Metode za konstrukciju eliptičkih krivulja velikog ranga

Andrej Dujella

Neke je $\mathbb{K}$ proizvoljno polje. *Eliptička krivulja* nad $\mathbb{K}$ je nesingularna projektivna kubna krivulja nad $\mathbb{K}$ s barem jednom točkom. 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 $a, b, c, \ldots, j \in \mathbb{K}$, a nesingularnost znači da je u svakoj točki na krivulji, promatranoj u projektivnoj ravnini $\mathbb{P}^2(\overline{\mathbb{K}})$ nad algebarskim zatvorenjem od $\mathbb{K}$, barem jedna parcijalna derivacija od F različita od 0. Svaka takva jednadžba može se biracionalnim transformacijama svesti na oblik

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

koji se naziva *Weierstrassova forma*.

Programski paketi za rad s eliptičkim krivuljama (PARI/GP, KANT, SAGE, MAGMA, APECS) obično inicijaliziraju eliptičku krivulju kao vektor $[a_1, a_2, a_3, a_4, a_6]$.

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

$$y^2 = x^3 + ax + b, \qquad (2)$$

koji se naziva *kratka Weierstrassova forma*. Sada nesingularnost znači da kubni polinom $f(x) = x^3 + ax + b$ nema višestrukih korijena (u $\overline{\mathbb{K}}$), ili ekvivalentno da je *diskriminanta* $\Delta = -4a^3 - 27b^2 \neq 0$.

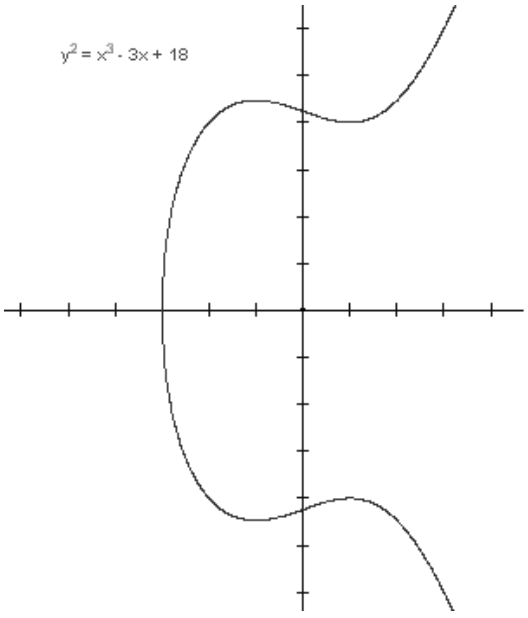
Stoga se u polju s $\mathrm{char}(\mathbb{K}) \neq 2, 3$ eliptička krivulja $E(\mathbb{K})$ nad $\mathbb{K}$ može definirati i kao skup točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koje zadovoljavaju jednadžbu

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

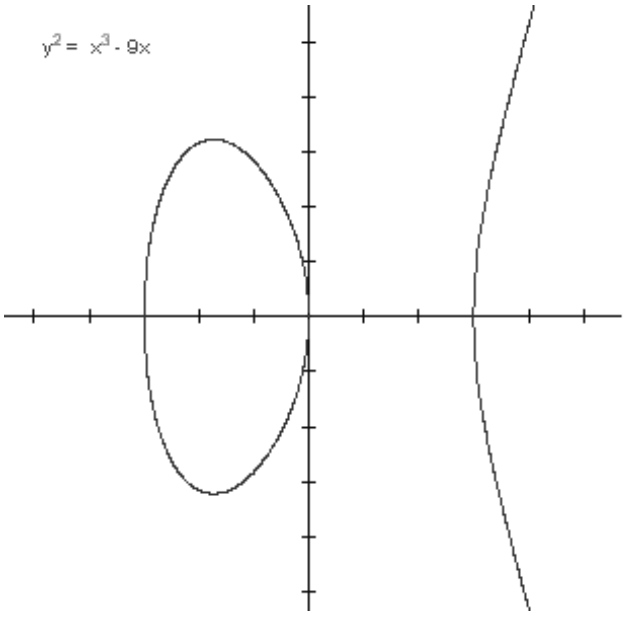
gdje su $a, b \in \mathbb{K}$ i $4a^3 + 27b^2 \neq 0$, zajedno s "točkom u beskonačnosti" $\mathcal{O}$ (točka u projektivnoj ravnini s Z-koordinatom jednakom 0).

Jedna od najvažijih činjenica o eliptičkim krivuljama jest da se na skupu točaka na eliptičkoj krivulji nad proizvoljnim poljem može uvesti binarna operacija uz koju taj skup postaje Abelova grupa.

Uzmimo na trenutak da je $\mathbb{K} = \mathbb{R}$. Ravninska krivulja $E(\mathbb{R})$ ima jednu ili dvije komponente, u ovisnosti o tome ima li polinom $f(x) = x^3 + ax + b$ jednu ili tri realne nultočke.

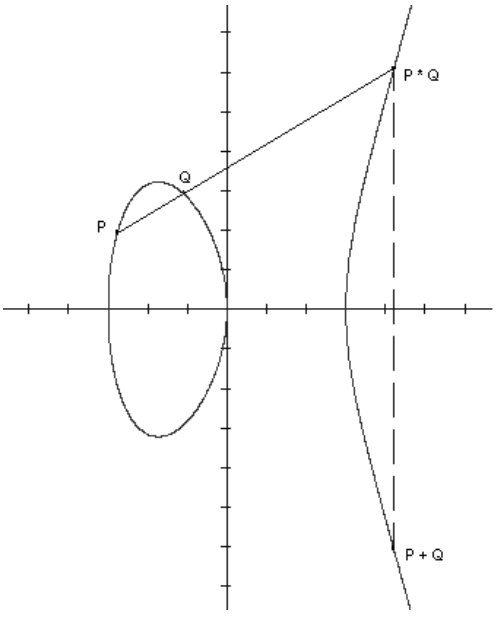


1 nultočka – 1 komponenta

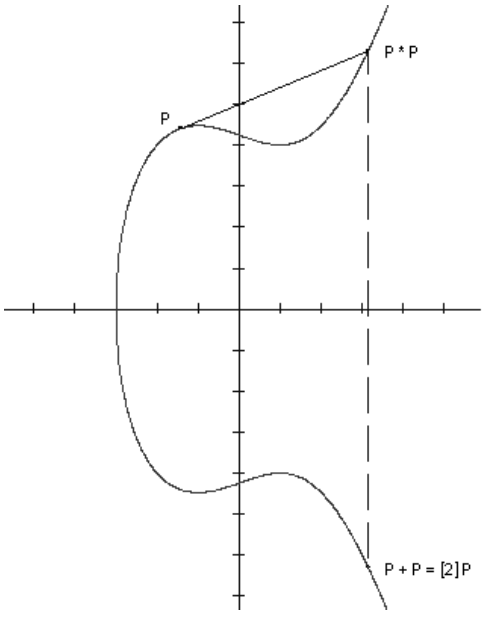


3 nultočke – 2 komponente

Neka je E eliptička krivulja nad $\mathbb{R}$, te P i Q dvije točke na E. Definiramo $-P$ kao točku 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 koristimo tangentu u točki P. Po definiciji stavljamo $P + \mathcal{O} = \mathcal{O} + P = P$ za sve $P \in E(\mathbb{R})$.



sekanta



tangeta

Iz ove geometrijske definicije, mogu se dobiti eksplicitne algebarske formule za koordinate zbroja točaka. Te formule imaju smisla nad bilo kojim poljem (uz male modifikacije u slučaju polja karakteristike 2 ili 3) i uz njih eliptička krivulja postaje Abelova grupa.

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

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

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

Ako je eliptička krivulja definirana nad poljem racionalnih brojeva $\mathbb{Q}$, onda je grupa $E(\mathbb{Q})$ konačno generirana abelova grupa (Mordell-Weilov teorem), pa je stoga izomorfna produktu torzijske grupe (koja se sastoji od elemenata konačnog reda) i $r \geq 0$ kopija beskonačne cikličke grupe:

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

Mazur je dokazao da 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 $1 \leq m \leq 4$.

S druge strane, nije poznato koje vrijednosti za r (rang krivulje) su moguće. Slutnja je da rang može biti proizvoljno velik, ali danas nije poznata niti jedna eliptička krivulja ranga većeg od 28. Rekordnu krivulju ranga 28 pronašao je Elkies 2006. godine.

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

200677624155755265850332082093385427509302303121789565 02x+

3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9

Nezavisne točke beskonačnog reda:

P_1=[−212415009125438107329213746 3,259854492051899599030515511070780628911531]

P_2=[233450986603470175688475453 7,188720041954944691808683165528036279315 31]

P_3=[−167173605406236906387903866 3,251709377261144287808506947241319126049131]

P_4=[213913026013915666649298213 7,366395091714397292024214596929412975275 31]

P_5=[153470676446712072388547733 7,854295853460176942890210328627810727995 31]

P_6=[−273107948787567703334157506 3,262521815484332191641284072623902143387531]

P_7=[277572626684457164970545853 7,128457554740140602488694876990826403699 31]

P_8=[149438572932718895754183381 7,884866055277334059861164945140492334114 51]

P_9=[186843822862088735850906525 7,592374032144377087127251403930593585891 31]

P_{10}=[200894510882574377486654253 7,476906778801255528821517507815414247115 31]

P_{11}=[234836054091802516965163293 7,174929300062005578573403324764488043635 31]

P_{12}=[−147208400709048117447000866 3,246643450653503714199947441549759798469131]

P_{13}=[292412860770806121336328893 7,283502644314888785014883564747673758995 31]

P_{14}=[537499389106606189329393453 7,286188908427263386451175031916479893731531]

P_{15}=[170969076823335452333400855 7,718988349746860894661597005292159809216 31]

P_{16}=[245095401135359314407259518 7,444522817353263435704926255061071473653 1]

P_{17}=[296925470927355916746467493 7,327668930753662708013336825431604696875 31]

P_{18}=[271191493494169260133288293 7,206843661277838169865041398150659061353 1]

P_{19}=[200785860779968545287783289 37,277960854113780660465605172562462403009 1531]

P_{20}=[215808245024073477431781069 7,349943734019640268099696622418009012547 31]

P_{21}=[200464545824705902240322493 7,480493297807046455224398669998884754675 31]

P_{22}=[297574945094799626494709133 7,333989898260753223202089344101048578691 31]

P_{23}=[−210249046768628515014734786 3,259576391459875789571677393171687203227531]

P_{24}=[311583179915063034902194537,168104385229980603540109472915660153473931]

P_{25}=[277393100834186523144377181 7,126321628346499210024141162737692758134 51]

P_{26}=[215658118814376840936346138 7,351250929640229088970041505163751780873 31]

P_{27}=[386633049987241250881565913 7,121197755655944226293036926715025847322531]

P_{28}=[223086828977357602377867873 7,285587600305974856633870206007686400285 31]

Povijesni razvoj rekordnih rangova:

rang $\geq$	godina	autor(i)
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

`http://web.math.hr/~duje/tors/rankhist.html`

Postoji i još jača slutnja da za svaku od 15 mogućih torzijskih grupa T vrijedi $B(T) = \infty$, gdje je

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

Montgomery (1987): Predložio korištenje eliptičkih krivulja s velikom torzijskom grupom za faktorizaciju velikih prirodnih brojeva.

Iz rezultata koje su dobili Montgomery, Suyama, Atkin & Morain (*Finding suitable curves for the elliptic curve method of factorization*, 1993), slijedi da je $B(T) \geq 1$ za sve torzijske grupe T.

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

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

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

Najbolje poznate donje ograde za $B(T)$:

T	$B(T) \geq$	autor(i)
0	28	Elkies (06)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (09)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (07,08,09)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (06)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (09), Eroshkin (09)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (08), Dujella & Eroshkin (08), Elkies (08), Dujella (08)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (01), Elkies (06), Eroshkin (2009), Dujella & Eroshkin (2009), Dujella & Lecacheux (2009)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (09)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (05,08), Elkies (06)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (09)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (05), Eroshkin (08), Dujella & Eroshkin (08)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (06)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (00), Dujella (00,01,06), Campbell & Goins (03), Rathbun (03,06), Flores, Jones, Rollick & Weigandt (07), Fisher (09)

`http://web.math.hr/~duje/tors/tors.html`

Glavni koraci u konstrukciji eliptičkih krivulja velikog ranga

1. Naći parametarsku familiju eliptičkih krivulja nad $\mathbb{Q}$ koja sadrži krivulje s relativno velikim rangom (tj. eliptičku krivulju nad $\mathbb{Q}(t)$ s velikim generičkim rangom).

2. U promatranoj familiji izabrati najbolje kandidate za još veći rang. Opća ideja: izglednije je da će krivulja imati veliki rang ako je $|E(\mathbb{F}_p)|$ (broj točaka na krivulji dobivenoj redukcijom koeficijenata modulo p) relativno velik za mnogo prostih brojeva p (Birch - Swinnerton-Dyerova slutnja; Mestre-Nagaove sume).

3. Pokušati izračunati rang (Cremonin program MWRANK - vrlo dobar za krivulje koje imaju racionalnu točku reda 2), ili barem dobiti dobre donje i gornje ograde za rang.

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

Najbolje poznate donje ograde za $G(T)$:

T	$B(T) \geq$	autor(i)
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)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2008)
$\mathbb{Z}/8\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2002), Rabarison (2008)
$\mathbb{Z}/9\mathbb{Z}$	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)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	3	Lecacheux (2001), Elkies (2007), Eroshkin (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	1	Kulesz (1998), Campbell (1999), Lecacheux (2002), Dujella (2007), Rabarison (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

`http://web.math.hr/~duje/tors/generic.html`

Mestreova polinomijalna metoda (1991):

Lema: Neka je $p(x) \in \mathbb{Q}[x]$ normirani 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 se može dobiti 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. Krivulja

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

sadrži točke $(a_i, \pm q(a_i))$, $i = 1, \ldots, 2n$. Ako je $\deg r = 3$ ili 4, te $r(x)$ ima samo jednostruke korijene, tada je C eliptička krivulja. Ova tvrdnja je očita za $\deg r = 3$. Ako je $\deg r = 4$, izaberemo racionalnu točki na C (npr. $(a_1, q(a_1))$) za točku u beskonačnosti i transformiramo C u eliptičku krivulju.

Za $n = 5$, skoro svi izbori a_i-ova daju $\deg r = 4$. Tada C ima 10 racionalnih točaka oblika $(a_i, q(a_i))$, pa prije spomenutom trasformacijom možemo očekivati da ćemo dobiti eliptičku krivulju ranga ≥ 9. Mestre je konstruirao familiju krivulja (tj. krivulju nad $\mathbb{Q}(t)$) s rangom ≥ 11, tako da je uzeo $n = 6$ i $a_i = b_i + t$, $i = 1, \ldots, 6$; $a_i = b_{i-6} - t$, $i = 7, \ldots, 12$, te izabrao brojeve $b_1, \ldots, b_6$ tako da koeficijent uz x^5 u $r(x)$ bude jednak 0 (npr. $b_1 = -17$, $b_2 = -16$, $b_3 = 10$, $b_4 = 11$, $b_5 = 14$, $b_6 = 17$).

- poboljšali Mestre, Nagao i Kihara do ranga 14 nad $\mathbb{Q}(t)$

- poopćili Fermigier, Kulesz i Lecacheux na krivulje s netrivijalnom torzijskom grupom

- Elkies (2006): rang 18 nad $\mathbb{Q}(t)$ (metode iz algebarske geometrije)

Gornje ograde za rang:

Ako E ima racionalnu točku reda 2, tj. jednadžbu oblika $y^2 = x^3 + ax^2 + bx$, onda se metodom 2-silaska, dobije ograda

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

gdje je $b' = a^2 - 4b$, a $\omega(b)$ označava broj različitih prostih faktora od b.

Za krivulje s netrivijalnom torzijskom točkom, može se koristiti *Mazurova ograda*. Neka je E dana svojom minimalnom Weierstrassovom jednadžbom, te neka E ima racionalnu točku prostog reda p. Tada vrijedi

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

- b je broj prostih brojeva s lošom redukcijom;
- a je broj prostih brojeva s aditivnom redukcijom;
- m je broj prostih brojeva q s multiplikativnom redukcijom za koje vrijedi da p ne dijeli eksponent od q u rastavu na proste faktore diskriminante Δ, te $q \not\equiv 1 \pmod{p}$.

Primjer (Dujella-Lecacheux): Izračunati rang od

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

Rješenje: Imamo:

$$E(\mathbb{Q})_{\text{tors}}=\{\mathcal{O},[888689186,8116714362487], [-139719349,-33500922231893], [-139719349,33500922231892], [888689186,-8116714362488]\}\cong\mathbb{Z}_5.$$

Izračunajmo Mazurovu ogradu m_5:

$$\Delta=-3^{15}\cdot5^5\cdot7^5\cdot11^5\cdot19^5\cdot41^5\cdot127^5\cdot1409\cdot10864429,$$

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

Nalazimo sljedećih 6 nezavisnih točaka modulo $E(\mathbb{Q})_{\text{tors}}$:

$$[624069446,7758948474007],[763273511,4842863582287]$$
$$[680848091,5960986525147],[294497588,20175238652299]$$
$$[-206499124,35079702960532],[676477901,6080971505482],$$

čime smo dokazali da je $\text{rank}(E)=6$ (2001. godine to je bila krivulja najvećeg poznatog ranga s torzijskom grupom $\mathbb{Z}/5\mathbb{Z}$).

Krivulje velikog ranga među eliptičkim krivuljama s nekim drugim dodatnim svojstvima:

- Mordellove krivulje ($j = 0$): $y^2 = x^3 + k$,
  $r = 15$, Elkies (2009)

- kongruentni brojevi: $y^2 = x^3 - n^2x$,
  $r = 7$, Rogers (2004)

- Hardy-Ramanujanov problem taksija: $x^3 + y^3 = m$,
  $r = 11$, Elkies & Rogers (2004)

- Diofantove trojke:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)$
  $r = 9$, Dujella (2007);
  $r = 11$, Aguirre, Dujella & Peral (2010)

- Diofantove četvorke:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)(dx + 1)$
  $r = 8$, Dujella & Gibbs (2000);
  $r = 9$, Aguirre, Dujella & Peral (2010)

- $E(\mathbb{Q}(i))_{\mathsf{tors}} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
  $r = 7$, Dujella & Jukić-Bokun (2010)

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

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

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

Baker & Davenport (1969): Fermatov skup se ne može proširiti do Diofantove petorke.

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

Fujita (2010): Postoji najviše 10^{276} Diofantovih petorki.

Neka je $\{a, b, c\}$ (racionalna) Diofantova trojka. Definirajmo nenegativne racionalne brojeve q, s, t:

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

Da bi proširili ovu trojku do četvorke, trebamo riješiti sustav

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

Prirodno je ovom sustavu pridružiti eliptičku krivulju

$$E: \quad y^2 = (ax + 1)(bx + 1)(cx + 1).$$

Transformacijom $x \mapsto \frac{x}{abc}$, $y \mapsto \frac{y}{abc}$ dobivamo

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

Tri racionalne točke na E' reda 2:

$$T_1 = [-bc, 0], \quad T_2 = [-ac, 0], \quad T_3 = [-ab, 0],$$

te još dvije očite racionalne točke

$$P = [0, abc], \quad Q = [1, qst].$$

U općem slučaju (za slučajno izabranu trojku) možemo očekivati da će točke P i Q biti dvije nezavisne točke beskonačnog reda, te da je $\operatorname{rank} E(\mathbb{Q}) \geq 2$. Stoga, uzeši u obzir različite standardne slutnje, možemo očekivati da će većina eliptičkih krivulja induciranih Diofantovim trojkama imati Mordell-Weilovu grupu $E(\mathbb{Q})$ izomorfnu ili $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}^2$ ili $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}^3$.

Pitanje: Koje su još grupe moguće?

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

Dujella (2001): Ako su a, b, c prirodni brojevi, onda slučajevi $m = 2$ i $m = 4$ nisu mogući.

Za svaki $1 \leq r \leq 11$, postoji Diofantova trojka $\{a, b, c\}$ takva da eliptička krivulja $y^2 = (ax + 1)(bx + 1)(cx + 1)$ ima torzijsku grupu izomorfnu $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$ i rang jednak r.

$y^2 = ((k-1)x + 1)((k+1)x + 1)((16k^3 - 4k)x + 1)$
generički rang $= 2$

Meste-Nagaova suma:

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

$s(523) > 22$ & $s(1979) > 33$ & Selmer rank ≥ 8

$k = 3593/2323$, $\boxed{r = 9}$

Aguirre, Dujella & Peral (2010): Krenuši od familije generičkog ranga 5, dobije se krivulja ranga 11, inducirana s Diofantovom trojkom:

$$\left\{\frac{795025}{3128544}, -\frac{22247424}{7791245}, \frac{24807390285149}{97501011189120}\right\}.$$

Za svaki $0 \leq r \leq 7$, postoji Diofantova trojka $\{a, b, c\}$ takva da eliptička krivulja $y^2 = (ax + 1)(bx + 1)(cx + 1)$ ima torzijsku grupu izomorfnu $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$ i rang jednak r.

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

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

Usporedbom s $y^2 = x(x + ac - ab)(x + bc - ab)$ dobivamo uvjete $ac-ab = \square$, $bc-ab = \square$. Jedan jednostavan način za ispunjavanje ovih uvjeta je da izaberemo a i b tako da je $ab = -1$. Tada je $ac - ab = ac + 1 = s^2$ i $bc - ab = bc + 1 = t^2$, pa preostaje naći c tako da je $\{a, -1/a, c\}$ Diofantova trojka.

Parametarsko rješenje:

$$a = \frac{2T + 1}{T - 2}, \quad c = \frac{8T}{(2T + 1)(T - 2)}.$$

$T = 7995/6562$, $\boxed{r = 7}$

Za svaki $1 \leq r \leq 4$, postoji Diofantova trojka $\{a, b, c\}$ takva da eliptička krivulja $y^2 = (ax + 1)(bx + 1)(cx + 1)$ ima torzijsku grupu izomorfnu $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}}$ i rang jednak r.

Opći oblik krivulje s torzijskom grupom izomorfnom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ je

$$y^2 = (x + \alpha^2)(x + \beta^2)\left(x + \frac{\alpha^2\beta^2}{(\alpha - \beta)^2}\right).$$

Usporedba daje: $\alpha^2 + 1 = bc + 1 = t^2$, $\beta^2 + 1 = ac + 1 = s^2$, $\alpha^2\beta^2 + (\alpha - \beta)^2 = \square$. Imamo: $\alpha = \frac{2u}{u^2-1}$, $\beta = \frac{v^2-1}{2v}$, te uvrštavajući ovo u treći uvjet dobivamo jednadžbu oblika $F(u, v) = z^2$.

Parametarsko rješenje: $u = \frac{v^3+v}{v^2-1}$

$v = 7$, $\boxed{r = 3}$

$u = 34/35$, $v = 8$, $\boxed{r = 4}$

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

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

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

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

Dujella (2007): $\boxed{r = 3}$ (4-silazak, MAGMA)

$$\left\{\frac{451352}{974415}, -\frac{974415}{451352}, -\frac{745765964321}{439804159080}\right\}.$$