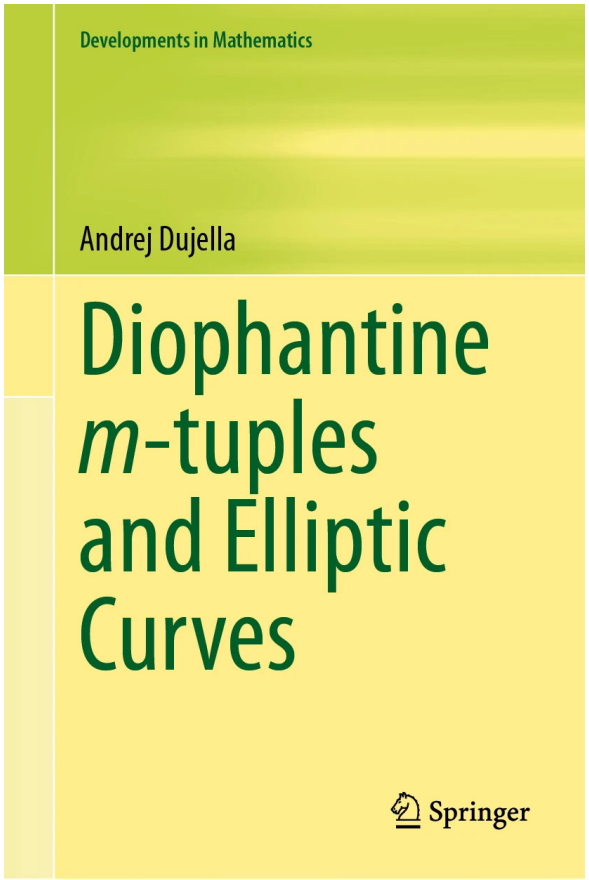
Predstavljanje knjige akademika Andreja Dujelle: Diophantine *m*-tuples and Elliptic Curves



prezentacija: Filip Najman, Knjižnica HAZU, 10. listopad 2024.

Tema knjige

Definicija

Diofantova m-torka je skup $\{x_1, \ldots, x_m\}$ *cijelih brojeva takvih da je* $x_i x_j + 1$ *potpun kvadrat za sve* $1 \leq i < j \leq m$.
Ukoliko je dopušteno da su x_i*-evi racionlani brojevi, taj se skup zove racionalna Diofantova m-torka.*

Ova knjiga daje sveobuhvatan pregled glavnih rezultata i problema vezanih uz Diofantove *m*-torke, te istražuje njihove veze s eliptičkim krivuljama.

Diofantove *m*-torke, njihove generalizacije, te veze s eliptičkim krivuljama su teme s kojima se akademik Dujella bavio cijelu karijeru, te postigao značajne rezultate.

Teorem (Dujella, 2004)

Ne postoji Diofantova šestorka, te ne postoji beskonačno mnogo Diofantovih petorki.

Pregled knjige

Knjiga ima 5 poglavlja.

1. U Poglavlju 1 predstavljeni su doprinosi Diofanta, Fermata i Eulera na ovu temu, koji su poslužili kao motivacija za daljnja istraživanja.

   Iskazane su glavne definicije, rezultati i otvoreni problemi o kojima će se raspravljati u knjizi.

2. U Poglavlju 2 obrađeni su su preduvjeti o eliptičkim krivuljama nad $\mathbb{Q}$, koji su potrebni kasnije u knjizi.

   Daje se pregled mogućih torzijskih grupa eliptičkih krivulja nad $\mathbb{Q}$ s posebnim naglaskom na grupe koje se mogu pojaviti za krivulje inducirane Diofantovim trojkama.

Pregled knjige

3. Poglavlje 3 predstavlja središnji dio knjige. U njemu su uvedene eliptičke krivulje inducirane Diofantovim trojakama i objašnjena su njihova svojstva i primjene.

   Jedna od glavnih primjena odnosi se na konstrukciju beskonačnih familija racionalnih Diofantovih šestorki, što je bio otvoreni problem još od doba kada je Euler pronašao familije takvih petorki. Prikazane su četiri poznate različite konstrukcije takvih familija, koje sve na neki način koriste eliptičke krivulje.

   Druga važna primjena eliptičkih krivulja induciranih Diofantovim trojkama odnosi se na konstrukciju eliptičkih krivulja visokog ranga s određenim torzijskim grupama.

   Detaljno su opisane konstrukcije nekih rekordnih krivulja nad $\mathbb{Q}(t)$ i $\mathbb{Q}$, a opisane su i druge veze između Diofantovih m-torki i eliptičkih krivulja.

Pregled knjige

4. U Poglavlju 4 prvo su opisane opće metode za pronalaženje cjelobrojnih točaka na eliptičkim krivuljama. Ove metode su potom primijenjene na problem pronalaženja svih cjelobrojnih točaka na eliptičkim krivuljama induciranim Diofantovim trojkama.

   Predstavljen je dokaz gornje granice za veličinu Diofantovih m-torki i ukratko su opisani glavni koraci u rezultatima koji vode do dokaza o nepostojanju Diofantovih petorki.
5. U Poglavlju 5 izneseni su detalji o generalizacijama Diofantovih m-torki, naime onoj u kojoj je uvjet da je $ab+1$ kvadrat zamijenjen uvjetom da je $ab+n$ bude kvadrat za neki fiksni cijeli ili racionalni broj n.

   Proučava se problem postojanja cjelobrojnih $D(n)$-četvorki i racionalnih $D(n)$-petorki. Pokazuje se da je ovaj problem povezan s distribucijom rangova u familijama kvadratnih zakreta određenih eliptičkih krivulja.

Eliptičke krivulje

Fokus ove prezentacije će biti na eliptičkim krivuljama i njihovim vezama s Diofantovim m-torkama.

Eliptička krivulja je glatka projektivna krivulja genusa 1 sa specificiranom točkom O.

Eliptička krivulja nad $\mathbb{Q}$ ima afin model

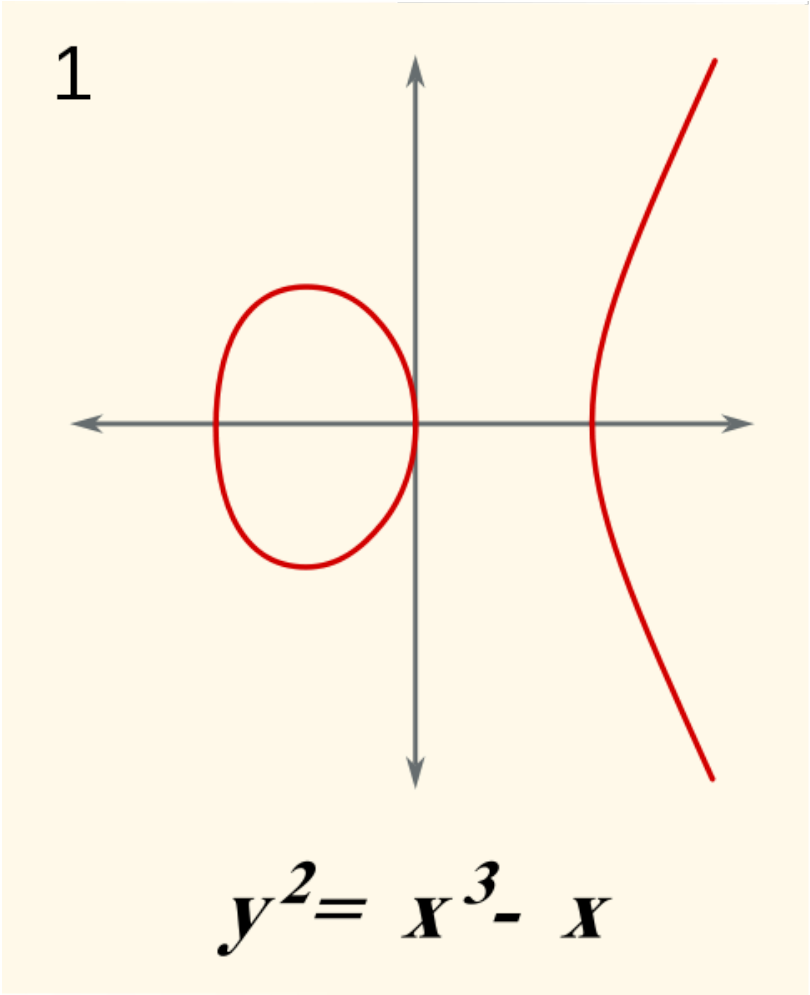
$$E : y^2 = x^3 + ax + b$$

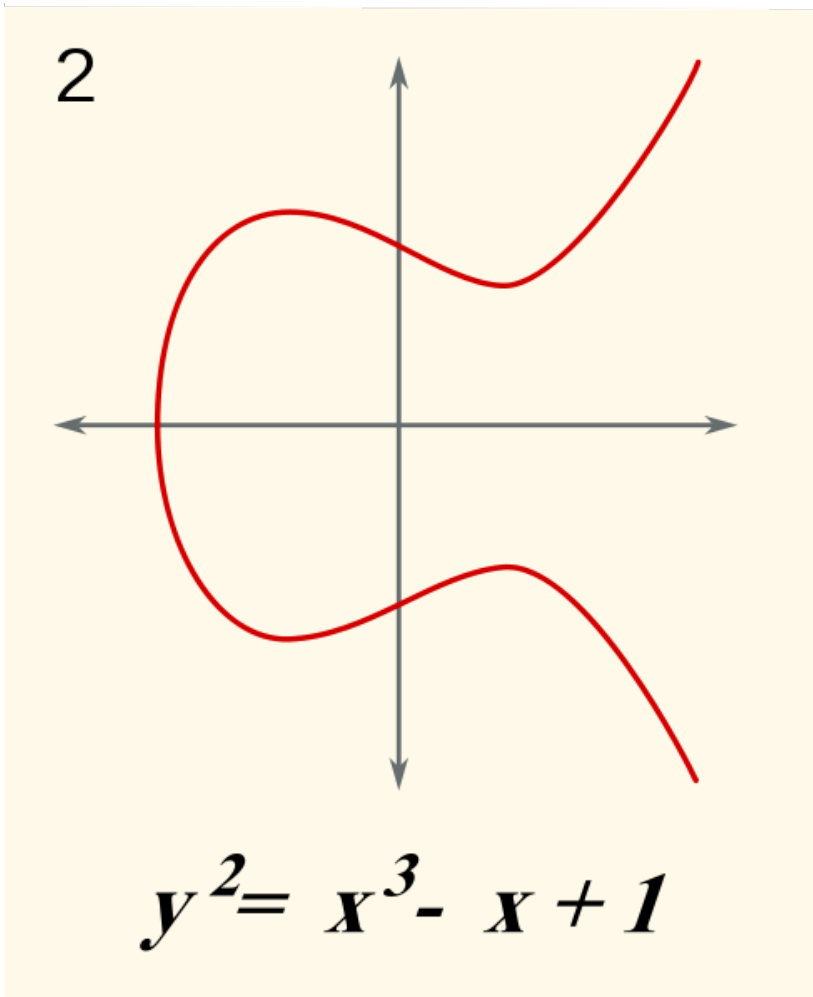
za koji vrijedi $\Delta(E) = -16(4a^3 + 27b^2) \neq 0$.

Specificirana točka O postaje "točka u beskonačnosti".

Dakle, $E(\mathbb{Q})$ je

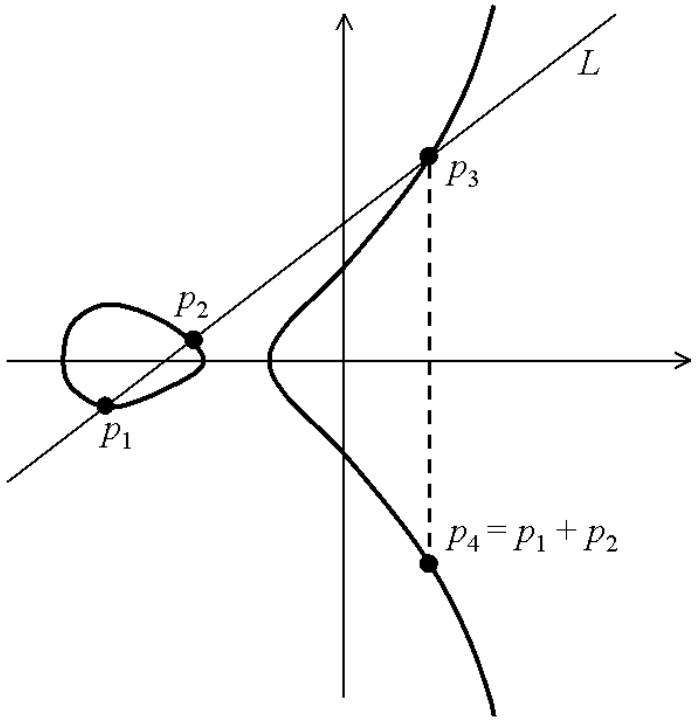
$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 | y^2 = x^3 + ax + b\} \cup \{\infty\}.$$


1
$y^2 = x^3 - x$


2
$y^2 = x^3 - x + 1$

Grupovni zakon

Uvodimo operaciju zbrajanja na skupu točaka na eliptičkoj krivulji: $P + Q + R = 0$ ako su P, Q, R kolinearni. Točka u beskonačnosti je 0.



$p_3 + p_4 + 0 = 0 \Longrightarrow p_3 = -p_4$. $p_1 + p_2 + p_3 = 0 \Longrightarrow p_1 + p_2 = p_4$.

Mordell-Weilov teorem

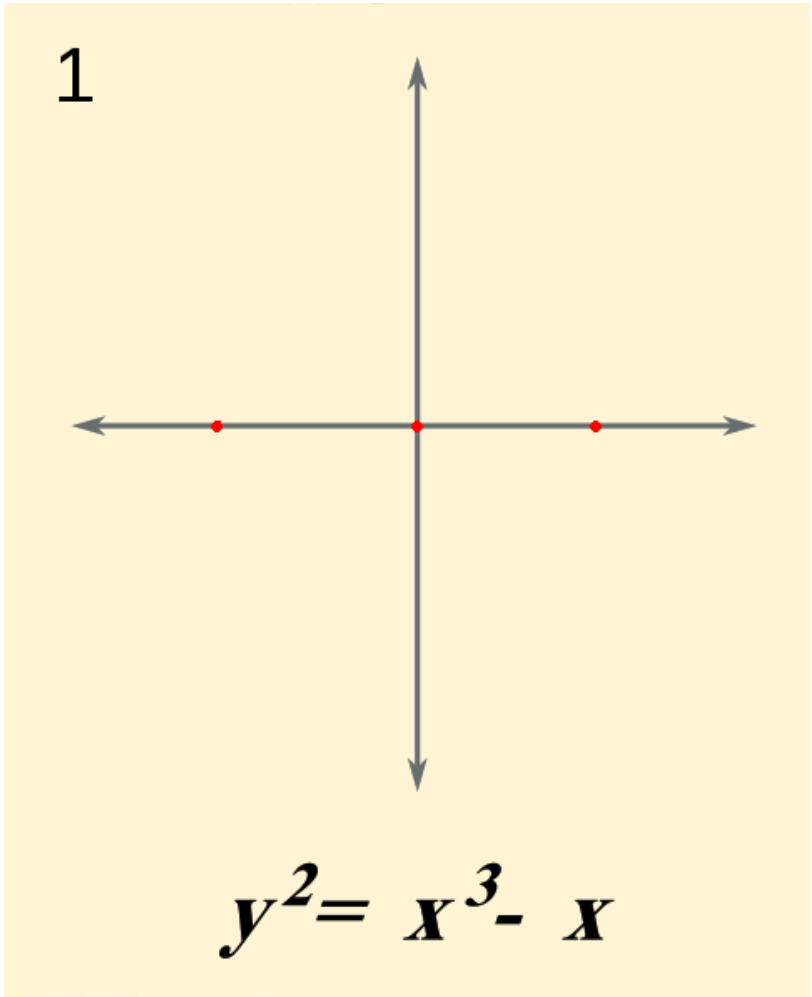
S ovom operacijom $E(\mathbb{Q})$ postaje grupa.

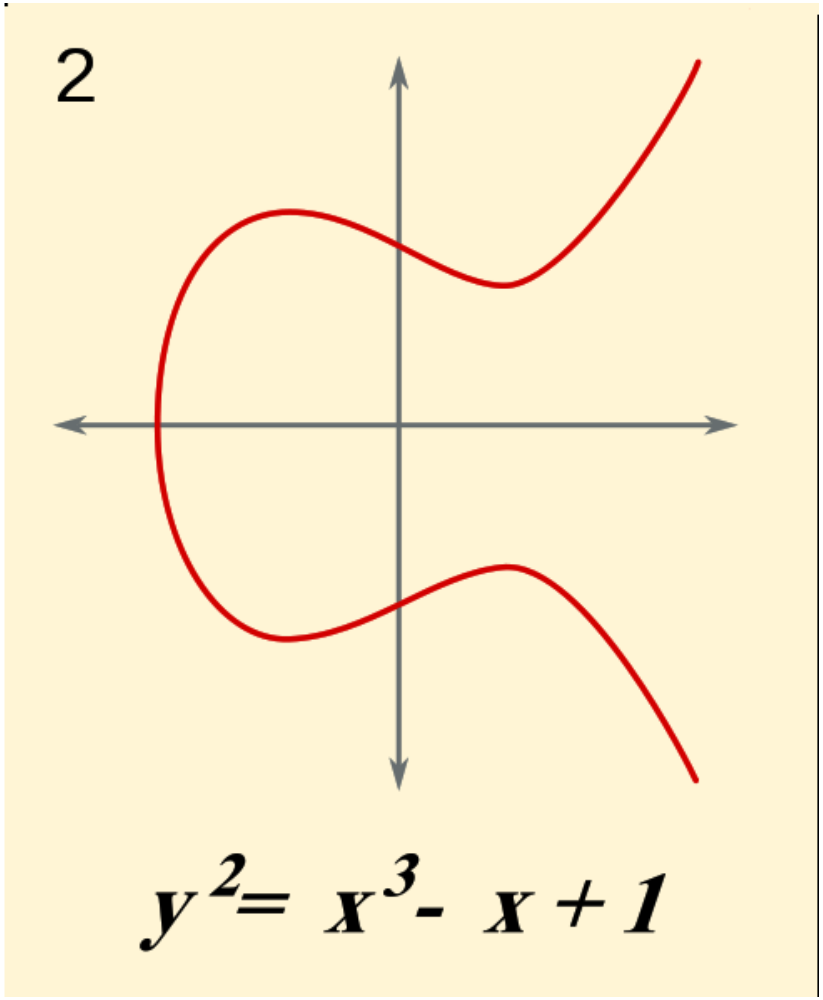
Teorem (Mordell-Weilov)

Neka je E eliptička krivulja nad $\mathbb{Q}$. Tada je $E(\mathbb{Q})$ konačno generirana Abelova grupa. Drugim rječima

$$E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r,$$

*gdje je T podgrupa elemenata konačnog reda - **torzija**, dok je $r \geq 0$, **rang** eliptičke krivulje.*





$E_1(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$E_2(\mathbb{Q}) \simeq \mathbb{Z}.$

Teorem (Mazurov torzijski teorem, 1977)

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

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}, & n = 1, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & m = 1, \ldots, 4. \end{cases}$$

Neka je a, b, c Diofantova trojka. Tada kažemo da je eliptička krivulja

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

inducirana Diofantovom trojkom a, b, c.

Eliptičke krivulje inducirane Diofantovim trojkama mogu imati torziju $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ za $n = 1, 2, 3, 4$.

Zanimljivo je da su sve eliptičke krivulje s najvećom torzijom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ inducirane Diofantovim trojkama.

Rangovi eliptičkih krivulja

Jedno od najvećih otvorenih pitanja u teoriji brojeva je koliko velik može biti rang eliptičkih kirvulja i je li taj broj uopće ograničen.

Pogledajmo povijest najvećih poznatih rangova eliptičkih krivulja.

rank >=	year	Author(s)
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

Rangovi eliptičkih krivulja

rank >=	year	Author(s)
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

Ove godine je (nakon 18 godina) oboren rekord, te je pronađena krivulja ranga 29.

Rangovi eliptičkih krivulja sa zadanom torzijom

Možemo se isto promatrati rekordne rangove, ako promatramo samo eliptičke krivulje sa zadanom torzijskom grupom.

T	$B(T)>=$	Author(s)
0	29	Elkies - Klagsbrun (2024)
Z/2Z	20	Elkies - Klagsbrun (2020)
Z/3Z	15	Elkies - Klagsbrun (2020)
Z/4Z	13	Elkies - Klagsbrun (2020)
Z/5Z	9	Klagsbrun (2020)
Z/6Z	9	Klagsbrun (2020), Voznyy (2020)
Z/7Z	6	Klagsbrun (2020)
Z/8Z	6	Elkies (2006), Dujella - MacLeod - Peral (2013), Voznyy (2021)
Z/9Z	4	Fisher (2009), van Beek (2015), Dujella - Petricevic (2021), Dujella - Petricevic - Rathbun (2022)
Z/10Z	4	Dujella (2005,2008), Elkies (2006), Fisher (2016)
Z/12Z	4	Fisher (2008)
Z/2Z × Z/2Z	15	Elkies (2009)
Z/2Z × Z/4Z	9	Dujella - Peral (2012,2019), Klagsbrun (2020)
Z/2Z × Z/6Z	6	Elkies (2006), Dujella - Peral - Tadic (2015), Dujella - Peral (2020)
Z/2Z × Z/8Z	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell - Goins (2003), Rathbun (2003,2006,2013,2022), Dujella - Rathbun (2006), Flores - Jones - Rollick - Weigandt - Rathbun (2007), Fisher (2009), AttarBashi - Rathbun - Voznyy (2022), AttarBashi - Fisher - Rathbun - Voznyy (2022), AttarBashi - Fisher - Voznyy (2022)

Rangovi eliptičkih krivulja

T	$B(T)>=$	Author(s)
0	29	Elkies - Klagsbrun (2024)
Z/2Z	20	Elkies - Klagsbrun (2020)
Z/3Z	15	Elkies - Klagsbrun (2020)
Z/4Z	13	Elkies - Klagsbrun (2020)
Z/5Z	9	Klagsbrun (2020)
Z/6Z	9	Klagsbrun (2020), Voznyy (2020)
Z/7Z	6	Klagsbrun (2020)
Z/8Z	6	Elkies (2006), Dujella - MacLeod - Peral (2013), Voznyy (2021)
Z/9Z	4	Fisher (2009), van Beek (2015), Dujella - Petricevic (2021), Dujella - Petricevic - Rathbun (2022)
Z/10Z	4	Dujella (2005,2008), Elkies (2006), Fisher (2016)
Z/12Z	4	Fisher (2008)
Z/2Z × Z/2Z	15	Elkies (2009)
Z/2Z × Z/4Z	9	Dujella - Peral (2012,2019), Klagsbrun (2020)
Z/2Z × Z/6Z	6	Elkies (2006), Dujella - Peral - Tadic (2015), Dujella - Peral (2020)
Z/2Z × Z/8Z	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell - Goins (2003), Rathbun (2003,2006,2013,2022), Dujella - Rathbun (2006), Flores - Jones - Rollick - Weigandt - Rathbun (2007), Fisher (2009), AttarBashi - Rathbun - Voznyy (2022), AttarBashi - Fisher - Rathbun - Voznyy (2022), AttarBashi - Fisher - Voznyy (2022)

U ovoj "kategoriji" akademik Dujella drži brojne rekorde, koji su postignuti upravo promatranjem eliptičkih krivulja induciranih Diofantovim trojkama.

Rangovi eliptičkih krivulja

Spomenimo i za kraj da su ove slike uzete s web stranice akademika Dujelle, koja je postala svjetska referentna točka za rekorde rangova eliptičkih krivulja.

Svakome zainteresiranom za konstrukciju eliptičkih krivulja s velikim rangom će knjiga *Diophantine m-tuples and elliptic curves* biti prva i najvažnija referenca.