Diofantov i Eulerov problem o skupovima u kojima je $xy + x + y$ uvijek kvadrat

Andrej Dujella

PMF - Matematički odjel
Sveučilište u Zagrebu, Hrvatska
e-mail: duje@math.hr
URL: http://web.math.hr/~duje/

Diofant: Naći brojeve sa svojstvom da produkt svaka dva među njima, uvećan za sumu ta dva broja, daje potpun kvadrat:

$$\{4, 9, 28\} \quad \text{i} \quad \left\{\frac{3}{10}, \frac{7}{10}, \frac{21}{5}\right\}$$

$4{\cdot}9+4+9 = 7^2$, $4{\cdot}28+4+28 = 12^2$, $9{\cdot}28+9+28 = 17^2$

Euler: $\left\{\frac{5}{2}, \frac{9}{56}, \frac{9}{224}, \frac{65}{224}\right\}$

Takvi skupovi se zovu *Eulerove m-torke*.

Pitanja: Postoji li Eulerova

1. *petorka* koja je sastoji od *racionalnih brojeva*?

2. *petorka* koja je sastoji od *pozitivnih racionalnih brojeva*?

3. *četvorka* koja je sastoji od *cijelih brojeva*?

4. *četvorka* koja je sastoji od *prirodnih brojeva*?

Odgovori:

1. $\boxed{\text{DA}}$ (Dujella 1999)

$$\left\{-\frac{27}{40}, \frac{17}{8}, \frac{27}{10}, 9, \frac{493}{40}\right\}$$

(MacLeod 2006)

$$\left\{0, \frac{9}{25}, \frac{64}{25}, 324, \frac{50176}{11449}\right\}$$

2. $\boxed{\text{DA}}$ (D. 2002)

dokaz zasnovan na činjenici da postoji beskonačno mnogo racionalnih točaka na krivulji

$$y^2 = -(x^2 - x - 3)(x^2 + 2x - 12).$$

4. $\boxed{\text{NE}}$ (D. & C. Fuchs 2005)

koristi se veza s *Diofantovim m-torkama*: ako je $\{a_1, \ldots, a_m\}$ Eulerova m-torka, onda je $\{a_1 + 1, \ldots, a_m + 1\}$ $D(-1)$-m-torka, tj. $(a_i+1)(a_j+1)-1 = a_i a_j + a_i + a_j$ je potpun kvadrat za $i \neq j$.

3. $\boxed{??}$

- Ne postoji *Eulerova petorka* koja se sastoji od *cijelih brojeva* [D. & C. Fuchs (2005)].

- Ako postoji *Eulerova četvorka* koja se sastoji od *cijelih brojeva*, onda ona nužno sadrži ili 0 ili -2 [D. & C. Fuchs (2005)].

- Postoji najviše konačno mnogo *Eulerovih četvorki* koje se sastoje od *cijelih brojeva*. Preciznije, ako je $\{a, b, c, d\}$ cjelobrojna Eulerova četvorka, onda je
$\max\{|a|, |b|, |c|, |d|\} < 10^{10^{23}}$
[D. & A. Filipin & C. Fuchs (2007)].

Konstrukcija beskonačne familije Eulerovih petorki s pozitivnim racionalnim elementima

Ekvivalentan problem: Naći racionalne $D(-1)$-petorke s elementima > 1.

Polazna ideja: Interpretirati Eulerovu petorku

$$\left\{-\frac{27}{40}, \frac{17}{8}, \frac{27}{10}, 9, \frac{493}{40}\right\}$$

kao točku na nekoj eliptičkoj krivulji.

Ova Eulerova petorka odgovara $D(-1600)$-petorki

$$\{13, 125, 148, 400, 533\}. \qquad (1)$$

Jednostavna činjenica (Euler; možda već i Diofant):
Ako je $B \cdot C + n = k^2$, onda je $\{B, C, B + C \pm 2k\}$ $D(n)$-trojka.

Petorka (1) ima oblik

$$\{A, B, C, D, z^2\}, \tag{2}$$

gdje je $A = B+C-2k$, $D = B+C+2k$. Ako je $A = a^2-\alpha$, $B = b^2-\alpha$, $C = c^2-\alpha$, $D = d^2-\alpha$, onda će (2) biti $D(\alpha z^2)$-petorka ako i samo ako vrijedi:

$$(b^2-\alpha)(c^2-\alpha)+\alpha z^2 = k^2,$$
$$(a^2-\alpha)(d^2-\alpha)+\alpha z^2 = y^2.$$

Postoji parametarsko rješenje: skup

$$\Big\{\tfrac{1}{3}(x^2+6x-18)(-x^2+2x+2),$$
$$\tfrac{1}{3}x^2(x+5)(-x+3),\ (x-2)(5x+6),$$
$$\tfrac{1}{3}(x^2+4x-6)(-x^2+4x+6),\ 4x^2\Big\}$$

je $D(\frac{16}{9}x^2(x^2-x-3)(x^2+2x-12))$-petorka (za svaki x).

$x = \frac{5}{2} \quad \longmapsto \quad (1).$

$D(-n^2) \quad \longmapsto^{:n} \quad D(-1) \quad \longmapsto^{-1} \quad$ Eulerova

Promotrimo kvartiku

$$Q: \quad y^2 = -(x^2 - x - 3)(x^2 + 2x - 12),$$

s racionalnom točkom $(\frac{5}{2}, \frac{3}{4})$.

Preko supstitucija

$$x = \frac{63s+10t+2619}{18s+4t+2403},$$

$$y = \frac{24s^3-6777s^2-12t^2-34749t+54898479}{(18s+4t+2403)^2},$$

krivulja Q je biracionalno ekvivalentna eliptičkoj krivulji

$$\begin{aligned} E: \quad t^2 &= s^3 - 18981s - 1001700 \\ &= (s-159)(s+75)(s+84). \end{aligned}$$

$E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, T_1, T_2, T_3\}$,
$T_1 = (159, 0)$, $T_2 = (-75, 0)$, $T_3 = (-84, 0)$
$\boxed{\operatorname{rank} E(\mathbb{Q}) = 1}$
$E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}} = <P>$, $P = (2103, -96228)$.

Pet dodatnih uvjeta:

$$\frac{(x^2+6x-18)(-x^2+2x+2)}{4xy} > 1,$$
$$\frac{x(x+5)(-x+3)}{4y} > 1, \ \frac{3(x-2)(5x+6)}{4xy} > 1,$$
$$\frac{(x^2+4x-6)(-x^2+4x+6)}{4xy} > 1, \ \frac{3x}{y} > 1$$

Rješenja:

$$x \in \langle 2.303, 2.306\rangle \cup \langle 2.602, 2.605\rangle, \ y > 0,$$

$x \in \langle -4.605, -4.482\rangle \cup \langle -1.338, -1.303\rangle, \ y < 0.$

U terminima eliptičke krivulje E:

$s \in \langle -79.22, -76.85\rangle \cup \langle 458.64, 937.54\rangle, \ t > 0,$

$s \in \langle -82.09, -79.69\rangle \cup \langle 232.03, 348.77\rangle, \ t < 0.$

Koje točke oblika mP, $T_1 + mP$, $T_2 + mP$, $T_3 + mP$ zadovoljavaju ove nejednakosti?

Parametrizacija pomoću Weierstrassove funkcije: $s = \wp(z)$, $t = \frac{1}{2}\wp'(z)$

Za točke oblika mP, uvjet postaje:

$$\{m \cdot 0.2145...\} \in \langle 0.5362, 0.6782 \rangle.$$

α je iracionalan $\Rightarrow$ razlomljeni djelovi $\{m \cdot \alpha\}$ su gusti u $\langle 0, 1 \rangle$

$\Rightarrow$ beskonačno mnogo racionalnih Eulerovih petorki s pozitivnim elementima

Npr. $m = -2, -3, -11, 12, -16, 17, -25, 26, \ldots$

točka na E	Eulerova petorka
$-2P$	$\left\{\frac{122537388240717681609028093312728053 81}{1335628473872653736133733961581468085 6}, \frac{402280625581345978468093983 33}{202737766604925271257562607 2}, \frac{904102036076757756322317387 35}{264016552841465436885252699 8}, \frac{145924966081583314171992018275332758858 9}{1335628473872653736133733961581468085 6}, \frac{164634788770687616 15}{200378051669604563}\right\}$
$T_3 - 2P$	$\left\{\frac{243840048108266478952509085840250160 17}{1226018751971657626989240363062470220}, \frac{111745345725318807760778453 73}{122557572473080331255380185 2}, \frac{200408761263308135110463918}{200450485329612350005456055}, \frac{287670780013453292618651769213853277 7}{1226018751971657626989240363062470220}, \frac{132925398856151742 2}{200378051669604563}\right\}$

Teorem: (D. & Fuchs (2005)) Ne postoji $D(-1)$-četvorka $\{a,b,c,d\}$ takva da je $2 \leq a < b < c < d$.

Korolari:

- Ne postoji Eulerova četvorka koja se sastoji od prirodnih brojeva.

- Ne postoji $D(-1)$-petorka.

- Ako je $\{a,b,c,d\}$ $D(-1)$-četvorka i $0 < a < b < c < d$, onda je $a = 1$ i $b \geq 65$.

- Ako postoji Eulerova četvorka s cjelobrojnim elementima, onda ona sadrži ili 0 ili -2.

Prethodni rezultati - sljedeće $D(-1)$-trojke se ne mogu proširiti do $D(-1)$-četvorke:

- Mohanty & Ramasamy (1984): $\{1, 5, 10\}$
- Brown (1985): $\{1, 2, 5\}$, $\{17, 26, 37\}$
- Kedlaya (1998): $\{1, 2, 145\}$, $\{1, 2, 4901\}$, $\{1, 5, 65\}$, $\{1, 5, 20737\}$, $\{1, 10, 17\}$, $\{1, 26, 37\}$
- Dujella (1998): $\{1, 2, c\}$
- Filipin (2005): $\{1, 5, c\}$, $\{1, 10, c\}$
- Fujita (2006): $\{1, 17, c\}$, $\{1, 26, c\}$, $\{1, 37, c\}$, $\{1, 50, c\}$

Teorem: (D. & Filipin & Fuchs (2007)) Neka je $\{1, b, c\}$ $D(-1)$-trojka.

(i) Ako je $c > b^9$, onda ne postoji proširenje do $D(-1)$-četvorke $\{1, b, c, d\}$ takvo da je $d > c$.

(ii) Ako je $11b^6 \leq c \leq b^9$, onda se $\{1, b, c\}$ ne može proširiti do $D(-1)$-četvorke.

Pretpostavimo da je $\{1, b, c, d\}$, $1 < b < c < d$, $D(-1)$-četvorka.

(iii) Ako je $b^3 < c < 11b^6$, onda je $c < 10^{238}$, $d < 10^{10^{23}}$.

(iv) Ako je $b^{1.1} < c \leq b^3$, onda je $c < 10^{491}$, $d < 10^{10^{23}}$.

(v) Ako je $3b < c \leq b^{1.1}$, onda je $c < 10^{94}$, $d < 10^{10^{21}}$.

(vi) Ako je $c = 1 + b + 2\sqrt{b-1}$, onda je $c < 10^{74}$, $d < 10^{10^{21}}$.

Korolari:

- Postoji najviše konačno mnogo $D(-1)$-četvorki.

- Postoji najviše konačno mnogo Eulerovih četvorki s cjelobrojnim elementima.

- Ako je $\{a, b, c, d\}$ $D(-1)$-četvorka, onda je $\max\{a, b, c, d\} < 10^{10^{23}}$.

- Postoji najviše 10^{903} $D(-1)$-četvorki.

Ovo su ujedno i prvi netrivijalni rezultati (tj. za brojeve $\not\equiv 2 \pmod 4$) vezani uz sljedeću slutnju:

Slutnja: Ako n nije potpun kvadrat, onda postoji najviše konačno mnogo $D(n)$-četvorki.

Budući svi elementi u $D(-4)$-četvorki moraju biti parni, gornji teorem povlači da je slutnja točna za $n = -1$ i $n = -4$.

Neka je $\{1,b,c\}$ $D(-1)$-trojka, $1<b<c$, te neka su r,s,t prirodni brojevi definirani sa

$$b-1=r^2,\ c-1=s^2,\ bc-1=t^2.$$

Pretpostavimo da postoji prirodan broj $d>c$ tako da je $\{1,b,c,d\}$ $D(-1)$-četvorka. Tada vrijedi:

$$d-1=x^2,\ bd-1=y^2,\ cd-1=z^2,$$

za neke cijele brojeve x,y,z. Eliminirajući d, dobivamo sustav pellovskih jednadžbi

$$\begin{aligned} z^2-cx^2 &= c-1, \\ bz^2-cy^2 &= c-b. \end{aligned}$$

Ovaj sustav pellovskih jednadžbi se može transformirati u konačno mnogo jednadžbi oblika $z = v_m = w_n$, gdje su (v_m) i (w_n) rekurzivni nizovi zadani sa

$$v_0 = z_0,\ v_1 = (2c-1)z_0 + 2scx_0,$$
$$v_{m+2} = (4c-2)v_{m+1} - v_m,$$

$$w_0 = z_1,\ w_1 = (2bc-1)z_1 + 2tcy_1,$$
$$w_{m+2} = (4bc-2)w_{n+1} - w_n,$$

a fundamentalna rješenja zadovoljavaju sljedeće nejednakosti:

$$|x_0| < s,\ 0 < z_0 < c,\ |y_1| < t,\ 0 < z_1 < c.$$

Napomena: Ako je $c \leq b^9$, onda je $z_0 = z_1 = s$, $x_0 = 0,\ y_1 = \pm r$.

Kongruencije::

$$
\begin{aligned}
v_m &\equiv (-1)^m z_0 \pmod{2c},\\
w_n &\equiv (-1)^n z_1 \pmod{2c},\\
v_m &\equiv (-1)^m (z_0 - 2acm^2 z_0 - 2csmx_0) \pmod{8c^2},\\
w_n &\equiv (-1)^n (z_1 - 2bcn^2 z_1 - 2ctny_1) \pmod{8c^2}.
\end{aligned}
$$

metoda kongruencija $\Rightarrow$ ograde odozdo za netrivijalna rješenja

Npr.

Ako je $v_m = w_n$, $n \neq 0, 1$ i $c \geq 11b^6$, onda je $n > c^{1/6}$.

Ako je $v_m = w_n$, $n \neq 0, 1$, $b^{1.1} \leq c < b^3$ i $c > 10^{100}$, onda je $n \geq c^{0.04}$.

Rješenja našeg sustava pellovskih jednadžbi induciraju jako dobre racionalne aproksimacije iracionalnih brojeva $\theta_1 = \sqrt{1 + \frac{1-b}{bc-1}}$ and $\theta_2 = \sqrt{1 + \frac{1}{bc-1}}$:

$$\max\left\{\left|\theta_1 - \frac{bsx}{ty}\right|, \left|\theta_2 - \frac{bz}{ty}\right|\right\} < \frac{b-1}{y^2}.$$

Ako je $c \geq 11b^6$, onda možemo primijeniti Bennettov teorem (Fujitinu modifikaciju) o simultanim racionalnim aproksimacijama kvadratnih korijena bliskih jedinici.

Za $c < 11b^6$, transformiramo eksponencijalnu jednadžbu $v_m = w_n$ u logaritamsku nejednadžbu i primijenimo Bakerovu teoriju linearnih formi u logaritmima algebarskih brojeva (Baker-Wüstholzov ili Matveevljev teorem).

Diofantske aproksimacije $\Rightarrow$ ograde odozgo na rješenja

ograde odozdo i odozgo $\Rightarrow$ kontradikcija (za dovoljno velike c)