Pellove i Pellovske jednadžbe

Granoša, Ivana

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij Matematika

Ivana Granoša

Pellove i pellovske jednadžbe

Završni rad

Osijek, 2022.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij Matematika

Ivana Granoša

Pellove i pellovske jednadžbe

Završni rad

Voditelj: Izv. prof. dr. sc. Mirela Jukić Bokun

Osijek, 2022.

Sažetak: Kroz ovaj rad upoznajemo i obrađujemo Pellove jednadžbe, tražimo njihova rješnja, razmatramo razne slučaje postojanja rješenja i njihov oblik. Bitnu ulogu u radu čine i verižni razlomci pomoću kojih također možemo tražiti rješenja ovih jednadžbi. Naposljetku proučavamo pellovsku jednadžbu, dodajemo nove pojmove i svojstva. Cijeli rad prožet je primjerima kojima bolje predočavamo teoreme i upotrebe određenih algoritama.

Ključne riječi: verižni razlomci, Pellove jednadžbe, pellovske jednadžbe

Pell's and Pellian equations

Abstract: Through this paper we will get to know and elaborate Pell's equations and look for their solutions. We will consider some cases of the existence of solution and their form. Continued fractions have an important role in the paper because using them we can also find solutions for these equation. Finally, we will study Pellian equation with some new and special concept. Entire paper contains examples that better ilustrate theorems and applications.

Keywords: continued fractions, Pell's equation, Pellian equation

Sadržaj

Uvod

Algebarsku jednadžbu s dvije ili više nepoznanica čiji su koeficijenti i rješenja cjelobrojni nazivamo diofantska jednadžba. U ovom radu naglasak će biti na posebnom obliku diofantskih jednadžbi drugog reda - *Pellovim jednadžbama.* Iako je ovaj tip jednadžbi dobio ime po Johnu Pellu - engleskom matematičaru, njemu ne možemo prepisati zasluge za rješavanje ove jednadžbe. Štoviše, povijest ovih jednadžbi započela je davno prije Pellovog vremena. Arhimed je jedan od prvih matematičara koji se bavio ovakvim tipom jednadžbi, a poznati Arhimedov problem stoke u kojem se prebrojavaju krave i bikovi različitih boja bazira se na rješavanju Pellovih jednadžbi. Sredovjekovni indijski matematičar Brahmagupta također je proučavao jednadžbe ovog oblika, te ćemo i kasnije u radu spomenuti Brahmaguptino kompoziciono pravilo u obliku propozicije. Tek u 17. stoljeću Pierre de Fermat izazvao je poznate europske matematičare da riješe Pellovu jednadžbu, a William Brouncker bio je prvi kojemu je to pošlo za rukom.

Prvo ćemo se upoznati s verižnim razlomcima - razlomcima zanimljivog izgleda i široke primjene. Kako bismo razvili racionalan broj u verižni razlomak trebat ćemo se prisjetiti Euklidovog algoritma, što ćemo dodatno pokazati i na primjeru radi lakšeg shvaćanja. Poseban značaj dat ćemo periodskim verižnim razlomcima koje ćemo kasnije povezivati s Pellovim jednadžbama.

Kako i sam naslov rada kaže, glavna tema bit će Pellove jednadžbe. Naučit ćemo uz koje uvjete ova jednadžba ima rješenja, a uz koje nema. Ukoliko jednadžba ima rješenja, prirodno nam se postavljaju pitanja poput: *"Ima li jednadžba konačno ili beskonačno mnogo rješenja?"*, ili pak *"Kojeg su oblika rješenja?"*. Na ta, i na još puno pitanja dat ćemo odgovore kroz cijeli rad.

U posljednjem poglavlju obrađujemo pellovske jednadžbe - nešto općenitiji oblik Pellovih jednadžbi. Proučavat ćemo njihova rješenja i vezu s rješenjima Pellove jednadžbe, te na primjeru pokazati postupak rješavanja.

1. Verižni razlomci

U ovom ćemo se poglavlju upoznati s verižnim razlomcima, njihovim osnovnim svojstvima i primjenama. Posebno ćemo istaknuti periodske verižne razlomke i njihova svojstva važna za rješavanje Pellovih jednadžbi.

1.1. Uvod u verižne razlomke

Neka je α realan broj, te definirajmo $a_0 := \lfloor \alpha \rfloor$.

Ako je $a_0 \neq \alpha$, neka je $\alpha = a_0 + \dfrac{1}{\alpha_1}$ (uočimo da je tada $\alpha_1 = \frac{1}{\alpha - a_0}$) i $a_1 = \lfloor \alpha_1 \rfloor$.
Ako je $a_1 \neq \alpha_1$, neka je $\alpha_1 = a_1 + \dfrac{1}{\alpha_2}$ i $a_2 = \lfloor \alpha_2 \rfloor$.

Postupak nastavimo analogno sve dok ne dođemo do prirodnog broja m (ako postoji) takvog da je $a_m = \alpha_m$. Tada je

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

i taj izraz nazivamo ***razvoj broja α u verižni razlomak***.

Napomena 1.1. *Razvoj broja α u verižni razlomak je konačan ako i samo ako je α racionalan broj. U suprotnom, ako je α iracionalan broj, tada je razvoj u verižni razlomak beskonačan.*

Napomena 1.2. *Izraz (1) možemo pisati i kao $\alpha = [a_0, a_1, \ldots, a_m]$. Brojevi $a_0, a_1, \ldots, a_m$ nazivaju se parcijalni kvocijenti.*

Primjer 1.1. *Razvijmo broj $\frac{163}{52}$ u verižni razlomak.*

Prema gore definiranom postupku, za $\alpha = \frac{163}{52}$ imamo da je $a_0 = \lfloor \frac{163}{52} \rfloor = 3$, te $\alpha_1 = \frac{1}{\alpha - a_0} = \frac{52}{7}$. Zatim, $a_1 = 7$ i $\alpha_2 = \frac{7}{3}$, $a_2 = 2$. Nadalje, $\alpha_3 = 3$ i uočavamo da je sada i $a_3 = \alpha_3 = 3$, što znači da stajemo s postupkom.

Dakle, zapis broja $\frac{163}{52}$ u verižni razlomak je sljedeći:

$$\frac{163}{52} = 3 + \cfrac{1}{7 + \cfrac{1}{2 + \cfrac{1}{3}}}.$$

Kraće, možemo pisati i $\dfrac{163}{52} = [3, 7, 2, 3]$.

Prisjetimo li se Euklidovog algoritma, na puno lakši i elegantniji način možemo doći do parcijalnih kvocijenata koji su nam potrebni da bismo racionalni broj razvili u verižni razlomak.

Neka je $\alpha \in \mathbb{Q}$. Tada postoje $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ takvi da je $\alpha = \frac{b}{a}$. Imamo:

$$\begin{aligned}
b &= aq_1 + r_1, & 0 < r_1 < a, \qquad (2)\\
a &= r_1 q_2 + r_2, & 0 < r_2 < r_1, \qquad (3)\\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n q_{n+1}. & \qquad (4)
\end{aligned}$$

Uočimo da iz (2) slijedi da je $\frac{b}{a} = q_1 + \frac{r_1}{a}$ i $q_1 = \lfloor \frac{b}{a} \rfloor = a_0$. Iz drugog retka Euklidovog algoritma, odnosno iz (6) imamo $\frac{a}{r_1} = q_2 + \frac{r_2}{r_1}$, tj. $q_2 = \lfloor \frac{a}{r_1} \rfloor = a_1$.
Analogno nastavimo, te je iz (4) $\frac{r_{n-1}}{r_n} = q_{n+1} = \lfloor \frac{r_{n-1}}{r_n} \rfloor = a_m$.
Dobivamo da je $\alpha = [q_1, q_2, \ldots, q_{n+1}]$.

Vratimo li se sada na Primjer 1.1, koristeći Euklidov algoritam također dobivamo razvoj broja $\frac{163}{52}$ u verižni razlomak:

$$\begin{aligned}
163 &= 52 \cdot \mathbf{3} + 7,\\
52 &= 7 \cdot \mathbf{7} + 3,\\
7 &= 3 \cdot \mathbf{2} + 1,\\
2 &= 1 \cdot \mathbf{3},
\end{aligned}$$

pa je

$$\frac{163}{52} = [3, 7, 2, 3]\,.$$

Napomena 1.3. *Ako je dan razvoj broja α u verižni razlomak, onda se racionalni broj definiran s*

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$$

naziva n-ta konvergenta u razvoju broja α u verižni razlomak.

Vrijede sljedeće tvrdnje:

Teorem 1.1. ([2]) *Brojevi p_n, q_n, pri čemu je $n \geq 2$, zadovoljavaju sljedeće rekurzije:*

$$\begin{aligned}
p_n &= a_n p_{n-1} + p_{n-2}, \quad p_0 = a_0, \quad p_1 = a_0 a_1 + 1,\\
q_n &= a_n q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_1 = a_1.
\end{aligned}$$

Teorem 1.2. ([2]) *Za $n \geq 1$ vrijedi: $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$.*

Korolar 1.1. ([5]) *Za $n \geq 1$ vrijedi: $(p_n, q_n) = 1$.*

U gornjim smo razmatranjima već naveli da razvoj u verižni razlomak može biti i beskonačan, a idući teorem govori nam kako tada zapisujemo racionalan broj α.

Teorem 1.3. ([5]) *Ako je $\alpha \in \mathbb{I}$, onda je*

$$\lim_{n \to +\infty} \frac{p_n}{q_n} = \alpha.$$

Tada α pišemo kao: $\alpha = [a_0, a_1, a_2, \dots]$.

Vidimo da kovergente zapravo aproksimiraju broj α, a nas zanima nas koliko će dobra ta aproksimacija biti. Sljedećim ***zakonom najboljih aproksimacija*** pronaći ćemo najbolju aproksimaciju od α. Detaljniji raspis ovog zakona uz primjere može se pronaći u [5].

Teorem 1.4. ([2]) *Za $1 \leq q \leq q_n$, $p \in \mathbb{Z}$ vrijedi:*

$$|\alpha q - p| \geq |\alpha q_{n-1} - p_{n-1}| > |\alpha q_n - p_n|.$$

Uočimo da je tada $\frac{p_{n-1}}{q_{n-1}}$ najbolja aproksimacija od α.

Sljedeća tvrdnja bitna je za dalje i pozivat ćemo se na nju nešto kasnije u radu.

Teorem 1.5. ([2]) *Neka su $p, q \in \mathbb{Z}, q \geq 1$ i $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$. Tada je $\frac{p}{q}$ neka konvergenta od α.*

1.2. Periodski verižni razlomci

Narednih nekoliko definicija i teorema ključne su za daljnje razumijevanje rada te za lakše pronalaženje rješenja Pellovih jednadžbi koje ćemo obraditi u idućem poglavlju.

Definicija 1.1. *Za beskonačni verižni razlomak $[a_0, a_1, a_2, \dots]$ kažemo da je **periodski** ako postoje cijeli broj $k \geq 0$ i prirodni broj m takvi da je $a_{m+n} = a_n$, za svaki $n \geq k$. Najmanji takav broj m nazivamo **periodom** verižnog razlomka i pišemo*

$$[a_0, a_1, \dots] = [a_0, a_1, \dots, a_{k-1}, \overline{a_k, a_{k+1}, \dots, a_{k+m-1}}].$$

Primjer 1.2. *Odredimo razvoj broja $\sqrt{3}$ u jednostavni verižni razlomak.*

Dakle, $\alpha = \sqrt{3}$, $a_0 = \lfloor \sqrt{3} \rfloor = 1$.
Nadalje,

$$\alpha_1 = \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2} \implies a_1 = \lfloor \alpha_1 \rfloor = 1$$

i $\alpha_2 = \sqrt{3} + 1$, te je $a_2 = \lfloor \alpha_2 \rfloor = 2$, $\alpha_3 = \frac{\sqrt{3}+1}{2}$.
Nastavimo li analogno, parcijalni kvocijenti naizmjence će se ponavljati, tj. 1 i 2 periodski će se ponavljati. Stoga,

$$\sqrt{3} = [1, 1, 2, 1, 2, 1, 2, \dots] = \left[1, \overline{1, 2}\right].$$

Definicija 1.2. *Za iracionalan broj α kažemo da je **kvdratna iracionalnost** ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Primijetimo, ako je α kvadratna iracionalnost, tada je α oblika $\frac{a\pm\sqrt{b}}{c}$, pri čemu je b prirodan broj različit od potpunog kvadrata, a $c \neq 0$.

Teorem 1.6. (Euler, Lagrange, [2]) *Iracionalan broj α ima periodski razvoj u jednostavni verižni razlomak ako i samo ako je α kvadratna iracionalnost.*

Ovaj teorem nećemo dokazivati, već ćemo samo iskoristiti njegovu konstruktivnost koja nam daje algoritam za razvoj broja $\alpha_0 = \frac{s_0+\sqrt{d}}{t_0}$ u verižni razlomak.
Neka je d prirodan broj koji nije potpun kvadrat i $\alpha_0 = \frac{s_0+\sqrt{d}}{t_0}$ kvadratna iracionalnost. Za $i \in \mathbb{N}_0$ imamo:

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

Ako su $s_i, t_i > 0$, onda vrijedi

$$\left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor = \left\lfloor \frac{s_i + \lfloor \sqrt{d} \rfloor}{t_i} \right\rfloor$$

Iskoristimo ovaj algoritam na sljedećem primjeru.

Primjer 1.3. *Razvijmo broj $\alpha_0 = \frac{25+\sqrt{53}}{22}$ u verižni razlomak.*

Vidimo da je $s_0 = 25$, $t_0 = 22$, $d = 53$ te $\lfloor \sqrt{53} \rfloor = 7$. Tada je

$$a_0 = \lfloor \alpha_0 \rfloor = \left\lfloor \frac{25 + \sqrt{53}}{22} \right\rfloor = 1.$$

Zatim imamo $\quad s_1 = a_0 t_0 - s_0 = 1 \cdot 22 - 25 = -3, \quad t_1 = \frac{d-s_1^2}{t_0} = \frac{53-9}{22} = 2$, te

$$a_1 = \lfloor \alpha_1 \rfloor = \left\lfloor \frac{-3 + \sqrt{53}}{2} \right\rfloor = 2.$$

Nadalje je $\quad s_2 = 7, \quad t_2 = 2 \quad$ i

$$a_2 = \lfloor \alpha_2 \rfloor = \left\lfloor \frac{7 + \sqrt{53}}{2} \right\rfloor = 7,$$

te $\quad s_3 = 7, \quad t_3 = 2.$

Uočimo da vrijedi $s_3 = s_2$ i $t_3 = t_2$, pa onda znamo i da mora biti $a_3 = a_2$.

Nastavimo li dalje s algoritmom, dobivat ćemo jednake rezultate iznova, te zaključujemo da α možemo pisati kao

$$\alpha = [1, 2, 7, 7, 7, \ldots], \text{ tj. } \quad \alpha = \left[1, 2, \overline{7}\right].$$

2. Pellove jednadžbe

2.1. Upoznavanje s Pellovim jednadžbama

Definicija 2.1. *Diofantska jednadžba*

$$x^2 - dy^2 = 1,$$

pri čemu je $d \in \mathbb{N}$ i d nije potpun kvadrat, naziva se ***Pellova jednadžba****.*

Napomena 2.1. *Ako je d cijeli broj za koji vrijedi $d < 0$ ili je d potpun kvadrat, tada gornja jednadžba ima konačno mnogo rješenja. Kasnije u radu ćemo iskazati i dokazati lemu kojom tvrdimo da Pellova jednadžba ima beskonačno mnogo rješenja u prirodnim brojevima.*

Promotrimo sljedeće:

Neka je a bilo koji realni broj. Podijelimo interval $[0, 1\rangle$ na t jednakih dijelova tako da je u svakom podintervalu lijevi rub uključen, a desni isključen.

Neka je sada $y \in \mathbb{Z}$, $y \geq 0$, te neka je x najmanji cijeli broj za koji vrijedi $x \geq ay$. Tada imamo

$$0 \leq x - ay < 1.$$

Stavljajući redom $y = 0, 1, \ldots, t$, prema Dirichletovom principu[1] dobivamo $t + 1$ brojeva oblika $x - ay$ koji svi pripadaju intervalu $[0, 1\rangle$. Kako imamo t podintervala, to barem jedan podinterval sadrži barem dva broja oblika $x - ay$. Shodno tome, postoji prirodan broj $h \leq t$ i cijelih brojevi, $x^{'}, y^{'}, x^{''}, y^{''}$ takvi da je

$$\frac{h-1}{t} \leq x^{'} - ay^{'} < \frac{h}{t}, \qquad \frac{h-1}{t} \leq x^{''} - ay^{''} < \frac{h}{t}.$$

Stavimo li $x = x^{''} - x^{'}$ i $y = y^{''} - y^{'}$, dobivamo

$$|x - ay| < \frac{1}{t}. \tag{5}$$

Ako pretpostavimo da je $y^{''} > y^{'}$, tada je y neki od brojeva $0, 1, \ldots, t$, te nejednakost (5) možemo pisati i kao

$$\left|\frac{x}{y} - a\right| < \frac{1}{yt}. \tag{6}$$

Zbog $1 \leq y \leq t$ dobivamo i

$$\left|\frac{x}{y} - a\right| < \frac{1}{y^2}. \tag{7}$$

Uočimo da u obje gornje nejednakosti, (5) i (7), možemo pretpostaviti da su x i y relativno prosti. Dodatno, ako je a racionalan broj kojeg sada označimo s $\frac{m}{n}$, $(m, n) = 1$, $n > 0$, tada nejednadžba (7) ima konačno mnogo rješenja, jer ako je $a \neq \frac{x}{y}$ i $y > 0$ imamo

[1]Dirichletov princip u slaboj formi: "Ako $n + 1$ predmeta rasporedimo u n kutija, tada bar jedna kutija sadrži bar dva predmeta."

$$\left|\frac{x}{y} - a\right| = \left|\frac{x}{y} - \frac{m}{n}\right| = \frac{|nx - my|}{ny} \geq \frac{1}{ny}.$$

Stoga, ako vrijedi (7) , onda je $y < n$.
Dakle, ako je a racionalan broj, onda nejednadžba (7) ima konačno mnogo rješenja, dok ćemo u idućem teoremu dokazati da, ukoliko je a iracionalan, ista nejednadžba ima beskonačno mnogo rješenja.

Teorem 2.1. ([4]) *Ako je a iracionalan broj, tada nejednadžba*

$$\left|\frac{x}{y} - a\right| < \frac{1}{y^2} \tag{8}$$

ima beskonačno mnogo rješenja za relativno proste cijele brojeve x i y.

Dokaz. Neka je t_1 prirodan broj. Prema nejednakosti (6) i komentaru ispod, postoje relativno prosti cijeli brojevi x_1, y_1 za koje je

$$\eta_1 = \left|\frac{x_1}{y_1} - a\right| < \frac{1}{y_1 t_1},$$

gdje je $1 \leq y_1 \leq t_1$. Kako je a iracionalan broj, slijedi da je $\eta_1 \neq 0$. Tada odaberemo prirodni broj $t_2 > \frac{1}{\eta_1}$ i odredimo par relativno prostih cijelih brojeva x_2, y_2 za koje je

$$\eta_2 = \left|\frac{x_2}{y_2} - a\right| < \frac{1}{y_2 t_2} \leq \frac{1}{t_2} < \eta_1,$$

gdje je $1 \leq y_2 \leq t_2$. Analognim postupkom dolazimo do beskonačno rastućeg niza pozitivnih brojeva

$$\eta_1 > \eta_2 > \cdots > \eta_i > \cdots ,$$

čime je dokazana tvrdnja teorema.

$\square$

Lema 2.1. ([4]) *Neka je d prirodan broj koji nije potpun kvadrat. Tada postoji beskonačno mnogo parova prirodnih brojeva (x, y) koji zadovoljavaju nejednadžbu*

$$\left|x^2 - dy^2\right| < 1 + 2\sqrt{d}.$$

Dokaz. Budući da d nije potpun kvadrat, $\sqrt{d}$ je iracionalan broj, pa po Teoremu 2.1 postoji beskonačno mnogo parova prirodnih brojeva (x, y) za koje je

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2}.$$

Nadalje, vrijedi

$$\left|\frac{x}{y} + \sqrt{d}\right| = \left|\frac{x}{y} - \sqrt{d} + 2\sqrt{d}\right| < \frac{1}{y^2} + 2\sqrt{d},$$

pa je

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

$\square$

Teorem 2.2. ([4]) *Ako je d prirodan broj koji je različit od potpunog kvadrata, tada postoji barem jedan par prirodnih brojeva (x, y) koji zadovoljava Pellovu jednadžbu $x^2 - dy^2 = 1$.*

Dokaz. Prvo uočimo da prema Lemi 2.1 postoji barem jedan cijeli broj $k \neq 0$ takav da je

$$x^2 - dy^2 = k,$$

za beskonačno mnogo parova (x, y), odnosno, cijelih brojeva sa svojstvom $|k| < 1 + 2\sqrt{d}$ ima konačno mnogo. Od tih beskonačno mnogo parova (x, y), postoje barem dva para (x_1, y_1) i (x_2, y_2) koji zadovoljavaju kongruencije

$$x_1 \equiv x_2 \pmod{|k|} \quad i \quad y_1 \equiv y_2 \pmod{|k|}. \tag{9}$$

Ostatke modulo $|k|$ brojeva x_1, x_2, y_1, y_2 možemo kombinirati na k^4 načina. Stoga, možemo pretpostaviti da vrijedi

$$x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k, \tag{10}$$

pri čemu x_1, x_2, y_1, y_2 zadovoljavaju kongruencije (9). Sada imamo

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 - y_1y_2d + (x_1y_2 - x_2y_1)\sqrt{d}.$$

Iz (9) i (10) dobivamo

$$\begin{aligned} x_1x_2 - y_1y_2d &\equiv x_1^2 - y_1^2d \equiv 0 \pmod{|k|}, \\ x_1y_2 - x_2y_1 &\equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}. \end{aligned}$$

Dakle, vrijedi

$$\begin{aligned} x_1x_2 - y_1y_2d &= kp, \\ x_1y_2 - x_2y_1 &= kq, \end{aligned}$$

gdje su p i q cijeli brojevi. Uočimo da sada vrijedi i sljedeće:

$$\begin{aligned} (x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) &= k(p + q\sqrt{d}), \\ (x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) &= k(p - q\sqrt{d}). \end{aligned}$$

Množenjem ovih jednakosti član po član dobivamo

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = k^2 = k^2(p^2 - dq^2).$$

Dakle, $p^2 - dq^2 = 1$. Trebamo dokazati da je $q \neq 0$. Pretpostavimo suprotno, tj. $q = 0$. Sada imamo da vrijedi $x_1y_2 = x_2y_1$, $p = \pm 1$ i

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) = \pm k(x_2 - y_2\sqrt{d}).$$

Dijeljenjem prethodnog izraza s k dobivamo

$$x_1 - y_1\sqrt{d} = \pm(x_2 - y_2\sqrt{d})$$

što implicira $x_1 = \pm x_2$ i $y_1 = \pm y_2$. Kako mi možemo birati proizvoljne $|x_1| \neq |x_2|$ dolazimo do kontradikcije, te je teorem dokazan.

$\square$

Ako cijeli brojevi x i y zadovoljavaju Pellovu jednadžbu $x^2 - dy^2 = 1$ tada kažemo da je broj $x + y\sqrt{d}$ rješenje te jednadžbe. Ekvivalentno je reći i da je uređeni par (x, y) rješenje jednadžbe.

Dva rješenja $x + y\sqrt{d}$ i $x' + y'\sqrt{d}$ jednaka su ako je $x = x'$ i $y = y'$. Za rješenje $x' + y'\sqrt{d}$ kažemo da je veće od rješenja $x + y\sqrt{d}$ ako vrijedi $x' + y'\sqrt{d} > x + y\sqrt{d}$.
Najmanje rješenje $(x, y) \in \mathbb{N} \times \mathbb{N}$ nazivamo ***fundamentalno rješenje*** jednadžbe.

Teorem 2.3. ([4]) *Pellova jednadžba*

$$x^2 - dy^2 = 1 \tag{11}$$

ima beskonačno mnogo rješenja u prirodnim brojevima. Ako je (x_1, y_1) *fundamentalno rješenje, onda su sva rješenja dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}, \tag{12}$$

gdje je

$$x_n = x_1^n + \sum_{k=1} \binom{n}{2k} x_1^{n-2k} y_1^{2k} d^k,$$

$$y_n = \sum_{k=1} \binom{n}{2k-1} x_1^{n-2k+1} y_1^{2k-1} d^{k-1}.$$

Dokaz. Iz (12) očito slijedi

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n,$$

pa množenjem ove jednadžbe i (12) dobivamo

$$x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (x_1^2 - dy_1^2)^n = 1,$$

iz čega je jasno da je (x_n, y_n) rješenje jednadžbe (11).

Pretpostavimo da je $(u, v) \in \mathbb{N} \times \mathbb{N}$ rješenje jednadžbe (11) koje ne zadovoljava (12). Tada postoji priorodan broj m takav da je

$$(x_1 + y_1\sqrt{d})^m < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1},$$

odnosno

$$x_n + y_n\sqrt{d} < u + v\sqrt{d} < (x_n + y_n\sqrt{d})(x_1 + y_1\sqrt{d}).$$

Množenjem prethodne nejednakosti s $x_n - y_n\sqrt{d}$ dobivamo

$$1 < (u + v\sqrt{d})(x_n - y_n\sqrt{d}) < x_1 + y_1\sqrt{d}. \tag{13}$$

Stavimo li

$$(u + v\sqrt{d})(x_n - y_n\sqrt{d}) = x + y\sqrt{d},$$

pri čemu je $x = ux_n - vy_n d$ i $y = vx_n - uy_n$, dobili bismo i da je

$$(u - v\sqrt{d})(x_n + y_n\sqrt{d}) = x - y\sqrt{d},$$

te množenjem zadnje dvije nejednakosti imamo

$$1 = (u^2 - dv^2)(x_n^2 - dy_n^2) = x^2 - dy^2.$$

Slijedi da je (x, y) rješenje jednadžbe (11). Sada, po (13), imamo da je

$$x + y\sqrt{d} > 1.$$

Također imamo i

$$0 < x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}} < 1.$$

Nejednakost (13) sada povlači da za rješenje (x, y) vrijedi $(x, y) < (x_1, y_1)$, što nije moguće jer je (x_1, y_1) fundamentalno, odnosno najmanje rješenje, te dolazimo do kontradikcije.

□

Propozicija 2.1. (Brahmaguptino kompoziciono pravilo, [3]) *Ako su (x_1, y_1) i (x_2, y_2) rješenja Pellove jednadžbe $x^2 - dy^2 = 1$, tada je i $(x_3, y_3) = (x_1y_1 + dy_1y_2, x_1y_2 + x_2y_1)$ također rješenje.*

Dokaz. Uočimo kako je $(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 + y_1y_2d + (x_1y_2 + x_2y_1)\sqrt{d}$.
Znamo da vrijedi $x_1^2 - dy_1^2 = 1$ i $x_2^2 - dy_2^2 = 1$ jer su (x_1, y_1) i (x_2, y_2) rješenja Pellove jednadžbe $x^2 - dy^2 = 1$, te iz toga slijedi

$$1 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2).$$

Raspišemo li malo ovaj izraz dobivamo

$$\begin{aligned}
1 &= (x_1 - y_1\sqrt{d})(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})(x_2 + y_2\sqrt{d}) \\
&= (x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d})(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) \\
&= (x_1x_2 + y_1y_2d - \sqrt{d}(x_1y_2 + x_2y_1))(x_1x_2 + y_1y_2d + \sqrt{d}(x_1y_2 + x_2y_1)) \\
&= (x_1x_2 + y_1y_2d)^2 - d(x_1y_2 + x_2y_1)^2 \\
&= x_3^2 - dy_3^2,
\end{aligned}$$

pa slijedi i da je (x_3, y_3) rješenje Pellove jednadžbe $x^2 - dy^2 = 1$.

□

2.2. Veza Pellovih jednadžbi s verižnim razlomcima

Traženje fundamentalnog rješenja Pellove jednadžbe ponekad može biti trivijalno, uvrštavamo redom $y = 1, 2, 3, \ldots$ i provjeravamo je li $1+dy^2$ potpun kvadrat. Međutim, u većini slučajeva trebali bismo se dosta pomučiti ukoliko bismo tražili rješenje na ovaj način. Primjerice, za $d = 97$ fundamentalno rješenje je $62809633 + 6377353\sqrt{97}$.
Lakše i učinkovitije je tražiti rješenja pomoću algoritma, tj. korištenjem razvoja iracionalnog broja $\sqrt{d}$ u verižni razlomak.

U nastavku ćemo često spominjati razvoj broja $\sqrt{d}$ u verižni razlomak, pa ćemo prvo navesti teorem u kojem prikazujemo kako zapravo izgleda taj razvoj.

Teorem 2.4. ([5]) *Neka je d prirodan broj koji nije potpun kvadrat. Tada razvoj broja $\sqrt{d}$ u verižni razlomak ima oblik*

$$\sqrt{d} = [a_o, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}].$$

Primjer 2.1. *Pogledajmo primjere razvoja nekih prirodnih brojeva u verižni razlomak i obratimo pozornost na njihov oblik koji je naveden u prethodnom teoremu.*

$$\begin{aligned} \sqrt{7} &= \left[2, \overline{1, 1, 1, 4}\right], \\ \sqrt{19} &= \left[4, \overline{2, 1, 3, 1, 2, 8}\right], \\ \sqrt{28} &= \left[5, \overline{3, 2, 3, 10}\right], \\ \sqrt{34} &= \left[5, \overline{1, 4, 1, 10}\right]. \end{aligned}$$

Teorem 2.5. ([4]) *Neka je d prirodan broj koji nije potpun kvadrat i neka je $\frac{p_n}{q_n}$ konvergenta u razvoju broja $\sqrt{d}$ u verižni razlomak. Tada su sva rješenja u prirodnim brojevima jednadžbe*

$$x^2 - dy^2 = 1$$

oblika $x = p_n$, $y = p_n$, za neki prirodan broj n.

Dokaz. Neka je $(x, y) \in \mathbb{N} \times \mathbb{N}$ rješenje jednadžbe $x^2 - dy^2 = 1$. Ovu jednadžbu možemo zapisati i kao

$$(x - y\sqrt{d})(x + y\sqrt{d}) = 1.$$

Dijeljenjem gornjeg izraza s $y(x + y\sqrt{d})$ dobivamo

$$\frac{x - y\sqrt{d}}{y} = \frac{1}{y(x + y\sqrt{d})} > 0. \tag{14}$$

Kako je $x - y\sqrt{d} > 0$, odnosno $x + y\sqrt{d} > 2y\sqrt{d} > 2y$, slijedi da je

$$\frac{1}{x + y\sqrt{d}} < \frac{1}{2y}.$$

Uočimo da sada iz (14) slijedi

$$0 < \frac{x - y\sqrt{d}}{y} = \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2}.$$

Podsjetimo li se prethodnog poglavlja i Teorema 1.5, zaključujemo da je $\frac{x}{y}$ neka konvergenta od $\sqrt{d}$.

□

Napomena 2.2. *Uočimo da prethodni teorem možemo iskoristi i ukoliko imamo jednadžbu oblika $x^2 - dy^2 = -1$. Sličnim postupkom kao u dokazu Teorema 2.5 dobili bismo da vrijedi*

$$0 < \frac{y}{x} - \frac{1}{\sqrt{d}} < \frac{1}{2x^2},$$

pa zaključujemo da je $\frac{y}{x}$ konvergenta od $\frac{1}{\sqrt{d}}$.

Štoviše, kako je $\frac{1}{\sqrt{d}} < 1$, uočavamo sljedeću vezu između razvoja brojeva $\sqrt{d}$ i $\frac{1}{\sqrt{d}}$ u verižni razlomak:

$$\frac{1}{\sqrt{d}} = [0, a_0, a_1, \dots], \quad \sqrt{d} =]a_0, a_1, \dots].$$

Dakle, ako je $\frac{y}{x}$ n-ta kovergenta u razvoju u verižni razlomak od $\frac{1}{\sqrt{d}}$, tada je $\frac{x}{y}$ $(n-1)$-va konvergenta u razvoju broja $\sqrt{d}$ u verižni razlomak.

Idući teorem često koristimo u zadacima, a govori nam kojeg su oblika rješenja jednadžbe (ukoliko jednadžba ima rješenja), ovisno o tome je li period paran ili neparan.

Teorem 2.6. ([2]) *Neka je r duljina perioda, a $\frac{p_n}{q_n}$ n-ta konvergenta broja $\sqrt{d}$ u razvoju u verižni razlomak.*

- *Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja u prirodnim brojevima, dok su sva rješenje jednadžbe $x^2 - dy^2 = 1$ dana s $x = p_{nr-1}$, $y = q_{nr-1}$, za $n \in \mathbb{N}$.*
- *Ako je r neparan, onda sva rješenja u prirodnim brojevima jednadžbe $x^2 - dy^2 = -1$ dana s $x = p_{nr-1}$, $y = q_{nr-1}$, za neparan $n \in \mathbb{N}$, a sva rješenje jednadžbe $x^2 - dy^2 = 1$ dana su s $x = p_{nr-1}$, $y = q_{nr-1}$, za paran $n \in \mathbb{N}$.*

Ovaj teorem nećemo dokazivati, ali ćemo na idućem primjeru demonstrirati njegovu uporabu.

Primjer 2.2. *Nađimo sva rješenja u prirodnim brojevima jednadžbi $x^2 - 3y^2 = \pm 1$ sa svojstvom $0 < x < 100$.*

Prema Primjeru 1.2 znamo da je $\sqrt{3} = \left[1, \overline{1, 2}\right]$, iz čega vidimo da je period $r = 2$. Kako je period paran, to jednadžba $x^2 - 3y^2 = -1$ nema rješenja u prirodnim brojevima.

Sva rješenja jednadžbe $x^2 - 3y^2 = 1$ u prirodnim brojevima su oblika

$$x = p_{2n-1}, \quad y = q_{2n-1}.$$

Redom uzimamo prirodne brojeve za n i tražimo rješenja. Prvo ćemo naći fundamentalno rješenje i potom ostala.

Za $n = 1$ imamo $x_1 = p_1$, $y_1 = q_1$. Zapišemo li sada prvu konvergentu broja $\sqrt{3}$ kao

$$\frac{x_1}{y_1} = \frac{p_1}{q_1} = [1, 1] = 1 + \frac{1}{1} = \frac{2}{1},$$

dobivamo

$$x_1 = 2, \quad y_1 = 1.$$

Dakle, $(2, 1)$ je fundamentalno rješenje, pa su po Teoremu 2.3 sva rješenja jednadžbe dana s

$$x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n.$$

Za $n = 2$ je $x_2 + y_2\sqrt{3} = (2 + \sqrt{3})^2 = 7 + 4\sqrt{3}$, iz čega slijedi da je

$$x_2 = 7, \quad y_2 = 4.$$

Ponavljamo postupak dok ne dobijemo $x > 100$.

Za $n = 3$ je $\quad x_3 + y_3\sqrt{3} = (2+\sqrt{3})^3 = 26 + 15\sqrt{3},$ te

$$x_3 = 26, \quad y_3 = 15.$$

Za $n = 4$ imamo $\quad x_4 + y_4\sqrt{3} = (2+\sqrt{3})^4 = 97 + 56\sqrt{3},$ odnosno

$$x_4 = 97, \quad y_3 = 56.$$

Očito će biti $x_5 > 100$, pa ovdje stajemo s algoritmom i naša rješenja su $(2,1), (7,4), (26,15)$ i $(97,56)$.

U ovom smo primjeru rješenja tražili preko konvergenti i formulom koju smo već naučili, a sada ćemo iskazati i dokazati teorem koji zadaje rekurzivne relacije vezane za rješavanje Pellovih jednadžbi, te ćemo na istom primjeru potražiti rješenja drugom metodom.

Teorem 2.7. ([4]) *Neka je (x_n, y_n), $n \in \mathbb{N}$, niz svih rješenja Pellove jednadžbe $x^2 - dy^2 = 1$, te neka je $(x_0, y_0) = (1, 0)$. Tada vrijedi*

$$x_{n+2} = 2x_1x_{n+1} - x_n, \quad y_{n+2} = 2x_1y_{n+1} - y_n, \quad n \geq 0.$$

Dokaz. Već smo pokazali da vrijedi $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Sada imamo

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

Nadalje je

$$\begin{aligned} x_{n+2} &= x_1x_{n+1} + dy_1y_{n+1}, \\ x_n &= x_1x_{n+1} - dy_1y_n + 1, \end{aligned}$$

iz čega zbrajanjem dobivamo

$$x_{n+2} = 2x_1x_{n+1} - x_n.$$

Analognim postupkom dobijemo i da vrijedi $y_{n+2} = 2x_1y_{n+1} - y_n$.

□

Vratimo se sada na Primjer 2.2. Već smo rekli da je period paran, što povlači da jednadžba $x^2 - 3y^2 = -1$ nema rješenja u prirodnim brojevima. Najmanje rješenje Pellove jednadžbe $x^2 - 3y^2 = 1$ je $(x_1, y_1) = (2, 1)$. Sada prema prethodnom teoremu računamo ostala rješenja.

$$\begin{aligned} x_2 &= 2 \cdot 2 \cdot 2 - 1 = 7, & y_2 &= 2 \cdot 2 \cdot 1 - 0 = 4, \\ x_3 &= 2 \cdot 2 \cdot 7 - 2 = 26, & y_3 &= 2 \cdot 2 \cdot 4 - 1 = 15, \\ x_4 &= 2 \cdot 2 \cdot 26 - 7 = 97, & y_4 &= 2 \cdot 2 \cdot 15 - 4 = 56. \end{aligned}$$

Za x_5 dobivamo broj veći od 100. Dakle, jednadžba $x^2 - 3y^2 = 1$ ima 4 rješenja, a to su $(2,1), (7,4), (26,15), (97,56)$.

Primjer 2.3. *Pronađimo sva rješenja u prirodnim brojevima jednadžbi* $x^2 - 7y^2 = \pm 1$ *za koja vrijedi* $1 < x < 2000$.

Iz Primjera 2.1 znamo da je $\sqrt{7} = \left[2, \overline{1, 1, 1, 4}\right]$, te je period paran, $r = 4$. Zbog parnog perioda, jednadžba $x^2 - 7y^2 = -1$ nema rješenja.

Najmanje rješenje jednadžbe $x^2 - 7y^2 = 1$ je $(x_1, y_1) = (8, 3)$.
Nadalje, imamo $x_2 = 2 \cdot 8 \cdot 8 - 1 = 127$, $y_2 = 2 \cdot 8 \cdot 3 - 0 = 48$, te je već $x_3 = 2024 > 2000$.
Zaključujemo da su $(8, 3)$ i $(127, 48)$ rješenja jednadžbe $x^2 - 7y^2 = 1$, uz uvjet $1 < x < 2000$.

3. Pellovske jednadžbe

U prethodnom poglavlju promatrali smo Pellovu jednadžbu $x^2 - dy^2 = 1$, a sada ćemo stvari proširiti, odnosno promatrat ćemo jednadžbe u nešto općenitijem obliku. Čak smo već i ranije, u Teoremu 2.6, spomenuli jednadžbu $x^2 - dy^2 = -1$, te uvjet za postojanje i oblik rješenja.

3.1. Fundamentalna rješenja pellovske jednadžbe

Definicija 3.1. *Jednadžba oblika*

$$x^2 - dy^2 = k, \tag{15}$$

gdje su k i d prirodni brojevi i d nije potpun kvadrat, naziva se ***pellovska jednadžba.***

Pretpostavimo da jednadžba (15) ima cjelobrojnih rješenja i da je $u+v\sqrt{d}$ njezino rješenje. Ako je $x + y\sqrt{d}$ rješenje Pellove jednadžbe $x^2 - dy^2 = 1$, tada je

$$(u + v\sqrt{d})(x + y\sqrt{d}) = ux + vyd + (uy + vx)\sqrt{d}$$

također rješenje jednadžbe (15). U ovom slučaju kažemo da je su rješenja $x + y\sqrt{d}$ i $u + v\sqrt{d}$ ***asocirana.*** Skup svih asociranih rješenja nazivamo ***klasom rješenja*** jednadžbe (15). Prema Teoremu 2.3 svaka klasa sadrži beskonačno mnogo rješenja.

Moguće je provjeriti pripadaju li dva rješenja $x+y\sqrt{d}$ i $x' + y'\sqrt{d}$ istoj klasi. Treba uočiti da je nužan i dovoljan uvjet asociranosti rješenja taj da su ova dva broja

$$\frac{xx' - yy'd}{k} \quad \text{i} \quad \frac{yx' - xy'}{k}$$

cijeli brojevi.

Ako je $\mathbf{K}$ klasa koja se sastoji od rješenja $x_i + y_i\sqrt{d}, i = 1, 2, 3, \ldots$, očigledno rješenja $x_i - y_i\sqrt{d}, i = 1, 2, 3, \ldots$, također čine klasu rješenja koju možemo označiti s $\overline{\mathbf{K}}$. Za klase $\mathbf{K}$ i $\overline{\mathbf{K}}$ kažemo da su ***konjugirane***. Konjugirane klase većinom se razlikuju, no ako se podudaraju tada govorimo o ***dvoznačnoj*** klasi.

Od svih mogućih rješenja klase $\mathbf{K}$, odaberimo rješenje $x^* + y^*\sqrt{d}$ tako da je y^* najmanji nenegativan broj koji se nalazi u klasi $\mathbf{K}$. Ako $\mathbf{K}$ nije dvoznačna klasa, tada je y^* jednoznačno određen. Ako je $\mathbf{K}$ dvoznačna, onda će y^* biti jednoznačno određen ako vrijedi $y^* \geq 0$. Rješenje $x^* + y^*\sqrt{d}$ definirano na ovaj način je ***fundamentalno rješenje klase***.

Dodatno, uočimo kako $|x^*|$ poprima najmanju moguću vrijednost u klasi $\mathbf{K}$. Slučaj kada je $x^* = 0$ može se dogoditi samo ako je klasa dvoznačna. Ako je $k = \pm 1$, postoji samo jedna klasa i ona je dvoznačna.

Teorem 3.1. ([4]) *Ako je $x + y\sqrt{d}$ fundamentalno rješenje klase $\boldsymbol{K}$ jednadžbe*

$$x^2 - dy^2 = k, \tag{16}$$

te ako je $u_1+v_1\sqrt{d}$ *fundamentalno rješenje od* $u^2-dv^2=1$*, onda vrijede sljedeće nejednakosti*

$$0 \le y \le \frac{v_1}{\sqrt{2(u_1+1)}}\sqrt{k}, \tag{17}$$

$$0 < |x| \le \sqrt{\frac{1}{2}(u_1+1)k}. \tag{18}$$

Dokaz. Ukoliko nejednakosti (17) i (18) vrijede za klasu $\mathbf{K}$, onda vrijede i za konjugiranu klasu $\overline{\mathbf{K}}$. Tada možemo pretpostaviti da je x pozitivan. Vrijedi

$$xu_1 - dyv_1 = xu_1 - \sqrt{(x^2-k)(u_1^2-1)} > 0. \tag{19}$$

Neka je

$$(x+y\sqrt{d})(u_1-v_1\sqrt{d}) = xu_1 - dyv_1 + (u_1y - v_1x)\sqrt{d}$$

rješenje koje pripada istoj klasi kao i $x+y\sqrt{d}$. Kako je $x+y\sqrt{d}$ fundamentalno rješenje klase, te je po (19) $xu_1 - dyv_1$ pozitivan, dobivamo

$$xu_1 - dyv_1 \ge x. \tag{20}$$

Iz ove nejednakosti slijedi nam

$$x^2(u_1-1)^2 \ge dy^2v_1^2 = (x^2-k)(u_1^2-1)$$

ili

$$\frac{u_1-1}{u_1+1} \ge 1 - \frac{k}{x^2},$$

te konačno imamo

$$x^2 \le \frac{1}{2}(u_1+1)k.$$

Ovime smo dokazali nejednakost (18), a iz (18) lako se dođe do (17), čime je teorem dokazan.

□

Primjenimo ovaj teorem na sljedećem primjeru.

Primjer 3.1. *Nađimo fundamentalna rješenja jednadžbe* $x^2-3y^2=37$*.*

Prema Primjeru 2.2 fundamentalno rješenje jednadžbe $u^2-3v^2=1$ je $(u_1,v_1)=(2,1)$. Koristeći prethodni teorem dobivamo da vrijedi

$$0 \le y \le \frac{v_1}{\sqrt{2(u_1+1)}}\sqrt{k} \le \frac{1}{\sqrt{2(2+1)}}\sqrt{37} \le 2.4833,$$

odnosno $0 \le y \le 2$.

Za x imamo

$$|x| \le \sqrt{\frac{1}{2}(u_1+1)k} \le \sqrt{\frac{1}{2}(2+1)37} \le 7.4498,$$

odnosno $|x| \le 7$.

Sada provjerimo za koje $y = 0, 1, 2$ početna jednadžba ima rješenja.

Za $y = 0$ dobijemo $x^2 = 37$, tj. za $y = 0$ jednadžba nema rješenja.
Slično, za $y = 1$ imamo $x^2 = 40$, pa ni za $y = 1$ jednadžba nema rješenja.
Za $y = 2$ je $x^2 = 49$, odnosno $x = \pm 7$.

Dakle, fundamentalna rješenja polazne jednadžbe su $(7 + 2\sqrt{3})$ i $(-7 + 2\sqrt{3})$.

Ukoliko imamo jednadžbu oblika $x^2 - dy^2 = -k$, gdje su, kao i ranije, k i d prirodni brojevi i d nije potpun kvadrat, onda vrijedi teorem vrlo sličan prethodnom:

Teorem 3.2. ([4]) *Ako je $x + y\sqrt{d}$ fundamentalno rješenje klase $\boldsymbol{K}$ jednadžbe*

$$x^2 - dy^2 = -k,$$

te ako je $u_1 + v_1\sqrt{d}$ fundamentalno rješenje od $u^2 - dv^2 = 1$, onda vrijede sljedeće nejednakosti

$$0 \leq y \leq \frac{v_1}{\sqrt{2(u_1 - 1)}}\sqrt{k}, \tag{21}$$

$$0 < |x| \leq \sqrt{\frac{1}{2}(u_1 - 1)k}. \tag{22}$$

Dokaz. Analogno kao i u Teoremu 3.1.

3.2. Rješavanje pellovske jednadžbe

U ovom dijelu pokazat ćemo kako se generiraju rješenja pellovske jednadžbe. Kao posljedica dva teorema iz prethodnog potpoglavlja slijedi tvrdnja:

Teorem 3.3. ([4]) *Ako su d i k prirodni brojevi, gdje d nije potpun kvadrat, tada diofantske jednadžbe $x^2 - dy^2 = k$ i $x^2 - dy^2 = -k$ imaju konačno mnogo klasa rješenja. Fundamentalna rješenja svih klasa mogu se pronaći u konačno mnogo pokušaja pomoću nejednakosti iz Teorema 3.1 i Teorema 3.2.*
Ako je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje klase $\boldsymbol{K}$, onda su sva rješenja $x + y\sqrt{d}$ iz $\boldsymbol{K}$ dana formulom

$$x + y\sqrt{d} = (x_1 + y_1\sqrt{d})(u + v\sqrt{d}),$$

gdje $u + v\sqrt{d}$ prolazi kroz sva rješenja jednadžbe $x^2 - dy^2 = 1$.
Diofantska jednadžba $x^2 - dy^2 = k$, odnosno $x^2 - dy^2 = -k$, nema rješenja ukoliko ne postoji rješenje koje zadovoljava nejednakosti (17) i (18), odnosno (21) i (22).

Ukoliko primjenimo prethodno iskazani teorem i Teorem 2.3 na Primjeru 3.1, dobivamo beskonačno mnogo rješenja jednadžbe $x^2 - 3y^2 = 37$ dana s

$$x_n + y_n\sqrt{3} = (7 + 2\sqrt{3})(2 + \sqrt{3})^n, \qquad n \in \mathbb{N},$$
$$x_n + y_n\sqrt{3} = (-7 + 2\sqrt{3})(2 + \sqrt{3})^n, \qquad n \in \mathbb{N}.$$

Kombinirajući Teorem 3.1 i Teorem 3.2 uz dodatne uvjete dolazimo do sljedećeg teorema.

Teorem 3.4. ([4]) *Ako je p prost broj, jednadžba oblika*

$$x^2 - dy^2 = \pm p \tag{23}$$

ima najviše jedno rješenje $x + y\sqrt{d}$ u kojem x i y zadovoljavaju nejednakosti (17) *i* (18)*, ili* (21) *i* (22)*, pri čemu je $x \geq 0$. Ako je jednadžba* (23) *rješiva, ona ima jednu ili dvije klase rješenja, ovisno o tome je li $2d$ djeljiv s p ili nije.*

Dokaz. Pretpostavimo da jednadžba (23) ima dva rješenja i da su to $x + y\sqrt{d}$ i $x_1 + y_1\sqrt{d}$, te da oni zadovoljavaju uvjete teorema. Brojevi x, y, x_1, y_1 su nenegativni. Iz jednadžbi

$$x^2 - dy^2 = \pm p, \quad x_1^2 - dy_1^2 = \pm p, \tag{24}$$

dobivamo

$$x^2y_1^2 - x_1^2y^2 = \pm p(y_1^2 - y^2),$$

te

$$xy_1 \equiv \pm x_1 y \pmod{p}. \tag{25}$$

Nadalje, množenjem jednakosti (24) član po član dobivamo

$$(xx_1 \mp dyy_1)^2 - d(xy_1 \mp x_1y)^2 = p^2,$$

tj.

$$\left(\frac{xx_1 \mp dyy_1}{p}\right)^2 - d\left(\frac{xy_1 \mp x_1y}{p}\right)^2 = 1. \tag{26}$$

Kvadrati na lijevoj strani jednakosti (26) cijeli su brojevi ukoliko je zadovoljena kongruencija (25).

Ukoliko je $xy_1 \mp x_1y \neq 0$, iz (26) i činjenice da je $u_1 + v_1\sqrt{d}$ fundamentalno rješenje, zaključujemo da je

$$|xy_1 \mp x_1y| \geq v_1 p.$$

S druge strane, primjenjujući nejednakosti (17) i (18), ili (21) i (22) dobivamo

$$|xy_1 \mp x_1y| < v_1 p,$$

te dolazimo do kontradikcije i time je dokazan prvi dio teorema. Dokaz drugog dijela može se pronaći u [4].

□

Literatura

[1] D. Curd, *Pell's equations: History, Methods, and Number Theory*, Department of Mathematics, Texas Christian University, 2014.

[2] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta).

[3] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište J.J.Strossmayera u Osijeku, 2014.

[4] T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.

[5] C.D. Olds, *Continued fractions*, Random House, New York, 1963.

[6] J. Unger, *Solving Pell's Equation with Continued Fractions*, University of Canterbury, 2009.