiv t' \pmod{120}$ i t,t' nisu djeljivi s 4, jer su kvadratno slobodni, onda mora vrijediti $t_{(30)} \equiv t'_{(30)} \pmod 4$. Sada slijedi

$$-t_{(30)}t'_{(30)} \equiv -\left(t'_{(30)}\right)^2 \pmod 4.$$

Dalje imamo $\left(\frac{-1}{-t_{(30)}t'_{(30)}}\right) = \left(\frac{-1}{4k-\left(t'_{(30)}\right)^2}\right) = -1$, jer -1 nije kvadratni ostatak broja oblika $4l-1$. Vrijedi $4k - \left(t'_{(30)}\right)^2 \equiv -1 \pmod 4$, jer je $\left(t'_{(30)}\right)^2$ neparan kvadrat.

(c) Lagano slijedi iz (a) i (b).

(d) Ako je $t \bmod 120$ jednak $6,7,9,11,14,15,22,26,30,35,39,41,43,50,51,53,54,58,59,$ $61,65,66,67,71,73,74,75,77,81,82,85,86,89,90,93,95,97,99,103,105,109,110,111,$

114, 117, 118 ili 119 i t je pozitivan i kvadratno slobodan, onda je $W(E_t) = -1$. Uz pretpostavku Slutnje o parnosti, rang od $E_t(\mathbb{Q})$ je neparan, stoga je i pozitivan.

Ako je t mod 120 jednak $1,2,3,5,10,13,17,18,19,21,23,25,27,29,31,33,34,37,38,42,45,46,47,49,55,57,62,63,69,70,78,79,83,87,91,94,98,101,102,106,107,113$ ili 115 i t je negativan i kvadratno slobodan, onda je $W(E_t) = -1$. Uz pretpostavku Slutnje o parnosti, rang od $E_t(\mathbb{Q})$ je neparan, stoga je i pozitivan.

■

Napomena 3.3.3. Za svaku krivulju $E^{(i)}$, period od $W(E^{(i)})$ je djeljiv s 8. Ovu činjenicu koristimo kako bismo dokazali izjavu Teorema 3.3.2 (b), da je $W(E_t^{(i)}) = -W(E_{t'}^{(i)})$, za sve krivulje $E^{(i)}$.

Teorem 3.3.4. Preslikavanja $q \mapsto W\left(E_q^{(i)}\right)$ i $q \mapsto W\left(E_{-q}^{(i)}\right)$ periodična su na kvadratno slobodnim $q \in \mathbb{N}$ s periodima N_i. Posljedično, uz pretpostavku Slutnje o parnosti, funkcije $q \mapsto \text{Rang}\left(E_q^{(i)}\right) \bmod 2$ i $q \mapsto \text{Rang}\left(E_{-q}^{(i)}\right) \bmod 2$ periodične su na kvadratno slobodnim $q \in \mathbb{N}$ s periodima N_i.

Dokaz. Tvrdnja za $i = 6$ slijedi iz Teorema 3.3.2 (c) i (b). Periodi N_i za sve krivulje E_i navedeni su u Tablici 3.2. ■

Tablica 3.2: Osnovni podaci krivulja $E^{(i)}$.

$E^{(i)}$	Weierstrassov oblik	C	Δ	N_i, period od $W(E_q^{(i)})$
$E^{(1)}$	$y^2 = x^3 - 33210675x + 6964980750$	$2 \cdot 3 \cdot 5^2 \cdot 11$	$2^{20}3^{18}5^8 11^4$	$6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11$
$E^{(2)}$	$y^2 = x^3 - 24651x + 1453194$	$2^4 \cdot 3 \cdot 13$	$2^{10}3^{20}13$	$312 = 2^3 \cdot 3 \cdot 13$
$E^{(3)}$	$y^2 = x^3 - 97227x + 10789254$	$2 \cdot 3 \cdot 5 \cdot 11$	$2^{16}3^{16}5^2 11^2$	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$
$E^{(4)}$	$y^2 = x^3 - 7155x + 187650$	$2^4 \cdot 5^2 \cdot 11$	$-2^{10}3^{12}5^3 11^2$	$88 = 2^3 \cdot 11$
$E^{(5)}$	$y^2 = x^3 + 274725x + 126596250$	$2^4 \cdot 3 \cdot 5^2 \cdot 11^2$	$-2^{10}3^{18}5^6 11^3$	$264 = 2^3 \cdot 3 \cdot 11$
$E^{(6)}$	$y^2 = x^3 - 24003x + 1296702$	$2 \cdot 3 \cdot 5$	$2^{14}3^{18}5^2$	$120 = 2^3 \cdot 3 \cdot 5$
$E^{(7)}$	$y^2 = x^3 - 132867x + 17106174$	$2 \cdot 3 \cdot 5 \cdot 11$	$2^{16}3^{14}5^4 11^2$	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$
$E^{(8)}$	$y^2 = x^3 - 1196883x + 46619118$	$2 \cdot 3 \cdot 5 \cdot 23$	$2^{18}3^{22}5^2 23^2$	$2760 = 2^3 \cdot 3 \cdot 5 \cdot 23$

Tablica 3.3: Predznak $W\left(E_t^{(i)}\right)$ raščlanjen na lokalne faktore.

$E^{(i)}$	$W(E_t^{(i)})$ dani pomoću $W_p(E_t^{(i)})$ i $\left(\frac{-1}{\lvert t_{(6\Delta)}\rvert}\right)$	periodi od $W_p(E_t^{(i)})$ i $\left(\frac{-1}{\lvert t_{(6\Delta)}\rvert}\right)$
$E^{(1)}$	$-W_2\left(E_t^{(1)}\right)\cdot W_3\left(E_t^{(1)}\right)\cdot W_5\left(E_t^{(1)}\right)\cdot W_{11}\left(E_t^{(1)}\right)\cdot\left(\frac{-1}{\lvert t_{(330)}\rvert}\right)$	$8,3,25,11,132$
$E^{(2)}$	$-W_2\left(E_t^{(2)}\right)\cdot W_3\left(E_t^{(2)}\right)\cdot W_{13}\left(E_t^{(2)}\right)\cdot\left(\frac{-1}{\lvert t_{(78)}\rvert}\right)$	$8,3,13,24$
$E^{(3)}$	$-W_2\left(E_t^{(3)}\right)\cdot W_3\left(E_t^{(3)}\right)\cdot W_5\left(E_t^{(3)}\right)\cdot W_{11}\left(E_t^{(3)}\right)\cdot\left(\frac{-1}{\lvert t_{(330)}\rvert}\right)$	$8,3,5,11,132$
$E^{(4)}$	$-W_2\left(E_t^{(4)}\right)\cdot W_3\left(E_t^{(4)}\right)\cdot W_5\left(E_t^{(4)}\right)\cdot W_{11}\left(E_t^{(4)}\right)\cdot\left(\frac{-1}{\lvert t_{(330)}\rvert}\right)$	$8,3,1,11,132$
$E^{(5)}$	$-W_2\left(E_t^{(5)}\right)\cdot W_3\left(E_t^{(5)}\right)\cdot W_5\left(E_t^{(5)}\right)\cdot W_{11}\left(E_t^{(5)}\right)\cdot\left(\frac{-1}{\lvert t_{(330)}\rvert}\right)$	$8,3,1,1,132$
$E^{(6)}$	$-W_2\left(E_t^{(6)}\right)\cdot W_3\left(E_t^{(6)}\right)\cdot W_5\left(E_t^{(6)}\right)\cdot\left(\frac{-1}{\lvert t_{(30)}\rvert}\right)$	$8,3,5,12$
$E^{(7)}$	$-W_2\left(E_t^{(7)}\right)\cdot W_3\left(E_t^{(7)}\right)\cdot W_5\left(E_t^{(7)}\right)\cdot W_{11}\left(E_t^{(7)}\right)\cdot\left(\frac{-1}{\lvert t_{(330)}\rvert}\right)$	$8,3,5,11,132$
$E^{(8)}$	$-W_2\left(E_t^{(8)}\right)\cdot W_3\left(E_t^{(8)}\right)\cdot W_5\left(E_t^{(8)}\right)\cdot W_{23}\left(E_t^{(8)}\right)\cdot\left(\frac{-1}{\lvert t_{(690)}\rvert}\right)$	$8,3,5,23,552$

Teorem 3.3.5. Neka je q kvadratno slobodan cijeli broj, takav da je rang krivulje $E_q^{(i)}(\mathbb{Q})$ pozitivan za barem jedan $i \in \{1,\ldots,8\}$. Tada postoji beskonačno racionalnih $D(q)$-petorki.

Dokaz. Bez smanjenja općenitosti možemo pretpostaviti da je $i = 6$, tako da je rang krivulje $E_q^{(6)}(\mathbb{Q})$ pozitivan. Ako je i bilo koji drugi indeks, dokaz je sličan. Petorka

$$\Big\{9(u-1)^3(4u-1)(u+1),$$

$$(u^4-6u^3+5u+27/4)(u^4-6u^3+8u^2-3u+3/4),$$

$$u^8-16u^6+32u^5-39/2u^4+10u^3+6u^2-9u+9/16,$$

$$(4u^4-16u^3+14u^2+4u+3)(u^4-2u^3+5/2u^2+3/4),$$

$$9(u^2-2u-1/2)^2(u^2+1/2)^2\Big\}$$

je $D(q(u))$-petorka za

$$q(u) = (4u^4-20u^3+13u^2+12u)\cdot\left(3(u-1)(u^2+1/2)(u^2-2u-1/2)\right)^2.$$

Evaluirajući elemente petorke te $q(u)$ u nekom $u_1 \in \mathbb{Q}$, dobit ćemo racionalnu $D(q_1)$-petorku za sve osim konačno mnogo iznimaka u_1. Moguće iznimke su racionalni u_1 takvi da je $q(u_1) = 0$, ili takvi da je neki element petorke evaluiran u u_1 jednak nuli, ili takvi da su bilo koja dva

elementa petorke evaluirani u u_1 jednaki. Takvi brojevi u_1 su korijeni konačnog broja polinoma u jednoj varijabli pa je skup iznimaka konačan.

Za fiksan q koji zadovoljava uvjete teorema, znamo da postoji beskonačno racionalnih parova (y_1, u_1) tako da vrijedi

$$y_1^2 q = 4u_1^4 - 20u_1^3 + 13u_1^2 + 12u_1. \tag{3.30}$$

Za svaki takav par (y_1, u_1), neka je

$$\eta = \frac{1}{y_1 \cdot 3(u_1-1)(u_1^2+1/2)(u_1^2-2u_1-1/2)}.$$

Vrijedi da je $q(u_1)\eta^2 = q$.

Tada je petorka

$$\begin{gathered}\Big\{9(u_1-1)^3(4u_1-1)(u_1+1)\eta,\\ (u_1^4-6u_1^3+5u_1+27/4)(u_1^4-6u_1^3+8u_1^2-3u_1+3/4)\eta,\\ (u_1^8-16u_1^6+32u_1^5-39/2u_1^4+10u_1^3+6u_1^2-9u_1+9/16)\eta,\\ (4u_1^4-16u_1^3+14u_1^2+4u_1+3)(u_1^4-2u_1^3+5/2u_1^2+3/4)\eta,\\ 9(u_1^2-2u_1-1/2)^2(u_1^2+1/2)^2\eta\Big\}\end{gathered} \tag{3.31}$$

racionalna $D(q)$-petorka, za sve osim konačno mnogo iznimnih parova (y_1, u_1). Zadnja stvar koju treba obrazložiti je zašto upravo opisan skup racionalnih $D(q)$-petorki nije konačan. Za svaku takvu petorku $\{A,B,C,D,E\}$ promatramo *kvadratnu* petorku $\{A^2,B^2,C^2,D^2,E^2\}$.

Kada bi skup (3.31) racionalnih $D(q)$-petorki bio konačan, onda bi bio konačan i njoj pridružen skup kvadratnih petorki. Lako se vidi da su elementi svake kvadratne petorke racionalne funkcije u varijabli u. Nije teško pokazati da ako postoji samo konačno mnogo različitih kvadratnih petorki, da se pojavljuje samo konačno različitih brojeva u_1. Budući da to nije istina, lažna je i pretpostavka da postoji samo konačno mnogo petorki opisanih sa (3.31). ■

Teorem 3.3.6. Uz pretpostavku Slutnje o parnosti vrijedi:

(a) Za svaki kvadratno slobodan $q \in \mathbb{N}$ u barem 295026 klasa ostataka mod 394680 postoji beskonačno racionalnih $D(q)$-petorki.

(b) Za svaki kvadratno slobodan $q \in -\mathbb{N}$ u barem 295435 klasa ostataka mod 394680 postoji beskonačno racionalnih $D(q)$-petorki.

Dokaz. Magma kod nalazi se u Odjeljku 5.2.3. Najmanji zajednički višekratnik perioda N_i iz Teorema 3.3.4 je 394680. Dokaz za negativne q se provodi na isti način kao i za pozitivne q pa pretpostavljamo da je q kvadratno slobodan prirodan broj. Teorem 3.3.4 (d) kaže da ako je q mod 120 u jednoj od 47 klasa ostataka da je rang krivulje $E_q^{(6)}(\mathbb{Q})$ pozitivan. Kombinirajući rezultate za preostale krivulje $E^{(i)}$ zaključujemo da ako je q u jednoj od 295026 klasa ostataka mod 394680 da je rang bar jedne od krivulja $E_q^{(i)}(\mathbb{Q})$ pozitivan. Teorem 3.3.5 završava dokaz. ■

Napomena 3.3.7. Postoji 296010 klasa ostataka mod 394680 koje sadrže kvadratno slobodne brojeve. Teorem 3.3.6 pokriva 99.5% svih klasa mod 394680. Slutimo da Teorem 3.3.6 vrijedi za sve kvadratno slobodne $q \in \mathbb{Z}$, a time i za sve $q \in \mathbb{Q}$, ali to nismo uspjeli dokazati.

Slutnja 3.3.8. Za svaki $q \in \mathbb{Q}$ postoji beskonačno mnogo racionalnih $D(q)$-petorki.

Napomena 3.3.9. Za svaki kvadratno slobodan $q \in \mathbb{Z}$ takav da je $|q| < 1000$ te $q \neq 19,341$ vrijedi da je rang barem jedne od krivulja $E_q^{(i)}$ neparan, a onda nužno i pozitivan. Posebno, za $q = 341$ vrijedi $\mathrm{Rang}(E_q^{(1)}) = \mathrm{Rang}(E_q^{(3)}) = \mathrm{Rang}(E_q^{(8)}) = 2$. Za $q = 19$, Petričević je eksperimentalno pronašao velik broj racionalnih $D(q)$-petorki. Najmanji pozitivan q za kojeg ne znamo postoje li racionalne $D(q)$-petorke je 1579.

Radi potpunosti, navodimo $D(q(u))$-petorke za sve $E_i, i \in \{1,\ldots,8\}$.

$$\Big\{900u^4+4320u^3-1161u^2-3438u+1404,$$
$$1600u^4-1600u^3+1100u^2-920u+396,$$
$$100u^4+1760u^3-1201u^2-542u+324, \tag{3.32}$$
$$2500u^4-4000u^3+959u^2+514u+36,$$
$$3600u^4-2880u^3-1584u^2+864u+324\Big\}$$

je $D\Big((-1200u^3+1645u^2-410u-35)\cdot\big[6(10u^2-4u-3)\big]^2\Big)$-petorka,

$$\Big\{378u^2-405u+108,$$
$$32u^4-64u^3+122u^2-117u+36,$$
$$32u^4-16u^3+80u^2-78u+18,$$
$$128u^4-160u^3+26u^2+15u,$$

$$288u^4-288u^3+90u^2-9u\Big\}$$

je $D\left((-80u^4+148u^3-65u^2-12u+9)\cdot[3(4u-1)]^2\right)$-petorka,

$$\Big\{352u^4-244u^3-129u^2+122u-20,$$

$$4u^6+16u^5+48u^4+48u^3-164u^2+104u-20,$$

$$4u^6-24u^5+112u^4-120u^3+47u^2-14u+4,$$

$$16u^6-16u^5-32u^4+100u^3-105u^2+58u-12,$$

$$36u^6-96u^5+112u^4-88u^3+48u^2-16u+4\Big\}$$

je $D\left((-28u^4-44u^3+157u^2-106u+21)\cdot\left[2(3u^2-u+1)\cdot(u-1)\right]^2\right)$-petorka,

$$\Big\{-54u^2+171u-90,$$

$$32u^4-96u^3-6u^2+127u-30,$$

$$32u^4+144u^3-24u^2-26u-18,$$

$$128u^4+96u^3-6u^2+31u-6,$$

$$288u^4+576u^3-54u^2-117u-18\Big\}$$

je $D\left((112u^4-100u^3-93u^2+92u-11)\cdot[3\cdot(4u+1)]^2\right)$-petorka,

$$\Big\{450u^4-1665u^3+2052u^2-909u+72,$$

$$50u^4-545u^3+1092u^2-317u+44,$$

$$800u^4-350u^3+30u^2-158u+2,$$

$$1250u^4-125u^3+192u^2-41u+20,$$

$$4050u^4-405u^3-648u^2-81u\Big\}$$

je $D\left((300u^3-65u^2+16u+1)\cdot[9\cdot(5u+1)\cdot(u-1)]^2\right)$-petorka,

$$\Big\{576u^5-1296u^4+288u^3+1152u^2-864u+144,$$

$$16u^8-192u^7+704u^6-736u^5-72u^4-80u^3+624u^2-264u+81,$$

$$16u^8-256u^6+512u^5-312u^4+160u^3+96u^2-144u+9,$$

$$64u^8-384u^7+896u^6-1024u^5+528u^4-128u^3+288u^2+48u+36,$$

$$144u^8-576u^7+576u^6-288u^5+504u^4+144u^3+144u^2+72u+9\Big\}$$

je $D\left((4u^4-20u^3+13u^2+12u)\left[12\cdot(2u^2+1)\cdot(2u^2-4u-1)\cdot(u-1)\right]^2\right)$-petorka,

$$\Big\{25u^2+30u+20,$$

$$4u^2+24u+20,$$

$$9u^2-2u-4,$$

$$u^2+14u+12,$$

$$16u^2-4\Big\}$$

je $D\left((-40u^3-19u^2+38u+21)\cdot 2^2\right)$-petorka i konačno

$$\Big\{324u^4+423u^2-198u+180,$$

$$64u^4+320u^3-52u^2-248u+60,$$

$$100u^4-256u^3+239u^2+106u+36,$$

$$4u^4+128u^3-49u^2-86u+12,$$

$$144u^4-576u^3+432u^2+288u+36\Big\}$$

je $D\left((-144u^3+61u^2+94u-11)\cdot\left[6\cdot(2u^2-4u-1)\right]^2\right)$-petorka.

4. RACIONALNE $D(q)$-TROJKE

U ovom poglavlju parametriziramo racionalne $D(q)$-trojke, za svaki racionalan q koji nije potpun kvadrat. Koristimo tu parametrizaciju kako bismo parametrizirali sve racionalne $D(q)$-trojke koje su ujedno i $D(0)$-trojke te kako bismo parametrizirali sve racionalne $D(q)$-četvorke koje sadrže barem jednu regularnu $D(q)$-trojku.

4.1. PRETHODNI REZULTATI I KONSTRUKCIJE

Kazalicki i Naskręcki su u [28] otkrili nov način za parametrizaciju racionalnih Diofantovih trojki. Prilagodit ćemo njihovu konstrukciju kako bismo parametrizirali racionalne $D(q)$-trojke.

Prateći [28], neka je K polje karakteristike različite od 2 te $\mathbb{A}$ afini prostor nad K. Neka je

$$\mathcal{D}\colon \quad ab+q=r^2, \quad ac+q=s^2, \quad bc+q=t^2$$

afina mnogostrukost u $\mathbb{A}^6$, i neka je

$$\widetilde{\mathcal{D}}=\mathcal{D}\setminus\{abc(a-b)(a-c)(b-c)=0\}.$$

Definiramo mnogostrukosti X i $\widetilde{X}$ u $\mathbb{A}^4$ sa

$$\begin{aligned} X\colon &\quad (x^2-q)(y^2-q)(z^2-q)=k^2,\\ \widetilde{X}\colon &\quad X\setminus\{k(x^2-y^2)(x^2-z^2)(y^2-z^2)=0\}. \end{aligned}$$

Biracionalna preslikavanja $p\colon \mathcal{D}\to X$ te $p'\colon X\to\mathcal{D}$ dana sa

$$\begin{aligned} p(a,b,c,r,s,t)&=(r,s,t,abc),\\ p'(x,y,z,k)&=\left(\frac{k}{z^2-q},\frac{k}{y^2-q},\frac{k}{x^2-q},x,y,z\right) \end{aligned}$$

definiraju bijekciju skupova $\widetilde{\mathcal{D}}(K)$ i $\widetilde{X}(K)$, K-racionalnih točaka na mnogostrukostima $\widetilde{\mathcal{D}}$ i $\widetilde{X}$.

Fiksirajmo $K = \mathbb{Q}(\sqrt{q})$ za neki racionalan q koji nije potpun kvadrat. Neka je $\overline{X} \subset \mathbb{P}^4$ projektivno zatvorenje mnogostrukosti X,

$$\overline{X}\colon (x^2 - w^2q)(y^2 - w^2q)(z^2 - w^2q) = k^2w^4.$$

Propozicija 4.1.1. Projektivna mnogostrukost $\overline{X}$ je biracionalno ekvivalentna $\mathbb{P}^3(K)$.

Dokaz. Neka je $\phi\colon \overline{X} \to \mathbb{P}^3(K)$ racionalno preslikavanje

$$\begin{aligned}\phi([x:y:z:k:w]) = [&y\cdot(w\sqrt{q}-x)(w^2q-y^2):\\ &z\cdot(w\sqrt{q}-x)(w^2q-y^2):\\ &kw^3\sqrt{q}:\\ &w\sqrt{q}\cdot(w\sqrt{q}-x)(w^2q-y^2)]\end{aligned}$$

te neka je $\psi\colon \mathbb{P}^3(K) \to \overline{X}$ preslikavanje

$$\begin{aligned}\psi([t_1:t_2:t_3:t_0]) = \Big[&t_0\cdot\Big(t_3^2(t_1^2-t_2^2)-(t_0^2-t_2^2)(t_0^2+t_3^2)\Big):\\ &t_1\cdot\Big((t_0^2-t_2^2)(t_0^2-t_3^2)+t_3^2(t_1^2-t_2^2)\Big):\\ &t_2\cdot\Big((t_0^2-t_2^2)(t_0^2-t_3^2)+t_3^2(t_1^2-t_2^2)\Big):\\ &2qt_3\cdot(t_1^2-t_0^2)(t_2^2-t_0^2):\\ &\frac{t_0}{\sqrt{q}}\cdot\Big((t_0^2-t_2^2)(t_0^2-t_3^2)+t_3^2(t_1^2-t_2^2)\Big)\Big].\end{aligned}$$

Direktnim računom (Magma kod u odjeljku 5.3.1) provjeravamo da su $\phi\circ\psi$ i $\psi\circ\phi$ identitete pa su oba preslikavanja ϕ i ψ biracionalna. ■

4.2. PARAMETRIZACIJA $D(q)$-TROJKI

Koristeći preslikavanja p' i ψ možemo parametrizirati K-racionalne $D(q)$-trojke. To su trojke brojeva $\{a,b,c\}$ u K takve da su $ab+q$, $bc+q$, $ac+q$ kvadrati u K.

Računamo

$$\begin{aligned}a &= \left.\frac{\frac{k}{w}}{\left(\frac{z}{w}\right)^2-q}\right|_{t_0=1} = \frac{2\sqrt{q}\cdot t_3(t_1^2-1)}{t_3^2(t_1^2-1)+1-t_2^2},\\ b &= \left.\frac{\frac{k}{w}}{\left(\frac{y}{w}\right)^2-q}\right|_{t_0=1} = \frac{2\sqrt{q}\cdot t_3(t_2^2-1)}{t_3^2(t_1^2-1)+1-t_2^2},\\ c &= \left.\frac{\frac{k}{w}}{\left(\frac{x}{w}\right)^2-q}\right|_{t_0=1} = \frac{\sqrt{q}\cdot(t_3^2(t_1^2-1)+1-t_2^2)}{2t_3}.\end{aligned}$$

Iz prethodnih jednakosti slijedi

$$ac+q=qt_1^2, \quad bc+q=qt_2^2, \quad ab+q=q\cdot\left(\frac{t_3^2(t_1^2-1)+t_2^2-1}{t_3^2(t_1^2-1)-(t_2^2-1)}\right)^2.$$

Nas zanimaju racionalne $D(q)$-trojke. Da bi K-racionalna $D(q)$-trojka bila racionalna $D(q)$-trojka, brojevi a,b i c moraju biti racionalni, a brojevi $ab+q, bc+q$ i $ac+q$ moraju biti racionalni kvadrati. Navedene uvjete možemo pojednostavniti, dovoljno je da su $ab+q, bc+q$ i $ac+q$ racionalni kvadrati te da je jedan od brojeva a,b ili c racionalan, jer racionalnost preostala dva lagano slijedi.

Teorem 4.2.1. Neka su u_1,u_2,u i $q\in\mathbb{Q}$, takvi da q nije potpun kvadrat. Trojka (a,b,c) definirana sa

$$\begin{aligned} a&=\frac{(u^2-q)(u_1^2-q)}{(u^2+q)(u_2-u_1)+2u(u_1u_2-q)},\\ b&=\frac{(u^2-q)(u_2^2-q)}{(u^2+q)(u_2-u_1)+2u(u_1u_2-q)},\\ c&=\frac{(u^2+q)(u_2-u_1)+2u(u_1u_2-q)}{u^2-q} \end{aligned}$$

je racionalna $D(q)$-trojka, ako nije degenerirana, to jest, ako su a,b i c racionalni, međusobno različiti brojevi koji su različiti od nule. Svaka racionalna $D(q)$-trojka ostvaruje se ovom parametrizacijom. Uvjetima degeneriranosti bavimo se u Propoziciji 4.2.2

Dokaz. Kako bi ispunili $ac+q=\square$ i $bc+q=\square$, očito mora vrijediti

$$t_1=u_1\sqrt{q} \quad \text{i} \quad t_2=u_2\sqrt{q}, \quad \text{za neke } u_1,u_2\in\mathbb{Q}.$$

Označimo $t_3=\alpha+\beta\sqrt{q}, \quad \text{za } \alpha,\beta\in\mathbb{Q}$, kao i

$$r_1=\alpha^2+q\beta^2, \quad r_2=t_2^2-1=qu_2^2-1, \quad r_3=2\alpha\beta(t_1^2-1)=2\alpha\beta(qu_1^2-1).$$

Tada je

$$\begin{aligned} ab+q&=q\left(\frac{r_1+r_2+r_3\sqrt{q}}{r_1-r_2+r_3\sqrt{q}}\right)^2=q\left(\frac{(r_1+r_2+r_3\sqrt{q})(r_1-r_2-r_3\sqrt{q})}{(r_1-r_2)^2-qr_3^2}\right)^2\\ &=q\left(\frac{r_1^2-r_2^2-qr_3^2-2r_2r_3\sqrt{q}}{(r_1-r_2)^2-qr_3^2}\right)^2. \end{aligned}$$

Kako bi posljednji izraz bio racionalan kvadrat mora vrijediti

$$r_1^2-r_2^2-qr_3^2=0\iff\alpha^2-q\beta^2=\pm\frac{qu_2^2-1}{qu_1^2-1}=\varepsilon\frac{qu_2^2-1}{qu_1^2-1}. \tag{4.1}$$

Konačno, analiziramo uvjet $c \in \mathbb{Q}$. Označimo sa $\overline{t_3} = \alpha - \beta\sqrt{q}$. Jednakost (4.1) možemo zapisati kao

$$t_3\overline{t_3}(qu_1^2 - 1) = \varepsilon(qu_2^2 - 1). \tag{4.2}$$

$$\begin{aligned} c &= \frac{\sqrt{q}\cdot(t_3^2(t_1^2-1)+1-t_2^2)}{2t_3} = \frac{\sqrt{q}\cdot(t_3\cdot t_3\cdot\overline{t_3}(qu_1^2-1)+\overline{t_3}(1-qu_2^2))}{2t_3\cdot\overline{t_3}} \\ &\overset{(4.2)}{=} \frac{\sqrt{q}\cdot(t_3\cdot\varepsilon(qu_2^2-1)+\overline{t_3}(1-qu_2^2))}{2(\alpha^2-q\beta^2)} = \frac{qu_2^2-1}{2(\alpha^2-q\beta^2)}\cdot\sqrt{q}\cdot(t_3\varepsilon-\overline{t_3}). \end{aligned}$$

Broj $\sqrt{q}(t_3\varepsilon - \overline{t_3})$ mora biti racionalan iz čega slijedi $\varepsilon = 1$. Preostalo je pronaći sve racionalne α, β, u_1 te u_2 koji zadovoljavaju (4.1), uz uvjet $\varepsilon = 1$. Primijetimo da ako nađemo jedno rješenje (α_0, β_0) u varijablama (α, β), da možemo pronaći sva, jer je (4.1) konika u varijablama α i β. Koristimo normu na $\mathbb{Q}(\sqrt{q})$ kako bismo pronašli jedno rješenje.

$$N(\alpha+\beta\sqrt{q}) = \alpha^2 - q\beta^2 = \frac{qu_2^2-1}{qu_1^2-1} = \frac{N(1+u_2\sqrt{q})}{N(1+u_1\sqrt{q})} = N\left(\frac{1-u_1u_2q+(u_2-u_1)\sqrt{q}}{1-qu_1^2}\right)$$

nas vodi do

$$\alpha_0 = \frac{1-u_1u_2q}{1-qu_1^2}, \quad \beta_0 = \frac{u_2-u_1}{1-qu_1^2}. \tag{4.3}$$

Koristimo istu tehniku kao i pri rješavanju jednadžbe (3.19).

Pravac $\alpha - \alpha_0 = u\cdot(\beta - \beta_0)$ za $u \in \mathbb{Q}$ siječe koniku (4.1) u dvije racionalne točke. Jedna od njih je (α_0, β_0), a druga je opće rješenje jednadžbe (4.1):

$$\begin{aligned} \alpha &= \frac{(u^2+q)(1-u_1u_2q)+2qu(u_1-u_2)}{(u^2-q)(qu_1^2-1)}, \\ \beta &= \frac{(u^2+q)(u_1-u_2)+2u(1-u_1u_2q)}{(u^2-q)(qu_1^2-1)}. \end{aligned}$$

Uvrštavanjem t_1, t_2 i t_3 koji ovise o racionalnim brojevima u_1, u_2 te u u jednadžbe za a, b i c dobivamo

$$\begin{aligned} a &= \frac{(u^2-q)(1-u_1^2q)}{(u^2+q)(u_2-u_1)+2u(u_1u_2q-1)}, \\ b &= \frac{(u^2-q)(1-u_2^2q)}{(u^2+q)(u_2-u_1)+2u(u_1u_2q-1)}, \\ c &= -q\frac{(u^2+q)(u_2-u_1)+2u(u_1u_2q-1)}{u^2-q}. \end{aligned}$$

Konačno, ako zamijenimo parametre u_1 te u_2 sa u_1/q te u_2/q i promijenimo predznak brojevima a, b i c, dolazimo do tvrdnje teorema. Napomenimo kako vrijede jednakosti

$$ac+q = u_1^2, \quad bc+q = u_2^2, \quad ab+q = \left(\frac{(q+u^2)(u_1u_2-q)+2qu(u_2-u_1)}{(q+u^2)(u_2-u_1)+2u(u_1u_2-q)}\right)^2.$$

■

Propozicija 4.2.2. Trojka (a,b,c) dobivena parametrizacijom iz Teorema 4.2.1 je degenerirana ako i samo ako vrijedi bilo koji od sljedećih uvjeta:

(i) $u_1^2 = u_2^2$,

(ii) $u_2 = \dfrac{2uq+(u^2+q)u_1}{u^2+q+2uu_1}$,

(iii) $u_1 = \dfrac{w_1^2+q}{2w_1}$ te $\left(u_2 = \dfrac{q+uw_1}{u+w_1} \quad \text{ili} \quad u_2 = \dfrac{q(u+w_1)}{q+uw_1}\right)$, za neki $w_1 \in \mathbb{Q}$,

(iv) $u_2 = \dfrac{w_2^2+q}{2w_2}$ te $\left(u_1 = \dfrac{q+uw_2}{u+w_2} \quad \text{ili} \quad u_1 = \dfrac{q(u+w_2)}{q+uw_2}\right)$, za neki $w_2 \in \mathbb{Q}$.

Dokaz. Trojka je degenerirana ako je bilo koji element jednak nuli, bilo koji element nije definiran ili ako su bilo koja dva elementa međusobno jednaka.

Budući da q nije potpun kvadrat, a i b ne mogu biti jednaki nula, a broj c je uvijek definiran. Nazivnici od a i b te brojnik od c su isti broj (barem u neskraćenom obliku u parametrizaciji Teorema 4.2.1) pa je dovoljno gledati kada je taj broj jednak nula. Lako se izračuna da je to točno slučaj (ii) naše propozicije. Također se lako vidi da je uvjet $a = b$ slučaj (i) naše propozicije.

Uvjeti $a = c$ te $b = c$ su simetrični za računanje (zamjenom varijabli u_1 i u_2) te je dovoljno riješiti jedan od ta dva uvjeta. Promotrimo što se zbiva kada je $a = c$. Izjednačavanjem izraza za a i c imamo

$$u_1^2 - q = \left(\frac{(u^2+q)(u_2-u_1)+2u(u_1u_2-q)}{u^2-q}\right)^2 = c^2. \tag{4.4}$$

Vidimo da $u_1^2 - q$ mora biti potpun kvadrat, što je istina ako i samo ako je $u_1 = \dfrac{w_1^2+q}{2w_1}$, za $w_1 \in \mathbb{Q}$. Korjenovanjem jednadžbe (4.4) nakon malo sređivanja imamo

$$u_2 = \frac{(u^2+q)(w_1^2+q)+2uq \pm (u^2-q)(w_1^2-q)}{2(u+w_1)(q+uw_1)}.$$

Ako u brojniku umjesto $\pm$ piše $+$, odnosno $-$, dobijemo da je

$$u_2 = \frac{q+uw_1}{u+w_1} \quad \text{odnosno} \quad u_2 = \frac{q(u+w_1)}{q+uw_1}.$$

Uvjet $a = c$ je opisan slučajem (iii) naše propozicije. Kao što smo već naveli, uvjet $b = c$ je simetričan računom i opisan je slučajem (iv) propozicije. Time je propozicija dokazana. ■

4.3. REZULTATI KOJI KORISTE PARAMETRIZACIJU

4.3.1. Racionalne $D(q)$-trojke koje su i $D(0)$-trojke

Definicija 4.3.1. *Racionalna $D(0)$-trojka* (a,b,c) je trojka racionalnih brojeva takvih da su ab, bc i ac potpuni kvadrati.

Želimo parametrizirati sve racionalne $D(q)$-trojke koje su ujedno i $D(0)$-trojke. Primijetimo da ako su dva broja iz skupa $\{ab,bc,ac\}$ kvadrati, da je nužno i treći broj kvadrat jer je $(ab)(bc)(ac) = (abc)^2$. Koristeći parametrizaciju racionalnih $D(q)$-trojki Teorema 4.2.1 možemo parametrizirati $D(q)$-trojke koje su ujedno i $D(0)$-trojke.

Teorem 4.3.2. Svaka racionalna $D(q)$-trojka koja je i $D(0)$-trojka parametrizirana je sa $w_1, w_2, u \in \mathbb{Q}$ izrazima

$$\begin{aligned} a &= \frac{w_2(w_1^2-q)^2(u^2-q)}{2w_1(uw_1-uw_2-w_1w_2+q)(uw_1w_2-qu-qw_1+qw_2)}, \\ b &= \frac{w_1(w_2^2-q)^2(u^2-q)}{2w_2(uw_1-uw_2-w_1w_2+q)(uw_1w_2-qu-qw_1+qw_2)}, \\ c &= \frac{(uw_1-uw_2-w_1w_2+q)(uw_1w_2-qu-qw_1+qw_2)}{2w_1w_2(u^2-q)}, \end{aligned}$$

ako trojka (a,b,c) nije degenerična.

Dokaz. Vrijedi $ac = u_1^2 - q$ te $bc = u_2^2 - q$ iz čega se lako dobije da je nužno i dovoljno da je

$$u_1 = \frac{w_1^2+q}{2w_1}, \quad u_2 = \frac{w_2^2+q}{2w_2}, \quad w_1, w_2 \in \mathbb{Q}.$$

■

Postoji elegantnija, simetrična parametrizacija takvih trojki.

Teorem 4.3.3. Sve racionalne $D(q)$-trojke koje su i $D(0)$-trojke parametrizirane su sa $t_1, t_2, t_3 \in \mathbb{Q}$ izrazima

$$a = \frac{1}{2}\frac{\left(\frac{q}{t_1}-t_1\right)\left(\frac{q}{t_2}-t_2\right)}{\frac{q}{t_3}-t_3}, \quad b = \frac{1}{2}\frac{\left(\frac{q}{t_2}-t_2\right)\left(\frac{q}{t_3}-t_3\right)}{\frac{q}{t_1}-t_1}, \quad c = \frac{1}{2}\frac{\left(\frac{q}{t_3}-t_3\right)\left(\frac{q}{t_1}-t_1\right)}{\frac{q}{t_2}-t_2}.$$

Trojka nije degenerična ako vrijede sljedeći uvjeti, gdje je $i \neq j$:

$$t_i \neq 0, \quad t_i \neq \pm t_j, \quad t_i t_j \neq \pm q.$$

Dokaz. Neka je $ab+q=r^2$ te $ab=d^2$. Slično kao u dokazu Teorema 4.3.2, nužno je i dovoljno da je $d=\frac{1}{2}\left(\frac{q}{t_1}-t_1\right)$, za neki $t_1\in\mathbb{Q}$. Slično, ako je $ac=e^2$ i $bc=f^2$, mora biti

$$e=\frac{1}{2}\left(\frac{q}{t_2}-t_2\right),\quad f=\frac{1}{2}\left(\frac{q}{t_3}-t_3\right),\qquad \text{za neke } t_2,t_3\in\mathbb{Q}.$$

Sada je

$$|a|=\sqrt{a^2}=\sqrt{(ab)(ac)/(bc)}=\sqrt{d^2e^2/f^2}=|de/f|$$

iz čega slijedi $|b|=|fd/e|$ te $|c|=|ef/d|$. Primijetimo da su elementi a,b i c ili svi istovremeno pozitivni ili istovremeno negativni jer su umnošci ab,bc te ac kvadrati. Ako nam parametri (t_1,t_2,t_3) daju trojku (a,b,c), onda nam parametri $(-t_1,t_2,t_3)$ daju trojku $(-a,-b,-c)$, zato je svaka trojka ostvarena navedenom parametrizacijom.

Računski se provjeri da je trojka (a,b,c) opisana gornjom parametrizacijom zaista racionalna $D(q)$ i $D(0)$-trojka. ■

Propozicija 4.3.4. Parametrizacije iz Teorema 4.3.2 i 4.3.3 su biracionalno ekvivalentne.

Dokaz. Definiramo preslikavanja $\phi_1\colon \mathbb{A}^3(\mathbb{Q})\to\mathbb{A}^3(\mathbb{Q})$ i $\psi_1\colon \mathbb{A}^3(\mathbb{Q})\to\mathbb{A}^3(\mathbb{Q})$ jednadžbama

$$\phi_1(w_1,w_2,u)=\left(w_1,\frac{w_2w_1u+w_2q-w_1q-qu}{w_2w_1+w_2u-w_1u-q},w_2\right),$$

$$\psi_1(t_1,t_2,t_3)=\left(t_1,t_3,\frac{q(t_2+t_3-t_1)-t_1t_2t_3}{q+t_2t_3-t_1t_2-t_1t_3}\right).$$

Računski se provjeri da su $\phi\circ\psi$ te $\psi\circ\phi$ identitete, kao i sljedeća činjenica: Ako je $\mathcal{P}_1(w_1,w_2,u)$ parametrizacija iz Teorema 4.3.2, a $\mathcal{P}_2(t_1,t_2,t_3)$ parametrizacija iz Teorema 4.3.3, onda vrijedi

$$\mathcal{P}_1=\mathcal{P}_2\circ\phi_1,\quad \mathcal{P}_2=\mathcal{P}_1\circ\psi_1.$$

■

4.3.2. Racionalne $D(q)$-četvorke koje sadrže regularnu trojku

Neka je (a,b,c) racionalna $D(q)$-trojka dobivena parametrizacijom iz Teorema 4.2.1. Znamo da je $ac+q=u_1^2$ i definiramo $d=a+c+2u_1$, tada su $ad+q$ te $cd+q$ kvadrati. Da bi (a,b,c,d) bila racionalna $D(q)$-četvorka, broj $bd+q$ mora biti kvadrat, a četvorka (a,b,c,d) ne smije biti degenerična. Pripadajući Magma kod je u Odjeljku 5.3.2. Izraz $bd+q$ jednak je

$$bd+q=f_3(u,u_1,u_2,q)^{-2}\left(f_2(u,u_2,q)u_1^2+f_1(u,u_2,q)u_1+f_0(u,u_2,q)\right),$$

gdje su f_i polinomi zadani formulama

$$\begin{aligned}
f_3(u,u_1,u_2,q) &= (u_2u-u^2/2-q/2)u_1+u_2u^2/2+u_2q/2-uq,\\
f_2(u,u_2,q) &= u_2^4u^2-2u_2^3uq+u_2^2q^2-u_2u^3q+u_2uq^2+u^4q/4+u^2q^2/2-3q^3/4,\\
f_1(u,u_2,q) &= u_2^4u^3+u_2^4uq-3u_2^3u^2q-u_2^3q^2+2u_2^2uq^2-u_2u^4q/2+u2q^3/2+u^3q^2-uq^3,\\
f_0(u,u_2,q) &= \frac{1}{4}(u_2^4u^4+2u_2^4u^2q+u_2^4q^2-4u_2^3u^3q-4u_2^3uq^2-u_2^2u^4q\\
&\qquad +6u_2^2u^2q^2-u_2^2q^3+u^4q^2-2u^2q^3+q^4).
\end{aligned}$$

Zanima nas kada će

$$\mathcal{P}(u_1) := f_2(u,u_2,q)u_1^2+f_1(u,u_2,q)u_1+f_0(u,u_2,q),$$

polinom varijable u_1 nad poljem $\mathbb{Q}(u,u_2,q)$, biti potpun kvadrat. Računskom provjerom vidimo da vrijedi

$$\mathcal{P}(u_2) = f_2(u,u_2,q)u_2^2+f_1(u,u_2,q)u_2+f_0(u,u_2,q) = \Big((u_2u+u^2/2-q/2)(u_2^2-q)\Big)^2.$$

Slično kao pri rješavanju jednadžbi (3.19) ili (4.1), uvodimo novi parametar z te želimo pronaći rješenja kvadratne jednadžbe

$$\Big(z(u_1-u_2)+(u_2u+u^2/2-q/2)(u_2^2-q)\Big)^2 = \mathcal{P}(u_1)$$

po varijabli u_1. Znamo da je jedno rješenje $u_1=u_2$, a drugo rješenje je racionalna funkcija $u_1(u,u_2,z,q)$ takva da je $\mathcal{P}(u_1(u,u_2,z,q)) \in (\mathbb{Q}(u,u_2,z,q)^*)^2$. Opće rješenje je

$$u_1 = \frac{\mathcal{B}(u,u_2,z,q)}{\mathcal{N}(u,u_2,z,q)} \tag{4.5}$$

gdje su polinomi $\mathcal{B}$ i $\mathcal{N}$ dani formulama

$$\begin{aligned}
\mathcal{B}(u,u_2,z,q) =& -u_2^5u^2-u_2^4u^3+u_2^4uq+3u_2^3u^2q+2u_2^3uz+u_2^2u^3q+u_2^2u^2z-3u_2^2uq^2-u_2^2qz\\
&+u_2u^4q/4-u_2u^2q^2/2-2u_2uqz+u_2q^3/4-u_2z^2-u^3q^2-u^2qz+uq^3+q^2z,\\
\mathcal{N}(u,u_2,z,q) =& u_2^4u^2-2u_2^3uq+u_2^2q^2-u_2u^3q+u_2uq^2+u^4q/4+u^2q^2/2-3q^3/4-z^2.
\end{aligned}$$

Teorem 4.3.5. Neka su u,u_2 te z slobodni racionalni parametri, u_1 određen jednadžbom (4.5), brojevi a,b te c određeni parametrizacijom Teorema 4.2.1, te $d=a+c+2u_1$.

Četvorka brojeva (a,b,c,d) parametrizirana sa (u,u_2,z) je racionalna $D(q)$-četvorka koja sadrži regularnu trojku (a,c,d), ako četvorka (a,b,c,d) nije degenerična. Svaka racionalna $D(q)$-četvorka koja sadrži regularnu trojku realizira se ovom parametrizacijom.

Napomena 4.3.6. Mnoge dosadašnje konstrukcije $D(q)$-m-torki počinjale su od $D(q)$-para kojeg se po regularnosti proširilo do $D(q)$-trojke. Parametrizacija svih $D(q)$-trojki može dovesti do novih ideja u takvim konstrukcijama. Kao primjere navodimo konstrukciju petorki u Poglavlju 3, kao i konstrukciju *jakih $D(q)$-trojki* u članku Dujelle, Paganina i Sadeka [20].

5. MAGMA KODOVI

U ovom poglavlju navodimo eksplicitne kodove u računalnom programu Magma koje smo koristili u radu, zajedno s komentarima kako bi se lakše koristili. Kodovi su pripremljeni kako bi se mogli direktno kopirati i koristiti, svaki komentar unutar koda počinje s dvije kose crte //.

5.1. KODOVI KORIŠTENI U DRUGOM POGLAVLJU

5.1.1. Osnovni račun za krivulju E_m

Kod korišten za račune na stranicama 26 i 27 :

```
QQ:=Rationals();
U<x1,y1,q>:=FunctionField(QQ,3);
   // Funkcijsko polje u parametrima x1,y1,q.
L<x,y>:=PolynomialRing(U,2);
m:=(x1^2-q)*(y1^2-q);
   // Kako bi (x1,y1) stvarno bila na D_m, broj m definiramo ovako.
D:=Curve(AffineSpace(L),(x^2-q)*(y^2-q)-m);
Dbar:=ProjectiveClosure(D);
   //Krivulja D_m i njeno projektivno zatvorenje.
P1:=Dbar![x1,y1];
RDbar:=Dbar![-y1,x1];
SDbar:=Dbar![-x1,y1];
   // tocke na krivulji Dbar
E1,f1:=EllipticCurve(Dbar,P1);
d2:=4*q^2-2*m;
d1:=m^2;
```

```
E:=EllipticCurve([0,d2,0,d1,0]);
_,e1:=IsIsomorphic(E1,E);
_,ff1:=IsInvertible(f1);
_,ee1:=IsIsomorphic(E,E1);
   // Krivulje Dbar, E1 te E (u radu oznacavana sa E_m) su biracionalne.
   // Krivulja E1 je pomocna krivulja koju ne spominjemo u radu.
R:=e1(f1(RDbar));
S:=e1(f1(SDbar));    //tocke na E
f:=f1*e1;
_,f_inv:=IsInvertible(f);
   // biracionalna preslikavanja f:Dbar -> E te f_inv:E -> Dbar
DD<j,k>:=FunctionField(Dbar);
pom:=f([j,k]);
   //[j,k] je genericka tocka na Dbar, pom je njena slika na E.
f_inv(S-pom);
f_inv(R+pom);        // Provjera jednakosti (2.1).
de:=DefiningEquations(f_inv);
proj_g:=map<Domain(f_inv)->ProjectiveSpace(U,1)|
[(de[1]^2-q*de[3]^2)*(x1^2-q),de[3]^2]>;
g:=map<Domain(f_inv)->AffineSpace(U,1)|
[((de[1]/de[3])^2-q)*(x1^2-q)]>;
   // Projektivna i afina verzija funkcije g.
```

5.1.2. Kod iz Propozicije 2.2.1

Kod korišten u dokazu dijelova Propozicije 2.2.1. Kako bi računali nad poljem $\mathbb{Q}(\sqrt{q})$ koristimo trik. Funkcijsko polje ćemo definirati pomoću parametra q1, a onda ćemo staviti $q = (q1)^2$.

```
QQ:=Rationals();
U<x1,y1,q1>:=FunctionField(QQ,3);
q:=q1^2;
L<x,y>:=PolynomialRing(U,2);
m:=(x1^2-q)*(y1^2-q);
```

```
D:=Curve(AffineSpace(L),(x^2-q)*(y^2-q)-m);
Dbar:=ProjectiveClosure(D);
P1:=Dbar![x1,y1];
RDbar:=Dbar![-y1,x1];
SDbar:=Dbar![-x1,y1];
  // tocke na krivulji Dbar
E1,f1:=EllipticCurve(Dbar,P1);
d2:=4*q^2-2*m;
d1:=m^2;
E:=EllipticCurve([0,d2,0,d1,0]);
_,e1:=IsIsomorphic(E1,E);
_,ff1:=IsInvertible(f1);
_,ee1:=IsIsomorphic(E,E1);
R:=e1(f1(RDbar));
S:=e1(f1(SDbar));
f:=f1*e1;
_,f_inv:=IsInvertible(f);

de:=DefiningEquations(f_inv);
proj_g:=map<Domain(f_inv)->ProjectiveSpace(U,1)|
[(de[1]^2-q*de[3]^2)*(x1^2-q),de[3]^2]>;
g:=map<Domain(f_inv)->AffineSpace(U,1)|
[((de[1]/de[3])^2-q)*(x1^2-q)]>;

_,R1:=IsDivisibleBy(S,2);
R2:=R1+2*R;
S1:=R1-R;
S2:=R2+R;
  // Definicija tocaka R1, R2, S1, S2.
proj_g(S1);
proj_g(S2);
proj_g(R1);
```

```
proj_g(R2);
  // Provjera da su tocke S1, S2 nultocke od g te R1, R2 polovi od g.
```

5.1.3. Kod za primjer iz Propozicije 2.4.2

U Odjeljku 2.4 nalaze se primjeri, ovo je kod za računanje s primjerom iz Propozicije 2.4.2:

```
QQ:=Rationals();
U<t>:=FunctionField(QQ);
x1:=1;
q:=-3;
y1:=t;
L<x,y>:=PolynomialRing(U,2);
m:=(x1^2-q)*(y1^2-q);
D:=Curve(AffineSpace(L),(x^2-q)*(y^2-q)-m);
Dbar:=ProjectiveClosure(D);
P1:=Dbar![x1,y1];
RDbar:=Dbar![-y1,x1];
SDbar:=Dbar![-x1,y1];
E1,f1:=EllipticCurve(Dbar,P1);
d2:=4*q^2-2*m;
d1:=m^2;
E:=EllipticCurve([0,d2,0,d1,0]);
_,e1:=IsIsomorphic(E1,E);
_,ff1:=IsInvertible(f1);
_,ee1:=IsIsomorphic(E,E1);
R:=e1(f1(RDbar));
S:=e1(f1(SDbar));
f:=f1*e1;
_,f_inv:=IsInvertible(f);

function g(A)
        return (f_inv(A)[1]^2-q)*(x1^2-q);
```

```
end function;

function g2(A)
        return (f_inv(A)[1]^2-q);
end function;
  // alternativna definicija funkcije g i jedna pokrata.
function dajcetvorku(A,B,C)
        t1:=g2(A);
        t2:=g2(B);
        t3:=g2(C);
        _,a1:=IsSquare(t1*t2*t3/m);
        a2:=t1/a1;
        a3:=t2/a1;
        a4:=t3/a1;
        return [a1,a2,a3,a4];
end function;
 // funkcija "dajcetvorku" uzima trojku tocaka (A,B,C) na E,
 //za koje pretpostavljamo da zadovoljavaju uvjete
 //nedegenericnosti i vraca racionalnu D(q)-cetvorku.
Q1:=S+R;
Q2:=2*S;
Q3:=3*S;
cetvorka:=dajcetvorku(Q1,Q2,Q3);
cetvorka;
```

5.2. KODOVI KORIŠTENI U TREĆEM POGLAVLJU

5.2.1. Krivulja E

Kod koji smo koristili kako bi našli jednadžbu krivulje E, danu sa (3.24) te računali točke S_i dane sa (3.25). Ujedno, provjeravamo je li eliptički regulator točaka S_i različit od nule.

```
QQ:=Rationals();
```

```
P<u>:=FunctionField(QQ);
R<c,z1>:=PolynomialRing(P,2);

SetClassGroupBounds("GRH");

function Fnum(x)
return Factorization(Numerator(x));
end function;

  // Polinom "pol" je desna strana jednakosti (3.22).
pol:=(u^4 + u^2 + 7)*c^4 + (-6*u^5 - 21*u^3 + 6*u^2 - 9*u + 3)/
(u^2 - 1/4)*c^3 + (-2*u^8 + 2*u^7 + 121/4*u^6 - 19/2*u^5 +
199/8*u^4 - 83/4*u^3 + 47/8*u^2 +5/4*u - 13/8)/(u^4 - 1/2*u^2 +
1/16)*c^2 + (3*u^7 - 15/2*u^6 - 75/2*u^5 + 33*u^4 - 81/4*u^3 +
21/2*u^2 - 9/4*u + 3/4)/(u^4 - 1/2*u^2 + 1/16)*c + (u^8+ u^7 -
29/4*u^6 + 5/2*u^5 + 409/16*u^4 - 77/4*u^3 + 25/16*u^2 - 5/4*u +
    19/16)/(u^4 - 1/2*u^2 + 1/16);

  // C je krivulja definirana u (3.22),
  //PC je njeno projektivno zatvorenje.
C:=Curve(AffineSpace(R),z1^2-pol);
PC:=ProjectiveClosure(C);

  // ptPC je "ocita" tocka na PC pomocu koje dolazimo do E.
  // f: PC -> E je biracionalno preslikavanje.
ptPC:=PC![1,(4*u^3 - 8*u^2 + 4*u)/(u^2 - 1/4)];
E,f:=EllipticCurve(PC,ptPC);
  // f_inv :E -> PC je biracionalni inverz preslikavanja f.
_,f_inv:=IsInvertible(f);
  // ptPCi su tocke na PC takve da je f(ptPCi)=Si na E.
  // Koordinate tocaka Si su navedene u (3.25).
ptPC1:=PC![(-1/2*u^2 + u + 1/4)/(u^2 - 1/4),(3/4*u^6 + 3/2*u^5 -
```

```
3/2*u^4 - 3*u^3 + 3/4*u^2 + 3/2*u)/(u^4 - 1/2*u^2 + 1/16)];
S1:=f(ptPC1);
ptPC2:=PC![1/(2*u-1),(u^5 - 7/2*u^3 + 3*u^2 - 1/2*u)/(u^3 -
1/2*u^2 - 1/4*u + 1/8)];
S2:=f(ptPC2);
ptPC3:=PC![5/(2*u-1),(u^5 - 13/2*u^3 + 29/2*u + 9)/(u^3 -
1/2*u^2 - 1/4*u + 1/8)];
S3:=f(ptPC3);
ptPC4:=PC![3/(2*u+1),(u^5 + u^4 - 7/2*u^3 - u^2 + 7/2*u - 1)/
(u^3 + 1/2*u^2 - 1/4*u - 1/8)];
S4:=f(ptPC4);
ptPC5:=PC![3/(2*u+1),-(u^5 + u^4 - 7/2*u^3 - u^2 + 7/2*u - 1)/
(u^3 + 1/2*u^2 - 1/4*u - 1/8)];
S5:=f(ptPC5);

// Provjera je li elipticki regulator tocaka Si razlicit od nule.
Determinant(HeightPairingMatrix([S1,S2,S3,S4,S5]));
```

5.2.2. Kod za računanje petorki iz točaka na E

Prvo računamo točke Q_i iz Tablice 3.2.

```
  // niz koordinata u tockama Si koje odredjuju tocke Qi,
  // dane u Tablici 3.1.
seq_of_coords:=
[
[ -4, -2, -2, 3, 5 ],
[ -4, -1, -2, 2, 4 ],
[ -3, -1, -2, 1, 4 ],
[ -3, -1, -1, 2, 3 ],
[ -2, -1, -2, 2, 4 ],
[ -2, 0, -2, 1, 3 ],
[ -1, -1, -1, 1, 3 ],
```

```
[ 0, 0, 0, -1, 1]
];

function coords_to_point(coor)
pom:=coor[1]*S1+coor[2]*S2+coor[3]*S3+coor[4]*S4+coor[5]*S5;
return pom;
end function;

  // Tocke Qi iz Tablice 3.1

Q1:=coords_to_point(seq_of_coords[1]);
Q2:=coords_to_point(seq_of_coords[2]);
Q3:=coords_to_point(seq_of_coords[3]);
Q4:=coords_to_point(seq_of_coords[4]);
Q5:=coords_to_point(seq_of_coords[5]);
Q6:=coords_to_point(seq_of_coords[6]);
Q7:=coords_to_point(seq_of_coords[7]);
Q8:=coords_to_point(seq_of_coords[8]);
```

Definiramo funkciju 6 varijabli, IsQuintuple. Prvih 5 varijabli su elementi $D(q)$-petorke, šesta varijabla je broj (ili funkcija) q (ili $q(u)$). Funkcija IsQuintuple provjerava jesu li prvih 5 elemenata $D(q)$-petorka gdje je q šesti element.

```
function IsQuintuple(quint)
        if quint[1] ne quint[2] and quint[1] ne quint[3] and
        quint[1] ne quint[4] and quint[1] ne quint[5] and quint[2]
        ne quint[3] and quint[2] ne quint[4] and quint[2] ne quint[5]
        and quint[3] ne quint[4] and quint[3] ne quint[5] and quint[4]
         ne quint[5] and quint[1] ne 0 and quint[2] ne 0 and quint[3]
         ne 0 and quint[4] ne 0 and quint[5] ne 0 and quint[6] ne 0
        and IsSquare(quint[1]*quint[2]+quint[6])
        and IsSquare(quint[1]*quint[3]+quint[6])
        and IsSquare(quint[1]*quint[4]+quint[6])
        and IsSquare(quint[1]*quint[5]+quint[6])
```

```
        and IsSquare(quint[2]*quint[3]+quint[6])
        and IsSquare(quint[2]*quint[4]+quint[6])
        and IsSquare(quint[2]*quint[5]+quint[6])
        and IsSquare(quint[3]*quint[4]+quint[6])
        and IsSquare(quint[3]*quint[5]+quint[6])
        and IsSquare(quint[4]*quint[5]+quint[6])
        then give:=true;
        else give:=false;
        end if;
        return give;
end function;
```

Kod koji opisuje kako računamo petorke iz točaka Q_i. Koristimo f_inv: $E \to PC$ i uzimamo prvu kordinatu, funkciju $c(u)$, u kodu označenu sa c. Funkcija PointToQuint uzima neku točku na E te koristeći opis na stranici 43 (odmah ispod (3.25) definira ostale brojeve potrebne za račun.

```
function PointToQuint(pt)
c:=f_inv(pt)[1];
r:=1;
p:=(u^2*c+c/2+1/2-2*u)/(u^2-1);
b:=(u^2-3*u*c/2-u/2+1)/(u^2-1);
x:=p+r+c;
v:=c^2+x^2-p^2-r^2;
a:=p-r;
d:=p+r;
alpha:=1/v*(p^2-x^2+v)*(r^2-x^2+v);

A:=a^2-alpha;
B:=b^2-alpha;
C:=c^2-alpha;
D:=d^2-alpha;
quint:=[A,B,C,D,x^2,alpha*x^2];
if IsQuintuple(quint) eq true then give:=quint;
```

```
        else give:=false;
end if;
return give;
end function;
```

Funkcija mod_square koja računa polinom P određen jednadžbom (3.27). Funkcija prima racionalnu funkciju varijable u te vraća kvadratno slobodan polinom varijable u. Polinom P je određen do na množenje racionalnim kvadratom pa se može razlikovati od vrijednosti u Tablici 3.2. Prvi izlaz funkcije Fnum (definirane na početku prvog koda ovog odjeljka) vraća faktorizaciju brojnika racionalne funkcije, a drugi izlaz vraća vodeći koeficijent. U principu brišemo sve kvadratne faktore polinoma koji je jednak brojniku racionalne funkcije pomnoženom sa nazivnikom racionalne funkcije.

```
function mod_square(rat_func)
        pol:=rat_func*Denominator(rat_func)^2;
        help,help2:=Fnum(pol);
        max:=#help;
        give:=help2;
        for i in [1..max] do
                give:=give*help[i][1]^(help[i][2] mod 2);
        end for;
        return Evaluate(give,u);
end function;

  // Primjer za tocku Q6.

quint:=PointToQuint(Q6);
IsQuintuple(quint);
mod_square(quint[6]);
```

5.2.3. Kod vezan uz Teorem 3.3.6

Krivulje $E^{(i)}$ (u kodu označene sa Ei) iz tablice 3.2 definirane polinomima P_{Qi} iz Tablice 3.2. Podaci za svaku krivulju su dan u Tablici 3.2, u kodu ih ponavljamo radi lakšeg snalaženja.

```
QQ:=Rationals();
SetClassGroupBounds("GRH");
R<u,y>:=PolynomialRing(QQ,2);

  // Konduktor ove krivulje je 1650, period od W(E^{1}_t) je 6600
C1:=Curve(AffineSpace(R),y^2-(-3/4*u^3 + 329/320*u^2 -
41/160*u - 7/320));
PC1:=ProjectiveClosure(C1);
E1:=EllipticCurve(PC1);

// Konduktor ove krivulje je 624, period od W(E^{2}_t) je 312
C2:=Curve(AffineSpace(R),y^2-(-5/4*u^4 + 37/16*u^3 -
65/64*u^2 - 3/16*u + 9/64));
PC2:=ProjectiveClosure(C2);
E2:=EllipticCurve(PC2);

// Konduktor ove krivulje je 330, period od W(E^{3}_t) je 1320
C3:=Curve(AffineSpace(R),y^2-(-7*u^4 - 11*u^3 + 157/4*u^2 -
53/2*u + 21/4));
PC3:=ProjectiveClosure(C3);
E3:=EllipticCurve(PC3);

// Konduktor ove krivulje je 4400, period od W(E^{4}_t) je 88
C4:=Curve(AffineSpace(R),y^2-(7/4*u^4 - 25/16*u^3 - 93/64*u^2 +
23/16*u - 11/64));
PC4:=ProjectiveClosure(C4);
E4:=EllipticCurve(PC4);

// Konduktor ove krivulje je 14520, period od W(E^{5}_t) je 264
C5:=Curve(AffineSpace(R),y^2-(3*u^3 - 13/20*u^2 + 4/25*u + 1/100));
PC5:=ProjectiveClosure(C5);
E5:=EllipticCurve(PC5);
```

```
// Konduktor ove krivulje je 30, period od W(E^{6}_t) je 120
C6:=Curve(AffineSpace(R),y^2-(4*u^4 - 20*u^3 + 13*u^2 + 12*u));
PC6:=ProjectiveClosure(C6);
E6:=EllipticCurve(PC6);

// Konduktor ove krivulje je 330, period od W(E^{7}_t) je 1320
C7:=Curve(AffineSpace(R),y^2-(-5/2*u^3 - 19/16*u^2 + 19/8*u + 21/16));
PC7:=ProjectiveClosure(C7);
E7:=EllipticCurve(PC7);

// Konduktor ove krivulje je 690, period od W(E^{8}_t) je 2760
C8:=Curve(AffineSpace(R),y^2-(-9/4*u^3 + 61/64*u^2 + 47/32*u - 11/64));
PC8:=ProjectiveClosure(C8);
E8:=EllipticCurve(PC8);

  // Pomocna funkcija radi kraceg pisanja.
  // QT(E,d) je kvadratni tvist krivulje E za d.
  // Ako je E dana sa y^2=p(x), onda je
  // QT(E,d) definiran sa dy^2=p(x).

function QT(E,d)
return QuadraticTwist(E,d);
end function;
```

Ovdje definiramo nizove seq_Ei, gdje svaki član niza ima dvije koordinate. Neka je i fiksan broj iz skupa $\{1,\ldots,8\}$. Prva koordinata nekog elementa seq_Ei$[j][1]$ je $j \bmod N_i$, gdje je N_i je period za krivulju $E^{(i)}$, dan u Tablici 3.2. Posebno, seq_Ei$[N_i][1]$ stavljamo da je jednak N_i, a ne nula. Druga koordinata seq_Ei$[j][2]$ je 0 ili 1. Nadalje u računu pretpostavljamo da vrijedi Slutnja o parnosti. Kako bi izračunali drugu koordinatu, na primjer seq_E6$[j][2]$, uzimamo kvadratno slobodan broj $j1$ istog predznaka kao j, za koji vrijedi $j1 \equiv j \pmod{120}$. Nakon toga racunamo predznak kvadratnog tvista za $j1$ krivulje $E^{(6)}$, to jest, RootNumber$(QT(E6, j1))$. Vrijednost $(1 - \text{RootNumber}(QT(E6, j1)))/2$ spremamo u seq_E6$[j][2]$. Broj seq_E6$[j][2]$ je

jednak Rank$(QT(E6, j1))\pmod 2$ prema Slutnji o parnosti. seqfinal je niz za koji uzimamo u obzir svaki seq_Ei kao uniju. Broj 394680 je najmanji zajednički višekratnik perioda N_i. seqfinal$[j][2]$ ima vrijednost 1, ako postoji krivulja $E^{(i)}$ takva da je seq_Ei$[j \bmod Ni][2] = 1$. U konačnosti, ako je q prirodan kvadratno slobodan broj takav da je $q \equiv j \pmod{394680}$ te seqfinal$[j][2] = 1$, onda postoji beskonačno racionalnih $D(q)$-petorki.
Ako je q negativan kvadratno slobodan cijeli broj takav da je $-q \equiv j \pmod{394680}$ te seqfinal_neg$[j][2] = 1$, onda postoji beskonačno racionalnih $D(q)$-petorki.

```
seqfinal:=[[n,0]:n in [1..394680]];


seq_E1:=[[n,0]:n in [1..6600]];
seq_E2:=[[n,0]:n in [1..312]];
seq_E3:=[[n,0]:n in [1..1320]];
seq_E4:=[[n,0]:n in [1..88]];
seq_E5:=[[n,0]:n in [1..264]];
seq_E6:=[[n,0]:n in [1..120]];
seq_E7:=[[n,0]:n in [1..1320]];
seq_E8:=[[n,0]:n in [1..2760]];

  // Racunanje seq_Ei[j][2] objasnjeno na E1.
  // Za krivulju E1, period N_1 je 6600 pa iskljucujemo brojeve j
  // koji su visekratnici od 4 ili 25 (za njih stavimo seq_Ei[j][2]=0).
  // Provjerimo je li j kvadratno slobodan. Ako nije, pronadjemo
  // kvadratno slobodan j1 istog predznaka kao j takav da je
  // j1==j mod 6600. Za j1 racunamo parnost ranga od QT(E6,j1) koristeci
  // predznak  krivulje QT(E6,j1) (naravno, uz pretpostavku Slutnje
  // o parnosti) i taj podatak spremamo u seq_E1[j][2].

for j in [1..6600] do
        if j mod 4 ne 0 and j mod 25 ne 0 then
                i:=0;
                        while not IsSquarefree(i*6600+j) do i:=i+1;
                        end while;
```

```
                seq_E1[j][2]:=(1-RootNumber(QT(E1,i*6600+j)))/2;
        end if;
end for;

for j in [1..312] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*312+j) do i:=i+1;
                        end while;
                seq_E2[j][2]:=(1-RootNumber(QT(E2,i*312+j)))/2;
        end if;
end for;

for j in [1..1320] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*1320+j) do i:=i+1;
                        end while;
                seq_E3[j][2]:=(1-RootNumber(QT(E3,i*1320+j)))/2;
        end if;
end for;

for j in [1..88] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*88+j) do i:=i+1;
                        end while;
                seq_E4[j][2]:=(1-RootNumber(QT(E4,i*88+j)))/2;
        end if;
end for;

for j in [1..264] do
```

```
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*264+j) do i:=i+1;
                        end while;
                seq_E5[j][2]:=(1-RootNumber(QT(E5,i*264+j)))/2;
        end if;
end for;

for j in [1..120] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*120+j) do i:=i+1;
                        end while;
                seq_E6[j][2]:=(1-RootNumber(QT(E6,i*120+j)))/2;
        end if;
end for;

for j in [1..1320] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*1320+j) do i:=i+1;
                        end while;
                seq_E7[j][2]:=(1-RootNumber(QT(E7,i*1320+j)))/2;
        end if;
end for;

for j in [1..2760] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*2760+j) do i:=i+1;
                        end while;
                seq_E8[j][2]:=(1-RootNumber(QT(E8,i*2760+j)))/2;
```

```
        end if;
end for;

  // Racunamo doprinos svakog seq_Ei u niz seqfinal.

for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 120;
                        if temp eq 0 then temp:= 120;
                        end if;
                seqfinal[i][2]:=seq_E6[temp][2];
        end if;
end for;

for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 1320;
                        if temp eq 0 then temp:= 1320;
                        end if;
                seqfinal[i][2]:=seq_E3[temp][2];
        end if;
        if seqfinal[i][2] eq 0 then
                seqfinal[i][2]:=seq_E7[temp][2];
        end if;
end for;

for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 264;
                        if temp eq 0 then temp:= 264;
                        end if;
                seqfinal[i][2]:=seq_E5[temp][2];
```

```
        end if;
end for;

for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 88;
                        if temp eq 0 then temp:= 88;
                        end if;
                seqfinal[i][2]:=seq_E4[temp][2];
        end if;
end for;


for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 6600;
                        if temp eq 0 then temp:= 6600;
                        end if;
                seqfinal[i][2]:=seq_E1[temp][2];
        end if;
end for;


for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 312;
                        if temp eq 0 then temp:= 312;
                        end if;
                seqfinal[i][2]:=seq_E2[temp][2];
        end if;
end for;
```

```
for i in [1..# seqfinal] do
        if seqfinal[i][2] eq 0 then
                temp:=i mod 2760;
                        if temp eq 0 then temp:= 2760;
                        end if;
                seqfinal[i][2]:=seq_E8[temp][2];
        end if;
end for;

  // Ukupan broj prirodnih kvadratno slobodnih brojeva j mod 394680
  // za koje postoji beskonacno racionalnih D(j)-petorki.

b:=0;
for i in [1..# seqfinal] do
b:=b+seqfinal[i][2];
end for;
b;

  // Slican racun za negativne j.

seqfinal_neg:=[[n,0]:n in [1..394680]];

seq_E1_neg:=[[n,0]:n in [1..6600]];
seq_E2_neg:=[[n,0]:n in [1..312]];
seq_E3_neg:=[[n,0]:n in [1..1320]];
seq_E4_neg:=[[n,0]:n in [1..88]];
seq_E5_neg:=[[n,0]:n in [1..264]];
seq_E6_neg:=[[n,0]:n in [1..120]];
seq_E7_neg:=[[n,0]:n in [1..1320]];
seq_E8_neg:=[[n,0]:n in [1..2760]];
```

```
for j in [1..6600] do
        if j mod 4 ne 0 and j mod 25 ne 0 then
                i:=0;
                        while not IsSquarefree(i*6600+j) do i:=i+1;
                        end while;
                seq_E1_neg[j][2]:=(1-RootNumber(QT(E1,-i*6600-j)))/2;
        end if;
end for;

for j in [1..312] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*312+j) do i:=i+1;
                        end while;
                seq_E2_neg[j][2]:=(1-RootNumber(QT(E2,-i*312-j)))/2;
        end if;
end for;

for j in [1..1320] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*1320+j) do i:=i+1;
                        end while;
                seq_E3_neg[j][2]:=(1-RootNumber(QT(E3,-i*1320-j)))/2;
        end if;
end for;

for j in [1..88] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*88+j) do i:=i+1;
                        end while;
```

```
                seq_E4_neg[j][2]:=(1-RootNumber(QT(E4,-i*88-j)))/2;
        end if;
end for;

for j in [1..264] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*264+j) do i:=i+1;
                        end while;
                seq_E5_neg[j][2]:=(1-RootNumber(QT(E5,-i*264-j)))/2;
        end if;
end for;

for j in [1..120] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*120+j) do i:=i+1;
                        end while;
                seq_E6_neg[j][2]:=(1-RootNumber(QT(E6,-i*120-j)))/2;
        end if;
end for;

for j in [1..1320] do
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*1320+j) do i:=i+1;
                        end while;
                seq_E7_neg[j][2]:=(1-RootNumber(QT(E7,-i*1320-j)))/2;
        end if;
end for;

for j in [1..2760] do
```

```
        if j mod 4 ne 0 then
                i:=0;
                        while not IsSquarefree(i*2760+j) do i:=i+1;
                        end while;
                seq_E8_neg[j][2]:=(1-RootNumber(QT(E8,-i*2760-j)))/2;
        end if;
end for;

  // Racunamo doprinos svakog seq_Ei_neg u niz seqfinal_neg.

for i in [1..# seqfinal_neg] do
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 120;
                        if temp eq 0 then temp:= 120;
                        end if;
                seqfinal_neg[i][2]:=seq_E6_neg[temp][2];
        end if;
end for;

for i in [1..# seqfinal_neg] do
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 1320;
                        if temp eq 0 then temp:= 1320;
                        end if;
                seqfinal_neg[i][2]:=seq_E3_neg[temp][2];
        end if;
        if seqfinal_neg[i][2] eq 0 then
                seqfinal_neg[i][2]:=seq_E7_neg[temp][2];
        end if;
end for;

for i in [1..# seqfinal_neg] do
```

```
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 264;
                        if temp eq 0 then temp:= 264;
                        end if;
                seqfinal_neg[i][2]:=seq_E5_neg[temp][2];
        end if;
end for;

for i in [1..# seqfinal_neg] do
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 88;
                        if temp eq 0 then temp:= 88;
                        end if;
                seqfinal_neg[i][2]:=seq_E4_neg[temp][2];
        end if;
end for;


for i in [1..# seqfinal_neg] do
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 6600;
                        if temp eq 0 then temp:= 6600;
                        end if;
                seqfinal_neg[i][2]:=seq_E1_neg[temp][2];
        end if;
end for;


for i in [1..# seqfinal_neg] do
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 312;
                        if temp eq 0 then temp:= 312;
```

```
                        end if;
                seqfinal_neg[i][2]:=seq_E2_neg[temp][2];
        end if;
end for;



for i in [1..# seqfinal_neg] do
        if seqfinal_neg[i][2] eq 0 then
                temp:=i mod 2760;
                        if temp eq 0 then temp:= 2760;
                        end if;
                seqfinal_neg[i][2]:=seq_E8_neg[temp][2];
        end if;
end for;

  // Ukupan broj negativnih kvadratno slobodnih cijelih brojeva j
  // mod 394680 za koje postoji beskonacno racionalnih D(j)-petorki.

bneg:=0;
for i in [1..# seqfinal_neg] do
bneg:=bneg+seqfinal_neg[i][2];
end for;
bneg;
```

5.3. KODOVI KORIŠTENI U ČETVRTOM POGLAVLJU

5.3.1. Kod iz Propozicije 4.1.1

Računska provjera Propozicije 4.1.1

```
QQ:=Rationals();
P<q1>:=FunctionField(QQ);
P3<t1,t2,t3,t0>:=ProjectiveSpace(P,3);
```

```
q:=q1^2;
  //isti trik kao i ranije
R<x,y,z,k>:=PolynomialRing(P,4);
pol:=(x^2-q)*(y^2-q)*(z^2-q)-k^2;
X:=Scheme(AffineSpace(R),pol);
Xbar:=ProjectiveClosure(X);
psi1:=t0*(t3^2*(t1^2-t2^2)-(t0^2-t2^2)*(t0^2+t3^2));
psi2:=t1*((t0^2-t2^2)*(t0^2-t3^2)+t3^2*(t1^2-t2^2));
psi3:=t2*((t0^2-t2^2)*(t0^2-t3^2)+t3^2*(t1^2-t2^2));
psi4:=2*q1^2*t3*(t1^2-t0^2)*(t2^2-t0^2);
psi5:=t0/q1*((t0^2-t2^2)*(t0^2-t3^2)+t3^2*(t1^2-t2^2));

psi:=map<P3->Xbar | [psi1,psi2,psi3,psi4,psi5]>;
tr,phi:=IsInvertible(psi);
tr;
phi;
```

5.3.2. Kod za Odjeljak 4.3.1

```
QQ:=Rationals();
P<u2,u,q,z>:=FunctionField(QQ,4);
R<u1>:=PolynomialRing(P);
a:=(u^2-q)*(u1^2-q)/((u^2+q)*(u2-u1)+2*u*(u1*u2-q));
b:=(u^2-q)*(u2^2-q)/((u^2+q)*(u2-u1)+2*u*(u1*u2-q));
c:=((u^2+q)*(u2-u1)+2*u*(u1*u2-q))/(u^2-q);
d:=a+c+2*u1;
f2:=(u2^4*u^2 - 2*u2^3*u*q + u2^2*q^2 - u2*u^3*q +
u2*u*q^2 + 1/4*u^4*q + 1/2*u^2*q^2 - 3/4*q^3);
f1:=(u2^4*u^3 + u2^4*u*q - 3*u2^3*u^2*q - u2^3*q^2
     + 2*u2^2*u*q^2 - 1/2*u2*u^4*q + 1/2*u2*q^3 + u^3*q^2 - u*q^3);
f0:=1/4*u2^4*u^4 + 1/2*u2^4*u^2*q + 1/4*u2^4*q^2 -u2^3*u^3*q
- u2^3*u*q^2 -1/4*u2^2*u^4*q + 3/2*u2^2*u^2*q^2 - 1/4*u2^2*q^3
```

```
+ 1/4*u^4*q^2 - 1/2*u^2*q^3 + 1/4*q^4;
f3:=(u2*u - 1/2*u^2 - 1/2*q)*u1 + 1/2*u2*u^2 + 1/2*u2*q - u*q;
pol:=f2*u1^2+f1*u1+f0;
(b*d+q)*f3^2-pol;
_,temp:=IsSquare(Evaluate(pol,u2));
  //u varijablu temp spremamo vrijednost korijena od pol(u2)
kvadpol:=pol-(z*(u1-u2)+temp)^2;
Factorization(Numerator(kvadpol));
B:=-(u2^5*u^2 + u2^4*u^3 - u2^4*u*q - 3*u2^3*u^2*q - 2*u2^3*u*z -
        u2^2*u^3*q - u2^2*u^2*z + 3*u2^2*u*q^2 + u2^2*q*z - 1/4*u2*u^4*q
        1/2*u2*u^2*q^2 + 2*u2*u*q*z - 1/4*u2*q^3 + u2*z^2 + u^3*q^2 + u^2
        u*q^3 - q^2*z);
N:=u2^4*u^2 - 2*u2^3*u*q + u2^2*q^2 - u2*u^3*q + u2*u*q^2 +
        1/4*u^4*q + 1/2*u^2*q^2 - 3/4*q^3 - z^2;
opciu1:=B/N;
IsSquare(Evaluate(b*d+q,opciu1));
```

ZAKLJUČAK

U ovom radu proučavali smo racionalne $D(q)$-m-torke, za $m = 3,4$ te 5 i racionalne brojeve q različite od nule koji nisu potpuni kvadrati.

Parametrizirali smo racionalne brojeve m za koje postoje racionalne $D(q)$-četvorke umnoška elemenata jednakog m. Pritom smo dokazali da za svaki $q \in \mathbb{Q}$ različit od nule postoji beskonačno brojeva m takvih da postoji racionalna $D(q)$-četvorka umnoška elemenata jednakog m. Za svaki takav par (m,q), parametrizirali smo racionalne $D(q)$-četvorke umnoška elemenata jednakog m, koristeći trojke točaka na eliptičkoj krivulji $E_m\colon T^3 + (4q^2 - 2m)T^2 + m^2T$, koje zadovoljavaju poseban uvjet.

Konstruirali smo nove familije racionalnih $D(q)$-petorki. Dokazali smo da, uz pretpostavku Slutnje o Parnosti, za svaki kvadratno slobodan $q \in \mathbb{Z}$ u barem 99.5% klasa ostataka mod 394680 koje sadrže kvadratno slobodne brojeve, postoji beskonačno mnogo racionalnih $D(q)$-petorki.

Konačno, parametrizirali smo sve racionalne $D(q)$-trojke. Koristeći taj rezultat parametrizirali smo sve racionalne $D(q)$-trojke koje su i $D(0)$-trojke te sve racionalne $D(q)$-četvorke koje sadrže barem jednu regularnu racionalnu $D(q)$-trojku.

BIBLIOGRAFIJA

[1] Adžaga, Nikola, Andrej Dujella, Dijana Kreso i Petra Tadić: *Triples which are $D(n)$-sets for several n's*. J. Number Theory, 184:330–341, 2018, ISSN 0022-314X. https://doi.org/10.1016/j.jnt.2017.08.024. ↑ 2.

[2] Atiyah, M. F. i I. G. Macdonald: *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy izdanje, 2016, ISBN 978-0-8133-5018-9; 0-201-00361-9; 0-201-40751-5. For the 1969 original see [MR0242802]. ↑ 10.

[3] Baker, A. i H. Davenport: *The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$*. Quart. J. Math. Oxford Ser. (2), 20:129–137, 1969, ISSN 0033-5606. https://doi.org/10.1093/qmath/20.1.129. ↑ 1.

[4] Bosma, Wieb, John Cannon i Catherine Playoust: *The Magma algebra system. I. The user language*. J. Symbolic Comput., 24(3-4):235–265, 1997, ISSN 0747-7171. https://doi.org/10.1006/jsco.1996.0125, Computational algebra and number theory (London, 1993). ↑ iii, 3, 27, 30, 43, 44, 48.

[5] Desjardins, Julie: *Root number of twists of an elliptic curve*. J. Théor. Nombres Bordeaux, 32(1):73–101, 2020, ISSN 1246-7405. http://jtnb.cedram.org/item?id=JTNB_2020__32_1_73_0. ↑ 46, 47, 48.

[6] Dražić, Goran: *A parametrization of rational $D(q)$-triples*. Mat. Bilten, prihvaćen, 2021. ↑ 3.

[7] Dražić, Goran: *Rational $D(q)$-quintuples*. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM, prihvaćen, 2021. ↑ 3.

[8] Dražić, Goran i Matija Kazalicki: *Rational $D(q)$-quadruples*. arXiv preprint arXiv:2002.02006v3, 2020. ↑ 3.

[9] Dujella, Andrej: *An extension of an old problem of Diophantus and Euler*. Fibonacci Quart., 37:312–314, 1999, ISSN 0015-0517. ↑ 3, 38.

[10] Dujella, Andrej: *A note on Diophantine quintuples*. U *Algebraic number theory and Diophantine analysis (Graz, 1998)*, stranice 123–127. de Gruyter, Berlin, 2000. ↑ 2.

[11] Dujella, Andrej: *There are only finitely many Diophantine quintuples*. J. Reine Angew. Math., 566:183–214, 2004, ISSN 0075-4102. https://doi.org/10.1515/crll.2004.003. ↑ 1.

[12] Dujella, Andrej: *Rational Diophantine sextuples with mixed signs*. Proc. Japan Acad. Ser. A Math. Sci., 85(4):27–30, 2009, ISSN 0386-2194. https://doi.org/10.3792/pjaa.85.27. ↑ 2.

[13] Dujella, Andrej i Clemens Fuchs: *On a problem of Diophantus for rationals*. J. Number Theory, 132(10):2075–2083, 2012, ISSN 0022-314X. https://doi.org/10.1016/j.jnt.2012.04.004. ↑ 2, 3, 38, 44.

[14] Dujella, Andrej i Matija Kazalicki: *More on Diophantine sextuples*. U *Number Theory–Diophantine Problems, Uniform Distribution and Applications*, stranice 227–235. Springer, 2017. ↑ 2, 24, 29.

[15] Dujella, Andrej i Matija Kazalicki: *Diophantine m-tuples in finite fields and modular forms*. Res. Number Theory, 7(1):Paper No. 3, 24, 2021, ISSN 2522-0160. https://doi.org/10.1007/s40993-020-00232-y. ↑ 24.

[16] Dujella, Andrej, Matija Kazalicki, Miljen Mikić i Márton Szikszai: *There are infinitely many rational Diophantine sextuples*. Int. Math. Res. Not. IMRN, (2):490–508, 2017, ISSN 1073-7928. https://doi.org/10.1093/imrn/rnv376. ↑ 1, 2.

[17] Dujella, Andrej, Matija Kazalicki i Vinko Petričević: *D (n)-quintuples with square elements*. Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM 115, Article 172, 2021. ↑ 2, 41.

[18] Dujella, Andrej, Matija Kazalicki i Vinko Petričević: *Rational Diophantine sextuples containing two regular quadruples and one regular quintuple*. Acta mathematica Spalatensia, 1(1):19–27, jan 2021. ↑ 2.

[19] Dujella, Andrej, Matija Kazalicki i Vinko Petričević: *Rational Diophantine sextuples with square denominators*. J. Number Theory, 205:340–346, 2019, ISSN 0022-314X. https://doi.org/10.1016/j.jnt.2019.06.006. ↑ 2.

[20] Dujella, Andrej, Matteo Paganin i Mohammad Sadek: *Strong rational Diophantine $D(q)$-triples*. Indag. Math. (N.S.), 31(3):505–511, 2020, ISSN 0019-3577. https://doi.org/10.1016/j.indag.2020.03.007. ↑ 64.

[21] Dujella, Andrej i Juan Carlos Peral: *High rank elliptic curves induced by rational Diophantine triples*. Glas. Mat. Ser. III, 55(75)(2):237–252, 2020, ISSN 0017-095X. ↑ 2.

[22] Galbraith, Steven D.: *Mathematics of public key cryptography*. Cambridge University Press, Cambridge, 2012, ISBN 978-1-107-01392-6. https://doi.org/10.1017/CBO9781139012843. ↑ 12, 32.

[23] Gibbs, Philip: *Some rational Diophantine sextuples*. Glas. Mat. Ser. III, 41(61)(2):195–203, 2006, ISSN 0017-095X. https://doi.org/10.3336/gm.41.2.02. ↑ 1.

[24] Halberstadt, Emmanuel: *Signes locaux des courbes elliptiques en 2 et 3*. C. R. Acad. Sci. Paris Sér. I Math., 326(9):1047–1052, 1998, ISSN 0764-4442. https://doi.org/10.1016/S0764-4442(98)80060-8. ↑ 46, 47.

[25] Hartshorne, Robin: *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977, ISBN 0-387-90244-9. Graduate Texts in Mathematics, No. 52. ↑ 4, 6, 8, 11, 13, 15.

[26] He, Bo, Alain Togbé i Volker Ziegler: *There is no Diophantine quintuple*. Trans. Amer. Math. Soc., 371(9):6665–6709, 2019, ISSN 0002-9947. https://doi.org/10.1090/tran/7573. ↑ 1.

[27] Heath, Thomas L.: *Diophantus of Alexandria: A study in the history of Greek algebra*. Dover Publications, Inc., New York, second izdanje, 1964. With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler. ↑ 1.

[28] Kazalicki, Matija i Bartosz Naskręcki: *Diophantine triples and K3 surfaces*. arXiv preprint arXiv:2101.11705, 2021. https://arxiv.org/pdf/2101.11705.pdf, posjećeno 2021-05-25. ↑ 2, 3, 56.

[29] Lozano-Robledo, Álvaro: *Elliptic curves, modular forms, and their L-functions*, svezak 58 iz *Student Mathematical Library*. American Mathematical Society, Providence, RI; Institute for Advanced Study (IAS), Princeton, NJ, 2011, ISBN 978-0-8218-5242-2. https://doi.org/10.1090/stml/058, IAS/Park City Mathematical Subseries. ↑ 23.

[30] Najman, Filip: *Eliptičke krivulje nad poljima algebarskih brojeva*, 2013. https://web.math.pmf.unizg.hr/~fnajman/elipticke.pdf, posjećeno 2021-06-03. ↑ 23.

[31] Najman, Filip: *Aritmetička geometrija*, 2015. https://web.math.pmf.unizg.hr/~fnajman/ag.pdf, posjećeno 2021-05-20. ↑ 4, 15, 16.

[32] Piezas, Tito: *Extending rational Diophantine triples to sextuples*. https://mathoverflow.net/questions/233538/extending-rational-diophantine-triples-to-sextuples, posjećeno 2021-06-03. ↑ 2.

[33] Rizzo, Ottavio G.: *Average root numbers for a nonconstant family of elliptic curves*. Compositio Math., 136(1):1–23, 2003, ISSN 0010-437X. https://doi.org/10.1023/A:1022669121502. ↑ 46, 47, 48, 49.

[34] Rohrlich, David E.: *Variation of the root number in families of elliptic curves*. Compositio Math., 87(2):119–151, 1993, ISSN 0010-437X. http://www.numdam.org/item?id=CM_1993__87_2_119_0. ↑ 46.

[35] Rohrlich, David E.: *Galois theory, elliptic curves, and root numbers*. Compositio Math., 100(3):311–349, 1996, ISSN 0010-437X. http://www.numdam.org/item?id=CM_1996__100_3_311_0. ↑ 46.

[36] Silverman, Joseph H.: *Advanced topics in the arithmetic of elliptic curves*, svezak 151 iz *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994, ISBN 0-387-94328-5. https://doi.org/10.1007/978-1-4612-0851-8. ↑ 20, 21.

[37] Silverman, Joseph H.: *The arithmetic of elliptic curves*, svezak 106 iz *Graduate Texts in Mathematics*. Springer, Dordrecht, second izdanje, 2009, ISBN 978-0-387-09493-9. https://doi.org/10.1007/978-0-387-09494-6. ↑ 4, 14, 15, 16, 18, 19, 20, 22, 28, 31, 45.

[38] Stoll, Michael: *Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational Diophantine quintuples*. Acta Arith., 190(3):239–261, 2019, ISSN 0065-1036. https://doi.org/10.4064/aa180416-4-10. ↑ 1.

ŽIVOTOPIS

Goran Dražić rođen je 27. studenog 1987. u Zagrebu. Godine 2006. upisao je studij matematike Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te 2009. završio preddiplomski studij. Godine 2012. upisao je diplomski studij teorijske matematike, a diplomirao 2015. s temom "Eliptičke krivulje i Mordell-Weilov teorem" pod vodstvom izv. prof. dr. sc. Matije Kazalickog.

Nakon diplome upisao je Doktorski studij matematike na Prirodoslovno-matematičkom fakultetu Sveučilišta u Zagrebu te je zaposlen kao asistent na Prehrambeno-biotehnološkom fakultetu istog Sveučilišta, gdje radi i danas.

Sudjeluje u radu *Seminara za teoriju brojeva i algebru*, izlagao je na međunarodnoj konferenciji "Journées Arithmétiques 2019" sa radom naslova "Rational $D(q)$-quadruples" te je sudjelovao na domaćim i međunarodnim konferencijama te ljetnim školama. Ima 2 prihvaćena članka koji čekaju objavljivanje. Suradnik je na projektu Hrvatske zaklade za znanost koji vodi izv. prof. dr. sc. Matija Kazalicki.