O egzistenciji racionalnih Diofantovih petorki sa svojstvom $D(q)$

Andrej Dujella

Neka je q racionalan broj različit od nule. Skup od m racionalnih brojeva različitih od nule $\{a_1, a_2, \ldots, a_m\}$ naziva se *racionalna Diofantova m-torka sa svojstvom $D(q)$* ili kraće *racionalna $D(q)$-m-torka*, ako je $a_i a_j + q$ potpun kvadrat za sve $1 \leq i < j \leq m$. Ako su $q, a_1, \ldots, a_m$ s gornjim svojstvom cijeli brojevi, onda govorimo o $D(q)$-m-torki.

Postavlja se pitanje koliko veliki mogu biti ovi skupovi, tj. za dani q koliko velik može biti m (u cjelobrojnom, odnosno u racionalnom slučaju). Ili još preciznije, za dane q i m, pitamo se postoji li (racionalna) $D(q)$-m-torka, te ako postoji, ima li takvih m-torki konačno ili beskonačno mnogo.

Neki poznati rezultati u cjelobrojnom slučaju:

- postoji beskonačno $D(n)$-trojki da svaki cijeli broj n ($\{a, b, a+b+2r\}$, gdje je $ab + n = r^2$, Diofant?);
- postoji $D(256)$-četvorka ($\{1, 33, 68, 105\}$, Diofant);
- postoji $D(1)$-četvorka ($\{1, 3, 8, 120\}$, Fermat);
- postoji beskonačno mnogo $D(1)$-četvorki i općenitije $D(k^2)$-četvorki ($\{a, b, a + b + 2r, 4r(a + r)(b + r)\}$, Euler);
- ne postoji $D(n)$-četvorka za $n \equiv 2 \pmod 4$ (Brown, Gupta & Singh, Mohanty & Ramasamy, 1985);
- ako $n \not\equiv 2 \pmod 4$ i $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, onda postoji barem jedna $D(n)$-četvorka (Dujella, 1993);
- ne postoji $D(1)$-šestorka (Dujella, 2004), te najviše konačno mnogo $D(1)$-petorki (Dujella, 2004);
- ne postoji $D(4)$-šestorka (Filipin, 2008), te najviše konačno mnogo $D(4)$-petorki (Filipin, 2011);

- ne postoji $D(-1)$-petorka (Dujella & Fuchs, 2005), te najviše konačno mnogo $D(-1)$-četvorki (Dujella, Filipin & Fuchs, 2007);
- postoji $D(256)$-petorka ($\{1, 33, 105, 320, 18240\}$, Dujella, 1997) i $D(-255)$-petorka ($\{8, 32, 77, 203, 528\}$, Dujella, 1997);
- postoji $D(2985984)$-šestorka ($\{99, 315, 9920, 32768, 44460, 19534284\}$, Gibbs, 1999)

Neki poznati rezultati u racionalnom slučaju:

- postoji racionalna $D(1)$-četvorka ($\{1/16, 33/16, 17/4, 105/16\}$, Diofant);
- za svaki racionalan broj q postoji beskonačno mnogo racionalnih $D(q)$-četvorki (Dujella, 2000);
- postoji beskonačno mnogo racionalnih $D(1)$-petorki (svaka cjelobrojna $D(1)$-četvorka oblika $\{a, b, a+b+2r, 4r(a+r)(b+r)\}$ može se nadopuniti do racionalne $D(1)$-petorke, npr. $\{1, 3, 8, 120, 777480/8288641\}$ je racionalna $D(1)$-petorka, Euler), (svaka racionalna $D(1)$-četvorka $\{a, b, c, d\}$ takva da je $abcd \neq 1$ može se nadopuniti do racionalne $D(1)$-petorke, Dujella, 1997);
- racionalna $D(1)$-četvorka se na samo konačno mnogo načina može nadopuniti do racionalne $D(1)$-petorke (Herrmann, Pethő & Zimmer, 1999);
- postoji beskonačno mnogo racionalnih $D(-3)$-petorki (koristi činjenicu da eliptička krivulja $y^2 = x^3 + 42x^2 + 432x + 1296$ ima pozitivan rang, Dujella, 2000);
- postoji beskonačno mnogo racionalnih $D(-1)$-petorki (koristi činjenicu da eliptička krivulja pridružena krivulji $y^2 = -(x^2-x-3)(x^2+2x-12)$ ima pozitivan rang, Dujella, 2002);
- postoji racionalna $D(1)$-šestorka (s pozitivnim članovima, Gibbs, 1999; za proizvoljan izbor predznaka, Dujella, 2009).

Teorem 1: *Za svaki racionalan broj q postoji beskonačno mnogo racionalnih $D(q)$-četvorki.*

Dokaz: Promotrimo skup

$$\{k, 16k+8, 25k+14, 36k+20\}. \tag{1}$$

To je (racionalna) $D(16k+9)$-četvorka za sve osim konačno mnogo cjelobrojnih (racionalnih) k-ova (za koje je neki element jednak 0 ili su neka dva elementa međusobno jednaka). Zaista, skup ima oblik $\{a, b, a+b+2r, 4a+b+4r\}$ i dodatno svojstvo da je $b(4a+b+4r)+n$ također kvadrat.

Neka je sada $s \neq 0$ proizvoljan racionalan broj. Definiramo racionalan broj k sa $16k+9 = qs^2$, tj. $k = \frac{qs^2-9}{16}$. Sada iz (1) dobivamo racionalnu $D(q)$-četvorku

$$\left\{ \frac{qs^2-9}{16s}, \frac{qs^2-1}{s}, \frac{25qs^2-1}{16s}, \frac{9qs^2-1}{4s} \right\}$$

(za sve osim konačno mnogo s-ova). Tvrdimo da smo na ovaj način dobili beskonačno mnogo različitih racionalnih $D(q)$-četvorki. Zaista, samo konačno mnogo različitih s-ova može inducirati istu četvorku. Za $\alpha \in \mathbb{Q}$, uvjet $\frac{qs^2-9}{16s} = \alpha$ daje kvadratnu jednadžbu u s, koja ima najviše dva rješenja. Isto vrijedi za ostale elemente četvorke.

$\square$

Pitanje: *Za koje racionalne brojeve q postoji beskonačno mnogo racionalnih $D(q)$-petorki?*

Jasno je da u ovom pitanju možemo pretpostaviti da je q kvadratno slobodan cijeli broj, budući da množenjem elemenata $D(q)$-m-torke sa r dobivamo $D(qr^2)$-m-torku.

U dokazu Teorema 1 koristili smo polinomijalnu Diofantovu četvorku sa svojstvom $D(n)$, gdje je n bio linearan polinom, a također su i svi elementi četvorke linearni polinomi. Poznato je puno primjera takvih polinomijalnih četvorki. Postavlja se stoga pitanje možemo li naći polinomijalnu petorku čiji su svi elementi linearni polinomi. Odgovor je negativan, i to su dokazali Dujella, Fuchs & Walsh (2006).

Skicirat ćemo dokaz tog rezultata. Neka je $\{ax+b, cx+d, ex+f\}$ polinomijalna $D(ux+v)$-trojka, gdje su svi koeficijenti cijeli brojevi. Tada je $\{a^2x+ab, acx+ad, aex+af\}$ polinomijalna $D(a^2ux+a^2v)$-trojka. Supstitucijom $ax+b=z$ dobivamo polinomijalnu $D(auz+v')$-trojku $\{az, cz+d', ez+f'\}$. Možemo pretpostaviti da je $\gcd(a,c,e)=1$ (inače uvedemo supstituciju $z' = z\gcd(a,c,e)$), pa dobivamo da su a, c, e potpuni kvadrati: $a = A^2$, $c = C^2$, $e = E^2$. Uvršavanjem $z = 0$ vidimo da je i v' potpun kvadrat: $v' = V^2$. Ali, $v' = a^2v - abu = A^4v - A^2bu$, pa je $V = AW$, uz $W^2 = A^2v - bu$. Sada iz

$$A^2z(C^2z+d') + (A^2uz + A^2W^2) = (ACz \pm AW)^2,$$

usporedbom koeficijenata uz z dobivamo da je $d' = \pm 2CW - u$. I analogno $f' = \pm 2EW - u$. Dakle, imamo $D(A^2uz + A^2W^2)$-trojku

$$\{A^2z, C^2z \pm 2CW - u, E^2z \pm 2EW - u\}.$$

Pritom još treba biti zadovoljen uvjet da je

$$(C^2z \pm 2CW - u)(E^2z \pm 2EW - u) + (A^2uz + A^2W^2)$$

kvadrat linearnog polinoma (u varijabli z), a to povlači da je diskriminanta ovog kvadratnog polinoma jednaka 0. Faktorizacijom diskriminante dobivamo uvjet

$$(C-E-A)(C-E+A)(\pm 2CEW-Cu-Eu+Au)(\pm 2CEW-Cu-Eu-Au) = 0.$$

Uvjet $\pm 2CEW - Cu - Eu \pm Au = 0$ se može zapisati kao

$$(\pm 2CW - u)(\pm 2EW - u) = u^2 \pm 2AWu.$$

Dakle, ako polinomijalna petorka s linearnim polinomima postoji, onda postoji $D(A^2uz + A^2W^2)$-petorka čiji je jedan element A^2z, a ostali imaju oblik

$$m_i^2z + 2m_iW - u, \quad i = 1, 2, 3, 4.$$

Pritom za $i \neq j$ vrijedi $|m_i - m_j| = A$ (to odgovara općoj konstrukciji trojki oblika $\{a, b, a + b + 2r\}$) ili $(\pm 2m_iW - u)(\pm 2m_jW - u) = u^2 \pm 2AWu$.

Dujella, Fuchs & Walsh (2006) su pokazali ovo vodi do kontradikcije, što znači da je postoji polinomijalna petorka traženim svojstvom.

No, Dujella & Fuchs (2012) su pokazali da je ove uvjete moguće zadovoljiti ako se ispusti samo jedan uvjet (primjerice $(i, j) = (3, 4)$). Štoviše, takva "skoro petorka" je u biti jedinstvena (sve ostale se iz nje mogu dobiti "dopustivim" transformacijama). Taj skup je

$$\{x, 9x + 8, 25x + 20, 4x + 2, 16x + 14\}$$

koji sadrži dvije polinomijalne $D(10x+9)$-četvorke: $\{x, 9x+8, 25x+20, 4x+2\}$ i $\{x, 9x + 8, 25x + 20, 16x + 14\}$.

Dakle, za racionalan broj x, skup

$$\{x, 4x + 2, 9x + 8, 16x + 14, 25x + 20\}$$

će biti racionalna $D(10x + 9)$-petorka ako vrijedi

$$(4x + 2)(16x + 14) + 10x + 9 = y^2 \qquad (2)$$

za $y \in \mathbb{Q}$. Ovo je krivulja genusa 0. Uvrstimo $y = 8x + t$ u (2), dobivamo parametarsko rješenje

$$x = \frac{t^2 - 37}{2(49 - 8t)}.$$

Nakon sređivanja (rješavanja nazivnika), dobivamo sljedeći rezultat

Teorem 2: *Skup*

$$\{t^2 - 37, 4t^2 - 32t + 48, 9t^2 - 128t + 451, 16t^2 - 224t + 780, 25t^2 - 320t + 1035\} \tag{3}$$

je $D(4(8 - t)(5t - 32)(8t - 49))$*-petorka.*

Neka je sada q racionalan broj različit od nule. Zanima nam može li se Teorem 2 iskoristiti za dobivanje racionalne $D(q)$-petorke. Ako postoje racionalni brojevi $s \neq 0$ i t takvi da je

$$4(8 - t)(5t - 32)(8t - 49) = qs^2, \tag{4}$$

onda dijeljenjem svi elemenata skupa (3) sa s, dobivamo upravo jednu $D(q)$-petorku. Jednadžba (4) definira eliptičku krivulju nad $\mathbb{Q}$. Dakle, zanima sam ima li ta krivulja točku s s-koordinatom različitom od 0, a to nas dovodi do promatranja krivulja pozitivnog ranga u familiji eliptičkih krivulja (u ovisnosti o parametru q). U stvari, to je familija twistova eliptičke krivulje

$$s^2 = 4(8 - t)(5t - 32)(8t - 49).$$

Supstitucijama $t = -x/40 + 49/8, s = y/20$, dobivamo jednadžbu krivulje E u Weierstrassovoj formi

$$E\colon\ y^2 = x(x + 11)(x + 75) = x^3 + 86x^2 + 825x. \tag{5}$$

Krivulja E ima diskriminantu $D = 2^{16}3^2 5^4 11^2$ i konduktor $C = 330 = 2 \cdot 3 \cdot 5 \cdot 11$. Njezina minimalna jednadžba je dana sa $y^2 + xy = x^3 + x^2 - 102x + 324$. Torzijska grupa joj je izomorfna sa $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (jedine netrivijalne torzijske točke su one s y-koordinatom jednakom 0), a rang je jednak 1 s generatorom $(x, y) = (-15, 60)$.

Pitamo se sada koji q-twistovi krivulje E imaju pozitivan rang. I ovdje možemo pretpostaviti da je q kvadratno slobodan cijeli broj. Promatramo familiju eliptičkih krivulja E_q danu sa

$$E_q\colon\ qy^2 = x^3 + 86x^2 + 825x. \tag{6}$$

Općenito, na krivulji oblika $f(t)y^2 = f(x)$ leži racionalna točka $(x, y) = (t, 1)$ beskonačnog reda. Ako zapišemo $t = u/v$, $\gcd(u, v) = 1$, dobivamo da ako je q oblika

$$q = uv(u^2 + 86uv + 825v^2), \tag{7}$$

za cijele brojeve $u, v \neq 0$, onda je $(u/v, 1/v^2)$ točka beskonačnog reda na E_q. To nam daje beskonačno mnogo vrijednosti od q za koje je rang pozitivan, i stoga za njih postoji beskonačno mnogo racionalnih $D(q)$-petorki. Može se pokazati (Gouvêa & Mazur, 1991) da za $\varepsilon > 0$ i dovoljno velik N, postoji barem $N^{1/2-\varepsilon}$ kvadratno slobodnih brojeva q, $|q| \leq N$, oblika (7).

Ako pretpostavimo da vrijedi Slutnja o parnosti ("Parity Conjecture") za twistove od E, onda možemo dati precizni opis onih q-ova za koje je rang q-twista neparan (pa stoga i pozitivan). Slutnja o parnosti (za E) kaže da je rang Mordell-Weilove grupe od E iste parnosti kao red iščezavanja pridružene L-funkcije $L(E, s)$ u $s = 1$. Ova slutnja je slabiji oblik poznate Birch & Swinerton-Dyerove slutnje. Slutnja o parnosti povlači da za neparan kvadratno slobodan cijeli broj q koji je relativno prost s konduktorom C od E, rangovi od E i E_q su iste parnosti ako i samo ako je $\chi_q(-C) = 1$, gdje je χ_q kvadratni Dirichletov karakter pridužen kvadratnom polju $\mathbb{Q}(\sqrt{q})$.

Spomenimo i Goldfeldovu slutnju koja predviđa da je prosječan rang svih twistova od E jednak $1/2$. Zajedno sa Slutnjom o parnosti, ovo povlači da je broj kvadratno slobodnih q-ova, $|q| \leq N$, takvih da E_q ima rang 0 (odnosno 1) je asimptotski $6N/\pi^2$ kada $N \to \infty$. Za našu svrhu, dovoljno je da je rang pozitivan, a Slutnja o parnosti povlači da takvih kvadratno slobodnih q-ova sa $|q| \leq N$ ima $\geq 6N/\pi^2$.

Teorem 3: *Za beskonačno mnogo kvadratno slobodnih cijeli brojeva q postoji beskonačno mnogo racionalnih $D(q)$-petorki. Ako pretpostavimo da vrijedi Slutnja o parnosti, onda za sve kvadratno slobodne brojeve q u najmanje 497 klasa ostataka* $\pmod{1320}$ *postoji beskonačno mnogo racionalnih $D(q)$-petorki.*

Dokaz: Prvu tvrdnju iz teorema smo zapravo već dokazali. Ostaje još provjeriti da najviše konačno mnogo različitih točaka na eliptičkoj krivulji E_q može inducirati istu petorku. Za $\alpha \in \mathbb{Q}$, uvjet $\frac{t^2-37}{s} = \alpha$ za točku (t, s) na (4) daje polinom 4. stupnja u t, pa najviše četiri točke mogu zadovoljavati taj uvjet. Isto vrijedi za ostale elemente petorke.

Pretpostavimo sada da vrijedi Slutnja o parnosti. Ako je $\gcd(q, 330) = 1$, onda Slutnja o parnosti povlači da su rangovi od E i njezinog q-twista iste parnosti ako i samo ako je $\chi_q(-330) = 1$, gdje je χ_q kvadratni Dirichletov karakter pridručzen kvadratnom polju $\mathbb{Q}(\sqrt{q})$. Posebno, ako je $q \equiv 1$

(mod 4), onda je

$$\chi_q(-330) = \left(\frac{-330}{|q|}\right),$$

gdje $(\frac{\cdot}{\cdot})$ označava Jacobijev simbol. Dobivamo da za sve q-ove koji zadovoljavaju

$$\gcd(q, 330) = 1, \ \ q \equiv 1 \pmod 4 \ \text{ i } \ \left(\frac{-330}{|q|}\right) = 1,$$

q-twist ima neparan rang. Nalazimo da točno 80 klasa ostataka (mod $330 \cdot 4 = 1320$) zadovoljava ove uvjete. Za $q \equiv 3 \pmod 4$, q-twist promatramo kao $(-q)$-twist od (-1)-twista of E. Izračunamo da (-1)-twist ima konduktor $2^4 \cdot 3 \cdot 5 \cdot 11$ i "root number" 1 (tako da je rang uvjetno paran; ali lako se provjeri da je rang zaista jednak 0). Stoga dobivamo da je za sve q-ove koji zadovoljavaju

$$\gcd(q, 330) = 1, \ \ q \equiv 3 \pmod 4 \ \text{ i } \ \left(\frac{-165}{|q|}\right) = -1,$$

rang q-twista neparan. To je zadovoljeno za 40 klasa ostataka (mod $165 \cdot 4$), tj. 80 klasa (mod 1320). Ako je $\gcd(q, 330) = g > 1$, postupamo slično. Stavimo $q = gh$, te tada q-twist promatramo kao h-twist od g-twista od E (ili $(-h)$-twist od $(-g)$-twista). Za $g \in \{\pm 2, \pm 3, \pm 5, \pm 11, \pm 6, \pm 10, \pm 15, \pm 22, \pm 30, \pm 33, \pm 55, \pm 66, \pm 110, \pm 165, \pm 330\}$ izračunamo konduktor i "root number" od g-twista. U svakom od slučajeva dobivamo da je konduktor oblika $2^k \cdot |g| \cdot 330$ za $k \in \{0, 3, 4\}$). U povlači da se uvjeti za q mogu u svakom slučaju napisati u terminima klasa ostataka (mod 1320). Konačno, dobivamo točno 497 klasa ostataka (mod 1320) ($q \equiv i \pmod{1320}$, $i = 1, 7, 9, 10, 11, 18, 21, 22, 23, 30, \ldots,$) koje zadovoljavaju uvjet da je rang od q-twista neparan (promatramo samo one klase čiji elementi nisu djeljivi sa 4, jer nas zanimaju samo kvadratno slobodni brojevi). $\square$

Spomenimo da u promatranoj familiji postoje i krivulje ranga većeg od 1, npr. E_{-21} ima rang 2, E_{-551} ima rang 3, E_{5217} ima rang 4, $E_{19712449}$ ima rang 5, $E_{18427939089}$ ima rang 6.

Primjer 1:

Najmanji prirodan broj $q > 1$ za kojeg gornja konstrukcija daje $D(q)$-petorke je $q = 7$. Imamo twist $7y^2 = x(x + 11)(x + 75)$ s rangom 1 i generatorom $P = (x, y) = (-25, 50)$. On inducira točku $(t, s) = (27/4, 5/2)$ na (4). Sada iz Teorema 2 dobivamo racionalnu $D(7)$-petorku

$$\left\{\frac{137}{40}, \frac{57}{10}, -\frac{47}{40}, -\frac{6}{5}, \frac{45}{8}\right\}.$$

Množeći elemente ove petorke s 40, dobivamo cjelobrojnu $D(11200)$-petorku. Pogledajmo sada točku $2P = (4/7, 414/49)$. Ona inducira točku $(t, s) = (1711/280, 207/490)$ na (4). Sada iz Teorema 2 dobivamo racionalnu $D(7)$-petorku (ovaj puta s pozitivnim članovima)

$$\left\{ \frac{2969}{3680}, \frac{35681}{8280}, \frac{383849}{33120}, \frac{42401}{2070}, \frac{205285}{6624} \right\}.$$