STUDENTSKA RUBRIKA

Pellova jednadžba

IVONA MANDIĆ* IVAN SOLDO†

Sažetak. *Članak sadrži riješene primjere i probleme koji se svode na analizu skupa rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ te njenu usku povezanost sa diofantskim aproksimacijama i verižnim razlomcima.*

Ključne riječi: *Pellova jednadžba, verižni razlomak*

Pell's equation

Abstract. *This article contains solved examples and problems which are reduced to the study of the set of solutions of Pell's equation $x^2 - dy^2 = 1$ and their tight connection to diophantine approximation and continued fractions.*

Key words: *Pell's equation, continued fraction*

1. Uvod

Algebarska jednadžba dviju ili više varijabli s cjelobrojnim koeficijentima kod koje se traže cjelobrojna ili racionalna rješenja naziva se diofantska jednadžba. Diofantska jednadžba

$$x^2 - dy^2 = 1 \tag{1}$$

gdje je d prirodan broj koji nije potpun kvadrat, naziva se *Pellova jednadžba*. Ako je d potpun kvadrat, tj. $d = c^2$, $c \in \mathbb{Z}$ onda iz

$$x^2 - dy^2 = (x - cy)(x + cy) = 1$$

slijedi

$$(x - cy) = (x + cy) = \pm 1.$$

U tom slučaju imamo trivijalna rješenja $x = \pm 1$, $y = 0$.
Jednadžba je dobila ime po engleskom matematičaru Johnu Pellu (1611. - 1685.)

*studentica Odjela za matematiku, Sveučilište u Osijeku, Trg Ljudevita Gaja 6, HR-31 000 Osijek, imandic@mathos.hr

†Odjel za matematiku, Sveučilište u Osijeku, Trg Ljudevita Gaja 6, HR-31 000 Osijek, isoldo@mathos.hr

kojemu je Leonhard Euler (1707. - 1783.), po svemu sudeći, pogrešno pripisao zasluge za njezino rješavanje. Neke pojedinačne jednadžbe ovog tipa nalaze se u tekstovima starogrčkih matematičara Arhimeda (287. pr. Kr. - 212. pr. Kr.) i Diofanta (200. po. Kr. - 284. po. Kr.). Ipak, prvi su ih sustavno proučavali srednjovjekovni indijski matematičari. Europski matematičari koji su dali metode za rješavanje Pellovih jednadžbi su Pierre de Fermat (1601. - 1665.), Leonhard Euler (1707. - 1783.) i Joseph Louis Lagrange (1736. - 1813.) koji je prvi dao i strogi dokaz korektnosti predložene metode. U članku ćemo pokazati neke primjere i probleme koji se svode na rješavanje Pellove jednadžbe.

2. Pellova jednadžba $x^2 - dy^2 = 1$

Pri rješavanju Pellove jednadžbe prirodno je pitati se koliko ona ima rješenja. Neka je $S = \{(x_n, y_n) : n, x_n, y_n \in \mathbb{N}\}$ skup rješenja Pellove jednadžbe. Uređeni par (x_1, y_1), $x_1 = min\{x_n : x_n \in \mathbb{N}\}$, $y_1 = min\{y_n : y_n \in \mathbb{N}\}$ koji zadovoljava jednadžbu (1) zove se njeno *fundamentalno rješenje.* To je najmanje rješenje te iste jednadžbe u prirodnim brojevima. Ponekad ga označavamo i $x_1 + y_1\sqrt{d}$. Sljedeći teorem daje nam broj rješenja i odnos fundamentalnog i svih drugih rješenja Pellove jednadžbe (1).

Teorem 1. *Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Ako je (x_1, y_1) njeno fundamentalno rješenje, onda su sva rješenja ove jednadžbe u prirodnim brojevima dana sa*

$$x_n \quad + \quad y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}. \tag{2}$$

Dokaz teorema može se pronaći u [1].

Primjer 1. *Nađite sva rješenja Pellove jednadžbe $x^2 - 3y^2 = 1$.*

Rješenje:

Fundamentalno rješenje Pellove jednadžbe $x^2 - 3y^2 = 1$ je $(x_1, y_1) = (2, 1)$. Prema Teoremu 2.1 sva rješenja dana su sa

$$x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n, \quad n \in \mathbb{N}$$

pa jednadžba ima beskonačno mnogo rješenja u $\mathbb{N}$.

◇

Iz (2) lako dobivamo

$$\begin{aligned}(x_{n+1} + y_{n+1}\sqrt{d})(x_1 + y_1\sqrt{d}) &= x_{n+2} + y_{n+2}\sqrt{d},\\ (x_{n+1} + y_{n+1}\sqrt{d})(x_1 - y_1\sqrt{d}) &= x_n + y_n\sqrt{d}.\end{aligned}$$

Sada izjednačavanjem slobodnih članova imamo

$$\begin{aligned}x_{n+2} &= x_1x_{n+1} + dy_1y_{n+1},\\ x_n &= x_1x_{n+1} - dy_1y_{n+1},\end{aligned}$$

odakle zbrajanjem dobivamo rekurziju $x_{n+2} = 2x_1x_{n+1} - x_n$. Analognim računom, tj. izjednačavanjem članova uz $\sqrt{d}$ i zbrajanjem dobivamo rekurziju $y_{n+2} = 2x_1y_{n+1} - y_n$. Za početnu iteraciju uzima se trivijalno rješenje jednadžbe (1), $(x_0, y_0) = (1, 0)$.

Zadatak 1. *Neka je (x_n, y_n) rastući niz rješenja Pellove jednadžbe (1) u prirodnim brojevima. Pokažite da za sve prirodne brojeve m, n vrijedi*

$$\begin{aligned} x_{n+m} &= x_m x_n + d y_m y_n, \\ y_{n+m} &= x_m y_n + y_m x_n, \\ \frac{x_{2m}}{y_{2m}} &= \frac{1}{2}\left(\frac{x_m}{y_m} + \frac{d y_m}{x_m}\right). \end{aligned}$$

Rješenje:
Dokaz provedimo indukcijom po m. Uvrštavanjem $m = 1$ u prve dvije jednakosti dobivamo

$$x_{n+1} = x_1 x_n + d y_1 y_n,$$

$$y_{n+1} = x_1 y_n + y_1 x_n.$$

Prema prethodnom računu, izjednačavanjem slobodnih članova i članova uz $\sqrt{d}$, gornje jednakosti vrijede za svaki prirodni broj n. Pretpostavimo da jednakosti vrijede za $m = k$, tj.

$$x_{n+k} = x_k x_n + d y_k y_n,$$

$$y_{n+k} = x_k y_n + y_k x_n.$$

Pokažimo istinitost za $m = k + 1$. Koristeći rezultate baze i pretpostavke indukcije slijedi

$$x_{n+k+1} = x_1 x_{n+k} + d y_1 y_{n+k} = x_1(x_k x_n + d y_k y_n) + d y_1 (x_k y_n + y_k x_n).$$

Množenjem i grupiranjem članova dobivamo

$$x_{n+k+1} = x_n(x_1 x_k + d y_1 y_k) + d y_n (x_1 y_k + y_1 x_k) = x_{k+1} x_n + d y_{k+1} y_n.$$

Time je dokazana prva jednakost. Analognim računom lako se pokaže i istinitost druge jednakosti, tj.

$$y_{n+k+1} = x_{k+1} y_n + y_{k+1} x_n.$$

Posljednju jednakost dobivamo dijeljenjem prve jednakosti drugom, uz uvjet $m = n$.

$$\frac{x_{2m}}{y_{2m}} = \frac{x_m x_m + d y_m y_m}{2 x_m y_m} = \frac{1}{2}\left(\frac{x_m}{y_m} + \frac{d y_m}{x_m}\right).$$

◇

Zadatak 2. *Neka su m i d proizvoljni prirodni brojevi i d nije potpun kvadrat. Pokažite da postoji beskonačno mnogo rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ pri čemu je y djeljiv s m.*
Rješenje:
Neka je y djeljiv s m. To znači da postoji $k \in \mathbb{Z}$ takav da je $y = mk$, $m \in \mathbb{N}$. Trebamo pokazati da Pellova jednadžba $x^2 - dy^2 = 1$ uz taj uvjet ima beskonačno mnogo rješenja. Uvrštavanjem dobivamo jednadžbu

$$x^2 - d(mk)^2 = 1.$$

Sada, kvadriranjem i grupiranjem imamo

$$x^2 - (dk^2)m^2 = 1.$$

Označimo $d' := dk^2$. Dobivamo jednadžbu

$$x^2 - d'm^2 = 1, \tag{3}$$

d' nije potpun kvadrat (jer d nije potpun kvadrat). Primjenom Teorema 2.1 jednadžba (3) ima beskonačno mnogo rješenja u $\mathbb{N}$. Time je tvrdnja zadatka u potpunosti pokazana.

◇

Zadatak 3. *Pokažite da postoji beskonačno mnogo prirodnih brojeva n sa svojstvom da je suma prvih n prirodnih brojeva jednaka kvadratu nekog prirodnog broja. Nađite barem 2 prirodna broja s tim svojstvom.*
Rješenje:
Vrijedi

$$\sum_{i=1}^{n} i = m^2,$$

tj.

$$\frac{n(n+1)}{2} = m^2.$$

Sada, množenjem s 8 dobivamo

$$4n^2 + 4n = 8m^2.$$

Svođenjem na potpuni kvadrat imamo

$$(2n+1)^2 - 1 = 8m^2,$$

odnosno

$$(2n+1)^2 - 8m^2 = 1.$$

Uvedimo supstituciju $x = 2n+1$, $y = m$. Sada se problem svodi na određivanje broja rješenja Pellove jednadžbe

$$x^2 - 8y^2 = 1.$$

Prema Teoremu 2.1 gornja jednadžba ima beskonačno mnogo rješenja u $\mathbb{N}$. Fundamentalno rješenje je očito $(x_1, y_1) = (3, 1)$. Stoga iz $2n_1 + 1 = x_1$ slijedi $n_1 = 1$, $m_1 = 1$. Zaista, vrijedi $1 = 1^2$.
Sva rješenja jednadžbe $x^2 - 8y^2 = 1$ dana su sa

$$x_k + y_k\sqrt{8} = (3 + \sqrt{8})^k, \quad k \in \mathbb{N}.$$

Neka je npr. k = 2. Sada je

$$x_2 + y_2\sqrt{8} = (3+\sqrt{8})^2 = 17 + 6\sqrt{8}.$$

Stoga je $2n_2 + 1 = x_2 = 17$ pa je $n_2 = 8$, $m_2 = 6$. Zaista, vrijedi $\sum_{i=1}^{8} i = 6^2$. Analogno, možemo pronaći beskonačno mnogo parova (n, m) tako da je $\sum_{i=1}^{n} i = m^2$.

$\diamond$

Teorem 2.1 nam pokazuje kako možemo generirati sva rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ ukoliko znamo njeno fundamentalno rješenje. Međutim, pitanje je kako naći to fundamentalno rješenje? Jedna mogućnost je uvrštavajući redom $y = 1, 2, 3, \ldots$ i provjeravajući je li $dy^2 + 1$ potpun kvadrat. No, već i za relativno male d - ove fundamentalno rješenje može biti vrlo veliko. Primjerice, za $d = 94$ fundamentalno rješenje je $2143295 + 221064\sqrt{94}$. Stoga je potrebno naći efikasniji način za nalaženje fundamentalnog rješenja.
Jedan način nalaženja fundamentalnog rješenja je korištenje verižnih razlomaka. Naime, svako netrivijalno rješenje jednadžbe $x^2 - dy^2 = 1$ inducira jako dobru aproksimaciju iracionalnog broja $\sqrt{d}$. Zaista,

$$\begin{aligned}\left|\sqrt{d} - \frac{x}{y}\right| &= \left|\frac{x - y\sqrt{d}}{y}\right| = \left|\frac{x - y\sqrt{d}}{y}\right| \cdot \left|\frac{x + y\sqrt{d}}{x + y\sqrt{d}}\right| \\ &= \left|\frac{x^2 - dy^2}{xy + y^2\sqrt{d}}\right| = \frac{1}{y|x + y\sqrt{d}|} < \frac{1}{2\sqrt{d}y^2}.\end{aligned}$$

Poznato je da se sve jako dobre racionalne aproksimacije realnog broja mogu dobiti iz njegovog razvoja u verižni razlomak.
Neka je $\alpha \in \mathbb{R}$. Izraz oblika

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}$$

gdje su $a_0 \in \mathbb{Z}$, $a_1, a_2, \cdots \in \mathbb{N}$, zove se razvoj broja α u *jednostavni verižni razlomak.* Verižni razlomak kraće zapisujemo u obliku $[a_0; a_1, a_2, \ldots]$. Brojevi $a_0, a_1, \ldots$ zovu se *parcijalni kvocijenti* i definiraju se s:

$$a_0 = \lfloor\alpha\rfloor, \alpha = a_0 + \frac{1}{\alpha_1}, a_1 = \lfloor\alpha_1\rfloor, \alpha_1 = a_1 + \frac{1}{\alpha_2}, \ldots$$

Postupak se nastavlja sve dok je $a_k \neq \alpha_k$. Razvoj u jednostavni verižni razlomak broja α je konačan ako i samo ako je α racionalan broj. Racionalne brojeve

$$\frac{p_k}{q_k} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k}}} = [a_0; a_1, \ldots, a_k]$$

zovemo *konvergente verižnog razlomka.* Brojnici i nazivnici konvergenti zadovoljavaju sljedeće rekurzije:

$$\begin{aligned} p_{n+2} &= a_{n+2}p_{n+1} + p_n,\ p_0 = a_0,\ p_1 = a_0a_1 + 1,\ (p_{-1} = 1, p_{-2} = 0), && (4)\\ q_{n+2} &= a_{n+2}q_{n+1} + q_n,\ q_0 = 1,\ q_1 = a_1,\ (q_{-1} = 0, p_{-2} = 1). && (5) \end{aligned}$$

Za svako rješenje Pellove jednadžbe $x^2 - dy^2 = 1$, $\frac{x}{y}$ je neka konvergenta u razvoju od $\sqrt{d}$ u verižni razlomak. Broj $\sqrt{d}$ je kvadratna iracionalnost pa mu je razvoj periodičan. On ima razvoj oblika

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{l-1}, 2a_0}]$$

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$. Precizni rezultati i veze verižnih razlomaka s diofantskim aproksimacijama i jednadžbama mogu se naći u [1] i [2].
Sada navedimo algoritam za razvoj kvadratnih iracionalnosti u verižni razlomak: Neka je α kvadratna iracionalnost. Prikažimo je u obliku $\alpha = \frac{s_0+\sqrt{d}}{t_0}$ gdje su $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, d nije potpun kvadrat i $t_0|(d - s_0^2)$. Ako je $\alpha = \sqrt{d}$, onda je $s_0 = 0$, $t_0 = 1$. Brojeve a_i računamo rekurzivno na sljedeći način:

$$a_i = \lfloor \frac{s_i + a_0}{t_i} \rfloor,\ s_{i+1} = a_i t_i - s_i,\ t_{i+1} = \frac{d - s_{i+1}^2}{t_i}.$$

Može se pokazati da je razvoj u verižni razlomak periodičan i da je duljina perioda $l(d) < 2d$ [vidi [1]]. Koristeći razvoj u verižni razlomak pokazuje se da Pellova jednadžba uvijek ima beskonačno rješenja. Bez dokaza navedimo sljedeći teorem:

Teorem 2. *Neka je l duljina perioda u razvoju $\sqrt{d}$.*
Ako je l paran, sva rješenja od $x^2 - dy^2 = 1$ dana su sa $(x, y) = (p_{nl-1}, q_{nl-1})$, $n \in \mathbb{N}$. Posebno, fundamentalno rješenje je (p_{l-1}, q_{l-1}).
Ako je l neparan, sva rješenja od $x^2 - dy^2 = 1$ dana su sa $(x, y) = (p_{2nl-1}, q_{2nl-1})$, $n \in \mathbb{N}$. Posebno, fundamentalno rješenje je (p_{2l-1}, q_{2l-1}).

Primjer 2. *Razvijte $\sqrt{15}$ u verižni razlomak.*
Rješenje:
$s_0 = 0,\ t_0 = 1,\ a_0 = 3,$

$s_1 = a_0t_0 - s_0 = 3$, $t_1 = \frac{15-s_1^2}{t_0} = 6$, $a_1 = \lfloor \frac{s_1+a_0}{t_1} \rfloor = \lfloor \frac{3+3}{6} \rfloor = 1,$

$s_2 = 3$, $t_2 = 1$, $a_2 = \lfloor \frac{3+3}{1} \rfloor = 6,$

$s_3 = 3$, $t_3 = 6.$

Vidimo da je $(s_1, t_1) = (s_3, t_3)$ pa je $\sqrt{15} = [3, \overline{1, 6}]$.

◇

Primjer 3. *Razvijte $\sqrt{29}$ u verižni razlomak.*
Rješenje:
$s_0 = 0,\ t_0 = 1,\ a_0 = 5,$

$s_1 = a_0t_0 - s_0 = 5$, $t_1 = \frac{29-s_1^2}{t_0} = 4$, $a_1 = \lfloor \frac{s_1+a_0}{t_1} \rfloor = \lfloor \frac{5+5}{4} \rfloor = 2,$

$s_2 = 3$, $t_2 = 5$, $a_2 = \lfloor \frac{3+5}{5} \rfloor = 1,$

$s_3 = 2$, $t_3 = 5$, $a_3 = \lfloor \frac{2+5}{5} \rfloor = 1$,

$s_4 = 3$, $t_4 = 4$, $a_4 = \lfloor \frac{3+5}{4} \rfloor = 2$,

$s_5 = 5$, $t_5 = 1$, $a_5 = \lfloor \frac{5+5}{1} \rfloor = 10$,

$s_6 = 5$, $t_6 = 4$.

Jer je $(s_1, t_1) = (s_6, t_6)$, vrijedi $\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$.

◇

Zadatak 4. *Nađite sva rješenja jednadžbe $x^2 - 15y^2 = 1$ za koja je $1 < x < 1000$.*
Rješenje:
Prema prethodnom primjeru je $\sqrt{15} = [3, \overline{1, 6}]$. Dakle, period $l = 2$ je paran. Najmanje rješenje jednadžbe $x^2 - 15y^2 = 1$ je $(x_1, y_1) = (4, 1)$. Nadalje je

$$\begin{aligned} x_2 &= 8 \cdot 4 - 1 = 31,\ y_2 = 8, \\ x_3 &= 8 \cdot 31 - 4 = 244,\ y_3 = 63, \end{aligned}$$

x_4 je već veći od 1000. Prema tome, sva rješenja koja zadovoljavaju traženi uvjet su $(x, y) = (4, 1), (31, 8), (244, 63)$.

◇

Zadatak 5. *Nađite najmanje rješenje jednadžbe $x^2 - 29y^2 = 1$ u prirodnim brojevima.*
Rješenje:
Iz razvoja $\sqrt{29}$ u verižni razlomak očito je period $l = 5$ neparan. Prema tome fundamentalno rješenje jednadžbe je $(x_1, y_1) = (p_{2l-1}, q_{2l-1}) = (p_9, q_9)$. Računamo:
$p_0 = a_0 = 5$, $q_0 = 1$,

$p_1 = a_0 a_1 + 1 = 11$, $q_1 = a_1 = 2$,

$p_2 = a_2 p_1 + p_0 = 16$, $q_2 = a_2 q_1 + q_0 = 3$,

$p_3 = a_3 p_2 + p_1 = 27$, $q_3 = a_3 q_2 + q_1 = 5$,

$p_4 = 70$, $q_4 = 13$,

$p_5 = 727$, $q_5 = 135$,

$p_6 = 1524$, $q_6 = 283$,

$p_7 = 2251$, $q_7 = 418$,

$p_8 = 3775$, $q_8 = 701$,

$p_9 = 9801$, $q_9 = 1820$.

Stoga je najmanje rješenje $(x_1, y_1) = (9801, 1820)$.

◇

Literatura

[1] A. DUJELLA, *Diofantske jednadžbe*, Skripta, PMF - matematički odjel, Sveučilište u Zagrebu, Zagreb, 2007.

[2] A. DUJELLA, *Uvod u teoriju brojeva*, Skripta, PMF - matematički odjel, Sveučilište u Zagrebu, Zagreb, 2006.

[3] N. P. SMART, *The Algorithmic Resolution to Diophantine Equations*, Cambridge University Press, 1998.