Racionalne Diofantove šestorke

Andrej Dujella

http://web.math.pmf.unizg.hr/~duje/dtuples.html

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

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

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

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

Euler: $\{1, 3, 8, 120, \frac{777480}{8288641}\}$

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

Pitanje: Koliko veliki mogu biti ovi skupovi?

M. Waldschmidt, Open Diophantine problems, Conference on Hilbert's problems today, Moscow Math. J. (2004).

R. K. Guy, Unsolved Problems in Number Theory, 3rd edition, Springer, 2004, Section D29. Diophantine m-tuples.

A. Dujella, What is a Diophantine m-tuple?, Notices Amer. Math. Soc. (2016).

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

Slutnja: Ne postoji Diofantova petorka u cijelim brojevima.

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

D. (2004): Ne postoji Diofantova šestorka u cijelim brojevima, a petorki ima najviše konačno mnogo.

Elsholtz, Filipin & Fujita (2014), Cipu & Trudgian (2016): Postoji najviše $5.441 \cdot 10^{27}$ Diofantovih petorki.

Arkin, Hoggatt & Strauss (1978): Neka je $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$. Definiramo $d_{+,-}=a+b+c+2abc\pm 2rst$. Tada je $\{a,b,c,d_{+,-}\}$ Diofantova četvorka (ako je $d_-\neq 0$).

Slutnja: Ako je $\{a,b,c,d\}$ Diofantova četvorka, onda je $d=d_+$ ili $d=d_-$, tj. sve Diofantove četvoke zadovoljavaju $(a-b-c+d)^2=4(ad+1)(bc+1)$. Takve četvorke nazivaju se *regularne*.

Fujita (2009): Ako je $\{a,b,c,d,e\}$, $a<b<c<d<e$, Diofantova petorka, onda je $\{a,b,c,d\}$ regularna Diofantova četvorka.

Proširenje trojke $\{a, b, c\}$, $a < b < c$, do četvorke $\{a, b, c, d\}$:

$$ad + 1 = x^2, \quad bd + 1 = y^2, \quad cd + 1 = z^2.$$

Sustav pellovskih jednadžbi:

$$cx^2 - az^2 = c - a, \quad cy^2 - bz^2 = c - b.$$

Binarni rekurzivni nizovi:
konačno mnogo jednadžbi oblika $v_m = w_n$.

Linearne forme u logaritmima:
$v_m \approx \alpha\beta^m$, $w_n \approx \gamma\delta^n \Rightarrow$
$m \log \beta - n \log \delta + \log \frac{\alpha}{\gamma} \approx 0$

Bakerova teorija: Linearna kombinacija logaritama algebarskih brojeva koja nije jednaka nuli ne može biti jako blizu nule (efektivne ocjene uključuju visine tih algebarskih brojeva i veličinu cjelobrojnih koeficijenata uključenih u linearnu kombinaciju).
Tako dobivamo gornje ograde za m, n (logaritamske funkcije od c).

Metoda kongruencija (D. & Pethő (1998)):
$v_m \equiv w_n \pmod{c^2}$
Ako su m, n mali (u usporedbi s c), onda $\equiv$ možemo zamijeniti s $=$, za što se možemo nadati da će dati kontradikciju (ako je $m, n > 2$, tj. ako d ne odgovara regularnoj četvorci). Tako dobivamo donje ograde za m, n (male pozitivne potencije od c).

Zaključak: Kontradikcija za dovoljno veliki c.

Poopćenja i modifikacije:

Uvjet $a_i \cdot a_j + 1 = x^2$ u $\mathbb{Z}$ ili $\mathbb{Q}$ može se zamijeniti sa:

- $a_i \cdot a_j + 1 = x^2$ (i modifikacije) u $\mathbb{Z}[X]$, $\mathbb{K}[X]$ (Jones, D., Fuchs, Luca, Tichy, Walsh, Ramasamy, Jurasić, Filipin)

- $a_i \cdot a_j + 1 = x^2$ (i modifikacije) u $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{d}]$, $\mathbb{Z}[\sqrt[3]{d}]$ (Franušić, Soldo, Jukić Matić, Kreso, Bayad, Filipin, Togbé)

- $a_i \cdot a_i + 1 = x^2$ u $\mathbb{Q}$ (D., Petričević)

- $a_i \cdot a_j + n = x^2$, za $n \in \mathbb{Z}$, posebno za $n = -1$ i $n = 4$
  (D., Filipin, Fuchs, Fujita, He, Togbé, Bonciocat, Cipu, Mignotte, Elsholtz, Srinivasan, Soldo, Ramasamy, Baćić, Bliznac)

- $a_i \cdot a_j + 1 = x^k$, $k \geq 2$ fiksan ili proizvoljan
  (D., Bugeaud, Luca, Gyarmati, Sarkozy, Stewart, Bérczes, Hajdu)

- $a_i \cdot a_j + 1 = F_k$ (ili neki drugi rekurzivni niz umjesto Fibonaccijevog)
  (Luca, Fuchs, Szalay, Alp, Irmak, Hutle)

Racionalne Diofantove m-torke

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

Jedna Langova slutnja povlači da postoji apsolutna gornja ograda za broj racionalnih točaka na krivuljama genusa 2. Ako je $\{a_1, a_2, a_3, a_4, a_5\}$ racionalna Diofantova petorka, onda hipereliptička krivulja

$$y^2 = (a_1x + 1)(a_2x + 1)(a_3x + 1)(a_4x + 1)(a_5x + 1)$$

ima genus 2. Ako uvedemo oznaku $B(g, \mathbb{Q}) = \max_C |C(\mathbb{Q})|$, gdje C prolazi po svim glatkim krivuljama nad $\mathbb{Q}$ genusa g, onda imamo sljedeću ogradu za broj elemenata u racionalnoj Diofantovoj m-torki: $m \leq 5 + B(2, \mathbb{Q})$.

Racionalna Diofantova četvorka ima konačno mnogo proširenja do petorke (Herrmann, Pethő & Zimmer (1999)).

Euler: Postoji beskonačno mnogo racionalnih Diofantovih petorki. Svaki par $\{a, b\}$ takav da je $ab + 1 = r^2$ može se nadopuniti do petorke.

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

D. (1997): Svaka racionalna Diofantova četvorka $\{a, b, c, d\}$ u kojoj je $abcd \neq 1$ može se nadopuniti do petorke (u pravilu na dva različita načina, osim ako nije regularna (takve su one iz Eulerove i AHS konstrukcije), u kojem slučaju je jedno od proširenja trivijalno proširenje s nulom).

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

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

gdje je

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

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

D. (2009): $\left\{\frac{5}{14}, \frac{7}{2}, \frac{48}{7}, \frac{1680}{361}, -\frac{2310}{19321}, \frac{93840}{71407}\right\}$

D., Kazalicki, Mikić & Szikszai (2016): Postoji beskonačno mnogo racionalnih Diofantovih šestorki.

Štoviše, postoji beskonačno mnogo racionalnih Diofantovih šestorki s pozitivnim elementima, a također i za bilo koju drugu kombinaciju predznaka.

Otvorena pitanja:

Postoji li racionalna Diofantova sedmorka?

Postoji li racionalna Diofantova petorka (četvorka) koja se na barem dva različita načina može proširiti do šestorke?

Prema DKMS (2016), postoji beskonačno mnogo racionalnih Diofantovih trojki sa svojstvom da se svaka od njih može proširiti do šestorke na beskonačno mnogo načina.

Piezas (2016): Postoji beskonačno mnogo racionalnih Diofantovih šestorki kod kojih je produkt četiri elementa fiksan (npr. jednak $\frac{27}{2}$).

Eliptička krivulja inducirana Diofantovom trojkom

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

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

Množeći ova tri uvjeta, dobivamo jedan uvjet

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

koji predstavlja jednadžbu eliptičke krivulje (nesingularne kubne krivulje s racionalnom točkom).

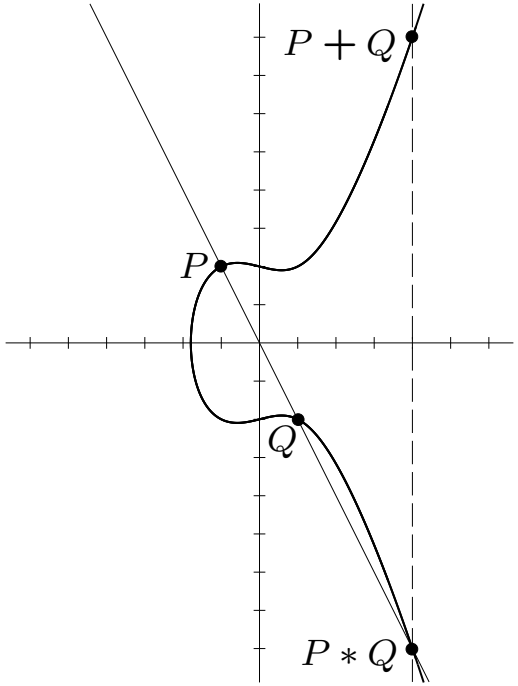
Kažemo da je *eliptička krivulja $\mathcal{E}$ inducirana trojkom* $\{a, b, c\}$.

Na $E(\mathbb{Q})$, skupu racionalnih točaka na eliptičkoj krivulji nad $\mathbb{Q}$ (afine točke $[x, y]$ koje zadovoljavaju jednadžbe zajedno s "točkom u beskonačnosti" $\mathcal{O}$), može se na prirodan način uvesti binarna operacija uz koju taj skup postaje Abelova grupa.

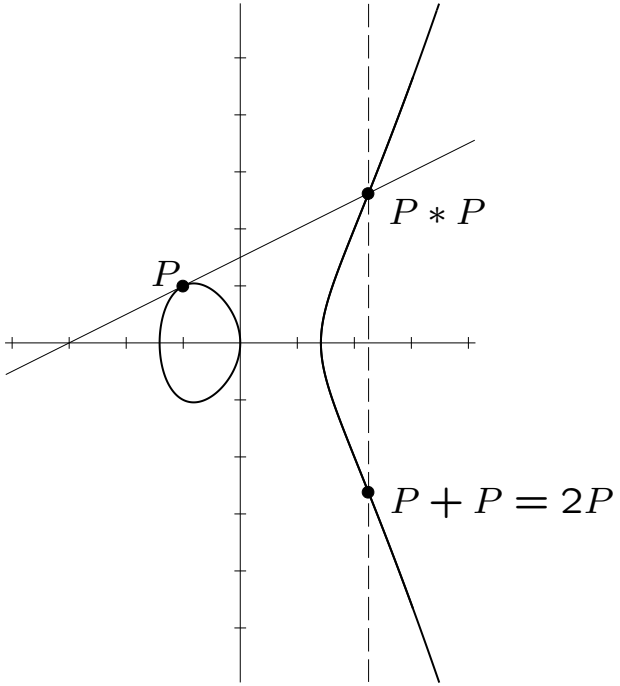
Točka u beskonačnosti $\mathcal{O}$ je neutralni element. Suprotna točka $-P$ je točka s istom x-koordinatom kao P, ali y-koordinatom suprotnog predznaka.

Ako P i Q imaju različite x-koordinate, onda pravac kroz točke P i Q siječe krivulju u točno još jednoj točki, koju označimo s $P * Q$. Definiramo $P + Q$ kao $-(P * Q)$.

Ako je $P = Q$, onda umjesto sekante povlačimo tangentu u točki P.



sekanta



tangenta

Mordell-Weilov teorem: Neka je E eliptička krivulja nad poljem racionalnih brojeva $\mathbb{Q}$ (ili općenitije nad poljem algebarskih brojeva $\mathbb{K}$). Tada je $E(\mathbb{Q})$ konačno generirana Abelova grupa. Drugim riječima

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

gdje je $E(\mathbb{Q})_{\text{tors}}$ podgrupa elemenata konačnog reda – *torzijska grupa*, dok je $r \geq 0$ *rang* eliptičke krivulje.

Mazur (1977): Postoji točno 15 mogućih torzijskih grupa $E(\mathbb{Q})_{\text{tors}}$:
$\mathbb{Z}/n\mathbb{Z}$ za $1 \leq n \leq 10$ ili $n = 12$,
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ za $1 \leq m \leq 4$.

Eliptička krivulja $\mathcal{E}$ zadana jednadžbom

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

ima tri racionalne točke reda 2:

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

Stoga su moguće torzijske grupe od $\mathcal{E}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, s time da se $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ne mogu pojaviti ako je $\{a, b, c\}$ cjelobrojna Diofantova trojka (D. & Mikić (2014)).

$\mathcal{E}$ ima još dvije očite racionalne točke

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

x-koordinate točaka $P \pm S$ su upravo brojevi $d_{+,-}$ iz definicije regularne četvorke.

Općenito, P i S će biti nezavisne točke beskonačnog reda. Međutim, važno pitanje, sa značajnim posljedicama, je mogu li one za neke trojke $\{a, b, c\}$ biti konačnog reda, te koji redovi su pritom mogući.

x-koordinata točke $T \in \mathcal{E}(\mathbb{Q})$ zadovoljava sustav (1) ako i samo ako je $T - P \in 2\mathcal{E}(\mathbb{Q})$.

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

$$R = [(rs + rt + st + 1)/abc, (r + s)(r + t)(s + t)/abc] .$$

Stoga, ako $x(T)$ zadovoljava sustav (1), onda brojevi $x(T \pm S)$ također zadovoljavaju taj sustav.

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

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

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

potpun kvadrat.

Dokaz: Promotrimo krivulju

$$y^2 = f(x) - (x - x(Q))(x - x(T))(x - x(Q+T)).$$

To je konika koja sadrži tri kolinearne točke: Q, T, $-(Q+T)$. Stoga je ona unija dvaju pravaca, tj.

$$y^2 = (\beta x + \gamma)^2.$$

Uvrstimo li ovdje $x = 0$, dobivamo

$$x(Q)x(T)x(Q+T) + \alpha^2 = \gamma^2.$$

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

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

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

Primijenimo li Propoziciju 1 uz $Q = \pm S'$, budući da je $x(S') = 1$, zaključujemo da je $x(T)x(T \pm S) + 1$ potpun kvadrat (nakon što $x(T')x(T' \pm S') + a^2b^2c^2 = \square$ podijelimo sa $a^2b^2c^2$).

Dakle, imamo konstrukciju kojom se racionalna Diofantova četvorka proširuje do petorke na dva različita načina. Stoga je unija te dvije petorke,

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

"skoro" racionalna Diofantova šestorka.

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

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

Da bi našli primjere koji zadovoljavaju ovaj zadnji uvjet, primijenit ćemo Propoziciju 1 za $Q = [2]S'$. To će nam dati željeni zaključak ako je ispunjen uvjet $x([2]S') = 1$. Sada iz $x([2]S') = x(S')$ dobivamo uvjet $[2]S' = -S'$, tj. $[3]S' = \mathcal{O}$.

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

$$\begin{aligned} -a^4b^2c^2 + 2a^3b^3c^2 + 2a^3b^2c^3 - a^2b^4c^2 + 2a^2b^3c^3 \\ -a^2b^2c^4 + 12a^2b^2c^2 + 6a^2bc + 6ab^2c + 6abc^2 \\ +4ab + 4ac + 4bc + 3 = 0. \end{aligned} \tag{3}$$

Polinom u (3) je simetričan u nepoznanicama a, b, c. Stoga uvjet (3) možemo prikazati preko elementarnih simetričnih polinoma $\sigma_1 = a + b + c$, $\sigma_2 = ab + ac + bc$, $\sigma_3 = abc$:

$$\sigma_2 = (\sigma_1^2\sigma_3^2 - 12\sigma_3^2 - 6\sigma_1\sigma_3 - 3)/(4 + 4\sigma_3^2). \qquad (4)$$

Uvrstimo li (4) 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. $1 + \sigma_3^2 = \square$.

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:

$$(\sigma_1^3\sigma_3 - 9\sigma_1^2 - 27\sigma_1\sigma_3 - 54\sigma_3^2 - 27)(1 + \sigma_3^2)(\sigma_1\sigma_3 + 2\sigma_3^2 - 1) = \square. \qquad (5)$$

Za fiksni σ_3, možemo shvatiti (5) kao kvartiku u σ_1. Budući da $1+\sigma_3^2$ mora biti potpun kvadrat, iz (5) dobivamo kvartiku s racionalnom točkom (točkom u beskonačnosti), koja se stoga može transformirati u eliptičku krivulju.

Uvjet $1+\sigma_3^2 = \square$ zadovoljimo tako da stavimo $\sigma_3 = \frac{t^2-1}{2t}$. Dobivenu kvartiku prebacimo u eliptičku krivulju nad $\mathbb{Q}(t)$

$$y^2 = x^3 + (3t^4 - 21t^2 + 3)x^2$$
$$+(3t^8 + 12t^6 + 18t^4 + 12t^2 + 3)x + (t^2+1)^6. \quad (6)$$

Ova krivulja ima pozitivan rang, jer sadrži točku $R = [0, (t^2+1)^3]$ beskonačnog reda.

Ako uzmemo točke $[m]R$, 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 $[3]S' = \mathcal{O}$.

Budući da uvjet $1 + \sigma_3^2 = \square$ povlači $rst \in \mathbb{Q}$, a $S' = -[2]S' \in 2E'(\mathbb{Q})$, 2-spust na 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 $[2]R$, dobivamo familiju trojki

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

Promotrimo 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
$[3]P$, $[3]P + S$, $[3]P - S$.

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

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

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:

$$\left\{\frac{3780}{73}, \frac{26645}{252}, \frac{7}{13140}, \frac{791361752602550684660}{1827893092234556692801},\right.$$
$$\frac{9510485270981580922898 1184}{3510419116546513356332669 55},$$
$$\left.\frac{3210891270762333567521084544}{2171271922392358100535 5}\right\}.$$

Konstrukcija navedene parametarske familije racionalnih Diofantovih šestorki zasniva se na činjenici da kubni polinom koji odgovara točki $[2]R$ ima racionalne korijene.

Je li to točno za svaki višekratnik $[m]R$ točke R? DA!

Je li to točno za sve ostale točke na krivulji (6) (u slučaju kada je rang > 1)? NE!

Npr. za $t = 31$ (kada je rang od (6) 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.

Višekratnici od R

Svakom višekratniku $[m]R = [x, y]$ 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 (4).

Uz odgovarajuće transformacije koordinata, krivulja E' postaje

$$E'' : \quad Y^2 = X^3 + \frac{((t^2+1)^2 x^{-1}+1)^2}{4} X^2 + \frac{t^2((t^2+1)^2 x^{-2}+x^{-1})}{2} X + \frac{t^4 x^{-2}}{4}. \qquad (7)$$

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 $[m]R$, $m > 1$, ima tri racionalne točke reda 2 (tj. odgovarajući brojevi a, b, c su racionalni).

Efektivna verzija Hilbertovog teorema o ireducibilnosti 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.

Krivulje velikog ranga

Naša parametarska formula za racionalne Diofantove šestorke $\{a, b, c, d, e, f\}$ može se iskoristiti za dobivanje eliptičke krivulje nad $\mathbb{Q}(t)$ relativno velikog ranga. Promotrimo krivulju

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

Ona ima tri očite točke reda dva, te također racionalne točke s x-koordinatama

$$0, \quad \frac{1}{def}, \quad a, \quad b, \quad c.$$

Može se provjeriti da su ovih pet točaka nezavisne točke beskonačnog reda na krivulji C nad $\mathbb{Q}(t)$, pa je rang ≥ 5 (torzijska grupa je $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), što izjednačava trenutni rekord za rang eliptičkih krivulja nad $\mathbb{Q}(t)$ induciranih racionalnim Diofantovim trojkama.

Za racionalne Diofantove trojke $\{a, b, c\}$ koje zadovoljavaju uvjet (3), inducirana eliptička krivulja ima torzijsku grupu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, budući da sadrži točku S reda 3. Naša parametarska familija trojki $\{a, b, c\}$ daje krivulju nad $\mathbb{Q}(t)$ s generičkim rangom 1.

Unutar ove familije krivulja, moguće je pronaći potfamilije generičkog ranga 2, te pojedinačne krivulje ranga 6, što u oba slučaja izjednačava trenutne rekorde za rang za ovu torzijsku grupu (D. & Peral (2016)).

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

Trenutni rekordi za rang eliptičkih krivulja nad $\mathbb{Q}$ (rang 9) i nad $\mathbb{Q}(t)$ (rang 4) s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ su dobiveni preko krivulja induciranih racionalnim Diofantovim trojkama (D. & Peral (2014)).

Nad kvadratnim poljima, za eliptičke krivulje inducirane Diofantovim trojkama, osim navedene četiri torzijske grupe koje se mogu pojaviti nad $\mathbb{Q}$, još su moguće i sljedeće tri torzijske grupe $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ (ova zadnja samo nad $\mathbb{Q}(i)$). U konstrukciji krivulja s torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ koriste se parametarske formule za racionalne Diofantove šestorke (D. & Jukić Bokun & Soldo (2016)).