Diofantove m-torke i eliptičke krivulje

Andrej Dujella

PMF – MO, Sveučilište u Zagrebu, 2021./2022.

Sadržaj

Poglavlje 1

Uvod

1.1 Diofant iz Aleksandrije

Starogrčki matematičar Diofant iz Aleksandrije (III. st. prije Krista) prvi je proučavao problem pronalaženja brojeva sa svojstvom da produkt svaka dva među njima uvećan za 1 daje potprun kvadrat. U četvrtom dijelu njegove knjige *Aritmetika*, 20. zadatak glasi:

> Nađi četiri broja (kod Diofanta to je značilo pozitivna racionalna broja) sa svojstvom da produkt svaka dva među njima uvećan za 1 daje kvadrat.

Diofant je riješio zadatak, tj. našao četiri pozitivna racionalna broja s traženim svojstvom:

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

Zaista,

$$\begin{aligned}
&\frac{1}{16}\cdot\frac{33}{16}+1=\frac{289}{256}=\left(\frac{17}{16}\right)^2, \quad \frac{1}{16}\cdot\frac{17}{4}+1=\frac{81}{64}=\left(\frac{9}{8}\right)^2,\\
&\frac{1}{16}\cdot\frac{105}{16}+1=\frac{361}{256}=\left(\frac{19}{16}\right)^2, \quad \frac{33}{16}\cdot\frac{17}{4}+1=\frac{625}{64}=\left(\frac{25}{8}\right)^2,\\
&\frac{33}{16}\cdot\frac{105}{16}+1=\frac{3721}{256}=\left(\frac{61}{16}\right)^2, \quad \frac{17}{4}\cdot\frac{105}{16}+1=\frac{1849}{64}=\left(\frac{43}{8}\right)^2.
\end{aligned}$$

Prikazat ćemo kako je Diofant došao do rješenja (koristeći današnju matematičku notaciju). Dva broja s traženim svojstvom možemo lako dobiti tako da uzmemo $a = x$ i $b = x + 2$, pa je $ab + 1 = (x + 1)^2$. Svaki par $\{a, b\}$ takav da je $ab + 1 = r^2$, može se proširiti do trojke tako da se uzme $c = a + b + 2r$. Zaista, imamo: $ac + 1 = a^2 + 2ar + ab + 1 = (a + r)^2$ i $bc + 1 = (b + r)^2$. Za $a = x$ i $b = x + 2$, dobivamo $c = 4x + 4$. Sada primijenimo istu konstrukciju na par $\{a, c\}$ i jednakost $ac + 1 = (2x + 1)^2$. Dobivamo $d = x + (4x + 4) + 2(2x + 1) = 9x + 6$. Dakle, dobili smo skup

$\{a, b, c, d\}$ koji zadovoljava pet od šest svojstava iz definicije Diofantove četvorke. Jedini uvjet koji nedostaje je da $bd + 1$ bude kvadrat. Stoga trebamo naći racionalno rješenje jednadžbe

$$9x^2 + 24x + 13 = y^2. \tag{1.1}$$

Diofant je poznavao metodu za rješavanje jednadžbi ovog tipa. Tražio je rješenja u obliku $y = 3x + t$, te nakon uvrštavanja u jednadžbu, dobio je linearnu jednadžbu u x. On nije tražio opće rješenje (vjerojatno i zbog problema s notacijom), već bi uvrstio neku konkretnu vrijednost za parametar t i tako dobio jedno rješenje problema. U ovom slučaju, stavio je $y = 3x - 4$ te dobio linearnu jednadžbu $48x = 3$ čije je rješenje $x = 1/16$. Na taj je način našao prvi primjer skupa koji danas nazivamo racionalna Diofantova četvorka.

Općenitije, uvrštavanjem $y = 3x + t$, dobivamo $x = \frac{t^2-13}{6(4-t)}$ i beskonačnu familiju racionalnih Diofantovih četvorki

$$\left\{\frac{t^2 - 13}{6(4 - t)}, \frac{(t - 5)(t - 7)}{6(4 - t)}, \frac{2(t^2 - 6t + 11)}{3(4 - t)}, \frac{3(t - 1)(t - 3)}{2(4 - t)}\right\}.$$

Jednadžba (1.1) je specijalni slučaj jednadžbe oblika

$$\alpha^2x^2 + \beta x + \gamma = y^2. \tag{1.2}$$

Diofant je poznavao metodu za rješavanje ovakvih jednadžbi tako da se rješenje traži u obliku $y = \alpha x + t$. Jednadžba (1.2) se može shvatiti kao jednadžba krivulje genusa 0 s racionalnom točkom u beskonačnosti. Uvođenjem projektivnih koordinata $x = X/Z$, $y = Y/Z$, dobivamo projektivnu jednadžbu krivulje

$$\alpha^2X^2 + \beta XZ + \gamma Z^2 = Y^2$$

koja ima racionalnu točku s koordinatama $(X, Y, Z) = (1, \alpha, 0)$. Jednadžba pravca kroz tu točku ima oblik $\alpha X - Y + tZ = 0$, što u afinim koordinatama daje upravo $y = \alpha x + t$.

Trojke oblika $\{a, b, a + b + 2r\}$, gdje je $ab + 1 = r^2$, se nazivaju *regularne Diofantove trojke*. Sasvim analogna konstrukcija trojki je moguća i za problem u kojem se umjesto produkata uvećanih za 1 promatraju produkti uvećani za fiksirani proizvoljni racionalni broj q. Naime, ako je $ab + q = r^2$, onda je $a(a + b + 2r) + q = (a + r)^2$ i $b(a + b + 2r) + q = (b + r)^2$, pa trojka $\{a, b, a + b + 2r\}$ ima traženo svojstvo i naziva se *regularna $D(q)$-trojka*. U 3. i 4. zadatku iz petog dijela knjige *Aritmetika*, Diofant je promatrao skupove od četiri racionalna broja sa svojstvom da je produkt svaka dva elementa uvećan za q potpun kvadrat, tj. racionalne $D(q)$-četvorke. Našao je jednu racionalnu $D(5)$-četvorku

$$\left\{1, \frac{2861}{676}, \frac{7645}{676}, \frac{5084}{169}\right\},$$

te jednu racionalnu $D(-6)$-četvorku

$$\left\{1, \frac{4993}{784}, \frac{6729}{784}, \frac{5665}{196}\right\},$$

no njegova konstrukcija zapravo daje puno općeniji rezultat da za svaki racionalan broj q postoji beskonačno mnogo racionalnih $D(q)$-četvorki. Taj rezultat se posebno zanimljiv u svjetlu činjenice da do danas nije poznato postoji li za svaki racionalan broj q beskonačno mnogo racionalnih $D(q)$-petorki. Uzmimo kao Diofant da je $a = 1$. Tada bi mogli uzeti $b = x^2 - q$, $c = (x+1)^2 - q$, ali zbog nesto estetskijih formula uzet ćemo (poopćujući Diofantov izbor za $q = 5$) $b = (x + (q+1)/2)^2 - q$, $c = (x + 1 + (q+1)/2)^2 - q$. Tada je $\{a, b, c\}$ regularna $D(q)$-trojka. Proširimo sada par $\{b, c\}$ do regularne $D(q)$-trojke $\{b, c, d\}$. Dobivamo

$$d = 4x^2 + 4xq + 8x + q^2 + 4.$$

Ostaje jos samo zadovoljiti uvjet da je $ad + q$ kvadrat, što daje

$$4x^2 + (8 + 4q)x + q^2 + q + 4 = (2x + q + 2 + t)^2$$

(opet smo ovo $q + 2$ uveli samo zbog estetskijih formula), te se dobije

$$x = -\frac{3q + 2qt + 4t + t^2}{4t}.$$

Uvrštavanjem se dobije beskonačna familija $D(q)$-četvorki

$$\left\{1, \frac{9q^2 + 12qt - 10qt^2 + 4t^2 + 4t^3 + t^4}{16t^2}, \right.$$
$$\left. \frac{9q^2 - 12qt - 10qt^2 + 4t^2 - 4t^3 + t^4}{16t^2}, \frac{(-9q + t^2)(-q + t^2)}{4t^2}\right\}.$$

(Ovdje je t proizvoljan racionalan broj različit od 0 koji zadovoljava uvjet da su elementi dobivene četvorke međusobno različiti racionalni brojevi različiti od 0.)

1.2 Pierre de Fermat

Prvi skup od četiri prirodna broja s Diofantovim svojstvom, skup

$$\{1, 3, 8, 120\},$$

našao je Pierre de Fermat, francuski pravnik i matematičar (1601. – 1665.). Zaista, vrijedi:

$$1 \cdot 3 + 1 = 2^2, \quad 1 \cdot 120 + 1 = 11^2,$$
$$1 \cdot 8 + 1 = 3^2, \quad 3 \cdot 120 + 1 = 19^2,$$
$$3 \cdot 8 + 1 = 5^2, \quad 8 \cdot 120 + 1 = 31^2.$$

U svojoj konstrukciji Fermat je krenuo od trojke $\{1, 3, 8\}$ i pokušao naći prirodan broj d takav da su $d+1$, $3d+1$ i $8d+1$ potpuni kvadrati. Prvi uvjet je zadovoljen za $d = y^2 + 2y$. Preostala dva uvjeta su sada

$$3(y^2 + 2y) + 1 = u^2,$$
$$8(y^2 + 2y) + 1 = v^2.$$

Oduzimanjem dobivamo

$$5y(y + 2) = (v + u)(v - u),$$

te tražimo rješenje koje zadovoljava $5y = v + u$, $y + 2 = v - u$, tj. $v = 3y + 1$, $u = 2y - 1$. Sada iz

$$8(y^2 + 2y) + 1 = (3y + 1)^2$$

dobivamo $y = 10$, tj. $d = 120$ (drugo rješenje kvadratne jednadžbe, $y = 0$, daje trivijalno proširenje $d = 0$ koje ne zadovoljava uvjet iz definicije da je d prirodan broj).

Fermat je ovu metodu primjenjivao i na druge probleme koji vode do sustava jednadžbi oblika $ax+p^2 = y^2$, $bx+q^2 = u^2$, $cx+r^2 = v^2$. Primjerice, ako krenemo od $D(-1)$-trojke $\{1, 2, 5\}$ i pitamo se postoji li prirodan broj d takav da su $d + 1$, $2d + 1$ i $5d + 1$ kvadrati (za takav skup se kaže da ima svojstvo $D(-1; 1)$), supstitucijom $d = y^2 + 2y$, dobivamo sustav

$$2(y^2 + 2y) + 1 = u^2,$$
$$5(y^2 + 2y) + 1 = v^2.$$

Oduzimanjem dobivamo

$$3y(y + 2) = (v + u)(v - u),$$

te tražimo rješenje koje zadovoljava $3y = v + u$, $y + 2 = v - u$, tj. $v = 2y + 1$, $u = y - 1$, pa iz

$$2(y^2 + 2y) + 1 = (y - 1)^2$$

dobivamo $y = -6$ i $d = 24$.

1.3 Leonhard Euler

Znameniti švicarski matematičar Leonhard Euler (1707. – 1783.) dao je brojne važne doprinose proučavanju cjelobrojnih i racionalnih Diofantovih m-torki te drugih skupova sa sličnim svojstvima. Spomenut ćemo ovdje neke od njegovih rezultata. Euler je poopćio Fermatov primjer cjelobrojne Diofantove četvorke te pokazao da takvih skupova ima beskonačno mnogo. Preciznije, pokazao je da ako su a i b prirodni brojevi takvi da je $ab + 1 = r^2$, onda je skup

$$\{a, b, a + b + 2r, 4r(r + a)(r + b)\} \tag{1.3}$$

Diofantova četvorka.

Kao što smo već vidjeli, proširiti par $\{a, b\}$ do (regularne) trojke $\{a, b, a+b+2r\}$, znao je već i Diofant. Pokažimo kako je Euler pronašao proširenje ove trojke s četvrtim (cjelobrojnim) elementom d. Želimo da $ad+1$, $bd+1$ i $(a+b+2r)d+1$ budu kvadrati, pa onda i njihov produkt treba biti kvadrat. Množeći ova tri uvjeta, dobivamo jednadžbu

$$(ad+1)(bd+1)((a+b+2r)d+1) = y^2. \tag{1.4}$$

(U modernoj terminologiji mogli bi reći da smo dobili jednadžbu eliptičke krivulje u varijablama d i y.) Ideja je potražiti rješenje jednadžbe (1.4) u obliku $y = u + vd + wd^2$, gdje se racionalni brojevi u, v, w izabiru tako da se obje strane od (1.4) podudaraju u članovima malih stupnjeva, tj. u slobodnom članu te članovima uz d i d^2. Uspoređivanjem dobivamo: $u^2 = 1$, $2uv = 2(a+b+r)$, $2wu + v^2 = a^2 + 2br + 2ar + 2ab + b^2 + r^2 - 1$. Stoga možemo uzeti $u = 1$, $v = a+b+r$, $w = -1/2$. Uvrštavajući ovo u (1.4), dobivamo

$$ab(a+b+2r) = -(a+b+r) + \frac{1}{4}d,$$

pa je

$$\begin{aligned} d &= 4(a+b+r) + 4ab(a+b+2r) \\ &= 4(ab+1)(a+b+r) + 4abr \\ &= 4r^2(a+b+r) + 4abr \\ &= 4r(r+a)(r+b). \end{aligned}$$

Sada se direktnim računom provjeri da su $ad+1$, $bd+1$ i $(a+b+2r)d+1$ kvadrati. Zaista,

$$\begin{aligned} ad+1 &= 4ar(r+a)(r+b)+1 = (2r^2+2ar-1)^2, \\ bd+1 &= 4br(r+a)(r+b)+1 = (2r^2+2br-1)^2, \\ (a+b+2r)d+1 &= 4r(a+b+2r)(r+a)(r+b)+1 = (4r^2+2ar+2br-1)^2. \end{aligned}$$

Za $a = 1$ i $b = 3$, dobivamo $a+b+2r = 8$ i $4r(r+a)(r+b) = 120$, tj. Fermatovu četvorku $\{1, 3, 8, 120\}$.

Četvorke oblika (1.3) su specijalni slučaj takozvanih *regularnih Diofantovih četvorki*, što su četvorke koje zadovoljavaju jednakost

$$(a+b-c-d)^2 = 4(ab+1)(cd+1). \tag{1.5}$$

Zaista, za $c = a+b+2r$, $d = 4r(r+a)(r+b)$, imamo

$$\begin{aligned} (a+b-c-d)^2 &= (2r(1+2(r+a)(r+b))^2 \\ &= 4r^2(4r^2+2ar+2br-1)^2 = 4(ab+1)(cd+1). \end{aligned}$$

Euler je uspio naći peti racionalan broj koji proširuje četvorku (1.3) do racionalne Diofantove četvorke. Posebno je Fermatovu četvorku $\{1, 3, 8, 120\}$ proširio do petorke s racionalnim brojem

$$777480/8288641.$$

Pitanje je li ovo proširenje jedinstveno ostalo je otvoreno sve dok jedinstvenost proširenja nije dokazao Stoll 2019. godine. S druge strane, pitanje postojanja racionalnih Diofantovih šestorki je bilo otvoreno do 1999. godine kada je prvu takvu šestorku pronašao Gibbs. Bila je to šestorka

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

Prikažimo sada Eulerovu konstrukciju racionalnih Diofantovih petorki. Neka je $c = a + b + 2r$, $d = 4r(r + a)(r + b)$. Želimo naći racionalan broj e takav da su $ae + 1$, $be + 1$, $ce + 1$ i $de + 1$ kvadrati racionalnih brojeva. Pomnožimo li ova četiri izraza, dobivamo

$$P(e) = 1 + \sigma_1 e + \sigma_2 e^2 + \sigma_3 e^3 + \sigma_4 e^4,$$

gdje su σ_i elementarni simetrični polinomi u varijablama a, b, c, d, tj. $\sigma_1 = a + b + c + d$, $\sigma_2 = ab + ac + ad + bc + bd + cd$, $\sigma_3 = abc + abd + acd + bcd$, $\sigma_4 = abcd$. Neka je $P(e) = (1 + \frac{1}{2}\sigma_1 e + \rho e^2)^2$. Izjednačavanjem članova uz e^2, dobivamo

$$\rho = \frac{1}{2}\sigma_2 - \frac{1}{8}\sigma_1^2. \tag{1.6}$$

Sada je $\sigma_3 + \sigma_4 e = \sigma_1\rho + \rho^2 e$, pa dobivamo da je

$$e = \frac{\sigma_3 - \sigma_1\rho}{\rho^2 - \sigma_4}. \tag{1.7}$$

Pokažimo da su σ_1, σ_2 i σ_4 povezani relacijom

$$4\sigma_2 = \sigma_1^2 - 4\sigma_4 - 4. \tag{1.8}$$

Računamo:

$$\begin{aligned}
&\sigma_1^2 - 4\sigma_2 - 4\sigma_4 - 4 \\
&= (a + b + c + d)^2 - 4(ab + ac + ad + bc + bd + cd) - 4abcd - 4 \\
&= (a + b - c - d)^2 - 4(ab + 1)(cd + 1) = 0,
\end{aligned}$$

zbog (1.5). Uvrstimo li (1.6) i (1.8) u (1.7), dobivamo

$$e = \frac{4\sigma_3 + 2\sigma_1(\sigma_4 + 1)}{(\sigma_4 - 1)^2}. \tag{1.9}$$

Provjerimo da je $ae+1$ kvadrat (ostala tri uvjeta se provjeravaju sasvim analogno). Treba provjeriti da je $4\sigma_3 a + 2\sigma_1(\sigma_4+1)a + (\sigma_4-1)^2$ kvadrat. Iskoristimo sada da je $P(-1/a)=0$, tj.

$$a^4 - \sigma_1 a^3 + \sigma_2 a^2 - \sigma_3 a + \sigma_4 = 0,$$

odakle je $4\sigma_3 a = 4a^4 - 4\sigma_1 a^3 + 4\sigma_2 a^2 + 4\sigma_4$, pa je

$$\begin{aligned}
&4\sigma_3 a + 2\sigma_1(\sigma_4+1)a + (\sigma_4-1)^2 \\
&= 4a^4 - 4\sigma_1 a^3 + 4\sigma_2 a^2 + 4\sigma_4 + 2\sigma_1(\sigma_4+1)a + (\sigma 4 - 1)^2 \\
&= 4a^4 - 4\sigma_1 a^3 + 4\sigma_2 a^2 + 2\sigma_1(\sigma_4+1)a + (\sigma_4+1)^2 \\
&= (2a^2 - \sigma_1 a - (\sigma_4+1))^2,
\end{aligned}$$

gdje smo iskoristili i relaciju (1.8).

Euler je proučavao i skupove sa svojstvom da produkt svaka dva njihova element uvećan za sumu ta dva elementa daje potpun kvadrat. Budući da je

$$xy + x + y = (x+1)(y+1) - 1,$$

vidimo da su takvi skupovi usko povezani s $D(-1)$-m-torkama. I ovdje je motivacija došla od Diofanta, koji je u 15. zadatku trećeg dijela *Aritmetike* našao dva tročlana skupa sa zadanim svojstvom: $\{4, 9, 28\}$ i $\{\frac{3}{10}, \frac{21}{5}, \frac{7}{10}\}$. Nadalje, Diofant je u 5. zadatku petog dijela *Aritmetike* našao tročlani skup s istim svojstvom kojem su dodatno svi elementi kvadrati: $\{\frac{25}{9}, \frac{64}{9}, \frac{196}{9}\}$. Ovu trojku se može nadopuniti do četvorke prije spomenutom Fermatovom metodom, ali Fermat nije eksplicitno proveo svoju metodu u ovom slučaju. Prvi eksplicitni primjer racionalne četvorke s ovim svojstvom dao je Euler. Bio je to skup

$$\left\{\frac{65}{224}, \frac{9}{224}, \frac{9}{56}, \frac{5}{2}\right\}.$$

Euler koristi prije spomenutu vezu s $D(-1)$-četvorkama. Neka je $ab-1 = r^2$. Tada će skup $\{a, b, a+b+2r, a+b-2r\}$ biti $D(-1)$-četvorka ako je $(a+b+2r)(a+b-2r)-1$ potpun kvadrat. Dakle, imamo

$$(a+b)^2 - 4r^2 - 1 = x^2.$$

Odavde je

$$(a-b)^2 = x^2 + 1 + 4r^2 - 4ab = x^2 - 3.$$

Iz $x^2-3=(x-y)^2$, dobivamo $x = \frac{y^2+3}{2y}$. Nadalje, iz $4r^2+1+x^2=(2r+z)^2$, dobivamo $r = \frac{x^2+1-z^2}{4z}$. Sada je Euler uzeo $y=2$ i $z=\frac{7}{2}$, te dobio $x=\frac{7}{4}$, $r=-\frac{131}{224}$, $a-b=\frac{1}{4}$, $a+b=\frac{261}{112}$, $a=\frac{289}{224}$, $b=\frac{233}{224}$, $c=\frac{65}{56}$, $d=\frac{7}{2}$. Odavde se umanjivanjem svakog elementa $D(-1)$-četvorke za 1 dobiva gore navedena *Eulerova četvorka*.

Poznato je da ne postoji Eulerova četvorka u prirodnim brojevima (Dujella i Fuchs su 2005. dokazali da svaka $D(-1)$-četvorka u prirodnim brojevima mora sadržavati broj 1), a također ni u cijelim brojevima (Bonciocat, Cipu i Mignotte su nedavno dokazali da ne postoji cjelobrojna $D(-1)$-četvorka). S druge strane, poznato je da postoji beskonačno mnogo racionalnih Eulerovih petorki (npr. $\{9, \frac{17}{8}, \frac{27}{10}, -\frac{27}{40}, \frac{493}{40}\}$ (Dujella), $\{\frac{29}{24}, \frac{71}{54}, \frac{79}{675}, \frac{1637}{216}, \frac{2911}{200}\}$ (Petričević)).

1.4 Definicije, glavna pitanja i slutnje

Primjeri skupova koje smo do sada naveli motiviraju sljedeće definicije.

Definicija 1.1. *Skup od m prirodnih brojeva $\{a_1, a_2, \ldots, a_m\}$ naziva se* Diofantova m-torka *ako je $a_i \cdot a_j + 1$ potpun kvadrat za sve $1 \leq i < j \leq m$.*

Definicija 1.2. *Skup od m racionalnih brojeva $\{a_1, a_2, \ldots, a_m\}$ različitih od nule naziva se* racionalna Diofantova m-torka *ako je $a_i \cdot a_j + 1$ kvadrat racionalnog broja za sve $1 \leq i < j \leq m$.*

Prirodno se postavlja pitanje koliko veliki mogu biti ovi skupovi, u cjelobrojnom, odnosno u racionalnom slučaju. Ovo je pitanje nedavno u potpunosti riješeno u cjelobrojnom slučaju. S druge strane, čini se da u racionalnom slučaju nemamo niti opće prihvaćenu slutnju što bi trebao biti odgovor. Posebice, nije poznata nikakva gornja ograda za veličinu racionalnih Diofantovih m-torki.

U cjelobrojnom slučaju dugo vremena je bila otvorena slutnja da ne postoji Diofantova petorka, tzv. "Diophantine quintuple conjecture".

Prvi važan rezultat vezan uz ovu slutnju dokazali su 1969. godine Baker i Davenport. Koristeći Bakerovu teoriju linearnih formi u logaritmima algebarskih brojeva te metodu redukcije zasnovanu na verižnim razlomcima, dokazali su da ako je d prirodan broj takav da je $\{1, 3, 8, d\}$ Diofantova četvorka, onda je nužno $d = 120$. Ovaj rezultat povlači da se Fermatov skup $\{1, 3, 8, 120\}$ ne može nadopuniti do Diofantove petorke. Isti rezultat su nekoliko godina kasnije, različitim metodama, dokazali i Kanagasabapathy & Ponnudurai, Sansone i Grinstead.

Obično se u literaturi navodi da je ovaj problem prvi put postavljen 1967. godine u Gardnerovoj kolumni u časopisu *Scientific American*, dok je prve netrivijalne rezultate u vezi ovog problema iznio 1968. van Lint na konferenciji u Oberwolfachu. Ipak čini se da se problem pojavio već 1957. godine u časopisu *The Sunday Times*, u kolumni naslova *A holiday brain teaser* čiji je autor Denton. U kolumni su dani brojevi $1, 3, 8$, te je ponuđena nagrada od £5 za nalaženje četvrtog prirodnog broja koji s ova tri čini Diofantovu četvorku i nagrada od £25 za nalaženje petog prirodnog broja koji s prethodna četiri čini Diofantovu petorku. Prvi zadatak je naravno puno lakši i za

njega je pristiglo 131 (uglavnom točno) rješenje, dok za drugi zadatak nije pristiglo konkretno rješenje (danas znamo da rješenja nema) te se u drugom nastavku kolumne navode razmišljanja rješavača o tome je li moguće rješenje jako veliko ili uopće ne postoji.

U već spomenutoj kolumni u časopisu *Scientific American* iz 1967. godine, čuveni polularizator znanosti, a posebice matematike, Martin Gardner navodi da brojevi $1, 3, 8, 120$ imaju zanimljivo svojstvo da je produkt svaka dva među njima za 1 manji od potpunog kvadrata, te pita da se nađe peti broj koji se može dodati ovim četirima brojevima tako da se ne naruši ovo svojstvo. Isti zadatak je naveden i u njegovoj knjizi *Mathematical Magic Show* iz 1977. godine. Kao odgovor je dan broj 0, ali uz komentar da je to naravno trivijalno rješenje koje je zamišljeno kao šala, te da je vrlo teško pitanje postoji li prirodan broj s takvim svojstvom. U knjizi je navedena i daljnja kronologija koja je dovela do rješenja ovog problema. Jedan student Bouwkampa, profesora iz Eindhovena, vidio je zadatak u *Scientific Americanu* i spomenuo ga Bouwkampu, a ovaj ga je spomenuo svom kolegi van Lintu. Van Lint je pokazao da ako 120 želimo zamijeniti s prirodnim brojem s istim svojstvom, onda taj broj mora imati više od 1700000 znamenaka. Njegov dokaz koristio je svojstva pelovskih jednadžbi i verižnih razlomaka. Prikazao ga je na konferenciji u Oberwolhachu u ožujku 1968. godine, te ga je objavio iste godine u publikaciji u izdanju Technological University Eindhoven. To je motiviralo Alana Bakera i njegovog mentora Harolda Davenporta da pokušaju u potpunosti riješiti problem primjenom tada vrlo nove Bakerove metode pomoću koje se mogla za široku klasu diofantskih jednadžbi dobiti konkretna (obično vrlo velika) gornja ograda za cjelobrojna rješenja. Za tu metodu je Baker nagrađen Fieldsovom medaljom 1970. godine. Da bi smanjili tu vrlo veliku ogradu do granice za koju se moglo provjeriti da nema dodatnih rješenja, uveli su metodu redukcije koja se danas naziva Baker-Davenportova redukcija.

Glavne ideje koje su koristili Baker i Davenport u svom dokazu neproširivosti Fermatove četvorke $\{1, 3, 8, 120\}$, odnosno jedinstvenosti proširenja trojke $\{1, 3, 8\}$ do četvorke, kasnije su drugi autori poopćili, te uveli neke nove metode koje su bile nužne kod promatranja proširenja parametarskih trojki i četvorki (primjerice metoda kongruencija i efektivne ocjene za simultane racionalne aproksimacije kvadratnih iracionalnosti).

Konačno su He, Togbé i Ziegler 2019. dokazali da ne postoji Diofantova petorka. Kasnije ćemo reći nešto više o ovom rezultati i nekima koji su mu prethodili.

Uočimo da Baker-Davenportov rezultat kaže i više od toga da se Fermatova četvorka ne može proširiti do petorke. Naime, kaže da je jedino proširenje trojke $\{1, 3, 8\}$ do četvorke s brojem 120; drugim riječima da je jedina četvorka koja sadrži trojku $\{1, 3, 8\}$ regularna četvorka $\{1, 3, 8, 120\}$. Ovaj, a i brojni analogni rezultati (primjerice za trojke oblika $\{k - 1, k + 1, 4k\}$ ili $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$), motivirali su sljedeću slutnju:

Slutnja 1.1. *Sve Diofantove četvorke su regularne. Drugim riječima, ako je $\{a, b, c, d\}$ Diofantova četvorka, onda je $d = d_+$ ili $d = d_-$, gdje je*

$$d_+ = a + b + c + 2abc + 2\sqrt{(ab+1)(ac+1)(bc+1)},$$
$$d_- = a + b + c + 2abc - 2\sqrt{(ab+1)(ac+1)(bc+1)}.$$

To da se svaka Diofantova trojka $\{a, b, c\}$ može nadopuniti do četvorke s d_+ i d_- (ako je $d_- \neq 0$), prvi su uočili Gibbs 1978. godine te Arkin, Hoggatt & Strauss 1979. godine, te tako poopćili Eulerovo proširenje regularnih trojki do četvorki. Zaista, lako se vidi da je

$$ad_+ + 1 = (a\sqrt{bc+1} + \sqrt{(ab+1)(ac+1)})^2,$$
$$bd_+ + 1 = (b\sqrt{ac+1} + \sqrt{(ab+1)(bc+1)})^2,$$
$$cd_+ + 1 = (c\sqrt{ab+1} + \sqrt{(ac+1)(bc+1)})^2,$$

te da vrijede analogne jednakosti za d_-.

Neka je $a < b < c$. Očito je da je $d_+ > c$, dok iz

$$\begin{aligned} d_+d_- &= (a+b+c+2abc)^2 - 4(ab+1)(ac+1)(bc+1) \\ &= a^2+b^2+c^2-2ab-2ac-2bc-4 = (c-a-b)^2 - 4(ab+1) \\ &= (c-a-b-2r)(c-a-b+2r), \end{aligned}$$

gdje je $ab + 1 = r^2$, slijedi da je $d_- < c$ te da je $d_- = 0$ ako i samo ako je $c = a + b \pm 2r$, tj. ako i samo ako je trojka $\{a, b, c\}$ regularna (to obašnjava zašto smo kod trojke $\{1, 3, 8\}$ imali samo jedno proširenje do četvorke sa 120, dok primjerice kod trojke $\{1, 3, 120\}$ imamo (barem) dva proširenja: 8 i 1680). Stoga Slutnju 1.1 možemo izreći i tako da kažemo da je za svaku trojku $\{a, b, c\}$, jedino proširenje do četvorke $\{a, b, c, d\}$ takvo da je $d > \max(a, b, c)$ dano s $d = d_+$. Ova slutnja je i dalje otvorena. I nekom smislu najbolji poznati rezultat je onaj koji su dokazali Cipu, Fujita & Miyazaki 2018., a to je da se proizvoljna trojka može nadopuniti do četvorke s najvećim elementom na najviše osam različitih načina. Spomenimo i nedavni rezultat koji su dobili Cipu, Dujella i Fujita da za proizvoljnu trojku $\{b, c, d\}$ postoje najviše dva proširenja do četvorke $\{a, b, c, d\}$ takva da je $a < \min(b, c, d)$.

Neka je $\{a, b, c\}$ Diofantova trojka koju želimo proširiti do četvorke $\{a, b, c, x\}$, onda treba vrijediti da su $ax + 1$, $bx + 1$, $cx + 1$ potpuni kvadrati. Množeći ova tri uvjeta, dobivamo jednadžbu eliptičke krivulje

$$y^2 = (ax+1)(bx+1)(cx+1). \tag{1.10}$$

Za ovu eliptičku krivulju kažemo da je inducirana s trojkom $\{a, b, c\}$. O ovakvim eliptičkim krivuljama će biti puno riječi u nastavku. Za sada navedimo samo sljedeću slutnju koja je jača od Slutnje 1.1.

Slutnja 1.2. *Neka je $\{a,b,c\}$ Diofantova trojka. Tada sva cjelobrojna rješenja jednadžbe (1.10) zadovoljavaju $x=0$ ili $x=d_+$ ili $x=d_-$, te dodatno $x=-1$ ako je $1\in\{a,b,c\}$.*

Recimo sada nešto o racionalnom slučaju. Već je rečeno da je Euler pokazao da postoji beskonačno mnogo racionalnih Diofantovih petorki. Prve primjere racionalnih Diofantovih šestorki pronašao je Gibbs 1999. godine. Dujella, Kazalicki, Mikić i Szikszai su 2017. godine dokazali da racionalnih Diofantovih šestorki ima beskonačno mnogo. Štoviše, dokazali su da postoji beskonačno mnogo trojki (primjerice $\{\frac{15}{14},-\frac{16}{21},\frac{7}{6}\}$) koje se svaka mogu nadopuniti od šestorke na beskonačno mnogo različitih načina (primjerice prethodna trojka se može nadopuniti do šestorke $\{\frac{15}{14},-\frac{16}{21},\frac{7}{6},-\frac{1680}{3481},-\frac{910}{1083},\frac{624}{847}\}$. Nadalje, postoji beskonačno mnogo racionalnih šestorki s pozitivnim elementima, a isto vrijedi i za bilo koji drugi izbor predznaka. Ova konstrukcija bitno koristi svojstva eliptičkih krivulja induciranih racionalnim Diofantovim trojkama, te će biti detaljno opisana kasnije.

Dujella i Kazalicki su 2017., koristeći ideju T. Piezasa, opisali alternativnu konstrukciju parametarske familije racionalnih Diofantovih šestorki. I ta konstrukcija koristi eliptičke krivulje, ali ovdje u tzv. Edwardsovom obliku. Ovdje konstrucija ne kreće od trojke, nego od četvorke $\{a,b,c,d\}$. Iz uvjeta $ab+1=t_{12}^2$, $ac+1=t_{13}^2$, $ad+1=t_{14}^2$, $bc+1=t_{23}^2$, $bd+1=t_{24}^2$, $cd+1=t_{34}^2$, dobivaju se racionalne točke na krivulji $(x^2-1)(y^2-1)=abcd$, čija se svojstva dalje koriste u konstrukciji familija šestorki $\{a,b,c,d,e,f\}$, od kojih je najjednostavnija:

$$\begin{aligned}
a &= \frac{(t^2-2t-1)(t^2+2t+3)(3t^2-2t+1)}{4t(t^2-1)(t^2+2t-1)},\\
b &= \frac{4t(t^2-1)(t^2-2t-1)}{(t^2+2t-1)^3},\\
c &= \frac{4t(t^2-1)(t^2+2t-1)}{(t^2-2t-1)^3},\\
d &= \frac{(t^2+2t-1)(t^2-2t+3)(3t^2+2t+1)}{4t(t^2-1)(t^2-2t-1)},\\
e &= \frac{-t^5+14t^3-t}{t^6-7t^4+7t^2-1},\\
f &= \frac{3t^6-13t^4+13t^2-3}{4t(t^4-6t^2+1)}.
\end{aligned}$$

Sličnu konstrukciju su primijenili Dujella, Kazalicki i Petričević 2019. godine da bi dokazali postojanje beskonačno mnogo racionalnih Diofantovih šestorki u kojima su nazivnici svih (potpuno skraćenih) elemenata potpuni kvadrati. Ta je konstrukcija bila motivirana sljedećim eksperimentalno pro-

nađenim primjerom šestorke

$$\left\{\frac{75}{8^2}, -\frac{3325}{64^2}, -\frac{12288}{125^2}, \frac{123}{10^2}, \frac{3498523}{2260^2}, \frac{698523}{2260^2}\right\}.$$

Isti autori su 2021. godine dali još jednu konstrukciju beskonačne familije racionalnih Diofantovih šestorki. Tako dobivene šestorke imaju specijalnu strukturu, naime, sadrže dvije regularne četvorke i jednu regularnu petorku (petorku dobivenu generalizacijom prije opisane Eulerove konstrukcije petorki). Polazište u konstrukciji bila je sljedeća parametrizacija racionalnih Diofantovih trojki koju ju pronašao Lasić:

$$\left\{\frac{2t_1(1+t_1t_2(1+t_2t_3))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}, \frac{2t_2(1+t_2t_3(1+t_3t_1))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}, \frac{2t_3(1+t_3t_1(1+t_1t_2))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}\right\}.$$

Sada se naravno postavlja pitanje postoji li neka racionalna Diofantova sedmorka. To pitanje je otvoreno i nije jasno što bi trebao biti odgovor na njega.

Pitanje 1.1. *Postoji li racionalna Diofantova sedmorka?*
Kako naći gornju ogradu za veličinu racionalnih Diofantovih m-torki?

Poznati su primjeri "gotovo" sedmorki, tj. skupova od sedam elemenata kojima samo jedan uvjet nedostaje da bi bili racionalne Diofantove sedmorke. Drugim riječima, postoje racionalne Diofantove petorke koje se mogu na dva različita načina proširiti do šestorke. Primjerice, petorka

$$\left\{\frac{243}{560}, \frac{1147}{5040}, \frac{1100}{63}, \frac{7820}{567}, \frac{95}{112}\right\}$$

se može proširiti do šestorke s $\frac{38269}{6480}$ i sa $\frac{196}{45}$.

Ovdje možemo spomenuti i da su Herrmann, Pethő & Zimmer 1999. dokazali da se svaka racionalna Diofantova četvorka može na najviše konačno mnogo načina proširiti do racionalne Diofantove petorke. Krenemo li od četvorke $\{a, b, c, d\}$ koju želimo nadopuniti do petorke, možda bi prva ideja bila promatrati krivulju $y^2 = (ax+1)(bx+1)(cx+1)(dx+1)$. Ovo je krivulja genusa 1 (biracionalno je ekvivalentna eliptičkoj krivulji) i ona može imati beskonačno mnogo racionalnih točaka. No ako naprije iz uvjeta da je $ae+1 = x^2$ izrazimo $e = (x^2-1)/a$, pa to uvrstimo u $(be+1)(ce+1)(de+1)$, dobivamo krivulju $y^2 = a(bx^2+a-b)(cx^2+a-c)(dx^2+a-d)$ genusa 2, koja po Faltingsovom teoremu ima samo konačno mnogo racionalnih točaka.

1.5 Poopćenja Diofantovih m-torki

Postoji više prirodnih poopćenja pojma Diofantovih m-torki. Možemo zamijeniti kvadrate s k-tim potencijama za neki fiksni $k \geq 3$. Takvi skupovi se

nazivaju *Diofantove m-torke k-stupnja*. Primjeri Diofantovih trojki trećeg i četvrtog stupnja su $\{2, 171, 25326\}$, odnosno $\{1352, 8539880, 9768370\}$. Bugeaud & Dujella su 2003. godine pokazali da ne postoje Diofantove četvorke k-stupnja za $k \geq 177$, te dobili slične (iako nešto slabije) ocjene za $k \leq 176$.

Promatran je i problem u kojem se kvadrati zamjenjuju s proizvoljnom potencijom. Znači, $a_i a_j + 1 = x^{k_{ij}}$, gdje je $k_{ij} \geq 2$. Luca je 2005. godine dokazao, uz pretpostavku da vrijedi abc-slutnja, da je veličina takva skupa ograničena s apsolutnom konstantom. Najbolji poznati bezuvjetni rezultat je dobio Stewart 2008. godine: ako skup $D \subseteq \{1, 2, \ldots, N\}$ ima svojstvo da je $ab + 1$ potencija nekog prirodnog broja za sve $a, b \in D$, $a \neq b$, onda je $|D| \ll (\log N)^{2/3} (\log \log N)^{1/3}$.

Više je autora promatralo verzije problema u kojem se kvadrati zamjenjuju s članovima nekog rekurzivno zadanog niza. Spomenimo ovdje da su 2008. godine Luca & Szalay pokazali da ne postoje tri različita prirodna brojeva a, b, c takva da su $ab+1$, $ac+1$ i $bc+1$ svi Fibonaccijevi brojevi ($F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ za $n \geq 2$), dok su isti autori 2009. godine dokazali da je jedina trojke prirodnih brojeva $a < b < c$ sa svojstvom da su $ab + 1$, $ac + 1$ i $bc + 1$ svi Lucasovi brojevi ($L_0 = 2$, $L_1 = 1$, $L_n = L_{n-1} + L_{n-2}$ za $n \geq 2$) trojka $(a, b, c) = (1, 2, 3)$.

Možemo zamijeniti broj 1 u uvjetu "$ab+1$ je kvadrat" s nekim drugim fiksiranim cijelim brojem n. Takvi skupovi se nazivaju $D(n)$-*m-torke* ili m-torke sa svojstvom $D(n)$. Slučaj $n = 4$ ima puno sličnosti s klasičnim slučajem $n = 1$. Množeći sve elemente $D(1)$-m-torke s 2, dobivamo $D(4)$-m-torku. Lako je vidjeti da u $D(4)$-m-torki najviše dva elementa mogu biti neparna. Zaista, kad bismo imali tri neparna elementa, recimo a_1, a_2, a_3, onda bi iz $a_i a_j + 4 \equiv 1 \pmod 8$, slijedilo da je $a_1 a_2 \equiv 5 \pmod 8$, $a_1 a_3 \equiv 5 \pmod 8$, $a_2 a_3 \equiv 5 \pmod 8$. Množeći ove tri kongruencije, dobivamo $(a_1 a_2 a_3)^2 \equiv 5 \pmod 8$, što je nemoguće. Dakle, svaki rezultat o veličini $D(1)$-m-torki ima izravnu, ali nešto slabiju, posljedicu na veličinu $D(4)$-m-torki. Primjerice, nepostojanje $D(1)$-petorki povlači nepostojanje $D(4)$-sedmorki. Međutim, pažljivom i tehnički zahtjevnom modifikacijom argumenata iz $n = 1$ slučaja, Bliznac Trebješanin i Filipin uspjeli su 2019. godine dokazati da ne postoji $D(4)$-petorka.

Lako je pokazati da ne postoji $D(n)$-četvorka ako je $n \equiv 2 \pmod 4$. Ovaj su rezultat neovisno dokazali 1985. godine Brown, Gupta & Singh te Mohanty & Ramasamy.

Teorem 1.1. *Ako je $n \equiv 2 \pmod 4$, onda ne postoji $D(n)$-četvorka.*

Dokaz: Iz pretpostavke da je $a_i a_j + n$ kvadrat i činjenice da kvadrati cijelih brojeva pri dijeljenju s 4 daju ostatke 0 ili 1, slijedi da je $a_i a_j \equiv 2$ ili $3 \pmod 4$. Odavde slijedi da nijedan od brojeva a_i nije djeljiv s 4. Dakle, imamo četiri broja, koja daju neki od tri moguća ostatka: $1, 2, 3$. Stoga dva od njih daju isti ostatak. Recimo da je $a_1 \equiv a_2 \pmod 4$. Tada je $a_1 a_2 \equiv$

$a_2^2 \equiv 0$ ili $1 \pmod 4$, što je u kontradikciji s prije pokazanim $a_1 a_2 \equiv 2$ ili $3 \pmod 4$. □

S druge strane, može se pokazati da ako je $n \not\equiv 2 \pmod 4$ i $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, onda postoji barem jedna $D(n)$-četvorka. Zaista, cijeli broj n koji nije oblika $4k+2$ ima jedan od sljedećih oblika:

$$4k+3, \;\; 8k+1, \;\; 8k+5, \;\; 8k, \;\; 16k+4, \;\; 16k+12.$$

A za svaki od tih oblika je, metodom sličnom onoj kojom se koristio Diofant, pronađena formula za $D(n)$-četvorku (Dujella, 1993.). Primjerice,

$$\{1, 9k^2+8k+1, 9k^2+14k+6, 36k^2+44k+13\}$$

je jedna $D(4k+3)$-četvorka. Uočimo da za $a = 9k^2+8k+1$, $b = 9k^2+14k+6$ imamo $ab + (4k+3) = r^2$, gdje je $r = 9k^2+11k+3$, te $a+b-2r = 1$ i $a+b+2r = 36k^2+44k+13$, pa znamo da je pet uvjeta iz definicije $D(4k+3)$-četvorke ispunjeno. No lako se provjeri i šesti uvjet: $1 \cdot (36k^2+44k+13) + (4k+3) = (6k+4)^2$. Izuzetci iz skupa S se pojavljuju zato što se za neke (male) k-ove može dogoditi da ove četvorke imaju dva elementa jednaka.

Za $n \in S$, pitanje postojanja $D(n)$-četvorki je još uvijek otvoreno. U slučaju $n = -1$, već smo u vezi Eulerovih m-torki spomenuli du su Dujella i Fuchs 2007. dokazali da ne postoji $D(-1)$-petorka, te zajedno s Filipinom da $D(-1)$-četvorki ima najviše konačno mnogo. Vrlo nedavno su Bonciocat, Cipu & Mignotte dokazali nepostojanje $D(-1)$-četvorki. Metode korištene u dokazu se slične onima koje su korištene u dokazu nepostojanja $D(1)$-petorki, ali je bilo potrebno uvođenje i nekih novih tehnika. Primijetimo da ovaj rezultat povlači nepostojanje $D(-4)$-četvorki, budući da nije teško dokazati da svi elementi $D(-4)$-četvorke moraju biti parni, pa bi dijeljenjem elemenata $D(-4)$-četvorke s 2 dobili $D(-1)$-četvorku.

Jasno da je ako je $n = m^2$ potpun kvadrat, onda postoji beskonačno mnogo $D(n)$-četvorki. Naime, prije spomenuti Eulerov rezultat pokazuje da postoji beskonačno mnogo $D(1)$-četvorki, a očito je da množenjem svih elemenata $D(1)$-četvorke s m dobivamo $D(m^2)$-četvorku. Otvoreno je pitanje koliko ima $D(n)$-četvorki u slučaju kada n nije potpun kvadrat i nije neki od n-ova za koje znamo da ne postoji $D(n)$-četvorka ($n \equiv 2 \pmod 4$, $n = -1$, $n = -4$).

Slutnja 1.3. *Ako je n cijeli broj koji nije potpun kvadrat, onda postoji najviše konačno mnogo $D(n)$-četvorki.*

Neka je

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

te

$$M = \sup\{M_n \,:\, n \in \mathbb{Z} \setminus \{0\}\}.$$

Poznato je da je M_n konačan za svaki cijeli broj $n \neq 0$. Slutnja je da je broj M također konačan, tj. da su brojevi M_n odozgo omeđeni konstantom neovisnom o n. To je međutim otvoren problem. Poznato je da je M_p za p prost omeđeno s konstantom neovisnom o p (Dujella & Luca su 2005. dokazali da vrijedi $M_p < 3 \cdot 2^{168}$), ali za opći n poznati su tek rezultati poput $M_n \leq 31$ za $|n| \leq 400$, $M_n < 15.476 \ln |n|$ za $|n| > 400$, $M_n < 2.6071 \ln |n|$ za dovoljno veliki $|n|$ (Dujella 2002. i 2004., Becker & Ram Murty 2019.).

Ako kombiniramo dva prethodno navedena poopćenja Diofantovih m-torki, onda možemo dobiti proizvoljno velike skupove. Naime, za svaki prirodni broj m postoji prirodni broj n i skup prirodnih brojeva A takav da je $|A| \geq m$ i $ab + n$ je potencija nekog prirodnog broja za sve $a, b \in A$, $a \neq b$. Preciznije, za dovoljno veliki x, može se uzeti $m = \left\lfloor \left(\frac{\ln \ln x}{2 \ln \ln \ln x} \right)^{1/3} \right\rfloor$ te (s pomoću Kineskog teorema o ostatcima) konstruirati skup $A_m = \{a_1, \ldots, a_m\} \subset [1, x]$ i prirodni broj $n_m \in [1, x]$ tako da je $a_j a_j + n_m = x_{ij}^{k_{ij}}$ za $1 \leq i < j \leq m$, gdje su x_{ij} prirodni brojevi, a eksponenti k_{ij} su prvih $\binom{m}{2}$ prostih brojeva (Bérczes, Dujella, Hajdu & Luca, 2011.).

Kod promatranja $D(n)$-m-torki obično se unaprijed fiksira cijeli broj n. Međutim, možemo se pitati može li jedan te isti skup imati istodobno svojstvo $D(n)$ za više različitih n-ova. To su pitanje postavili A. Kihel i O. Kihel 2001. godine. Primjerice, skup $\{8, 21, 55\}$ je istodobno i $D(1)$-trojka i $D(4321)$-trojka, dok je $\{1, 8, 120\}$ istodobno i $D(1)$-trojka i $D(721)$-trojka. Adžaga, Dujella, Kreso & Tadić su 2018. dokazali da postoji beskonačno mnogo trojki $\{a, b, c\}$ koje su istodobno $D(1)$, $D(n_2)$ i $D(n_3)$ trojke za $1 < n_2 < n_3$. Jedan primjer takve beskonačne familije trojki je

$$a = 2(i+1)i, \quad b = 2(i+2)(i+1), \quad c = 4(2i^2 + 4i + 1)(2i+3)(2i+1),$$

uz

$$n_2 = 32i^4 + 128i^3 + 172i^2 + 88i + 16,$$
$$n_3 = 256i^8 + 2048i^7 + 6720i^6 + 11648i^5 + 11456i^4 + 6400i^3 + 1932i^2 + 280i + 16,$$

za proizvoljan prirodni broj i. Konstrukcija se koristi cjelobrojnim točkama na eliptičkoj krivulji

$$y^2 = (x + ab)(x + ac)(x + bc).$$

Uočimo da, iako je ova krivulja izomorfna s prije spomenutom krivuljom $y^2 = (ax + 1)(bx + 1)(cx + 1)$ (preko transformacija $x \mapsto abcx$, $y \mapsto abcy$), pa su racionalne točke na jednoj i drugoj krivulji izravno povezane ovim transformacijama, kod cjelobrojnih točaka veza nije sasvim jasna te za razliku od krivulje $y^2 = (ax + 1)(bx + 1)(cx + 1)$, broj cjelobrojnih točaka na $y^2 = (x + ab)(x + ac)(x + bc)$ bitno ovisi o rangu ove eliptičke krivulje.

Poznato je da postoje skupovi koji su istodobno $D(n_1)$ i $D(n_2)$-četvorke za $n_1 \neq n_2$. Primjerice, $\{27, 115, 160, 1755\}$ je $D(-2016)$-četvorka i $D(37296)$-četvorka, dok je $\{1458, 66248, 5000, 14112\}$ i $D(16769025)$ i $D(406425600)$-četvorka (a također i $D(0)$-četvorka budući da su joj svi elementi dvostruki kvadrati; $n = 0$ se često isključuje iz definicije $D(n)$-m-torke jer je trivijalno vidjeti da postoje beskonačni skupovi s $D(0)$-svojstvom – kvadrati ili kvadrati pomnoženi s istim brojem, ali kad se taj uvjet kombinira s drugim netrivijalnim uvjetima pojave se zanimljivi problemi pa u takvom kontekstu ima smisla dozvoliti i $n = 0$ u definiciji) Štoviše, četvorki s ovim svojstvima ima beskonačno mnogo (Dujella & Petričević, 2020.). Nedavno su Dujella, Kazalicki & Petričević dokazali da postoji beskonačno mnogo $D(n)$-petorki čiji su elementi kvadrati (pa su ujedno i $D(0)$-petorke). Jedan takav primjer je $D(480480^2)$-petorka $\{225^2, 286^2, 819^2, 1408^2, 2548^2\}$.

Umjesto nad cijelim ili racionalnim brojevima, Diofantov problem se može promatrati nad bilo kojim komutativnim prstenom s jedinicom. Spomenimo rezultate koje su dobili Franušić i Soldo nad prstenima cijelih brojeva u nekim kvadratnim poljima, koji pokazuju da postoji uska (ali još ne sasvim razjašnjena) veza između postojanja $D(n)$-četvorki i prikazivosti elementa n kao razlike dvaju kvadrata u promatranom prstenu. Uočimo da su cijeli brojevi $n \equiv 2 \pmod 4$ iz Teorema 1.1 upravo oni cijeli brojevi koji se ne mogu prikazati kao razlika dvaju kvadrata. Spomenimo i da je Adžaga nedavno dokazao da u prstenu cijelih brojeva u imaginarnom kvadratnom polju ne postoji $D(1)$-m-torka za $m \geq 43$.

Jednostavna veza između problema postojanja $D(n)$-četvorke i prikazivosti broja n kao razlike dva kvadrata u promatranom prstenu, pojavi se ako dopustimo da dva elementa četvorke budu jednaka. Naime, ako je $n = k^2 - a^2$, onda četiri broja $a, a, 2a + 2k, 5a + 4k$ imaju svojstvo da je

$$\begin{aligned} a \cdot a + n &= k^2, \\ a \cdot (2a + 2k) + n &= (a + k)^2, \\ a \cdot (5a + 4k) + n &= (2a + k)^2, \\ (2a + 2k) \cdot (5a + 4k) + n &= (3a + 3k)^2. \end{aligned}$$

Ovo naravno ne rješava problem egzistencije $D(n)$-četvorki, ali daje naslutiti da će za brojeve koji se mogu prikazati kao razlika dva kvadrata ili postojati $D(n)$-četvorka ili će dokazivanje nepostojanja $D(n)$-četvorke biti težak problem (jer ga nećemo moći riješiti jednostavnim ispitivanje kongruencija po nekom modulu kao u slučaju brojeva oblika $4k + 2$ iz Teorema 1.1).

Različite verzije Diofantova problema su proučavane i u prstenima polinoma. Dujella i Fuchs su 2004. dokazali da je svaka Diofantova četvorka u $\mathbb{Z}[x]$ regularna. Nedavno su Filipin i Jurasić dokazali da ista tvrdnja vrijedi i u $\mathbb{R}[x]$. S druge strane, Dujella i Jurasić su 2010. pokazali da ta tvrdnja ne

vrijedi u $\mathbb{C}[x]$ jer je za svaki $p \in \mathbb{C}[x]$,

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

Diofantova četvorka koja nije regularna.

Uočimo da smo u definiciji (racionalne) Diofantove m-torke isključili zahtjev da produkt elementa sa samim sobom uvećan za 1 daje kvadrat. Očito je da u cijelim brojevima taj uvjet ne može biti zadovoljen (jednadžba $a^2 + 1 = r^2$ nema rješenja u skupu prirodnih brojeva). No u skupu racionalnih brojeva nema nekog očitog razloga zašto takvi skupovi (koje bismo mogli nazvati *jake Diofantove m-torke*) ne bi postojali. Svaki element a takvog skupa trebao bi zadovoljavati da je a^2+1 kvadrat, pa je stoga $a = X/Y$, gdje je (X, Y, Z) Pitagorina trojka, tj. $X^2 + Y^2 = Z^2$. Dujella i Petričević su 2008. godine dokazali je da postoji beskonačno mnogo jakih racionalnih Diofantovih trojki (primjerice

$$\left\{\frac{1976}{5607}, \frac{3780}{1691}, \frac{14596}{1197}\right\}$$

je jedna takva trojka), ali nije poznato postoji li ijedna jaka Diofantova četvorka. Poznato je da postoje četvorke kojima nedostaje samo jedan uvjet da bi bile jake Diofantove četvorke. Primjerice, za

$$\left\{\frac{140}{51}, \frac{2223}{30464}, \frac{278817}{33856}, \frac{3182740}{17661}\right\},$$

jedini uvjet koji nedostaje je da produkt trećeg i četvrtog elementa uvećan za 1 nije kvadrat. Proučavane su i jake $D(-1)$-trojke (Dujella, Gusić, Petričević & Tadić, 2018.), te općenitije jake $D(q)$-trojke (Dujella, Paganin & Sadek, 2020.), te je poznato da za beskonačno mnogo kvadratno slobodnih cijelih brojeva q, postoji beskonačno mnogo jakih $D(q)$-trojki. Primjerice,

$$\left\{1, \frac{5}{4}, \frac{14645}{484}\right\}$$

je jedna jaka $D(-1)$-trojka, dok je

$$\left\{\frac{7769}{1638}, \frac{38893009}{50902488}, \frac{50817649}{35348950}\right\}$$

je jedna jaka $D(2)$-trojka.

Poglavlje 2

Eliptičke krivulje na poljem racionalnih brojeva

2.1 Uvod u eliptičke krivulje

Eliptičke krivulje imaju važnu ulogu u više područja matematike (teorija brojeva, algebarska geometrija, kompleksna analiza), a odnedavno su postale i vrlo bitne za primjene u kriptografiji. Eliptička krivulja može se definirati nad proizvoljnim poljem. U teoriji brojeva najvažniji je slučaj polja racionalnih brojeva $\mathbb{Q}$, dok su za primjene najvažnija konačna polja. U problemima vezanim uz (racionalne) Diofantove m-torke prirodno se pojavljuju eliptičke krivulje nad $\mathbb{Q}$, pa će o njima u ovom pregledu svojstava eliptičkih krivulja biti najviše riječi.

Neka je K polje. *Eliptička krivulja* nad K je nesingularna projektivna kubna krivulja nad K s barem jednom točkom nad K. Ona ima (afinu) jednadžbu oblika

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

gdje su koeficijenti $a, b, c, \ldots, j \in K$, a nesingularnost znači da je u svakoj točki na krivulji, promatranoj u projektivnoj ravnini $\mathbb{P}^2(\overline{K})$ nad algebarskim zatvorenjem od K, barem jedna parcijalna derivacija funkcije F različita od 0. Može se pokazati da se svaka takva jednadžba može biracionalnim transformacijama (racionalnim transformacijama čiji je inverz također racionalna transformacija) svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

koji nazivamo *Weierstrassova forma* eliptičke krivulje.

Nadalje, ako je karakteristika polja K različita od 2 i 3 (pa smijemo nadopunjavati na potpuni kvadrat i potpuni kub dijeleći s 2 i 3 ako je potrebno),

onda se ova jednadžba može transformirati u oblik

$$y^2 = x^3 + ax + b, \tag{2.2}$$

koji nazivamo *kratka Weierstrassova forma*. Uvjet nesingularnosti je sada da kubni polinom $f(x) = x^3+ax+b$ nema višestrukih nultočaka (u algebarskom zatvorenju $\overline{K}$), a to je pak ekvivalentno uvjetu da je *diskriminanta* $\Delta = -16(4a^3 + 27b^2)$ različita od 0.

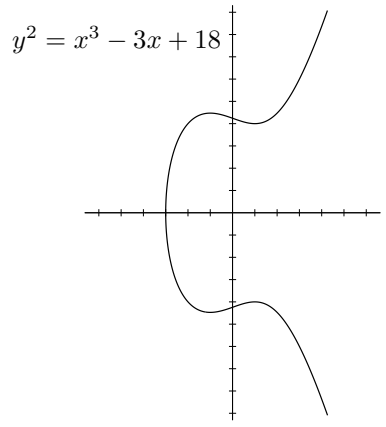
Često se pod eliptičkom krivuljom E nad poljem K (karakteristike različite od 2 i 3) podrazumijeva skup svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu $y^2 = x^3 + ax + b$, gdje su $a, b \in K$ i $4a^3 + 27b^2 \neq 0$, zajedno s "točkom u beskonačnosti" $\mathcal{O}$. Taj skup ćemo označavati s $E(K)$.

Točka u beskonačnosti se pojavljuje prirodno ako eliptičku krivulju prikažemo u projektivnoj ravnini. *Projektivnu ravninu* $\mathbb{P}^2(K)$ dobijemo tako da na skupu $K^3 \setminus \{(0, 0, 0)\}$ uvedemo relaciju ekvivalencije $(X, Y, Z) \sim (kX, kY, kZ)$, $k \in K$, $k \neq 0$. Ako u (afinoj) jednadžbi eliptičke krivulje uvedemo supstituciju $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, dobivamo projektivnu jednadžbu

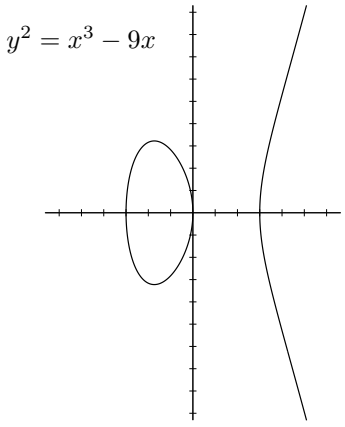
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Ako je $Z \neq 0$, onda klasa ekvivalencije od (X, Y, Z) ima reprezentant $(x, y, 1)$, pa tu klasu možemo identificirati s (x, y). Međutim, postoji i jedna klasa ekvivalencije koja sadržava točke za koje je $Z = 0$. Ona ima reprezentant $(0, 1, 0)$ i tu klasu identificiramo s točkom u beskonačnosti $\mathcal{O}$.

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na skupu $E(K)$, njihovih K-racionalnih točaka, može na prirodan način uvesti operacija uz koju one postaju Abelove grupe. Da bismo to objasnili, uzmimo da je $K = \mathbb{R}$ polje realnih brojeva. Tada eliptičku krivulju $E(\mathbb{R})$ (bez točke u beskonačnosti) možemo prikazati kao podskup ravnine. Polinom $f(x)$ može imati ili jedan (ako je $\Delta < 0$) ili tri (ako je $\Delta > 0$) realna korijena. U ovisnosti o tome, graf pripadne eliptičke krivulje ima jednu ili dvije komponente, kao što je prikazano na sljedećim slikama.

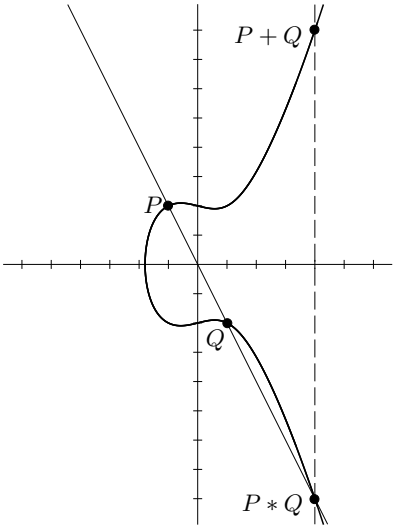


jedna komponenta

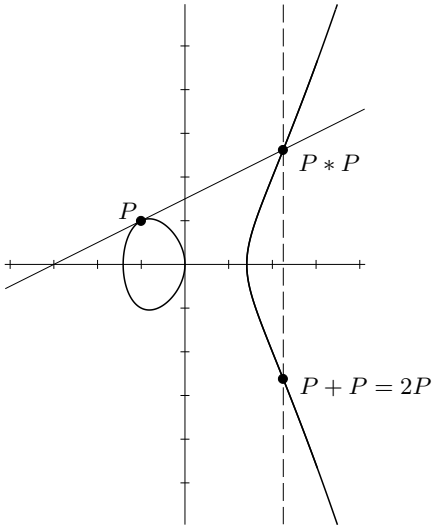


dvije komponente

Definirat ćemo operaciju zbrajanja na $E(\mathbb{R})$. Neka su $P, Q \in E(\mathbb{R})$. Povucimo pravac kroz točke P i Q. On općenito siječe krivulju E u tri točke. Treću točku označimo s $P * Q$. Sada definiramo da je $P + Q$ osnosimetrična točka točki $P * Q$ s obzirom na os x. Ako je $P = Q$, onda umjesto sekante povlačimo tangentu kroz točku P. Ako je P točka infleksije, onda uzimamo da je $P * P = P$. Nadalje, uzimamo da pravac siječe točku u beskonačnosti $\mathcal{O}$ ako i samo ako je okomit na os x, tako da vrijedi $P + \mathcal{O} = \mathcal{O} + P = P$ za svaki $P \in E(\mathbb{R})$.



sekanta



tangenta

Dakle, operacija (zbrajanje) na skupu $E(\mathbb{R})$ se uvodi "geometrijski", tako da je zbroj triju različitih točaka na krivulji jednak neutralnom elementu ako i samo ako su one kolinearne. Naravno da se ovaj geometrijski zakon može opisati i eksplicitnim formulama za koordinate zbroja točaka. Tako dobivene formule onda mogu poslužiti za definiciju zbrajanja točaka na eliptičkoj krivulji nad proizvoljnim poljem (uz malu modifikaciju ako je karakteristika polja 2 ili 3). Navedimo sada te formule.

Neka je $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Tada je

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

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

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

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

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

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

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

Broj λ je koeficijent smjera pravca kroz P i Q, odnosno tangente u točki P u slučaju $P = Q$. Uvrštavanjem jednadžbe pravca kroz točku P, tj. $y = \lambda(x-x_1)+y_1$ u jednadžbu eliptičke krivulje te izjednačavanjem koeficijenata uz x^2 (Vièteove formule) u

$$x^3 + ax + b - (\lambda(x - x_1) + y_1)^2 = (x - x_1)(x - x_2)(x - x_3),$$

dobivamo gore navedenu formulu za koordinatu x_3.

Pokazuje se da je $(E(K), +)$ Abelova grupa. Sva svojstva Abelove grupe su evidentna, osim asocijativnosti, čiji je dokaz nešto kompliciraniji. Jedan način za dokazivanje asocijativnosti je raspisivanje svih mogućih slučajeva (u ovisnosti o tome koji se od slučajeva iz definicije zbrajanja pojavljuje) te usporedba izraza koji se dobiju na lijevoj, odnosno desnoj strani od $(P + Q) + R = P + (Q + R)$. Ima i elegantnijih dokaza (neke ćemo uskoro spomenuti), ali oni zahtijevaju poznavanje nekih činjenica iz kompleksne analize ili projektivne geometrije.

Za primjene u kriptografiji najvažniji je slučaj kada je K konačno polje $\mathbb{F}_q$. Posebno su važni slučajevi $q = p$ (prosti broj) i $q = 2^k$. S druge strane, u teoriji brojeva najvažniju ulogu imaju eliptičke krivulje nad poljem racionalnih brojeva $\mathbb{Q}$.

Možemo se pitati otkud dolazi naziv eliptička krivulja. Naziv jasno asocira na elipsu, ali za sada nismo vidjeli nikakvu vezu između ta dva pojma. Veza između eliptičkih krivulja i elipse dolazi preko problema računanja opsega elipse. Neka je elipsa zadana jednadžbom $q^2x^2 + p^2y^2 = p^2q^2$. Tada je njezin opseg jednak vrijednosti integrala

$$4\int_0^1 \frac{p^2 - (p^2 - q^2)t^2}{\sqrt{(1 - t^2)(p^2 - (p^2 - q^2)t^2)}}\, dt.$$

S pomoću racionalne supstitucije ovaj se integral može svesti na sličan integral u kojem se pod korijenom nalazi kubna funkcija. Općenito se integrali u kojima je javljaju drugi korijeni polinoma trećeg ili četvrtog stupnja (bez višestrukih korijena nazivaju) *eliptički integrali*. Oni se ne mogu izraziti s pomoću elementarnih funkcija. Međutim, moguće ih je izraziti s pomoću *Weierstrassove $\wp$-funkcije*. Ova funkcija zadovoljava diferencijalnu jednadžbu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

Ovdje je njezina uloga analogna ulozi funkcije sinus (ili kosinus) u računanju integrala kod kojih se ispod korijena javljaju kvadratne funkcije. Naime, funkcija $y = \sin x$ zadovoljava diferencijalnu jednadžbu $y^2+(y')^2 = 1$. Slično kao što jediničnu kružnicu možemo parametrizirati s $(\cos t, \sin t)$, tako se kompleksne točke na eliptičkoj krivulji $y^2 = x^3 + ax + b$ mogu parametrizirati s $(\wp(t), \frac{1}{2}\wp'(t))$. Štoviše, pokazuje se da ako je $P = (\wp(t), \frac{1}{2}\wp'(t))$ i

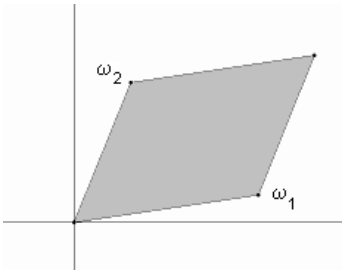
$Q = (\wp(u), \frac{1}{2}\wp'(u))$, onda je $P + Q = (\wp(t+u), \frac{1}{2}\wp'(t+u))$. Dakle, zbrajanje točaka na $E(\mathbb{C})$ odgovara zbrajanju kompleksnih brojeva. Poznavanje te činjenice daje elegantni dokaz asocijativnosti zbrajanja točaka na eliptičkoj krivulji.

Kad se promatra nad poljem $\mathbb{R}$, eliptička krivulja je stvarno "krivulja", tj. 1-dimenzionalni objekt. No promatrana nad $\mathbb{C}$ ona postaje 2-dimenzionalni objekt ("ploha") u 4-dimenzionalnom (realnom) prostoru. Pokušajmo vizualizirati tu plohu.

Tu nam može pomoći funkcija $\wp$. Ona posjeduje mnoga važna svojstva. Jedno od njih jest da je dvostruko periodična, tj. postoje kompleksni brojevi ω_1 i ω_2 (takvi da $\omega_1/\omega_2 \notin \mathbb{R}$) sa svojstvom $\wp(z + m\omega_1 + n\omega_2) = \wp(z)$ za sve cijele brojeve m, n. (I tu imamo analogiju s (jednostrukom) periodičnošću trigonometrijskih funkcija sinus i kosinus.) Označimo s L "rešetku" svih točaka oblika $m\omega_1 + n\omega_2$. Funkcija $\wp$ je analitička u svim točkama kompleksne ravnine, osim u točkama iz rešetke L u kojima ima pol drugog reda (tj. $\wp$ je meromorfna funkcija). Naime, vrijedi da je

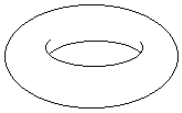
$$\wp(z) = \frac{1}{z^2} + \sum_{w \in L,\, w \neq 0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

Općenito se meromorfne, dvostruko periodične funkcije nazivaju *eliptičke funkcije*. Gore navedena parametrizacija točaka na eliptičkoj krivulji pomoću funkcije $\wp$ zapravo je izomorfizam grupa $E(\mathbb{C})$ i $\mathbb{C}/L$. Funkcija $\wp$ je potpuno određena svojim vrijednostima u "fundamentalnom paralelogramu" koji se sastoji od svih kompleksnih brojeva oblika $\alpha\omega_1 + \beta\omega_2$, $0 \leq \alpha, \beta < 1$.



fundamentalni paralelogram

Razlika točaka koje se nalaze nasuprot jedna drugoj na paralelnim stranicama tog paralelograma je element iz L. Stoga su te točke poistovjećene u skupu $\mathbb{C}/L$. Da bismo vizualizirali taj skup, možemo zamisliti da smo najprije "slijepili" dvije suprotne stranice paralelograma. Tako dobivamo valjak. Nakon toga "slijepimo" baze toga valjka. Tako dobivamo torus.



torus

Torus možemo zamisliti i kao sferu s "rupom". Pokazuje se da se ravninske algebarske krivulje mogu prikazati u trodimenzionalnom prostoru kao sfere s konačno mnogo rupa. Taj broj rupa se može shvatiti kao neformalna definicija *genusa* (ili *roda*) krivulje. Alternativna (šira) definicija eliptičke krivulje je da je to nesingularna projektivna algebarska krivulja genusa jednakog 1 s barem jednom točkom definiranom nad promatranim poljem. Ova definicija uključuje ne samo nesingularne kubne krivulje već i sve one krivulje koje su im biracionalno ekvivalentne. Biracionalne transformacije čuvaju genus krivulje, ali ne čuvaju njezin stupanj.

Ako krivulja ima stupanj n, onda je njezin genus $\leq (n-1)(n-2)/2$, s tim da ako je krivulja nesingularna, onda joj je genus upravo jednak $(n-1)(n-2)/2$. Poznato je da tzv. hipereliptičke krivulje čija je jednadžba $y^2 = f(x)$, gdje je $f(x)$ polinom stupnja $n \geq 3$ bez višestrukih korijena, imaju genus $\lfloor (n-1)/2 \rfloor$. To posebno znači da, uz slučaj kada je $n = 3$, i u slučaju kad je $n = 4$ također imamo eliptičku krivulju (ukoliko krivulja ima barem jednu racionalnu točku; za razliku od slučaja $n = 3$, gdje uvijek postoji racionalna točka (točka u beskonačnosti), za $n = 4$ takva točka ne mora uvijek postojati). Uvjerimo se u to na jednom primjeru. Neka je C krivulja zadana jednadžbom

$$y^2 = x^4 + 3x^2 + 2x.$$

Ona ima očitu racionalnu točku $(0, 0)$. Supstitucijama $x = \frac{2}{v}$, $y = \frac{2t}{v^2}$ dobivamo krivulju $t^2 = v^3 + 3v^2 + 4$ te konačno supstitucijom $v + 1 = s$ dobivamo eliptičku krivulju E u kratkoj Weiestrassovoj formi

$$t^2 = s^3 - 3s + 6.$$

Dakle, transformacija koja prevodi C u E je $x = \frac{2}{s-1}$, $y = \frac{2t}{(s-1)^2}$. Inverzna transformacija je $s = \frac{x+2}{x}$, $t = \frac{2y}{x^2}$. Stoga je ovo biracionalna transformacija.

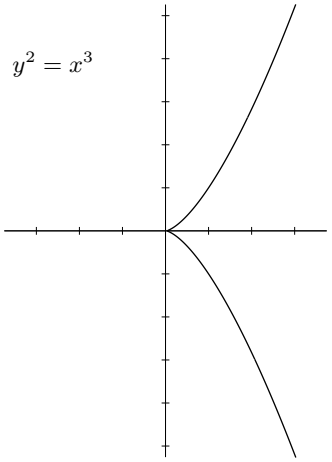
Genus krivulje igra važnu ulogu kod klasifikacije diofantskih jednadžbi. Naime, o njemu ovisi broj cjelobrojnih, odnosno racionalnih rješenja jednadžbe te struktura skupa tih rješenja.

Krivulje genusa 0 (s barem jednom racionalnom točkom) su upravo one koje posjeduju parametrizaciju s pomoću racionalnih funkcija. Svaka krivulja drugog stupnja (konika) ima genus 0. Npr. krivulja $x^2 + y^2 = 1$ ima racionalnu parametrizaciju

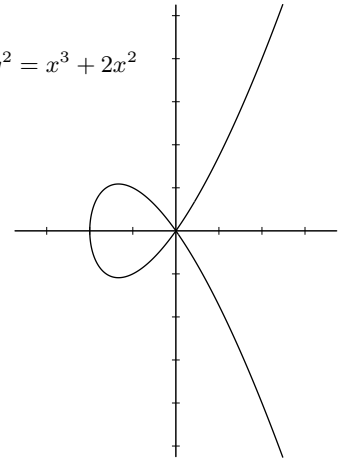
$$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}.$$

(što možemo zaključiti iz formula za Pitagorine trojke i očite veze između cjelobrojnih rješenja jednadžbe $X^2 + Y^2 = Z^2$ i racionalnih rješenja jednadžbe $x^2 + y^2 = 1$, tako da stavimo $t = n/m$ u $X = m^2 - n^2$, $Y = 2mn$, $Z = m^2 + n^2$, $x = X/Z$, $y = Y/Z$, ili kao u dolje navedenim primjerima, povlačenjem pravca s racionalnim koeficijentom smjera t kroz racionalnu točku $(-1, 0)$ na krivulji).

Kubne singularne krivulje također imaju genus 0. Npr. krivulja $y^2 = x^3$ ima singularnu točku $(0, 0)$ (šiljak – *cusp*). Stoga ova kubna krivulja nije eliptička. Njezina racionalna parametrizacija je $x = t^2$, $y = t^3$. Kao drugi primjer navedimo krivulju $y^2 = x^3 + 2x^2$. Ona također ima singularnu točku $(0, 0)$ (čvor – *node*) i ima racionalnu parametrizaciju $x = t^2 - 2$, $y = t^3 - 2t$.



singularna krivulja – šiljak



singularna krivulja – čvor

Očito je da ove dvije kubne krivulje imaju beskonačno mnogo cjelobrojnih točaka. Pellova jednadžba $x^2 - dy^2 = 1$ (d je prirodni broj koji nije potpun kvadrat) je primjer krivulje drugog stupnja koja ima beskonačno mnogo cjelobrojnih točaka. Krivulja genusa 1 može imati samo konačno mnogo cjelobrojnih točaka. Racionalnih točaka može biti beskonačno mnogo, ali su "konačno generirane" (sve se mogu dobiti iz konačno točaka primjenom grupovne operacije na eliptičkoj krivulji). Krivulja genusa većeg od 1 može imati samo konačno mnogo racionalnih točaka. Ova tvrdnja je poznata Mordellova slutnja koju je 1983. godine dokazao Faltings.

2.2 Jednadžbe eliptičke krivulje

Iako su za teoriju brojeva najzanimljivije eliptičke krivulje nad poljem $\mathbb{Q}$, započet ćemo s razmatranjima koja su valjana u bilo kojem polju karakteristike različite od 2 i 3, a i za te karakteristike se mogu dobiti analogni rezultati uz manje modifikacije. Zanimat će nas najprije kako se različite jednadžbe eliptičkih krivulja (i općenitije krivulja genusa 1) mogu transformirati u Weierstrassov oblik.

Neka je K polje karakteristike različite od 2 i promotrimo kubnu krivulju s koeficijentima iz polja K koja ima barem jednu K-racionalnu točku (p, q). Opisat ćemo Nagellov algoritam s pomoću kojeg se jednadžba krivulje može transformirati u Weierstrassovu formu (ili ustanoviti da je krivulja singularna, pa nije eliptička).

Zamjenom u s $u+p$ i v s $v+q$, možemo pretpostaviti da je K-racionalna točka upravo $(0,0)$. Dakle, imamo jednadžbu

$$f(u,v) = s_1u^3 + s_2u^2v + s_3uv^2 + s_4v^3 + s_5u^2 + s_6uv + s_7v^2 + s_8u + s_9v = 0. \tag{2.3}$$

Ako bi bilo $s_8 = s_9 = 0$, onda bi točka $(0,0)$ bila singularna. Stoga (zamjenjujući u i v ako je potrebno) možemo pretpostaviti da je $s_9 \neq 0$. Uvedimo projektivne koordinate: $u = \frac{U}{W}$, $v = \frac{V}{W}$ te prikažimo jednadžbu u obliku

$$F = F_3 + F_2W + F_1W^2 = 0,$$

gdje su F_i, $i = 1,2,3$, homogeni polinomi stupnja i:

$$\begin{aligned} F_3 &= s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3, \\ F_2 &= s_5U^2 + s_6UV + s_7V^2, \\ F_1 &= s_8U + s_9V. \end{aligned}$$

Racionalna točka $P = (u,v) = (0,0)$ sada ima koordinate $(U,V,W) = (0,0,1)$. Tangenta u točki P je dana jednadžbom $F_1 = 0$ i siječe krivulju u točki $Q = (-e_2s_9, e_2s_8, e_3)$, gdje je $e_i = F_i(s_9, -s_8)$ za $i = 2,3$. Uočimo da e_2 i e_3 ne mogu oba biti 0 jer bi tada tangenta bila komponenta krivulje, pa ne bismo imali eliptičku krivulju ($e_2 = 0$ znači da je $P = Q$ točka infleksije, dok $e_3 = 0$ znači da je Q točka u beskonačnosti). Ako je $e_3 \neq 0$, uvodimo supstituciju

$$U = U' - \frac{s_9e_2}{e_3}W', \quad V = V' + \frac{s_8e_2}{e_3}W', \quad W = W',$$

a ako je $e_3 = 0$, onda uvodimo supstituciju

$$U = U' - s_9W', \quad V = V' + s_8W', \quad W = U'.$$

U oba slučaja točka Q je u ishodištu novog koordinatnog sustava $(U',V',W') = (0,0,1)$, a tangenta u točki P ima jednadžbu $s_8U' + s_9V' = 0$.

Sada se možemo vratiti na afine koordinate $u' = \frac{U'}{W'}$, $v' = \frac{V'}{W'}$ jer su nam projektivne koordinate u biti trebale samo da razriješimo slučaj kada je Q bila točka u beskonačnosti u originalnim koordinatama.

Prikažimo jednadžbu u u' i v' kao $f' = f'_1 + f'_2 + f'_3 = 0$, gdje su $f'_i = f'_i(u',v')$ homogeni dijelovi od f' stupnja i. Dakle, imamo

$$u'^2f'_3(1,t) + u'f'_2(1,t) + f'_1(1,t) = 0, \tag{2.4}$$

gdje je $t = \frac{v'}{u'}$. Jednadžbu (2.4) možemo shvatiti kao kvadratnu jednadžbu po u'. Rješenja su joj

$$u' = \frac{-\phi_2 \pm \sqrt{\delta}}{2\phi_3}, \tag{2.5}$$

gdje je $\phi_i = f_i'(1,t)$ i $\delta = \phi_2^2 - 4\phi_1\phi_3$. Vrijednosti od t za koje je $\delta = 0$ su koeficijenti smjera tangenata na krivulju koje prolaze točkom $Q = (0,0)$ (jer pravci kroz Q imaju jednadžbu $v' = tu'$). Jedna od tih vrijednosti je $t_0 = -\frac{s_8}{s_9}$. Vidimo da je δ polinom četvrtog stupnja čija je jedna nultočka t_0. Stavimo $t = t_0 + \frac{1}{\tau}$, pa je $\rho = \tau^4\delta$ kubni polinom u τ.

Naposljetku, ako je

$$\rho = c\tau^3 + d\tau^2 + e\tau + k,$$

onda mora biti $c \neq 0$ (jer za $c = 0$ ne bismo imali eliptičku krivulju), pa nam supstitucije $\tau = \frac{x}{c}$, $\rho = \frac{y^2}{c^2}$ daju Weierstrassovu jednadžbu

$$y^2 = x^3 + dx^2 + cex + c^2k.$$

Veza originalnih varijabli u, v s x, y se može dobiti preko (2.5), gdje je $t = t_0 + \frac{c}{x}$, $\delta = \frac{c^2y^2}{x^4}$.

Primjer 2.1. *Ilustrirajmo upravo opisanu konstrukciju na primjeru krivulje dane jednadžbom $u^3 + v^3 = 1$, koja je usko povezana s Fermatovom jednadžbom za eksponent 3: $x^3 + y^3 = z^3$.*

Rješenje: Krivulja $u^3 + v^3 - 1 = 0$ ima očitu racionalnu točku $(u,v) = (0,1)$. Da bi ju translatirali u točku $(0,0)$, zamijenimo v s $v+1$. Tako dobivamo jednadžbu $u^3 + (v+1)^3 - 1 = 0$, tj.

$$u^3 + v^3 + 3v^2 + 3v = 0.$$

Ovdje je $e_8 = 0$, $e_9 = 3 \neq 0$. Nadalje, imamo $e_2 = 0$, $e_3 = 27$, pa je $P = Q$. Uz supstituciju $v = tu$, dobivamo kvadratnu jednadžbu po u:

$$(t^3+1)u^2 + 3ut^2 + 3t = 0,$$

čija je diskriminanta $\delta = -3t^4 - 12t$. Vidimo (a i znamo iz konstrukcije) da dobiveni polinom četvrtog stupnja ima racionalnu nultočku $t_0 = 0$, pa uvodimo supstituciju $t = 1/\tau$. Tako dobivamo $\rho = -12\tau^3 - 3$. Konačno, supstitucijom $\tau = -x/12$, dobivamo jednadžbu eliptičke krivulje

$$y^2 = x^3 - 432. \qquad \diamondsuit$$

Često se eliptičke krivulje prikazuju u (dugoj) Weierstrassovoj formi

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

Ta je forma "dobra" nad svakim poljem (bez obzira na karakteristiku), a vrlo je prikladna za opis eliptičkih krivulja nad $\mathbb{Q}$ s točkama zadanog konačnog reda. Pokažimo kako se od nje (u polju karakteristike različite od 2 i 3)

dobiva kratka Weierstrassova forma. Supstitucijom $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ eliminiramo sve članove koji sadržavaju y, osim y^2 (ovo možemo napraviti ako karakteristika nije 2, pa smijemo dijeliti s 2). Dobivamo

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.6}$$

gdje je

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

Još se definira i $b_8 = \frac{1}{4}(b_2b_6 - b_4^2) = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$. Uočimo da ako svakom a_i pridijelimo "težinu" i, onda je svaki od b_i-ova homogeni izraz težine i; ako još x-u pridijelimo težinu 2, a y-u težinu 3, onda svi pribrojnici u (2.6) imaju težinu 6.

Ako je karakteristika polja različita i od 3, onda možemo uvesti supstitucije $x \mapsto \frac{x-3b_2}{36}$, $y \mapsto \frac{y}{108}$ te dobiti jednadžbu u kratkoj Weierstrassovoj formi

$$y^2 = x^3 - 27c_4x - 54c_6,$$

gdje je

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

U različitim situacijama (primjerice kod konstrukcije krivulja velikog ranga) pojavljuju se krivulje oblika

$$v^2 = au^4 + bu^3 + cu^2 + du + e, \quad a \neq 0. \tag{2.7}$$

Pretpostavimo da polinom na desnoj strani od (2.7) nema višestrukih nultočaka te da krivulja ima barem jednu točku (p, q) s koordinatama iz K. Tada se (2.7) može transformirati u Weierstrassovu formu s pomoću biracionalnih transformacija (s koeficijentima u K). Zamjenom u s $u + p$ možemo pretpostaviti da je $p = 0$, tj. da je K-racionalna točka na (2.7) točka $(0, q)$.

Pretpostavimo najprije da je $q = 0$. Tada je $e = 0$, pa mora biti $d \neq 0$ jer bi inače $u = 0$ bila višestruka nultočka. Množenjem (2.7) s $\frac{d^2}{u^4}$ dobivamo

$$\left(\frac{dv}{u^2}\right)^2 = \left(\frac{d}{u}\right)^3 + c\left(\frac{d}{u}\right)^2 + bd\left(\frac{d}{u}\right) + ad^2,$$

tj. Weierstrassovu jednadžbu u $\frac{d}{u}$ i $\frac{dv}{u^2}$. Točka $(0, 0)$ odgovara točki u beskonačnosti $\mathcal{O}$.

Slučaj $q \neq 0$ je kompliciraniji, no izravnim računom se provjerava da vrijedi sljedeća propozicija.

Propozicija 2.1. *Neka je K polje karakteristike različite od 2. Promotrimo krivulju danu jednadžbom*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2,$$

gdje su $a, b, c, d, q \in K$. Neka je

$$x = \frac{2q(v+q)+du}{u^2}, \quad y = \frac{4q^2(v+q)+2q(du+cu^2)-\frac{d^2u^2}{2q}}{u^3},$$

te definirajmo

$$a_1 = \frac{d}{q},\ a_2 = c - \frac{d^2}{4q^2},\ a_3 = 2qb,\ a_4 = -4q^2a,\ a_6 = a_2a_4.$$

Tada je

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

Inverzna transformacija je dana s

$$u = \frac{2q(x+c)-\frac{d^2}{2q}}{y}, \quad v = -q + \frac{u(ux-d)}{2q}.$$

Točka $(u, v) = (0, q)$ odgovara točki u beskonačnosti $\mathcal{O}$, a točka $(u, v) = (0, -q)$ odgovara točki $(x, y) = (-a_2, a_1a_2 - a_3)$.

Edwards je 2007. godine opisao novi zanimljiv oblik jednadžbe krivulje koja je biracionalno ekvivalentna eliptičkoj krivulji. Zanimljivost kod tog oblika jest da dopušta jedinstvene formule za zbrajanje točaka, tj. ne treba razlikovati slučajeve $P + Q$ za $P \neq Q$ i $P + P$. Nadalje, pokazalo se da taj oblik nudi i neke prednosti kod implementacije (manji broj množenja u polju za računanje zbroja točaka). Stoga su *Edwardsove krivulje* i njihove varijante predmet vrlo velikog interesa i istraživanja u zadnjih desetak godina.

I tu je potrebno razlikovati slučaj karakteristike 2. Stoga ćemo ovdje dati Edwardsovu jednadžbu samo za slučaj polja karakteristike različite od 2.

Propozicija 2.2. *Neka je K polje karakteristike različite od 2. Neka su $c, d \in K \setminus \{0\}$ i d nije kvadrat u K. Tada je krivulja*

$$C: \quad u^2 + v^2 = c^2(1 + du^2v^2)$$

biracionalno ekvivalentna eliptičkoj krivulji

$$E: \quad y^2 = (x - c^4d - 1)(x^2 - 4c^4d),$$

pri čemu su pripadne supstitucije dane s

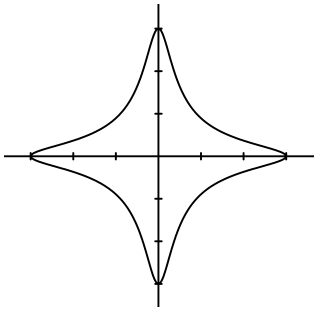
$$x = \frac{-2c(w-c)}{u^2}, \quad y = \frac{4c^2(w-c)+2c(c^4d+1)u^2}{u^3},$$

gdje je $w = (c^2du^2 - 1)v$.

Točka $(0, c)$ *je neutralni element za zbrajanje na krivulji* C. *Suprotni element od* (u, v) *je* $-(u, v) = (-u, v)$, *a zakon zbrajanja je dan sljedećom formulom*

$$(u_1, v_1) + (u_2, v_2) = \left(\frac{u_1v_2 + u_2v_1}{c(1 + du_1u_2v_1v_2)}, \frac{v_1v_2 - u_1u_2}{c(1 - du_1u_2v_1v_2)} \right),$$

za sve točke $(u_i, v_i) \in C(K)$.



Edwardsova krivulja $u^2 + v^2 = 9(1 - u^2v^2)$

Jednadžba krivulje C može se zapisati u obliku

$$u^2 - c^2 = (c^2du^2 - 1)v^2 = \frac{w^2}{c^2du^2 - 1},$$

odnosno

$$w^2 = c^2du^4 - (c^4d + 1)u^2 + c^2.$$

Ova se kvartika, s racionalnom točkom $(0, c)$, sada na gore opisani način može transformirati u Weierstrassovu jednadžbu.

Provjerimo da su nazivnici u formuli za zbrajanje različiti od 0. Pretpostavimo da je $du_1u_2v_1v_2 = -1$ (slučaj $du_1u_2v_1v_2 = 1$ je sličan). Tada je $u_1v_1 = -\frac{1}{du_2v_2}$ te uvrštavanjem u jednadžbu od C dobivamo

$$u_1^2 + v_1^2 = c^2 \left(1 + \frac{1}{du_2^2v_2^2} \right) = \frac{u_2^2 + v_2^2}{du_2^2v_2^2}.$$

Odavde je

$$(u_1 + v_1)^2 = \frac{1}{d} \left(\frac{u_2^2 + v_2^2 - 2u_2v_2}{u_2^2v_2^2} \right) = \frac{1}{d} \frac{(u_2 - v_2)^2}{(u_2v_2)^2}.$$

Budući da prema pretpostavci d nije kvadrat, odavde slijedi da je $u_1 + v_1 = u_2 - v_2 = 0$. Analogno se iz

$$(u_1 - v_1)^2 = \frac{1}{d} \frac{(u_2 + v_2)^2}{(u_2v_2)^2}$$

dobiva $u_1 - v_1 = u_2 + v_2 = 0$. Dobili smo da je $u_1 = v_1 = u_2 = v_2 = 0$, što je u kontradikciji s $du_1u_2v_1v_2 = -1$.

Vratimo se sada na Weierstrassovu jednadžbu

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

S pomoću njezinih koeficijenata a_1, a_2, a_3, a_4, a_6, definirali smo veličine b_2, b_4, b_6, b_8, c_4, c_6. S pomoću njih možemo definirati još dvije važne veličine:

- *diskriminantu* $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728}$,
- *j-invarijantu* $j = \frac{c_4^3}{\Delta}$.

Krivulja je nesingularna ako i samo ako je $\Delta \neq 0$. Ovako definirana diskriminanta je jednaka $1/16 \times \operatorname{Disc}(4x^3 + b_2x^2 + 2b_4x + b_6)$. Općenito se diskriminanta polinoma f stupnja n s vodećim koeficijentom a_n i korijenima $x_1, \ldots, x_n$ (iz algebarskog zatvorenja $\overline{K}$) može definirati kao

$$\operatorname{Disc}(f) = a_n^{2n-2} \prod_{i<j}^{n} (x_i - x_j)^2$$

i jednaka je 0 ako i samo ako f ima višestrukih korijena. Ako je eliptička krivulja dana jednadžbom $y^2 = x^3 + ax + b$, onda je $\Delta = -16(4a^3 + 27b^2)$. Za krivulje definirane nad $\mathbb{R}$, predznak diskriminante nam govori koliko komponenti ima graf krivulje: ako je $\Delta < 0$, onda imamo jednu komponentu, a ako je $\Delta > 0$, onda imamo dvije komponente.

Naziv j-invarijanta dolazi od toga što izomorfne krivulje imaju iste j-invarijante. Najopćenitiji oblik izomorfizma između dviju eliptičkih krivulja nad $\mathbb{Q}$ danih općom Weierstrassovom formom je

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t, \end{aligned} \tag{2.8}$$

gdje je $r, s, t \in \mathbb{Q}$ i $u \in \mathbb{Q}^*$. Efekt ovih supstitucija na koeficijente a_i je

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1, \end{aligned}$$

odakle se dobiva da vrijedi

$$u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta' = \Delta, \quad j' = j.$$

U slučaju kratkih Weierstrassovih formi jedine dopustive supstitucije su

$$x = u^2x', \quad y = u^3y', \quad u \in \mathbb{Q}^*.$$

Vrijedi i svojevrstan obrat ovog svojstva j-invarijanti. Naime, dvije eliptičke krivulje su izomorfne nad algebarskim zatvorenjem $\overline{\mathbb{Q}}$ ako i samo ako imaju istu j-invarijantu.

Ako promatramo krivulje nad algebarski zatvorenim poljem, onda nam j-invarijanta govori jesu li krivulje izomorfne. No ako polje nije algebarski zatvoreno, primjerice ako promatramo krivulje nad $\mathbb{Q}$, onda dvije krivulje mogu imati jednake j-invarijante, a da se ne mogu transformirati jedna u drugu pomoću racionalnih funkcija s koeficijentima iz $\mathbb{Q}$. Na primjer, krivulje $y^2 = x^3 - 4x$ i $y^2 = x^3 - 25x$ obje imaju $j = 1728$. Prva od njih ima konačno mnogo racionalnih točaka, dok ih druga ima beskonačno mnogo (točka $(-4, 6)$ je beskonačnog reda). Dakle, ove krivulje nisu izomorfne nad $\mathbb{Q}$, ali jesu nad $\mathbb{Q}(\sqrt{10})$ (supstitucije su $(x, y) \mapsto (u^2x, u^3y)$, $u = \frac{\sqrt{10}}{2}$).

Za $j \neq 0, 1728$, krivulja

$$y^2 = x^3 - \frac{3j}{j - 1728}x + \frac{2j}{j - 1728}$$

ima j-invarijantu upravo jednaku j. Krivulje oblika $y^2 = x^3 + b$ imaju j-invarijantu jednaku 0, dok krivulje oblika $y^2 = x^3 + ax$ imaju j invarijantu jednaku $1728 = 12^3$.

Neka je E eliptička krivulja definirana nad $\mathbb{Q}$. Promjenom varijabli, ako je potrebno, možemo pretpostaviti da je E dana jednadžbom

$$y^2 = x^3 + ax + b, \tag{2.9}$$

gdje su $a, b \in \mathbb{Z}$ (takvu jednadžbu nazivamo cjelobrojni model za E). Za prosti broj $p > 3$ možemo promatrati jednadžbu $y^2 = x^3 + ax + b \bmod p$. Ako je ovom jednadžbom definirana eliptička krivulja nad poljem $\mathbb{F}_p$, onda kažemo da E ima *dobru redukciju* modulo p.

Uočimo da za krivulju E postoji više izbora za $a, b \in \mathbb{Z}$ u prikazu (2.9). U definiciji dobre (loše) redukcije pretpostavljamo da su a, b izabrani tako da E ima "najbolja moguća" svojstva. Dakle, za svaki p tražimo a, b sa svojstvom da kubni polinom $P(x) = x^3 + ax + b$ ima što više različitih korijena modulo p, te da je diskriminanta $\Delta = -16(4a^3+27b^2)$ djeljiva sa što manjom potencijom broja p. Kažemo da je takva jednadžba minimalna za p. Pokazuje se da je moguće izabrati takve a, b koji imaju ovo svojstvo za sve p. Pripadna jednadžba se naziva (globalna) *minimalna Weierstrassova jednadžba* od E. Da bi se analogni pojmovi definirali za $p = 2$ i $p = 3$, trebamo gledati opću (dugu) Weierstrassovu formu.

Kod prostih brojeva s lošom redukcijom kubni polinom $P(x) = x^3+ax+b$ ima višestruki korijen modulo p. Ako polinom P ima trostruki korijen, kažemo da E ima *aditivnu redukciju*, a ako polinom P ima dvostruki korijen,

onda kažemo da E ima *multiplikativnu redukciju*. Dodatno se razlikuje rascjepiva i nerascjepiva multiplikativna redukcija. *Rascjepiva* je ako su koeficijenti smjera tangenata u singularnoj točki iz $\mathbb{F}_p$, a *nerascjepiva* inače. Ovo posljednje se može odrediti tako da se jednadžba krivulje napiše u obliku $y^2 = x^2(x + c)$. Jednadžbe tangenti u singularnoj točki $(0, 0)$ su $y = \pm\sqrt{c}x$, pa vidimo da ćemo imati rascjepivu multiplikativnu redukciju ako i samo ako je c kvadrat u $\mathbb{F}_p$ (tj. ako i samo ako je c kvadratni ostatak modulo p).

Primjer 2.2. Promotrimo eliptičku krivulju nad $\mathbb{Q}$ zadanu jednadžbom

$$y^2 = x^3 - 1037232x + 965662992.$$

Njezina diskriminanta je $\Delta = -2^{12}3^{12}7^{12}11$. Zaključujemo da E ima dobru redukciju svugdje, osim možda u $p = 2, 3, 7, 11$. Također, odmah vidimo da se loša redukcija u $p = 11$ neće moći ukloniti (jer se diskriminante izomorfnih krivulja razlikuju za faktor oblika u^{12}), dok je za $p = 2, 3, 7$ to možda moguće. Supstitucijama

$$x = 7^2x_1, \quad y = 7^3y_1$$

dobivamo jednadžbu

$$y_1^2 = x_1^3 - 432x_1 + 8208,$$

čija je diskriminanta $-2^{12}3^{12}11$, pa E ima dobru redukciju u 7.

Kod razmatranja redukcije u $p = 2$ i $p = 3$ morat ćemo odustati od kratke Weierstrassove forme. Za $p = 3$ koristimo se supstitucijama oblika $x_1 = 3^2x_2 + r$, $y_1 = 3^3y_2$ te iz uvjeta da su koeficijenti Weierstrassove jednadžbe cjelobrojni dobivamo uvjet $r \equiv -3 \pmod 9$. Uzmimo $r = -12$, pa supstitucijama

$$x_1 = 9x_2 - 12, \quad y_1 = 27y_2$$

dobivamo jednadžbu

$$y_2^2 = x_2^3 - 4x_2^2 + 16, \tag{2.10}$$

čija je diskriminanta $-2^{12}11$, pa E ima dobru redukciju i u $p = 3$.

Za $p = 2$, koristimo se supstitucijama oblika $x_2 = 2^2x_3$, $y_2 = 2^3y_3+t$, gdje iz uvjeta da su koeficijenti Weierstrassove jednadžbe cjelobrojni dobivamo da je $t \equiv 4 \pmod 8$. Uzmimo $t = 4$, pa supstitucijom

$$x_2 = 4x_3, \quad y_2 = 8y_3 + 4$$

dobivamo jednadžbu

$$y_3^2 + y_3 = x_3^3 - x_3^2. \tag{2.11}$$

Ova krivulja je nesingularna za $p = 2$ jer joj je diskriminanta jednaka -11 (drugi način da se to vidi je iz parcijalne derivacije po y_3, tj. $2y_3 + 1 = 1$ u $\mathbb{F}_2$, koja je uvijek različita od nule). Stoga E ima dobru redukciju u $p = 2$.

Zaključujemo da E ima dobru redukciju u svim prostim brojevima, osim u $p = 11$, gdje ima lošu redukciju. Jednadžba (2.11) je minimalna Weierstrassova jednadžba od E.

Promotrimo još malo situaciju za $p = 11$, i to preko jednadžbe (2.10). U $\mathbb{F}_{11}$ imamo

$$x_2^3 - 4x_2^2 + 16 = (x_2 + 1)^2(x_2 + 5),$$

pa vidimo da E ima multiplikativnu redukciju u $p = 11$. Tangente u singularnoj točki $(x_2, y_2) = (-1, 0)$ imaju koeficijente smjera $\pm 2 \in \mathbb{F}_{11}$ (jer jednadžba $\alpha^2 = 4$ ima rješenja u $\mathbb{F}_{11}$), pa E ima rascjepivu multiplikativnu redukciju u $p = 11$. ♢

Globalna minimalna jednadžba od E ima svojstvo da joj je $|\Delta|$ minimalno među svim cjelobrojnim modelima od E. U izomorfizmu između dvije minimalne jednadžbe mora biti $u = \pm 1$, dok su $r, s, t \in \mathbb{Z}$. Izborom parametara r, s, t uvijek se može postići da je $a_1, a_3 \in \{0, 1\}$, $a_2 \in \{-1, 0, 1\}$. Jednadžba koja zadovoljava ove uvjete zove se *reducirana*. Nije teško vidjeti da je jedina transformacija (osim identitete) koja jednu reduciranu jednadžbu preslikava u drugu reduciranu jednadžbu transformacija $(r, s, t, u) = (0, -a_1, -a_3, -1)$. To je transformacija koja točki (x, y) pridružuje njezin inverz $-(x, y) = (x, -y - a_1x - a_3)$ i ne mijenja jednadžbu.

Zaključujemo da svaka eliptička krivulja ima jedinstvenu reduciranu minimalnu Weierstrassovu jednadžbu. Ova činjenica omogućava vrlo lako razlikovanje krivulja. Tako se u različitim tablicama s podatcima o konkretnim eliptičkim krivuljama najčešće nalaze samo podatci za reducirane minimalne jednadžbe.

Neka je eliptička krivulja dana jednadžbom s cjelobrojnim koeficijentima. Ako je $\nu_p(\Delta) < 12$ ili $\nu_p(c_4) < 4$ ili $\nu_p(c_6) < 6$, onda je ta jednadžba minimalna za prosti broj p. Ako je $p \neq 2, 3$, onda vrijedi i obrat: ako je $\nu_p(\Delta) \geq 12$ i $\nu_p(c_4) \geq 4$, onda jednadžba nije minimalna za p. Situacija s $p = 2$ i $p = 3$ je kompliciranija. Tu se minimalna jednadžba za p može izračunati Tateovim algoritmom. To je algoritam koji računa minimalne jednadžbe za svaki p, globalnu minimalnu jednadžbu, konduktor i još neke podatke.

Za krivulju definiranu nad $\mathbb{Q}$ se definira veličina povezana s diskriminantom koja se naziva *konduktor*

$$N = \prod_p p^{f_p}.$$

Ako je $p \neq 2, 3$, onda se f_p može lako odrediti iz minimalnog Weierstrassovog modela za E:

- $f_p = 0$ ako $p \nmid \Delta$;
- $f_p = 1$ ako $p \mid \Delta$ i $p \nmid c_4$;

- $f_p \geq 2$ ako $p \mid \Delta$ i $p \mid c_4$; ako je $p \neq 2, 3$, onda je $f_p = 2$.

U različitim tablicama i bazama eliptičkih krivulja nad $\mathbb{Q}$ uglavnom se navode samo minimalne Weierstrassove jednadžbe krivulje, dok su krivulje obično sortirane prema svom konduktoru. Najmanji N za kojeg postoje eliptičke krivulje nad $\mathbb{Q}$ s konduktorom jednakim N je $N = 11$. Sljedeće krivulje imaju konduktor 11:

$$\begin{aligned} &y^2 + y = x^3 - x^2, \\ &y^2 + y = x^3 - x^2 - 10x - 20, \\ &y^2 + y = x^3 - x^2 - 7820x - 263580. \end{aligned}$$

Diskriminante su im redom: -11, -11^5, -11. Prve dvije imaju točke reda 5, dok treća nema netrivijalnih racionalnih točaka.

Iduće mogućnosti za konduktor su $N = 14, 15, 17, 19, 20, 21, 24, \ldots$ Sve krivulje s konduktorom manjim od 37 imaju samo konačno mnogo racionalnih točaka (imaju rang jednak 0). Jedna od krivulja s konduktorom 37,

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

ima točku beskonačnog reda $(0, 0)$ (i rang jednak 1).

2.3 Eliptičke krivulje u programskom paketu PARI/GP

U programskom paketu PARI/GP (`https://pari.math.u-bordeaux.fr/`) implementiran je veći broj važnijih funkcija vezanih uz eliptičke krivulje. Sada ćemo navesti samo neke, dok ćemo ostale spomenuti onda kada se prirodno pojave u gradivu koje ćemo obrađivati (popis svih funkcija vezanih uz eliptičke krivulje može se dobiti sa `?12`).

Pretpostavljamo da je krivulja dana u Weierstrassovoj formi

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

te ju u PARI-ju reprezentiramo kao pet-komponentni vektor

$$e = [a_1, a_2, a_3, a_4, a_6].$$

Točke na E su reprezentirane kao dvo-komponentni vektori $[x, y]$, osim točke u beskonačnosti koja je reprezentirana kao jedno-komponentni vektor $[0]$.

Prije primjene bilo koje od ostalih funkcija, eliptičku krivulje "inicijaliziramo" pomoću funkcije `ellinit`.

$E =$ `ellinit`(e): računa sljedeće podatke za eliptičku krivulju nad $\mathbb{Q}$:

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6,\ b_2,\ b_4,\ b_6,\ b_8,\ c_4,\ c_6,\ \Delta,\ j.$$

Npr. diskriminanta od E se može dobiti kao $E[12]$ ili $E.\texttt{disc}$, dok je j-invarijanta $E[13]$ ili $E.\texttt{j}$. Koeficijenti c_4 i c_6 se dobivaju kao $E.\texttt{c4}$ i $E.\texttt{c6}$.

Dodatni podatci ovise o polju nad kojim je definirana krivulja. Tako su za krivulje nad poljem $\mathbb{C}$ primjerice dostupni i ovi podatci:

- $E.\texttt{omega}[1]$ je realni, a $E.\texttt{omega}[2]$ je kompleksni period od E. Drugim riječima, $\omega_1 = E.\texttt{omega}[1]$ i $\omega_2 = E.\texttt{omega}[2]$ čine bazu kompleksne rešetke od E.
- $E.\texttt{area}$ je površina fundamentalnog paralelograma od E.

Navedimo sada neke od funkcija vezanih uz eliptičke krivulje koje su dostupne u PARI-ju. Kasnije ćemo spomenuti još neke, primjerice one za računanje torzijske grupe i ranga.

$\texttt{elladd}(E, P1, P2)$: zbroj točaka $P1$ i $P2$ na eliptičkoj krivulji E.

$\texttt{ellsub}(E, P1, P2)$: razlika $P1 - P2$ točaka na eliptičkoj krivulji E.

$\texttt{ellmul}(E, P, n)$: višekratnik nP točke P na eliptičkoj krivulji E.

$\texttt{ellordinate}(E, x)$: daje vektor koji sadrži y-koordinate točka na eliptičkoj krivulji E čija je x-koordinata jednaka x.

$\texttt{ellisoncurve}(E, P)$: daje 1 (tj. "istina") ako je P točka na E, a 0 (tj. "laž") inače.

$\texttt{ellchangecurve}(E, v)$: daje eliptičku krivulju koja se iz E dobije pomoću supstitucija koje su određene vektorom $v = [u, r, s, t]$, tj. veza starih koordinata x, y i novih x', y' je dana sa $x = u^2x' + r$, $y = u^3y' + su^2x' + t$.

$\texttt{ellminimalmodel}(E, \{\&v\})$: daje reducirani minimalni model za eliptičku krivulju nad $\mathbb{Q}$. Opcionalnoj varijabli v pridružuje se vektor $[u, r, s, t]$ koji daje odgovarajuću promjenu varijabli, tako da je krivulja koja se dobije pomoću ove funkcije upravo $\texttt{ellchangecurve}(E, v)$.

$\texttt{ellglobalred}(E)$: računa konduktor, globalni minimalni model od E i globalni Tamagawin broj c. Rezultat ove funkcije je pet-komponentni vektor $[N, v, c, faN, L]$, gdje je N konduktor, v daje promjenu varijabli pomoću koje se iz E dobiva minimalni integralni model ($\texttt{ellminimalmodel}$), dok je c produkt lokalnih Tamagawinih brojeva c_p, što je veličina koja se pojavljuje u eksplicitnoj verziji Birch i Swinnerton-Dyerove slutnje, faN je faktorizacija od N, dok L predstavlja podatke iz lokalnih redukcija po prostim faktorima od N ($L[i]$ je $\texttt{elllocalred}(E, faN[i, 1])$).

$\texttt{ellwp}(E, \{z = x\})$: računa vrijednost u z Weierstrassove $\wp$ funkcije pridružne eliptičkoj krivulji E (zadanoj sa $\texttt{ellinit}$ ili kao rešetka $[\omega_1, \omega_2]$).

$\texttt{ellpointtoz}(E, P)$: računa kompleksan broj t (modulo rešetka određena sa E) koji odgovara točki P (njezin parametar), tj. $\wp(t) = P[1]$, $\wp'(t) = P[2]$.

`ellztopoint`(E, z): računa koordinate $[x, y]$ točke na eliptičkoj krivulji E koja odgovara kompleksnom broju z. Dakle, ovo je inverzna funkcija od `ellpointtoz`. Točka $[x, y]$ prikazuje vrijednost Weierstrassove $\wp$ funkcije i njezine derivacije u točki z. Ako je z točka rešetke koja definira E nad $\mathbb{C}$, onda je rezultat ove funkcije točka u beskonačnosti $[0]$.

Primjer 2.3. *Ilustrirat ćemo korištenje nekih funkcija iz PARI-ja na primjeru eliptičke krivulje iz Primjera 2.11.*

```
? E=ellinit([0,0,0,-1037232,965662992])
%1 = [0, 0, 0, -1037232, 965662992, 0, -2074464, 3862651968,
-1075850221824, 49787136, -834332825088, -331424164353036496896,
-4096/11]
? factor(E.disc)
%2 = [-1, 1; 2, 12; 3, 12; 7, 12; 11, 1]
? F=ellminimalmodel(E, &v);
? [F.a1,F.a2,F.a3,F.a4,F.a6]
%3 = [0, -1, 1, 0, 0]
? v
%4 = [42, -588, 0, 37044]
? ellordinate(F,0)
%5 = [0, -1]
? P = [0, 0]; for(n=2,5,print(ellmul(F,P,n)))
[1, -1] [1, 0] [0, -1] [0]                                    ♢
```

Primjer 2.4. *U ovom primjeru ćemo uzeti krivulju*

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

za koju smo rekli da je krivulja s najmanjim konduktorom koja ima beskonačno mnogo cjelobrojnih točaka.

```
? E=ellinit([0,0,1,-1,0])
%1 = [0, 0, 1, -1, 0, 0, -2, 1, -1, 48, -216, 37, 110592/37]
? P = [0,0]
%2 = [0,0]
? ellisoncurve(E,P)
%3 = 1
? for(n=2,8,print(ellmul(E,P,n)))
[1, 0] [-1, -1] [2, -3] [1/4, -5/8] [6, 14] [-5/9, 8/27]
[21/25, -69/125]
? t1 = ellpointtoz(E,P)
%4 = 0.92959271528539567440519934445 + 1.22569469099339503042711241 6*I
? t2 = ellpointtoz(E,[2, -3])
%5 = 0.72491221490962306778878739 84
? t2 - 4*t1
```

```
%6 = -2.9934586462319596298320099800 - 4.9027787639735801217084496640*I
? E.omega[1]
%7 = 2.9934586462319596298320099800
? 2*E.omega[2]
-4.9027787639735801217084496640*I
? G=ellglobalred(E)
%8 = [37, [1, 0, 0, 0], 1, Mat([37, 1]), [[1, 5, 0, 1]]]
? cond = G[1]
%9 = 37
```

♢

Primjer 2.5. *U PARI-ju je implementiran i algoritam za prevođenje opće kubne jednadžbe u (dugi) Weierstrassov oblik, i to preko funkcije* `ellfromeqn`*. Ilustrirajmo njezinu primjenu na primjeru krivulje iz Primjera 2.1. Da bi se uvjerili da je eliptička krivulja koju dobivamo primjenom ove funkcije ekvivalentna eliptičkoj krivulji dobivenoj u Primjeru 2.1, usporedit ćemo njihove reducirane minimalne jednadžbe. Funkcija* `ellfromeqn` *se može primijeniti i na ostale oblike krivulja genusa* 1*, kao što su Edwardsove krivulje i hipereliptičke krivulje stupnja* 4*.*

```
? ellfromeqn(x^3+y^3-1)
%1 = [0, 0, -9, 0, -27]
? e1=ellinit([0, 0, -9, 0, -27]);
? e2=ellinit([0, 0, 0, 0, -432]);
? f1=ellminimalmodel(e1);
? [f1.a1,f1.a2,f1.a3,f1.a4,f1.a6]
%2 = [0, 0, 1, 0, -7]
? f2=ellminimalmodel(e2);
? [f2.a1,f2.a2,f2.a3,f2.a4,f2.a6]
%3 = [0, 0, 1, 0, -7]
? ellfromeqn(u^2+v^2-9*(1-u^2*v^2))
%4 = [0, 80, 0, 324, 25920]
? ellfromeqn(y^2-(x+1)*(3*x+1)*(8*x+1)*(120*x+1))
%5 = [0, 1475, 0, 546048, 51031296]
```

♢

2.4 Torzijska grupa

Najvažnija činjenica o eliptičkim krivuljama nad $\mathbb{Q}$ jest Mordell-Weilov teorem.

Teorem 2.1 (Mordell-Weil)**.** *Grupa $E(\mathbb{Q})$ je konačno generirana Abelova grupa.*

Ovaj teorem je 1922. godine dokazao britanski matematičar Louis Joel Mordell (1888. – 1972.), dok ga je 1928. godine francuski matematičar

André Weil (1906. – 1998.) poopćio na Abelove mnogostrukosti nad poljima algebarskih brojeva.

Mordell-Weilov teorem nam, drugim riječima, kaže da postoji konačan skup racionalnih točaka $\{P_1, \ldots, P_k\}$ na E iz kojih se sve ostale racionalne točke na E mogu dobiti povlačeći sekante i tangente. Kako je svaka konačno generirana Abelova grupa izomorfna produktu cikličkih grupa (preciznije, produktu oblika $\mathbb{Z}^n \times \mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_m}$ tako da $k_1 \mid k_2 \mid \cdots \mid k_m$, gdje smo sa $\mathbb{Z}_k$ označili kvocijentni prsten $\mathbb{Z}/k\mathbb{Z}$), dobivamo sljedeću neposrednu posljedicu Mordell-Weilova teorema.

Korolar 2.1.

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

Podgrupa $E(\mathbb{Q})_{\text{tors}}$ od $E(\mathbb{Q})$ koja se sastoji od svih točaka konačnog reda naziva se *torzijska grupa* od E, a nenegativni cijeli broj r se naziva *rang* od E i označava se s $\text{rank}(E)$ (preciznije $\text{rank}(E(\mathbb{Q}))$). Korolar nam kaže da postoji r racionalnih točaka $P_1, \ldots, P_r$ beskonačnog reda na krivulji E sa svojstvom da se svaka racionalna točka P na E može prikazati u obliku

$$P = T + m_1 P_1 + \cdots + m_r P_r,$$

gdje je T neka točka konačnog reda, a $m_1, \ldots, m_r$ cijeli brojevi. Ovdje $m_1 P_1$ označava sumu $P_1 + \cdots + P_1$ od m_1 pribrojnika, koja se često označava i s $[m_1]P_1$.

Prirodno se postavlja pitanje koje sve vrijednosti mogu poprimiti $E(\mathbb{Q})_{\text{tors}}$ i $\text{rank}(E)$. Nadalje, pitanje je kako ih izračunati za konkretnu krivulju E. Pokazuje se da je puno lakše dati odgovore na ova pitanja za torzijsku grupu nego za rang.

Promotrimo na trenutak točke konačnog reda nad $\mathbb{C}$ i $\mathbb{R}$. Rekli smo da se eliptička krivulja nad $\mathbb{C}$ može poistovjetiti s kvocijentnom grupom $\mathbb{C}/L$, gdje je $L = \{m_1\omega_1 + m_2\omega_2 : m_1, m_2 \in \mathbb{Z}\}$. Stoga je $nP = \mathcal{O}$ ako i samo ako je parametar od P (z iz fundamentalnog paralelograma takav da je $\wp(z) = x(P)$) oblika $\frac{m_1}{n}\omega_1 + \frac{m_2}{n}\omega_2$, $0 \leq m_1, m_2 < n$. Dakle, rješenja jednadžbe $nP = \mathcal{O}$ čine grupu izomorfnu sa $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

U slučaju krivulje s realnim koeficijentima, rešetka L ima bazu u kojoj je jedan od perioda, recimo ω_1, realan, a u slučaju kada je $\Delta > 0$ (tj. graf od E ima dvije komponente) je drugi, ω_2, čisto imaginaran (dakle, tada je fundamentalni paralelogram u stvari pravokutnik). Točkama iz $E(\mathbb{R})$ odgovaraju parametri $t \in [0, \omega_1\rangle$ (donja osnovica paralelograma) te u slučaju kad graf od E ima dvije komponente još i $t - \frac{1}{2}\omega_2 \in [0, \omega_1\rangle$ (srednjica pravokutnika paralelna s osnovicom). Dakle, grupa $E(\mathbb{R})$ je izomorfna ili grupi kružnice S^1 (kada je $\Delta < 0$) ili $\mathbb{Z}/2\mathbb{Z} \times S^1$ (kada je $\Delta > 0$). Rješenja jednadžbe $nP = \mathcal{O}$ čine grupu izomorfnu sa $\mathbb{Z}/n\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Vratimo se sada na krivulje nad $\mathbb{Q}$. Iz onoga što smo do sada rekli, slijedi da bi grupa $E(\mathbb{Q})_{\text{tors}}$ trebala biti konačna podgrupa od S^1 ili $\mathbb{Z}/2\mathbb{Z} \times S^1$.

Poznato je da su sve konačne podgrupe od S^1 cikličke. Stoga je $E(\mathbb{Q})_{\text{tors}}$ izomorfna jednoj od grupa oblika $\mathbb{Z}/k\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ (uočimo da ako je k neparan, onda je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}/2k\mathbb{Z}$).

Mazur je 1978. godine dokazao da postoji točno 15 mogućih torzijskih grupa za eliptičke krivulje nad $\mathbb{Q}$. To su grupe:

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

Točke reda 2 na krivulji $y^2 = x^3 + ax^2 + bx + c$ su upravo točke s y-koordinatom jednakom 0. Možemo imati 0, 1 ili 3 takve točke, što ovisi o broju racionalnih nultočaka polinoma $x^3 + ax^2 + bx + c$. Te točke, zajedno s točkom $\mathcal{O}$, čine podgrupu od $E(\mathbb{Q})_{\text{tors}}$ koja je ili trivijalna ili izomorfna $\mathbb{Z}/2\mathbb{Z}$ ili izomorfna $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ostale točke konačnog reda možemo naći s pomoću Lutz-Nagellova teorema. Ideja je naći model krivulje u kojem će sve torzijske točke biti cjelobrojne. To je upravo model s jednadžbom $y^2 = x^3 + ax^2 + bx + c$ koji dobijemo iz opće Weierstrassove jednadžbe (2.1) eliminirajući članove uz xy i y (supstitucijama (2.8) s $u = 2$ ako je potrebno). Ako je $a_1 = a_3 = 0$, onda već Weierstrassova jednadžba ima željeni oblik; inače stavimo $a = b_2$, $b = 8b_4$, $c = 16b_6$. Zatim se za torzijsku točku $P = (x, y)$ iskoristi činjenica da i P i $2P$ imaju cjelobrojne koordinate, da bi se dobila ocjena za y. Često se Lutz-Nagellov teorem navodi za jednadžbu oblika $y^2 = x^3 + ax + b$, što nije gubitak općenitosti jer se član uz x^2 može eliminirati nadopunjavanjem na potpun kub, međutim, to eliminiranje uključuje dodatno skaliranje koordinata te za rezultat ima (nepotrebno) veću ocjenu za y. Napomenimo da kod krivulje s općom Weierstrassovom jednadžbom za točku konačnog reda $P(x, y)$ vrijedi da su $4x$ i $8y$ cijeli brojevi.

Teorem 2.2 (Lutz-Nagell)**.** *Neka je E eliptička krivulja zadana jednadžbom*

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{2.12}$$

gdje su $a, b, c \in \mathbb{Z}$. Ako je $P = (x_1, y_1)$ točka konačnog reda u $E(\mathbb{Q})$, tada su $x_1, y_1 \in \mathbb{Z}$.

Teorem je dobio ime po francuskoj matematičarki Élisabeth Lutz (1914 – 2008) i norveškom matematičaru Trygve Nagellu (1895 – 1988) koji su ga neovisno dokazali 30-tih godina 20. stoljeća.

Propozicija 2.3. *Neka je E eliptička krivulja zadana jednadžbom (2.12), gdje su $a, b, c \in \mathbb{Z}$. Ako je $P = (x_1, y_1)$ točka konačnog reda u $E(\mathbb{Q})$, tada je ili $y_1 = 0$ ili $y_1^2 \mid \Delta_0$, gdje je $\Delta_0 = -\Delta/16 = 27c^2 + 4a^3c + 4b^3 - a^2b^2 - 18abc$.*

Dokaz: Ako je $2P = \mathcal{O}$, onda je $P = -P = (x_1, -y_1)$, pa je $y_1 = 0$. U protivnom je $2P = (x_2, y_2)$, gdje je po Lutz-Nagellovu teoremu $x_2, y_2 \in \mathbb{Z}$.

Iz formule za zbrajanje na E imamo $2x_1 + x_2 = \lambda^2 - a$, gdje je $\lambda = \frac{f'(x_1)}{2y_1}$ koeficijent smjera tangente na E u točki P. Vidimo da je $\lambda \in \mathbb{Z}$, što povlači da $y_1 \mid f'(x_1)$. Sada iz formule

$$\Delta_0 = (-27f(x) + 54c + 4a^3 - 18ab)f(x) + (f'(x) + 3b - a^2)f'(x)^2 \quad (2.13)$$

i $y_1^2 = f(x_1)$ slijedi da $y_1^2 \mid \Delta_0$. Formula (2.13) se dobije primjenom (proširenog) Euklidova algoritma na polinome $f(x)$ i $(f'(x))^2$. □

Lutz-Nagellov teorem nam daje konačnu listu kandidata za torzijske točke. Točnije, daje nam kandidate za y-koordinate točaka. No za dani y nije teško naći cjelobrojna rješenja jednadžbe $x^3 + ax^2 + bx + c - y^2 = 0$ (ili ispitivanjem faktora od $y^2 - c$ ili preko Cardanovih formula za rješenja kubne jednadžbe). Ako je P torzijska točka, onda za svaki prirodni broj n točka nP mora biti ili $\mathcal{O}$ ili jedna od točaka s liste. Budući da je lista konačna, ili ćemo dobiti da je $nP = mP$ za neke $m \neq n$, u kojem je slučaju $(n-m)P = \mathcal{O}$ i točka P torzijska, ili će neki višekratnik nP biti izvan liste pa P nije torzijska. Alternativno, možemo se koristiti i Mazurovim teoremom, prema kojem je red svake torzijske točke ≤ 12. Stoga, ako je $nP \neq \mathcal{O}$ za sve $n \leq 12$, onda P nije torzijska.

Pretpostavimo da smo našli sve torzijske točke te da nakon toga želimo odrediti strukturu torzijske grupe. Prema Mazurovu teoremu jedini slučajevi kada red grupe ne određuje potpuno strukturu grupe su slučajevi $|E(\mathbb{Q})_{\text{tors}}| = 4$, 8 i 12, kada imamo dvije mogućnosti: $\mathbb{Z}/4k\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$, $k = 1, 2, 3$. Ako imamo jednu točku reda 2, onda je $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/4k\mathbb{Z}$, a ako imamo tri točke reda dva, onda je $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$.

Primjer 2.6. *Odredimo torzijsku grupu eliptičke krivulje*

$$E: \quad y^2 = (-x + 4)(3x + 4)(4x + 4)$$

inducirane $D(4)$-trojkom $\{-1, 3, 4\}$.

Rješenje: Prebacimo najprije krivulju u oblik iz Lutz-Nagellovog teorema (pomnožimo jednadžbu s $(-3)^2$ te zamijenimo x sa $x/(-3)$):

$$y^2 = x^3 + 5x^2 - 72x + 144 = (x - 3)(x - 4)(x + 12).$$

Ovdje je $\Delta_0 = -57600$. Ako je $y = 0$, onda je $x = 3$, 4 ili -12, pa imamo tri točke $(3, 0)$, $(4, 0)$ i $(-12, 0)$ reda 2. Ako je $y \neq 0$, onda $y^2 \mid 576000$, tj. $y \mid 240$. Testiranjem svih mogućnosti, npr. pomoću ovog kôda u PARI-ju:

```
fordiv(240,y,f=factor(x^3+5*x^2-72*x+144-y^2);\
if(length(f~)>1,print(y," ",f)))
```

nalazimo sljedeće točke s cjelobrojnim koordinatama: $P_1 = (0, 12)$, $P_2 = (8, 20)$, $-P_1 = (0, -12)$, $-P_2 = (8, -20)$ (koje odgovaraju $y = 12$ i $y = 20$). Računajući višekratnike, dobivamo $2P_1 = (4, 0)$, $2P_2 = (4, 0)$. Dakle, točke $\pm P_1$ i $\pm P_2$ su točke

reda 4. Budući da imamo ukupno 8 točaka konačnog reda (zajedno s točkom u beskonačnosti), od kojih su 3 točke reda 2, zaključujemo da je

$$E(\mathbb{Q})_{\text{tors}} = \Big\{\mathcal{O}, (-1,0), (-\frac{4}{3},0), (4,0), (0,8), (0,-8), (-\frac{8}{3},\frac{40}{3}), (-\frac{8}{3},-\frac{40}{3})\Big\}$$
$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Spomenumo da je $\{-1,3,4\}$ jedina $D(4)$-trojka koja inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Sve ostale $D(4)$-trojke induciraju krivulje s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (Dujella & Mikić, 2014). Slutnja je da se ni grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ne može ovdje pojaviti. ♢

Problem s primjenom Lutz-Nagellova teorema može se javiti ako je teško faktorizirati diskriminantu Δ ili ako ona ima jako puno kvadratnih faktora.

Tada nam može pomoći sljedeća činjenica.

Propozicija 2.4. *Neka je E eliptička krivulja zadana jednadžbom*

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

gdje su $a, b, c \in \mathbb{Z}$. Neka je p neparni prosti broj takav da $p \nmid \Delta_0$ te neka je

$$\rho_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$$

redukcija modulo p. Ako je točka $P \in E(\mathbb{Q})$ konačnog reda i $\rho_p(P) = \mathcal{O}$, onda je $P = \mathcal{O}$.

Dokaz: Prema Lutz-Nagellovu teoremu sve torzijske točke (osim $\mathcal{O}$) imaju cjelobrojne koordinate, pa se kod redukcije modulo p ne reduciraju u $\mathcal{O}$. □

Prema Propoziciji 2.4, jezgra (skup svih elemenata domene koji se preslikavaju u neutralni element kodomene) restrikcije preslikavanja ρ_p na $E(\mathbb{Q})_{\text{tors}}$ je trivijalna. Slika te restrikcije je podgrupa od $E(\mathbb{F}_p)$, pa budući da red podgrupe dijeli red grupe, zaključujemo da $|E(\mathbb{Q})_{\text{tors}}|$ dijeli $|E(\mathbb{F}_p)|$. Ako uzmemo nekoliko vrijednosti od p, tada najveći zajednički djelitelj g pripadnih vrijednosti od $|E(\mathbb{F}_p)|$ mora biti višekratnik od $|E(\mathbb{Q})_{\text{tors}}|$.

Računanje reda od $E(\mathbb{F}_p)$ za velike p-ove nije jednostavan problem. No u primjenama za računanje torzijske grupe p-ovi su u pravilu vrlo mali (biramo najmanje neparne p-ove koji ne dijele diskriminantu), tako da je tu za računanje $|E(\mathbb{F}_p)|$ sasvim zadovoljavajuća sljedeća formula s pomoću Legendreova simbola

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \Big(\frac{x^3 + ax^2 + bx + c}{p}\Big).$$

U PARI-ju se $|E(\mathbb{F}_p)|$ može dobiti kao $p + 1 -$ `ellap`(E, p).

Primjer 2.7. *Odredimo torzijsku grupu eliptičke krivulje*

$$E : \ y^2 = (x+1)(3x+1)(8x+1)$$

inducirane Diofantovom trojkom $\{1, 3, 8\}$.

Rješenje: Minimalna Weierstrassova jednadžba od E je

$$y^2 = x^3 - x^2 - 120x + 432.$$

Ovdje je $\Delta_0 = -2822400 = -2^8 3^2 5^2 7^2$, pa bismo, koristeći se Lutz-Nagellovim teoremom, trebali testirati sve djelitelje $y \mid 1680$. Umjesto toga, možemo provjeriti da je $|E(\mathbb{F}_{11})| = 12$ i $|E(\mathbb{F}_{13})| = 20$, odakle, budući da je $\mathrm{nzd}(12, 20) = 4$ te znamo da krivulja ima tri točke reda 2 i točku u beskonačnosti, izravno slijedi da je $E(\mathbb{Q})_{\text{tors}} = \left\{\mathcal{O}, (-1, 0), (-\frac{1}{3}, 0), (-\frac{1}{8}, 0)\right\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ♢

U programskom paketu PARI torzijska grupa eliptičke krivulje nad $\mathbb{Q}$ može se izračunati preko funkcije `elltors`. Rezultat je 3-komponentni vektor $[t, v_1, v_2]$, gdje je t red torzijske grupe, v_1 daje strukturu torzijske grupe kao produkta cikličkih grupa, dok v_2 daje generatore tih cikličkih grupa.

Već smo spomenuli da je 1978. godine Mazur dokazao sljedeći teorem.

Teorem 2.3. *Postoji točno 15 mogućih torzijskih grupa za eliptičke krivulje nad $\mathbb{Q}$. To su grupe:*

$$\begin{aligned} &\mathbb{Z}/k\mathbb{Z}, \quad \textit{za } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, \quad \textit{za } k = 1, 2, 3, 4. \end{aligned}$$

Težina ovog rezultata leži u dokazivanju da se grupe koje nisu navedene u teoremu ne mogu pojaviti kao torzijske grupe eliptičke krivulje nad $\mathbb{Q}$.

S druge strane, nije teško pokazati da se za svaku od 15 grupa navedenih u Mazurovu teoremu može konstruirati beskonačno mnogo eliptičkih krivulja s tom torzijskom (pod)grupom. Mi ćemo to detaljno napraviti za grupe oblika $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ jer su to grupe koje se javljaju kod eliptičkih krivulja induciranih racionalnim Diofantovim trojkama (i četvorkama).

Ipak recimo nešto kratko i o torzijskim grupama oblika $\mathbb{Z}/k\mathbb{Z}$. Pokazuje se da je za tu svrhu prikladno promatrati krivulje u dugoj Weierstrassovoj formi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.14}$$

Stoga navedimo formule za zbrajanje točaka na krivulji danoj s (2.14): ako je $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, onda je $P_1 + P_2 = (x_3, y_3)$, gdje je

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y_3 &= -(\lambda + a_1)x_3 - \mu - a_3, \end{aligned}$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{ako je } P_2 = P_1, \end{cases}$$

$$\mu = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & \text{ako je } P_2 = P_1. \end{cases}$$

Nadalje, $-P_1 = (x_1, -y_1 - a_1x_1 - a_3)$.

Neka je P točka iz $E(\mathbb{Q})$ reda k. Bez smanjenja općenitosti možemo pretpostaviti da je $P = (0, 0)$ (supstitucijom, tj. translacijom, $(x, y) \mapsto (x - x_P, y - y_P)$). Tada je u jednadžbi (2.14) $a_6 = 0$, a zbog nesingularnosti je jedan od brojeva a_3 i a_4

različit od nule. Ako je $k \geq 4$, onda možemo pretpostaviti da su i a_2 i a_3 različiti od nule. Tada se jednadžba krivulja može transformirati u u *Tateovu normalnu formu*

$$y^2 + (1-c)xy - by = x^3 - bx^2, \tag{2.15}$$

gdje su b i c racionalni brojevi takvi da je krivulja nesingularna. U ovoj jednadžbi, prvih nekoliko višekratnika točke P ima vrlo jednostavne koordinate. Npr.

$$-P = (0,b),\ \ 2P = (b,bc),\ \ -2P = (b,0),\ \ 3P = (c,b-c),\ \ -3P = (c,c^2),$$

$$4P = \left(\frac{b(b-c)}{c^2}, \frac{-b^2(b-c-c^2)}{c^3}\right), \quad -4P = \left(\frac{b(b-c)}{c^2}, \frac{b(b-c)^2}{c^3}\right).$$

Sada uvjet $2kP = \mathcal{O}$ zapisujemo u obliku $kP = -kP$, dok uvjet $(2k+1)P = \mathcal{O}$ zapisujemo u obliku $(k+1)P = -kP$. Tako primjerice dobivamo:

- Točka P je reda 4, tj. $2P = -2P$ ako i samo ako je $c = 0$. Dakle, opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}/4\mathbb{Z}$ je

  $$y^2 + xy - by = x^3 - bx^2, \quad b \in \mathbb{Q} \setminus \{-\tfrac{1}{16}, 0\}.$$

  Vrijednosti $b = -1/16$ i $b = 0$ smo isključili (a slično će biti s izuzetcima u idućim formulama) jer se za njih dobivaju singularne krivulje.

- Točka P je reda 5, tj. $3P = -2P$ ako i samo ako je $b = c$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}/5\mathbb{Z}$ je

  $$y^2 + (1-b)xy - by = x^3 - bx^2, \quad b \in \mathbb{Q} \setminus \{0\}.$$

- Točka P je reda 6, tj. $3P = -3P$ ako i samo ako je $b = c + c^2$. Dakle, opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}/6\mathbb{Z}$ je

  $$y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2, \quad c \in \mathbb{Q} \setminus \{-\tfrac{1}{9}, -1, 0\}.$$

- Točka P je reda 7, tj. $4P = -3P$ ako i samo ako je $b(b-c) = c^3$. Jednadžbu $b^2 - bc = c^3$ možemo shvatiti kao jednadžbu singularne kubike, sa singularitetom u $(b,c) = (0,0)$. Uvrstimo $b = cd$ u jednadžbu, pa dobivamo parametrizaciju $c = d^2 - d$, $b = d^3 - d^2$. Dakle, opći oblik krivulje s torzijskom grupom $\mathbb{Z}/7\mathbb{Z}$ je

  $$y^2 + (1-c)xy - by = x^3 - bx^2,$$
  $$b = d^3 - d^2,\ \ c = d^2 - d,\ \ d \in \mathbb{Q} \setminus \{0,1\}.$$

Razmotrit ćemo sada torzijske grupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ za $k = 1,2,3,4$. Sve takve krivulje imaju tri točke reda 2. Stoga ćemo ovdje promatrati krivulje s jednadžbom

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma), \tag{2.16}$$

gdje su α, β, γ tri različita racionalna broja. Jednadžba (2.16) ima tri racionalne točke reda 2, pa stoga ima torzijsku podgrupu izomorfnu sa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

U konstrukciji krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ koristimo se sljedećom činjenicom.

Teorem 2.4. *Neka je E eliptička krivulja nad poljem K, $\mathrm{char}(K) \neq 2, 3$. Neka je*

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

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

Dokaz: Dokažimo najprije da ako postoji točka P takva da je $Q = 2P$, onda su $x_2 - \alpha$, $x_2 - \beta$ i $x_2 - \gamma$ kvadrati.

Neka je $P = (x_1, y_1)$ točka s traženim svojstvom te neka je $y = \lambda x + \mu$ tangenta u P. Promotrimo polinom

$$(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2.$$

Njegovi korijeni su x_1 (korijen kratnosti 2) i x_2 (jer točka $-Q = (x_2, -y_2)$ leži na tangenti). Dakle,

$$(x-\alpha)(x-\beta)(x-\gamma) - (\lambda x + \mu)^2 = (x-x_1)^2(x-x_2). \tag{2.17}$$

Uvrstimo $x = \alpha$ u (2.17), pa dobivamo

$$-(\lambda\alpha + \mu)^2 = (\alpha - x_1)^2(\alpha - x_2),$$

odakle zaključujemo da je $x_2 - \alpha$ kvadrat. Uvrštavanjem $x = \beta$, odnosno $x = \gamma$, dobivamo da su i $x_2 - \beta$ i $x_2 - \gamma$ kvadrati.

Pretpostavimo sada da su $x_2 - \alpha$, $x_2 - \beta$ i $x_2 - \gamma$ kvadrati, te želimo naći (x_1, y_1) tako da je $2(x_1, y_1) = (x_2, y_2)$. Zamjenom varijabli, možemo pretpostaviti da je $x_2 = 0$. Dakle, $\alpha = -\alpha_1^2$, $\beta = -\beta_1^2$, $\gamma = -\gamma_1^2$, te možemo izabrati predznake od $\alpha_1, \beta_1, \gamma_1$ tako da je $y_2 = \alpha_1\beta_1\gamma_1$.

Tangenta u točki (x_1, y_1) prolazi točkom $(0, -y_2)$, pa ima jednadžbu oblika $y = kx - y_2$. Kubni polinom

$$p(x) = (x-\alpha)(x-\beta)(x-\gamma) - (kx - y_2)^2$$

ima korijen 0 i dvostruki korijen x_1, pa je jednak $x(x-x_1)^2$. Stoga kvadratni polinom

$$p(x)/x = x^2 - (\alpha + \beta + \gamma + k^2)x + \alpha\beta + \alpha\gamma + \beta\gamma + 2ky_2$$

ima dvostruku nultočku, pa mu je diskriminanta jednaka 0. Tako dobivamo jednadžbu četvrtog stupnja po k. Ako pokažemo da ta jednadžba ima korijen k_0 u K, onda će $x_1 = \frac{1}{2}(\alpha + \beta + \gamma + k_0^2)$ biti dvostruki korijen od $p(x)$, pa će točka $(x_1, y_1) = (x_1, k_0x_1 - y_2)$ imati traženo svojstvo da je $2(x_1, y_1) = (0, y_2)$.

Preostaje dakle pokazati da jednadžba

$$k^4 + (2\alpha + 2\beta + 2\gamma)k^2 - 8y_2k + \alpha^2 + \beta^2 + \gamma^2 - 2\alpha\beta - 2\alpha\gamma - 2\beta\gamma = 0 \tag{2.18}$$

ima racionalni korijen. Ako usporedimo polinom na lijevoj strani jednadžbe (2.18) s $(k^2 - \alpha + \beta + \gamma)^2$, te izrazimo $\alpha, \beta, \gamma, y_2$ pomoću $\alpha_1, \beta_1, \gamma_1$, dobivamo jednadžbu

$$(k^2 + \alpha_1^2 - \beta_1^2 - \gamma_1^2)^2 = (2(\alpha_1 k + \beta_1\gamma_1))^2,$$

odnosno

$$k^2 + \alpha_1^2 - \beta_1^2 - \gamma_1^2 = \pm 2(\alpha_1 k + \beta_1\gamma_1),$$

čija su rješenja $k = \alpha_1 \pm (\beta_1 + \gamma_1)$ (za predznak $+$), odnosno $k = -\alpha_1 \pm (\beta_1 - \gamma_1)$ (za predznak $-$). Dakle, dokazali smo da jednadžba (2.18) ima četiri racionalna korijena. □

Vratimo se sada na konstrukciju krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Bez smanjenja općenitosti možemo pretpostaviti da je točka $P = (0, 0)$ jedna od točaka reda 2, i to upravo ona točka za koju postoji $Q \in E(\mathbb{Q})$ takva da je $2Q = P$. To znači da krivulja ima jednadžbu

$$y^2 = x(x - \alpha)(x - \beta)$$

te da su brojevi $-\alpha$ i $-\beta$ kvadrati u $\mathbb{Q}$. Dakle, opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ je

$$y^2 = x(x + r^2)(x + s^2), \quad r, s \in \mathbb{Q} \setminus \{0\},\ r \neq \pm s, \tag{2.19}$$

odnosno (dijeleći jednadžbu s r^6 i uz oznaku $u = s/r$)

$$y^2 = x(x + 1)(x + u^2), \quad u \in \mathbb{Q} \setminus \{0, \pm 1\}. \tag{2.20}$$

Točka reda 4 na (2.19) je točka $(rs, rs(r + s))$, dok je na (2.20) to točka $Q = (u, u(u+1))$. Da bismo dobili krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, trebala bi postojati točka R (reda 8) takva da je $2R = Q$. Prema Teoremu 2.4 nužan i dovoljan uvjet za postojanje takve točke jest da u, $u + 1$ i $u(u + 1)$ budu kvadrati racionalnih brojeva. Dakle, imamo: $u = v^2$ i $v^2 + 1 = w^2$. Odavde je $v = \frac{2t}{t^2-1}$ za neki $t \in \mathbb{Q}$. Stoga je opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

$$y^2 = x(x + 1)\Big(x + \Big(\frac{2t}{t^2 - 1}\Big)^4\Big), \quad t \in \mathbb{Q} \setminus \{-1, 0, 1\}, \tag{2.21}$$

odnosno

$$y^2 = x(x + (t^2 - 1)^4)(x + 16t^4), \quad t \in \mathbb{Q} \setminus \{-1, 0, 1\}, \tag{2.22}$$

Kao zanimljivost navedimo sljedeći rezultat:

Teorem 2.5. *Svaka krivulja nad $\mathbb{Q}$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ je biracionalno ekvivalentna krivulji oblika*

$$y^2 = (ax + 1)(bx + 1)(cx + 1), \tag{2.23}$$

gdje je $\{a, b, c\}$ neka racionalna Diofantova trojka.

Dokaz: Množeći jednadžbu (2.23) s $a^2b^2c^2$, te uvodeći supstituciju $x \mapsto (x - ab)/abc$, dobivamo jednadžbu

$$y^2 = x(x + ac - ab)(x + bc - ab).$$

Ako je $ab = -1$, tj. $b = -1/a$, onda su $ac - ab$ i $bc - ab$ kvadrati, pa dobivamo eliptičku krivulju čija torzijska grupa sadrži $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Jedna od točaka reda 4 je $Q = (\sigma\tau, \sigma\tau(\sigma+\tau))$, gdje je $ac+1 = \sigma^2$, $bc+1 = \tau^2$. Uzmimo da je trojka $\{a, b, c\}$ regularna, tj. da je oblika

$$\Big\{a, -\frac{1}{a}, a - \frac{1}{a}\Big\}.$$

Tada je $\sigma = a$, $\tau = \frac{1}{a}$, pa je $Q = (1, a + \frac{1}{a})$, a krivulja ima jednadžbu

$$y^2 = x(x + a^2)\Big(x + \frac{1}{a^2}\Big).$$

Da bi dobili točku reda 8 i torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, želimo da točka Q bude oblika $Q = 2R$ za neku točku $R \in E(\mathbb{Q})$. Po Teoremu 2.4, nužan i dovoljan uvjet za to je da $a^2 + 1$ bude kvadrat racionalnog broja, tj. $a = \frac{2t}{t^2-1}$. Dobili smo jednadžbu

$$y^2 = x\Big(x + \frac{4t^2}{(t^2-1)^2}\Big)\Big(x + \frac{(t^2-1)^2}{4t^2}\Big).$$

Pomnožimo jednadžbu s $(4t^2(t^2-1)^2)^3$ te uvedemo supstituciju $x \mapsto x/(4t^2(t^2-1)^2)$, pa dobivamo upravo jednadžbu (2.21). □

Preostala nam je torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Da bismo nju dobili, trebali bismo na njoj imati točku P reda 3 (bez smanjenja općenitosti možemo pretpostaviti da joj je prva koordinata jednaka 0) za koju postoji točka Q reda 6 takva da je $2Q = P$. Prema Teoremu 2.4, tada u (2.16) moramo imati $\alpha = -r^2$, $\beta = -s^2$, $\gamma = -t^2$. Dakle, dobili smo krivulju

$$y^2 = (x + r^2)(x + s^2)(x + t^2), \tag{2.24}$$

koja uz tri točke drugog reda, ima još jednu očitu racionalnu točku $P = (0, rst)$. Ako bi točka P bila reda 3, onda bismo dobili traženu torzijsku grupu. Dakle, moramo zadovoljiti uvjet $-P = 2P$, koji daje

$$\frac{(r^2s^2 + r^2t^2 + s^2t^2)^2}{4r^2s^2t^2} - r^2 - s^2 - t^2 = 0,$$

tj.

$$(sr + ts + tr)(-sr + ts + tr)(-sr + ts - tr)(sr + ts - tr) = 0.$$

Možemo uzeti da je $t = \frac{rs}{r-s}$, pa dobivamo da je opći oblik krivulje s torzijskom podgrupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

$$y^2 = (x + r^2)(x + s^2)\left(x + \frac{r^2s^2}{(r-s)^2}\right), \quad r, s \in \mathbb{Q} \setminus \{0\},\ r \neq \pm s, \frac{1}{2}s, 2s,$$

odnosno, uz oznaku $u = s/r$,

$$y^2 = (x + 1)(x + u^2)\Big(x + \frac{u^2}{(u-1)^2}\Big), \quad u \in \mathbb{Q} \setminus \{0, \pm 1, \frac{1}{2}, 2\}.$$

2.5 Rang eliptičke krivulje

Pitanja koja se tiču ranga eliptičke krivulje nad $\mathbb{Q}$ su puno teža od pitanja vezanih uz torzijske grupe, a zadovoljavajući odgovori još uvijek nisu poznati. Dugo se vjerovalo da rang može biti proizvoljno velik, tj. da za svaki $M \in \mathbb{N}$ postoji eliptička krivulja E nad $\mathbb{Q}$ takva da je $\text{rank}(E) \geq M$. No nedavno se pojavilo nekoliko članaka koji daju različite heurističke argumente zašto bi rang možda ipak mogao biti ograničen. Danas se tek zna da postoji eliptička krivulja ranga ≥ 28. Tu je krivulju 2006. godine pronašao Noam Elkies. Klagsbrun, Sherman i Weigandt su dokazali

2019. godine da je rang te krivulje jednak 28, uz pretpostavku da vrijedi generalizirana Riemannova slutnja. Jednadžba (minimalna) joj je:

$$y^2+xy+y=x^3-x^2-$$
$$2006776241557552658503320820933854275093023031217895650 2x+$$
$$3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9.$$

Pregled pronalazaka rekordnih krivulja dan je u sljedećoj tablici (detalji o rekordnim krivuljama mogu se naći na *web* stranici
`https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`):

rang$\geq$	godina	autori
3	1938.	Billing
4	1945.	Wiman
6	1974.	Penney & Pomerance
7	1975.	Penney & Pomerance
8	1977.	Grunewald & Zimmert
9	1977.	Brumer - Kramer
12	1982.	Mestre
14	1986.	Mestre
15	1992.	Mestre
17	1992.	Nagao
19	1992.	Fermigier
20	1993.	Nagao
21	1994.	Nagao & Kouya
22	1997.	Fermigier
23	1998.	Martin & McMillen
24	2000.	Martin & McMillen
28	2006.	Elkies

Striktno govoreći, nije poznat nijedan algoritam za računanje ranga. Naime, za "algoritme" (uobičajeno ih je ipak tako nazivati) koji se rabe za računanje ranga, od kojih ćemo neke sada i prikazati, nema jamstva da će dati rezultat u svim slučajevima. Važan dio tih algoritama uključuje odluku ima li racionalnih točaka na određenoj krivulji genusa 1 za koju je poznato da ima točaka svugdje lokalno (tj. nad $\mathbb{R}$ te nad p-adskim poljem $\mathbb{Q}_p$ za sve proste brojeve p). No nije poznat algoritam koji bi dao odgovor na to pitanje. Nadalje, čak i ako zanemarimo ovaj problem (jer nam se možda neće pojaviti za konkretnu krivulju koju promatramo), kod krivulja koje nemaju racionalnih točaka reda 2 i imaju velike koeficijente, poznati algoritmi uglavnom nisu dovoljno efikasni za praktičnu primjenu.

Pretpostavimo da E ima točku reda 2. U tom slučaju je računanje ranga obično lakše nego u općem slučaju. Opisat ćemo metodu za računanje ranga koja se naziva "silazak s pomoću 2-izogenije". Promjenom koordinata možemo pretpostaviti da je točka reda 2 upravo točka $(0,0)$ te da E ima jednadžbu

$$y^2=x^3+ax^2+bx, \tag{2.25}$$

gdje su $a, b \in \mathbb{Z}$. Ako je polazna krivulja bila dana jednadžbom $y^2 = x^3+a_2x^2+a_4x+a_6$ te ako je x_0 korijen polinoma $x^3 + a_2x^2 + a_4x + a_6$, onda stavimo $a = 3x_0 + a_2$, $b = (a + a_2)x_0 + a_4$. Ako je polazna krivulja bila dana s pomoću Weierstrassove jednadžbe, onda za x_0 uzimamo korijen kubnog polinoma $x^3 + b_2x^2 + 8b_4x + 16b_6$ i stavimo $a = 3x_0 + b_2$, $b = (a + b_2)x_0 + 8b_4$. Uvjet nesingularnosti za krivulju E je $\Delta = 16b^2(a^2 - 4b) \neq 0$.

Za krivulju E' koja ima jednadžbu

$$y^2 = x^3 + a'x^2 + b'x, \tag{2.26}$$

gdje je $a' = -2a$ i $b' = a^2 - 4b$, kažemo da je 2-izogena krivulji E. Uvjet nesingularnosti za obje krivulje E i E' je isti i može se iskazati u obliku $bb' \neq 0$. Općenito, izogenijom zovemo homomorfizam između dvije eliptičke krivulje koji je dan s pomoću racionalnih funkcija. U našem slučaju radi se o preslikavanju $\phi : E \to E'$, $\phi(P) = (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2})$ za $P = (x, y) \neq \mathcal{O}, (0, 0)$, a $\phi(P) = \mathcal{O}$ inače. Analogno se definira $\psi : E' \to E$ sa $\psi(P') = (\frac{y'^2}{4x'^2}, \frac{y'(x'^2-b')}{8x'^2})$ za $P' = (x', y') \neq \mathcal{O}, (0, 0)$, a $\psi(P') = \mathcal{O}$ inače. Vrijedi $(\psi \circ \phi)(P) = 2P$ za sve $P \in E$ i $(\phi \circ \psi)(P') = 2P'$ za sve $P' \in E'$.

Definirajmo još i preslikavanja $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, $\beta : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, s $\alpha(\mathcal{O}) = 1\cdot\mathbb{Q}^{*2}$, $\alpha(0, 0) = b\cdot\mathbb{Q}^{*2}$, $\alpha(x, y) = x\cdot\mathbb{Q}^{*2}$ za $P = (x, y) \neq \mathcal{O}, (0, 0)$, te sasvim analogno za β. Jasno je da je $\mathrm{Ker}(\phi) = \{\mathcal{O}, (0, 0)\}$, $\mathrm{Ker}(\psi) = \{\mathcal{O}, (0, 0)\}$, a pokazuje se da vrijedi $\mathrm{Im}(\phi) = \mathrm{Ker}(\beta)$ i $\mathrm{Im}(\psi) = \mathrm{Ker}(\alpha)$. Broj 2 u nazivu 2-izogenija dolazi od toga što su jezgre od ϕ i ψ dvočlane.

Ovim preslikavanjima se koristi u prvom koraku dokaza Mordell-Weilova teorema, tj. u dokazu da podgrupa $2E(\mathbb{Q})$ ima konačan indeks u grupi $E(\mathbb{Q})$. Naime, lako se vidi da ta tvrdnja slijedi iz konačnosti indeksa $[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))]$ i $[E'(\mathbb{Q}) : \phi(E(\mathbb{Q}))]$, a to pak, prema Teoremu o izomorfizmu grupa, slijedi iz konačnosti grupa $\mathrm{Im}(\alpha)$ i $\mathrm{Im}(\beta)$. Zapravo je veza ovih preslikavanja s rangom još eksplicitnija. Naime, vrijedi

$$2^r = \frac{[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))] \cdot [E'(\mathbb{Q}) : \phi(E(\mathbb{Q}))]}{4} = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|}{4},$$

gdje je $r = \mathrm{rank}(E(\mathbb{Q}))$.

Vrijedi i da je $r = \mathrm{rank}(E'(\mathbb{Q}))$, no torzijske grupe od E i E' općenito ne moraju biti izomorfne, već vrijedi $|E(\mathbb{Q})_{\mathrm{tors}}| = 2^i|E'(\mathbb{Q})_{\mathrm{tors}}|$, gdje je $i \in \{-1, 0, 1\}$.

Želimo dobiti opis elemenata iz $\mathrm{Im}(\alpha)$. S $\tilde{x}$ ćemo označiti klasu od x u $\mathbb{Q}/\mathbb{Q}^{*2}$.

Neka je $(x, y) \in E(\mathbb{Q})$. Ako je $x = 0$, onda je $(x, y) = (0, 0)$ i $\alpha(x, y) = \tilde{b}$. Ako je $x \neq 0$, zapišimo x i y u obliku $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $\mathrm{nzd}(m, e) = \mathrm{nzd}(n, e) = 1$ te ih uvrstimo u jednadžbu od E. Dobivamo

$$n^2 = m(m^2 + ame^2 + be^4).$$

Stavimo $b_1 = \pm\,\mathrm{nzd}(m, b)$, gdje je predznak odabran tako da je $mb_1 > 0$. Tada je $m = b_1m_1$, $b = b_1b_2$, $n = b_1n_1$, pa dobivamo

$$n_1^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4).$$

Budući da su faktori na desnoj strani posljednje jednadžbe relativno prosti, te $m_1 > 0$, zaključujemo da postoje cijeli brojevi M i N tako da vrijedi $m_1 = M^2$, $b_1m_1^2 + am_1e^2 + b_2e^4 = N^2$, te tako naposljetku dobivamo jednadžbu

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4, \tag{2.27}$$

u kojoj su nepoznanice M, e i N. Sada je $\alpha(x,y) = (\frac{b_1M^2}{e^2}) \cdot \mathbb{Q}^{*2} = \tilde{b_1}$.

Zaključujemo da se $\mathrm{Im}(\alpha)$ sastoji od $\tilde{1}$, $\tilde{b}$ te od svih $\tilde{b_1}$ gdje je b_1 djelitelj broja b za koji jednadžba (2.27), gdje je $b_1b_2 = b$, ima rješenja $N, M, e \in \mathbb{Z}$, $e \neq 0$. Tada je $(\frac{b_1M^2}{e^2}, \frac{b_1MN}{e^3}) \in E(\mathbb{Q})$. Uočimo da jednadžba (2.27) uvijek ima rješenje za $b_1 = 1$, a to je $(M, e, N) = (1, 0, 1)$ i za $b_1 = b$, a to je $(M, e, N) = (0, 1, 1)$.

Pri ispitivanju rješivosti jednadžbe (2.27) možemo pretpostaviti da je $\mathrm{nzd}(M, e) = 1$. Također, nije gubitak općenitosti ako se gledaju samo oni djelitelji b_1 koji su kvadratno slobodni. Alternativno, ako se gledaju svi djelitelji b_1, onda se mogu tražiti samo rješenja koja zadovoljavaju $\mathrm{nzd}(N, e) = \mathrm{nzd}(M, N) = 1$.

Imamo sljedeći algoritam za računanje ranga eliptičke krivulje E koja ima racionalnu točku reda 2, tj. ima jednadžbu oblika (2.25). Za svaku faktorizaciju $b = b_1b_2$, gdje je b_1 kvadratno slobodan cijeli broj, napišemo jednadžbu (2.27). Pokušamo odrediti ima li ta jednadžba netrivijalnih cjelobrojnih rješenja (uočimo da za ovakve jednadžbe ne mora vrijediti lokalno-globalni princip Hassea i Minkowskog, što znači da zapravo nemamo algoritam koji bi sa sigurnosti odgovorio na ovo pitanje). Svako rješenje (M, e, N) jednadžbe (2.27) inducira točku na krivulji E s koordinatama $x = \frac{b_1M^2}{e^2}$, $y = \frac{b_1MN}{e^3}$. Neka je r_1 broj faktorizacija za koje pripadna jednadžba (2.27) ima rješenja, te neka je r_2 broj definiran na isti način za krivulju E'. Tada postoje nenegativni cijeli brojevi e_1 i e_2 takvi da je $r_1 = 2^{e_1}$, $r_2 = 2^{e_2}$ i pritom vrijedi da je

$$\mathrm{rank}(E) = e_1 + e_2 - 2.$$

Primjer 2.8. *Promotrimo skup $\{1, 2, 5\}$. To je jedna $D(-1)$-trojka. Naime, $1 \cdot 2 - 1$, $1 \cdot 5 - 1$ i $2 \cdot 5 - 1$ su potpuni kvadrati. Postavlja se pitanje, može li se ovaj skup proširiti do $D(-1)$-četvorke, tj. postoji li $x \in \mathbb{Z}$ takav da su*

$$1 \cdot x - 1, \quad 2 \cdot x - 1, \quad 5 \cdot x - 1$$

kvadrati cijelih brojeva? Pokazat ćemo da je jedino rješenje $x = 1$, pa budući da je $1 \in \{1, 2, 5\}$, to će značiti da se skup $\{1, 2, 5\}$ ne može proširiti do $D(-1)$-četvorke. Zapravo, mi ćemo ovdje riješiti i općenitiji problem nalaženja svih racionalnih točaka na eliptičkoj krivulji

$$y^2 = (x - 1)(2x - 1)(5x - 1) \tag{2.28}$$

te dokazati da se $\{1, 2, 5\}$ ne može proširiti ni do racionalne $D(-1)$-četvorke.

Rješenje: Dovedimo najprije krivulju u Weierstrassov oblik, množenjem obiju strana jednadžbe s 10^2 i supstitucijom $10y \mapsto y$, $10x \mapsto x$. Dobivamo

$$y^2 = x^3 - 17x^2 + 80x - 100.$$

Translacijom $x \mapsto x + 5$ dovedimo krivulju u oblik prikladan za računanje ranga:

$$E: \quad y^2 = x^3 - 2x^2 - 15x.$$

Njezina 2-izogena krivulja je

$$E': \quad y^2 = x^3 + 4x^2 + 64x.$$

Za krivulju E, mogućnosti za broj b_1 su ± 1, ± 3, ± 5, ± 15. Pripadne diofantske jednadžbe su $N^2 = M^4 - 2M^2e^2 - 15e^4$, $N^2 = -M^4 - 2M^2e^2 + 15e^4$, $N^2 =$

$3M^4-2M^2e^2-5e^4$, $N^2=-3M^4-2M^2e^2+5e^4$, $N^2=5M^4-2M^2e^2-3e^4$, $N^2=-5M^4-2M^2e^2+3e^4$, $N^2=15M^4-2M^2e^2-e^4$, $N^2=-15M^4-2M^2e^2+e^4$. Zbog simetričnosti je dovoljno ispitati rješivost prvih četiriju jednadžbi. Prva jednadžba ima rješenje $(M,e,N)=(1,0,1)$, a četvrta ima rješenje $(M,e,N)=(1,1,0)$. Druga jednadžba je ekvivalentna s $N^2=(3e^2-M^2)(5e^2+M^2)$. Lako se vidi da je $\mathrm{nzd}(3e^2-M^2,5e^2+M^2)\in\{1,2\}$, pa imamo dvije mogućnosti: ili su oba faktora kvadrati ili su oba dvostruki kvadrati. No $3e^2-M^2=s^2$ je nemoguće modulo 3 jer je $(\frac{-1}{3})=-1$, dok je $5e^2+M^2=2t^2$ nemoguće modulo 5 jer je $(\frac{2}{5})=-1$. Treća jednadžba je ekvivalentna s $N^2=(M^2+e^2)(3M^2-5e^2)$. Ponovno imamo iste dvije mogućnosti za faktore u zadnjem izrazu i ponovno obje mogućnosti otpadaju: $3M^2-5e^2=t^2$ je nemoguće modulo 5 jer je $(\frac{3}{5})=-1$, dok je $3M^2-5e^2=2t^2$ nemoguće modulo 8 jer je $3M^2-5e^2\equiv 6 \pmod 8$, a $2t^2\equiv 2 \pmod 8$. Dakle, $e_1=2$.

Za E' je $b_1'\in\{\pm1,\pm2\}$, pa su pripadne diofantske jednadžbe $N^2=M^4+4M^2e^2+64e^4$, $N^2=-M^4+4M^2e^2-64e^4$, $N^2=2M^4+4M^2e^2+32e^4$ i $N^2=-2M^4+4M^2e^2-32e^4$. Prva jednadžba ima rješenje $(M,e,N)=(1,0,1)$. Druga i četvrta jednadžba su ekvivalentne s $N^2=-(M^2-2e^2)^2-60e^4$, odnosno $N^2=-2(M^2-e^2)^2-30e^2$ te očito nemaju netrivijalnih rješenja. Treća jednadžba je ekvivalentna s $2\cdot(N/2)^2=(M^2+e^2)^2+15e^4$ te nema rješenja modulo 5 jer je $(\frac{2}{5})=-1$. Dakle, $e_2=0$. Zaključujemo da je $\mathrm{rank}(E)=2+0-2=0$.

Treba još samo naći torzijske točke na E. Ona ima tri točke reda 2: $(0,0)$, $(-3,0)$, $(5,0)$. Budući da $7\nmid\Delta=2^{10}3^25^2$ te da je $|E(\mathbb{F}_7)|=4$, zaključujemo da su jedine racionalne točke na E $(0,0)$, $(-3,0)$, $(5,0)$, pa su jedine racionalne točke na krivulji (2.28): $(1,0)$, $(\frac{1}{2},0)$, $(\frac{1}{5},0)$. Budući da $1\cdot\frac{1}{2}-1$ i $1\cdot\frac{1}{5}-1$ nisu kvadrati racionalnih brojeva, dobivamo da je jedini racionalni broj x sa svojstvom da su $1\cdot x-1$, $2\cdot x-1$ i $5\cdot x-1$ kvadrati, broj $x=1$. ♢

Primjer 2.9. *Izračunajmo rang eliptičke krivulje*

$$y^2=(x+1)(3x+1)(8x+1)$$

inducirane Diofantovom trojkom $\{1,3,8\}$.

Rješenje: Kao i u prethodnom primjeru, krivulju dovodimo u oblik prikladan za računanje ranga, tako da ju najprije dovedemo u Weierstrassov oblik

$$y^2=(x+3)(x+8)(x+24),$$

a potom translacijom $x\mapsto x-8$ dobivamo

$$E:\quad y^2=x^3+11x^2-80x.$$

Njezina 2-izogena krivulja je

$$E':\quad y^2=x^3-22x^2+441x.$$

Za krivulju E, mogućnosti za broj b_1 su ±1, ±2, ±5, ±10. Tvrdimo da svih osam pripadnih jednadžbi ima rješenja: $N^2=M^4+11M^2e^2-80e^4$, $N^2=-M^4+11M^2e^2+80e^4$, $N^2=2M^4+11M^2e^2-40e^4$, $N^2=-2M^4+11M^2e^2+40e^4$, $N^2=5M^4+11M^2e^2-16e^4$, $N^2=-5M^4+11M^2e^2+16e^4$, $N^2=10M^4+11M^2e^2-8e^4$, $N^2=-10M^4+11M^2e^2+8e^4$. Zaista, rješenja su redom: $(M,e,N)=(1,0,1)$, $(4,1,0)$, $(2,1,6)$, $(1,1,7)$, $(1,1,0)$, $(0,1,4)$, $(2,1,14)$, $(1,1,3)$. Dakle, $e_1=3$.

Za E' je $b_1' \in \{\pm 1, \pm 3, \pm 7, \pm 21\}$. Jednadžba za $b_1' = 1$ očito ima rješenja, dok jednadžbe za $b_1' < 0$ očito nemaju rješenja. Pokazat ćemo da preostale tri jednadžbe nemaju rješenja. Za $b_1' = 3$ dobivamo jednadžbu

$$3N^2 = (3M^2 - 11e^2)^2 + 320e^4,$$

koja nema rješenja modulo 5 jer je $(\frac{3}{5}) = -1$, tj. 3 nije kvadratni ostatak modulo 5. Slično, za $b_1' = 7$, jednadžba

$$7N^2 = (7M^2 - 11e^2)^2 + 320e^4$$

nema rješenja modulo 5 jer je $(\frac{7}{5}) = (\frac{2}{5}) = -1$. Konačno, promotrimo jednadžbu za $b_1' = 21$:

$$21N^2 = (21M^2 - 11e^2)^2 + 320e^4. \tag{2.29}$$

Ako je neki od brojeva M, e paran, onda, budući da kvadrat neparnog broj pri dijeljenju s 8 daje ostatak 1, lijeva strana od (2.29) je $\equiv 5 \pmod 8$, dok je desna strana $\equiv 1 \pmod 8$. Ako su brojevi M, e oba neparni, onda je $21M^2 - 11e^2 \equiv 2 \pmod 8$, pa je desna strana od (2.29) djeljiva s 4, a nije djeljiva s 8. Zato je $N \equiv 2 \pmod 4$. Nakon dijeljenja sa 4, lijeva strana od (2.29) je $\equiv 5 \pmod 8$, dok je desna strana $\equiv 1 \pmod 8$. Dakle, $e_2 = 0$. Zaključujemo da je $\operatorname{rank}(E) = 3 + 0 - 2 = 1$. $\diamondsuit$

Uočimo da smo se u prethodnom primjeru kod eliminiranja b_1'-ova za koje pripadna diofantska jednadžba nema rješenja koristili činjenicama da negativni broj ne može biti kvadrat u $\mathbb{R}$ te da brojevi 2 i 3 nisu kvadrati u $\mathbb{Z}/5\mathbb{Z}$. No kod diofantskih jednadžbi stupnja većeg od 2 može se dogoditi da one imaju rješenja u $\mathbb{R}$ te da imaju rješenja u $\mathbb{Z}/m\mathbb{Z}$ za svaki cijeli broj m, ali da ipak nemaju netrivijalnih rješenja u $\mathbb{Q}$. Jedan takav primjer je jednadžba

$$N^2 = 17M^4 - 4e^4$$

koja se pojavljuje kod računanja ranga eliptičke krivulje $y^2 = x^3 + 17x$. U takvim slučajevima je određivanje ranga znatno teže.

Označimo s $\omega(b)$ broj različitih prostih faktora od b. Tada b ima $2^{\omega(b)+1}$ (pozitivnih i negativnih) kvadratno slobodnih faktora. Sada iz formule $2^r = \frac{|\mathrm{Im}(\alpha)| \cdot |\mathrm{Im}(\beta)|}{4}$ slijedi izravno da je $r \leq \omega(b) + \omega(b')$. No iz jednadžbe (2.27) slijedi da ako je $a \leq 0$ i $b > 0$, onda b_1 mora biti pozitivan. Analogno, ako je $a' \leq 0$ i $b' > 0$, onda b_1' mora biti pozitivan. Isto tako iz

$$N^2 = b_1\Big(M^2 + \frac{ae^2}{2b_1}\Big)^2 - \frac{b'e^4}{4b_1}$$

slijedi da ako je $b' < 0$, onda b_1 mora biti pozitivan te analogno ako je $b < 0$, onda b_1' mora biti pozitivan. Uočimo da b i b' ne mogu biti istodobno negativni jer je $4b + b' = a^2$. Očito je $a \leq 0$ ili $a' \leq 0$. Stoga se negativni djelitelji ne mogu pojaviti u barem jednom od skupova $\mathrm{Im}(\alpha)$, $\mathrm{Im}(\beta)$. Zaključujemo da je

$$r \leq \omega(b) + \omega(b') - 1.$$

Recimo sada nešto o provjeravanju lokalne rješivosti jednadžbe

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4, \tag{2.30}$$

odnosno njoj pridružene (afine) jednadžbe

$$u^2 = b_1 v^4 + a v^2 + b_2. \tag{2.31}$$

Općenito, kriterij za rješivost nad $\mathbb{R}$ (tj. za $p = \infty$) jednadžbe $Y^2 = g(X)$ je vrlo jednostavan: polinom g mora u nekoj točki x poprimiti nenegativnu vrijednost. To će sigurno biti zadovoljeno ako g ima realnih korijena, a ako g nema realnih korijena, onda vodeći koeficijent od g mora biti pozitivan.

Što se tiče rješivosti jednadžbe (2.31) u $\mathbb{Q}_p$ (odnosno jednadžbe (2.30) modulo p^k za svaki $k \geq 1$), dovoljno je promatrati samo one proste brojeve p za koje vrijedi $p \mid 2\Delta$. Naime, pokazuje se da su za sve ostale p-ove jednadžbe sigurno rješive.

Jednadžbu (2.30) možemo zapisati i u obliku

$$N^2 = b_1 \left(M^2 + \frac{ae^2}{2b_1} \right)^2 - \frac{b' e^4}{4b_1},$$

odakle dobivamo uvjet da za svaki neparni prosti djelitelj p od b' mora za Legendreov simbol vrijediti $(\frac{b_1}{p}) = 1$. Ovo daje samo nužni, a ne i dovoljni uvjet za rješivost u $\mathbb{Q}_p$. Opći algoritam koristi se Henselovom lemom, tako da za dano rješenje modulo p^k provjerava može li se to rješenje "podići" do rješenja modulo p^{k+1}. Čim je k dovoljno velik ($k > \nu_p(\Delta)$), algoritam sigurno daje odgovor na to pitanje te tako rješava pitanje rješivosti u $\mathbb{Q}_p$.

Pretpostavimo da smo u gore opisanom algoritmu "silaska s pomoću 2-izogenije" naišli na jednadžbu

$$u^2 = b_1 v^4 + a v^2 + b_2, \quad b_1 b_2 = b \tag{2.32}$$

koja je svugdje lokalno rješiva, ali nismo na njoj uspjeli naći racionalnu točku. Tada se može primijeniti metoda "drugog silaska", s pomoću koje se može katkad pronaći racionalna točka (u, v) na (2.32) ili dokazati da (2.32) nema racionalnih točaka. Ideja je da budući da je (2.32) svugdje lokalno rješiva, onda je i pripadna konika

$$u^2 = b_1 w^2 + a w + b_2 \tag{2.33}$$

svugdje lokalno rješiva. No za ovakve kvadratne jednadžbe vrijedi lokalno-globalni princip Hassea i Minkowskoga, koji povlači da je tada (2.33) i globalno rješiva, tj. da ima racionalnu točku (u_0, w_0). Možemo pretpostaviti da je $w_0 \neq 0$, jer ako je $w_0 = 0$, onda je b_2 kvadrat, pa jednadžba (2.32) sigurno ima rješenja. Sve racionalne točke na (2.33) mogu se dobiti sljedećim parametarskim formulama:

$$\begin{aligned} w &= \frac{w_0 t^2 - 2u_0 t + a + b_1 w_0}{t^2 - b_1}, \\ u &= \frac{-u_0 t^2 + (a + 2b_1 w_0) t - u_0 b_1}{t^2 - b_1}. \end{aligned}$$

Želimo naći (ili dokazati da ne postoji) racionalni broj t takav da je $w = \frac{f(t)}{g(t)}$ kvadrat racionalnog broja. Ovaj uvjet dovodi do novih kvartika. Sada se s njima ponavlja postupak ispitivanja lokalne rješivosti te traženja rješenja s relativno malom visinom. Ponovno nema jamstva da ćemo u svakom slučaju dobiti odgovor.

Skup svih $\tilde{b_1}$-ova za koje je jednadžba (2.27) svugdje lokalno rješiva također čini grupu (i analogno za b_1'). Ako su pripadni redovi 2^{f_1} i 2^{f_2}, onda se broj $s = f_1 + f_2 - 2$

naziva *2-Selmerov rang* od E. Jasno je da je $r \leq s$. Vidjeli smo da može biti $r = s$, ali i $r < s$. Slutnja je da je uvijek $r \equiv s \pmod 2$.

Opisani algoritam je implementiran u programu MWRANK autora Johna Cremone koji je uključen u programski paket SageMath. Algoritmi za računanje ranga postoje i u programskom paketu Magma, a od nedavno i u PARI-ju preko funkcije `ellrank`.

U općem slučaju, kada E ne mora imati točku reda 2, ponovno je ideja pridružiti krivulji E familiju kvartika. U ovom slučaju one imaju općenitiji oblik

$$H \,:\, y^2 = g(x) = ax^4 + bx^3 + cx^2 + dx + e. \tag{2.34}$$

Ovdje su $a, b, c, d, e \in \mathbb{Q}$, i to takvi da je

$$12ae - 3bd + c^2 = \lambda^4 c_4, \quad 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3 = 2\lambda^6 c_6$$

za neki $\lambda \in \mathbb{Q}$. I ovaj algoritam sadržan u MWRANK-u (iako radi znatno neefikasnije od verzije za krivulje s točkom reda 2).

Izaberemo li eliptičku krivulju na "slučajan" način, ona će najvjerojatnije imati trivijalnu torzijsku grupu i vrlo mali rang (0 ili 1). Slutnja je da je prosječan rang $1/2$ ("pola" krivulja ima rang 0, "pola" rang 1, a broj krivulja s rangom ≥ 2 je asimptotski zanemariv). Iz rezultata Manjula Bhargave, dobitnika Fieldsove medalje 2014. godine, i suradnika slijedi da je prosječan rang strogo manji od 1 (ovdje pretpostavljamo da smo eliptičke krivulje $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$, uredili s obzirom na veličinu od $\max(4|A|^3, 27B^2)$). Prije smo vidjeli kako možemo osigurati da krivulja ima unaprijed zadanu torzijsku podgrupu. Sada ćemo razmotriti metode za nalaženje eliptičkih krivulja relativno velikog ranga (jako velik rang ne možemo očekivati imajući u vidu da trenutačno nije poznata nijedna eliptička krivulja s rangom većim od 28). Kao što smo već spomenuli, iako nam nisu poznati primjeri krivulja s vrlo velikim rangom, dugo je bila opće prihvaćena slutnja da rang može biti proizvoljno velik. Jedan teoretski rezultat koji daje izvjesnu potporu toj slutnji je rezultat Tatea i Šafarevića koji kaže da rang eliptičkih krivulja nad poljem $\mathbb{F}_q(t)$ (polje funkcija od jedne varijable nad konačnim poljem) neograničen.

Opća metoda za nalaženje krivulja s velikim rangom se sastoji od sljedeće tri faze:

- *Konstrukcija:* Generiramo familiju eliptičkih krivulja nad $\mathbb{Q}$ (npr. krivulju nad poljem racionalnih funkcija $\mathbb{Q}(t)$) za koju vjerujemo (ili znamo) da sadržava eliptičke krivulje velikog ranga, npr. zato što je "generički" rang krivulje nad $\mathbb{Q}(t)$ relativno velik. Prema Silvermanovu specijalizacijskom teoremu, tada će za sve osim konačno mnogo racionalnih brojeva t_0, rang nad $\mathbb{Q}$ krivulje koja se dobije uvrštavanjem (specijalizacijom) $t = t_0$ biti veći ili jednak od generičkog ranga. Spomenimo da algoritam, čiji su autori Ivica Gusić i Petra Tadić, za krivulje s barem jednom točkom reda 2 nad $\mathbb{Q}(t)$ omogućava nalaženje odgovarajućih injektivnih specijalizacija $t = t_0$ te računanje generičkog ranga takvih krivulja.
- *Sito:* Za svaku krivulju u promatranoj familiji izračunamo neke podatke koje nam daju određene informacije o rangu (npr. donju i gornju ogradu za rang – možda uz pretpostavku da vrijedi neka od opće prihvaćenih slutnji). Ovdje je

bitno da se te (premda možda dosta neprecizne) informacije o rangu mogu izračunati puno brže od samog ranga. Na osnovi tih informacija, izabiremo ("prosijemo") u promatranoj familiji mali podskup najboljih kandidata za veliki rang.

- *Računanje ranga:* Za svaku krivulju iz (malog) skupa najboljih kandidata pokušavamo egzaktno izračunati rang ili barem što bolju donju ogradu za rang da bismo potvrdili da ta krivulja zaista ima velik rang.

Većinu metoda kojima se i danas koristi u prve dvije faze uveo je Jean-Francois Mestre 80-ih i 90-ih godina 20. stoljeća.

Prikazat ćemo jednu njegovu konstrukciju kojom je 1991. godine dobio beskonačno mnogo eliptičkih krivulja ranga ≥ 11. Ta konstrukcija se obično naziva *Mestreova polinomijalna metoda*. Polazište u konstrukciji je sljedeća činjenica, koju bismo, po analogiju s "teoremom o dijeljenju s ostatkom", mogli nazvati "lema o korjenovanju s ostatkom".

Lema 2.1. *Neka je K polje karakteristike 0. Ako je $A \in K[x]$ normirani polinom i $\deg A = mn$, gdje su $m, n \geq 1$, onda postoji normirani polinom $B \in K[x]$ tako da je $\deg B = n$ i $\deg(A - B^m) < n(m-1)$.*

Dokaz: Matematičkom indukcijom po i ćemo dokazati da za svaki $i \leq n$ postoji $B_i \in K[x]$ takav da je $\deg B_i = n$ i $\deg(A - B_i^m) < nm - i$. Za $i = 0$ možemo uzeti $B_0 = x^n$. Pretpostavimo da tvrdnja vrijedi za $i-1$, gdje je $0 < i \leq n$. Dakle, postoji polinom B_{i-1} stupnja n takav da je $\deg(A - B_{i-1}^m) < nm - i + 1$. Polinom B_i tražimo u obliku $B_i = B_{i-1} + cx^{n-i}$. Imamo

$$B_i^m = B_{i-1}^m + mcB_{i-1}^{m-1}x^{n-i} + \binom{m}{2}c^2 B_{i-1}^{m-2}x^{2(n-i)} + \cdots,$$

gdje su stupnjevi svih pribrojnika počevši od drugog na dalje $\leq n(m-2) + 2(n-i) = nm - 2i < nm - i$. Stupanj od $B_{i-1}^{m-1}x^{n-i}$ je $nm - i$, pa možemo izabrati c tako da se članovi s x^{nm-i} pokrate te dobivamo $\deg(A - B_i^m) = \deg(A - B_{i-1}^m - mcB_{i-1}^{m-1}x^{n-i}) < nm - i$. Budući da je polinom B_0 normiran, iz konstrukcije slijedi da su svi polinomi B_i normirani. □

Korolar 2.2. *Neka je $p(x) \in \mathbb{Q}[x]$ normiran polinom i $\deg p = 2n$. Tada postoje jedinstveni polinomi $q(x), r(x) \in \mathbb{Q}[x]$ takvi da je $p = q^2 - r$ i $\deg r \leq n - 1$.*

Polinom q iz Korolara 2.2 možemo naći sukcesivnim računanjem nepoznatih koeficijenata polinoma q ili iz asimptotskog razvoja od $\sqrt{p}$.

Pretpostavimo sada da je $p(x) = \prod_{i=1}^{2n}(x - a_i)$, gdje su $a_1, \ldots, a_{2n}$ različiti racionalni brojevi. Tada na krivulji

$$C: \quad y^2 = r(x)$$

leže točke $(a_i, \pm q(a_i))$, $i = 1, \ldots, 2n$. Ako je $\deg r = 3$ ili 4, te $r(x)$ nema višestrukih korijena, onda C predstavlja eliptičku krivulju. Za $\deg r = 3$ to je sasvim jasno. Ako je $\deg r = 4$, onda izaberemo jednu racionalnu točku na C (npr. $(a_1, q(a_1))$) za točku u beskonačnosti i transformiramo C u eliptičku krivulju.

Za $n = 5$ gotovo svi izbori a_i-ova daju $\deg r = 4$. Tada C ima 10 racionalnih točaka oblika $(a_i, q(a_i))$ i možemo očekivati da ćemo dobiti eliptičku krivulju ranga

≥ 9. Mestre je konstruirao familiju eliptičkih krivulja (tj. eliptičku krivulju nad poljem racionalnih funkcija $\mathbb{Q}(t)$) ranga ≥ 11, tako da je uzeo $n = 6$ i $a_i = b_i + t$, $i = 1, \ldots, 6$; $a_i = b_{i-6} - t$, $i = 7, \ldots, 12$. Sada polinom $r(x)$ općenito ima stupanj 5. Zato možemo pokušati izabrati brojeve $b_1, \ldots, b_6$ tako da koeficijent uz x^5 bude jednak 0. U prvom Mestreovu primjeru iz 1991. godine bilo je $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$.

Poslije su Mestre, Nagao i Kihara, koristeći se sličnim konstrukcijama, poboljšali ovaj rezultat te konstruirali krivulje nad $\mathbb{Q}(t)$ ranga 14. Godine 2006., koristeći se bitno drugačijim metodama, koje svoje izvorište imaju u algebarskoj geometriji, Elkies je uspio konstruirati krivulju nad $\mathbb{Q}(t)$ ranga 18. Sve ove krivulje imaju trivijalnu torzijsku grupu. Fermigier, Kulesz, Lecacheux i Nagao su modificirali Mestreovu metodu te dobili familije krivulja s (relativno) velikim rangom i netrivijalnom torzijskom grupom. Kao što ćemo kasnije vidjeti, eliptičke krivulje povezane s Diofantovim m-torkama također mogu poslužiti za konstrukciju eliptičkih krivulja (nad $\mathbb{Q}$ i $\mathbb{Q}(t)$) velikog ranga za torzijske grupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$, $k = 2, 4, 6, 8$.

U drugoj fazi, "sijanju", gruba ideja je da je izglednije da će krivulja imati "puno" racionalnih točaka (tj. veliki rang) ako ima puno točaka pri redukciji modulo p (tj. ako je broj $N_p = |E(\mathbb{F}_p)|$ velik) za "većinu" p-ova. Napomenimo da po Hasseovu teoremu vrijedi

$$p + 1 - 2\sqrt{p} \leq N_p \leq p + 1 + 2\sqrt{p},$$

pa to da je broj N_p velik, zapravo znači da je blizu gornje ograde iz Hasseova teorema.

Puno preciznija verzija ove grube ideje je poznata *Birch i Swinnerton-Dyerova (BSD) slutnja*

$$\prod_{p \leq X,\, p \nmid 2\Delta} \frac{N_p}{p} \sim const \cdot (\ln X)^r,$$

gdje je $r = \text{rank}(E)$. BSD-slutnja se obično iskazuje s pomoću L-funkcije, koja je definirana s

$$L(E, s) = \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \cdot \prod_{p \mid \Delta} \left(1 - a_p p^{-s}\right)^{-1},$$

gdje je $a_p = p + 1 - N_p$ za p-ove u kojima E ima dobru redukciju, $a_p = 0$ u slučaju aditivne redukcije, $a_p = 1$ u slučaju multiplikativne rascjepive, a $a_p = -1$ u slučaju multiplikativne nerascjepive redukcije. Ovu funkciju možemo shvatiti kao analogon Riemannove zeta-funkcije i Dirichletove L-funkcije ako se prisjetimo Eulerove formule $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$. Funkcija $L(E, s)$ ima analitičko produljenje na cijelu kompleksnu ravninu $\mathbb{C}$ te zadovoljava funkcionalnu jednadžbu

$$\Lambda(s) = w_E \cdot \Lambda(2 - s),$$

gdje je $w_E \in \{-1, 1\}$, dok je

$$\Lambda(s) = N^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s),$$

gdje je Γ gama funkcija, a N označava konduktor od E.

Sada se BSD-slutnja može iskazati tako da je red iščezavanja od $L(E, s)$ u $s = 1$ (tzv. *analitički rang* od E) jednak rangu r, tj. da je

$$L(E, s) = c \cdot (s - 1)^r + \text{članovi višeg reda},$$

gdje je $c \neq 0$ konstanta. Poznato je da slutnja vrijedi ako je analitički rang jednak 0 ili 1 (Kolyvagin, 1989.).

Slutnja je da vrijednost w_E određuje parnost ranga: $w_E = (-1)^r$, tj. ako je $w_E = 1$, onda je rang paran, a ako je $w_E = -1$, onda je rang neparan (to se naziva "Parity Conjecture" i omogućava nam da uvjetno odredimo rang u slučajevima kad ostalim metodama dobijemo zaključak da je $r \in \{r', r'+1\}$ za neki r'). Vrijednost w_E se može izračunati u PARI-ju s pomoću funkcije `ellrootno`.

Iako je sama Birch i Swinnerton-Dyerova slutnja vrlo važna za razumijevanje ranga eliptičkih krivulja, ona uglavnom nije prikladna za izravno računanje (makar uvjetno) ranga. Zato se u fazi "sijanja" obično rabe neke druge varijacije gore spomenute grube ideje.

Možemo fiksirati konačan skup prostih brojeva $\mathcal{P}$, pa za svaki $p \in \mathcal{P}$ naći sve vrijednosti parametara modulo p koje maksimiziraju N_p. Ako promatramo krivulju oblika $y^2 = x^3 + ax + b$, parametri će biti $(a, b) \in \mathbb{F}_p^2$, a maksimalni N_p je $p + 1 + \lfloor 2\sqrt{p} \rfloor$. Ako tražimo krivulje velikog ranga sa zadanom torzijskom grupom, onda se koristimo odgovarajućim prije navedenim parametrizacijama, a maksimalni N_p je $|E(\mathbb{Q})_{\text{tors}}| \cdot \left\lfloor \frac{p+1+\lfloor 2\sqrt{p} \rfloor}{|E(\mathbb{Q})_{\text{tors}}|} \right\rfloor$. Nakon toga, s pomoću Kineskog teorema o ostatcima, konstruiramo listu s parametrima koji maksimiziraju N_p za sve $p \in \mathcal{P}$. Ovo se naziva metoda konačnog polja.

Mestre i Nagao su dali heurističke argumente (motivirane BSD-slutnjom) koji sugeriraju da bi za krivulje velikog ranga određene sume trebale poprimati velike vrijednosti (najveće u promatranoj familiji). Neke od tih suma su

$$S_1(X) = \sum_{p \leq X} \frac{N_p + 1 - p}{N_p} \ln p,$$
$$S_2(X) = \sum_{p \leq X} \frac{N_p + 1 - p}{N_p},$$
$$S_3(X) = \sum_{p \leq X} (N_p - p - 1) \ln p.$$

U primjenama ove ideje izabere se nekoliko prirodnih brojeva $X_1 < X_2 < \cdots < X_k$, pa se računa $S_i(X_1)$, $S_i(X_2), \ldots$ ali tako da se u svakom koraku odbaci, recimo, 80 % "najlošijih" krivulja, tj. onih s najmanjom vrijednosti pripadne sume. Uočimo da za efikasnu implementaciju ove metode X_k ne bi smio biti prevelik (recimo $X_k < 100000$) jer nemamo vrlo efikasan algoritam za računanje N_p za jako velike p-ove. U PARI-ju se broj a_p može izračunati s pomoću funkcije `ellap`(E, p), pa se N_p dobije kao $N_p = p + 1 - a_p$.

Pogledajmo koji heuristički argument povezuje sumu $S_1(N)$ i BSD slutnju. BSD slutnja povlači da je $L(E, s) = L(s) = (s-1)^r \cdot g(s)$, gdje je $g(1) \neq 0$. (U stvari, preciznija verzija BSD slutnje točno predviđa čemu je jednako $g(1)$. U opisu, se pored ostalih veličina, pojavljuju redovi torzijske i Tate-Šafarevićeve grupe, te regulator.) Logaritamska derivacija daje

$$\frac{L'(s)}{L(s)} = \frac{r}{s-1} + \frac{g'(s)}{g(s)},$$

Dakle, očekujemo da logaritamska derivacija od L kad s teži u 1 brže teži u besko-

načno što je rang veći. Sada ćemo promotriti produkt

$$L(s,N)=\prod_{p\leq N}(1-a_pp^{-s}+p^{1-2s})^{-1}$$

koji se od $L(s)$ razlikuje po tome što smo produkt "prerezali" u N, te što smo ignorirali razliku u faktorima između prostih brojeva s dobrom i lošom redukcijom. Stavimo $f(s,N)=\log L(s,N)$. Tada je

$$f'(s,N)=-\sum_{p\leq N}\frac{a_pp^{-s}-2p^{1-2s}}{1-a_pp^{-s}+p^{1-2s}}\log p.$$

Čini se da je razumno uzeti da je $\lim_{N\to\infty}f'(s,N)$ dobra aproksimacija za $\frac{L'(s)}{L(s)}$. Stoga brzina divergencije limesa

$$\lim_{s\to 1}\lim_{N\to\infty}f'(s,N) \tag{2.35}$$

može biti indikator veličine ranga. Kad bismo smjeli zamijeniti poredak limesa u (2.35), dobili bismo upravo

$$\lim_{N\to\infty}f'(1,N)=\lim_{N\to\infty}-\frac{a_p-2}{p+1-a_p}\log p=\lim_{N\to\infty}S_1(N),$$

čime smo pokazali najavljenu vezu između BSD slutnje i sume $S_1(N)$.

Vidjeli smo prije da u slučaju kada E ima racionalnu točku reda 2, imamo vrlo jednostavnu gornju ogradu za rang: $r\leq\omega(b)+\omega(b')-1$, a također i $r\leq s$, gdje je s Selmerov rang. Općenito, u slučaju kada E ima točku konačnog reda moguće je dati jednostavnu gornju ogradu za rang. Ako imamo sreće da se ta gornja ograda podudara s donjom ogradom koju dobijemo pretragom za točkama s malom visinom, na taj način možemo dobiti egzaktnu vrijednost za rang bez potrebe za primjenom zahtjevnijih metoda. Spomenuta gornja ograda se naziva *Mazurova ograda*. Neka je E eliptička krivulja nad $\mathbb{Q}$ zadana svojom minimalnom Weierstrassovom jednadžbom te neka E ima racionalnu točku neparnog prostog reda p. Tada vrijedi

$$r\leq m_p=b+a-m-1,$$

gdje je

- b broj prostih brojeva s lošom redukcijom;
- a broj prostih brojeva s aditivnom redukcijom;
- m broj prostih brojeva q s multiplikativnom redukcijom za koje dodatno vrijedi da p ne dijeli eksponent od q u Δ i da je $q\not\equiv 1\pmod p$.

Primjer 2.10 (Dujella-Lecacheux, 2001.)**.** *Izračunajmo rang krivulje E zadane jednadžbom*

$$y^2+y=x^3+x^2-1712371016075117860x+885787957535691389512940164.$$

Rješenje: Imamo

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (888689186, 8116714362487),$$
$$(-139719349, -33500922231893), (-139719349, 33500922231892),$$
$$(888689186, -8116714362488)\} \cong \mathbb{Z}/5\mathbb{Z}.$$

Zato možemo izračunati Mazurovu ogradu m_5. Diskriminanta je

$$\Delta = -3^{15} \cdot 5^5 \cdot 7^5 \cdot 11^5 \cdot 19^5 \cdot 41^5 \cdot 127^5 \cdot 1409 \cdot 10864429,$$

pa imamo: $b = 9$, $a = 0$, $m = 2$ te dobivamo da je $r \leq m_5 = 6$.

Pretragom za točkama $P = (x, y)$ na E s cjelobrojnim koordinatama i $|x| < 10^9$ (u PARI-ju se to može napraviti pomoću funkcije `ellratpoints`), nalazimo sljedećih 6 nezavisnih točaka modulo $E(\mathbb{Q})_{\text{tors}}$ (o tome kako provjeriti nezavisnost točaka, bit će riječi u sljedećem potpoglavlju):

$$(624069446, 7758948474007), (763273511, 4842863582287)$$
$$(680848091, 5960986525147), (294497588, 20175238652299)$$
$$(-206499124, 35079702960532), (676477901, 6080971505482),$$

čime smo dokazali da je $\text{rank}(E) = 6$ (ovo je u trenutku pronalaska bila krivulja najvećeg poznatog ranga s torzijskom grupom $\mathbb{Z}/5\mathbb{Z}$). $\diamondsuit$

Ako primjenom gore navedenih metoda, gornja ograda za rang bude veća od donje barem za 2, tako da ni uz informaciju o uvjetnoj parnost ranga ne možemo odrediti rang, možemo pokušati dodatno povećati donju ogradu ili smanjiti gornju. Za povećanje donje ograde, možemo povećati granicu do koje algoritmi traže točke na krivulji odnosno odgovarajućim jednadžbama četvrtog stupnja. U PARI-ju se to može napraviti tako da se koristi dodatni parametar u funkciji `ellrank`, primjerice `ellrank`$(e, 6)$, dok se u MWRANK-u to može napraviti pomoću opcije `-b`, primjerice `-b 12` (dodatna korisna, a i nužna kod krivulja s vrlo velikim koeficijentima, je opcija `-p` koja povećava zadanu preciznost).

Za dobivanje gornje ograde za rang (ili smanjivanje one prethodno dobivene), može se koristiti Mestreova uvjetna gornja ograda (Mestre, 1986.), koja daje gornju ogradu za rang uz pretpostavku da vrijede Birch i Swinnerton-Dyerova slutnja i generalizirana Riemannova slutnja:

$$\text{rank} \leq \frac{\pi^2}{8\lambda}\Big(\log N - 2\sum_{p^m \leq e^\lambda} b(p^m) F_\lambda(m \log p) \frac{\log p}{p^m} - M_\lambda\Big),$$

gdje je N konduktor, $b(p^m) = a_p^m$ ako $p \mid N$, $b(p^m) = \alpha_p^m + \alpha_p'^m$ ako $p \nmid N$, gdje su α_p, α_p' korijeni od $x^2 - a_p x + p$,

$$M_\lambda = 2\Big(\log 2\pi + \int_0^{+\infty} (F_\lambda(x)/(e^x - 1) - e^{-x}/x)dx\Big),$$

$F_\lambda(x) = F(x/\lambda)$, dok je F funkcija s određenim svojstvima, za koju se može uzeti primjerice $F(x) = (1 - |x|)\cos(\pi x) + \sin(\pi|x|)/\pi$ za $x \in [-1, 1]$ i $F(x) = 0$ inače. Primjerice, za rekordnu Elkiesovu krivulju ranga ≥ 28, Mestreova ograda daje da je rank ≤ 30, dok za prethodnu rekordnu krivulju ranga ≥ 24 daje da je rang točno jednak 24 (uz pretpostavku da vrijede BSD i GRH) (Bober, 2011.).

Neka je T jedna od 15 mogućih torzijskih grupa za eliptičku krivulju nad $\mathbb{Q}$ (prema Mazurovu teoremu). Definiramo

$$B(T) = \sup\{\text{rank}(E(\mathbb{T})) \,:\, E(\mathbb{Q})_{\text{tors}} = T\}.$$

I ovdje je postojala slutnja da je $B(T)$ neograničeno za sve T, no kao što smo već spomenuli, postoje nedavni članci koji sugeriraju ograničenost ranga, pa time i veličina $B(T)$. Danas znamo tek da je $B(T) \geq 3$ za sve T. U sljedećoj tablici su dani trenutačno najbolje poznate donje ograde za $B(T)$. Crvenom bojom su označeni rangovi koji se mogu dobiti pomoću eliptičkih krivulja induciranih racionalnim Diofantovim trojkama. Detalji o rekordnim krivuljama se mogu naći na *web* stranici `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`.

T	$B(T) \geq$	autori
0	28	Elkies (2006.)
$\mathbb{Z}/2\mathbb{Z}$	20	Elkies & Klagsbrun (2020.)
$\mathbb{Z}/3\mathbb{Z}$	15	Elkies & Klagsbrun (2020.)
$\mathbb{Z}/4\mathbb{Z}$	13	Elkies & Klagsbrun (2020.)
$\mathbb{Z}/5\mathbb{Z}$	9	Klagsbrun (2020.)
$\mathbb{Z}/6\mathbb{Z}$	9	Klagsbrun (2020.), Voznyy (2020.)
$\mathbb{Z}/7\mathbb{Z}$	6	Klagsbrun (2020.)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006.), Dujella, MacLeod & Peral (2013.), Voznyy (2021.)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009.), van Beek (2015.), Dujella & Petričević (2021.), Dujella, Petričević & Rathbun (2022.)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005., 2008.), Elkies (2006.), Fisher (2016.)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	**9**	Dujella & Peral (2012., 2019.), Klagsbrun (2020.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	**6**	Elkies (2006.), Dujella, Peral & Tadić (2015.), Dujella & Peral (2020.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	**3**	Connell (2000.), Dujella (2000., 2001., 2006., 2008.), Campbell & Goins (2003.), Rathbun (2003., 2006., 2013.), Dujella & Rathbun (2006.), Flores, Jones, Rollick, Weigandt & Rathbun (2007.), Fisher (2009.), AttarBashi, Rathbun & Voznyy (2022.)

Rekli smo da je prvi korak u nalaženju eliptičkih krivulja velikog ranga (pa onda i onih s nekim dodatnim svojstvom, poput torzijske grupe), konstrukcija familija eliptičkih krivulja (najčešće su to eliptičke krivulje nad poljem racionalnih funkcija $\mathbb{Q}(t)$) relativno velikog "generičkog" ranga. Stoga su od interesa sljedeće veličine:

$$G(T) = \sup\{\text{rank}\, E(\mathbb{Q}(t)) \,:\, E(\mathbb{Q}(t))_{\text{tors}} \cong T\},$$
$$C(T) = \limsup\{\text{rank}\, E(\mathbb{Q}) \,:\, E(\mathbb{Q})_{\text{tors}} \cong T\}.$$

U slučaju kad je u dolje navedenim tablicama $C(T) > G(T)$, to znači da trenutni rekord za $C(T)$ dolazi od familije parametrizirane racionalnim točkama na nekoj eliptičkoj krivulji pozitivnog ranga. I ovdje su crvenom bojom označeni rangovi koji dolaze od eliptičkih krivulja induciranih racionalnim Diofantovim trojkama.

T	$G(T) \geq$	autori
0	18	Elkies (2006.)
$\mathbb{Z}/2\mathbb{Z}$	11	Elkies (2009.)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007.)
$\mathbb{Z}/4\mathbb{Z}$	5	Kihara (2004.), Elkies (2007.), Dujella, Peral & Tadić (2014.), Khoshnam & Moody (2016.)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001.), Eroshkin (2009.), MacLeod (2014.)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001.), Kihara (2006.), Eroshkin (2008.), Woo (2008.), Dujella & Peral (2012., 2020.), MacLeod (2014., 2015.), Voznyy (2021)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998.), Lecacheux (2003.), Rabarison (2008.), Harrache (2009.), MacLeod (2014.)
$\mathbb{Z}/8\mathbb{Z}$	2	Dujella & Peral (2012.), MacLeod (2013.) Dujella, Kazalicki & Peral (2021.)
$\mathbb{Z}/9\mathbb{Z}$	0	Kubert (1976.)
$\mathbb{Z}/10\mathbb{Z}$	0	Kubert (1976.)
$\mathbb{Z}/12\mathbb{Z}$	0	Kubert (1976.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	7	Elkies (2007.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	**4**	Dujella & Peral (2012.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	**2**	Dujella & Peral (2012., 2015., 2017.), MacLeod (2013.) Dujella, Kazalicki & Peral (2021.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	**0**	Kubert (1976.)

T	$C(T) \geq$	PPVW	autori
0	19	21	Elkies (2006.)
$\mathbb{Z}/2\mathbb{Z}$	11	13	Elkies (2007.)
$\mathbb{Z}/3\mathbb{Z}$	7	9	Elkies (2007.)
$\mathbb{Z}/4\mathbb{Z}$	6	7	Elkies (2007.)
$\mathbb{Z}/5\mathbb{Z}$	4	5	Eroshkin (2009.)
$\mathbb{Z}/6\mathbb{Z}$	**5**	5	Eroshkin (2009.)
$\mathbb{Z}/7\mathbb{Z}$	2	3	Lecacheux (2003.), Elkies (2006.), Rabarison (2008.), Harrache (2009.)
$\mathbb{Z}/8\mathbb{Z}$	**3**	3	Dujella & Peral (2012.), Dujella, Kazalicki & Peral (2021.)
$\mathbb{Z}/9\mathbb{Z}$	1	2	Atkin & Morain (1993.), Kulesz (1998.), Rabarison (2008.), Gasull, Manosa & Xarles (2010.)
$\mathbb{Z}/10\mathbb{Z}$	1	2	Atkin & Morain (1993.), Kulesz (1998.), Rabarison (2008.)
$\mathbb{Z}/12\mathbb{Z}$	1	2	Suyama (1985.), Kulesz (1998.), Rabarison (2008.), Halbeisen, Hungerbühler, Voznyy & Zargar (2021.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8	9	Elkies (2007.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	**5**	5	Eroshkin (2009.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	**3**	3	Dujella & Peral (2013.), Dujella, Kazalicki & Peral (2021)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1	2	Atkin & Morain (1993.), Kulesz (1998.), Lecacheux (2002.), Campbell & Goins (2003.), Rabarison (2008.)

Postoje i preciznija previđanja o tome koliko velik može biti rang uz zadanu torzijsku grupu. Možda je zanimljivo spomenuti da je u članku Park, Poonen, Voight, Wood (2019.) navedeno predviđanje da samo konačno mnogo eliptičkih krivulja s torzijskim grupama $\mathbb{Z}/8\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ima rang ≥ 4. S druge strane, Dujella i Peral (2015.) su dokazali da postoji beskonačno mnogo eliptičkih krivulja s tim torzijskim grupama i rangom ≥ 3, pa ako je gore navedeno predviđanje točno, ovaj rezultat bi za te torzijske grupe bio najbolji mogući. Slično vrijedi za rezultate koje je za torzijske grupe $\mathbb{Z}/6\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ dobio Eroshkin (2009.). Ta četiri "granična" ranga su u tablici označeni plavom bojom. Općenito, predviđanje je da samo konačno mnogo (neizomorfnih) krivulja s danom torzijskom grupom ima rang veći od onog navedenog u stupcu PPVW. Spomenimo i da su u članku Dujella, Kazalicki, Peral (2021.) dane dodatne beskonačne familije s rangom ≥ 3 i torzijskom grupom $\mathbb{Z}/8\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, te eksperimenti koji sugeriraju da bi moglo postojati beskonačno mnogo krivulja s ovim torzijskim grupama i rangom ≥ 4.

Montgomery (1987.) te Atkin i Morain (1993.) su predložili su korištenje eliptičkih krivulja nad $\mathbb{Q}$ s velikom torzijskom grupom i pozitivnim rangom da bi se povećala šansa za uspjeh Lenstrinog algoritma za faktorizaciju velikih prirodnih brojeva. U pozadini te ideje je Propozicija 2.4 koja povlači da je $|E(\mathbb{F}_p)|$ djeljiv s redom torzijske grupe od $E(\mathbb{Q})$, pa veća torzijska grupa od $E(\mathbb{Q})$ povećava vjerojatnost da će red $|E(\mathbb{F}_p)|$ imati male proste faktore, što je važno za uspjeh Lenstrinog algoritma. Nadalje, pokazuje se da dodatnu prednost možemo dobiti koristeći se eliptičkim krivuljama koje imaju još veću torzijsku grupu nad nekim poljem algebarskih brojeva malog stupnja. Tu se postavlja pitanje koje su torzijske grupe moguće, primjerice, nad kvadratnim ili kubnim poljima.

U kvadratnim poljima Kenku i Momose (1988.) te Kamienny (1992.) su dokazali da se može pojaviti točno sljedećih 26 grupa:

$$\begin{aligned} \mathbb{Z}/k\mathbb{Z}, &\quad 1 \leq k \leq 18,\ k \neq 17, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, &\quad 1 \leq k \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3k\mathbb{Z}, &\quad k = 1, 2, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. & \end{aligned} \tag{2.36}$$

Slično kao kod Mazurova teorema, i ovdje se svaka od ovih 26 grupa pojavljuje kao torzijska grupa nad nekim kvadratnim poljem za beskonačno mnogo neizomorfnih eliptičkih krivulja. Kod kubnih polja situacija je drugačija. Naime, Najman (2016.) je dokazao da postoji jedinstvena krivulja s torzijskom grupom $\mathbb{Z}/21\mathbb{Z}$ nad nekim kubnim poljem. Za svaku od 26 grupa iz (2.36) postoji eliptička krivulja nad nekim kvadratnim poljem s tom torzijskom grupom i pozitivnim rangom (štoviše, i s rangom ≥ 2). Trenutni rekordni rangovi se mogu naći na web stranici
`https://web.math.pmf.unizg.hr/~duje/tors/torsquad.html`.

2.6 Kanonska visina i Mordell-Weilova baza

Dva osnovna koraka u dokazu Mordell-Weilova teorema su

- dokaz da je indeks $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ konačan;
- svojstva *visine* h, definirane s $h(P) = \ln H(x)$, gdje je $P = (x, y)$ i $H(\frac{m}{n}) = \max\{|m|, |n|\}$, dok je $h(\mathcal{O}) = 0$.

Funkcija H se katkad naziva i "naivna" visina, a h logaritamska visina. Očito je da je za svaku konstantu C skup

$$\{P \in E(\mathbb{Q}) : h(P) \leq C\}$$

konačan (nema više od $2(2e^C + 1)^2$ elemenata).

Želimo vidjeti koja je veza između visina točaka P i $2P$ (ugrubo koliko se puta poveća broj znamenaka u prikazu točke $2P$ u odnosu na prikaz točke P). Neka je krivulja dana jednadžbom $y^2 = x^3+ax+b$ i $P = (x, y) \in E(\mathbb{Q})$. Tada je x-koordinata točke $2P$

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}.$$

Budući da se kvadriranjem broja njegova visina udvostručuje, a najveća potencija od x koja se pojavljuje u izrazu od $x(2P)$ je x^4, zaključujemo da je $h(2P) \approx 4h(P)$.

Još bolja i važnija svojstva ima *kanonska* ili *Néron-Tateova visina* $\hat{h}$, čija je definicija

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}. \tag{2.37}$$

Može se pokazati da za kanonsku visinu vrijedi $\hat{h}(2P) = 4\hat{h}(P)$ i, općenitije, $\hat{h}(mP) = m^2\hat{h}(P)$. Nadalje, funkcija $\hat{h}$ ima još i sljedeća svojstva:

- Za sve $P \in E(\mathbb{Q})$ vrijedi $\hat{h}(P) \geq 0$. Pritom jednakost $\hat{h}(P) = 0$ vrijedi ako i samo ako je $P \in E(\mathbb{Q})_{\text{tors}}$.
- Za svaku konstantu C je skup $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq C\}$ konačan.
- Za sve $P, Q \in E(\mathbb{Q})$ vrijedi "relacija paralelograma"

$$\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q). \tag{2.38}$$

Skicirajmo sada dokaz Mordell-Weilova teorema (uz pretpostavku da je indeks $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ konačan, o čemu smo nešto rekli (barem u specijalnom slučaju krivulja s točkom reda 2) u prethodnom potpoglavlju).

Neka je $\{R_1, R_2, \ldots, R_n\}$ skup reprezentanata iz $E(\mathbb{Q})/2E(\mathbb{Q})$, tj.

$$E(\mathbb{Q}) = (R_1 + 2E(\mathbb{Q})) \cup (R_2 + 2E(\mathbb{Q})) \cup \cdots \cup (R_n + 2E(\mathbb{Q})), \tag{2.39}$$

te neka je $k = \max_i(\hat{h}(R_i))$. Neka su $Q_1, \ldots, Q_m$ sve točke iz $E(\mathbb{Q})$ za koje je $\hat{h}(Q_i) \leq k$ (znamo da je skup takvih točaka konačan). Neka je G podgrupa od $E(\mathbb{Q})$ generirana točkama

$$R_1, \ldots, R_n, Q_1, \ldots, Q_m.$$

Tvrdimo da je $G = E(\mathbb{Q})$. Pretpostavimo suprotno, tj. da postoji $P \in E(\mathbb{Q})$ takav da $P \notin G$. Budući da postoji samo konačno mnogo točaka s kanonskom visinom manjom od $\hat{h}(P)$, bez smanjenja općenitosti možemo pretpostaviti da je P točka s najmanjom visinom za koju vrijedi $P \notin G$. Iz (2.39) imamo da za neki indeks i i točku $P_1 \in E(\mathbb{Q})$ vrijedi

$$P = R_i + 2P_1.$$

Iz navedenih svojstava kanonske visine te zbog činjenice da je $\hat{h}(P) > k$ (zato što je $P \neq Q_i$), imamo

$$\begin{aligned} 4\hat{h}(P_1) = \hat{h}(2P_1) = \hat{h}(P - R_i) &= 2\hat{h}(P) + 2\hat{h}(R_i) - \hat{h}(P + R_i) \\ &\leq 2\hat{h}(P) + 2k < 2\hat{h}(P) + 2\hat{h}(P) = 4\hat{h}(P). \end{aligned}$$

Dakle, $\hat{h}(P_1) < \hat{h}(P)$, pa budući da je P točka s najmanjom kanonskom visinom koja nije u G, to mora biti da je $P_1 \in G$. No tada je i $P = R_i + 2P_1 \in G$, pa smo dobili kontradikciju. Stoga je $G = E(\mathbb{Q})$, što dokazuje da je grupa $E(\mathbb{Q})$ konačno generirana. □

Računanje kanonske visine $\hat{h}(P)$ po definiciji (preko limesa) je problematično jer zahtjeva računanje vrlo velikih cijelih brojeva koji se javljaju u brojniku i nazivniku točaka $x(2^n P)$, a moramo ih egzaktno izračunati jer nam u idućem koraku trebaju vrijednosti brojnika i nazivnika nakon eventualnih kraćenja (a samo iz približnih vrijednosti ne možemo znati koja će kraćenja nastupiti). Silverman je 1988. godine dao efikasniji algoritam za računanje kanonske visine. Ideja je prikazati "globalnu visinu" $\hat{h}(P)$ kao sumu "lokalnih visina" $\hat{h}_p(P)$, gdje je p prosti broj ili je $p = \infty$. U PARI-ju je taj algoritam implementiran u funkciji `ellheight`.

Relacija paralelograma (2.38) sugerira da ćemo, analogno kao u slučaju norme koja zadovoljava istoimenu relaciju, s pomoću kanonske visine moći definirati neku varijantu "skalarnog produkta".

Definicija 2.1. Néron-Tateovo sparivanje visina *točaka* $P, Q \in E(\mathbb{Q})$ *je*

$$\begin{aligned} \langle P, Q \rangle &= \frac{1}{2}(\hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q)) \\ &= \frac{1}{4}(\hat{h}(P + Q) - \hat{h}(P - Q)). \end{aligned}$$

Iz $\hat{h}(2P) = 4\hat{h}(P)$ slijedi da je $\hat{h}(P) = \langle P, P \rangle$. Néron-Tateovo sparivanje visina je očito simetrično, a nije teško pokazati (primjenom relacije paralelograma) da je i bilinearno.

Propozicija 2.5. *Ako je T torzijska točka, a P bilo koja točka na $E(\mathbb{Q})$, onda vrijedi*

$$\hat{h}(P + T) = \hat{h}(P) \;\; i \;\; \langle P, T \rangle = 0.$$

Dokaz: Neka je T točka reda m. Tada je

$$\hat{h}(P + T) = \frac{\hat{h}(m(P + T))}{m^2} = \frac{\hat{h}(mP)}{m^2} = \hat{h}(P),$$

pa je

$$\langle P, T \rangle = \frac{1}{2}(\hat{h}(P) - \hat{h}(P) - 0) = 0.$$ □

Definirat ćemo sada analogon Gramove determinante skalarnih produkata.

Definicija 2.2. Determinanta visina *točaka* $P_1, \ldots, P_m$ *je* $\det(\langle P_i, P_j \rangle)$.

U PARI-ju se determinanta visina može izračunati s pomoću funkcije `ellheightmatrix`.

Vrijedi da je

$$\hat{h}(n_1P_1 + \cdots + n_mP_m) = N(\langle P_i, P_j\rangle)N^\tau,$$

gdje je $N = (n_1, \ldots, n_m)$.

Nadalje, točke $P_1, \ldots, P_m$ su zavisne mod $E(\mathbb{Q})_{\text{tors}}$, tj. postoje cijeli brojevi $n_1, \ldots, n_m$ koji nisu svi jednaki 0 tako da je $n_1P_1 + \cdots + n_mP_m \in E(\mathbb{Q})_{\text{tors}}$ ako i samo ako je $\det(\langle P_i, P_j\rangle) = 0$.

Posebno važan slučaj nezavisnih točaka je Mordell-Weilova baza. *Mordell-Weilova baza* $Q_1, \ldots, Q_r$ za $E(\mathbb{Q})$ je $\mathbb{Z}$-baza za $E(\mathbb{Q})$ mod $E(\mathbb{Q})_{\text{tors}}$, tj. svaki $P \in E(\mathbb{Q})$ se na jedinstven način može prikazati kao

$$P = n_1Q_1 + \cdots + n_rQ_r + T, \;\; n_i \in \mathbb{Z}, \;\; T \in E(\mathbb{Q})_{\text{tors}}.$$

Regulator od E je $\mathrm{Reg}(E) = \det(\langle Q_i, Q_j\rangle)$, gdje je $Q_1, \ldots, Q_r$ Mordell-Weilova baza. Ako je $r = 0$, onda se definira da je $\mathrm{Reg}(E) = 1$. Iz nezavisnosti točaka u bazi slijedi da je $\mathrm{Reg}(E) \neq 0$, no može se pokazati da uvijek vrijedi $\mathrm{Reg}(E) > 0$.

Neka su $P_1, \ldots, P_r$ r nezavisnih točaka mod $E(\mathbb{Q})_{\text{tors}}$, te pretpostavimo da $\{P_1, \ldots, P_r\} \cup E(\mathbb{Q})_{\text{tors}}$ generira podgrupu G od $E(\mathbb{Q})$ indeksa q. Tada je

$$\det(< P_i, P_j >) = q^2 \,\mathrm{Reg}(E).$$

Dakle, $\mathrm{Reg}(E)$ je najmanja determinanta visina od r nezavisnih točaka na $E(\mathbb{Q})$. Nadalje, r nezavisnih točaka čini bazu ako i samo ako im je determinanta visina jednaka regulatoru.

Ako je poznata Mordell-Weilova baza $P_1, \ldots, P_r$ eliptičke krivulje (ili barem neki nezavisan skup točaka), često je od interesa pronaći bazu (ili skup točaka koji generira istu podgrupu kao polazni skup točaka) s elementima sa što manjim (kanonskim) visinama. Za to se može iskoristiti LLL-algoritam, gdje će ulogu Gramove matrice odigrati matrica visina $(< P_i, P_j >)$. Tu je ideju iznio i realizirao Rathbun 2003. godine.

Recimo naprije nešto kratko o LLL-algoritmu koji je povezan s problemom nalaženja najkraćeg nenul-vektora u rešetki.

Neka je n prirodni broj te neka su $b_1, \ldots, b_n$ linearno nezavisni vektori u $\mathbb{R}^n$. *Rešetka* ($\mathbb{Z}$-modul) L razapeta ovim vektorima je skup svih njihovih cjelobrojnih linearnih kombinacija

$$L = \left\{ \sum_{i=1}^{n} x_i \, b_i \;:\; x_i \in \mathbb{Z} \right\}.$$

Kaže se da je $B = \{b_1, \ldots, b_n\}$ *baza rešetke* L. Npr. u $\mathbb{R}^2$, ako je $b_1 = (1, 0)$, $b_2 = (0, 1)$, onda je L rešetka svih točaka u ravnini s cjelobrojnim koordinatama.

Jedna rešetka može imati više različitih baza, pa se pitamo možemo li izabrati bazu koja bi imala neko dodatno dobro svojstvo. Jasno je da B predstavlja bazu vektorskog prostora $\mathbb{R}^n$. Znamo da Gram-Schmidtovim postupkom možemo dobiti ortogonalnu bazu za isti vektorski prostor ($b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*$, $i = 1, \ldots, n$, gdje je $\mu_{ij} = \frac{\langle b_i, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle}$). No ta nova baza ne mora razapinjati istu rešetku kao polazna baza B jer koeficijenti μ_{ij} ne moraju biti cijeli brojevi. Općenito, rešetka i ne mora imati ortogonalnu bazu. A. K. Lenstra, H. W. Lenstra i L. Lovász uveli su 1982. godine pojam *LLL-reducirane baze*, koja ima svojstva:

1) $|\mu_{i,j}| \leq \frac{1}{2}$, $1 \leq j < i \leq n$;

2) $\|b_i^*\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|b_{i-1}^*\|^2$.

Prvi uvjet se može interpretirati tako da se kaže da je LLL-reducirana baza "gotovo ortogonalna", dok drugi uvjet govori da niz normi vektora $\|b_i^*\|$ "gotovo raste". Dodatno važno svojstvo LLL-reducirane baze je da je prvi vektor u toj bazi vrlo kratak, tj. ima malu normu. Može se dokazati da uvijek vrijedi da je $\|b_1\| \leq 2^{(n-1)/2}\|x\|$, za sve nenul-vektore $x \in L$, no u primjenama se vrlo često događa da je $\|b_1\|$ upravo najkraći nenul-vektor iz L.

U svom članku iz 1982. godine A. K. Lenstra, H. W. Lenstra i L. Lovász prikazali su polinomijalni algoritam za konstrukciju LLL-reducirane baze iz proizvoljne baze rešetke (prema njima nazvan *LLL-algoritam*). Algoritam je ubrzo našao brojne primjene, npr. u faktorizaciji polinoma s racionalnim koeficijentima, kriptoanalizi kriptosustava RSA s malim javnim ili tajnim eksponentom, problemu ruksaka te diofantskim aproksimacijama i diofantskim jednadžbama.

De Weger je 1989. godine predložio varijantu LLL-algoritma koja se koristi samo cjelobrojnom aritmetikom (ako su ulazni podaci cjelobrojni) te izbjegava probleme vezane uz numeričku stabilnost algoritma.

U programskom paketu PARI je LLL-algoritam implementiran s pomoću funkcije `qflll`(x), koja kao rezultat vraća transformacijsku matricu T takvu da je xT LLL-reducirana baza rešetke generirane stupcima matrice x. Postoji i funkcija `qflllgram`(x), koja radi isto što i `qflll`, osim što je ovdje x Gramova matrica skalarnih produkata vektora rešetke, a ne matrica koordinata vektora. Rezultat je ponovo transformacijska matrica T čiji stupci daju vezu između inicijalnih vektora i vektora u reduciranoj bazi. Naredbe za nalaženje LLL-reducirane baze postoje i u drugim programskim paketima (npr. `lattice` (Maple), `LatticeReduce` (Mathematica), `LLL` (Magma)).

Navedimo sada prije spomenuti Rathbunov algoritam.

Reducirana Mordell-Weilova baza

ellLreduce$(e, plist)$=
$e =$ ellinit(e);
$n =$ length$(plist)$;
$u =$ qflllgram(ellheightmatrix$(e, plist)$);
$newplist =$ vector$(n, j, [0])$;
for$(i = 1, n,$ for$(j = 1, n,$
$newplist[i] =$ elladd$(e, newplist[i],$ ellpow$(e, plist[j], u[j, i])))$;

Primjer 2.11. *Promotrimo krivulju*

$$y^2 + xy = x^3 - 391397606765693763745924996738383 5x$$
$$+80614222594310898664080091661625700445673557913297.$$

To je jedna od krivulja s najvećim poznatim rangom među krivuljama s torzijskom grupom $\mathbb{Z}/10\mathbb{Z}$, te krivulja s najmanjim konduktorom od svih poznatih krivulja čija je Mordell-Weilova grupa izomorfna $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}^4$ (Dujella, 2005).

Pomoću programa MWRANK dobivamo da je rang jednak 4, te da je Mordell-Weilova grupa generirana točkama

$$P_1 = \left(\frac{630272629397544948862684139017006}{13379318255014009}, \frac{136233789132437251836981528851741590439605588749 1}{154757240337717017206302 7}\right),$$
$$P_2 = \left(\frac{10108627618965508383032350174}{590486201761}, -\frac{19583455876316733576568096346180064681984 97}{453747902505406991}\right),$$
$$P_3 = \left(\frac{27474451678475022336473802434668 6}{4890306578748529}, \frac{21095091791152839218465210600937926397829067896 39}{34198269430476738315058 3}\right),$$
$$P_4 = \left(\frac{50839337272548006001}{64}, \frac{36139644164828072797955276737 1}{512}\right).$$

Kanonske visine točaka P_1, P_2, P_3, P_4 su redom $34.02261806, 26.72628169, 45.34998979, 21.98466653$.

Primijenimo li Rathbunov algoritam, dobivamo novu Mordell-Weilovu bazu:

$$Q_1 = \left(-\frac{343612010825901006209}{6724}, \frac{66889930673648770057329762157 69}{551368}\right),$$
$$Q_2 = \left(-\frac{10216528923584657172449}{145924}, \frac{18867039044714009240612294658 9739}{55742968}\right),$$
$$Q_3 = (-71051466385703906, -13442883241925418821 6207),$$
$$Q_4 = \left(\frac{31277549200969930230818734}{515244601}, \frac{95528222879953330428431251943396378467}{11695537198099}\right),$$

s visinama 10.27648431, 12.33469261, 15.949425, 24.802228. Transformacijska matrica je

$$u = \begin{pmatrix} -1 & -1 & 0 & -1 \\ 1 & 1 & -1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

To znači da je $Q_1 = -P_1 + P_2$, $Q_2 = -P_1 + P_2 + P_4$, $Q_3 = -P_2 + P_3$, $Q_4 = -P_1 + 2P_2 + P_3$.

Do sada nismo koristili torzijske točke. Iz Propozicije 2.5 znamo da nam one ne mogu promijeniti kanonske visine točaka. No, one ipak mogu "pojednostavniti" bazu, u smislu da smanje naivnu visinu točaka ili da točke s racionalnim koordinatama zamijene s točkama s cjelobrojnim koordinatama. Budući da je u našem primjeru torzijska grupa velika ($\mathbb{Z}/10\mathbb{Z}$), izgledno je da će se na taj način barem neka od točaka pojednostavniti. Konačno dobivamo sljedeću Mordell-Weilovu bazu:

$$R_1 = (8185642345602334, 7008872315854122124478833),$$
$$R_2 = (-12386639730434786, -11278065707632343668729487),$$
$$R_3 = (-71051466385703906, -13442883241925418821 6207),$$
$$R_4 = \left(\frac{14512682959179656853 1936}{528529}, \frac{53943123228441855079366471262433889}{384240583}\right).$$

♢

Pretpostavimo da smo uspjeli izračunati rang r eliptičke krivulje E nekom od prethodno opisanih metoda. Te metode će nam uglavnom dati i r točaka $P_1, \ldots, P_r$ na E koje su nezavisne modulo $E(\mathbb{Q})_{\text{tors}}$. No to ne znači da će nužno $\{P_1, \ldots, P_r\} \cup E(\mathbb{Q})_{\text{tors}}$ generirati cijelu grupu $E(\mathbb{Q})$, već možda samo neku njezinu podgrupu konačnog indeksa. Tu podgrupu ćemo označiti s H. Željeli bismo, ako je moguće, naći generatore cijele Mordell-Weilove grupe, tj. Mordell-Weilovu bazu $Q_1, \ldots, Q_r$ (tako da se svaka točka $P \in E(\mathbb{Q})$ može, na jedinstven način, prikazati u obliku $P = n_1Q_1 + \cdots + n_rQ_r + T$, $n_i \in \mathbb{Z}$, $T \in E(\mathbb{Q})_{\text{tors}}$).

Pogledat ćemo najprije jedan jednostavan slučaj kada je $r = 1$ (pa se Mordell-Weilova grupa sastoji od jedne točke, koja se zove slobodni generator) i $\Delta > 0$. Tada E ima jednadžbu oblika $y^2 = (x - e_1)(x - e_2)(x - e_3)$, gdje su $e_i \in \mathbb{R}$. Neka je $e_1 < e_2 < e_3$. Tada je $E^0(\mathbb{Q}) = \{(x, y) \in E(\mathbb{Q}) : x \geq e_3\} \cup \{\mathcal{O}\}$ podgrupa od $E(\mathbb{Q})$ koja se zove parna ili neutralna komponentna, dok se $E^{gg}(\mathbb{Q}) = \{(x, y) \in E(\mathbb{Q}) : e_1 \leq x \leq e_2\}$ zove neparna komponenta ("jaje"). Neparna komponenta može biti prazna, a ako je neprazna, onda $E^0(\mathbb{Q})$ ima indeks 2 u $E(\mathbb{Q})$. Primijetimo da u rešetki $\mathbb{C}/L$ točke na $E^0(\mathbb{R})$ odgovaraju parametrima $z \in \mathbb{R}$, dok točke na $E^{gg}(\mathbb{R})$ odgovaraju parametrima z (iz fundametalnog pravokutnika) za koje je $z - \omega_2/2 \in \mathbb{R}$.

Propozicija 2.6. *Neka eliptička krivulja E s cjelobrojnim koeficijentima zadovoljava sljedeće uvjete:*

(i) *rank*$(E(\mathbb{Q})) = 1$*;*

(ii) *$E(\mathbb{Q})$ ima točku P beskonačnog reda takvu da $P+T$ ima cjelobrojne koordinate za sve $T \in E(\mathbb{Q})_{tors}$;*

(iii) *$\Delta > 0$;*

(iv) *neparna komponenta je neprazna.*

Tada se jedan slobodni generator Q neka od konačno mnogo točaka s cjelobrojnim koordinatama na neparnoj komponenti.

Dokaz: Neka je Q slobodni generator. Tada je $nQ = P + T$ za neki $n \in \mathbb{Z}$ i neku torzijsku točku T. Po pretpostavci (ii), točka nQ ima cjelobrojne koordinate. No, tada i točka $Q = (x, y)$ ima cjelobrojne koordinate.

To slijedi iz činjenice koja se koristi i u dokazu Lutz-Nagellovog teorema. Naime, pretpostavimo da je $\nu_p(x) < 0$ za neki prost broj p. Tada je $\nu_p(x) = -2k$, $\nu_p(y) = -3k$ za neki $k \in \mathbb{N}$. Činjenica koja ovdje trebamo jest da je

$$E(p^k) := \{(x, y) \in E(\mathbb{Q}) : \nu_p(x) \leq -2k\} \cup \{\mathcal{O}\}$$

podgrupa od $E(\mathbb{Q})$. Stoga iz $Q \in E(p^k)$ slijedi $nQ \in E(p^k)$, što je u suprotnosti s time da nQ ima cjelobrojne koordinate.

Za svaki $T' \in E(\mathbb{Q})_{\text{tors}}$ je točka $Q + T'$ slobodni generator, pa po upravo dokazanom ima cjelobrojne koordinate. Tvrdimo da se barem jedna od tih točaka nalazi u neparnoj komponenti. Pretpostavimo suprotno. Tada je Q u parnoj komponenti, a također i svi $T' \in E(\mathbb{Q})_{\text{tors}}$ su u parnoj komponenti. Ali $E(\mathbb{Q})$ je generiran s Q i $E(\mathbb{Q})_{\text{tors}}$, pa bi tada bio sadržan u svojoj parnoj komponenti, što je u suprotnosti s pretpostavkom (iv).

Točaka s cjelobrojnim koordinatama u neparnoj komponenti očito ima samo konačno mnogo, jer im se x-koordinate nalaze u segmentu $[e_1, e_2]$. □

Primjer 2.12. *Nađimo slobodni generator krivulje*

$$y^2 = (x+1)(3x+1)(8x+1).$$

Rješenje: Kao i u Primjeru 2.9, radit ćemo s izomorfnom krivuljom

$$E\ :\ y^2 = x^3 + 11x^2 - 80x.$$

U Primjeru 2.9 smo vidjeli smo da je rang od E jednak 1. Algoritam nam je dao i nekoliko točaka beskonačnog reda: $P_1 = (-10, 30)$, $P_2 = (-2, 14)$, $P_3 = (8, 24)$, $P_4 = (40, 240)$. Po Primjeru 2.7 znamo da su jedine netrivijalne torzijske točke na E točke reda 2: $T_1 = (-16, 0)$, $T_2 = (0, 0)$, $T_3 = (5, 0)$. Uzmimo točku $P_1 = (-10, 30)$. Točke P_1, $P_1 + T_1 = -P_4$, $P_1 + T_2 = P_3$, $P_1 + T_3 = -P_2$ imaju cjelobrojne koordinate. Stoga su zadovoljeni svi uvjeti Propozicije 2.6. Lako se vidi da su jedine točke s cjelobrojnim koordinatama čija je x-koordinata iz segmenta $[-16, 0]$ točke $\pm P_1 = (-10, \pm 30)$, $\pm P_2 = (-2, 14)$, T_1 i T_2. Zaključujemo da P_1 slobodni generator od $E(\mathbb{Q})$ (ostali slobodni generatori su $-P_1$, $\pm P_2$, $\pm P_3$ i $\pm P_4$). Sada slobodne generatore polazne krivulje dobivamo transformacijom $x \mapsto \frac{x-8}{24}$. To su točke: $(-\frac{3}{4}, \pm\frac{5}{4})$, $(-\frac{5}{12}, \frac{7}{12})$, $(0, \pm 1)$, $(\frac{4}{3}, \pm\frac{35}{3})$. Dakle, očita točka $(0, 1)$ (koja odgovara trivijalnom proširenju trojke s nulom) je jedan od slobodnih generatora. ♢

U općenitom slučaju imamo r nezavisnih točaka na $E(\mathbb{Q})$ i one zajedno sa $E(\mathbb{Q})_{\text{tors}}$ generiraju podgrupu H od $E(\mathbb{Q})$. Te nezavisne točke smo mogli dobiti kao produkt algoritma 2-silaska ili pretragom za točaka malih visina na $E(\mathbb{Q})$. Željeli bismo podgrupu H "uvećati" do cijele grupe $E(\mathbb{Q})$ (ili dokazati da je $H = E(\mathbb{Q})$).

U tu svrhu, koriste se eksplicitne ocjene za razliku između naivne i kanonske visine. Navest ćemo jedan opći rezultat takvog tipa kojeg je dokazao Silverman 1990. godine. Napomenimo da je za konkretne krivulje često moguće dobiti i znatno bolje ograde. Koristimo oznaku $\log^+(x) = \log \max\{1, |x|\}$ za $x \in \mathbb{R}$.

Propozicija 2.7. *Neka je E eliptička krivulja zadana Weierstrassovom jednadžbom s cjelobrojnim koeficijentima, te neka je Δ diskriminanta, a j njena j-invarijanta. Stavimo $2^* = 2$ ako je $b_2 \neq 0$, a $2^* = 1$ ako je $b_2 = 0$, te definirajmo*

$$\mu(E) = \frac{1}{6}(\log|\Delta| + \log^+(j)) + \log^+(b_2/12) + \log(2^*).$$

Tada za svaki $P \in E(\mathbb{Q})$ vrijedi

$$-\frac{1}{12}h(j) - \mu(E) - 1.922 \leq \hat{h}(P) - h(P) \leq \mu(E) + 2.14.$$

Propoziciju je vrlo jednostano primijeniti ako krivulja ima rang 1, a mi znamo jednu točku P beskonačnog reda. Ako P nije slobodni generator, onda je $P = kQ + T$ za generator Q i $k \geq 2$. Stoga je $\hat{h}(Q) \leq \frac{1}{4}\hat{h}(P)$, pa nam Propozicija 2.7 daje gornju ogradu B za naivnu visinu od Q. Ukoliko ne nađemo niti jednu racionalnu točku s $h(Q) \leq B$, onda znamo da je P generator, a inače je generator neka od pronađenih točaka.

Uočimo da nam Propozicija 2.7 daje još jednu metodu da nalaženje torzijskih točaka. Naime, budući da torzijske točke imaju kanonsku visinu 0, to je njihova naivna visina manja od $\frac{1}{12}h(j) + \mu(E) + 1.922$.

Poglavlje 3

Eliptičke krivulje inducirane Diofantovim trojkama

3.1 Istaknute točke i regularne m-torke

Opisat ćemo sada detaljnije vezu između racionalnih Diofantovih m-torki i eliptičkih krivulja. Neka je $\{a, b, c\}$ racionalna Diofantova trojka, tj. neka je

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2$$

za nenegativne racionalne brojeve r, s, t. Da bismo ovu trojku proširili do racionalne Diofantove četvorke, trebamo naći racionalni broj x sa svojstvom da su $ax+1$, $bx+1$ i $cx+1$ kvadrati racionalnih brojeva. Ako pomnožimo ova tri uvjeta, dobivamo jedan uvjet

$$y^2 = (ax + 1)(bx + 1)(cx + 1),$$

koji je jednadžba eliptičke krivulje. Objasnit ćemo uskoro koje točke na krivulji zadovoljavaju polazni sustav od tri jednadžbe te daju proširenje do racionalne Diofantove četvorke.

Označimo krivulju $y^2 = (ax+1)(bx+1)(cx+1)$ s $\mathcal{E}$. Reći ćemo da je $\mathcal{E}$ *inducirana Diofantovom trojkom* $\{a, b, c\}$. Na krivulji $\mathcal{E}$ imamo tri očite racionalne točke reda 2, to su $A = (-\frac{1}{a}, 0)$, $B = (-\frac{1}{b}, 0)$, $C = (-\frac{1}{c}, 0)$. Također imamo još dvije očite racionalne točke

$$P = (0, 1), \quad S = \Big(\frac{1}{abc}, \frac{rst}{abc}\Big). \tag{3.1}$$

Lako se provjeri da je x-koordinata točke $P - S$ upravo broj d_+ iz definicije regularne četvorke (dok je x-koordinata točke $P + S$ jednaka d_-). Da bi to napravili, transformacijama $x \mapsto x/abc$, $y \mapsto y/abc$, iz krivulje $\mathcal{E}$ dobivamo krivulju

$$\mathcal{E}' : \qquad y^2 = (x + bc)(x + ac)(x + ab)$$

s normiranim kubnim polinomom na desnoj strani jednadžbe. Točke A, B, C, P i S na $\mathcal{E}$ postaju $A' = (-bc, 0)$, $B' = (-ac, 0)$, $C' = (-ab, 0)$, $P' = (0, abc)$ i $S' = (1, rst)$ na $\mathcal{E}'$. Sada računamo x-koordinatu točke $P' - S'$ na $\mathcal{E}'$:

$$\begin{aligned}
&(rst + abc)^2 - (ab + ac + bc) - 0 - 1 \\
&= (ab + 1)(ac + 1)(bc + 1) + 2abcrst + a^2b^2c^2 - ab - ac - ab - 1 \\
&= abc(a + b + c + 2abc + 2rst),
\end{aligned}$$

otkud dijeljeljem s abc dobivamo da je x-koordinata točke $P-S$ na $\mathcal{E}$ jednaka d_+, što smo i tvrdili. Sasvim analogno se dokazuje da je x-koordinata točke $P+S$ na $\mathcal{E}$ jednaka d_-.

Općenito, možemo očekivati da će P i S biti nezavisne točke beskonačnog reda. Ali važno je pitanje, sa značajnim posljedicama, mogu li te točke biti konačnog reda i koji su redovi pritom mogući. Primijetimo da ako je trojka $\{a,b,c\}$ regularna, onda P i S nisu nezavisne, već vrijedi da je $2P=-S$. Zaista, u Potpoglavlju 1.4 smo pokazali da je trojka $\{a,b,c\}$ regularna ako i samo ako je $d_-=0$. A upravo smo vidjeli da je d_- x-koordinata točke $P+S$. Budući da je x-koordinata točke P jednaka 0, zaključujemo da je $P=P+S$ ili $P=-P-S$. Prva mogućnost otpada jer $S\neq\mathcal{O}$, a druga mogućnost daje $2P=-S$, što se i tvrdilo.

Sada možemo odgovoriti na pitanje koje točke na $\mathcal{E}$ daju proširenja polazne trojke do racionalne Diofantove četvorke. Naime, x-koordinata točke $T\in\mathcal{E}(\mathbb{Q})$ zadovoljava polazna tri uvjeta da su $ax+1$, $bx+1$ i $cx+1$ kvadrati racionalnih brojeva ako i samo ako je $T-P\in 2\mathcal{E}(\mathbb{Q})$. To će slijediti iz sljedećeg teorema koji se može shvatiti kao poopćenje Teorema 2.4, a tiče se preslikavanja koja su nam se javila u metodi za računanje ranga pomoću 2-izogenije.

Teorem 3.1. *Neka je E eliptička krivulja nad poljem $\mathbb{Q}$ dana jednadžbom*

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

Definirajmo preslikavanje $\varphi: E(\mathbb{Q})\to\mathbb{Q}^*/\mathbb{Q}^{*2}$ s

$$\varphi(P)=\begin{cases}(x-\alpha)\mathbb{Q}^{*2} & \text{ako je } P=(x,y)\neq\mathcal{O},(\alpha,0)\\ (\alpha-\beta)(\alpha-\gamma)\mathbb{Q}^{*2} & \text{ako je } P=(\alpha,0)\\ \mathbb{Q}^{*2} & \text{ako je } P=\mathcal{O}.\end{cases}$$

Tada je φ homomorfizam grupa.

Dokaz: Neka je $P_1+P_2=P_3$. Trebamo dokazati da je $\varphi(P_1)\varphi(P_2)\varphi(P_3)^{-1}$ iz $\mathbb{Q}^{*2}$. Budući da je $\varphi(P_3)=\varphi(-P_3)$ i $\varphi(P_3)=\varphi(P_3)^{-1}$, dovoljno je dokazati da $P_1+P_2+P_3=\mathcal{O}$ povlači da je $\varphi(P_1)\varphi(P_2)\varphi(P_3)$ iz $\mathbb{Q}^{*2}$.

Ako je neki od P_i, recimo P_1, jednak $\mathcal{O}$, onda tvrdnja lako slijedi, jer $P_2+P_3=\mathcal{O}$ povlači $\varphi(P_2)=\varphi(P_3)$, pa je $\varphi(P_1)\varphi(P_2)\varphi(P_3)$ iz $\mathbb{Q}^{*2}$. Stoga u daljnjem možemo pretpostaviti da su $P_i=(x_i,y_i)\neq\mathcal{O}$ za $i=1,2,3$.

Pretpostavimo da je $P_1=(\alpha,0)$. Tada su $P_2,P_3\neq(\alpha,0)$ jer bi inače jedna on njih bila $\mathcal{O}$. Iz pretpostavke da je $P_1+P_2+P_3=\mathcal{O}$ slijedi da točke P_1,P_2,P_3 leže na jednom pravcu. Neka je jednadžba tog pravca $y=kx+\ell$. Tada su $x_1=\alpha,x_2,x_3$ nultočke polinoma $(x-\alpha)(x-\beta)(x-\gamma)-(kx+\ell)^2$, pa je

$$(x-\alpha)(x-\beta)(x-\gamma)-(kx+\ell)^2=(x-\alpha)(x-x_2)(x-x_3).\tag{3.2}$$

Iz (3.2) slijedi da $x-\alpha$ dijeli $kx+\ell$, pa je $kx+\ell=k(x-\alpha)$. Nakon kraćenja s $x-\alpha$, (3.2) postaje

$$(x-\beta)(x-\gamma)-k^2(x-\alpha)=(x-x_2)(x-x_3).\tag{3.3}$$

Stavimo $x=\alpha$ u (3.3), pa dobivamo da je

$$(\alpha-\beta)(\alpha-\gamma)=(x_2-\alpha)(x_3-\alpha),$$

što povlači da je $\varphi(P_1)=\varphi(P_2)\varphi(P_3)$, pa je $\varphi(P_1)\varphi(P_2)\varphi(P_3)\in\mathbb{Q}^{*2}$.

Preostaje razmotriti slučaj kad su svi $P_i \neq (\alpha, 0)$. Neka je ponovno $y = kx + \ell$ pravac kroz točke P_1, P_2, P_3. Isto kao prije zaključujemo da vrijedi

$$(x-\alpha)(x-\beta)(x-\gamma) - (kx+\ell)^2 = (x-x_1)(x-x_2)(x-x_3). \tag{3.4}$$

Uvrstimo $x = \alpha$ u (3.4) pa dobivamo da je $(x_1-\alpha)(x_2-\alpha)(x_3-\alpha) = (k\alpha+\ell)^2$ te je $\varphi(P_1)\varphi(P_2)\varphi(P_3) \in \mathbb{Q}^{*2}$. □

Korolar 3.1. *Neka je $T \in \mathcal{E}(\mathbb{Q})$ te $x = x(T)$. Tada su $ax+1$, $bx+1$ i $cx+1$ kvadrati racionalnih brojeva ako i samo ako je $T - P \in 2\mathcal{E}(\mathbb{Q})$.*

Dokaz: Za proizvoljnu točku $X = (x, y) \in \mathcal{E}(\mathbb{Q})$, označavat ćemo sa $X' = (xabc, yabc)$ odgovarajuću točku u $\mathcal{E}'(\mathbb{Q})$. Po Teoremu 3.1, funkcija $\varphi_a : \mathcal{E}'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ definirana s

$$\varphi_a(X') = \begin{cases} (x+bc)\mathbb{Q}^{*2} & \text{ako je } X' = (x,y) \neq \mathcal{O}, A' \\ (ac-bc)(ab-bc)\mathbb{Q}^{*2} & \text{ako je } X = A' \\ \mathbb{Q}^{*2} & \text{ako je } X = \mathcal{O} \end{cases}$$

je homomorfizam grupa. Isto vrijedi i za analogno definirane funkcije φ_b i φ_c. Točka P zadovoljava zadani uvjet jer je $x(P) = 0$. Imamo: $\varphi_a(P') = bc\mathbb{Q}^{*2}$, $\varphi_b(P') = ac\mathbb{Q}^{*2}$, $\varphi_c(P') = ab\mathbb{Q}^{*2}$. Sada $x = x(T)$ zadovoljava zadani uvjet da su $ax+1$, $bx+1$ i $cx+1$ kvadrati ako i samo ako za $x' = xabc$ vrijedi da je $x' + bc = bc\square$, $x' + ac = ac\square$, $x' + ab = ab\square$, tj. ako i samo ako vrijedi

$$\varphi_a(T') = \varphi_a(P'), \quad \varphi_b(T') = \varphi_b(P'), \quad \varphi_c(T') = \varphi_c(P').$$

Budući da su $\varphi_a, \varphi_b, \varphi_c$ homomorfizmi, ovo je ekvivalentno s

$$\varphi_a(T'-P') = \varphi_b(T'-P') = \varphi_c(T'-P') = \mathbb{Q}^{*2}.$$

A po Teoremu 2.4, ovo je ekvivalentno s $T' - P' \in 2\mathcal{E}'(\mathbb{Q})$. □

Iz Teorema 2.4 slijedi da je $S \in 2\mathcal{E}(\mathbb{Q})$. Naime, $1+bc$, $1+ac$ i $1+ab$ su kvadrati pa je $S' \in 2\mathcal{E}'(\mathbb{Q})$. To nije teško ni direktno provjeriti. Naime, vrijedi da je $S' = 2R'$, gdje je

$$R' = \left(rs+rt+st+1, (r+s)(r+t)(s+t)\right).$$

Ovo zajedno s Korolarom 3.1 povlači da ako $x(T)$ zadovoljava polazni sustav, onda ga također zadovoljavaju i brojevi $x(T \pm S)$. Zanimljivo je da pritom vrijedi da je $x(T)x(T \pm S) + 1$ uvijek kvadrat racionalnog broja. Zaista, ova tvrdnja je posljedica sljedeće općenitije činjenice.

Propozicija 3.1. *Neka su Q, T i $(0, q)$ tri racionalne točke na eliptičkoj krivulji E nad $\mathbb{Q}$ danoj jednadžbom $y^2 = f(x)$, gdje je f normirani polinom stupnja 3. Pretpostavimo da $\mathcal{O} \notin \{Q, T, Q+T\}$. Tada je $x(Q)x(T)x(Q+T) + q^2$ kvadrat racionalnog broja.*

Dokaz: Promotrimo krivulju

$$y^2 = f(x) - (x - x(Q))(x - x(T))(x - x(Q+T)), \tag{3.5}$$

koja predstavlja koniku (krivulju drugog stupnja) koja sadržava tri kolinearne točke Q, T, $-(Q+T)$, pa stoga mora biti unija dvaju racionalnih pravaca, tj. vrijedi $y^2 =$

$(kx+\ell)^2$. Uvrstimo li sada u (3.5) $x=0$, dobivamo $x(Q)x(T)x(Q+T)+q^2=\ell^2$, što se i tvrdilo. □

Da bismo primijenili Propoziciju 3.1 za konstrukciju racionalnih Diofantovih petorki (a kasnije i šestorki), podsjetimo se da smo transformacijama $x\mapsto x/abc$, $y\mapsto y/abc$, iz krivulje $\mathcal{E}$ dobili krivulju

$$\mathcal{E}':\qquad y^2=(x+ab)(x+ac)(x+bc)$$

s normiranim kubnim polinomom na desnoj strani jednadžbe, te da su pritom točke P i S na $\mathcal{E}$ postale $P'=(0,abc)$ i $S'=(1,rst)$ na $\mathcal{E}'$. Primijenimo li Propoziciju 3.1 uz $Q=\pm S'$, budući da je prva koordinata točke S' jednaka 1, zaključujemo da je $x(T)x(T\pm S)+1$ potpun kvadrat (nakon dijeljenja jednakosti $x(T')x(T'\pm S')+a^2b^2c^2=\square$ sa $a^2b^2c^2$).

Dakle, na ovaj način možemo prozvoljnu racionalnu Diofantovu četvorku $\{a,b,c,d\}$, proširiti do racionalne Diofantove petorke $\{a,b,c,d,e\}$, tako da za T uzmemo točku na krivulji $\mathcal{E}$ kojoj je prva koordinata jednaka d, a za e uzmemo x-koordinatu točke $T+S$ (ili $T-S$) na istoj krivulji. Pritom trebaju biti zadovoljeni uvjeti da su svi elementi petorke različiti od nule te da su međusobno različiti i točka $T+S$ (odosno $T-S$) nije točka $\mathcal{O}$. Odavde možemo dobiti eksplicitnu formulu za proširenje racionalne Diofantove četvorke do petorke (koja poopćuje Eulerovu formulu za petorke iz potpoglavlja 1.3).

Teorem 3.2. *Neka su x_1,x_2,x_3,x_4 racionalni brojevi takvi da je $x_ix_j+1=y_{ij}^2$, $y_{ij}\in\mathbb{Q}$, za sve $1\le i<j\le 4$. Pretpostavimo da je $x_1x_2x_3x_4\neq 1$. Tada racionalni broj $x_5=A/B$, gdje je*

$$\begin{aligned}A=(&\pm 2y_{12}y_{13}y_{14}y_{23}y_{24}y_{34}+x_1x_2x_3x_4(x_1+x_2+x_3+x_4)\\&+2(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)+(x_1+x_2+x_3+x_4)]\,,\end{aligned}$$

$$B=(x_1x_2x_3x_4-1)^2\,,$$

ima svojstvo da su x_ix_5+1 kvadrati racionalnih brojeva za $i=1,2,3,4$. Preciznije, za $i\in\{1,2,3,4\}$ vrijedi:

$$x_ix_5+1=\left(\frac{x_iy_{jk}y_{jl}y_{kl}\pm y_{ij}y_{ik}y_{il}}{x_1x_2x_3x_4-1}\right)^2,$$

gdje je $\{i,j,k,l\}=\{1,2,3,4\}$.

Petorke dobivene pomoću formule iz Teorema 3.2, odnosno petorke oblika $\{a,b,c,x(T),x(T\pm S)\}$, nazivaju se *regularne racionalne Diofantove petorke*.

Ako je polazna četvorka oblika $\{a,b,a+b+2r,4r(a+r)(b+r)\}$, kao u Eulerovoj konstrukciji petorki, onda je $T=P-S$ i $2P=-S$, pa je $T=3P$, $T-S=5P$, dok je $T+S=P$, pa imamo samo jedno netrivijalno proširenje do petorke jer je $x(P)=0$. Isti slučaj je i s proširenjem proizvoljne trojke do petorke (Arkin, Hoggatt, Strauss, 1979.), jer i ono koristi regularne četvorke, pa je ponovno $T=P-S$ i $T+S=P$. Međutim, kod proširenja preko Teorema 3.2 (Dujella, 1997.), općenito imamo dva različita proširenja do petorke. Mogli bi reći da je situacija analogna kao kod proširenja cjelobrojnih trojki do četvorki, gdje općenito imamo dva proširenja s d_+ i d_-, a u slučaju kad je polazna trojka regularna jedno od ta dva proširenja otpada jer daje trivijalno proširenje s nulom. Važna razlika je ipak u tome

što se u cjelobrojnom slučaju sluti da nema drugih mogućnosti za proširenje, dok u racionalnom slučaju prostoje primjeri četvorki koje se do petorke mogu nadopuniti i na više od dva načina. Primjerice, Gibbs je 2016. našao primjer četvorke

$$\left\{\frac{81}{1400}, \frac{5696}{4725}, \frac{2875}{168}, \frac{4928}{3}\right\}$$

koja se do petorke može nadopuniti na barem šest različitih načina, tj. s bilo kojim od ovih šest racionalnih brojeva

$$\frac{98}{27}, \frac{104}{525}, \frac{96849}{350}, \frac{1549429}{1376646}, \frac{3714303488}{6103383075}, \frac{7694337252154322}{1857424629984075}.$$

3.2 Beskonačno mnogo racionalnih Diofantovih šestorki – 1. konstrukcija

U ovom potpoglavlju prikazat ćemo konstrukciju beskonačno mnogo racionalnih Diofantovih šestorki prema članku Dujella, Kazalicki, Mikić, Szikszai (2017.). Na kraju prethodnog potpoglavlja, prikazali smo konstrukciju kojom se racionalna Diofantova četvorka proširuje do petorke na dva različita načina. Stoga je unija te dvije petorke,

$$\{a, b, c, x(T-S), x(T), x(T+S)\},$$

"gotovo" racionalna Diofantova šestorka.

Ako pretpostavimo da $T, T \pm S \notin \{\mathcal{O}, \pm P\}$, jedini uvjet koji nedostaje je da

$$x(T-S)x(T+S)+1$$

bude kvadrat. Da bi našli primjere koji zadovoljavaju ovaj zadnji uvjet, primijenit ćemo Propoziciju 3.1 za $Q = 2S'$. To će nam dati željeni zaključak ako je ispunjen uvjet $x(2S') = 1$. Sada iz $x(2S') = x(S')$ dobivamo uvjet $2S' = -S'$, tj. $3S' = \mathcal{O}$.

Na taj smo način problem konstrukcije racionalnih Diofantovih šestorki povezali s eliptičkim krivuljama s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Pomoću formule da dupliciranje točaka na eliptičkoj kruvulji, uvjet $x(2S') = x(S')$ se može eksplicitno zapisati u obliku

$$\begin{aligned} -a^4b^2c^2 + 2a^3b^3c^2 + 2a^3b^2c^3 - a^2b^4c^2 + 2a^2b^3c^3 - a^2b^2c^4 + 12a^2b^2c^2 \\ +6a^2bc + 6ab^2c + 6abc^2 + 4ab + 4ac + 4bc + 3 = 0. \end{aligned} \tag{3.6}$$

Ovo je simetrična jednadžba, pa uvođenjem elementarnih simetričnih polinoma $\sigma_1 = a+b+c$, $\sigma_2 = ab+ac+bc$, $\sigma_3 = abc$, dobivamo jednostavniju jednadžbu, koju možemo riješiti po varijabli σ_2:

$$\sigma_2 = (\sigma_1^2\sigma_3^2 - 12\sigma_3^2 - 6\sigma_1\sigma_3 - 3)/(4 + 4\sigma_3^2). \tag{3.7}$$

Uvrstimo li (3.7) u $(ab+1)(ac+1)(bc+1) = (rst)^2$, dobivamo $(2\sigma_3^2+\sigma_1\sigma_3-1)^2/(4+4\sigma_3^2) = (rst)^2$, tj. dobivamo uvjet da je $1+\sigma_3^2$ kvadrat, pa možemo staviti $\sigma_3 = \frac{t^2-1}{2t}$.

Nužan uvjet da bi polinom

$$X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$$

imao racionalne korijene je da mu diskriminanta bude potpun kvadrat. To nam daje uvjet:

$$(\sigma_1^3\sigma_3 - 9\sigma_1^2 - 27\sigma_1\sigma_3 - 54\sigma_3^2 - 27)(1+\sigma_3^2)(\sigma_1\sigma_3 + 2\sigma_3^2 - 1) = \square. \tag{3.8}$$

Za fiksni σ_3, možemo shvatiti (3.8) kao kvartiku u σ_1. Budući da $1+\sigma_3^2$ mora biti potpun kvadrat, iz (3.8) dobivamo kvartiku s racionalnom točkom (točkom u beskonačnosti), koja se stoga može transformirati u jednadžbu eliptičke krivulje nad $\mathbb{Q}(t)$.

Dobivenu kvartiku prebacimo (primjenom Propozicije 2.1) u eliptičku krivulju nad $\mathbb{Q}(t)$

$$\begin{aligned} y^2 = x^3 + (3t^4 - 21t^2 + 3)x^2 \\ +(3t^8 + 12t^6 + 18t^4 + 12t^2 + 3)x + (t^2+1)^6. \end{aligned} \tag{3.9}$$

Ova krivulja ima pozitivan rang, jer sadrži točku $R = (0, (t^2+1)^3)$ beskonačnog reda.

Ako uzmemo točke mR, transformiramo ih natrag na kvartiku, te izračunamo odgovarajuće trojke $\{a,b,c\}$, možemo očekivati da ćemo dobiti beskonačno mnogo parametarskih familija racionalnih trojki za koje odgovarajuća točka S' na E' zadovoljava $3S' = \mathcal{O}$.

Budući da uvjet $1+\sigma_3^2 = \square$ povlači $rst \in \mathbb{Q}$, a $S' = -2S' \in 2\mathcal{E}'(\mathbb{Q})$, Teorem 2.4 primijenjen na krivulju $\mathcal{E}'$ povlači da su $ab+1$, $ac+1$, $bc+1$ kvadrati, te je $\{a,b,c\}$ dobivena ovom konstrukcijom zaista racionalna Diofantova trojka.

Specijalno, ako uzmemo točku $2R$, dobivamo familiju trojki

$$\begin{aligned} a &= \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)}, \\ b &= \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)}, \\ c &= \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}. \end{aligned}$$

Promotrimo eliptičku krivulju nad $\mathbb{Q}(t)$ induciranu trojkom $\{a,b,c\}$. Ona ima pozitivan rang jer je točka $P = (0,1)$ beskonačnog reda. Stoga opisana konstrukcija daje beskonačno mnogo racionalnih Diofantovih šestorki koje sadrže trojku $\{a,b,c\}$. Jedna takva šestorka $\{a,b,c,d,e,f\}$ se dobije iz x-koordinata točaka $3P$, $3P+S$, $3P-S$ (općenitije, možemo uzeti točke $(2n+1)P$, $(2n+1)P+S$, $(2n+1)P-S$ za $n \in \mathbb{N}$).

Dobivamo: $d = d_1/d_2$, $e = e_1/e_2$, $f = f_1/f_2$, gdje je

$$
\begin{aligned}
d_1=&6(t+1)(t-1)(t^2+6t+1)(t^2-6t+1)\\
&\times(8t^6+27t^5+24t^4-54t^3+24t^2+27t+8)\\
&\times(8t^6-27t^5+24t^4+54t^3+24t^2-27t+8)\\
&\times(t^8+22t^6-174t^4+22t^2+1),\\
d_2=&t(37t^{12}-885t^{10}+9735t^8-13678t^6+9735t^4-885t^2+37)^2,\\
e_1=&-2t(4t^6-111t^4+18t^2+25)\\
&\times(3t^7+14t^6-42t^5+30t^4+51t^3+18t^2-12t+2)\\
&\times(3t^7-14t^6-42t^5-30t^4+51t^3-18t^2-12t-2)\\
&\times(t^2+3t-2)(t^2-3t-2)(2t^2+3t-1)\\
&\times(2t^2-3t-1)(t^2+7)(7t^2+1),\\
e_2=&3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)\\
&\times(16t^{14}+141t^{12}-1500t^{10}+7586t^8-2724t^6+165t^4+424t^2-12)^2,\\
f_1=&2t(25t^6+18t^4-111t^2+4)\\
&\times(2t^7-12t^6+18t^5+51t^4+30t^3-42t^2+14t+3)\\
&\times(2t^7+12t^6+18t^5-51t^4+30t^3+42t^2+14t-3)\\
&\times(2t^2+3t-1)(2t^2-3t-1)(t^2-3t-2)\\
&\times(t^2+3t-2)(t^2+7)(7t^2+1),\\
f_2=&3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)\\
&\times(12t^{14}-424t^{12}-165t^{10}+2724t^8-7586t^6+1500t^4-141t^2-16)^2.
\end{aligned}
$$

Ove formule daju beskonačno mnogo racionalnih Diofantovih šestorki. Nadalje, izborom racionalnog parametra t iz odgovarajućih intervala, dobivamo beskonačno mnogo šestorki za bilo koju kombinaciju predznaka. Npr. za $5.83 < t < 6.86$ svi elementi su pozitivni. Za konkretan primjer uzmimo $t = 6$, pa dobivamo šestorku s pozitivnim elementima:

$$
\left\{\frac{3780}{73},\frac{26645}{252},\frac{7}{13140},\frac{791361752602550684660}{18278930922345566928 01},\right.
$$

$$
\left.\frac{95104852709815809228981184}{35104191165465133563326695 5},\frac{32108912707623335675210845 44}{21712719223923581005355}\right\}.
$$

Konstrukcija navedene parametarske familije racionalnih Diofantovih šestorki zasniva se na činjenici da kubni polinom koji odgovara točki $2R$ ima racionalne korijene. Može se pokazati da isto svojstvo ima svaki višekratnik mR točke R (dolje ćemo ugrubo skicirati dokaz). Budući da je diskriminanta pripadnog kubnog polinoma potpun kvadrat, dovoljno je dokazati za kubni polinom ima barem jedan racionalni korijen, jer će tada nužno i preostala dva korijena biti racionalna. Međutim, ovo svojstvo ne mora biti zadovoljeno za ostale točke na krivulji (3.9) (u slučaju kada je rang > 1). Npr. za $t = 31$ (kada je rang od (3.9) jednak 2) i točku $(x, y) = (-150072, 682327360)$ (koja nije višekratnik od R) polinom $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$ nema racionalnih korijena.

Svakom višekratniku $mR = (x, y)$ točke R (uz $m > 1$, tako da je $x \neq 0$), pridružujemo eliptičku krivulju

$$
E' : \quad Y^2 = X^3 + \sigma_2 X^2 + \sigma_1\sigma_3 X + \sigma_3^2.
$$

Ovdje je $\sigma_3 = \frac{t^2-1}{2t}$, $t \notin \{-1, 0, 1\}$,

$$\sigma_1 = \frac{-t^4 + 4t^2 - 1 - x^{-1}(t^2+1)^4}{(t^2-1)t},$$

dok je σ_2 dan sa (3.7).

Uz odgovarajuće transformacije koordinata, krivulja E' postaje

$$E'' : \quad Y^2 = X^3 + \frac{((t^2+1)^2x^{-1}+1)^2}{4}X^2 + \frac{t^2((t^2+1)^2x^{-2}+x^{-1})}{2}X + \frac{t^4x^{-2}}{4}. \tag{3.10}$$

Neka su $t \in \mathbb{Z}$ i (x, y) takvi da E'' ima dobru ili multiplikativnu redukciju (kubni polinom promatran modulo p ima ili jednostruke nultočke ili jednu dvostruku nultočku) za sve $p|t(t^2+1)$ i neka je $v_3(y) \leq 0$. Tada E'' ima tri racionalne točke reda 2.

Neka je $t \neq 1$ prirodan broj takav da je broj t^2+1 kvadratno slobodan. Tada eliptička krivulja E'' koja odgovara višekratniku mR, $m > 1$, ima tri racionalne točke reda 2 (tj. odgovarajući brojevi a, b, c su racionalni).

Efektivna verzija Hilbertovog teorema o ireducibilnosti (za svaki ireducibilni polinom $f(x,t) \in \mathbb{Z}[x,t]$ postoji "puno" specijalizacija $t = \tau \in \mathbb{Z}$ takvih da je polinom $f(x,\tau)$ ireducibilan u $\mathbb{Z}[x]$) sada povlači da ista tvrdnja vrijedi da svaki racionalan broj $t \notin \{-1, 0, 1\}$.

Primijetimo da u prije spomenutom primjeru $t = 31$, $(x, y) = (-150072, 682327360)$ krivulja E'' ima aditivnu redukciju u $13, 31$ i 37.

Kao što smo spomenuli u uvodnom poglavlju, otvoreno je pitanje postoji li neka racionalna Diofantova sedmorka. Primijetimo da samo primjenom Propozicije 3.1 ne možemo doći do kandidata za sedmorke. Naime, prirodni kandidat za proširenje šestorke $\{a, b, c, x(T-S), x(T), x(T+S)\}$ bi bio $x(T+2S)$, ali on se već nalazi u šestorki jer je $x(T+2S) = x(T-S)$ budući da točka S ima red 3.

3.3 Beskonačno mnogo racionalnih Diofantovih šestorki – 2. konstrukcija

Racionalne Diofantove šestorke konstruirane u prethodnom potpoglavlju sadrže dvije regularne petorke. U ovom potpoglavlju prikazat ćemo alternativnu konstrukciju beskonačno mnogo racionalnih Diofantovih šestorki (iz članka Dujella, Kazalicki & Petričević, 2021.) koje će sadržavati dvije regularne četvorke i jednu regularnu petorku.

Gibbs je 2016. sortirao do tada poznatih oko 1000 primjera racionalnih Diofantovih šestorki s obzirom na njihovu strukturu, posebno uključujući podatke u regularnim trojkama, četvorkama i petorkama koje su u njima sadržane. Petričević je proširio kolekciju primjera sa šestorkama s relativnom malim brojnicima i nazivnicima (te uključio i šestorke s miješanim predznacima – Gibbs je promatrao samo šestorke s pozitivnim elementima). Značajan broj tih primjera šestorki sadržavao je dvije regularne četvorke i jednu regularnu petorku, što je motiviralo pokušaj dokaza da takvih šestorki ima beskonačno mnogo.

Teorem 3.3. *Postoji beskonačno mnogo racionalnih Diofantovih šestorki koje sadrže dvije regularne Diofantove četvorke i jednu regularnu Diofantovu petorku.*

U konstrukciji krećemo od parametrizacije racionalnih Diofantovih trojki. Neka je $\{a_1, a_2, a_3\}$ racionalna Diofantova trojka te neka je $a_2 = (r^2-1)/a_1$ i $a_3 = (s^2-1)/a_1$ za racionalne brojeve r i s. Stavimo li $a_2a_3+1 = (a_2s^2 - a_2 + a_1)/a_1 = (1+(s-1)t)^2$, dobivamo

$$a_3 = \frac{-4t(t-1)(a_1t-a_2)}{(-a_2+a_1t^2)^2}.$$

Ova parametrizacija je iskorištena (Dujella, 2009.) za konstrukciju nekih primjera rationalnih Diofantovih šestorki s miješanim predznacima. Mi ćemo ovdje koristiti ekvivaletnu parametrizaciju koju je pronašao Lasić (objavljena je u dodatku članka Kazalicki & Naskręcki, 2022.), a koja je (ciklički) simetrična u trima parametrima:

$$\begin{aligned} a_1 &= \frac{2t_1(1+t_1t_2(1+t_2t_3))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}, \\ a_2 &= \frac{2t_2(1+t_2t_3(1+t_3t_1))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}, \\ a_3 &= \frac{2t_3(1+t_3t_1(1+t_1t_2))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}. \end{aligned}$$

Veza među dvjema navedenim parametrizacijama je dana sa

$$t_1 = \frac{a_1}{r-1}, \quad t_2 = \frac{-(1-r^2+a_1^2t^2)}{2(t-1)a_1}, \quad t_3 = \frac{2a_1t(t-1)}{1-r^2+a_1^2t^2},$$

$$a_1 = \frac{2t_1(1+t_1t_2(1+t_2t_3))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}, \quad r = \frac{1+2t_1t_2+2t_1t_2^2t_3+t_2^2t_3^2t_1^2}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}, \quad t = -t_2t_3.$$

Neka su sada $\{a_1, a_2, a_3, a_4\}$ i $\{a_1, a_2, a_3, a_5\}$ regularne racionalne Diofantove četvorke, tj. a_4 i a_5 su rješenja kvadratne jednadžbe

$$(a_1+a_2-a_3-x)^2 - 4(a_1a_2+1)(a_3x+1) = 0.$$

Dobivamo da je

$$\begin{aligned} a_4 &= \frac{-2(1-t_3+t_2t_3)(t_3t_1+1-t_1)(-t_2+1+t_1t_2)(-1+t_1t_2t_3)}{(1+t_1t_2t_3)^3}, \\ a_5 &= \frac{2(t_3+t_2t_3+1)(t_3t_1+t_1+1)(1+t_2+t_1t_2)(1+t_1t_2t_3)}{(-1+t_1t_2t_3)^3}. \end{aligned}$$

Da bi $\{a_1, a_2, a_3, a_4, a_5\}$ bila racionalna Diofantova petorka, treba još zadovoljiti uvjet da je a_4a_5+1 potpun kvadrat. Na taj način, dobivamo uvjet da je

$$\begin{aligned} p(t_1,t_2,t_3) = {} & (-8t_2^3t_3^3 - 8t_3^2t_2^2 - 3t_3^4t_2^4 + 4t_2^2 + 4t_2^2t_3^4 + 4t_2^4t_3^2 + 8t_2^3t_3)t_1^4 \\ & + (8t_2^2t_3 - 16t_2t_3^2 - 8t_2^3t_3^2 + 8t_2 - 8t_2^3t_3^4 - 8t_2^4t_3^3 - 8t_2^2t_3^3 + 8t_3^4t_2)t_1^3 \\ & + (-8t_3^2 - 8t_2^2 - 8t_2t_3 - 8t_2^3t_3^3 - 8t_2^2t_3^4 + 8t_3^3t_2 + 4t_3^4 + 4 - 18t_3^2t_2^2 \\ & \quad + 4t_3^4t_2^4 - 8t_2^4t_3^2 - 16t_2^3t_3)t_1^2 \\ & + (8t_2^4t_3^3 - 8t_2^2t_3 - 16t_2^2t_3^3 - 8t_2t_3^2 - 8t_2 + 8t_3^3 + 8t_2^3t_3^2 - 8t_3)t_1 \\ & - 3 - 8t_2t_3 + 4t_2^4t_3^2 - 8t_3^2t_2^2 + 4t_3^2 + 4t_2^2 + 8t_2^3t_3 \end{aligned} \tag{3.11}$$

potpun kvadrat. Ako izračunamo diskriminantu polinoma p s obzirom na varijablu t_1 i faktoriziramo ju, dobivamo da je jedan od faktora

$$p_1(t_2,t_3) = 3 + 10t_2t_3 - 3t_3^2 + 3t_3^2t_2^2$$

(ostali faktori su ili puno većeg stupnja ili odgovaraju petorkama čiji je jedan element jednak 0). Uvjet $p_1(t_2,t_3) = 0$, koji osigurava da polinom p s obzirom na t_1 ima dvostruki korijen, dovodi do uvjeta da je $9t_3^2+16$ potpun kvadrat, recimo $9t_3^2+16 = (3t_3+u)^2$. Odavde dobivamo

$$t_3 = \frac{16-u^2}{6u},$$
$$t_2 = \frac{u^2+10u+16}{(u-4)(u+4)}.$$

Uvrstimo li ovo u (3.11), dobivamo da je a_4a_5+1 potpun kvadrat. Tako smo dobili dvoparametarsku familiju (u parametrima t_1 i u) racionalnih Diofantovih petorki koje sadrže dvije regularne četvorke (takve petorke su se pojavile kod konstrukcije eliptičkih krivulja velikog ranga s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, Dujella, 2000.).

Sada proširimo neregularnu četvorku $\{a_1,a_3,a_4,a_5\}$ (ili bilo koju drugu neregularnu četvorku sadržanu u petorki $\{a_1,a_2,a_3a_4,a_5\}$) do regularnih petorki $\{a_1,a_3,a_4,a_5,a_6\}$ i $\{a_1,a_3,a_4,a_5,a_7\}$. Tj. a_6 i a_7 su rješenja kvadratne jednadžbe

$$(a_1a_3a_4a_5x+2a_1a_3a_4+a_1+a_3+a_4-a_5-x)^2-4(a_1a_3+1)(a_1a_4+1)(a_3a_4+1)(a_5x+1) = 0.$$

U daljnoj konstrukciji nećemo koristiti a_7, pa zato navodimo samo vrijednosti od a_6:

$$\begin{aligned}a_6 &= 6(u+4)(u+8)(u+2)(u-4)(2t_1u^2+3u^2+20t_1u+12u+32t_1)\\
&\quad\times(t_1u^2+10t_1u+16t_1-6u)(t_1u^2+10t_1u+16t_1+6u)(t_1u^2+10t_1u+16t_1-24-6u)\\
&\quad\times(4096t_1^2+15360t_1^2u+15168t_1^2u^2+5920t_1^2u^3+948t_1^2u^4+60t_1^2u^5+t_1^2u^6-12288t_1u\\
&\quad-7680t_1u^2+480t_1u^4+48t_1u^5-5184u^2-2592u^3-324u^4)^{-2}.\end{aligned}$$

Sada je jedini preostali uvjet da bi $\{a_1,a_2,a_3,a_4,a_5,a_6\}$ bila racionalna Diofantova šestorka taj da a_2a_6+1 bude potpun kvadrat. Ovaj uvjet vodi do kvartike u varijabli t_1 nad poljem $\mathbb{Q}(u)$:

$$\begin{aligned}&(u^{12}+120u^{11}+5496u^{10}+125600u^9+1639440u^8+13075200u^7+65656320u^6\\
&\quad+209203200u^5+419696640u^4+514457600u^3+360185856u^2+125829120u+16777216)t_1^4\\
&+(24u^{12}+1296u^{11}+32256u^{10}+446208u^9+3461760u^8+13047552u^7-208760832u^5\\
&\quad-886210560u^4-1827667968u^3-2113929216u^2-1358954496u-402653184)t_1^3\\
&+(36u^{12}+1296u^{11}+18072u^{10}+48096u^9-1681632u^8-22516992u^7-127051776u^6\\
&\quad-360271872u^5-430497792u^4+197001216u^3+1184366592u^2+1358954496u+603979776)t_1^2\\
&+(-432u^{11}-15552u^{10}-259200u^9-2267136u^8-9116928u^7+145870848u^5\\
&\quad+580386816u^4+1061683200u^3+1019215872u^2+452984832u)t_1\\
&+1296u^{10}+41472u^9+31643136u^6+670032u^8+6054912u^7+96878592u^5+171528192u^4\\
&\quad+169869312u^3+84934656u^2 = z^2.\end{aligned}$$

Budući da ova kvartika ima $\mathbb{Q}(u)$-racionalnu točku u beskonačnosti (jer je izraz uz t_1^4 kvadrat: $(u^2+40u+16)^2(u+8)^4(u+2)^4$) ona se može transformirati u eliptičku krivulju na $\mathbb{Q}(u)$, kao što je opisano u Potpoglavlju 2.2. Pritom singularna točka u beskonačnosti na kvartici odgovara točki u beskonačnosti i dodatnoj točki P_1 na eliptičkoj krivulji. Kvartika ima i $\mathbb{Q}(u)$-racionalnu točku, označimo je s P_2, koja odgovara $t_1 = \frac{-3(u+4)u}{2(u^2+10u+16)}$. Ta točka daje $a_6 = 0$, pa iz nje ne dobivamo racionalnu Diofantovu šestorku. Međutim, točka $2P_2$ na eliptičkoj krivulji odgovara točki na kvartici za koju je

$$t_1 = \frac{3(3u^4+40u^3+368u^2+1280u+1024)}{4(u^2+10u+16)(u+20)u},$$

pa uvrštavanjem ove vrijednosti dobivamo parametarsku familiju racionalnih Diofantovih šestorki

$$\left\{\frac{-12u(u+4)(3u^4+8u^3+224u^2+576u+512)(3u^3+28u^2+256u+256)}{(u+8)(u+2)(u-4)(3u^3+8u^2+144u+128)(3u^4+48u^3+528u^2+1280u+1024)},\right.$$
$$\frac{8u(u+20)(3u^5+8u^4+64u^3-640u^2-2304u-2048)(u+8)(u+2)}{3(u+4)(u-4)(3u^3+8u^2+144u+128)(3u^4+48u^3+528u^2+1280u+1024)},$$
$$\frac{2(u+4)(u-4)(39u^7+776u^6+8096u^5+48640u^4+226048u^3+587776u^2+770048u+393216)}{3(u+8)(u+2)(3u^3+8u^2+144u+128)(3u^4+48u^3+528u^2+1280u+1024)},$$
$$\frac{-8(u^2+4u+32)(3u^3+14u^2-40u-64)(9u^3+8u^2+112u+384)(3u^4+48u^3+528u^2+1280u+1024)}{3(u+8)(u+4)(u+2)(u-4)(3u^3+8u^2+144u+128)^3},$$
$$\frac{4u(u+2)(17u^2+48u+48)(3u^5+8u^4-176u^3-2944u^2-9216u-8192)(3u^3+8u^2+144u+128)(u+8)^2}{3(u+4)(u-4)(3u^4+48u^3+528u^2+1280u+1024)^3},$$
$$\left.\frac{12(u+2)(u-4)(5u+8)(u+4)(3u^2+8u+64)(3u^3+8u^2+144u+128)(3u^4+48u^3+528u^2+1280u+1024)}{(u+8)(16384+69632u+64768u^2+22272u^3+3680u^4+576u^5+9u^6)^2}\right\}$$

koja zadovoljava svojstva iz Teorema 3.3.

Primjerice, za $u=-1$ dobivamo racionalnu Diofantovu šestorku

$$\left\{\frac{27900}{17479}, \frac{471352}{112365}, \frac{261770}{17479}, \frac{185535272}{419265}, \frac{63737828}{526368735}, \frac{79554420}{408480247}\right\}.$$

Uzimajući druge linearne kombinacije točaka P_1 i P_2, može dobiti nove (ali kompliciranije) familije racionalnih Diofantovih šestorki.

3.4 Eliptičke krivulje velikog ranga sa zadanom torzijskom grupom

U Potpoglavlju 2.5 naveli smo tablice s najvećim poznatih rangovima nad $\mathbb{Q}$ i $\mathbb{Q}(t)$ za svaku od 15 torzijskih grupa iz Mazurovog teorema, te posebno naznačili rekordne rangove koji su povezani s eliptičkim krivuljama induciranim s racionalnim Diofantovim trojkama. Krivulje inducirane s racionalnim Diofantovim trojkama mogu imati jednu od sljedeće četiri torzijske grupe: $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, pa ćemo posebno promotriti ta četiri slučaja.

3.4.1 Torzijska grupa $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ nad $\mathbb{Q}(t)$

Eliptičke krivulje inducirane s racionalnim Diofantovim trojkama su u konstrukciji krivulja s velikim rangom prvi puta korištene u članku (Dujella, 2000.). U terminologiji iz Potpoglavlja 2.5, pokazano je da vrijedi: $G(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})\geq 4$ i $B(\mathbb{Z}/2\mathbb{Z}\times$

$\mathbb{Z}/2\mathbb{Z}) \geq 7$. Ideja je bila koristiti racionalne Diofantove petorke $\{a, b, c, d, e\}$ koje sadrže dvije regularne četvorke $\{a, b, c, d\}$ i $\{a, b, c, e\}$. U članku (Dujella, 2000.) je korištena jednoparametarska familija takvih petorki, a u Potpoglavlju 3.3 smo vidjeli kako se može dobiti takva dvoparametarska familija. Sada ako se promotri krivulja inducirana primjerice s $\{b, d, e\}$, tj.

$$y^2 = (bx + 1)(dx + 1)(cx + 1),$$

onda možemo očekivati da će ona imati barem četiri nezavisne točke beskonačnog reda, naime točke s x-koordinatama

$$0, \quad \frac{1}{bde}, \quad a, \quad c.$$

I zaista, u navedenom članku je pokazano da su za spomenutu jednoparametarsku familiju krivulja ove točke nezavisne, pa je rang krivulje nad $\mathbb{Q}(t) \geq 4$. Računanjem ranga (s tadašnjom verzijom mwranka) za male vrijedosti parametra t, dobiven je primjer krivulje ranga 7, što je u to vrijeme bio rekord za torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Slična ideja se može primijeniti za dobivanje familija krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i rangom ≥ 5 nad $\mathbb{Q}(t)$, ako se za polazište uzme neka parametarska familija racionalnih Diofantovih šestorki $\{a, b, c, d, e, f\}$, primjerice ona koju smo dobili u Potpoglavlju 3.2.

Promotrimo krivulju

$$E(t): \quad y^2 = (dx + 1)(ex + 1)(fx + 1).$$

Ona, pored tri očite točke reda dva, ima racionalne točke s x-koordinatama

$$0, \quad \frac{1}{def}, \quad a, \quad b, \quad c.$$

Tvrdimo da su ovih pet točaka nezavisne točke beskonačnog reda nad $\mathbb{Q}(t)$. Budući da je specijalizacijsko preslikavanje, koje za $t_0 \in \mathbb{Q}$ krivulju $E(t)$ nad $\mathbb{Q}(t)$ preslikava u krivulju E_{t_0} nad $\mathbb{Q}$, homomorfizam, dovoljno je naći jedan parametar t_0 za kojeg su ovih pet točaka nezavisne točke beskonačnog reda na E_{t_0}. Nije teško provjeriti da $t_0 = 2$ ima traženo svojstvo (provjerom da je determinanta odgovarajuće matrice visina različita od nule). Stoga je zaista rang krivulje $E(t)$ nad $\mathbb{Q}(t) \geq 5$.

Da bi dobili krivulju nad $\mathbb{Q}(t)$ ranga ≥ 6, krenut ćemo od "jednostavne" familije ranga ≥ 3, te u nekoliko koraka povećavati rang tako da pokušamo zadovoljiti uvjet da dodatna točka (koju će nam sugerirati metoda 2-spusta) bude na krivulji. Slijedit ćemo konstrukciju iz (Dujella & Peral, 2019., 2020.) koja je poboljšana verzija konstrukcije iz (Aguirre, Dujella & Peral, 2012.).

Krećemo od dvoparametarske familije neregularnih Diofantovih četvorki koja sadrži dvije regularne trojke (poput Diofantovog primjera s kojim smo započeli naša razmatranja). Ako onda uzmemo kao polazište jednu od neregularnih podtrojki te četvorke, možemo očekivati da ćemo dobiti krivulju ranga ≥ 3 (pored točaka P i S (odnosno R tako da je $2R = S$), koje su nezavisne zbog neregularnosti trojke, imamo još i točku koja dolazi od četvrtog elementa iz četvorke, a za koju možemo očekivati da je nezavisna s P i S zbog neregularnosti četvorke).

Slijedimo konstrukciju i oznake iz (Dujella, 1996.). Stavimo: $a_1 = a$, $a_2 = b$, $ab+q = x^2$, $a_4 = a+b+2x$, $a_3 = a+4b+4x$. Tada su $\{a_1, a_2, a_4\}$ i $\{a_2, a_3, a_4\}$ regularne $D(q)$-trojke. Da bi dobili $D(q)$-četvorku, ostaje zadovoljiti uvjet da je $a_1a_3 + q$ potpun kvadrat, tj.

$$a(a + 4b + 4x) + q = a^2 + 4ax + 4(x^2 - q) + q = y^2. \tag{3.12}$$

Jednadžbu (3.12) možemo zapisati kao

$$3q = (a + 2x)^2 - y^2 = (a + 2x - y)(a + 2x + y),$$

te je pokušati zadovoljiti tako da stavimo

$$a + 2x - y = 3, \quad a + 2x + y = q.$$

Zbrajanjem dobivamo $q = 2a + 4x - 3$. Uvrstimo li ovo u $ab + q = x^2$, dobivamo

$$a(b + 2) = (x - 1)(x - 3).$$

Stavimo ovdje $x = ak+1$, pa dobivamo $b = ak^2 - 2k - 2$ i $q = 2a(2k+1)+1$. Dakle, dobili smo $D(2a(2k + 1) + 1)$-četvorku

$$\{a, a(k + 1)^2 - 2\,k, a(2k + 1)^2 - 8k - 4, ak^2 - 2k - 2\}$$

s traženim svojstvom (ne)regularnosti. Da bi od nje dobili $D(1)$-trojku, stavimo najprije da je $2a(2k + 1) + 1 = n^2$, tj. $k = \frac{n^2-2a-1}{4a}$, a potom elemente $D(n^2)$-četvorke podijelimo s n. Tako dobivamo sljedeću dvoparametarsku familiju racionalnih $D(1)$-četvorki:

$$\begin{aligned}
c_1(a, n) &= \frac{a}{n}, \\
c_2(a, n) &= \frac{((n - 3)(n - 1) + 2\,a)((n + 1)(n + 3) + 2\,a)}{16\,a\,n}, \\
c_3(a, n) &= \frac{(n - 3)(n - 1)(n + 1)(n + 3)}{4\,a\,n}, \\
c_4(a, n) &= \frac{((n - 3)(n - 1) - 2\,a)((n + 1)(n + 3) - 2\,a)}{16\,a\,n}.
\end{aligned} \tag{3.13}$$

Prema konstrukciji, ova četvorka nije regularna, ali sadrži dvije regularne trojke $\{c_1, c_2, c_4\}$ i $\{c_2, c_3, c_4\}$.

Promotrimo sada eliptičku krivulju induciranu s trojkom $\{c_1, c_2, c_3\}$, tj.

$$y^2 = (c_1(a, n)x + 1)(c_2(a, n)x + 1)(c_3(a, n)x + 1).$$

Primijetimo da smo izabrali neregularnu podtrojku da bi tri poznate točke na krivulji, koje odgovaraju x-koordinatama

$$0, \quad c_4(a, n), \quad \frac{t_{1,2}\,t_{1,3} + t_{1,2}\,t_{2,3} + t_{1,3}\,t_{2,3} + 1}{c_1(a, n)c_2(a, n)c_3(a, n)}$$

gdje je $t_{i,j} = t_{i,j}(a, n) = \sqrt{c_i(a, n)c_j(a, n) + 1}$, $1 \le i < j \le 3$, bile nezavisne. U

terminima a i n, ove tri točke imaju koordinate

$$\begin{aligned}
P_1 &= (0,1),\\
P_2 &= \Big(\frac{(n^2+4n-2a+3)(n^2-4n-2\,a+3)}{16an},\\
&\qquad -\frac{(n^2-2a+3)(n^4-10n^2-4a^2+9)(n^4-2an^2-10n^2-6a+9)}{512a^2n^3}\Big),\\
P_3 &= \Big(\frac{6n}{(n-3)(n+3)}, \frac{(n^2+6a-9)(3n^2+2a-3)}{4a(n-3)(n+3)}\Big).
\end{aligned}$$

Krivulja

$$y^2 = (c_1(a,n)x+1)(c_2(a,n)x+1)(c_3(a,n)x+1)$$

ima torzijsku podgrupu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ i rang ≥ 3 nad $\mathbb{Q}(n,a)$. Točke P_1, P_2 i P_3 su nezavisne točke beskonačnog reda.

Zaista, dovoljno je naći specijalizaciju za koju su točke koje odgovaraju točkama P_1, P_2 i P_3 nezavisne točke beskonačnog reda. Primjerice, za $a=2$ i $n=5$, specijalizirane točke $(0,1)$, $(11/10,-1173/125)$, $(15/8,133/8)$ imaju to svojstvo.

Potražimo sada uvjet na a i n tako da krivulja ima dodatnu racionalnu točku. Na standardan način prebacimo jednadžbu krivulje u oblik $y^2=x^3+Ax^2+Bx$.

Najprije dobivamo jednadžbu

$$y^2 = x(x+c_1(a,n)c_3(a,n)-c_1(a,n)c_2(a,n))(x+c_2(a,n)c_3(a,n)-c_1(a,n)c_2(a,n)),$$

a potom se još rješimo i nazivnika tako da dobijemo oblik

$$y^2 = x^3+Ax^2+Bx \tag{3.14}$$

u kojem su $A(a,n)$ i $B(a,n)$ polinomi s cjelobrojnim koeficijentima:

$$\begin{aligned}
A(a,n) &= 81+108a+108a^2-96a^3-32a^4-180n^2-84an^2-120a^2n^2\\
&\qquad -32a^3n^2+118n^4-28an^4+12a^2n^4-20n^6+4an^6+n^8,\\
B(a,n) &= 4a^2(9+2a-n^2)(3+2a-4n+n^2)(3+2a+4n+n^2)\\
&\qquad \times(-3+2a+3n^2)(-9+4a^2+10n^2-n^4).
\end{aligned}$$

Nakon ovih transformacija, x-koordinate triju poznatih nezavisnih točaka beskonačnog reda postaju

$$\begin{aligned}
x_1 &= 4a^2(3+2a-4n+n^2)(3+2a+4n+n^2),\\
x_2 &= \frac{(3+2a-4n+n^2)(3+2a+4n+n^2)(9-6a-10n^2-2an^2+n^4)^2}{16n^2},\\
x_3 &= 2a(3+2a-4n+n^2)(3+2a+4n+n^2)(-3+2a+3n^2).
\end{aligned}$$

Motivirani metodom 2-spusta, gledamo faktore od B (to su b_1 iz metode 2-spusta) kao kandidate za dodatnu točku, te među njima tražimo one koji daju jednostavne uvjete za taj kandidat stvarno dao dodatnu točku. Primjerice, uvjet da bi $(3+2a-4n+n^2)(-3+2a+3n^2)(-9+4a^2+10n^2-n^4)$ bila x-koordinata dodatne točke je da

$$2(9+6a+8a^2-18n-4an+8n^2-2an^2+2n^3-n^4)$$

bude kvadrat. Jedna od nultočaka diskriminante ovog polinoma (po a) je $n = 7/3$, te tako možemo zadovoljiti taj uvjet. Uvrštavanjem $n = 7/3$, koeficijenti krivulje postaju

$$\begin{aligned} A(a) &= -2(-51200 + 109440a + 38880a^2 + 55404a^3 + 6561a^4) \\ B(a) &= 243a^2(20 + 3a)(-4 + 9a)(16 + 9a)(80 + 9a)(320 + 81a^2), \end{aligned}$$

dok su x-koordinate prethodne tri točke i nove četvrte točke

$$\begin{aligned} x_1 &= 81a^2(-4 + 9a)(80 + 9a) \\ x_2 &= 27a(20 + 3a)(-4 + 9a)(80 + 9a) \\ x_3 &= \frac{1}{441}(-4 + 9a)(80 + 9a)(160 + 171a)^2 \\ x_4 &= 3(20 + 3a)(-4 + 9a)(320 + 81a^2). \end{aligned} \tag{3.15}$$

Slično kao ranije, preko odgovarajuće specijalizacije može se pokazati da su ove četiri točke nezavisne, pa smo dobili krivulju ranga ≥ 4 nad $\mathbb{Q}(a)$.

Koristeći se malom modifikacijom gore opisane metode testiranja faktora polinoma $B(a)$ kao kandidata za dodatne točke (tako da gledamo i faktore od $B'(a) = A(a)^2 - 4B(a)$), moguće je naći veći broj krivulja ranga ≥ 5. Dat ćemo detalje za jednu od njih, kod koje se dodatno rang može povećati na 6.

Da bi $9a(-20+9a)(16+9a)(80+9a)$ bila x-koordinata nove točke na dobivenoj krivulji ranga 4, treba zadovoljiti uvjet da je

$$10(-20 + 9a)(-2 + 9a)$$

kvadrat. Ovaj uvjet odgovara krivulji genusa 0, koja ima očitu točku koja odgovara $a = 2/9$, pa ima parametarsko rješenje:

$$a = \frac{2(-1 + 10w)(1 + 10w)}{9(-1 + 10w^2)}. \tag{3.16}$$

Odgovarajuća krivulja ranga ≥ 5 je $Y^2 = X^3 + A(w)X^2 + B(w)X$, gdje je

$$\begin{aligned} A(w) &= -2(-169 - 12020w^2 + 678000w^4 - 12680000w^6 + 80000000w^8), \\ B(w) &= (-1 + 10w)^2(1 + 10w)^2(-1 + 20w^2)(1 + 80w^2)(-31 + 400w^2) \\ &\quad (-41 + 500w^2)(9 - 200w^2 + 2000w^4). \end{aligned}$$

Pet nezavisnih točaka beskonačnog reda imaju x-koordinate

$$\begin{aligned} x_1 &= \frac{1}{9}(-1 + 10w)^2(1 + 10w)^2(1 + 80w^2)(-41 + 500w^2), \\ x_2 &= \frac{1}{9}(-1 + 10w)(1 + 10w)(1 + 80w^2)(-31 + 400w^2)(-41 + 500w^2), \\ x_3 &= \frac{1}{49}(1 + 80w^2)(-11 + 300w^2)^2(-41 + 500w^2), \\ x_4 &= (1 + 80w^2)(-31 + 400w^2)(9 - 200w^2 + 2000w^4), \\ x_5 &= 9(-1 + 10w)(1 + 10w)(-1 + 20w^2)(-41 + 500w^2). \end{aligned} \tag{3.17}$$

Konačno, da bi dobili krivulju ranga ≥ 6, tražimo da

$$-9(-1 + 10w)^2(1 + 10w)^2(-1 + 20w^2)(-41 + 500w^2)$$

bude x-koordinata nove točke na prethodnoj krivulji ranga 5. To nam daje uvjet da je

$$-(-2+7w)(2+7w)$$

kvadrat, što ponovno odgovara krivulji genusa 0, pa dobivamo parametarsko rješenje

$$w = \frac{2(-1+v)(1+v)}{7(1+v^2)}. \tag{3.18}$$

Dobivena krivulja ranga ≥ 6 ima jednadžbu $Y^2 = X^3 + A(v)X^2 + B(v)X$, gdje je

$$\begin{aligned}
A(v) &= -2(130752711 - 35202346632v^2 + 260292593988v^4 - 1337869740984v^6 \\
&\quad + 1975889131370v^8 - 1337869740984v^{10} + 260292593988v^{12} - 35202346632v^{14} \\
&\quad + 130752711v^{16}), \\
B(v) &= -(9-80v+9v^2)(9+80v+9v^2)(-27+13v^2)^2(-13+27v^2)^2 \\
&\quad (9+8018v^2+9v^4)(31-258v^2+31v^4)(369-542v^2+369v^4) \\
&\quad (14409-41564v^2+400054v^4-41564v^6+14409v^8).
\end{aligned}$$

Šest nezavisnih točaka beskonačnog reda ima x-koordinate

$$\begin{aligned}
x_1 &= -\frac{1}{9}(-27+13v^2)^2(-13+27v^2)^2(9+8018v^2+9v^4) \\
&\quad (369-542v^2+369v^4), \\
x_2 &= -\frac{1}{9}(9-80v+9v^2)(9+80v+9v^2)(-27+13v^2) \\
&\quad (-13+27v^2)(9+8018v^2+9v^4)(369-542v^2+369v^4), \\
x_3 &= -\frac{1}{49}(9+8018v^2+9v^4)(369-542v^2+369v^4) \\
&\quad (661-3478v^2+661v^4)^2, \\
x_4 &= (9-80v+9v^2)(9+80v+9v^2)(369-542v^2+369v^4) \\
&\quad (14409-41564v^2+400054v^4-41564v^6+14409v^8), \\
x_5 &= -441(1+v^2)^2(-27+13v^2)(-13+27v^2)(9+8018v^2+9v^4) \\
&\quad (31-258v^2+31v^4), \\
x_6 &= -9(-27+13v^2)^2(-13+27v^2)^2(9+8018v^2+9v^4) \\
&\quad (31-258v^2+31v^4),
\end{aligned} \tag{3.19}$$

a pripadajuća četvorka je $\{q_1, q_2, q_3, q_4\}$, gdje je

$$\begin{aligned}
q_1 &= \frac{2(-27+13v^2)(-13+27v^2)}{21(9+178v^2+9v^4)}, \\
q_2 &= -\frac{(9+8018v^2+9v^4)(369-542v^2+369v^4)}{42(-27+13v^2)(-13+27v^2)(9+178v^2+9v^4)}, \\
q_3 &= -\frac{160(9+178v^2+9v^4)}{21(-27+13v^2)(-13+27v^2)}, \\
q_4 &= \frac{3(111-418v^2+111v^4)(237+2074v^2+237v^4)}{14(-27+13v^2)(-13+27v^2)(9+178v^2+9v^4)}.
\end{aligned} \tag{3.20}$$

Uzimajući odgovarajuću specijalizaciju možemo lako provjeriti da su danih šest točaka nezavisne te da je rang nad $\mathbb{Q}(v) \geq 6$. No koristeći algoritam koji su razvili Ivica Gusić i Petra Tadić možemo pokazati i da je rang nad $\mathbb{Q}(v)$ točno jednak 6. Da bi to napravili, trebamo naći specijalizaciju za koju je specijalizacijski homomorfizam injektivan (po Silvermanovom specijalizacijskom teoremu znamo da je to točno za sve osim konačno mnogo specijalizacija, no Gusić-Tadić algoritam nam omogućava da pronađemo specijalizacije za koje smo sigurni da su injektivne) te za koju je rang jednak 6. Jedna takva specijalizacija je $v = 5$ za koju su ispunjeni uvjeti sljedećeg teorema iz članka (Gusić & Tadić, 2015.).

Teorem 3.4. *Neka je E eliptička krivulja nad $\mathbb{Q}(t)$ (koja nije izomorfna nekoj krivulji nad $\mathbb{Q}$), dana jednadžbom*

$$E: \quad y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_1, e_2, e_3 \in \mathbb{Z}[t].$$

Pretpostavimo da $t_0 \in \mathbb{Q}$ zadovoljava uvjet da za svaki nekonstantni kvadratno slobodni djelitelj h u $\mathbb{Z}[t]$ polinoma $(e_1-e_2)(e_1-e_3)$, $(e_2-e_1)(e_2-e_3)$ i $(e_3-e_1)(e_3-e_2)$, racionalni broj $h(t_0)$ nije kvadrat racionalnog broja. Tada je specijalizacijski homomorfizam $\sigma : E(\mathbb{Q}(t)) \to E(t_0)(\mathbb{Q})$ injektivan.

U našem slučaju je

$$\begin{aligned}(e_1 - e_2)(e_1 - e_3) = \\ &- (9 - 80v + 9v^2)(9 + 80v + 9v^2)(-27 + 13v^2)^2(-13 + 27v^2)^2 \\ &\times (9 + 8018v^2 + 9v^4)(31 - 258v^2 + 31v^4)(369 - 542v^2 + 369v^4) \\ &\times (14409 - 41564v^2 + 400054v^4 - 41564v^6 + 14409v^8).\end{aligned}$$

Uvrštavajući $v = 5$ u ireduciblne faktore u ovom izrazu, te faktorizirajući dobivene cijele brojeve, lako se vidi da niti jedan od produkata ne daje kvadrat. Slično se provjere i uvjeti za $(e_2 - e_1)(e_2 - e_3)$ i $(e_3 - e_1)(e_3 - e_2)$.

Da je rang krivulje koja se dobije specijalizacijom $v = 5$,

$$y^2 = x^3 + 28734568134020268492 8x^2 + 124322953038724852483327512110950095912 96x,$$

jednak 6, može se provjeriti primjerice programom `mwrank` ili `ellrank` u PARI-ju.

Kombinirajući supstitucije (3.16) i (3.18), vidimo da iz krivulje ranga 4 dane jednadžbom $y^2 = x^3 + A(a)x^2 + B(a)x$ do krivulje ranga 6 možemo doći supstitucijom

$$a = -\frac{2(-27 + 13v^2)(-13 + 27v^2)}{9(9 + 178v^2 + 9v^4)}.$$

U člancima (Dujella & Peral, 2019., 2020.) dane su još četiri supstitucije koje tako-

đer daju krivulje ranga 6:

$$a = -\frac{64(831744 - 40128v + 4288v^2 - 44v^3 + v^4)}{9(-1520 + 88v + v^2)(-2736 - 264v + 5v^2)},$$
$$a = \frac{10732176 + 628992v + 19192v^2 + 576v^3 + 9v^4}{36v(27 + v)(364 + 9v)},$$
$$a = \frac{5(-10 + 6v + v^2)(-18 - 18v + 5v^2)}{9(12 - 2v + v^2)(3 - v + v^2)},$$
$$a = \frac{5(584820 + 135432v - 18288v^2 + 396v^3 + 5v^4)}{9(684 - 66v + v^2)(171 - 33v + v^2)}.$$

Postavlja se pitanje imaju li neke od ovih familija ranga 6 beskonačan presjek, te možemo li tako dobiti beskonačnu familiju krivulja ranga ≥ 7. Da bi odgovorili na to pitanje, možemo usporediti njihove j-invarijante j_i i j_k faktorizirajući njihovu razliku $j_i(v_i) - j_k(v_k)$ te gledajući pojavljuje li se neki faktor koji odgovara krivulji genusa ≤ 1. Uspoređujući drugu i treću od navedenih pet supstitucija, upravo nalazimo takva dva faktora:

$$\begin{aligned} &v_2^2v_3^2 + 72v_2^2v_3 + 88v_2v_3^2 + 1820v_2^2 - 1520v_3^2 \\ &- 96096v_2 - 65664v_3 - 995904 = 0, \end{aligned} \tag{3.21}$$

$$\begin{aligned} &5v_2^2v_3^2 + 216v_2^2v_3 - 264v_2v_3^2 + 3276v_2^2 - 2736v_3^2 \\ &+ 288288v_2 - 196992v_3 - 4979520 = 0. \end{aligned} \tag{3.22}$$

Rješavajući ove jednadžbe po v_2, u oba slučaja dobivamo uvjet

$$54v_3^4 + 2736v_3^3 + 66592v_3^2 + 2987712v_3 + 64393056 = \square. \tag{3.23}$$

Ova kvartika se na standardan način može transformirati u eliptičku krivulju

$$y^2 = x^3 + x^2 - 28174550x + 45644288448$$

koja ima rang 3, pa stoga i eliptička krivulja i kvartika imaju beskonačno mnogo racionalnih točaka. Može se pokazati (detalji su dani u članku (Dujella & Peral, 2020.)) da se tako dobiva beskonačno mnogo eliptičkih krivulja ranga ≥ 7 koje su inducirane racionalnim Diofantovim trojkama (nezavisnost 7 točaka se ponovno provjerava pomoću odgovarajuće specijalizacije, u ovom slučaju $(v_2, v_3) = (-\frac{76}{3}, 26)$).

3.4.2 Torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nad $\mathbb{Q}$

U ovom potpoglavlju ćemo prikazati konstrukciju eliptičke krivulje ranga 12 inducirane s racionalnom Diofantovom trojkom, što je trenutni rekord za krivulje tog oblika, prema članku (Dujella & Peral, 2020.). Prethodni rekordi su bili 7 (prije spomenuta konstrukcija koja koristi racionalne Diofantove petorke – Dujella, 2000.), 9 (pretragom po krivuljama induciranim neregularnim podtrojkama četvorke $\{k-1, k+1, 4k, 16k^3 - 4k\}$ – Dujella, 2007.) te 11 (pretragom po familijama ranga ≥ 5 poput onih iz prethodnog potpoglavlja – Aguirre, Dujella & Peral, 2012., Dujella & Peral, 2019.). Promatramo krivulje oblika

$$E' : \qquad y^2 = (x + ab)(x + ac)(x + bc), \tag{3.24}$$

gdje je $\{a,b,c\}$ racionalna Diofantova trojka. Pritom koristimo prije navedenu parametrizaciju:

$$a=\frac{2t_1(1+t_1t_2(1+t_2t_3))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)},$$
$$b=\frac{2t_2(1+t_2t_3(1+t_3t_1))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)},$$
$$c=\frac{2t_3(1+t_3t_1(1+t_1t_2))}{(-1+t_1t_2t_3)(1+t_1t_2t_3)}.$$

Kao što smo više puta rekli, možemo očekivati da će takva krivulja imati rang ≥ 2 jer na njoj imamo točke P i S. Eksperimentalno smo uočili da je rang >2 ako je $t_3(t_3-t_2)$ potpun kvadrat (te, ciklički, ako je $t_1(t_1-t_3)$ ili $t_2(t_2-t_1)$ potpun kvadrat). Zaista, ako uvrstimo

$$x=-\frac{4(t_2^2t_3-t_3+t_2)(t_3t_1^2t_2+1+t_3t_1)(t_2t_3+t_2t_3^2t_1+1)}{t_3(-1+t_1t_2t_3)^2(1+t_1t_2t_3)^2}$$

(uočimo da je $x+ab=\frac{b(c-b)}{t_2t_3}$) u jednadžbu (3.24), dobivamo

$$y^2=64(1+t_3t_1)^2(t_1t_2t_3-t_2-t_2^2t_3+t_3)^2(t_2t_3+t_2t_3^2t_1+1)^2(1+t_2t_3)^2$$
$$\times(t_3t_1^2t_2+1+t_3t_1)^2(t_3-t_2)t_3^{-3}(-1+t_1t_2t_3)^{-6}(1+t_1t_2t_3)^{-6},$$

što upravo daje uvjet da je $t_3(t_3-t_2)$ potpun kvadrat.

Dakle, ako nađemo trojku racionalnih brojeva (t_1,t_2,t_3) takvi da su

$$t_3(t_3-t_2),\quad t_1(t_1-t_3),\quad t_2(t_2-t_1) \tag{3.25}$$

svi potpuni kvadrati, možemo očekivati da će rank poskočiti barem za 3 te da ćemo dobiti krivulju ranga ≥ 5.

Jedan način za zadovoljiti uvjete (3.25) je pomoću tzv. gotovo savršenih kvadara (savršeni kvadar je onaj kojem su duljine svih bridova, plošnih dijagonala i prostorne dijagonale prirodni brojevi – otvoren je problem postoji li takav kvadar, a gotovo savršen kvadar je onaj u kojem ispustimo jedan od 7 uvjeta). Zaista, ako stavimo

$$t_3=s_3^2,\ \ t_1=-s_1^2,\ \ t_2=s_2^2,\ \ s_3^2-s_2^2=s_4^2,$$

imamo

$$s_1^2+s_2^2=\square,\ \ s_2^2+s_4^2=\square,\ \ s_1^2+s_2^2+s_4^2=\square, \tag{3.26}$$

pa smo dobili gotovo savršen kvadar (samo jedna plošna dijagonala nije cjelobrojna). Poznata su parametarska rješenja sustava (3.26) (Luijk, 2000.):

$$s_1=2(m^2+m+1)(m^2-1)^2(m^2+1+4m),$$
$$s_2=4(m^2+m+1)(2m+1)(m^2-1)(2m+m^2),$$
$$s_4=(2m+1)(2m+m^2)(3m^2+2m+1)(m^2+2m+3).$$

što nam daje

$$t_1=-4(m^2+m+1)^2(m^2-1)^4(m^2+1+4m)^2,$$
$$t_2=16(m^2+m+1)^2(2m+1)^2(m^2-1)^2(2m+m^2)^2,$$
$$t_3=m^2(2m+1)^2(m+2)^2(5m^2+8m+5)^2(m^2+1)^2.$$

Prikazat ćemo sada drugi način za dobivanje dvoparametarskog rješenja od (3.25) koje će biti prikladnije za pretragu za specijalizacijama većeg ranga. Prva dva uvjeta možemo zadovoljiti tako da stavimo

$$t_3(t_3-t_2)=(t_3+u)^2, \quad t_1(t_1-t_3)=(t_1+v)^2$$

pa dobijemo

$$t_2=-\frac{u(2t_3+u)}{t_3}, \quad t_3=-\frac{v(2t_1+v)}{t_1}.$$

Uvrstimo li ovo u treći uvjet $t_2(t_2-t_1)=\square$, dobivamo

$$\begin{aligned}(8uv^2-2u^2v)t_1^3+(-8u^3v+15u^2v^2+u^4+8uv^3)t_1^2\\ +(-4u^3v^2+16u^2v^3+2uv^4)t_1+4u^2v^4=\square.\end{aligned} \tag{3.27}$$

Jednadžbu (3.27) možemo shvatiti kao eliptičku krivulju nad $\mathbb{Q}(u,v)$, s očitom točkom $P_1=(0,2uv^2)$. Ako uzmemo točku $2P_1$, dobivamo

$$t_1=\frac{v^2(-v+16u)}{8u(-4v+u)},$$

što daje trojku

$$\begin{aligned}a&=-\frac{v^2(-v+16u)(16v^2-64u^2-v^4+16uv^3-4v^5u+v^4u^2)}{u(2+v)(4-2v+v^2)(v-2)(v^2+2v+4)(2u-v)(2u+v)(-4v+u)},\\ b&=\frac{16u(-4v+u)v(4v-64u+16uv^2-4u^2v-v^5+4u^2v^3)}{(2+v)(4-2v+v^2)(v-2)(v^2+2v+4)(2u-v)(2u+v)(-v+16u)},\\ c&=\frac{4(256uv-64u^2-16v^4+64u^2v^2+v^6-16v^5u)(2u-v)(2u+v)}{u(2+v)(4-2v+v^2)(v-2)(v^2+2v+4)(-v+16u)(-4v+u)}.\end{aligned}$$

Tako smo dobili eliptičku krivulju ranga ≥ 5 nad $\mathbb{Q}(u,v)$. Zaista, ako jednadžbu krivulje zapišemo u obliku $y^2=x^3+Ax^2+Bx$, gdje je

$$\begin{aligned}A=v(&256v^{13}-32v^{15}+v^{17}+140288v^9u^2+741888v^7u^4-4096v^{10}u-1167360v^8u^3\\ &-21258240v^6u^5-7936v^{12}u+664832v^{10}u^3+11440128v^8u^5+32192v^{11}u^2\\ &-2785824v^9u^4-32380416v^7u^6+28747776v^5u^6+6463488v^6u^7+71860224u^7v^4\\ &-2205696u^8v^5+1536v^{14}u-24192v^{13}u^2-22528v^{12}u^3+591360v^{11}u^4\\ &-3244800u^5v^{10}-128483328v^3u^8-12979200v^8u^7+7816v^{15}u^2-36160v^{14}u^3\\ &-8616v^{13}u^4+100992v^{12}u^5-128v^{16}u-2023776v^{11}u^6+4v^{18}u-449v^{17}u^2\\ &+7824v^{16}u^3-31368v^{15}u^4+2860032v^{10}u^7+70176v^{14}u^5+112296v^13u^6\\ &+9461760v^7u^8-2785824v^9u^8-332160v^{12}u^7+128188416v^2u^9-37027840v^4u^9\\ &-1441792v^6u^9+2659328v^8u^9+46368v^{11}u^8-6193152u^{10}v^5+515072u^{10}v^7\\ &-291840u^9v^{10}+16818240v^9u^6-29425664vu^{10}+32014336u^{10}v^3+140288v^9u^{10}\\ &-2097152u^{11}v^2+1572864u^{11}v^4-507904u^{11}v^6-16384u^{11}v^8+65536u^{12}v^5\\ &+65536u^{12}v-131072u^{12}v^3+1048576u^{11}),\end{aligned}$$

$$\begin{aligned}B &= 4(8vu^2-8u^2+16vu-v^2u+v^2+2v^3)(8vu^2+8u^2-16vu-v^2u-v^2+2v^3)\\ &\quad\times(-16v^2+64u^2+v^4-16v^3u)(4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)\\ &\quad\times(2vu^2-16u^2+2vu+8v^2u-4v^2-v^3)(16vu-4u^2-v^4+4v^2u^2)\\ &\quad\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)\\ &\quad\times(2vu^2+16u^2-2vu+8v^2u+4v^2-v^3)(-v+16u)^2(-4v+u)^2u^2v^3,\end{aligned}$$

tada su pet nezavisnih točaka beskonačnog reda

$$\begin{aligned}P &= (-4(4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)(-4v+u)^2(-v+16u)^2\\ &\quad\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)u^2v^3,\\ &\quad 8(64v^2u^2-64u^2-16v^5u+256vu+v^6-16v^4)(4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)\\ &\quad\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)(2u-v)^2(2u+v)^2(-4v+u)^2\\ &\quad\times(-v+16u)^2u^2v^3),\\ R &= (4(16vu-4u^2-v^4+4v^2u^2)(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)\\ &\quad\times(8vu^2-8u^2+16vu-v^2u+v^2+2v^3)(8vu^2+8u^2-16vu-v^2u-v^2+2v^3)\\ &\quad\times(-v+16u)(-4v+u)vu,\\ &\quad 4(8vu^2-8u^2+16vu-v^2u+v^2+2v^3)(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)\\ &\quad\times(8vu^2+8u^2+32vu-16v^2u-4v^2-v^3)(16vu-4u^2-v^4+4v^2u^2)\\ &\quad\times(8vu^2+8u^2-16vu-v^2u-v^2+2v^3)(8vu^2-8u^2-32vu-16v^2u+4v^2-v^3)\\ &\quad\times(2u+v)(2u-v)v^2(-v+16u)(-4v+u)u),\\ T_1 &= (16(16vu-4u^2-v^4+4v^2u^2)(2vu^2-16u^2+2vu+8v^2u-4v^2-v^3)\\ &\quad\times(2vu^2+16u^2-2vu+8v^2u+4v^2-v^3)(4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)\\ &\quad\times(-v+16u)(-4v+u)u,\\ &\quad 8(16vu-4u^2-v^4+4v^2u^2)(2vu^2-16u^2+2vu+8v^2u-4v^2-v^3)\\ &\quad\times(2vu^2+16u^2-2vu+8v^2u+4v^2-v^3)(-v+16u-4v^2u+vu^2)\\ &\quad\times(v^6-16v^5u+256vu-64u^2-16v^4+64v^2u^2)(8u^2-vu+2v^2)\\ &\quad\times(4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)(-v+16u)(-4v+u)u),\\ T_2 &= (-4(8vu^2-8u^2+16vu-v^2u+v^2+2v^3)(-16v^2+64u^2+v^4-16v^3u)\\ &\quad\times(16vu-4u^2-v^4+4v^2u^2)(8vu^2+8u^2-16vu-v^2u-v^2+2v^3)\\ &\quad\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)(-4v+u)u/v^2,\\ &\quad 4(8vu^2-8u^2+16vu-v^2u+v^2+2v^3)(8vu^2+8u^2-16vu-v^2u-v^2+2v^3)\\ &\quad\times(16vu-4u^2-v^4+4v^2u^2)(-16v^2+64u^2+v^4-16v^3u)(2u+v)(2u-v)\\ &\quad\times(8u^2-16vu-v^2)(-16v^4+64v^2u^2+v^6-16v^5u+256vu-64u^2)\\ &\quad\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)(-4v+u)u/v^3),\end{aligned}$$

$$\begin{aligned}T_3 = ((&4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)(-16v^2+64u^2+v^4-16v^3u)\\ &\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)(2u^2+8vu-v^2)^2(-v+16u),\\ 2&(-16v^2+64u^2+v^4-16v^3u)(8vu^2-8u^2-32vu-16v^2u+4v^2-v^3)\\ &\times(8vu^2+8u^2+32vu-16v^2u-4v^2-v^3)(-v+16u-4v^2u+vu^2)\\ &\times(16v^2-64u^2-v^4+16v^3u-4v^5u+v^4u^2)(2u^2+8vu-v^2)\\ &\times(4v-64u+16v^2u-4vu^2-v^5+4v^3u^2)(2u-v)(2u+v)(-v+16u)).\end{aligned}$$

Ovdje točka P odgovara točki $(0,abc)$ na $y^2=(x+ab)(x+ac)(x+bc)$, točka R zadovoljava $2R=S$, gdje S odgovara točki $(1,rst)$ na $y^2=(x+ab)(x+ac)(x+bc)$, točka T_1 odgovara uvjetu $t_3(t_3-t_2)=\square$, točka T_2 odgovara uvjetu $t_1(t_1-t_3)=\square$, dok točka T_3 odgovara uvjetu $t_2(t_2-t_1)=\square$. Za provjeriti nezavisnost, dovoljno je naći specijalizaciju (u_0,v_0) za koju su točke P, R, T_1, T_2 i T_3 nezavisne na specijaliziranoj krivulji nad $\mathbb{Q}$. Može se provjeriti da to vrijedi primjerice za $(u_0,v_0)=(2,1)$, budući da su $(170605,39532697)$, $(302665,-66247363)$, $(795565,-637321303)$, $(-447095,-24260803)$, $(8673115/4,-25165674989/8)$ nezavisne točke na krivulji $y^2=x^3+21361758597x^2-28803989016278714304x$.

Sada tražimo specijalizacije (u,v) za koje je rang bitno veći od 5, posebice one ranga 11 i 12. Kombiniramo neke od metoda za konstrukciju eliptičkih krivulja velikog ranga koje smo naveli u Poglavlju 2.5. Tražimo krivulje s relativno velikom Mestre-Nagaovom sumom

$$S(N,E)=\sum_{p=2}^{N}\frac{-a_p+2}{p+1-a_p}\log p,$$

gdje je $a_p=a_p(E)=p+1-\#E(\mathbb{F}_p)$, te velikim Selmerovim rangom (koristimo `mwrank` s opcijom `-s`). U potrazi za krivuljama ranga 12 možemo dodatno koristiti uvjet da je $w_E=1$, (preko PARI funkcije `ellrootno`), jer "Parity Conjecture" povlači da je tada rang paran. Osim u dvoparametarskoj familiji, pretragu vršimo i po nekim jednoparametarskim podfamilijama (primjerice za $u=v$). Za krivulje koje prođu sve testove, rang možemo pokušati izračunati pomoću programa `mwrank` ili `ellrank`.

Nalazimo krivulje ranga 11 za sljedeće vrijednosti parametara: $(u,v)=$

$$\left(\frac{11}{24},\frac{5}{9}\right),\left(-\frac{145}{6},\frac{29}{12}\right),\left(\frac{136}{19},\frac{68}{5}\right),\left(-\frac{16}{77},\frac{4}{21}\right),\left(\frac{473}{705},\frac{43}{47}\right),\left(-\frac{89}{135},\frac{89}{45}\right),$$
$$\left(-\frac{62}{43},\frac{93}{43}\right),\left(\frac{71}{273},\frac{142}{91}\right),\left(\frac{224}{67},\frac{7}{2}\right),\left(-\frac{1032}{923},\frac{172}{71}\right),\left(-\frac{1501}{87},\frac{158}{87}\right),$$
$$\left(\frac{1358}{1007},\frac{194}{53}\right),\left(-\frac{2072}{1819},\frac{148}{107}\right),\left(\frac{454}{481},\frac{227}{37}\right),\left(\frac{77}{173},\frac{77}{173}\right),\left(\frac{163}{137},\frac{163}{137}\right).$$

Spomenimo da krivulja koja odgovara parametrima $(u,v)=(-\frac{62}{43},\frac{93}{43})$, tj. trojki

$$\{a,b,c\}=\left\{\frac{21409906185}{74591676404},-\frac{31580198976}{18647919101},-\frac{10309975195}{18647919101}\right\},$$

s minimalnom Weierstrassovom jednadžbom

$$\begin{aligned}y^2+xy=x^3-x^2&-212522766406527987397078192 17x\\ &+938627524108684110053910801619511357084941,\end{aligned}$$

je krivulja s najmanjom diskriminantom među svim poznatim krivuljama s rangom 11 i torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Konačno, nalazimo i jednu krivulju ranga 12 i to za $(u, v) = (-\frac{95}{33}, \frac{50}{57})$, tj.

$$\{a, b, c\} = \left\{ \frac{6125241375}{11907531272}, \frac{5535371271425}{14277129995128}, -\frac{273138178560}{153430695649} \right\},$$

s minimalnom Weierstrassovom jednadžbom

$$y^2 + xy + y = x^3 - x^2 - 1444491707528591356856089186460491195711268950880x \\ + 55992158377962542124868358493956176245622429017043746155585148204143974 7,$$

torzijskim točkama

$$\mathcal{O},\ (9109543899208458360203 49, -45547719496042291801017 5),$$
$$(-5448727291190824028230629/4, 5448727291190824028230625/8),$$
$$(4512274328768601710373 09, -22561371643843008551865 5),$$

i 12 nezavisnih točaka beskonačnog reda

$$P_1 = (1588509325006496091348 09, 5783347758167145246162762217040428 45),$$
$$P_2 = (3511040172007843863922 09, 3098979669449451161946241983325938 45),$$
$$P_3 = (-4277226602909288139831 35, -1048576645526111528109185629948786727),$$
$$P_4 = (9545007819393757627429 09, 2253260088633452205430716187833709 45),$$
$$P_5 = (4236795982596765919909 09, 1548298109595478525933329876359661 45),$$
$$P_6 = (1535808449095818094207905, 1401421444080498380369785533616999513),$$
$$P_7 = (4448018874220560215353 83, 7356921614861339981734798685975894 5),$$
$$P_8 = (-1206006015871044278678751, -7402102456092176151432694523354543 75),$$
$$P_9 = (-1925622924386935236170 91, -9115568896405487670646301594563138 55),$$
$$P_{10} = (1050887966852735668292124 9, 3385180005318116892656836282547638 5625),$$
$$P_{11} = (9515144107333695556703 49, 2166765209212768052997033114390498 25),$$
$$P_{12} = (-7355680099955426717481581/81,$$
$$-6057056719332256026906514463906338491 25/729).$$

Spomenimo još i da se za $t_1 = \frac{44}{29}$, $t_2 = \frac{17}{42}$, $t_3 = \frac{3}{44}$, tj. $a = \frac{815848}{164547}$, $b = \frac{1512524}{1810017}$, $c = \frac{32060}{201113}$, dobiva krivulja

$$y^2 = x^3 + x^2 - 1939363608964699467721 76x \\ + 2945364125371813050613622952241674 0$$

ranga 10, koja je krivulja s najmanjim konduktorom među svim poznatim krivuljama s rangom 10 i torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ova krivulja je pronađena pretragom "grubom silom" po svim t_1, t_2, t_3 s malim brojnicima i nazivnicima (a ne po parametarskim familijama).

3.4.3 Torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

U ovom potpoglavlju prikazat ćemo konstrukciju eliptičkih krivulja induciranih Diofantovim trojkama s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ i rangom 4 nad $\mathbb{Q}(t)$ te

rangom 9 nad $\mathbb{Q}$. Rezultati su dobiveni u članku (Dujella & Peral, 2014.) te kasnije dopunjeni dodatnim primjerom krivulje ranga 9 (Dujella & Peral, 2021.) i još uvijek predstavljaju rekordne rangove za krivulje s tom torzijskom grupom (bez obzira jesu li inducirane racionalnim Diofantovim trojkama ili ne). Još jednu krivulju ranga 9 je, drugim metodama, našao Klagsbrun 2020.

U Potpoglavlju 2.4 vidjeli smo da je svaka eliptička krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ izomorfna krivulji oblika

$$y^2 = x(x + x_1^2)(x + x_2^2), \quad x_1, x_2 \in \mathbb{Q} \setminus \{0\},\ x_1 \neq \pm x_2. \tag{3.28}$$

Pritom je točka $(x_1x_2, x_1x_2(x_1 + x_2))$ racionalna točka na krivulji reda 4.

Eliptičku krivulju $y^2 = (ax + 1)(bx + 1)(cx + 1)$ induciranu racionalnom Diofantovom trojkom $\{a, b, c\}$ možemo na standardan način transformirati najprije u $y^2 = (x + ab)(x + ac)(x + bc)$, a potom translacijom u oblik

$$y^2 = x(x + ac - ab)(x + bc - ab). \tag{3.29}$$

Usporedimo li jednadžbe (3.28) i (3.29), vidimo da ako uspijemo naći racionalnu Diofantovu trojku $\{a, b, c\}$ takvu da su $ac - ab$ i $bc - ab$ kvadrati racionalnih brojeva, onda će eliptička krivulja inducirana s $\{a, b, c\}$ imati torzijsku podgrupu izomorfnu sa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Možemo očekivati da će ta krivulja imati pozitivan rang budući da (3.29) sadrži točku (ab, abc). Jedan jednostavan način za zadovoljiti ova dva uvjeta jest izabrati a i b tako da je $ab = -1$. Tada će $ac - ab = ac + 1$ i $bc - ab = bc + 1$ biti kvadrati po definiciji Diofantove trojke. Preostaje naći racionalan broj c tako da $\{a, -1/a, c\}$ bude racionalna Diofantova trojka. Imamo sljedeći sustav jednadžbi

$$ac + 1 = p^2, \quad -\frac{c}{a} + 1 = q^2. \tag{3.30}$$

Uvrstimo li $ac + 1 = p^2$ $-\frac{c}{a} + 1 = q^2$, dobivamo

$$1 - p^2 + a^2 = z^2, \tag{3.31}$$

gdje je $z = aq$. Racionalna rješenja jednadžbe (3.31) možemo parametrizirati tako da stavimo

$$1 - p^2 + a^2 = (-a + (p - 1)\tau)^2.$$

"Simetričniju" parametrizaciju dobijemo ako stavimo da je

$$p = \frac{\tau + \alpha}{\tau - \alpha},$$

te dobivamo da je

$$a = \frac{\alpha\tau + 1}{\tau - \alpha}.$$

Uvrstimo li ovo u (3.29), nakon malo sređivanja, dobivamo

$$y^2 = x^3 + 2(\alpha^2 + \tau^2 + 4\alpha^2\tau^2 + \alpha^4\tau^2 + \alpha^2\tau^4)x^2 + (\tau + \alpha)^2(\alpha\tau - 1)^2(\tau - \alpha)^2(\alpha\tau + 1)^2x. \tag{3.32}$$

Kao i ranije, dodatne točke na krivulji oblika $y^2 = x^3 + Ax^2 + Bx$ pokušavamo dobiti promatrajući faktore od B. U ovom slučaju, želimo da $x = (\tau + \alpha)^2(\alpha\tau - 1)(\alpha\tau + 1)$ zadovolji jednadžbu (3.32), što nam daje uvjet

$$\tau^2 + \alpha^2 + 2 = \square. \tag{3.33}$$

S druge strane, ako želimo da $x = (\tau + \alpha)(\alpha\tau - 1)^2(\tau - \alpha)$ zadovoljava jednadžbu (3.32), dobivamo uvjet

$$\alpha^2\tau^2 + 2\alpha^2 + 1 = \square. \tag{3.34}$$

Tražimo neko parametarsko rješenje sustava jednadžbi (3.33) i (3.34). Prema konstrukciji kako smo došli do ovog sustava, to parametarsko rješenja bi trebalo dati familiju eliptičkih krivulja ranga barem 3. Međutim, vidjet ćemo da, uz ponešto sreće, dobivamo familiju ranga 4.

Poznata su parametarska rješenja jednadžbe (3.33). Uzet ćemo rješenje dano u knjizi (Carmichael, 1959):

$$\tau = \frac{r^2 - s^2 - 2t^2 + 2v^2}{2(rt + sv)}, \quad \alpha = \frac{rs - 2tv}{rt + sv}. \tag{3.35}$$

Zbog homogenosti je jasno da ako koristimo racionalne parametre, onda jedan parametar možemo eliminirati. No zapravo je moguće eliminirati dva parametra. Kad ćemo tražiti pojedinačne krivulje s velikim rangom, pokazat će se prikladno raditi s četiri cjelobrojna parametra. No traženje parametarske familije velikog ranga će se olakšati ako (motivirani i nekim eksperimentalnim podatcima) uzmemo da je $v = 0$, $r = s + t + 1$. Ako sada uvrstimo (3.35) u (3.34), dobivamo kvartiku u varijabli s:

$$\begin{aligned}(12t^2 + 8t + 4)s^4 + (12t^3 + 20t^2 + 12t + 4)s^3 \\ + (13t^4 + 12t^3 + 10t^2 + 4t + 1)s^2 + (8t^5 + 8t^4)s + 4t^6 + 8t^5 + 4t^4 = g^2.\end{aligned} \tag{3.36}$$

Budući da ona sadrži racionalnu točku $(0, 2t^3 + 2t^2)$, može se na standardan način transformirati u eliptičku krivulju nad $\mathbb{Q}(t)$:

$$\begin{aligned}w^3 + (13t^4 + 12t^3 + 10t^2 + 4t + 1)w^2 \\ + (-96t^8 - 256t^6 - 256t^7 - 128t^5 - 32t^4)w \\ - 1152t^{12} - 3840t^{11} - 5504t^{10} - 4608t^9 - 2432t^8 - 768t^7 - 128t^6 = h^2.\end{aligned} \tag{3.37}$$

Provjeravajući faktore od

$$1152t^{12} + 3840t^{11} + 5504t^{10} + 4608t^9 + 2432t^8 + 768t^7 + 128t^6 = 128t^6(t+1)^2(3t^2+2t+1)^2$$

kao moguće w-koordinate točaka na (3.37), nalazimo da točka $(4t^2(3t^2 + 2t + 1), 4t^2(t-1)(3t+1)(3t^2+2t+1))$ leži na (3.37). Transformirajući ovu točku natrag na kvartiku (3.36), nalazimo da je

$$s = -\frac{7t^3 + 9t^2 + 3t + 1}{t^2 + 6t + 3}.$$

Dalje lako izračunamo:

$$\begin{aligned}
\tau =&\frac{(3t^2+6t+1)(5t^2+2t-1)}{4t(t-1)(3t+1)(t+1)},\\
\alpha =&-\frac{(t+1)(7t^2+2t+1)}{t(t^2+6t+3)},\\
a =&-\frac{(t+1)(31t^4+52t^3+22t^2-4t-1)(3t^2+2t+1)}{t(11t^4+12t^3+2t^2-4t-1)(9t^2+14t+7)},\\
b =&\frac{t(11t^4+12t^3+2t^2-4t-1)(9t^2+14t+7)}{(t+1)(31t^4+52t^3+22t^2-4t-1)(3t^2+2t+1)},\\
c =&\big(16(t-1)(3t+1)(t+1)t(t^2+6t+3)(3t^2+6t+1)\\
&(5t^2+2t-1)(7t^2+2t+1)\big)/\\
&((11t^4+12t^3+2t^2-4t-1)(9t^2+14t+7)\\
&(31t^4+52t^3+22t^2-4t-1)(3t^2+2t+1)).
\end{aligned}$$

Sada tvrdimo da inducirana eliptička krivulja

$$E: \quad y^2=x^3+A(t)x^2+B(t)x,$$

gdje je

$$\begin{aligned}
A(t)=&\\
&2(87671889t^{24}+854321688t^{23}+3766024692t^{22}+9923033928t^{21}\\
&+17428851514t^{20}+21621621928t^{19}+19950275060t^{18}\\
&+15200715960t^{17}+11789354375t^{16}+10470452464t^{15}+8925222696t^{14}\\
&+5984900048t^{13}+2829340620t^{12}+820299856t^{11}+59930952t^{10}\\
&-66320528t^9-35768977t^8-9381000t^7-1017244t^6+262760t^5\\
&+159130t^4+41096t^3+6468t^2+600t+25),\\
B(t)=&\\
&(t^2-2t-1)^2(69t^4+148t^3+78t^2+4t+1)^2(13t^2-2t-1)^2\\
&\times(9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\times(9t^2+14t+7)^2(31t^4+52t^3+22t^2-4t-1)^2(3t^2+2t+1)^2,
\end{aligned}$$

ima rang ≥ 4 nad $\mathbb{Q}(t)$. Zaista, ona sadrži četiri točke s x-koordinatama

$$\begin{aligned}
X_1=&(9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\times(69t^4+148t^3+78t^2+4t+1)^2,\\
X_2=&(3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1)\\
&\times(9t^4+28t^3+18t^2+4t+1)(11t^4+12t^3+2t^2-4t-1)^2\\
&\times(31t^4+52t^3+22t^2-4t-1),\\
X_3=&(3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1)\\
&\times(9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)\\
&\times(69t^4+148t^3+78t^2+4t+1),\\
X_4=&-(3t^2+2t+1)^2(9t^2+14t+7)^2(11t^4+12t^3+2t^2-4t-1)^2\\
&\times(31t^4+52t^3+22t^2-4t-1)^2.
\end{aligned}$$

Uočimo da točka X_4 odgovara točki $(-1,-c)$ na krivulji (3.29). Ostale točke se nalaze tražeći točke na E s x-koordinatama koje su djelitelji polinoma $B(t)$. Odgovarajuća specijalizacija, npr. $t=2$, dokazuje da su točke P_1,P_2,P_3,P_4, s x-koordinatama X_1,X_2,X_3,X_4, nezavisne točke beskonačnog reda. Stoga smo dobili eliptičku krivulju nad $\mathbb{Q}(t)$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ i rangom ≥ 4. Spomenimo da su prethodni rekord s krivuljama ranga ≥ 3 neovisno bili pronašli Lecacheux (2003.), Elkies (2007.) i Eroshkin (2008.).

Koristeći prije spomenuti Gusić-Tadić algoritam, može se pokazati da je $\mathrm{rank}(E(\mathbb{Q}(t)))=4$ te štoviše da su točke P_1,P_2,P_3,P_4 slobodni generatori od $E(\mathbb{Q}(t))$. Za tu svrhu, jednadžbu krivulje E zapišemo u obliku

$$y^2=(x-e_1)(x-e_2)(x-e_3),\quad e_1,e_2,e_3\in\mathbb{Z}[t],$$

promatramo kvadratno-slobodne faktore od $(e_1-e_2)(e_1-e_3)$, $(e_2-e_1)(e_2-e_3)$ i $(e_3-e_1)(e_3-e_2)$, te tražimo $t_0\in\mathbb{Q}$ koji zadovoljava uvjete Teorema 3.4. Tada će specijalizacijski homomorfizam $E(\mathbb{Q}(t))\to E(t_0)(\mathbb{Q})$ biti injektivan. Nadalje, ako je $|E(t_0)(\mathbb{Q})_{\mathrm{tors}}|=8$ i postoje točke $Q_1,\ldots,Q_r\in E(\mathbb{Q}(t))$ takve da su $Q_1(t_0),\ldots,Q_r(t_0)$ slobodni generatori od $E(t_0)(\mathbb{Q})$, onda je specijalizacijski homomorfizam $E(\mathbb{Q}(t))\to E(t_0)(\mathbb{Q})$ izomorfizam. Stoga $E(\mathbb{Q}(t))$ i $E(t_0)(\mathbb{Q})$ imaju isti rang r i $Q_1,\ldots,Q_r$ su slobodni generatori od $E(\mathbb{Q}(t))$. Nije teško provjeriti da $t_0=15$ zadovoljava uvjete Teorema 3.4. Koristeći `mwrank`, dobivamo da je $\mathrm{rank}(E(15)(\mathbb{Q}))=4$, te smo tako dokazali da je

$$\mathrm{rank}(E(\mathbb{Q}(t)))=4.$$

Nadalje, `mwrank` nalazi i slobodne generatore R_1,R_2,R_3,R_4 od $E(15)(\mathbb{Q})$. Ako prikažemo $P_1(15),P_2(15),P_3(15),P_4(15)$ u bazi R_1,R_2,R_3,R_4 (modulo torzija), dobivamo da je determinanta transformacijske matrice jednaka -1. Stoga $P_1(15)$, $P_2(15)$, $P_3(15)$, $P_4(15)$ također čine Mordell-Weilovu bazu za $E(15)(\mathbb{Q})$, te zaključujemo da su zaista P_1,P_2,P_3,P_4 slobodni generatori $E(\mathbb{Q}(t))$.

Pokažimo sada kako dobiti krivulju induciranu racionalnom Diofantovom trojkom s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ i rangom 9 nad $\mathbb{Q}$. Prethodno su bile poznate takve krivulje ranga 7 (Dujella, 2007.) koje su dobivene, uz gornju notaciju, za $\alpha=2$. Za dobiti krivulje ranga 9, pretraživat ćemo krivulje koji odgovaraju τ i α oblika (3.35). Kao što smo već spomenuli, te krivulje ranga 9 ne predstavljaju samo rekord među krivuljama induciranim Diofantovim trojkama, nego i među svim krivuljama s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Prethodne rekorde s rangom 8 su drugim metodama bili našli Elkies (2005.), Eroshkin (2008.) te Eroshkin & Dujella (2008.).

U članku (Dujella & Peral, 2014.), pretraga je vršena po svim cjelobrojnim parametrima r,s,t,v u rasponu $|r|+|s|+|t|+|v|\leq 420$. Korištene su prije opisane metode za "sijanje" i nalaženje dobrih kandidata za veliki rang, koje uključuju računanje Mestre-Nagaovih suma, Selmerovog ranka i Mestreove uvjetne gornje ograde za rang. Potom je za te kandidate rang računan pomoću programa `mwrank`. Na taj način je pronađeno pet krivulja ranga 8, koje odgovaraju parametrima

$$(r,s,t,v)=$$
$$(20,-11,25,68),(82,9,73,30),(55,31,142,15),(91,55,33,104),(157,127,43,12),$$

te jedna krivulja ranga 9, koja odgovara parametrima $(r,s,t,v)=(155,54,96,106)$.

Ta krivulja je inducirana Diofantovom trojkom

$$\left\{\frac{301273}{556614}, -\frac{556614}{301273}, -\frac{535707232}{290125899}\right\}.$$

Minimalna Weierstrassova jednadžba joj je

$$y^2 = x^3 + x^2 - 614100573770591167151980664421796984 0x + 585743317734880315858628578592963147780809517115906318 8,$$

torzijske točke su

$$\mathcal{O}, (-2861469472720778854, 0), (1431017969855150171, 0), (1430451502865628682, 0), (1381707195787460036, -10099001059166712975345063 0), (1381707195787460036, 10099001059166712975345063 0), (1480328743922840306, -10333725935570697294006372 0), (1480328743922840306, 10333725935570697294006372 0),$$

dok je devet nezavisnih točaka beskonačnog reda

$$(-612695149795875652, 30643098243490773810273083 58), (-431590874944672564, 29030057680838731041588594 30), (187501554154394546, 21708470738974153948323510 00), (-1383500708967173302, 34213149431638337745679174 08), (1428519047239049546, 45515491200217791375480000), (1430248713837731282, 81822600086915483159364 0), (1429305792931194266, 29012125229927554835577 60), (103900694057898826, 22848413651245620790872062 40), (1429854291102331316, 17269365047672031757199 10).$$

Ista krivulja se dobiva i za parametre $(r, s, t, v) = (82, -19, 87, 14)$, tj. racionalnu Diofantovu trojku

$$\left\{-\frac{126555}{2686}, \frac{2686}{126555}, -\frac{9107022944}{249946125}\right\}.$$

U člancima (Dujella & Peral, 2019., 2021.) pretraga je proširena za različite specijalne vrijednosti parametara r, s, t, v izvan prije spomenutog raspona. Tako je pronađeno još pet krivulja ranga 8, koje odgovaraju parametrima

$$(r, s, t, v) = (131, -29, 49, 96), (186, -57, 62, 199), (107, 107, 149, 430), (103, 103, 168, 725), (749, 749, 138, 245),$$

te jedna nova krivulja ranga 9, koja odgovara parametrima $(r, s, t, v) = (155, 54, 96, 106)$. Krivulja je inducirana racionalnom Diofantovom trojkom

$$\left\{\frac{301273}{556614}, -\frac{556614}{301273}, -\frac{535707232}{290125899}\right\}.$$

Minimalna Weierstrassova jednadžba joj je

$$y^2 = x^3 + x^2 - 614100573770591167151980664421796984 0x + 585743317734880315858628578592963147780809517115906318 8.$$

3.4.4 Torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Eliptičke krivulje inducirane racionalnim Diofantovim trojkama s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ su prvi puta promatrane u članku (Dujella, 2007.). Konstruirana je krivulja nad $\mathbb{Q}(t)$ ranga ≥ 1 i krivulja nad $\mathbb{Q}$ ranga 4. Trenutni rekordi za rang eliptičkih krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (bez obzira jesu li krivulje inducirane racionalnim Diofantovim trojkama) su rang 2 nad $\mathbb{Q}(t)$ i rang 6 nad $\mathbb{Q}$. Pokazat ćemo da ih je moguće dobiti pomoću eliptičkih krivulja induciranih racionalnim Diofantovim trojkama (iako u slučaju rekordnih krivulja nad $\mathbb{Q}$ originalno nisu bile otkrivene na taj način).

Koristit ćemo ideju iz Potpoglavlja 3.2, gdje smo vidjeli da uvjet da je točka S reda 3 dovodi do jednadžbe (3.6, koju možemo zapisati kao

$$-a^2b^2c^4 + (2a^3b^2 + 2a^2b^3)c^3 + (6ab + 12a^2b^2 - a^4b^2 - a^2b^4 + 2a^3b^3)c^2 + (4a + 4b + 6a^2b + 6ab^2)c + 3 + 4ab = 0. \tag{3.38}$$

Neka su a i b takvi da je $c = 0$ jedno od rješenja jednadžbe (3.38). Dobivamo $4ab + 3 = 0$, tj. $b = -\frac{3}{4a}$. Uvrstimo li ovo u uvjet da je $bc + 1$ kvadrat, dobivamo da je $a(4a - 3c)$ kvadrat, recimo $a(4a - 3c) = (2a + t)^2$, tj.

$$c = -\frac{t(4a + t)}{3a}.$$

Jednadžba postaje

$$36a^2t + (-24 + 24t^2)a + 4t^3 - 9t = 0,$$

pa iz uvjeta da je diskriminanta kvadrat, dobivamo da je $t^2 + 4$ kvadrat, tj. $t = \frac{4u}{u^2-1}$. Tako dobivamo

$$a = \frac{(u^3 - 9u)}{6(u^2 - 1)},$$
$$b = -\frac{18(u^2 - 1)}{4(u^3 - 9u)},$$

te tri rješenja jednadžbe za c različita od nule

$$c_1 = \frac{(9 - 12u - 18u^2 + 4u^3 + u^4)}{6(u(u^2 + 2u - 3))},$$
$$c_2 = \frac{(9 + 12u - 18u^2 - 4u^3 + u^4)}{6(u(u^2 - 2u - 3))},$$
$$c_3 = -\frac{16u(u^2 - 3)}{3(u^4 - 10u^2 + 9)}.$$

Lako se provjeri da je $\{a, b, c_1, c_2, c_3\}$ racionalna Diofantova petorka. Budući da trojke $\{a, b, c_1\}$, $\{a, b, c_2\}$ i $\{a, b, c_3\}$ zadovoljavaju jednadžbu (3.38), eliptičke krivulje inducirane tim trojkama imaju torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ i rang ≥ 1 nad

$\mathbb{Q}(u)$. Ove tri krivulje su biracionalno ekvivalentne, pa ćemo u daljnjem promatrati samo krivulju induciranu trojkom $\{a, b, c_1\}$. Ta se krivulja može zapisati u obliku $y^2 = x^3 + A(u)x^2 + B(u)x$, gdje je

$$A(u) = 81 - 162u + 54u^2 + 162u^3 + 162u^4 - 54u^5 + 6u^6 + 6u^7 + u^8,$$
$$B(u) = -27(-1+u)^3u^3(3+u)^3(6-3u+u^2)(3+3u+2u^2).$$

Jedna točka beskonačnog reda je

$$P(u) = (-27(-1+u)^2u^2(3+u)^2, 27(-3+u)(-1+u)^2u^2(1+u)(3+u)^2(-3+6u+u^2)).$$

Da bi povećali rang, postavljamo uvjet da je

$$\frac{4(-1+u)u^2(3+u)^2(6-3u+u^2)(3+3u+2u^2)}{(-3+u)^2}$$

x-koordinata nove točke na krivulji, te dobivamo uvjet da je $4 - u + u^2$ kvadrat, što možemo parametrizirati s $u = -\frac{(-2+w)(2+w)}{1+2w}$. Tako smo dobili krivulju ranga ≥ 2 nad $\mathbb{Q}(w)$. Krivulju možemo zapisati u obliku $y^2 = x^3 + A_1(w)x^2 + B_1(w)x$, gdje je

$$\begin{aligned}A_1(w) = {} & 185257 + 401184w + 530914w^2 + 1218012w^3 + 1041238w^4 - 925272w^5 \\ & - 1369658w^6 + 53676w^7 + 519130w^8 + 93984w^9 - 59978w^{10} - 12924w^{11} \\ & + 3286w^{12} + 792w^{13} - 14w^{14} - 12w^{15} + w^{16},\end{aligned}$$
$$\begin{aligned}B_1(w) = {} & 27(-7+w)^3(-2+w)^3(-1+w)^3(1+w)^3(2+w)^3(3+w)^3(1+2w)^3 \\ & (10 + 19w^2 + 6w^3 + w^4)(47 + 36w - 7w^2 - 6w^3 + 2w^4).\end{aligned}$$

Dvije nezavisne točke beskonačnog reda imaju x-koordinate

$$x_1 = -27(-7+w)^2(-2+w)^2(-1+w)^2(1+w)^2(2+w)^2(3+w)^2(1+2w)^2,$$
$$\begin{aligned}x_2 = {} & -\frac{4}{(-1+6w+w^2)^2}(-7+w)^2(-2+w)^2(-1+w)(1+w)^2(2+w)^2 \\ & (3+w)(1+2w)(10+19w^2+6w^3+w^4)(47+36w-7w^2-6w^3+2w^4).\end{aligned}$$

Specijalizacija $w_0 = 57$ zadovoljava uvjete iz Teorema 3.4, što pokazuje da je rang nad $\mathbb{Q}(w)$ jednak 2.

U ovoj familiji krivulja mogu se naći primjeri krivulja s rangom 5 nad $\mathbb{Q}$ za sljedeće vrijednosti parametra: $w = \frac{1}{7}$, $w = \frac{12}{11}$ i $w = \frac{33}{14}$.

Drugi način za dobiti krivulju ranga 2 iz polazne krivulje ranga 1, je postaviti uvjet da

$$\frac{4(-1+u)u^3(3+u)^3(3+3u+2u^2)}{(1+u)^2}$$

bude x-koordinata nove točke na krivulji. To daje uvjet da je $u^2 + u + 2$ kvadrat, tj. $u = -\frac{-2+w^2}{-1+2w}$. Tako dobivamo novu krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ i rangom 2 nad $\mathbb{Q}(w)$. Koeficijenti te krivulje su

$$\begin{aligned}A_2(w) = {} & 3517 - 26568w + 74462w^2 - 102612w^3 + 138610w^4 - 283680w^5 \\ & + 346730w^6 - 107316w^7 - 122138w^8 + 84648w^9 + 7418w^{10} - 15084w^{11} \\ & + 1690w^{12} + 576w^{13} + 14w^{14} - 12w^{15} + w^{16},\end{aligned}$$
$$\begin{aligned}B_2(w) = {} & 27(-1+w)^3(3+w)^3(-1+2w)^3(-2+w^2)^3(1-6w+w^2)^3 \\ & (16 - 36w + 17w^2 + 6w^3 + w^4)(5 + 7w^2 - 6w^3 + 2w^4),\end{aligned}$$

dok dvije nezavisne točke beskonačnog reda ima sljedeće x-koordinate

$$\begin{aligned}x_1 =& -27(-1+w)^2(3+w)^2(-1+2w)^2(-2+w^2)^2(1-6w+w^2)^2,\\ x_2 =& -\frac{4}{(-1-2w+w^2)^2}(-1+w)(3+w)(-1+2w)(-2+w^2)^3\\ & (1-6w+w^2)^3(5+7w^2-6w^3+2w^4).\end{aligned}$$

Specijalizacija $w_0 = 18$ zadovoljava uvjete Teorema 3.4, što pokazuje da je rang nad $\mathbb{Q}(w)$ jednak 2.

Za $w = \frac{7}{19}$ odgovarajuća krivulja ima rang 6 nad $\mathbb{Q}$. Tu je krivulju prethodno bio pronašao Elkies 2006., pretragom po općenitoj familiji krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, i predstavlja rekordni rang za ovu torzijsku grupu. Vidimo da se ta rekordna krivulja može dobiti i pomoći Diofantovih trojki. Preciznije, inducirana je racionalnom Diofantovom trojkom

$$\left\{\frac{31269599}{31628160}, -\frac{23721120}{31269599}, \frac{1461969791}{7144352640}\right\}$$

Dodatne primjere krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ i rangom 6 nad $\mathbb{Q}$ našli su (Dujella, Peral & Tadić. 2015.) i (Dujella & Peral, 2020.), tako da su danas poznate četiri takve krivulje.

Treću familiju krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ i rangom 2 dobit ćemo tako da krenemo od racionalne Diofantove trojke $\{a, b, c\}$ iz parametarske familije racionalnih Diofantovih šestorki iz Potpoglavlja 3.2. To je trojka

$$\begin{aligned}a =& \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)},\\ b =& \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)},\\ c =& \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}.\end{aligned}$$

Znamo da ona zadovoljava uvjet da je točka S reda 3, te stoga eliptička krivulja inducirana s trojkom $\{a, b, c\}$ ima torzijsku grupu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ i rank ≥ 1 nad $\mathbb{Q}(t)$. Tu krivulju možemo zapisati u obliku $y^2 = x^3 + A(t)x^2 + B(t)x$, gdje je

$$\begin{aligned}A_3(t) &= t^8 - 212t^6 - 5184t^5 - 4314t^4 - 5184t^3 - 212t^2 + 1,\\ B_3(t) &= -3456t^3(t^2 - 18t + 1)(t^2 + 1)(t^2 + 6t + 1)^3,\end{aligned}$$

Da bi povećali rang, tražimo x-koordinatu dodatne točke u obliku $kt(t+1)^2(t^2+6t+1)^2$, gdje je k konstanta. Kandidate za k nalazimo kao nultočke diskriminante izraza dobivenog uvrštavanjem u kubni polinom iz jednadžbe eliptičke krivulje (nakon eliminiranja kvadratnih faktora). Tako nalazimo da je dobar kandidat $k = 27$ (jer se u faktorizaciji diskriminante pojavljuje faktor $(k-27)^7$, te dobivamo uvjet da je $t^2 - 3t + 1$ kvadrat, tj. $t = -\frac{(-1+w)(1+w)}{3+2w}$. Nakon sređivanja, jednadžba krivulje

postaje $y^2 = x^3 + A_3(w)x^2 + B_3(w)x$, gdje je

$$\begin{aligned}A_4(w) &= -1899008 - 5996544w - 1469440w^2 + 13980672w^3 + 14383360w^4\\ &\quad - 6990336w^5 - 16274176w^6 - 3491328w^7 + 5554240w^8 + 2814336w^9\\ &\quad - 219616w^{10} - 160416w^{11} + 120808w^{12} + 38928w^{13} - 856w^{14} + w^{16},\\ B_4(w) &= 3456(-1+w)^3(1+w)^3(3+2w)^3(-2+w^2)^3(-14-12w+w^2)^3\\ &\quad (10+12w+2w^2+w^4)(-44-24w+56w^2+36w^3+w^4),\end{aligned}$$

dok su x-koordinate dvaju nezavisnih točaka beskonačnog reda

$$\begin{aligned}x_1 &= \frac{108(-1+w)^2(1+w)^2(3+2w)^2(-2+w^2)^3(-14-12w+w^2)^3(2+2w+w^2)^2}{(10+12w+2w^2+w^4)^2},\\ x_2 &= -27(-1+w)(1+w)(3+2w)(-2+w^2)^2(-14-12w+w^2)^2(-4-2w+w^2)^2.\end{aligned}$$

Specijalizacija $w_0 = 14$ zadovoljava uvjete Teorema 3.4, što pokazuje da je rank nad $\mathbb{Q}(w)$ jednak 2.

Za $w = -39$ dobivamo ponovno prije navedenu Elkiesovu krivulju ranka 6 s jednadžbom

$$\begin{aligned}Y^2 + XY = X^3 &- 37680956700999226080263982005713090640\,X\\ &- 369928983979260787438945059025553621591626117724889024 00,\end{aligned}$$

ovaj puta induciranu racionalnom Diofantovom trojkom

$$\left\{\frac{7567037280}{7833785281}, \frac{4161669360289}{569762123040}, \frac{1359453258559}{948852707040}\right\}.$$

3.4.5 Torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

U Teoremu 2.5, dokazali smo da je svaka eliptička krivulja nad $\mathbb{Q}$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ inducirana nekom racionalnom Diofantovom trojkom. Preciznije, inducirana je trojkom oblika

$$\left\{\frac{2t}{t^2-1}, \frac{1-t^2}{2t}, \frac{6t^2-t^4-1}{2t(t^2-1)}\right\}. \tag{3.39}$$

Budući da elementi ove trojke očito imaju miješane predznake ($ab = -1$), možemo se pitati postoji li krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ koja je indicirana s racionalnom Diofantovom trojkom koja ima sve elemente pozitivne. Pokazat ćemo da je odgovor potvrdan.

Promotrimo familiju racionalnih Diofantovih trojki

$$\begin{aligned}\Bigg\{&\frac{2(2w^4+4w^3+2w^2+1)(1+2w)}{w(2w+2w^2-1)(2+w)(w-1)(w+1)}, -\frac{2(w+1)^2(w-1)^2}{(2+w)(2w+2w^2-1)w},\\ &\frac{2w^2(2+w)^2}{(2w+2w^2-1)(w-1)(w+1)}\Bigg\}.\end{aligned}$$

(Familija je dobivena faktorizacijom razlike j-invarijante krivulje inducirane općom troparametarskom racionalnom Diofantovom trojkom i j-invarijalne krivulje inducirane s $\{T, -1/T, T-1/T\}$ kojoj nedostaje samo uvjet da je T^2+1 kvadrat da bi

imala torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.) Usporedbom j-invarijante eliptičke krivulje inducirane ovom trojkom s j-invarijantom krivulje inducirane s (3.39), dobivamo uvjet da je $2w^4 + 4w^3 + 2w^2 + 1 = \square$. Krivulja definirana ovom jednadžbom se može transformirati u eliptičku krivulju $Y^2 = X^3 - X^2 - 9X + 9$ koja ima rang 1 i čiji je generator $P = (0, 3)$. Uzimajući odgovarajuće višekratnike točke P, primjerice $3P$, $5P$, $8P$, dobivamo racionalne Diofantove trojke s pozitivnim elementima. Npr. uzmimo točku $3P = (-360/169, -8211/2197)$. Transformiramo li ju natrag na kvartiku, dobivamo $w = 26/89$, te uvrštavanjem ove vrijednosti za w u gornju familiju Diofantovih trojki, dobivamo sljedeću racionalnu Diofantovu trojku pozitivnim elementima

$$\{a, b, c\} = \left\{\frac{37471518967}{1381254420}, \frac{5832225}{571948}, \frac{6251648}{1562505}\right\}$$

koja inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ i rangom 1. U stvari, na ovaj način dobivamo beskonačnu familiju eliptičkih krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ i pozitivnim rangom (budući da je točka $(0, abc)$ beskonačnog reda). To je najbolji poznati rezultat ovog tipa (nije poznato postoji li beskonačna familija s tom torzijom grupom i rangom ≥ 2), a ova familija je ekvivalentna familiji koju je pronašla Lecacheux 2004. Pitanje postoji li racionalna Diofantova trojka s pozitivnim elementima koja inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ i rangom 0 razmotrit ćemo u sljedećem potpoglavlju.

Što se tiče eliptičkih krivulja nad $\mathbb{Q}$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, poznato je da postoje takve eliptičke krivulje s rangom 3, a nije poznato postoji li takva krivulja ranga ≥ 4. Krivulja ranga 3 poznato je ukupno 29. Prvu su našli Connell i Dujella 2000., a posljednju AttarBashi, Rathbun & Voznyy 2022. Prema Teoremu 2.5, sve takve te krivulje su inducirane nekom racionalnom Diofantovom trojkom. Primjerice, prva spomenuta krivulja, čija je jednadžba

$$\begin{aligned} y^2 + xy = x^3 &- 15745932530829089880x \\ &+ 24028219957095969426339278400, \end{aligned}$$

a nezavisne točke beskonačnog reda

$$\begin{gathered} (2188064030, -7124272297330), \\ (396546810000/169, 1222553114825160/2197), \\ (16652415739760/3481, 49537578975823615480/205379), \end{gathered}$$

je inducirana racionalnom Diofantovom trojkom

$$\left\{\frac{408}{145}, -\frac{145}{408}, -\frac{145439}{59160}\right\},$$

dok je posljednja pronađena krivulja, čija je jednadžba

$$\begin{aligned} y^2 + xy = x^3 &- 125773582955215019659843433869443803612902341280x \\ &+ 16545780427234453690755618162313665193883053063142475175813942418662400, \end{aligned}$$

a nezavisne točke beskonačnog reda

$$(1771775825177555156843221169213 0/11826721,\ 726472136272254107745712870940674199608454816 30/40672093519),$$

$$(2526555996702832707895123084069857683030588014705814971872515494987472470664 0/ 790791213520751286266759148082862700455011291278553 69,$$
$$2106765868893950319477043345162195244251673901514805587788796833551378947204881017290520143806121408680205865582560/ 2223784776534944140293235405012383251829198584519671241447319362780762777144765 3),$$

$$(7044063247449150935860150533337469755962712091387727069976796077005710272856627181 6968/ 4587645686689656711878602031324194555260270870245087225111060 89,$$
$$2871377212968706356475083631022485212953145012423036589862235991435933446662052758136310080270470089675222273019085787874194981 04/ 9826181994367085850590085023465427811589979116750497045847031843961893432948406446334709108437),$$

inducirana racionalnom Diofantovom trojkom

$$\left\{\frac{1266720}{710719},\ -\frac{710719}{1266720},\ \frac{1099458061439}{900281971680}\right\}.$$

3.5 Krivulje ranga 0 inducirane racionalnim Diofantovim trojkama

U prethodnom poglavlju smo vidjeli kako se racionalne Diofantove trojke mogu iskoristiti za nalaženje eliptičkih krivulja velikog ranga. Sada ćemo razmotriti suprotan problem i pitati se koliko mali može biti rang krivulja induciranih racionalnim Diofantovim trojkama. Posebno, može li rang takve krivulje biti jedan 0. Vidjet ćemo da je dosta lako naći takve krivulje ako dopustimo na elementi trojke imaju miješane predznake. No za trojke s pozitivnim elementima problem postaje znatno teži i trenutno je poznata samo jedna takva krivulja (Dujella & Mikić, 2020.), čiju ćemo konstrukciju i prikazati.

Neka je $\{a,b,c\}$ racionalna Diofantova trojka te $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$. Znamo da krivulja E dana jednadžbom $y^2=(ax+1)(bx+1)(cx+1)$ ima tri točke reda 2, $A=(-1/a,0)$, $B=(-1/b,0)$, $C=(-1/c,0)$, te točke $P=(0,1)$ i $S=(1/abc,1/rst)$ koje su općenito nezavisne točke beskonačnog reda. Dakle, ako želimo naći krivulju ranga 0, točke P i S moraju biti konačnog reda. Podsjetimo se da za točku S vrijedi da je $S=2R$, gdje je $R=((rs+rt+st+1)/(abc),((r+s)(r+t)(s+t))(abc))$, te da je trojka $\{a,b,c\}$ regularna, tj. $c=a+b\pm 2r$ ako i samo ako je $S=\mp 2P$.

Iz Mazurovog teorema i činjenice da je $S\in 2E(\mathbb{Q})$ slijedi da imamo sljedeće mogućnosti da bi točke P i S bile konačnog reda:

- $mP=\mathcal{O}$, $m=3,4,6,8$;
- $mS=\mathcal{O}$, $m=2,3,4$.

Posebno, budući da točka P ne može biti reda 2, zaključujemo da nije moguće istovremeno imati rang 0 i torzijsku grupu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Uobičajenim transformacijama $x\mapsto\frac{x}{abc}$, $y\mapsto\frac{y}{abc}$, iz krivulje E dobivamo izomorfnu krivulju

$$E':\qquad y^2=(x+ab)(x+ac)(x+bc), \tag{3.40}$$

te pritom točke A, B, C, P i S na E odgovaraju točkama $A'=(-bc,0)$, $B'=(-ac,0)$, $C'=(-ab,0)$, $P'=(0,abc)$ i $S'=(1,rst)$ na E'. U sljedećoj lemi ispitat ćemo sve mogućnosti da bi točka S bila konačnog reda. Primijetimo da smo dio (ii)

već koristili (bez dokaza) na više mjesta (kod konstrukcije racionalnih Diofantovih šestorki te kod krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$).

Lema 3.1.

(i) Uvjet $2S = \mathcal{O}$ je ekvivalentan s

$$(ab+1)(ac+1)(bc+1) = 0.$$

(ii) Uvjet $3S = \mathcal{O}$ je ekvivalentan s

$$3+4(ab+ac+bc)+6abc(a+b+c)+12(abc)^2-(abc)^2(a^2+b^2+c^2-2ab-2ac-2bc) = 0.$$

(iii) Točka S je reda 4 ako i samo ako je

$$((ab+1)^2-ab(c-a)(c-b))((ac+1)^2-ab(c-a)(c-b))((bc+1)^2-ab(c-a)(c-b)) = 0.$$

Dokaz.

(i) Radit ćemo s izomorfnom krivuljom E'. Uvjet $2S' = \mathcal{O}$ povlači $rst = -rst$, tj. $rst = 0$ te

$$(ab+1)(ac+1)(bc+1) = 0.$$

(ii) Iz $3S' = \mathcal{O}$, tj. $x(2S') = x(-S') = x(S')$, te formule za dupliciranje točaka na eliptičkoj krivulji, dobivamo

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

Dakle, dobili smo

$$\begin{aligned} &4\left((abc)^2 + abc(a+b+c) + (ab+ac+bc) + 1\right)(3 + ab + ac + bc) \\ &= 9 + 12(ab+ac+bc) + \left(6abc(a+b+c) + 4(ab+ac+bc)^2\right) \\ &\quad + 4abc(ab+ac+bc)(a+b+c) + (abc(a+b+c))^2, \end{aligned}$$

što je ekvivalentno s

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

(iii) Uvjet da je točka S' reda 4 je ekvivalentan s $2S' \in \{A', B', C'\}$. Pretpostavimo da je $2S' = C'$ (preostala dva slučaja su sasvim analogni). Iz formule za dupliciranje, dobivamo

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

što je ekvivalentno s

$$(1+2ab-abc(c-a-b))^2=0,$$

odnosno

$$(ab+1)^2=ab(c-a)(c-b).$$

□

Razmotrimo sada tri mogućnosti za $mS=\mathcal{O}$.

Uzmimo najprije da je $2S=\mathcal{O}$. Prema Lemi 3.1(i), imamo $(ab+1)(ac+1)(bc+1)=0$, te zaključujemo da a,b,c ne mogu biti istog predznaka. Ako dopustimo miješane predznake, onda možemo pretpostaviti da je $b=-1/a$. U Potpoglavlju 3.4.3 su vidjeli da se sve racionalne Diofantove trojke oblika $\{a,-1/a,c\}$ mogu parametrizirati na sljedeći način:

$$a=\frac{ut+1}{t-u},\quad b=\frac{u-t}{ut+1},\quad c=\frac{4ut}{(ut+1)(t-u)}.$$

Da bi našli primjere krivulja ranga 0, pretpostavimo da je trojka $\{a,-1/a,c\}$ regularna. Ova pretpostavka nam daje uvjet $(u^2-1)(t^2-1)=0$, pa možemo uzeti da je $u=1$. Ako sada primjerice uzmemo $t=2$, dobivamo krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ i rangom 0, koja je inducirana trojkom

$$\left\{3,-\frac{1}{3},\frac{8}{3}\right\}.$$

Uzmimo sada da je $3S=\mathcal{O}$. Ako bi također bilo $3P=\mathcal{O}$, onda bi imali da je $P=\pm S$, što je kontradikcija. Stoga, ako točka P ima konačan red, jedina mogućnost je da je P točka reda 6. To povlači da je $2P=\pm S$ te $c=a+b\mp 2r$. Uvrštavajući $b=(r^2-1)/a$ i $c=a+b+2r$ u uvjet iz Leme 3.1(ii), dobivamo

$$(2ar-1+2r^2)(-a+2ar^2-2r+2r^3)(2a^2r-a-2r+4ar^2+2r^3)=0.$$

Odavde je

$$a=\frac{-2r(r^2-1)}{-1+2r^2},\quad\text{ili}\quad\frac{-(-1+2r^2)}{2r},\quad\text{ili}\quad\frac{1-4r^2\pm\sqrt{1+8r^2}}{4r}.$$

Uzmimo da je

$$(a,b,c)=\left(\frac{-2r(r-1)(r+1)}{-1+2r^2},\frac{-(-1+2r^2)}{2r},\frac{(-1+2r)(2r+1)}{2(-1+2r^2)r}\right).\tag{3.41}$$

Tada je uvjet $ab>0$ ekvivalentan s $r>1$ ili $r<-1$, dok je uvjet $bc>0$ ekvivalentan s $-1/2<r<1/2$. Stoga a,b,c ne mogu imati isti predznak.

Slučaj

$$(a,b,c)=\left(\frac{-(-1+2r^2)}{2r},\frac{-2r(r-1)(r+1)}{-1+2r^2},\frac{(-1+2r)(2r+1)}{2(-1+2r^2)r}\right)$$

je sasvim isti kao prethodni slučaj, samo sa zamjenjenom ulogom od a i b.

Konačno, neka je $8r^2+1=(2rt+1)^2$ (tako da se riješimo korijena u trećem slučaju). Dobivamo da je $r=\frac{-t}{-2+t^2}$, pa je

$$(a,b,c)=\left(\frac{-t(t-2)(t+2)}{2(-2+t^2)},\frac{2(t-1)(t+1)}{(-2+t^2)t},\frac{-(-2+t^2)}{2t}\right)$$

(ili uz zamjenu a i b). Uvjet $ac>0$ je ekvivalentan s $t>2$ ili $t<-2$, dok je uvjet $bc>0$ je ekvivalentan s $-1<t<1$. Dakle, niti u ovom slučaju a,b,c ne mogu imati isti predznak.

Ako pak dozvolimo miješane predznake, onda možemo dobiti primjere krivulja s rangom 0, primjerice iz trojki oblika (3.41). Tako za $t=4$ dobivamo krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ i rangom 0, koja je inducirana trojkom

$$\left\{-\frac{12}{7},\frac{15}{28},-\frac{7}{4}\right\}.$$

Preostaje nam razmotriti slučaj kada je točka S reda 4. Tada je točka R, takva da je $2R=S$, reda 8 pa stoga krivulja E ima torzijsku grupu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$. Vidjeli smo u Teoremu 2.5 da je svaka eliptička krivulja nad $\mathbb{Q}$ inducirana s racionalnom Diofantovom trojkom oblika

$$\left\{\frac{2t}{t^2-1},\ \frac{1-t^2}{2t},\ \frac{6t^2-t^4-1}{2t(t^2-1)}\right\}. \tag{3.42}$$

Jasno je da elementi trojke (3.42) imaju miješane predznake. Ako uzmemo primjerice $t=2$, dobivamo krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ i rangom 0, koja je inducirana trojkom

$$\left\{\frac{4}{3},-\frac{3}{4},\frac{7}{12}\right\}.$$

Preostaje razmotriti pitanje je li moguće dobiti krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ i rangom 0, koja je inducirana trojkom s pozitivnim članovima.

Ponovno pretpostavljamo da je točka S reda 4, te uzimamo $b=(r^2-1)/a$, $c=a+b+2r$. Uvrstimo li ovo u prvi faktor

$$(ab+1)^2-ab(c-a)(c-b)$$

iz Leme 3.1(iii), dobivamo kvadratnu jednadžbu u a:

$$(2r^3-2r)a^2+(4r^4-6r^2+1)a+2r^5-4r^3+2r=0.$$

Njezina diskriminanta,

$$-4r^4+4r^2+1$$

treba biti potpun kvadrat. Taj uvjet definira kvartiku koja je biracionalno ekvivalentna eliptičkoj krivulji

$$E_1:\quad Y^2=X^3+X^2+X+1$$

koja ima rang 1 i generator $P_1=(0,1)$. Stoga, računajući višekratnike točke P_1 na krivulji E_1 (dodavanje torzijske točke $T_1=(-1,0)$ reda 2 ima samo efekt zamjene r s $-r$), i prebacujući ih natrag na kvartiku, dobivamo kandidate za rješenje našeg problema. Međutim, treba još zadovoljiti uvjet da su svi elementi odgovarajuće trojke pozitivni (dovoljno je da svi elementi trojke imaju isti predznak, jer

množenjem svih elemenata racionalne Diofantove trojke s -1 dobivamo ponovno racionalnu Diofantovu trojku). Prva dva višekratnika od P_1 koja daju trojke s pozitivnim elementima su $6P_1$ i $11P_1$.

Točka $6P_1$ daje $r = -\frac{3855558}{3603685}$ i trojku

$$(a,b,c) = \left(\frac{1884586446094351}{25415891646864180}, \frac{14442883687791636}{7402559392524605}, \frac{60340495895762708555}{14487505263205637124}\right).$$

S dostupnim programima nismo uspjeli odrediti rang inducirane eliptičke krivulje. Naime, i `magma` i `mwrank` i `ellrank` daju da je $0 \leq \text{rank} \leq 2$. Uz pretpostavku da vrijedi Slutnja o parnosti, zaključujemo da bi rang trebao biti ili 0 ili 2.

Točka $11P_1$ daje $r = \frac{35569516882766685106979}{32383819387240952672281}$ i trojku (a,b,c), gdje je

$$a = \frac{69705492951192675600645567228019184577147632882703132983}{13201484334991246769290130383656126692130218445953676312 0},$$

$$b = \frac{47826829880079829075801189563942620732062701095548790400}{12233666942070950930363744264796639133659669496983545932 7},$$

$$c = \frac{47982111146649404421749331709393501777791774558546217987550257759801}{15400090753918257364093484910580652390786084055043677020804056653840}.$$

(Uspoređujući j-invarijante, dobivamo da je ova krivulja inducirana s trojkom (3.42) za $t = \frac{184517864081061331836 49}{41916048174422594852689}$.)

Za induciranu krivulju, i `mwrank` i `magma` funkcija `MordellWeilShaInformation` daju da je $0 \leq \text{rank} \leq 4$. Međutim, `magma` (verzija `V2.24-7`) funkcija `TwoPowerIsogenyDescentRankBound`, u kojoj je implementiran algoritam Toma Fishera (Fisher, 2017.), daje da je rang jednak 0 (taj rezultat daje peti od šest koraka algoritma, to je korak nakon tzv. 4-spusta, a prije tzv. 8-spusta). Tako smo pronašli željeni primjer racionalne Diofantove trojke s pozitivnim članovima koja inducira eliptičku krivulju ranga 0.

Napomenimo da `magma` funkcija `TwoPowerIsogenyDescentRankBound` primjenjena na gornju krivulju koja odgovara točki $6P_1$ daje samo rank ≤ 2 te ne daje konačan odgovor na pitanje je li rang te krivulje 0 ili 2. Opisana konstrukcija sigurno daje beskonačno mnogo višekratnika od P_1 koji odgovaraju trojkama s pozitivnim članovima (ovdje koristimo činjenicu da je skup $E_1(\mathbb{Q})$ gust u $E_1(\mathbb{R})$ – po Poincaré-Hurwitzovom teoremu, ako je rang eliptičke krivulje nad $\mathbb{Q}$ pozitivan, tj. ako krivulja ima beskonačno mnogo racionalnih točaka, onda je skup racionalnih točaka gust na parnoj komponenti krivulje te također i na neparnoj ako ona sadrži barem jednu racionalnu točku). Međutim, teško je nešto pouzdano reći o distribuciji rangova u ovakvoj familiji krivulja, tako da možemo samo špekulirati da bi možda moglo postojati beskonačno mnogo krivulja u ovoj familiji koje imaju rang 0.

3.6 Torzijske grupe eliptičkih krivulja induciranih cjelobrojnim Diofantovim trojkama

Do sada smo se bavili eliptičkim krivuljama induciranim racionalnim Diofantovim trojkama. Posebice, pokazali smo da se za takve krivulje svaka od četiri torzijske grupe dopuštene Mazurovim teoremom za krivulje s tri točke reda 2, tj. $\mathbb{Z}/2\mathbb{Z} \times$

$\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, moguća, i štoviše pojavljuje se za beskonačno mnogo racionalnih Diofantovih trojki.

Sada ćemo razmotriti isto pitanje, ali za krivulje inducirane cjelobrojnim Diofantovim trojkama. Vidjet ćemo da je ovdje odgovor drugačiji. Naime, torzijske grupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ nisu moguće, dok je i dalje otvoren problem može li se pojaviti torzijska grupa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Pritom ćemo razmotriti i malo širi problem, naime promatrat ćemo eliptičke krivulje inducirane s cjelobrojnim $D(4)$-trojkama. Jasno je da se množenjem elemenata $D(1)$-trojke s 2 dobiva $D(4)$-trojka, pa ćemo željeni rezultat za $D(1)$-trojke dobiti kao neposrednu posljedicu rezultata za $D(4)$-trojke. Pritom ćemo slijediti članak (Dujella & Mikić, 2014.) u kojem je ispravljena greška iz dokaza u članku (Dujella, 2001.).

Neka je $\{a, b, c\}$ $D(4)$-trojka, te neka su r, s, t nenegativni cijeli brojevi takvi da vrijedi

$$ab + 4 = r^2, \quad ac + 4 = s^2, \quad bc + 4 = t^2.$$

Promatrat ćemo eliptičku krivulju

$$E : y^2 = (ax + 4)(bx + 4)(cx + 4),$$

za koju ćemo reći da je inducirana trojkom $D(4)$-trojkom $\{a, b, c\}$.

Transformacijama $x \mapsto \frac{x}{abc}$, $y \mapsto \frac{y}{abc}$ krivulju dovodimo u oblik

$$E' : y^2 = (x + 4bc)(x + 4ac)(x + 4ab).$$

Na krivulji E' imamo tri točke reda 2:

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

te još dvije očite racionalne točke

$$P' = (0, 8abc),\ S' = (16, 8rst).$$

Pritom vrijedi da je $S' = 2R'$, gdje je

$$R' = (4rs + 4rt + 4st + 16, 8(r + s)(r + t)(s + t)).$$

Razmotrit ćemo najprije jedan specijalan slučaj, a to je jedina $D(4)$-trojka s miješanim predznacima: $\{-1, 3, 4\}$ (i njoj ekvivalentna $\{-4, -3, 1\}$). Eliptička krivulja inducirana s ovom trojkom ima rang 0 i torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. U ovom slučaju je $B' \in 2E'(\mathbb{Q})$, preciznije $B' = 2P'$, pa je točka P' reda 4. Primijetimo da je u ovom slučaju i točka R' također reda 4 budući da je $R' = P' + A'$ i $2R' = 2P'$.

Dakle, nadalje možemo pretpostaviti da su a, b, c prirodni brojevi i da je $a < b < c$.

Pokazat će se da će nam trebati precizna ocjena za veličinu trećeg elementa c u $D(4)$-trojki. Naravno, jedna mogućnost je da $\{a, b, c\}$ bude regularna, tj. $c = a + b + 2r$. Zanima nas što se može reći o c ako trojka nije regularna. Pritom ćemo koristiti konstrukciju koja poopćuje konstrukciju broja d_- iz slučaja $D(1)$-trojki. Taj broj je proširivao $D(1)$-trojku do $D(1)$-četvorke. U slučaju $D(n)$-trojki, taj četvrti element neće imati svojstvo da su produkti s njim uvećani za n kvadrati, već će produkte trebati uvećati za n^2 da bi se dobio kvadrat. Međutim u slučaju $n = 4$, bit će moguće, dijeljenjem s 4, prijeći od 16 na 4, te dobiti $D(4)$-četvorku.

Lema 3.2. *Ako je $\{a,b,c\}$ $D(n)$-trojka i $ab+n=r^2$, $ac+n=s^2$, $bc+n=t^2$, onda postoje cijeli brojevi e,x,y,z tako da vrijedi*

$$ae+n^2=x^2, \quad be+n^2=y^2, \quad ce+n^2=z^2$$

i

$$c=a+b+\frac{e}{n}+\frac{2}{n^2}(abe+rxy).$$

Dokaz: Definirajmo

$$e=n(a+b+c)+2abc-2rst.$$

Tada je

$$\begin{aligned}(ae+n^2)-(at-rs)^2 &= an(a+b+c)+2a^2bc-2arst+n^2\\ &\quad -a^2(bc+n)+2arst-(ab+n)(ac+n)=0.\end{aligned}$$

Stoga možemo uzeti $x=rs-at$, te analogno $y=rt-bs$, $z=cr-st$. Imamo

$$\begin{aligned}abe+rxy &= abn(a+b+c)+2a^2b^2c-2abrst\\ &\quad +rst(ab+n)-a(ab+n)(bc+n)-b(ab+n)(ac+n)+abrst\\ &= -abcn-n^2(a+b)+rstn,\end{aligned}$$

te konačno

$$a+b+\frac{e}{n}+\frac{2}{n^2}(abe+rxy)=2a+2b+c+\frac{2abc}{n}-\frac{2rst}{n}-\frac{2abc}{n}-2a-2b+\frac{2rst}{n}=c.$$

□

Lema 3.3. *Ako je $\{a,b,c\}$ $D(4)$-trojka, onda je $c=a+b+2r$ ili $c>ab+a+b+1>ab$.*

Dokaz: Po Lemi 3.2, postoji cijeli broj

$$e=4(a+b+c)+2(abc-rst) \tag{3.43}$$

i cijeli brojevi x,y,z takvi da je

$$ae+16=x^2, \tag{3.44}$$
$$be+16=y^2, \tag{3.45}$$
$$ce+16=z^2 \tag{3.46}$$

i $c=a+b+\frac{e}{4}+\frac{1}{8}(abe+rxy)$. Lako se vidi da su x i y iz Leme 3.2 za $n=4$ (i općenitije za $n>0$) pozitivni. Iz (3.46), slijedi da je $e\geq 0$ (slučaj $e=-1$ povlači $c\leq 16$, ali jedina takva $D(4)$-trojka je $\{1,5,12\}$ koja ne zadovoljava (3.44) i (3.45)). Za $e=0$ dobivamo $c=a+b+2r$, dok za $e\geq 1$ imamo da je $c>\frac{1}{4}abe+a+b+\frac{e}{4}$.

Promatrajući kongruencije modulo 8, lako se vidi da su među brojevima a,b,c najviše dva neparna. Zaista, ako bi a,b,c bili svi neparni, onda bi $ab+4$, $ac+4$, $bc+4$ bili neparni kvadrati pa bi stoga davali ostatak 1 pri dijeljenju s 8. Iz $ab+4\equiv 1 \pmod 8$ slijedi $ab\equiv 5 \pmod 8$ i analogno $ac\equiv 5 \pmod 8$ i $bc\equiv 5 \pmod 8$. Množeći ove tri kongruencije, dobivamo $(abc)^2\equiv 125\equiv 5 \pmod 8$, što je kontradikcija.

Zaključujemo da je $abc-rst$ paran. Stoga iz (3.43) slijedi da je $e\equiv 0 \pmod 4$, što povlači da je $e\geq 4$ i $c>ab+a+b+1$. □

Napomena 3.1. Lema 3.3 povlači da je u svakom slučaju $c \geq a+b+2r$. Zaista, nejednakost $ab+a+b+1 \geq a+b+2r$ je ekvivalentna s $(r-3)(r+1) \geq 0$, što je zadovoljeno za sve $D(4)$-trojke s pozitivnim elementima.

Napomena 3.2. Tvrdnja Leme 3.3 je najbolja moguća, u smislu da se nejednakost $c > ab$ ne može zamijeniti s $c > (1+\varepsilon)ab$ za neki fiksni $\varepsilon > 0$. Zaista, ako za $k \geq 3$ stavimo $a = k^2-4$, $b = k^2+2k-3$, $c = k^4+2k^3-3k^2-4k$, onda je $\{a,b,c\}$ $D(4)$-trojka i $\lim_{k\to\infty} \frac{c}{ab} = 1$.

Napomena 3.3. Iz dokaza Lema 3.2 i 3.3 slijedi da se svaka $D(4)$-trojka $\{a,b,c\}$ može proširiti do $D(4)$-četvorke s četvrtim elementom $d = a+b+c+\frac{1}{2}(abc \pm rst)$ jer je broj $abc \pm rst$ paran i vrijedi $ad+4 = (\frac{1}{2}(rs \pm at))^2$, $bd+4 = (\frac{1}{2}(rt \pm bs))^2$, $cd+4 = (\frac{1}{2}(cr \pm st))^2$.

Sada želimo dokazati da E' nema točaka reda 4.

Lema 3.4. $A', B', C' \notin 2E'(\mathbb{Q})$

Dokaz: Ako je $A' \in 2E'(\mathbb{Q})$, onda Teorem 2.4 povlači da je $4c(a-b)$ kvadrat. Ali $4c(a-b) < 0$, pa smo dobili kontradikciju. Slično, $B' \notin 2E'(\mathbb{Q})$ jer $4a(b-c) < 0$ nije kvadrat.

Preostaje razmotriti točku C' i taj slučaj je bitno zahtjevniji. Ako je $C' \in 2E'(\mathbb{Q})$, onda imamo da je

$$a(c-b) = X^2, \tag{3.47}$$

$$b(c-a) = Y^2, \tag{3.48}$$

za cijele brojeve X i Y. Vidimo da nemamo direktnu kontradikciju kao u prethodna dva slučaja, budući da su brojevi $a(c-b)$ i $b(c-a)$ pozitivni.

Po Lemi 3.3, imamo dvije mogućnosti: $c = a+b+2r$ ili $c > ab+a+b+1$.

Uzmimo najprije da je $c = a+b+2r$. Iz (3.47) and (3.48), imamo da je $a = kx^2$, $c-b = ky^2$, $b = lz^2$, $c-a = lu^2$, gdje su k,l,x,y,z,u prirodni brojevi. Odavde je $c = kx^2+lu^2 = ky^2+lz^2$, pa iz $c = a+b+2r$ dobivamo

$$2r = k(y^2-x^2) = l(u^2-z^2). \tag{3.49}$$

Kvadrirajući (3.49), dobivamo

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

što povlači da je $k \in \{1,2,4\}$ i $l \in \{1,2,4\}$. Budući da kl nije potpun kvadrat (inače bi imali $(2r)^2 = 16+(2xz\sqrt{kl})^2$ što povlači $2r = 5$), možemo bez gubitka općenitosti uzeti da je $k=1$, $l=2$ ili $k=2$, $l=4$. Za $k=1$, $l=2$, imamo $4r^2 = 16+8x^2z^2$, što povlači $r^2 = 4+2x^2z^2$, odakle zaključujemo da su r i xz parni. Dakle, $r^2 \equiv 4 \pmod 8$ i $r \equiv 2 \pmod 4$, ali iz $2r = 2(u^2-z^2)$ dobivamo da je $u^2-z^2 \equiv 2 \pmod 4$, što je kontradikcija. Ako je $k=2$, $l=4$, onda je $4r^2 = 16+32x^2z^2$, što povlači $r^2 = 4+8x^2z^2$. Odavde je $r^2 \equiv 4 \pmod 8$ i $r \equiv 2 \pmod 4$, ali iz $2r = 2(y^2-x^2)$ dobivamo $y^2-x^2 \equiv 2 \pmod 4$, što je kontradikcija.

Preostaje razmotriti slučaj kada je $c > ab+a+b+1 > ab$.

Zapišimo uvjete (3.47) i (3.48) u obliku

$$ac-ab = s^2-r^2 = (s-\alpha)^2, \tag{3.50}$$

$$bc-ab = t^2-r^2 = (t-\beta)^2, \tag{3.51}$$

gdje su $0 < \alpha < s$, $0 < \beta < t$. Tada imamo

$$r^2 = 2s\alpha - \alpha^2 = 2t\beta - \beta^2. \tag{3.52}$$

Iz (3.52) dobivamo

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

i

$$(\beta^2-4)^2 = b(4c\beta^2 - a^2b - 2a(4+\beta^2)). \tag{3.53}$$

Iz (3.53) zaključujemo da je ili $\beta = 1$ ili $\beta = 2$ ili $\beta^2 \geq \sqrt{b}+4$.

Ako je $\beta = 1$, onda je

$$b(4c - a^2b - 10a) = 9, \tag{3.54}$$

što povlači da $b \mid 9$, ali to je moguće samo za $b = 9$ (nema $D(4)$-trojki s $b < 4$). To povlači $a = 5$, ali onda (3.54) daje $c = 69$, a $\{5, 9, 69\}$ nije $D(4)$-trojka.

Ako je $\beta = 2$, onda iz (3.53) dobivamo

$$c = \frac{a^2b + 16a}{16}. \tag{3.55}$$

Sada imamo

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

pa je $s^2 > \left(\frac{ar}{4}\right)^2$ i $s^2 < \left(\frac{ar+8}{4}\right)^2$. Stoga imamo nekoliko mogućih slučajeva za razmotriti:

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

$$2a(rn - 6a) = 64 - n^2. \tag{3.56}$$

   Lijeva strana od (3.56) je parna, a desna neparna, pa smo dobili kontradikciju.

2. $s^2 = \left(\frac{ar+2}{4}\right)^2$, ili ekvivaventno $a(r-3a) = 15$. Ako je $a \leq 3$, onda (3.55) povlači da je $c < b$, kontradikcija. Slučaj $a = 5$ daje trojku $\{5, 64, 105\}$ koja ne zadovoljava $c > ab$ (c je jednako $a+b+2r$), dok slučaj $a = 15$ vodi na $15b + 4 = 46^2$, što nema cjelobrojnih rješenja.

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

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

Dakle, preostao nam je slučaj $\beta^2 \geq \sqrt{b}+4$, koji povlači

$$\beta > \max\{\sqrt[4]{b}, 2\} \tag{3.57}$$

Funkcija $f(\beta) = t^2 - (t-\beta)^2$ je rastuća za $0 < \beta < t$. Stoga je

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

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

$$c < a^2\sqrt{b}. \tag{3.58}$$

Pomoću (3.43) definirat ćemo cijeli broj d_- kao

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

Tada je $d_- \neq 0$ (jer je $c \neq a + b + 2r$) i $\{a, b, c, d_-\}$ je $D(4)$-četvorka. Posebno,

$$ad_- + 4 = \left(\frac{rs - at}{2}\right)^2. \tag{3.59}$$

Nadalje,

$$c = a + b + d_- + \frac{1}{2}(abd_- + \sqrt{(ab + 4)(ad_- + 4)(bd_- + 4)}) > abd_- \tag{3.60}$$

(prema dokazu Leme 3.3). Uspoređujući ovo s (3.58), dobivamo

$$d_- < \frac{a}{\sqrt{b}}. \tag{3.61}$$

Dakle, imamo $d_- < a < b$, što povlači da je b najveći element u $D(4)$-trojki $\{a, b, d_-\}$. To znači da je, po Napomeni 3.1, $b \geq a + d_- + 2\sqrt{ad_- + 4}$ ili ekvivalentno $d_- \leq a + b - 2r$. Definirajmo još i

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

Imamo

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

Ovo povlači da je

$$c < 2(a + b + d_- + \frac{1}{2}abd_-) < 4b + abd_- < 2abd_-. \tag{3.62}$$

(ovdje smo koristili da je $ad_- > 4$, što je točno jer je $\{a, d_-\}$ $D(4)$-par). Označimo $p = \frac{rs-at}{2}$. Tada je $p > 0$ i, po (3.59), imamo $ad_- + 4 = p^2$. Da bi ocijenili p, definiramo $p' = \frac{rs+at}{2}$. Tada je

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

i

$$p < \frac{2a(c + b)}{2at} < \frac{c + b}{\sqrt{bc}} = \frac{\sqrt{c}}{\sqrt{b}} + \frac{\sqrt{b}}{\sqrt{c}},$$

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

Nadalje, imamo

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

i stoga

$$p > \frac{\sqrt{c}}{\sqrt{b}} - \frac{2\sqrt{c}}{ab\sqrt{b}}. \tag{3.63}$$

Nejednakost (3.58) povlači da je $c < \frac{ab^2}{2}$, a ovo je ekvivalentno s

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

što povlači

$$p > \frac{\sqrt{c}}{\sqrt{b}} - \frac{\sqrt{b}}{\sqrt{c}}. \tag{3.64}$$

Uspoređujući dobivene dvije ocjene za p, dobivamo

$$\left| p - \frac{\sqrt{c}}{\sqrt{b}} \right| < \frac{\sqrt{b}}{\sqrt{c}}. \tag{3.65}$$

Definirajmo cijeli broj α sa

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

Pretpostavimo da je $\alpha = 0$. Tada (3.59) povlači da je $d_-(4\beta^2 d_- - a) = 4$, pa je $d_- \in \{1, 2, 4\}$. Imamo tri slučaja:

1. $d_- = 1$, što povlači $2\beta = p$. Uz ovu pretpostavku, (3.51) daje

$$r^2 + \frac{p^2}{4} = tp, \tag{3.66}$$

dok c zadovoljava nejednakosti

$$ab < ab + a + b + 1 < c < ab + 2a + 2b + 2 < ab + 4b < 2ab$$

(prema Lema 3.3 i (3.62) za $d_- = 1$). Lijeva strana od (3.66) je

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

S druge strane, prema (3.63), desna strana od (3.66) je

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

Uspoređujući dvije dobivene nejednakosti za (3.66), dobivamo

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

što je u kontradikciji s $b \geq 12$ (b je najveći element u $D(4)$-trojki $\{d_-, a, b\}$). Slično ćemo razriješiti i preostala dva slučaja.

2. $d_- = 2$, što povlači $4\beta = p$, a ovo daje

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

što je kontradikcija s $b \geq 16$ ($D(4)$-trojka oblika $\{2, a, b\}$ s najmanjim b je $\{2, 6, 16\}$).

3. $d_- = 4$ je ekvivalentno $8\beta = p$, što daje

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

ali jedina $D(4)$-trojka oblika $\{4, a, b\}$ s $b < 35$ je $\{4, 8, 24\}$, a ona ne zadovoljava (3.61), pa smo ponovno dobili kontradikciju.

Stoga, sada možemo pretpostaviti da je $\alpha \neq 0$. Ocijenit ćemo $2d_-t\beta$ i usporediti s c. Najprije dokazujemo da vrijedi

$$\beta^2 < \frac{a^2 b}{c}. \tag{3.67}$$

Budući da je $\beta < t$, a slučaj $\beta = t-1$ daje $b(c-a) = 1$, što je nemoguće, zaključujemo da je $t \geq \beta + 2$. Ovo povlači $t\beta \geq \beta^2 + 2\beta$ i $ab - t\beta \geq 2\beta - 4 > 0$ zbog (3.57). Stoga dobivamo da je $t\beta < ab$, a ovo očito povlači (3.67).

Dakle,

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

Iz $2t\beta = r^2 + \beta^2 > ab + 4$, slijedi $2d_-t\beta > abd_- + 4d_-$. S druge strane,

$$d_-\beta^2 < \frac{d_- a^2 b}{c} \Leftrightarrow 2d_-t\beta < abd_- + 4d_- + \frac{d_- a^2 b}{c} < abd_- + 4d_- + a.$$

Kombinirajući ove dvije ocjene, dobivamo

$$abd_- + 4d_- < 2d_-t\beta < abd_- + 4d_- + a. \tag{3.68}$$

Uspoređujući (3.68) s (3.60) i (3.62), zaključujemo da je

$$|2d_-t\beta - c| < 4b. \tag{3.69}$$

Kombinirajući ocjenu (3.65) za p s trivijalnom ocjenom za α, naime $|\alpha| \geq 1$, dobivamo

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

Uočimo da je $ad_- > 26$. Zaista, $D(4)$-parovi takvi da je $ad_- \leq 26$ su $\{1, 5\}$, $\{1, 12\}$, $\{1, 21\}$, $\{2, 6\}$, $\{3, 4\}$ i $\{3, 7\}$. Iz prva tri para, uzimajući u obzir (3.60) i (3.61), nalazimo trojke

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

koje ne zadovoljavaju niti (3.47) niti (3.48). Iz zadnja tri para ne možemo dobiti $D(4)$-trojku zbog (3.61).

Konačno, dobivamo

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

što je u kontradikciji s (3.69). □

Teorem 3.5. *$E'(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Dokaz. Po Mazurovom teoremu, budući da E' ima tri točke reda 2, jedine mogućnosti za $E'(\mathbb{Q})_{tors}$ su $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ za $k = 1, 2, 3, 4$. Ali Lema 3.4 pokazuje da slučajevi $k = 2, 4$ nisu mogući za eliptičke krivulje inducirane $D(4)$-trojkama s pozitivnim elementima. □

Korolar 3.2. *Neka je $\{a, b, c\}$ $D(1)$-trojka. Tada je torzijska grupa eliptičke krivulje $y^2 = (ax + 1)(bx + 1)(cx + 1)$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ili $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

Napomena 3.4. Primijetimo da analogon Teorema 3.5 i Korolara 3.2 ne vrijedi za općenite $D(n^2)$-trojke i njihove inducirane eliptičke krivulje

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

Ako u prije navedenim primjerima različitih torzijskih grupa s racionalnim Diofantovim $D(1)$-trojkama pomnožimo sve elemente s najmanjim zajedničkim višekratnikom njihovih nazivnika, nazovimo ga n, dobit ćemo $D(n^2)$-trojku s tom istom torzijskom grupom. Kao jedan konkretan jednostavan primjer, navedimo $D(9)$-trojku $\{8, 54, 104\}$ koja inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Napomenimo da nije poznat niti jedan primjer $D(1)$ ili $D(4)$-trojke koja inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Poznato je da se ta torzijska grupa ne može pojaviti za neke konkretne familije $D(1)$-trojki. Kao što smo već argumentirali, za općenite $D(n^2)$-trojke takvi primjeri postoje. Primjerice, $D(294^2)$-trojka $\{32, 539, 1215\}$ inducira eliptičku krivulju s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Poglavlje 4

Cjelobrojne točke na eliptičkim krivuljama

4.1 Mordellova jednadžba

Godine 1923. Mordell je dokazao da diofantske jednadžbe oblika

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

gdje kubni polinom na desnoj strani jednadžbe nema višestrukih korijena, imaju samo konačno mnogo cjelobrojnih rješenja. Drugim riječima, dokazao je da eliptičke krivulje s cjelobrojnim koeficijentima imaju konačno mnogo cjelobrojnih točaka. Mordellov dokaz koristi se svođenjem ovakve jednadžbe na konačno mnogo Thueovih jednadžbi, o čemu će biti više riječi poslije.

Problem nalaženja svih cjelobrojnih rješenja ovakvih jednadžbi, (tj. svih cjelobrojnih točaka na eliptičkim krivuljama) nije jednostavan. Ipak, poznato je dosta rezultata, posebno za *Mordellovu jednadžbu* oblika

$$y^2 = x^3 + k, \tag{4.1}$$

koji su dobiveni sasvim elementarnim metodama – razmatranjem konguencija modulo 4 i 8 te svojstava kvadratnih ostataka. U ovom potpoglavlju ćemo prikazati nekoliko takvih rezultata.

Propozicija 4.1. *Neka je $k = (4b-1)^3 - 4a^2$, gdje je a cijeli broj koji nema prostih faktora oblika $4l+3$. Tada jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Dokaz: Imamo $k \equiv -1 \pmod 4$, pa je $y^2 \equiv x^3 - 1 \pmod 4$. Budući da je $y^2 \equiv 0$ ili $1 \pmod 4$, x ne može biti paran ni kongruentan -1 modulo 4. Stoga je $x \equiv 1 \pmod 4$. Zapišimo jednadžbu $y^2 = x^3 + (4b-1)^3 - 4a^2$ u obliku

$$y^2 + 4a^2 = x^3 + (4b-1)^3 = (x + 4b - 1)(x^2 - x(4b-1) + (4b-1)^2).$$

Zadnji faktor $x^2 - x(4b-1) + (4b-1)^2$ je kongruentan 3 modulo 4. Stoga on mora imati barem jedan prosti faktor p, koji je također kongruentan 3 modulo 4. No taj prosti faktor p može dijeliti zbroj dvaju kvadrata $y^2 + 4a^2$ jedino ako su i y i a djeljivi s p (jer je s jedne strane Legendreov simbol $(\frac{-1}{p}) = (-1)^{(p-1)/2} = -1$, a s druge

strane bi bilo $(\frac{-1}{p}) = (\frac{-4a^2}{p}) = (\frac{y^2}{p}) = 1$), a to je u suprotnosti s pretpostavkom da a nema prostih faktora oblika $4l+3$. □

Nekoliko cijelih brojeva k koji zadovoljavaju uvjete Propozicije 4.1 su: $k = -5$, 11, -17, 23, -37, -57, -65, -73, 87.

Propozicija 4.2. *Neka je $k = 2b^2 - a^3$, gdje je $a \equiv 2$ ili $4 \pmod 8$, $b \equiv 1 \pmod 2$ i svi prosti faktori od b su oblika $8l \pm 1$. Tada jednadžba $y^2 = x^3 + k$ nema cjelobrojnih rješenja.*

Dokaz: Imamo $y^2 \equiv x^3 + 2 \pmod 4$, pa je $x \not\equiv 0 \pmod 2$ i $x \not\equiv 1 \pmod 4$. Stoga je $x \equiv 3 \pmod 4$, tj. $x \equiv 3$ ili $7 \pmod 8$. Nadalje,

$$y^2 - 2b^2 = x^3 - a^3 = (x-a)(x^2+ax+a^2).$$

Ako je $x \equiv 3 \pmod 8$, onda je $x^2 + ax + a^2 \equiv 1 + 3a + a^2 \equiv \pm 3 \pmod 8$, pa $x^2 + ax + a^2$ ima barem jedan prosti faktor p oblika $8l \pm 3$. Prema pretpostavci, p ne dijeli b, pa dobivamo

$$\left(\frac{2}{p}\right) = \left(\frac{2b^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1.$$

Dobili smo kontradikciju jer je $(\frac{2}{p}) = 1$ ako i samo ako je $p \equiv \pm 1 \pmod 8$.

Ako je $x \equiv 7 \pmod 8$, onda je $x - a \equiv 7 - a \equiv \pm 3 \pmod 8$, pa $x - a$ mora imati barem jedan prosti faktor oblika $8l \pm 3$, iz čega dobivamo kontradikciju na sasvim isti način kao i u prethodnom slučaju. □

Nekoliko vrijednosti od k koje zadovoljavaju uvjete Propozicije 4.2 su $k = -6$, 34, 58, -62, 66, 90.

Primjer 4.1. *Pokažimo da jednadžba $y^2 = x^3 + 45$ nema cjelobrojnih rješenja.*

Dokaz: Zbog $y^2 \equiv x^3 + 5 \pmod 8$, imamo da je $x \equiv 3$ ili $7 \pmod 8$. Ako bi bilo $x \equiv 0 \pmod 3$, onda bi iz $x = 3X$, $y = 3Y$, dobili $Y^2 = 3X^3 + 5 \equiv 2 \pmod 3$, što je kontradikcija jer 2 nije kvadratni ostatak modulo 3. Stoga x nije djeljiv s 3.

Pretpostavimo da je $x \equiv 3 \pmod 8$. Zapišimo jednadžbu u obliku

$$y^2 - 2 \cdot 6^2 = x^3 - 27 = (x-3)(x^2+3x+9).$$

Imamo da je $x^2 + 3x + 9 \equiv 3 \pmod 8$, pa taj broj mora imati neki prosti faktor p oblika $8l \pm 3$. Budući da smo provjerili da je $p \neq 3$, p ne može biti faktor od $y^2 - 2 \cdot 6^2$ jer 2 nije kvadratni ostatak modulo p.

Pretpostavimo da je $x \equiv 7 \pmod 8$. Sada ćemo polaznu jednadžbu zapisati u obliku

$$y^2 - 2 \cdot 3^2 = x^3 + 27 = (x+3)(x^2-3x+9).$$

Imamo da je $x^2 - 3x + 9 \equiv 5 \pmod 8$, pa taj broj mora imati neki prosti faktor p oblika $8l \pm 3$. No p ne može biti faktor od $y^2 - 2 \cdot 3^2$, pa smo ponovo dobili kontradikciju. ♢

Jednadžbu $y^2 = x^3 + k$ možemo zapisati u obliku $x^3 = y^2 - k$ te je faktorizirati u polju $\mathbb{Q}(\sqrt{k})$:

$$x^3 = (y + \sqrt{k})(y - \sqrt{k}). \tag{4.2}$$

Da bismo mogli ovu faktorizaciju iskoristiti za rješavanje polazne jednadžbe, potrebne su nam neke informacije o cijelim brojevima u kvadratnom polju $\mathbb{K} = \mathbb{Q}(\sqrt{k})$. Pretpostavit ćemo da je k kvadratno slobodan. Ponajprije, podsjetimo se da je prsten cijelih brojeva $\mathcal{O}_{\mathbb{K}}$ u $\mathbb{K}$ jednak $\{u + v\sqrt{k} \,:\, u, v \in \mathbb{Z}\}$ ako je $k \equiv 2$ ili $3 \pmod 4$, odnosno $\{u + v\frac{1+\sqrt{k}}{2} \,:\, u, v \in \mathbb{Z}\}$ ako je $k \equiv 1 \pmod 4$. Sljedeći važni podatak je struktura skupa jedinica (invertibilnih elemenata) u $\mathcal{O}_{\mathbb{K}}$. Ako je $k \geq 2$, onda ima beskonačno mnogo jedinica u $\mathbb{K}$, i one imaju oblik $\pm\varepsilon_k^n$, $n \in \mathbb{Z}$, gdje je ε_k fundamentalna jedinica. Ako je k negativan, onda $\mathbb{K}$ ima jedinice ± 1 i to su jedine jedinice, osim u slučajevima $k = -1$ i $k = -3$. Jedinice u $\mathbb{Q}(i)$ su ± 1, $\pm i$, a u $\mathbb{Q}(\sqrt{-3})$ su ± 1, $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

U relaciji (4.2) imamo da je produkt dvaju brojeva jednak kubu. Kad bi se radilo o produktu (običnih) cijelih brojeva i ako bi faktori bili relativno prosti, onda bismo mogli zaključiti da su oba faktora kubovi. U tom zaključku se rabi jedinstvenost rastava cijelih brojeva na proste faktore. Međutim, to svojstvo ne vrijedi za cijele brojeve u svim kvadratnim poljima. Preciznije, jedina kvadratna polja s takvim svojstvom za $k < 0$ su ona za $k = -1, -2, -3, -7, -11, -19, -43, -67, -163$, dok je slutnja da takvih polja za $k > 0$ ima beskonačno mnogo.

Na primjer, u $\mathbb{Q}(\sqrt{-5})$ imamo:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}) \tag{4.3}$$

i može se pokazati da su svi faktori $3, 7, 1 + 2\sqrt{-5}, 1 - 2\sqrt{5}, 4 + \sqrt{5}, 4 - \sqrt{5}$ *nerastavljivi*, tj. da su djeljivi samo s jedinicama i sebi pridruženim brojevima (brojevi su pridruženi ako im je kvocijent jedinica).

Ipak, jedinstvenost faktorizacije je moguće dobiti ako se umjesto brojeva promatraju ideali jer se svaki pravi ideal u $\mathcal{O}_{\mathbb{K}}$ može na jedinstven način prikazati kao produkt prostih ideala.

Primjer 4.2. *Nađimo sva cjelobrojna rješenja jednadžbe $y^2 = x^3 - 11$.*

Rješenje: Poznato je da $\mathbb{Q}(\sqrt{-11})$ ima svojstvo jedinstvene faktorizacije. Jedinice u $\mathbb{Q}(\sqrt{-11})$ su ± 1. Stoga iz

$$(y + \sqrt{-11})(y - \sqrt{-11}) = x^3$$

i činjenice da su faktori na desnoj strani ove jednadžbe relativno prosti (jer njihov zajednički faktor dijeli $2\sqrt{-11}$, a x ne može biti djeljiv ni sa 2 ni sa 11), slijedi da postoji algebarski cijeli broj $w \in \mathbb{Q}(\sqrt{-11})$ takav da je

$$y + \sqrt{-11} = \pm w^3.$$

Budući da je $-w^3 = (-w)^3$, predznak minus možemo izostaviti. Dakle,

$$y + \sqrt{-11} = w^3, \quad w = a + \frac{b}{2}(1 + \sqrt{-11}) = (a + \frac{b}{2}) + \frac{b}{2}\sqrt{-11}.$$

Izjednačavanjem koeficijenata uz $\sqrt{-11}$, dobivamo:

$$1 = 3\Big(a + \frac{b}{2}\Big)^2 \cdot \frac{b}{2} - 11 \cdot \Big(\frac{b}{2}\Big)^3,$$

odnosno

$$b(3a^2 + 3ab - 2b^2) = 2.$$

Odavde je $b = \pm 1$ ili ± 2, pa je $(a, b) = (0, -1), (1, -1), (1, 2), (-3, 2)$. Sada iz $y = (a + \frac{b}{2})^3 + 3(a + \frac{b}{2}) \cdot (\frac{b}{2})^2 \cdot (-11)$ slijedi $y = \pm 4, \pm 58$, pa su sva rješenja zadane jednadžbe $(x, y) = (3, \pm 4), (15, \pm 58)$. ♢

4.2 Thueova jednadžba

U sljedećem potpoglavlju prikazat ćemo kako se problem nalaženja cjelobrojnih točaka na eliptičkoj krivulji može svesti na problem rješavanja konačnog broja Thueovih jednadžbi. Pa kažimo zato najprije nešto o Thueovoj jednadžbi.

Neka je

$$F(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n$$

binarna forma s cjelobrojnim koeficijentima, ireducibilna nad $\mathbb{Q}$, stupnja $n \geq 3$. Primijetimo da forma F ne može biti ireducibilna nad $\mathbb{C}$. Naime, prema Osnovnom teoremu algebre,

$$F(x,1) = a_0(x-\theta_1)\cdot\ldots\cdot(x-\theta_n),$$

gdje su $\theta_1,\ldots,\theta_n$ algebarski brojevi stupnja n, pa je

$$F(x,y) = y^nF\big(\frac{x}{y},1\big) = a_0(x-\theta_1y)\cdot\ldots\cdot(x-\theta_ny).$$

Ireducibilnost nad $\mathbb{Q}$ povlači da $f(x) = F(x,1)$ nema višestrukih korijena, tj. da su θ_i-ovi međusobno različiti. Zaista, kada bi $f(x)$ imao višestruki korijen, onda bi $\mathrm{nzd}(f,f') \in \mathbb{Q}[x]$ bio netrivijalni faktor od f, pa $f(x)$, a onda i $F(x,y)$, ne bi bio ireducibilan nad $\mathbb{Q}$. Neka je $m \neq 0$ cijeli broj. Tada diofantsku jednadžbu $F(x,y) = m$ zovemo *Thueova jednadžba*. Godine 1909. norveški matematičar Axel Thue (1863. – 1922.) dokazao je da takva jednadžba ima samo konačno mnogo cjelobrojnih rješenja koristeći se svojim poznatim rezultatom iz diofantskih aproksimacija. Dokažimo najprije jednostavan specijalni slučaj.

Teorem 4.1. *Ako jednadžba $F(x,1) = 0$ nema realnih rješenja, tada jednadžba $F(x,y) = m$ ima samo konačno mnogo cjelobrojnih rješenja. Preciznije, sva rješenja zadovoljavaju nejednakost*

$$|y| \leq \frac{\sqrt[n]{|m|}}{\min_{1\leq i\leq n}|\operatorname{Im}(\theta_i)|},$$

gdje je $n \geq 3$ stupanj polinoma F, a θ_i korijeni polinoma $F(x,1)$.

Dokaz: Pretpostavimo da je (x,y) rješenje jednadžbe $F(x,y) = m$ i uzmimo θ_k tako da je $|x-\theta_ky| = \min_{1\leq i\leq n}|x-\theta_iy|$. Tada je očito $|y||\operatorname{Im}(\theta_k)| = |\operatorname{Im}(\theta_ky)| \leq |x-\theta_ky| \leq \sqrt[n]{|m|}$, pa dobivamo tvrdnju teorema. □

Navedimo i alternativni dokaz Teorema 4.1, s nešto drukčijom gornjom ogradom za $|y|$. Za $y = 0$ možemo imati najviše dva rješenja, pa pretpostavimo da je $y \neq 0$. Budući da polinom $F(x,1)$ nema realnih korijena, zaključujemo da postoji realni broj $c > 0$ takav da je $|F(z,1)| > c$ za svaki realni broj z. Sada iz

$$|m| = |F(x,y)| = |y|^n\big|F\big(\frac{x}{y},1\big)\big| > c|y|^n$$

slijedi da je $|y| < \sqrt[n]{|m|/c}$.

Primjer jednadžbe

$$F(x,y) = x^n + (x-y)^2(2x-y)^2\cdot\ldots\cdot\big(\frac{n}{2}x-y\big)^2 = 1,$$

za parni broj n, kod koje polinom $F(x,1)$ očito nema realnih korijena, a koja ima rješenja $\pm(1,1)$, $\pm(1,2)$, $\ldots$, $\pm(1,n/2)$, pokazuje da se ograda $|y| < \sqrt[n]{|m|/c}$ ne može bitno poboljšati.

Spomenuti Thueov rezultat iz diofantskih aproksimacija govori o racionalnim aproksimacijama algebarskih brojeva. Prvi važan rezultat tog tipa je Liouvilleov teorem.

Teorem 4.2 (Liouville, 1844.). *Neka je α realni algebarski broj stupnja d. Tada postoji konstanta $c(\alpha) > 0$ tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$$

za sve racionalne brojeve $\frac{p}{q}$, gdje je $q > 0$ i $\frac{p}{q} \neq \alpha$.

Dokaz: Neka je $P(x)$ cjelobrojni minimalni polinom od α. Bez smanjenja općenitosti možemo pretpostaviti da je $|\alpha - \frac{p}{q}| \leq 1$ (inače možemo staviti $c(\alpha) = 1$). Razvijemo li $P(x)$ u Taylorov red oko α, dobivamo

$$\left|P\Big(\frac{p}{q}\Big)\right| = \left|\sum_{i=1}^{d}\Big(\frac{p}{q} - \alpha\Big)^i \frac{1}{i!}P^{(i)}(\alpha)\right| < \frac{1}{c(\alpha)} \cdot \left|\alpha - \frac{p}{q}\right|, \tag{4.4}$$

gdje je $c(\alpha) = \big(2\sum_{i=1}^{d}\frac{1}{i!}|P^{(i)}(\alpha)|\big)^{-1}$.

Budući da je polinom $P(x)$ ireducibilan, to je $P(\frac{p}{q}) \neq 0$. Stoga je broj $q^d\big|P(\frac{p}{q})\big|$ prirodan, pa je $\big|P(\frac{p}{q})\big| \geq \frac{1}{q^d}$. Usporedimo li ovo s (4.4), dobivamo tvrdnju teorema. □

Neka je α realni algebarski broj stupnja $d \geq 2$. Liouvilleov teorem povlači da nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu} \tag{4.5}$$

ima samo konačno mnogo racionalnih rješenja $\frac{p}{q}$ ako je $\mu > d$.

Thue (1909) je dokazao da (4.5) ima samo konačno mnogo rješenja ako je $\mu > \frac{d}{2} + 1$, Siegel (1921) je dokazao da ista tvrdnja vrijedi ako je $\mu > 2\sqrt{d}$, dok su Dyson (1947) i Geljfond (1948) dokazali tvrdnju za $\mu > \sqrt{2d}$. Konačno je Roth (1955) dokazao da nejednadžba (4.5) ima samo konačno mnogo rješenja ako je $\mu > 2$. Za taj rezultat Klaus Roth je 1958. godine nagrađen Fieldsovom medaljom.

Teorem 4.3 (Roth, 1955.). *Neka je α realni algebarski broj stupnja $d \geq 2$. Tada za svaki $\delta > 0$ nejednadžba*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}} \tag{4.6}$$

ima samo konačno mnogo rješenja u racionalnim brojevima $\frac{p}{q}$.

Ideja dokaza Rothova teorema (a i prethodnih poboljšanja Liouvilleova teorema) je da se pokuša modificirati osnovne korake u dokazu Liouvilleova teorema. U Liovilleovu teoremu kreće se od minimalnog polinoma od α. U svom poboljšanju Liouvilleova teorema, Thue se koristio polinomom oblika $x_2Q(x_1) - P(x_1)$, Siegel se koristio općenitijim polinomom $P(x_1, x_2)$ u dvije varijable, dok se Roth koristio polinomom $P(x_1, \ldots, x_m)$ u više varijabli. Glavna poteškoća u ovakvu pristupu

nastupa kod provjere zadnjeg koraka iz dokaza Liouvilleova teorema. Kod polinoma u jednoj varijabli, zaključak da je $P(\frac{p}{q}) \neq 0$ bio je sasvim jednostavan. No kod polinoma u više varijabli, skup rješenja jednadžbe $P(x_1, \ldots, x_m) = 0$ je neka algebarska mnogostrukost u $\mathbb{R}^m$ i vrlo je teško pokazati da je $P(\frac{p}{q}, \ldots, \frac{p}{q}) \neq 0$. Ta se poteškoća pokušava riješiti korištenjem m-torki $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ različitih racionalnih aproksimacija i pokušava se dokazati da je $P(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}) \neq 0$. Pokazuje se da nazivnici $q_1 < q_2 < \cdots < q_m$ moraju brzo rasti. Primjerice, u slučaju $m = 2$, trebaju nam dvije dobre aproksimacije $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$ od α takve da je q_2 puno veći od q_1. To je razlog zbog čega jedna dobra aproksimacija ne daje nikakvu kontradikciju, te je Rothov teorem, kao i sva ostala poboljšanja Liouvilleovog teorema dobivena ovom metodom, "neefektivan", u smislu da ne daje nikakvu ogradu za veličinu nazivnika q u dobrim aproksimacijama.

Teorem 4.4 (Thue, 1909.)**.** *Thueova jednadžba ima samo konačno mnogo cjelobrojnih rješenja.*

Dokaz: Neka je $F(x, y) = m$ dana Thueova jednadžba. Uz gore uvedene oznake, možemo pisati

$$a_0(x - \theta_1 y) \cdot \ldots \cdot (x - \theta_n y) = m. \tag{4.7}$$

Možemo pretpostaviti da je $y \neq 0$ jer za $y = 0$ imamo najviše dva rješenja. Podijelimo (4.7) s y^n i uzmimo apsolutne vrijednosti, pa dobivamo

$$|a_0| \cdot \left|\theta_1 - \frac{x}{y}\right| \cdot \ldots \cdot \left|\theta_n - \frac{x}{y}\right| = \left|\frac{m}{y^n}\right|. \tag{4.8}$$

Kao i u dokazu Teorema 4.1, uzmimo θ_k tako da je

$$|x - \theta_k y| = \min_{1 \leq i \leq n} |x - \theta_i y|,$$

tj.

$$\left|\theta_k - \frac{x}{y}\right| = \min_{1 \leq i \leq n} \left|\theta_i - \frac{x}{y}\right|.$$

Neka je $\gamma = \frac{1}{2} \min_{i \neq j} |\theta_i - \theta_j| > 0$. Za y dovoljno velik, obje strane od (4.8) se mogu učiniti po volji male. Posebno to onda vrijedi i za najmanji faktor na lijevoj strani, tj. $|\theta_k - \frac{x}{y}|$. Dakle, postoji $y_0 > 0$ tako da za $y \geq y_0$ vrijedi $|\theta_k - \frac{x}{y}| < \gamma$. Za $i \neq k$ imamo

$$\left|\theta_i - \frac{x}{y}\right| \geq |\theta_i - \theta_k| - \left|\theta_k - \frac{x}{y}\right| \geq 2\gamma - \gamma = \gamma.$$

Stoga iz (4.8) slijedi

$$\left|\theta_k - \frac{x}{y}\right| \leq \left|\frac{m}{a_0 y^n \gamma^{n-1}}\right| = \frac{c}{|y|^n}. \tag{4.9}$$

Budući da je $n \geq 3$, Rothov teorem (u stvari već i Thueov, ali ne i Liouvilleov) povlači da nejednadžba (4.9) ima samo konačno mnogo rješenja, što je i trebalo dokazati. □

Napomena 4.1. Iz svojstava linearnih diofantskih jednadžbi i Pellovih jednadžbi znamo da tvrdnja Teorema 4.4 ne vrijedi ako je stupanj od F jednak 1 ili 2. S druge strane, tvrdnja Teorema 4.4 vrijedi ako se pretpostavka da je polinom $F(x, y)$ ireducibilan nad $\mathbb{Q}$ zamijeni s pretpostavkom da polinom $F(x, 1)$ ima barem tri različita korijena.

Zaista, pretpostavimo da je polinom $F(x, y)$ reducibilan nad $\mathbb{Q}$. Ako F ima barem dva različita ireducibilna faktora F_1 i F_2, onda dobivamo konačno mnogo sustava diofantskih jednadžbi $F_1(x, y) = m_1$, $F_2(x, y) = m_2$. Svaki od tih sustava ima konačno mnogo (kompleksnih) rješenja (prema Bezoutovu teoremu broj rješenja nije veći od produkta stupnjeva od F_1 i F_2). Ostaje razmotriti slučaj $F(x, y) = aG(x, y)^k$, gdje je polinom G ireducibilan nad $\mathbb{Q}$. Ako je $\deg G \geq 3$, onda iz Teorema 4.4 slijedi da jednadžba $F(x, y) = m$ ima konačno mnogo rješenja. Dakle, jedini slučajevi kada jednadžba $F(x, y) = m$, gdje je F binarna forma, može imati beskonačno mnogo rješenja su jednadžbe oblika

$$F(x, y) = a(bx + cy)^n \quad \text{ili} \quad F(x, y) = a(bx^2 + cxy + dy^2)^{n/2},$$

a to su upravo slučajevi kada $F(x, 1)$ ima manje od tri različita korijena.

4.3 Transformacija eliptičkih krivulja u Thueove jednadžbe

Promotrimo općenitu jednadžbu oblika

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

gdje su koeficijenti a, b, c cijeli brojevi, a kubni polinom na desnoj strani nema višestrukih korijena. Prikazat ćemo Mordellov argument kojim je pokazao da takva jednadžba ima samo konačno mnogo cjelobrojnih rješenja. Istodobno, to je i važan korak u jednoj od općih metoda za nalaženje svih cjelobrojnih točaka na eliptičkoj krivulji. Općenitiji rezultat da je broj cjelobrojnih točaka na bilo kojoj nesingularnoj kubnoj krivulji s cjelobrojnim koeficijentima konačan, dokazao je njemački matematičar Carl Ludwig Siegel 1929. godine. Ovdje je važno primijetiti da iako biracionalne transformacije čuvaju strukturu skupa racionalnih točaka na krivuljama, to nije točno za skup cjelobrojnih točaka koji bitno ovisi o izabranom modelu (jednadžbi) krivulje.

Ideja je faktorizirati polinom

$$f(x) = x^3 + ax^2 + bx + c = (x - \vartheta_1)(x - \vartheta_2)(x - \vartheta_3). \tag{4.10}$$

Tako dobivamo polja $\mathbb{Q}(\vartheta_i)$ u kojima promatramo jednadžbu (4.10). Moguća su tri slučaja:

1) sva tri korijena od f su racionalna (pa onda i cijela);

2) jedan korijen od f je racionalan, a ostala dva su kvadratne iracionalnosti;

3) f je ireducibilan nad $\mathbb{Q}$, korijeni su mu algebarski cijeli brojevi 3. stupnja.

Podsjetimo se da u $\mathbb{Z}$ vrijedi: ako je $XY = Z^\ell$ i $\mathrm{nzd}(X, Y) = 1$, onda postoje $U, V \in \mathbb{Z}$ tako da je $X = \pm U^\ell$, $Y = \pm V^\ell$, $Z = \pm UV$. Poopćenje tog rezultata na cijele brojeve u polju algebarskih brojeva $\mathbb{K}$ dano je sljedećom lemom.

Lema 4.1. *Sva rješenja (X, Y, Z) u $\mathcal{O}_\mathbb{K}$ jednadžbe*

$$XY = cZ^\ell,$$

gdje $<X,Y>|\ \delta$ za dani ideal δ, imaju oblik

$$X = \lambda\varepsilon_1 U^\ell, \quad Y = \mu\varepsilon_2 V^\ell, \quad Z = \nu\varepsilon_3 UV,$$

gdje su U, V proizvoljni cijeli brojevi iz $\mathbb{K}$, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ su jedinice, λ, μ, ν su elementi iz $\mathbb{K}$. Posljednjih šest brojeva $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \lambda, \mu, \nu)$ poprimaju samo konačno mnogo vrijednosti i zadovoljavaju $\lambda\mu\varepsilon_1\varepsilon_2 = c\nu^\ell\varepsilon_3^\ell$.

Vratimo se na jednadžbu (4.10). Promatramo je u polju $\mathbb{K} = \mathbb{Q}(\vartheta_i)$. Dat ćemo skicu algoritma za treći slučaj, kad je kubni polinom $f(x)$ ireducibilan. Transformacija eliptičke krivulje u Thueove jednadžbe u preostala dva slučaja provodi se na sličan način. Iz Leme 4.1 slijedi relacija

$$x - \vartheta_i = m(r + s\vartheta_i + t\vartheta_i^2)^2, \tag{4.11}$$

gdje su $r, s, t \in \mathbb{Z}$, a m poprima konačno mnogo vrijednosti iz $\mathbb{Q}(\vartheta_i)$. Zaista, ϑ_i je algebarski cijeli broj 3. stupnja, pa se svaki element iz $\mathbb{K}$ može napisati u obliku $\alpha + \beta\vartheta_i + \gamma\vartheta_i^2$, $\alpha, \beta, \gamma \in \mathbb{Q}$. No $\{1, \vartheta_i, \vartheta_i^2\}$ ne mora biti baza za $\mathcal{O}_\mathbb{K}$. Međutim, može se pokazati da ako je $\frac{1}{d}(r + s\vartheta_i + t\vartheta_i^2) \in \mathcal{O}_\mathbb{K}$ i $\mathrm{nzd}(d, r, s, t) = 1$, onda d^2 dijeli diskriminantu $\Delta(1, \vartheta_i, \vartheta_i^2) = (\vartheta_1 - \vartheta_2)^2(\vartheta_1 - \vartheta_3)^2(\vartheta_2 - \vartheta_3)^2$. Stoga imamo konačno mnogo mogućnosti za d, koje možemo "prebaciti" u m.

I broj m (svaki od konačno mnogo njih) možemo zapisati u obliku $m = r_0 + s_0\vartheta_i + t_0\vartheta_i^2$, gdje su $r_0, s_0, t_0 \in \mathbb{Q}$. Uvrstimo to u (4.11), izmnožimo, te ϑ_i^3, ϑ_i^4, ϑ_i^5 i ϑ_i^6 prikažemo s pomoću $1, \vartheta_i, \vartheta_i^2$. Usporedimo li koeficijente uz 1, ϑ_i i ϑ_i^2 na obje strane jednadžbe, dobivamo tri jednadžbe oblika

$$f_1(r, s, t) = 0, \quad f_2(r, s, t) = 1, \quad f_3(r, s, t) = x,$$

gdje su f_1, f_2, f_3 ternarne kvadratne forme s racionalnim koeficijentima. Poznato je da se rješivost jednadžbe $f_1(r, s, t) = 0$ može efikasno ustanoviti. Naime, takve jednadžbe zadovoljavaju lokalno-globalni princip, tj. ako imaju rješenja nad $\mathbb{R}$ te nad p-adskim poljem $\mathbb{Q}_p$ za sve proste brojeve p, onda imaju rješenja i nad $\mathbb{Q}$. Još eksplicitnije, svaka takva jednadžba se može zapisati u obliku $ax^2 + by^2 + cz^2 = 0$, gdje su a, b, c cijeli brojevi takvi da je abc kvadratno slobodan, a nužan i dovoljan uvjet za rješivost ove jednadžbe u racionalnim brojevima je da brojevi a, b, c nisu svi pozitivni niti svi negativni te vrijedi da je $-bc$ kvadratni ostatak modulo a, $-ac$ kvadratni ostatak modulo b i $-ab$ kvadratni ostatak modulo c (Legendreov teorem).

Nadalje, uz pretpostavku da netrivijalno rješenje postoji, sva rješenja dana s

$$gr = q_1(u, v), \quad gs = q_2(u, v), \quad gt = q_3(u, v),$$

gdje su q_1, q_2, q_3 binarne kvadratne forme s cjelobrojnim koeficijentima, a g poprima konačno mnogo cjelobrojnih vrijednosti. Uvrstimo li to u jednadžbu $f_2(r, s, t) = 1$, dobivamo konačno mnogo jednadžbi oblika

$$h(u, v) = g^2, \tag{4.12}$$

gdje je h homogeni polinom četvrtog stupnja s cjelobrojnim koeficijentima. Polinom h nije kvadrat polinoma drugog stupnja (inače bi polazna krivulja bila genusa 0). Stoga prema Thueovu teoremu zaključujemo da jednadžba (4.12) ima konačno mnogo rješenja, pa zato i polazna eliptička krivulja ima samo konačno mnogo cjelobrojnih točaka (koje dobijemo iz $f_3(r, s, t) = x$).

4.4 Algoritam za rješavanje Thueove jednadžbe

U prethodnom potpoglavlju smo vidjeli da se nalaženje cjelobrojnih točaka na eliptičkim krivuljama može svesti na rješavanje Thueovih jednadžbi. Thueove jednadžbe se javljaju i kod drugih važnih problema iz teorije brojeva. Stoga je od velikog interesa postojanje algoritma za sistematsko rješavanje Thueovih jednadžbi. Mi ćemo prikazati jedan takav algoritam – de Wegerov algoritam iz 1989. godine.

Podijelit ćemo skup mogućih rješenja u četiri klase:

- jako mala rješenja: $|y| \leq Y_1$ – provjera "grubom silom";
- mala rješenja: $Y_1 < |y| \leq Y_2$ – odgovaraju konvergentama verižnog razlomka od ϑ_i;
- velika rješenja: $Y_2 < |y| \leq Y_3$ – eliminiraju se LLL-redukcijom;
- jako velika rješenja: $|y| > Y_3$ – dokazuje se da ne postoje s pomoću linearnih formi u logaritmima.

Neka je $g(x) = F(x,1) = a_0(x-\vartheta_1)\cdots(x-\vartheta_n)$. Tada dobivamo jednadžbu $F(x,y) = a_0(x-\vartheta_1 y)\cdots(x-\vartheta_n y) = m$, koju ćemo promatrati u polju algebarskih brojeva $\mathbb{K} = \mathbb{Q}(\vartheta_i)$ (sva su ta polja $\mathbb{Q}$-izomorfna). Neka su $\vartheta_1, \ldots, \vartheta_s$ realni, a $\vartheta_{s+1} = \overline{\vartheta_{s+t+1}}, \ldots, \vartheta_{s+t} = \overline{\vartheta_{s+2t}}$ konjugirano kompleksni korijeni od $g(x)$. Vidjeli smo u Teoremu 4.1, da je slučaj $s = 0$ vrlo jednostavan. Stoga ćemo u daljnjem pretpostaviti da je $s \geq 1$.

Uvedimo oznaku: $\beta_i = x - \vartheta_i y$, za $i = 1, \ldots, n$. Pretpostavimo da je $|a_0| = |m| = 1$. Tada iz $\beta_1\beta_2\cdots\beta_n = \pm 1$, zaključujemo da je β_i jedinica (invertibilni element) u prstenu $\mathcal{O}_\mathbb{K}$. Po Dirichletovu teoremu o jedinicama je

$$\beta_i = \pm\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r},$$

gdje je $\varepsilon_1, \ldots, \varepsilon_r$ sustav fundamentalnih jedinica te $r = s + t - 1$. U općem slučaju ćemo imati

$$\beta_i = \pm\mu_i\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r},$$

gdje μ_i pripada konačnom skupu M neasociranih elemenata iz $\mathcal{O}_\mathbb{K}$ čija norma zadovoljava uvjet $a_0 \cdot N(\mu_i) = m$.

Neka je $|\beta_{i_0}| = \min\{|\beta_i| : 1 \leq i \leq n\}$. Može se pokazati da je tada $i_0 \in \{1, \ldots, s\}$ i vrijedi

$$|\beta_{i_0}| \leq c_1|y|^{-(n-1)}, \tag{4.13}$$
$$|\beta_i| \geq c_2|y|, \quad i \neq i_0, \tag{4.14}$$

gdje je

$$c_1 = \frac{2^{n-1}|m|}{\min\{|g'(\vartheta_i)| : 1 \leq i \leq s\}},$$
$$c_2 = \frac{1}{2}\min\{|\vartheta_i - \vartheta_j| : 1 \leq i < j \leq n\}$$

(vidjeti dokaz Teorema 4.4).

Lema 4.2. *Ako je $|y| > Y_1 = (4c_1)^{\frac{1}{n-2}}$, onda je $\frac{x}{y}$ konvergenta u razvoju u verižni razlomak broja ϑ_{i_0}.*

Dokaz: Imamo:

$$\left|\frac{x}{y}-\vartheta_{i_0}\right| = |\beta_{i_0}|\cdot|y|^{-1} \le c_1\cdot|y|^{-n} \le \frac{1}{4}Y_1^{n-2}\cdot|y|^{-n} < \frac{1}{4y^2},$$

pa tvrdnja slijedi iz Legendreova teorema. □

Promotrimo sada vezu između tri različita elementa $\beta_i = x-\vartheta_i y$, $\beta_j = x-\vartheta_j y$, $\beta_k = x-\vartheta_k y$. Eliminirajući x i y iz ove tri jednadžbe, dobivamo *Siegelov identitet*

$$\beta_i(\vartheta_j-\vartheta_k)+\beta_j(\vartheta_k-\vartheta_i)+\beta_k(\vartheta_i-\vartheta_j)=0.$$

Za β_i ćemo uzeti β_{i_0}, dok ćemo ϑ_j i ϑ_k uzeti da budu realni (ako je $s\ge 3$), odnosno da je $\vartheta_k=\overline{\vartheta_j}$ (ako je $s=1$). Detalje ćemo dati samo za prvi, realni, slučaj. Siegelov identitet možemo pisati i u obliku

$$\frac{\vartheta_{i_0}-\vartheta_j}{\vartheta_{i_0}-\vartheta_k}\cdot\frac{\beta_k}{\beta_j}-1 = -\frac{\vartheta_k-\vartheta_j}{\vartheta_k-\vartheta_{i_0}}\cdot\frac{\beta_{i_0}}{\beta_j}. \tag{4.15}$$

Identitet (4.15) će nam dati vezu s linearnim formama u logaritmima. Definirajmo:

$$\Lambda = \ln\left(\frac{\vartheta_{i_0}-\vartheta_j}{\vartheta_{i_0}-\vartheta_k}\cdot\frac{\beta_k}{\beta_j}\right).$$

Nije teško vidjeti da je izraz pod logaritmom pozitivan.

Lema 4.3. *Neka je*

$$c_3 = \max\left\{\left|\frac{\vartheta_{i_1}-\vartheta_{i_2}}{\vartheta_{i_1}-\vartheta_{i_3}}\right| : i_1\ne i_2\ne i_3\ne i_1\right\},$$
$$Y_2 = \max\left\{Y_1, \left(\frac{2c_1c_3}{c_2}\right)^{\frac{1}{n}}\right\}.$$

Ako je $|y|>Y_2$, onda vrijedi

$$|\Lambda| < \frac{1.39c_1c_3}{c_2}|y|^{-n}.$$

Dokaz: Lijeva strana od (4.15) je jednaka $e^\Lambda-1$. Iz definicije od c_3 te nejednakosti (4.13) i (4.14), imamo

$$e^\Lambda-1 < c_3\cdot\frac{c_1|y|^{-(n-1)}}{c_2|y|} = \frac{c_1c_3}{c_2}|y|^{-n} < \frac{1}{2}.$$

Stoga je

$$|\Lambda| \le 2\ln 2\cdot|e^\Lambda-1| \le \frac{1.39c_1c_3}{c_2}|y|^{-n}.$$ □

Podsjetimo se da je $\beta_i = \mu_i(\varepsilon_1^{(i)})^{a_1}\cdots(\varepsilon_r^{(i)})^{a_r}$. Stoga (4.15) postaje

$$\frac{\vartheta_{i_0}-\vartheta_j}{\vartheta_{i_0}-\vartheta_k}\cdot\frac{\mu_k}{\mu_j}\cdot\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right)^{a_i}-1 = -\frac{\vartheta_k-\vartheta_j}{\vartheta_k-\vartheta_{i_0}}\cdot\frac{\mu_{i_0}}{\mu_j}\cdot\prod_{i=1}^{r}\left(\frac{\varepsilon_i^{(i_0)}}{\varepsilon_i^{(j)}}\right)^{a_i}.$$

U realnom slučaju naša linearna forma Λ je

$$\ln\left|\frac{\vartheta_{i_0}-\vartheta_j}{\vartheta_{i_0}-\vartheta_k}\cdot\frac{\mu_k}{\mu_j}\right|+\sum_{i=1}^{r}a_i\cdot\ln\left|\frac{\varepsilon_i^{(k)}}{\varepsilon_i^{(j)}}\right|.$$

Neka je $A=\max\{|a_i|\,:\,i=1,\dots,r\}$. Želimo dobiti gornju ogradu za A. Uspijemo li naći relativno malu ogradu za A, onda ćemo moći ispitati sve mogućnosti za $\mu\cdot\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$, provjeriti koja od njih ima oblik $x-\vartheta y$ te konačno provjeriti je li $F(x,y)=m$.

Najprije ćemo prikazati kako se dobije gornja ograda za A u ovisnosti o y. Za $I=\{i_1,\dots,i_r\}\subset\{1,\dots,s+t\}$, definiramo matricu $U_I=(\ln|\varepsilon_i^{(i_l)}|)_{1\le l,i\le r}$. Primijetimo da iz $\beta=\mu\cdot\varepsilon_1^{a_1}\cdots\varepsilon_r^{a_r}$, slijedi

$$U_I\begin{bmatrix}a_1\\ \vdots\\ a_r\end{bmatrix}=\begin{bmatrix}\ln\left|\frac{\beta^{(i_1)}}{\mu^{(i_1)}}\right|\\ \vdots\\ \ln\left|\frac{\beta^{(i_r)}}{\mu^{(i_r)}}\right|\end{bmatrix}.$$

Analizirajući ovu relaciju, može se dobiti sljedeća nejednakost

$$A<c_5\ln(c_4|y|). \tag{4.16}$$

Konstante c_4 i c_5 su definirane na sljedeći način:

$$\begin{aligned}
U_I^{-1} &= [u_{il}],\\
N(U_I^{-1}) &= \max\{\sum_{l=1}^{r}|u_{il}|\,:\,i=1,\dots,r\},\\
\mu_- &= \min\{|\mu_i|\,:\,\mu\in M,\ i=1,\dots,n\},\\
\mu_+ &= \max\{|\mu_i|\,:\,\mu\in M,\ i=1,\dots,n\},\\
c_4 &= \frac{\frac{1}{2}+\max\{|\vartheta_{i_1}-\vartheta_{i_2}|\,:\,1\le i_1<i_2\le n\}}{\mu_-},\\
c_5 &= \min\{(n-1)\cdot\min_I N(U_I^{-1}),\max_I N(U_I^{-1})\}.
\end{aligned}$$

Tada se može pokazati da (4.16) vrijedi čim je $|y|>\max\{Y_1,2|m|^{\frac{1}{n}},\frac{\mu_+}{c_2}\}$.

Kombinirajući Lemu 4.3 i (4.16), dobivamo nejednakost

$$|\Lambda|<c_6\cdot e^{-\frac{n}{c_5}A}, \tag{4.17}$$

gdje je $c_6=\frac{1.39c_1c_3c_4^n}{c_2}$. S druge strane, iz Bakerove teorije linearnih formi u logaritmima algebarski brojeva (primjerice Baker-Wüstholzovog teorema primijenjenog na formu Λ), dobivamo nejednakost oblika

$$|\Lambda|>e^{-c_7(\ln A+c_8)}. \tag{4.18}$$

Usporedbom nejednakosti (4.17) i (4.18), dobivamo (vrlo veliku) gornju ogradu za A. Zatim tu veliku ogradu smanjujemo primjenom LLL-redukcije na nejednakost (4.17).

Spomenimo da su 1996. Bilu i Hanrot predložili algoritam za rješavanje Thueovih jednadžbi koji omogućava u razumnom vremenu rješavanje Thueovih jednadžbi dosta velikog stupnja (ako su dostupni svi nužni podatci o pripadnom polju algebarski brojeva). Kao ilustraciju svog algoritma, riješili su neke Thueove jednadžbe stupnja 19 i 33. Algoritam je implementiran u PARI-ju preko funkcije `thue`. Za riješiti jednadžbu $F(x,y)=m$, najprije se inicijalizira polinom $f(x)=F(x,1)$ s `tnf = thueinit(f)`, a potom pozove funkcija `thue(tnf,m)`.

4.5 Primjena eliptičkih logaritama

Prethodno opisane metode za nalaženje cjelobrojnih točaka na eliptičkim krivuljama nisu koristile Mordell-Weilovu grupu. Pokazat ćemo sada kako se poznavanje ranga i Mordell-Weilove grupe može iskoristiti za nalaženje cjelobrojnih točaka na eliptičkoj krivulji.

Kao što smo već bili rekli, u slučaju kada je rang jednak 0 (i mi to uspijemo dokazati), pomoću Lutz-Nagellovog teorema mogu se naći sve racionalne, pa onda i sve cjelobrojne točke na toj eliptičkoj krivulji.

U općem slučaju se primjenom tzv. eliptičkih logaritama može se dobiti ocjena $N \leq N_0$ za $N=\max\{|n_1|,\ldots,|n_r|\}$ u prikazu cjelobrojne točke u obliku $P=n_1P_1+\cdots+n_rP_r+T$. Potom se ova ograda, može značajno smanjiti pomoću LLL-algoritma. Ovu metodu su predložili 1994. godine Gebel, Pethő i Zimmer, te Stroeker i Tzanakis. No, za ovu metodu je nužno poznavati i rang i generatore $P_1,\ldots,P_r$, što može biti vrlo težak problem.

Promotrimo eliptičku krivulju zadanu Weierstrassovom jednadžbom s cjelobrojnim koeficijentima

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

Ona je izomorfna krivulji s jednadžbom

$$E'\ :\ Y^2=4X^3-g_2X-g_3,$$

što je upravo jednadžba koju zadovoljavaju Weierstrassova $\wp$-funkcija i njezina derivacija. Rekli smo već da je funkcija $\wp$ dvostruko periodična. Možemo pretpostaviti da njezini periodi zadovoljavaju $\omega_1\in\mathbb{R}$ i $\Im(\omega_1/\omega_2)>0$. Neka je L rešetka koja odgovara ω_1 i ω_2. Imamo izomorfizam $\phi:\mathbb{C}/L\to E$, dan sa

$$z\mapsto\begin{cases}(\wp(z)-\frac{b_2}{12},(\wp'(z)-a_1x-a_3)/2), & z\notin L,\\ \mathcal{O}, & z\in L,\end{cases}$$

gdje je $b_2=a_1^2+4a_2$. Inverzno preslikavanje ψ se zove *eliptički logaritam*. Može se izračunati kao

$$\psi(P)=\int_\infty^{x+b_2/12}\frac{dt}{\sqrt{4t^3-g_2t-g_3}}\ (\mathrm{mod}\,L) \tag{4.19}$$

(koristeći aritmetičko-geometrijsku sredinu). Spominjanje logaritama u nazivu opravdano je sljedećim svojstvom

$$\psi(P+Q)=\psi(P)+\psi(Q)\ (\mathrm{mod}\,L).$$

Neka je P cjelobrojna točka na krivulji E. Točku P možemo zapisati u obliku $P=n_1P_1+\cdots+n_rP_r+T$, gdje je $T\in E(\mathbb{Q})_{\text{tors}}$, a $\{P_1,\ldots,P_r\}$ je Mordell-Weilova

baza od $E(\mathbb{Q})$. Željeli bismo naći gornju ogradu za broj $N = \max\{|n_1|, \ldots, |n_r|\}$, jer bismo imali konačno mnogo linearnih kombinacija za ispitati, te bi (u principu) mogli naći sve cjelobrojne točke.

Cjelobrojne točke na neparnoj (kompaktnoj) komponenti $E^{gg}(\mathbb{Q})$ je lako naći, pa ćemo u daljnjem pretpostaviti da je $P \in E^0(\mathbb{Q})$. Željeli bismo i elemente Mordell-Weilove baze prebaciti u parnu komponentu. U tu svrhu definiramo: $m_i = 1$ ako je $P_i \in E^0(\mathbb{Q})$, a $m_i = 2$ inače. Tada za sve $i = 1, \ldots, r$ imamo da je $Q_i = m_i P_i \in E^0(\mathbb{Q})$. Nadalje, definiramo brojeve q_i, r_i sa:

$$n_i = m_i q_i + r_i, \quad 0 \leq r_i < m_i.$$

Ako sada stavimo $U = r_1 P_1 + \cdots r_r P_r$, tada cjelobrojnu točku P možemo prikazati u obliku

$$P = q_1 Q_1 + \cdots + q_r Q_r + T + U.$$

Budući da je $P \in E^0(\mathbb{Q})$ i $Q_i \in E^0(\mathbb{Q})$, to mora biti i $T + U \in E^0(\mathbb{Q})$. Uvodimo oznaku $Q_{r+1} = T + U$. Za Q_{r+1} imamo samo konačno mnogo mogućnosti, koje možemo efektivno odrediti (ako znamo torzijsku grupu i Mordell-Weilovu bazu). Stavimo $H = \max\{|q_i| \, : \, i = 1, \ldots r\}$. Jasno je da je $H \leq N$. Ako uspijemo naći gornju ogradu za H, to ćemo biti dovoljno za rješenje našeg problema.

Polazište nam je ocjena iz sljedeće leme. Ovdje i do kraja ovog potpoglavlja, konstante $c_1, c_2, \ldots$ ovise samo o E i njezinoj Mordell-Weilovoj bazi.

Lema 4.4. *Za svaku cjelobrojnu točku P, uz gornje oznake vrijedi*

$$\frac{1}{x(P)} \leq c_1 e^{-c_2 H^2}. \tag{4.20}$$

Dokaz: Budući da točka P ima cjelobrojne koordinate, to je $h(P) = \log|x(P)|$. Prema Propoziciji 2.7, postoji konstanta c_3 takva da je $h(P) \geq \hat{h}(P) - c_3$, pa je $\log|x(P)| \geq \hat{h}(P) - c_3$. Neka je $R = (< P_i, P_j >)$ regulator od E. Tada je $\hat{h}(P) = nRn^\tau$, gdje je $n = (n_1, \ldots, n_m)$. Matrica R je simetrična, pa se može prikazati u obliku ODO^τ, gdje je O ortogonalna matrica, a D dijagonalna matrica koja se sastoji od (realnih, pozitivnih) svojstvenih vrijednosti od R. Stavimo $c_2 = \min\{D_{i,i} \, : \, i = 1, \ldots r\}$, te $m = nO$. Tada je

$$\begin{aligned}
\hat{h}(P) &= nRn^\tau = mDm^\tau = \sum_{i=1}^{r} D_{i,i} m_i^2 \\
&\geq c_2 \sum_{i=1}^{r} m_i^2 = c_2 m m^\tau = c_2 n O O^\tau n^\tau = c_2 n n^\tau \\
&= c_2 \sum_{i=1}^{r} n_i^2 \geq c_2 N^2.
\end{aligned}$$

Stavimo li da je $c_1 = e^{c_3}$, te uvažimo da je $N \geq H$, dobivamo nejednakost (4.20). ♢

S druge strane, ispitivanjem integrala koji se pojavljuje u (4.19), može se dobiti da nejednakost

$$|\psi(P)|^2 \leq \frac{c_5}{|x(P)|} \tag{4.21}$$

vrijedi da sve točke $P \in E^0(\mathbb{Q})$ i $|x(P) + b_2/12| > c_4$. Ovdje se može uzeti da je $c_4 = 2\max\{|e_1|, |e_2|, |e_3|\}$, gdje su e_i nultočke polinoma $f(X) = 4X^3 - g_2X - g_3$, te da je $c_5 = 8 + \frac{|\omega_1^2 b_2|}{12}$.

Kombiniranjem nejednakosti (4.20) i (4.21) dobivamo da za sve cjelobrojne točke $P \in E^0(\mathbb{Q})$ za koje je $|x(P) + b_2/12| > c_4$ vrijedi

$$|\psi(P)| \leq \sqrt{c_5 c_1} e^{-c_2 H^2/2} = c_6 e^{-c_7 H^2}. \tag{4.22}$$

Imamo

$$\psi(P) = q_1\psi(Q_1) + \cdots + q_r\psi(Q_r) + \psi(Q_{r+1}) + m\omega_1,$$

gdje je $|m| \leq rN + 2$.

Sada možemo iskoristiti duboki rezultat Davida iz 1995. godine (može se shvatiti kao analogon Bakerovih rezultata o linearnim formama u logaritmima algebarskih brojeva), koji nam daje nejednakost oblika:

$$|\psi(P)| > e^{-c_8(\log H + c_9)(\log\log H + c_{10})^{r+2}}. \tag{4.23}$$

Usporedbom (4.22) i (4.23) dobivamo da je $H \leq H_0$, gdje je H_0 (vrlo velika) konstanta (obično nešto kao 10^{100}). Međutim, korištenjem LLL-redukcije, ova ogromna gornja ograda može se značajno smanjiti. Tako se dobije nova ograda $H \leq H_1$, gdje je H_1 obično oko 10 (H_1 je reda veličine $\sqrt{\log H_0}$). Stoga, ukoliko rang r nije prevelik (recimo ako je $r \leq 8$), onda možemo testirati svih $(2H_1 + 1)^r$ kandidata i naći sve cjelobrojne točke na polaznoj eliptičkoj krivulji E.

Primjer 4.3. *Odredimo sve cjelobrojne točke na eliptičkoj krivulji*

$$E : \ y^2 + y = x^3 - 7x + 6.$$

Rješenje: Pomoću programa `mwrank` (u kojem je implementiran opći 2-spust koji je primjenjiv za krivulje koje nemaju točaka reda 2), dobivamo da je rang od $E(\mathbb{Q})$ jednak 3, te da je jedna Mordell-Weilova baza od E dana sa $Q_1 = (1, 0)$, $Q_2 = (2, 0)$, $Q_3 = (0, 2)$. Supstitucijom $Y = 2y + 1$, $X = x$, dobivamo jednadžbu

$$Y^2 = 4X^3 - 28X + 25 = f(X).$$

Nultočke polinoma $f(X)$ su $e_1 = -3.0124$, $e_2 = 1.0658$, $e_3 = 1.9466$. Dakle, cjelobrojne točke na $E^{gg}(\mathbb{Q})$ zadovoljavaju $-3 \leq x(P) \leq 1$, i lako je vidjeti da su sve takve točke $(-3, 0)$, $(-2, 3)$, $(-1, 3)$, $(0, 2)$, $(1, 0)$ (i njihove negativne točke).

Vidimo da su točke Q_1 i Q_3 iz $E^{gg}(\mathbb{Q})$. Slijedeći knjigu Cohen: *Number Theory. Volume I: Tools and Diophantine Equations*, Poglavlje 8.7.4, zamijenit ćemo ih s točkama $Q_1' = -Q_1 - Q_2 - Q_3 = (4, 6)$, $Q_3' = -2Q_2 - 2Q_3 = (\frac{114}{49}, \frac{-720}{343})$ iz $E^0(\mathbb{Q})$. Dakle, točke P tražimo u obliku $P = q_1Q_1' + q_2Q_2 + q_3Q_3' + U$. Budući da E ima trivijalnu torzijsku grupu, to je $U = \mathcal{O}$ ili $-Q_2 - Q_3$, pa budući da tražimo točke iz $E^0(\mathbb{Q})$ imamo da je u stvari $U = \mathcal{O}$. Primjenom gore opisane metode, dobije se ograda $H \leq H_0 = 10^{60}$.

Sada se ova vrlo velika gornja ograda može značajno smanjiti primjenom LLL-redukcije.

Prikazati ćemo de Wegerov algoritam (1988) koji se može primijeniti i u mnogim drugim sličnim situacijama. Promotrimo nejednadžbu oblika

$$|\alpha_0 + x_1\alpha_1 + \cdots x_n\alpha_n| < C_2 e^{-C_3 X^q}, \tag{4.24}$$

gdje su α_i dani realni ili kompleksni brojevi, C_2 i C_3 pozitivne realne konstante, $q \in \mathbb{N}$, te $X = \max\{|x_1|, \ldots, |x_n|\}$. Rješenja tražimo u cijelim brojevima $x_1, \ldots, x_n$. Pretpostavimo da je poznato da je $X \leq X_0$, gdje je X_0 neka (velika) konstanta. Želimo dobiti novu gornju ogradu oblika $X^q \leq c \ln X_0$. Razmotrit ćemo slučaj kada su svi α_i realni.

Odaberimo konstantu $C \approx X_0^n$. Linearnoj formi $\alpha_0 + \sum_{i=1}^n x_i\alpha_i$ pridružimo rešetku L generiranu stupcima matrice

$$A = \begin{bmatrix} 1 & \cdots & 0 & 0 \\ \vdots & \ddots & 0 & 0 \\ 0 & \cdots & 1 & 0 \\ [C\alpha_1] & \cdots & [C\alpha_{n-1}] & [C\alpha_n] \end{bmatrix}.$$

Ovdje $[\alpha]$ označava najbliži cijeli broj realnom broju α. Konstantu C smo izabrali da bude približno jednaka X_0^n, jer tada iz svojstava LLL-reducirane baze možemo očekivati da će najmanji vektor LLL-reducirane baze imati normu približno X_0. Koristeći LLL-algoritam možemo naći donju ogradu C_4 za veličinu

$$l(L, y) = \begin{cases} \min\{\|x - y\| \,:\, x \in L\}, & y \notin L \\ \min\{\|x\| \,:\, x \in L,\ x \neq 0\}, & y \in L, \end{cases}$$

gdje je $y = [0, \ldots, 0, -[C\alpha_0]]^\tau$.

Lema 4.5. *Neka je $S = (n-1)X_0^2$ i $T = \frac{1+nX_0}{2}$. Ako je $C_4^2 \geq T^2 + S$, onda vrijedi*

$$X^q \leq \frac{1}{C_3}\left(\ln(CC_2) - \ln(\sqrt{C_4^2 - S} - T)\right),$$

ili je $x_1 = \cdots = x_{n-1}$, $x_n = -\frac{[C\alpha_0]}{[C\alpha_n]}$.

Dokaz: Neka je $\varphi = [C\alpha_0] + \sum_{i=1}^n x_i[C\alpha_i]$. Tada je

$$|\varphi - C(\alpha_0 + \sum_{i=1}^n x_i\alpha_i)| \leq \frac{1}{2} + \sum_{i=1}^n \frac{X_0}{2} = T.$$

Stoga je $|\varphi| \leq T + C \cdot C_2 e^{-C_3 X^q}$. Neka je $x = [x_1, \ldots, x_n]^\tau$, te $z = Ax$. Tada je $z - y = [x_1, \ldots, x_{n-1}, \varphi]^\tau$. Budući da je $z \in L$, imamo da je ili $z = y$ (pa je $x_1 = \cdots = x_{n-1} = 0$ i $x_n = -\frac{[C\alpha_0]}{[C\alpha_n]}$) ili

$$C_4^2 \leq l(L, y)^2 \leq \sum_{i=1}^{n-1} x_i^2 + \varphi^2 \leq S + \left(T + CC_2 e^{-C_3 X^q}\right)^2.$$

Po pretpostavci je $C_4^2 \geq S$, pa dobivamo

$$e^{-C_3 X^q} \geq \frac{1}{CC_2}(\sqrt{C_4^2 - S} - T). \tag{4.25}$$

Koristeći pretpostavku da je $C_4^2 \geq T^2 + S$, iz (4.25) logaritmiranjem dobivamo

$$X^q \leq \frac{1}{C_3}\left(\ln(CC_2) - \ln(\sqrt{C_4^2 - S} - T)\right).$$

□

Vratimo se na naš primjer. Nejednakost (4.24) ima oblik

$$|m\omega_1 + q_1\psi(Q_1') + q_2\psi(Q_2) + q_3\psi(Q_3')| \leq 58.21e^{-0.1614H^2}$$

(dobivena je uz uvjet $|x(P)| \geq 7$). Izaberimo $C = 10^{250}$, te primjenimo postupak iz Leme 4.5. Dobivamo novu, bitno manju, gornju ogradu $H \leq 51$. Postupak se može nastaviti, te ova ograda još dodatno smanjiti. Uzmemo li $C = 10^9$, dobivamo da je $H \leq H_1 = 11$.

Sada nam preostaje naći sve cjelobrojne točke na $E^0(\mathbb{Q})$ koje zadovoljavaju $|x(P)| \leq 6$, a to su

$$(-3,0),\ (-2,3),\ (-1,3),\ (0,2),\ (1,0),\ (2,0),\ (3,3),\ (4,6),$$

(i njima suprotne $-(x,y) = (x,-y-1)$), te sve cjelobrojne točke oblika $q_1Q_1' + q_2Q_2 + q_3Q_3'$, $|q_i| \leq 11$ (ukupno $23^3 = 12167$ mogućnosti), a to su (osim onih već navedenih)

$$(8,21) = Q_1' - Q_2' + Q_3',\ \ (11,35) = Q_1' + 2Q_2',\ \ (14,51) = -2Q_1' - Q_3',$$
$$(21,95) = -2Q_2',\ \ (37,224) = Q_2' - Q_3',\ \ (52,374) = Q_1' + Q_2' + Q_3',$$
$$(93,896) = -2Q_1' - Q_2,\ \ (342,6324) = -3Q_2' + Q_3,$$
$$(406,8180) = -2Q_1' + 2Q_2' - Q_3',\ \ (816,23309) = 3Q_1' + 2Q_2' + Q_3'$$

(i njima suprotne). ♢

Opisana metoda koja koristi eliptičke logaritme za nalaženje cjelobrojnih točaka na eliptičkoj krivulji implimentirana je u programskim paketima SageMath (funkcija `integral_points`) i Magma (funkcija `IntegralPoints`). Spomenimo da u Magmi postoji i funkcija `IntegralQuarticPoints` koja računa cjelobrojne točke na krivulji oblika $y^2 = ax^4 + bx^3 + cx^2 + dx + e$.