Eliptičke krivulje velikog ranga sa zadanom torzijskom grupom

Andrej Dujella

Prirodoslovno-matematički fakultet, Matematički odsjek
Sveučilište u Zagrebu
e-mail: duje@math.hr
URL: https://web.math.pmf.unizg.hr/~duje/

Zajednički rad s **Juanom Carlosom Peralom** i **Matijom Kazalickim**

Eliptičke krivulje

Neka je $\mathbb{K}$ polje. *Eliptička krivulja* nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom $\mathbb{K}$-racionalnom točkom. Svaka takva krivulja može se biracionalnim transformacijama transformirati u jednadžbu oblika

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

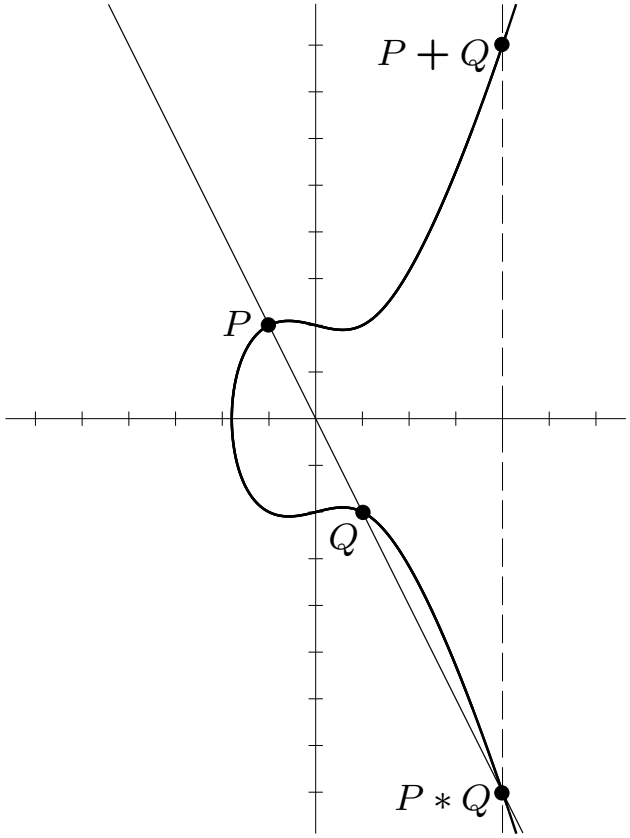
koja se naziva *Weierstrassova forma*.

Ako je $\mathrm{char}(\mathbb{K}) \neq 2, 3$, onda se jednadžba (1) može transformirati u oblik

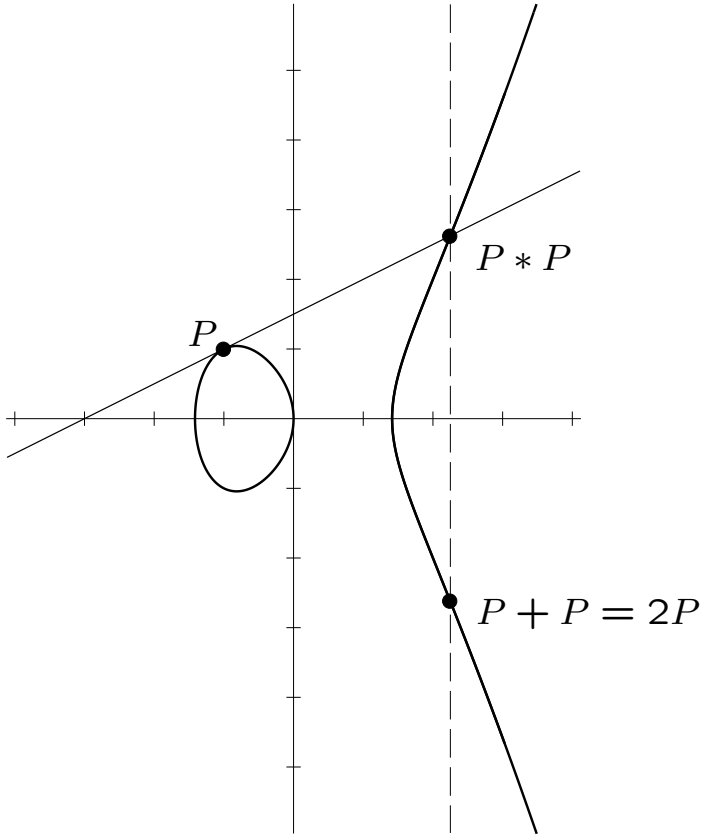
$$y^2 = x^3 + ax + b, \tag{2}$$

koji se naziva *kratka Weierstrassova forma*. Sada nesingularnost znači da kubni polinom $f(x) = x^3 + ax + b$ nema višestrukih korijena (u algebarskom zatvaraču $\overline{\mathbb{K}}$), ili ekvivalentno da je *diskriminanta* $\Delta = -4a^3 - 27b^2$ različita od nule.

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na skupu $E(\mathbb{K})$, njezinih $\mathbb{K}$-racionalnih točaka (afine točke (x, y) koje zadovoljavaju jednadžbu (1) zajedno s točkom u beskonačnosti $\mathcal{O}$), može na prirodan način uvesti operacija uz koju ona postaje Abelova grupa.



sekanta



tangenta

Torzijska grupa i rang eliptičkih krivulja nad $\mathbb{Q}$

Neka je E eliptička krivulja nad $\mathbb{Q}$.

Prema Mordell-Weilovom teoremu, grupa $E(\mathbb{Q})$ racionalnih točaka na E je konačno generirana Abelova grupa. Stoga je ona izomorfna produktu torzijske grupe i $r \geq 0$ kopija beskonačne cikličke grupe:

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

Prema Mazurovom teoremu, znamo da $E(\mathbb{Q})_{\text{tors}}$ može biti jedna od sljedećih 15 grupa:

$\mathbb{Z}/n\mathbb{Z}$ za $1 \leq n \leq 10$ ili $n = 12$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ za $1 \leq m \leq 4$.

Nije poznato koje vrijednosti ranga r su moguće. Dugo vremena je bila široko prihvaćena slutnja da postoje eliptičke krivulje proizvoljno velikog ranga.

Nedavni heuristički argumenti sugeriraju za bi rang mogao biti ograničen. Jedna od tih heuristika predviđa da postoji samo konačno mnogo eliptičkih krivulja nad $\mathbb{Q}$ s rangom većim od 21.

Trenutni rekord predstavlja krivulja ranga ≥ 29, koju su pronašli Noam Elkies i Zev Klagsbrun krajem kolovoza 2024.

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
29	2024	Elkies & Klagsbrun

Andrej Dujella
@dujella1

New record for the rank of elliptic curves over Q, due to Noam Elkies and Zev Klagsbrun, is 29!
web.math.pmf.unizg.hr/~duje/tors/rk2...

20	1993	Nagao
21	1994	Nagao - Kouya
22	1997	Fermigier
23	1998	Martin - McMillen
24	2000	Martin - McMillen
28	2006	Elkies
29	2024	Elkies - Klagsbrun

11:39 PM · Aug 29, 2024 **100K** Views

View post engagements

11 98 266 62

Now, two mathematicians — Noam Elkies of Harvard University and Zev Klagsbrun of the Center for Communications Research in La Jolla, California — have found an elliptic curve with the most complicated pattern of rational points to date, breaking an 18-year-old record. "It was a big question whether this barrier could be broken," said Andrej Dujella of the University of Zagreb in Croatia. "It's a very exciting result for all of us working and interested in elliptic curves."

$B(T) = \sup\{\text{rank}\,(E(\mathbb{Q})) : \text{torzijska grupa od } E \text{ nad } \mathbb{Q} \text{ je } T\}$.

Montgomery (1987): Predložio korištenje eliptičkih krivulja s velikom torzijskom grupom i pozitivnim rangom u faktorizaciji velikih prirodnih brojeva.

Montgomery, Suyama, Atkin & Morain (*Finding suitable curves for the elliptic curve method of factorization*, 1993): $B(T) \geq 1$ za sve dopustive torzijske grupe T.

Womack (2000): $B(T) \geq 2$ za sve T

D. (2003): $B(T) \geq 3$ za sve T

Konstrukcija eliptičkih krivulja velikog ranga

1. Naći parametarsku familiju krivulja nad $\mathbb{Q}$ koja sadrži krivulje s relativno velikim rangom (eliptičku krivulju nad $\mathbb{Q}(t)$ s velikim generičkim rangom) – Mestreova polinomijalna metoda ("vađenje kvadratnog korijena s ostatkom" $p(x) = q^2(x) - r(x)$), Elkiesova metoda koja koristi alate iz algebarske geometrije, eliptičke krivulje inducirane *Diofantovim trojkama*.

2. U promatranoj familiji, izabrati najbolje kandidate za što veći rang. Opća ideja: veća je šansa da će krivulja imati veliki rang ako je $|E(\mathbb{F}_p)|$ relativno veliko za većinu prostih brojeva p. Precizna formulacija: Birch i Swinnerton-Dyer slutnja – jedan od milenijskih problema.

Prikladniji za računanje: Mestreova uvjetna gornja ograda za rang (pretpostavlja BSD i GRH), Mestre-Nagaove sume, npr. suma:

$$s(N) = \sum_{p \leq N,\ p \text{ prost}} \frac{|E(\mathbb{F}_p)| + 1 - p}{|E(\mathbb{F}_p)|} \log(p)$$

(Elkies & Klagsbrun (2020) – optimizacije, Kim & Murty (2023) – preciznija veza ovih suma s BSD i Nagaovom slutnjom, Kazalicki & Vlah (2023), Bujanović, Kazalicki & Novak (2024) – korištenje dubokih konvolucijskih neuronskih mreža i usporedba različitih sličnih suma)

3. Pokušati izračunati rang (Cremonin program `mwrank`, `Magma`, `ellrank` u `PARI/GP`), ili barem dobre donje i gornje ograde za rang.

Diofantove m-torke

Diofant: Naći četiri (pozitivna racionalna) broja sa svojstvom da produkt svaka dva među njima, uvećan za 1, daje kvadrat:

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

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

$$\begin{aligned} 1\cdot 3+1 &= 2^2, & 3\cdot 8+1 &= 5^2,\\ 1\cdot 8+1 &= 3^2, & 3\cdot 120+1 &= 19^2,\\ 1\cdot 120+1 &= 11^2, & 8\cdot 120+1 &= 31^2. \end{aligned}$$

Definicija: Skup $\{a_1, a_2, \ldots, a_m\}$ od m cijelih (racionalnih) brojeva različitih od 0 naziva se *(racionalna) Diofantova m-torka* ako je $a_i \cdot a_j + 1$ potpun kvadrat za sve $1 \leq i < j \leq m$.

Pitanje: Koliko veliki mogu biti ovi skupovi?

Euler: Postoji beskonačno mnogo Diofantovih četvorki. Npr. $\{k-1, k+1, 4k, 16k^3 - 4k\}$ za $k \geq 2$.

Baker & Davenport (1969): $\{1, 3, 8, d\} \Rightarrow d = 120$

D. & Pethő (1998): $\{1, 3\}$ se ne može proširiti do Diofantove petorke.

D. (2001): Ne postoji Diofantova devetorka. Postoji najviše konačno mnogo Diofantovih osmorki.

D. (2004): Ne postoji Diofantova šestorka. Postoji najviše konačno mnogo Diofantovih petorki.

He, Togbé & Ziegler (2019): Ne postoji Diofantova petorka.

Racionalne Diofantove m-torke

Nije poznata gornja ograda za veličinu racionalnih Diofantovih m-torki.

Euler: Postoji beskonačno racionalnih Diofantovih petorki. Svaki par $\{a, b\}$ takav da je $ab + 1 = r^2$ može se proširiti do petorke. Npr. $\{1, 3, 8, 120, \frac{777480}{8288641}\}$.

Arkin, Hoggatt & Strauss (1979): Svaka racionalna Diofantova trojka $\{a, b, c\}$ može se proširiti do petorke.

D. (1997): Svaka racionalna Diofantova četvorka $\{a, b, c, d\}$, takva da je $abcd \neq 1$, može se proširiti do petorke (na dva različita načina, osim ako je četvorka "regularna" (kao u Eulererovoj i AHS konstrukciji), u kojem slučaju je jedno proširenje trivijalno s 0).

Ako je $abcd = 1$, onda su ab, ac, ad, bc, bd, cd svi kvadrati (D., Kazalicki & Petričević (2021)), a $\{a, b, c, d\}$ se može proširiti do petorke s $e = \frac{(a+b-c-d)^2-4(ab+1)(cd+1)}{4d(ab+1)(ac+1)(bc+1)}$.

Herrmann, Pethő & Zimmer (1999): Racionalna Diofantova četvorka se može na samo konačno mnogo načina proširiti do petorke.

Stoll (2019): Ako je $\{1, 3, 8, 120, e\}$ racionalna Diofantova petorka, onda je $e = \frac{777480}{8288641}$. Fermatov primjer četvorke se ne može proširiti to racionalne Diofantove šestorke.

Pitanje: Ako su $\{a, b, c, d, e\}$ i $\{a, b, c, d, f\}$ dva proširenja iz D. (1997) te $ef \neq 0$, može li $ef + 1$ biti kvadrat?

$$e, f = \frac{(a+b+c+d)(abcd+1) + 2abc + 2abd + 2acd + 2bcd \pm 2\sqrt{D}}{(abcd-1)^2},$$

gdje je

$$D = (ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1).$$

Gibbs (1999): $\left\{\frac{5}{36}, \frac{5}{4}, \frac{32}{9}, \frac{189}{4}, \frac{665}{1521}, \frac{3213}{676}\right\}$

D., Kazalicki, Mikić & Szikszai (2017): Postoji beskonačno mnogo racionalnih Diofantovih šestorki.

Alternativne konstrukcije: **D. & Kazalicki (2017)**, **D., Kazalicki & Petričević (2019,2021,2024)**

Inducirane eliptičke krivulje

Neka je $\{a, b, c\}$ racionalna Diofantova trojka. Da bi je proširili do četvorke, promatramo sustav

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{3}$$

Ovom sustavu se na prirodan način pridružuje eliptička krivulja

$$\mathcal{E}: \qquad y^2 = (ax + 1)(bx + 1)(cx + 1). \tag{4}$$

Kažemo da je $\mathcal{E}$ inducirana trojkom $\{a, b, c\}$.

Tri racionalne točke na $\mathcal{E}$ reda 2:

$$A = [-1/a, 0]\,, \quad B = [-1/b, 0]\,, \quad C = [-1/c, 0]$$

te očite racionalne točke

$$P = [0, 1], \quad S = [1/abc, \sqrt{(ab + 1)(ac + 1)(bc + 1)}/abc].$$

x-koordinata točke $T \in \mathcal{E}(\mathbb{Q})$ zadovoljava (3) ako i samo ako je $T - P \in 2\mathcal{E}(\mathbb{Q})$.

Vrijedi da je $S \in 2\mathcal{E}(\mathbb{Q})$. Zaista, ako je $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$, onda je $S = [2]V$, gdje je

$$V = \left[\frac{rs + rt + st + 1}{abc}, \frac{(r + s)(r + t)(s + t)}{abc}\right].$$

Ovo povlači da ako $x(T)$ zadovoljava sustav (3), onda $x(T \pm S)$ također zadovoljavaju sustav.

D. (1997,2001): $x(T)x(T \pm S) + 1$ je uvijek kvadrat. Uz $x(T) = d$, brojevi $x(T \pm S)$ su točno e i f.

Propozicija 1: Neka su Q, T i $[0, \alpha]$ tri racionalne točke na eliptičkoj krivulji $\mathcal{E}$ nad $\mathbb{Q}$ danoj s jednadžbom $y^2 = f(x)$, gdje je f normirani kubni polinom. Pretpostavimo da $\mathcal{O} \notin \{Q, T, T+Q\}$. Tada je

$$x(Q)x(T)x(T+Q) + \alpha^2$$

potpun kvadrat.

Supstitucijama $x \mapsto x/abc$, $y \mapsto y/abc$, iz $\mathcal{E}$ dobivamo

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

Točke P i S postaju $P' = [0, abc]$ i $S' = [1, rst]$.

Budući da je $x(S') = 1$, Propozicija 1 za $Q = \pm S'$ daje jednostavan dokaz da je $x(T)x(T \pm S)+1$ kvadrat (nakon dijeljenja $x(T')x(T' \pm S') + a^2b^2c^2 = \square$ s $a^2b^2c^2$).

Sada imamo opću konstrukciju koja daje dvije racionalne Diofantove petorke s četiri zajednička elementa. Stoga je unija te dvije petorke,

$$\{a, b, c, x(T - S), x(T), x(T + S)\},$$

"skoro" racionalna Diofantova šestorka.

Ako pretpostavimo da $T, T \pm S \notin \{\mathcal{O}, \pm P\}$, onda je jedini uvjet koji nedostaje

$$x(T - S) \cdot x(T + S) + 1 = \square.$$

Za konstrukciju primjera koji zadovoljavaju ovaj zadnji uvjet, koristit čemo Propoziciju 1 za $Q = [2]S'$. Da bi dobili željeni zaključak, morao bi biti zadovoljen uvjet da je $x([2]S') = 1$. Ovo vodi do $[2]S' = -S'$, tj. $[3]S' = \mathcal{O}$. U tom slučaju, krivulja $\mathcal{E}$ imat će torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Lema 1: Za točku $S' = [1, rst]$ na E' vrijedi $[3]S' = \mathcal{O}$ ako i samo ako

$$3 + 4(ab + ac + bc) + 6abc(a + b + c) + 12(abc)^2 - (abc)^2(a^2 + b^2 + c^2 - 2ab - 2ac - 2bc) = 0 \quad (5)$$

Ako zapišemo uvjet (5) pomoću elementarnih simetričnih polinoma, možemo dobiti familiju racionalnih Diofantovih trojki koje zadovoljavaju uvjet iz Leme 1:

$$a = \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)},$$
$$b = \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)},$$
$$c = \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}.$$

Promotrimo sada eliptičku krivulju nad $\mathbb{Q}(t)$ induciranu trojkom $\{a, b, c\}$. Ona ima pozitivan rang budući da sadrži točku $P = [0, 1]$ beskonačnog reda. Ova konstrukcija daje beskonačno mnogo racionalnih Diofantovih šestorki koje sadrže trojku $\{a, b, c\}$. Jedna takva šestorka $\{a, b, c, d, e, f\}$ se dobije tako da se uzmu x-koordinate točaka $[3]P$, $[3]P + S$, $[3]P - S$.

Dobivamo: $d = d_1/d_2$, $e = e_1/e_2$, $f = f_1/f_2$, gdje je

$$
\begin{aligned}
d_1 &= 6(t+1)(t-1)(t^2+6t+1)(t^2-6t+1)\\
&\quad\times(8t^6+27t^5+24t^4-54t^3+24t^2+27t+8)\\
&\quad\times(8t^6-27t^5+24t^4+54t^3+24t^2-27t+8)\\
&\quad\times(t^8+22t^6-174t^4+22t^2+1),\\
d_2 &= t(37t^{12}-885t^{10}+9735t^8-13678t^6+9735t^4-885t^2+37)^2,\\
e_1 &= -2t(4t^6-111t^4+18t^2+25)\\
&\quad\times(3t^7+14t^6-42t^5+30t^4+51t^3+18t^2-12t+2)\\
&\quad\times(3t^7-14t^6-42t^5-30t^4+51t^3-18t^2-12t-2)\\
&\quad\times(t^2+3t-2)(t^2-3t-2)(2t^2+3t-1)\\
&\quad\times(2t^2-3t-1)(t^2+7)(7t^2+1),\\
e_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)\\
&\quad\times(16t^{14}+141t^{12}-1500t^{10}+7586t^8-2724t^6+165t^4+424t^2-12)^2,\\
f_1 &= 2t(25t^6+18t^4-111t^2+4)\\
&\quad\times(2t^7-12t^6+18t^5+51t^4+30t^3-42t^2+14t+3)\\
&\quad\times(2t^7+12t^6+18t^5-51t^4+30t^3+42t^2+14t-3)\\
&\quad\times(2t^2+3t-1)(2t^2-3t-1)(t^2-3t-2)\\
&\quad\times(t^2+3t-2)(t^2+7)(7t^2+1),\\
f_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)\\
&\quad\times(12t^{14}-424t^{12}-165t^{10}+2724t^8-7586t^6+1500t^4-141t^2-16)^2.
\end{aligned}
$$

Krivulje velikog ranga sa zadanom torzijskom grupom

Neka je $\{a, b, c\}$ (racionalna) Diofantova trojka i E eliptička krivulja inducirana tom trojkom.

Prema Mazurovom teoremu: $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, $m = 1, 2, 3, 4$.

D. & Mikić (2014): Ako su a, b, c prirodni brojevi, onda slučajevi $m = 2$ i $m = 4$ nisu mogući.

Parametarske formule za racionalne Diofantove šestorke $\{a, b, c, d, e, f\}$ mogu se iskoristiti za dobivanje eliptičkih krivulja nad $\mathbb{Q}(t)$ relativno velikog ranga. Promotrimo krivulju

$$E: \quad y^2 = (dx + 1)(ex + 1)(fx + 1).$$

Ona ima tri očite racionalne točke reda 2, ali također i racionalne točke s x-koordinatama

$$0,\ 1/def,\ a,\ b,\ c.$$

Može se provjeriti da su ovih pet točaka nezavisne točke beskonačnog reda na krivulji E nad $\mathbb{Q}(t)$. Dakle, rang od E nad $\mathbb{Q}(t)$ je ≥ 5 (torzijska grupa je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

Aguirre, D. & Peral (2012), D. & Peral (2020): Krivulje s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i rangom 6 nad $\mathbb{Q}(t)$ te rangom 12 nad $\mathbb{Q}$.

Za racionalne Diofantove trojke $\{a, b, c\}$ koje zadovoljavaju uvjet (5), inducirana eliptička kruvulja ima torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, budući da sadrži točku S reda 3. Prije navedena familija trojki s ovim svojstvom daje krivulju nad $\mathbb{Q}(t)$ ranga 1.

Unutar ove familije moguće se naći podfamilije ranga 2 te pojedinačne primjere krivulja ranga 6 nad $\mathbb{Q}$, što oboje izjednačuje trenutne rekorde za rangove krivulja s torzijskog grupom $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}}$ (**D. & Peral (2019)**).

$$\left\{\frac{7567037280}{7833785281}, \frac{4161669360289}{569762123040}, \frac{1359453258559}{948852707040}\right\}$$

Eliptičke krivulje s torzijskom grupom $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$ imaju jednadžbu oblika

$$y^2 = x(x + x_1^2)(x + x_2^2), \quad x_1, x_2 \in \mathbb{Q}.$$

Točka $[x_1x_2, x_1x_2(x_1+x_2)]$ je racionalna točka na krivulji reda 4.

Eliptička krivulja inducirana trojkom $\{a, b, c\}$ može se zapisati u obliku

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

Uspoređujući ove dvije jednadžbe, dolazimo do uvjeta da su $ac - ab$ i $bc - ab$ kvadrati. Ova krivulja također sadrži točku $[ab, abc]$, pa možemo očekivati da će imati pozitivan rang.

Dva dobivena uvjeta mogu se zadovoljiti tako da izaberemo a i b za koje vrijedi $ab = -1$. Tada je $ac - ab = ac + 1 = s^2$ i $bc - ab = bc + 1 = t^2$. Preostaje naći a i c tako da je $\{a, -1/a, c\}$ racionalna Diofantova trojka. Parametarsko rješenje ovog problema je

$$a = \frac{\alpha\tau + 1}{\tau - \alpha}, \quad c = \frac{4\alpha\tau}{(\alpha\tau + 1)(\tau - \alpha)}.$$

Dodatne točke beskonačnog reda pojavljuju se ako su

$$\tau^2 + \alpha^2 + 2 \quad \text{ili} \quad \alpha^2\tau^2 + 2\alpha^2 + 1$$

kvadrati.

D. & Peral (2014, 2019): Krivulje s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ i rangom 4 nad $\mathbb{Q}(t)$ i rangom 9 nad $\mathbb{Q}$ (oba rezultata su još uvijek rekordi za krivulje s ovom torzijskom grupom).

Svaka eliptička krivulja nad $\mathbb{Q}$ s torzijskom grupom $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ inducirana je nekom racionalnom Diofantovom trojkom (**D. (2007), Campbell & Goins (2007)**).

D. (2007): Za svaki $0 \leq r \leq 3$, postoji racionalna Diofantova trojka $\{a, b, c\}$ takva da $y^2 = (ax+1)(bx+1)(cx+1)$ ima torzijsku grupu $\boxed{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}}$ i rang jednak r.

Connell (2000), D. (2000): $\boxed{r=3}$

$$\left\{\frac{408}{145}, -\frac{145}{408}, -\frac{145439}{59160}\right\}.$$

D., Jukić Bokun, Soldo (2017): eliptičke krivulje inducirane racionalnim Diofantovim trojkama nad kvadratnim poljima – pored torzijskih grupa koje se javljaju nad $\mathbb{Q}$, javljaju se još i grupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ i $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$

D. & Soydan (2022): eliptičke krivulje inducirane racionalnim Diofantovim četvorkama nad $\mathbb{Q}$ – javljaju se iste torzijske grupe kao kod trojki

Torzijska grupa $\mathbb{Z}/4\mathbb{Z}$

Skicirat ćemo konstrukciju eliptičke krivulje nad $\mathbb{Q}(t)$ s torzijskom grupom $\mathbb{Z}/4\mathbb{Z}$ i rangom 6 (D. & Peral (2024). Prethodno su bile poznate takve krivulje s rangom 5.

Polazi se od konstrukcije iz Elkies (2007), gdje je uočeno da se ova torzijska grupa i rang 4 može dobiti za neke $K3$ plohe. Pokazano da je u tom slučaju rang 4 maksimalan mogući, te opisano za koji tipove singularnih vlakana se maksimum postiže.

Opća krivulja s torzijskom grupom $\mathbb{Z}/4\mathbb{Z}$ ima oblik

$$Y^2 + aXY + abY = X^3 + bX^2,$$

gdje je $ab(a^2 - 16b) \neq 0$. Jedna torzijska točka reda 4 je $[0, 0]$. Zamjenom varijabli dobivamo jednadžbu

$$Y^2 = X^3 + (a^2 - 8b)X^2 + 16b^2X.$$

Elkies je pokazao da se rang 4 dobiva za sljedeće vrijednosti parametara:

$$a = (8t - 1)(32t + 7)$$
$$b = 8(t + 1)(15t - 8)(31t - 7).$$

Uvrštavanjem vrijednosti od a i b, dobivamo sljedeću $K3$ eliptičku plohu E:

$$E:\ Y^2 = X^3 + (65536t^4 - 17472t^3 - 10176t^2 + 18672t - 3535)X^2 + 1024(t+1)^2(15t-8)^2(31t-7)^2X$$

Ona ima torzijsku grupu $\mathbb{Z}/4\mathbb{Z}$ i rang 4. Jedna torzijska točka reda 4 u ovom modelu je

$$[32(t+1)(15t-8)(31t-7), 2^5(1+t)(-1+8t)(-8+15t)(-7+31t)(7+32t)]$$

dok su X-koordinate četiriju nezavisnih točaka beskonačnog reda:

$$\begin{aligned} X_1 &= -361(t+1)(31t-7), \\ X_2 &= -4(t+1)(15t-8)(16t-7)^2, \\ X_3 &= -16(t+1)(8t+7)^2(15t-8), \\ X_4 &= 4(15t-8)(16t+1)^2(31t-7). \end{aligned}$$

Da bi povećali rang, zahtijevamo da

$$\frac{-64(1+t)^2(-4+7t)(4+17t)}{(1+4t)^2}$$

bude X-koordinata nove točke na E. To daje uvjet $-(-4+7t)(4+17t) = \square$, koji se može zadovoljiti tako da se uzme

$$t \mapsto \frac{4(-1+u^2)}{(17+7u^2)}.$$

Tako se dobiva krivulja ranga 5 nad $\mathbb{Q}(u)$.

Drugi način za povećanje ranga je da zahtijevamo da

$$\frac{576(-4+7t)(-8+15t)^2(-1324+5551t)}{49(-39+28t)^2}$$

bude X-koordinata nove točke na E, što daje uvjet $(-4+7t)(-1324+5551t) = \square$, koji se može zadovoljiti tako da se uzme

$$t \mapsto \frac{4(-331+u^2)}{7(-793+u^2)}.$$

Ponovno dobivamo krivulju ranga 5 nad $\mathbb{Q}(u)$.

Uočimo sada da se u oba uvjeta

$$-(-4+7t)(4+17t) = \square,$$
$$(-4+7t)(-1324+5551t) = \square$$

pojavljuje zajednički faktor $(-4+7t)$. Stoga se ovi uvjeti mogu simultano zadovoljiti.

Naime, ako uvrstimo rješenje prvog uvjeta u drugi uvjet, dobivamo $1863 - 539u^2 = \square$, što se može zadovoljiti tako da se uzme

$$u \mapsto \frac{-7007 - 28r + 13r^2}{7(539 + r^2)}.$$

Dakle, oba uvjeta možemo istovremeno zadovoljiti tako da uzmemo

$$t \mapsto \frac{4\left(3r^2-14r-5390\right)\left(10r^2-14r-1617\right)}{7\left(72r^4-182r^3-13279r^2+98098r+20917512\right)}.$$

Uvrštavajući ovo u E, dobivamo krivulju nad $\mathbb{Q}(r)$ ranga 6 (da je rang točno jednak 6 (a ne samo ≥ 6), može se dokazati koristeći algoritam koji su razvili Ivica Gusić i Petra Tadić (2015)).

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

T	$B(T) \geq$	autori
0	29	Elkies & Klagsbrun (2024)
$\mathbb{Z}/2\mathbb{Z}$	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 (2003,2006,2013,2022), Flores, Jones, Rollick & Weigandt (2007), Fisher (2009), AttarBashi, Rathbun & Voznyy (2022), AttarBashi, Fisher, Rathbun & Voznyy (2022), AttarBashi, Fisher & Voznyy (2022)

rekordne krivulje inducirane Diofantovim trojkama

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

T	$G(T) \geq$	autori
0	18	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	Elkies (2009), Dujella & Peral (2023)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007), Eroshkin (2023)
$\mathbb{Z}/4\mathbb{Z}$	**6**	Dujella & Peral (2022)
$\mathbb{Z}/5\mathbb{Z}$	4	Eroshkin (2020)
$\mathbb{Z}/6\mathbb{Z}$	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)

rekordne krivulje inducirane Diofantovim trojkama

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

T	$C(T) \geq$	PPVW	autori
0	19	21	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	13	Elkies (2007,2009) Dujella & Peral (2023)
$\mathbb{Z}/3\mathbb{Z}$	8	9	Eroshkin (2023)
$\mathbb{Z}/4\mathbb{Z}$	**6**	7	Elkies (2007), Dujella & Peral (2021,2022)
$\mathbb{Z}/5\mathbb{Z}$	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), Voznyy (2022), Youmbai (2024)
$\mathbb{Z}/8\mathbb{Z}$	**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), Youmbai (2024)
$\mathbb{Z}/10\mathbb{Z}$	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)

poznata donja ograda se podudara s heurističkom gornjom ogradom iz članka Park, Poonen, Voight and Wood (2019)

Familija ranga 3 s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

D., Kazalicki & Peral (2021):

Krećemo s krivuljom $Y^2 = X^3 + aX^2 + bX$ ranga 2 nad $\mathbb{Q}(u)$ (dobivena je korištenjem Diofantovim trojki, D. & Peral (2015)):

$$\begin{aligned} a &= u^{16} - 60u^{15} + 1634u^{14} - 27768u^{13} + 334132u^{12} - 3017412u^{11} \\ &\quad + 20987282u^{10} - 113627424u^9 + 480725533u^8 - 1590783936u^7 \\ &\quad + 4113507272u^6 - 8279778528u^5 + 12836014912u^4 - 14934296832u^3 \\ &\quad + 12303261824u^2 - 6324810240u + 1475789056, \\ b &= -27u^3(u-4)^3(2u-7)^3(u^4 - 24u^3 + 152u^2 - 336u + 196) \\ &\quad \times (u^4 - 12u^3 + 62u^2 - 168u + 196)^3(2u^4 - 30u^3 + 169u^2 - 420u + 392). \end{aligned}$$

X-koordinate dvaju nezavisnih točaka beskonačnog reda su

$$-27u^2(u-4)^2(2u-7)^2(u^2 - 8u + 14)^2(u^4 - 24u^3 + 152u^2 - 336u + 196),$$
$$-\frac{27}{4}u^2(u-4)^2(2u-7)^2(u^2 - 7u + 14)^2(u^4 - 24u^3 + 152u^2 - 336u + 196).$$

Zahtjev da

$$\frac{27}{4}u(u-4)(2u-7)(u^2-7u+14)^2(u^4-12u^3+62u^2-168u+196)^2$$

bude X-koordinata nove točke na krivulji, vodi do uvjeta

$$4u^4-66u^3+383u^2-924u+784=t^2,$$

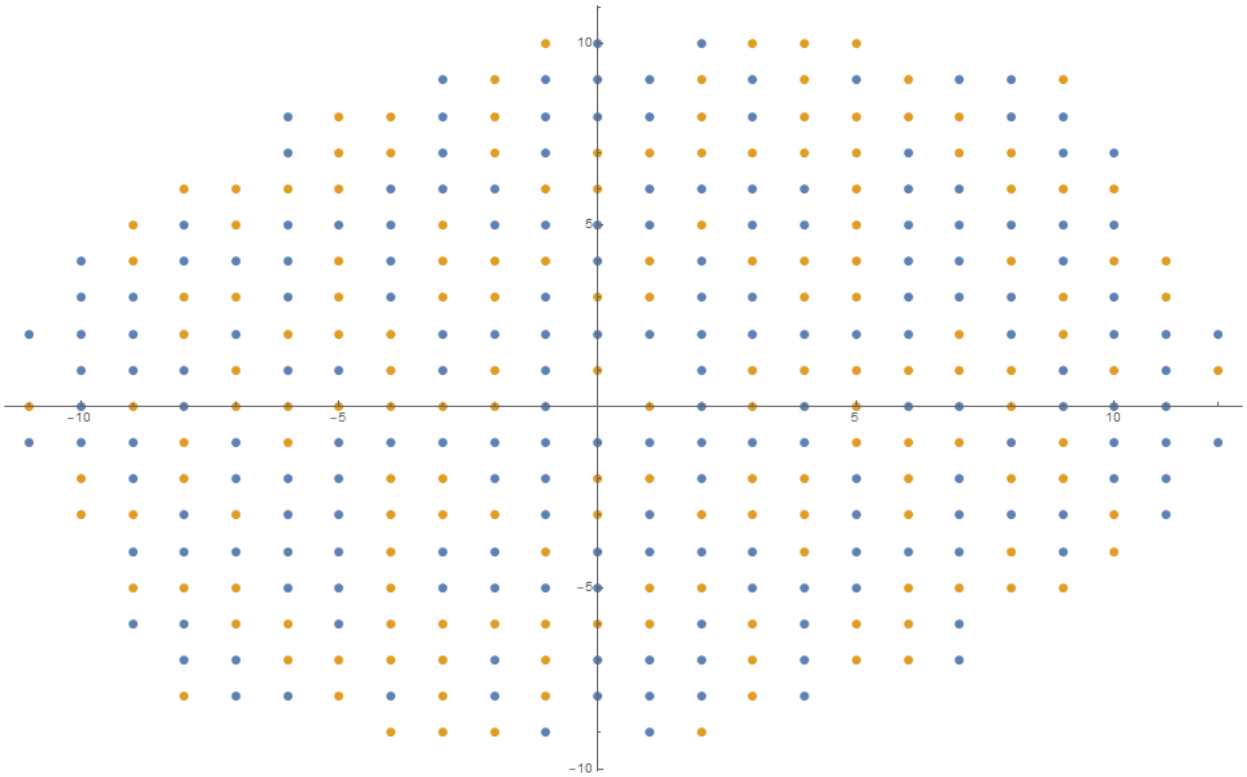
koji ima racionalno rješenje $(u,t)=(0,28)$, pa se može transformirati u eliptičku krivulju

$$y^2=x^3-x^2-456x+3456$$

ranga 2 (generatori su $R_1=[20,-44]$ i $R_2=[4/9,-1540/27]$) i torzijske grupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Za točke $nR_1 + mR_2$ za male $n, m \in \mathbb{Z}$, moguće se izračunati "root number" w_E koji predviđa parnost ranga (ako je $w_E = 1$, slutnja je da je rang paran, a ako je $w_E = -1$, slutnja je da je rang neparan). Dobivene vrijednosti su prikazane na sljedećem slajdu. Dobiveno je 194 krivulja za koje je $w_E = 1$, te 168 krivulja za koje je $w_E = -1$, što sugerira da bi parni i neparni rangovi mogli biti podjednako česti u ovoj familiji krivulja.

Ako bi to zaista bilo točno, onda bi u ovoj familiji postojalo beskonačno mnogo krivulja s rangom koji je paran i ≥ 3, pa je stoga rang ≥ 4. Ovo zapažanje sugerira da heuristika iz članka PPVW možda zahtjeva neke korekcija, barem u slučaju nekih torzijskih grupa.



Plave točke s koordinatama (n, m) reprezentiraju eliptičke krivulje koje odgovaraju točki $nR_1 + mR_2$ i koje imaju "root number" 1, a narančaste onima za koje je "root number" -1.

Hvala Vam na pozornosti!

Sretna 25. godišnjica mathosa!