Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Dajana Borojević

Pellove jednadžbe i problem stoke

Završni rad

Osijek, 2017.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Dajana Borojević

Pellove jednadžbe i problem stoke

Završni rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2017.

Sažetak. U ovom završnom radu upoznat ćemo se s Pellovim jednadžbama i nekim metodama za njihovo rješavanje. Pokazat ćemo usku povezanost Pellovih jednadžbi s diofantskim aproksimacijama i verižnim razlomcima. Rad također sadrži riješene primjere i probleme koji se svode na analizu skupa rješenja Pellove jednadžbe, gdje je naglasak na Arhimedovom problemu stoke.

Ključne riječi: Pellove jednadžbe, verižni razlomci, Arhimedov problem stoke

Abstract. In this final paper we will be introduced to Pell's equations and some methods for their solutions. We will show their tihgt connection to diophantine approximation and continued fractions. Paper also contains solved examples and problems which are reduced to the study of the set of solutions of Pell's equation, where the accent is on Archimedes' cattle problem.

Key words: Pell's equation, continued fraction, Archimedes' cattle problem

Sadržaj

1 Uvod

Pellove jednadžbe su posebna vrsta diofantskih jednadžbi. Diofantskim jednadžbama se bavio već starogrčki matematičar Diofant iz Aleksandrije (oko 250.g.) i njemu u čast su dobile ime. To su algebarske jednadžbe s dvjema ili više nepoznanica koje imaju cjelobrojne koeficijente, kojima se traže najčešće cjelobrojna ili pak racionalna rješenja.
Pellova jednadžba je diofantska jednadžba oblika

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

gdje je d prirodan broj i nije potpun kvadrat. Ona je jedna od najstarijih i najvažnijih diofantskih jednadžbi drugog reda. Dobila je ime po engleskom matematičaru Johnu Pellu, iako ne postoje dokazi da se on bavio njome. Po svemu sudeći Euler mu je pogrešno pripisao zasluge za njihovo rješavanje proglasivši Pella da je bio prvi koji je proučavao netrivijalna rješenja jednadžbe $x^2 - dy^2 = 1 (x \neq 1, y \neq 0)$. No, još su se starogrčki matematičari bavili pojedinačnim jednadžbama ovog tipa, pa je tako Teon iz Smirne pomoću rješenja jednadžbe $x^2 - 2y^2 = 1$ aproksimirao iracionalan broj $\sqrt{2}$ racionalnim brojem $\frac{x}{y}$, dok je Arhimed poopćio tu tvrdnju pokazavši da ako su x i y velika rješenja jednadžbe $x^2 - dy^2 = 1$, onda je $\frac{x}{y}$ dobra aproksimacija iracionalnog broja $\sqrt{d}$. Arhimed je također zaslužan za otkrivanje još jedne poznate Pellove jednadžbe. On je u formi epigrama od 44 retka postavio numerički zahtjevan problem, takozvani *problem stoke*, kojem rješenje nalazimo pomoću Pellove jednadžbe, o čemu ćemo govoriti malo kasnije u radu. Ovim jednadžbama su se također bavili i srednjovjekovni indijski matematičari (Baudhayana, Brahmagupta, Bhaskara II.), a od europskih matematičara metode za rješavanje Pellovih jednadžbi dali su Brouncher, Fermat, Euler i Lagrange.

2 Verižni razlomci

U pronalasku rješenja Pellovih jednadžbi od velike koristi će nam biti veza Pellovih jednadžbi s diofantskim aproksimacijama, te preko njih s verižnim razlomcima. Realnom broju se na različite načine mogu pridružiti racionalni brojevi koji ga dobro aproksimiraju, a jedna od najkorisnijih metoda za to je verižni razlomak. Stoga ćemo se prvo upoznati s osnovnim pojmovima vezanim uz verižni razlomak.

Neka je α proizvoljan realan broj. Najprije stavimo $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$, zapišimo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$, te neka je $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$, zapišimo α_1 u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tako da je $\alpha_2 > 1$, te neka je $a_2 = \lfloor \alpha_2 \rfloor$. Ukoliko je $a_n \neq \alpha_n$, za svaki n, ovaj postupak možemo nastaviti u nedogled. Ukoliko je $a_n = \alpha_n$, za neki n, postupak staje i dobivamo izraz oblika:

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

Njega ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, a_2, \ldots, a_n]$.
Pogledajmo na kratkom primjeru kako to izgleda.

Primjer 2.1. *Neka je $\alpha = \frac{90}{77}$. Redom je tada $a_0 = 1, \alpha_1 = \frac{77}{13}, a_1 = 5, \alpha_2 = \frac{13}{12}, a_2 = 1$, $\alpha_3 = 12, a_3 = 12$. Kako je $a_3 = \alpha_3$, postupak staje i racionalan broj $\frac{90}{77}$ zapisujemo u obliku:*

$$\frac{90}{77} = 1 + \frac{13}{77} = 1 + \cfrac{1}{\cfrac{77}{13}} = 1 + \cfrac{1}{5 + \cfrac{12}{13}} = 1 + \cfrac{1}{5 + \cfrac{1}{\cfrac{13}{12}}} = 1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{12}}},$$

odnosno, $\frac{90}{77} = [1, 5, 1, 12]$.

Ako je a_0 cijeli broj, $a_1, \ldots, a_n$ prirodni brojevi, izraz oblika (1) nazivamo *razvoj broja α u jednostavni verižni razlomak.* Brojevi $a_0, a_1, a_2, \ldots$ nazivaju se *parcijalni kvocijenti*, a brojevi

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

se nazivaju parcijalne konvergente od α.
Ukoliko je $a_n = \alpha_n$, za neko n, dobili smo *konačni razvoj broja α u jednostavni verižni razlomak*, te je u tom slučaju α racionalan broj. Primijetimo da ako je $\alpha = \frac{a}{b}$, brojevi $a_0, a_1, a_2, \ldots$ su upravo kvocijenti iz Euklidovog algoritma primjenjenog na brojeve a i b. Prikažimo to na Primjeru 2.1:

$$\begin{aligned} 90 &= 77 \cdot 1 + 13 \\ 77 &= 13 \cdot 5 + 12 \\ 13 &= 12 \cdot 1 + 1 \\ 12 &= 1 \cdot 12 \end{aligned}$$

Kvocijenti 1, 5, 1, 12 su parcijalni kvocijenti u razvoju broja $\frac{90}{77}$ u verižni razlomak.
Napomenimo da Euklidov algoritam funkcionira samo za razvoj racionalnih brojeva u verižni razlomak, tj. onda kada je $a_n = \alpha_n$, za neki n.
Neka je sada $a_n \neq \alpha_n$, za svaki n. Pokazat ćemo da to odgovara razvoju iracionalnih brojeva u verižni razlomak.

Teorem 2.1. *Brojevi p_n i q_n zadovoljavaju rekurzije*

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

Dokaz. Za $n = 2$ tvrdnja se provjerava direktno. Pretpostavimo da je $n > 2$ i da tvrdnja vrijedi za $n - 1$. Definirajmo brojeve p'_j, q'_j sa $\frac{p'_j}{q'_j} = [a_1, a_2, \ldots, a_{j+1}]$. Tada je

$$p'_{n-1} = a_n p'_{n-2} + p'_{n-3}, \quad q'_{n-1} = a_n q'_{n-2} + q'_{n-3}.$$

No,

$$\frac{p_j}{q_j} = a_0 + \frac{1}{[a_1, \ldots, a_j]} = a_0 + \frac{q'_{j-1}}{p'_{j-1}} = \frac{a_0 p'_{j-1} + q'_{j-1}}{p'_{j-1}}.$$

Stoga je $p_j = a_0 p'_{j-1} + q'_{j-1}, q_j = p_{j-1}$. Prema tome,

$$\begin{aligned} p_n &= a_0(a_n p'_{n-2} + p'_{n-3}) + (a_n q'_{n-2} + q'_{n-3}) \\ &= a_n(a_0 p'_{n-2} + q'_{n-2}) + (a_0 p'_{n-3} + q'_{n-3}) = a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n p'_{n-2} + p'_{n-3} = a_n q_{n-1} + q_{n-2}. \end{aligned}$$

□

Dogovorno uzimamo da je $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$, uz što lako vidimo da Teorem 2.1 vrijedi za sve $n \geq 0$.

Teorem 2.2. *Za sve $n \geq -1$ vrijedi $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.*

Dokaz. Dokaz provodimo indukcijom. Za $n = -1$ imamo:

$$q_{-1} p_{-2} - p_{-1} q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}.$$

Pretpostavimo da tvrdnja vrijedi za $n - 1$. Tada je

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} &= (a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1} \\ &= -(q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) \\ &= -(-1)^{n-1} = (-1)^n. \end{aligned}$$

□

Iz prethodnog teorema direktno slijedi da su brojevi p_n i q_n relativno prosti.

Teorem 2.3. *Vrijede sljedeće tvrdnje:*

1. $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots,$
2. $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots,$

3. Ako je n paran, a m neparan, onda je $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.

Teorem 2.4.

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

Dokaz. Kako je $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_1}{q_1}$, za paran n, $\lim_{n\to\infty} \frac{p_n}{q_n}$ postoji. Slično, limes postoji i za neparan n. Ali ta dva limesa su jednaka jer je $\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n-1}q_n}$ i zbog $q_n \geq n$ je $\lim_{n\to\infty} \frac{(-1)^n}{q_{n-1}q_n} = 0$. Neka je $\beta = \lim_{n\to\infty} \frac{p_n}{q_n}$.
Iz definicije brojeva $\alpha_1, \alpha_2, \ldots$ slijedi da je $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$, gdje je $0 < \frac{1}{\alpha_{n+1}} \leq \frac{1}{a_{n+1}}$. To znači da α leži između brojeva $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$. Prema Teoremu 2.3, to znači da je $\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$ za n paran i $\frac{p_{n+1}}{q_{n+1}} < \alpha < \frac{p_n}{q_n}$ za n neparan. Dakle, $\alpha = \beta$. □

Sada možemo zaključiti da ako je α racionalan broj, onda je $a_n = \alpha_n$, za neki n. No, ako je α iracionalan broj, onda uvodimo oznaku $\lim_{n\to\infty}[a_0, a_1, \ldots, a_n] = [a_0, a_1, a_2, \ldots]$. Ako je $\alpha = [a_0, a_1, a_2, \ldots]$, tj.

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

taj izraz zovemo *razvoj od α u beskonačni jednostavni verižni razlomak.*

Teorem 2.5 (Legendre)**.** *Neka su p, q cijeli brojevi takvi da je $q \geq 1$ i*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Tada je $\frac{p}{q}$ neka konvergenta od α.

Dokaz. Ako je $\alpha = \frac{p}{q}$ tvrdnja je trivijalno zadovoljena. Pretpostavimo stoga da je $\alpha \neq \frac{p}{q}$. Tada možemo pisati $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, gdje je $0 < \vartheta < \frac{1}{2}$ i $\varepsilon = \pm 1$.
Neka je

$$\frac{p}{q} = [b_0, b_1, \ldots, b_{n-1}]$$

razvoj od $\frac{p}{q}$ u jednostavni verižni razlomak, gdje je n izabran tako da vrijedi $(-1)^{n-1} = \varepsilon$. To uvijek možemo postići jer je $[a_0, a_1, \ldots, a_m] = [a_0, a_1, \ldots, a_m - 1, 1]$.
Definirajmo ω sa

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}},$$

tako da je $\alpha = [b_0, b_1, \ldots, b_{n-1}, \omega]$.
Vrijedi formula $q_n\alpha - p_n = q_n \cdot \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - p_n = \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}}$, za $\alpha = [a_0, a_1, \ldots, a_n, a_{n+1}]$, prema kojoj je onda

$$\frac{\varepsilon\vartheta}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}}(\alpha q_{n-1} - p_{n-1}) = \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}},$$

pa je $\vartheta = \frac{q_{n-1}}{\omega q_{n-1} + q_{n-2}}$. Rješavanjem ove relacije dobivamo $\omega = \frac{1}{\vartheta} - \frac{q_{n-2}}{q_{n-1}}$. Odavde slijedi da je $\omega > 2 - 1 = 1$. Razvijmo ω u (konačan ili beskonačan) jednostavan verižni razlomak,

$$\omega = [b_n, b_{n+1}, b_{n+2}, \ldots].$$

Kako je $\omega > 1$, svi b_j $(j = n, n+1, \dots)$ su prirodni brojevi. Stoga je

$$\alpha = [b_0, b_1, \dots, b_{n-1}, b_n, b_{n+1}, \dots]$$

razvoj u jednostavni verižni razlomak od α i

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, \dots, b_{n-1}]$$

je konvergenta od α, što je trebalo dokazati. □

Definicija 2.1. *Za beskonačni verižni razlomak $[a_0, a_1, a_2, \dots]$ kažemo da je periodski ako postoje cijeli brojevi $k \geq 0$, $m \geq 1$ takvi da je $a_{m+n} = a_n$ za sve $n \geq k$. Tada verižni razlomak pišemo u obliku*

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

gdje "crta" iznad brojeva $a_k, a_{k+1}, \dots, a_{k+m-1}$ znači da se taj blok ponavlja u nedogled.
Pretpostavljamo da je broj m najmanji broj sa gornjim svojstvom, te ga zovemo duljina perioda.
Za periodski verižni razlomak kažemo da je čisto periodski ako je $k = 0$, tj. ako nema početni blok koji se ne ponavlja.

Primjer 2.2. *Promotrimo sljedeće primjere:*

(i) Neka je $\beta = [3, 4, 3, 4, \dots] = [\overline{3, 4}]$. Tada je $\beta = 3 + \dfrac{1}{4 + \dfrac{1}{\beta}}$.

Sređivanjem izraza dobijemo $\beta = \dfrac{13\beta + 3}{4\beta + 1}$, tj. kvadratnu jednadžbu $4\beta^2 - 12\beta - 3 = 0$, a zbog $\beta > 0$, za korijen jednadžbe dobivamo $\beta = \dfrac{3 + 2\sqrt{3}}{2}$.

(ii) Neka je sada $\alpha = [2, 3, \overline{3, 4}]$. Uočimo da je tada $\alpha = [2, 3, \beta]$, pa imamo

$$\alpha = 2 + \frac{1}{3 + \dfrac{1}{\beta}} = 2 + \frac{\beta}{3\beta + 1} = \frac{23 + 4\sqrt{3}}{13}.$$

Ovaj primjer ilustrira opću situaciju.

Definicija 2.2. *Za iracionalan broj α kažemo da je kvadratna iracionalnost ako je α korijen kvadratne jednadžbe s racionalnim (cjelobrojnim) koeficijentima i pozitivnom diskriminantom.*

Primijetimo da je kvadratna iracionalnost α oblika $\frac{a \pm \sqrt{b}}{c}$, za $c \neq 0$ i $b > 0$ koji nije potpun kvadrat.

Teorem 2.6 (Euler, Lagrange)**.** *Razvoj u jednostavni verižni razlomak realnog broja α je periodski ako i samo ako je α kvadratna iracionalnost.*

Dokaz. Neka je $\alpha = [b_0, b_1, \ldots, b_{k-1}, \overline{a_0, a_1, \ldots, a_{m-1}}]$, te neka je $\beta = [\overline{a_0, a_1, \ldots, a_{m-1}}]$, tj. neka je β čisto periodski dio od α. Iz $\beta = [a_0, a_1, \ldots, a_{m-1}, \beta]$ slijedi da je

$$\beta = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}},$$

što je kvadratna jednadžba za β (s cjelobrojnim koeficijentima). Budući da je β iracionalan (jer mu je razvoj beskonačan), to je β kvadratna iracionalnost.

Zapišimo α pomoću β:

$$\alpha = \frac{\beta p + p'}{\beta q + q'}, \tag{2}$$

gdje su $\frac{p}{q}$ i $\frac{p'}{q'}$ zadnje dvije konvergente od $[b_0, b_1, \ldots, b_{k-1}]$. No, kako β ima oblik $\frac{a+\sqrt{b}}{c}$, iz (2) slijedi da i α ima isti oblik. Budući da α nije racionalan, prvi dio teorema je dokazan.

Dokažimo sada obrat. Neka je α kvadratna iracionalnost, tj. neka je $\alpha = \frac{a+\sqrt{b}}{c}, a, b, c \in \mathbb{Z}$ $b > 0, c \neq 0$ i b nije potpun kvadrat. Pomnožimo li brojnik i nazivnik od α sa $|c|$, dobivamo

$$\alpha = \frac{ac + \sqrt{bc^2}}{c^2} \quad \text{ili} \quad \alpha = \frac{-ac + \sqrt{bc^2}}{-c^2},$$

u ovisnosti o tome je li c pozitivan ili negativan. Stoga α možemo zapisati 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 $t_0 \mid (d - s_0^2)$.

Sada ćemo opisati razvoj $[a_0, a_1, \ldots]$ u jednostavni verižni razlomak broja α. Neka je $\alpha_0 = \alpha$, te neka je

$$a_i = \lfloor \alpha_i \rfloor, \quad \alpha_i = \frac{s_i + \sqrt{d}}{t_i}, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}. \tag{3}$$

Imamo:

$$\alpha_i - a_i = \frac{s_i + \sqrt{d} - a_i t_i}{t_i} = \frac{\sqrt{d} - s_{i+1}}{t_i} = \frac{d - s_{i+1}^2}{t_i(\sqrt{d} + s_{i+1})} = \frac{t_{i+1}}{\sqrt{d} + s_{i+1}} = \frac{1}{\alpha_{i+1}},$$

pa je zaista $\alpha = [a_0, a_1, \ldots]$.

Pokažimo matematičkom indukcijom da su s_i, t_i cijeli brojevi takvi da je $t_i \neq 0$ i $t_i \mid (d - s_i^2)$. To vrijedi za $i = 0$. Ako tvrdnja vrijedi za neki i, onda iz $s_{i+1} = a_i t_i - s_i$ slijedi da je s_{i+1} cijeli broj. Relacija

$$t_{i+1} = \frac{d - s_{i+1}^2}{t_i} = \frac{d - s_i^2}{t_i} + 2a_i s_i - a_i^2 t_i$$

pokazuje da je i t_{i+1} cijeli broj. Nadalje, $t_{i+1} \neq 0$, u suprotnom bi $d = s_{i+1}^2$ bio potpun kvadrat. Konačno, iz $t_i = \frac{d - s_{i+1}^2}{t_{i+1}}$ slijedi da $t_{i+1} \mid (d - s_{i+1}^2)$.

Označimo sada sa α_i' konjugat od α_i, tj. $\alpha_i' = \frac{s_i - \sqrt{d}}{t_i}$. Budući da je konjugat kvocijenata jednak kvocijentu konjugata, imamo $\alpha_0' = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}$. Odavde je

$$\alpha_n' = -\frac{q_{n-2}}{q_{n-1}} \left(\frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}} \right).$$

Kada $n \to \infty$, $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_{n-2}}{q_{n-2}}$ teže prema α_0, a $\alpha_0 \neq \alpha_0'$. Stoga izraz u zagradi teži prema 1, pa je zbog toga pozitivan za dovoljno velike n, recimo za $n > N$. Sada je za $n > N$ broj α_n' negativan. Ali, α_n je pozitivan za $n \geq 1$, pa je $\alpha_n - \alpha_n' = \frac{2\sqrt{d}}{t_n} > 0$. Dakle, $t_n > 0$ za $n > N$. Nadalje, za $n > N$ imamo

$$s_n^2 < s_n^2 + t_{n-1}t_n = d \Longrightarrow |s_n| < \sqrt{d},$$

dok iz $\alpha_n > 1$ i upravo dokazanog slijedi

$$t_n < s_n + \sqrt{d} < 2\sqrt{d}.$$

Iz ovoga slijedi da uređeni parovi (s_n, t_n) mogu poprimiti samo konačno mnogo vrijednosti, pa postoje prirodni brojevi $j, k,\ j < k$, takvi da je $s_j = s_k, t_j = t_k$. Sada (3) povlači da je $\alpha_j = \alpha_k$, pa je

$$\alpha = [a_0, \ldots, a_{j-1}, \overline{a_j, a_{j+1}, \ldots, a_{k-1}}],$$

što je i trebalo dokazati. □

Primijetimo da iz dokaza Teorema 2.6 slijedi algoritam za razvoj kvadratnih iracionalnosti u verižni razlomak, formule (3).

Primjer 2.3. *Razvijmo broj $\alpha = \frac{5+\sqrt{7}}{6}$ u verižni razlomak.*

Imamo $d = 7, s_0 = 5, t_0 = 6, \alpha_0 = \frac{5+\sqrt{7}}{6}$. Vidimo da vrijedi $t_0 \mid (d - s_{0^2})$, tj. $6 \mid (7 - 5^2)$, pa počnimo s postupkom (3) i raspišimo to tablično:

i	s_i	t_i	α_i	a_i
0	5	6	$\frac{5+\sqrt{7}}{6}$	1
1	1	1	$\frac{1+\sqrt{7}}{1}$	3
2	2	3	$\frac{2+\sqrt{7}}{3}$	1
3	1	2	$\frac{1+\sqrt{7}}{2}$	1
4	1	3	$\frac{1+\sqrt{7}}{3}$	1
5	2	1	$\frac{2+\sqrt{7}}{1}$	4
6	2	3		

Vidimo da je $s_2 = s_6, t_2 = t_6$, pa će biti $\alpha = [1, 3, \overline{1, 1, 1, 4}]$.

Teorem 2.7. *Kvadratna iracionalnost α ima čisto periodski razvoj u jednostavni verižni razlomak ako i samo ako je $\alpha > 1$ i $-1 < \alpha' < 0$, gdje je α' konjugat od α. (Za takvu kvadratnu iracionalnost kažemo da je reducirana.)*

Dokaz. Neka je $\alpha > 1$ i $-1 < \alpha' < 0$. Stavimo $\alpha_0 = \alpha$, te definirajmo rekurzivno α_i kao $\frac{1}{\alpha_{i+1}} = \alpha_i - a_i$. Tada je

$$\frac{1}{\alpha_{i+1}'} = \alpha_i' - a_i. \tag{4}$$

Sada je $a_i \geq 1$ za sve $i \geq 0$ (čak i za $i = 0$ zbog $\alpha > 1$). Zbog toga, ako je $\alpha_i' < 0$, onda je $\frac{1}{\alpha_{i+1}'} < -1$, odnosno $-1 < \alpha_{i+1}' < 0$. Kako je $-1 < \alpha_0' < 0$, indukcijom slijedi da je $-1 < \alpha_i' < 0$ za sve $i \geq 0$. Sada iz (4) slijedi

$$0 < -\frac{1}{\alpha_{i+1}'} - a_i < 1, \quad \text{tj.} \quad a_i = \left\lfloor -\frac{1}{\alpha_{i+1}'} \right\rfloor.$$

Iz Teorema 2.6 slijedi da postoje prirodni brojevi takvi da je $j < k$ i $\alpha_j = \alpha_k$. Sada je $\alpha'_j = \alpha'_k$, te

$$a_{j-1} = \left\lfloor -\frac{1}{\alpha'_j} \right\rfloor = \left\lfloor -\frac{1}{\alpha'_k} \right\rfloor = a_{k-1},$$
$$\alpha_{j-1} = a_{j-1} + \frac{1}{\alpha_j} = a_{k-1} + \frac{1}{\alpha_k} = \alpha_{k-1}.$$

Dakle, $\alpha_j = \alpha_k$ povlači da je $\alpha_{j-1} = \alpha_{k-1}$. Primjenimo li ovu implikaciju j puta, dobivamo $\alpha_0 = \alpha_{k-j}$, tj. $\alpha = [\overline{a_0, a_1, \ldots, a_{k-j}}]$.

Obrnuto, pretpostavimo da je razvoj od α čisto periodski,

$$\alpha = [\overline{a_0, a_1, \ldots, a_{n-1}}],$$

$a_0, a_1, \ldots, a_{n-1} \in \mathbb{N}$ (zbog $a_0 = a_n$). Imamo: $\alpha > a_0 \geq 1$. Također je

$$\alpha = [a_0, \ldots, a_{n-1}, \alpha] = \frac{\alpha p_{n-1} + p_{n-2}}{\alpha q_{n-1} + q_{n-2}}.$$

Prema tome, α zadovoljava kvadratnu jednadžbu

$$f(x) = x^2 q_{n-1} + x(q_{n-2} - p_{n-1}) - p_{n-2} = 0,$$

koja ima dva korijena, α i α'. Budući da je $\alpha > 1$, dovoljno je provjeriti da $f(x)$ ima korijen između -1 i 0. To ćemo provjeriti tako da pokažemo da $f(-1)$ i $f(0)$ imaju različite predznake. Vidimo da je $f(0) = -p_{n-2} < 0$, a $f(-1) = q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} > 0$ $\square$

3 Pellove jednadžbe

3.1 Osnovni pojmovi i rješenja Pellove jednadžbe

U ovom poglavlju upoznat ćemo se s Pellovim jednadžbama i njihovim rješenjima, te vidjeti kako su rješenja povezana s verižnim razlomcima.

Definicija 3.1. *Diofantska jednadžba*

$$x^2 - dy^2 = 1, \tag{5}$$

gdje je $d \in \mathbb{N}$ i d nije potpun kvadrat, zove se Pellova jednadžba.
Općenito, jednadžba oblika

$$x^2 - dy^2 = N, \tag{6}$$

gdje je d kao gore i $N \in \mathbb{N}$, zove se pellovska jednadžba.

Ako je $d \in \mathbb{N}$ potpun kvadrat, tj. $d = c^2, c \in \mathbb{Z}$ tada jednadžba (5) ima samo trivijalna rješenja. Naime iz $(x - cy)(x + cy) = 1$ slijedi $x - cy = x + cy = \pm 1$. Ako je $d \in \mathbb{Z}, d \leq 0$, jednadžba također ima samo trivijalno rješenje $(x, y) = (\pm 1, 0)$. Analogno vidimo da ako je $d \leq 0$ ili ako je d potpun kvadrat, jednadžba (6) ima najviše konačno mnogo rješenja.

Rješenje (x_1, y_1) u prirodnim brojevima jednadžbe (5) zvat ćemo najmanjim netrivijalnim rješenjem (fundamentalnim rješenjem) te jednadžbe ako za svako drugo rješenje (x_2, y_2) u prirodnim brojevima iste jednadžbe vrijedi $x_1 < x_2$. Uočimo da vrijedi: (x_1, y_1) je najmanje rješenje jednadžbe ako i samo ako vrijedi:

$$x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}. \tag{7}$$

To se može vidjeti iz sljedećeg: $x_1^2 - dy_1^2 = x_2^2 - dy_2^2$ povlači da je $x_1^2 - x_2^2 = d(y_1^2 - y_2^2)$ pa je $x_1 < x_2$ ako i samo ako $y_1 < y_2$. Stoga je (7) moguće ako i samo ako je $x_1 < x_2$.

Najmanje netrivijalno rješenje Pellove jednadžbe često nije lako naći. U nekim slučajevima, to ipak nije pretežak posao, kao npr. za jednadžbu $x^2 - 2y^2 = 1$. Njezino najmanje rješenje u prirodnim brojevima dano je s $(x, y) = (3, 2)$. No, napomenimo kako je najmanje rješenje jednadžbe $x^2 - 61y^2 = 1$ dano s $(x, y) = (1766319049, 226153980)$.

U nastavku ćemo pokazati da Pellova jednadžba uvijek ima beskonačno mnogo rješenja, svako od njih se može dobiti pomoću najmanjeg, a u tome će nam od velike koristi biti razvoj broja $\sqrt{d}$ u verižni razlomak.

Teorem 3.1. *Ako prirodan broj d nije potpun kvadrat, onda razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik:*

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

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, a $a_1, \ldots, a_{r-1}$ su centralno simetrični, tj. $a_1 = a_{r-1}, a_2 = a_{r-2}, \ldots$. Nadalje, u (3) uz $\alpha_0 = \sqrt{d}, t_0 = 1, s_0 = 0$, imamo $t_i \neq -1$ i $t_i = 1$ ako i samo ako $r \mid i$ (r označava duljinu najmanjeg perioda u razvoju od $\sqrt{d}$).

Dokaz. Promotrimo broj $\beta = \sqrt{d} + \lfloor \sqrt{d} \rfloor$. Očito je broj β reduciran, pa po Teoremu 2.7 ima čisto periodičan razvoj

$$\sqrt{d} + \lfloor \sqrt{d} \rfloor = [\overline{b_0, b_1, \ldots, b_{r-1}}] = [b_0, \overline{b_1, \ldots, b_{r-1}, b_0}]. \tag{8}$$

Razvoj od β i $\sqrt{d}$ se razlikuju samo u prvom članu, tj. $b_i = a_i$ za $i \geq 1$. Uočimo da je $b_0 = \lfloor \sqrt{d} + \lfloor \sqrt{d} \rfloor \rfloor = 2\lfloor \sqrt{d} \rfloor$. Sada je

$$\begin{aligned} \sqrt{d} &= -\lfloor \sqrt{d} \rfloor + \beta \\ &= -\lfloor \sqrt{d} \rfloor + [2\lfloor \sqrt{d} \rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}] \\ &= [\lfloor \sqrt{d} \rfloor, \overline{b_1, \ldots, b_{r-1}, b_0}] \\ &= [a_0, a_1, \ldots, a_{r-1}, 2a_0]. \end{aligned}$$

Da bi dokazali centralnu simetričnost, uočimo da je $\beta = b_0 + \frac{1}{\beta_1}$, gdje je

$$\begin{aligned} \beta_1 &= (\sqrt{d} - \lfloor \sqrt{d} \rfloor)^{-1} = -\frac{1}{\beta'} = -\frac{1}{\beta'_r} = \text{zbog (4)} = \left[b_{r-1}, -\frac{1}{\beta'_{r-1}} \right] = \ldots \\ &= \left[b_{r-1}, b_{r-2}, \ldots, b_0, -\frac{1}{\beta'} \right] \\ &= [\overline{b_{r-1}, b_{r-2}, \ldots, b_0}]. \end{aligned}$$

Dakle, $\beta = [b_0, \overline{b_{r-1}, b_{r-2}, \ldots, b_0}]$. Usporedimo li ovo s (8), dobivamo da je $b_1 = b_{r-1}$, $b_2 = b_{r-2} \ldots$.
Budući da je r duljina najmanjeg perioda, imamo da je $\beta_i = \beta$ ako i samo ako $r \mid i$.
Ako sada primjenimo algoritam (3) na $\beta_0 = \sqrt{d} + \lfloor \sqrt{d} \rfloor, t_0 = 1, s_0 = \lfloor \sqrt{d} \rfloor$, onda za sve $j \geq 0$ imamo:

$$\frac{s_{jr} + \sqrt{d}}{t_{jr}} = \beta_{jr} = \beta_0 = \frac{s_0 + \sqrt{d}}{t_0} = \lfloor \sqrt{d} \rfloor + \sqrt{d},$$

odnosno

$$s_{jr} - t_{jr} \lfloor \sqrt{d} \rfloor = (t_{jr} - 1)\sqrt{d},$$

pa je $t_{jr} = 1$ jer je $\sqrt{d}$ iracionalan. Nadalje, $t_i \neq 1$ za sve ostale vrijednosti od i. Zaista, $t_i = 1$ povlači $\beta_i = s_i + \sqrt{d}$. No, β_i ima čisto periodski razvoj, pa je po Teoremu 2.7, $-1 < s_i - \sqrt{d} < 0$. Odavde je $\sqrt{d} - 1 < s_i < \sqrt{d}$, tj. $s_i = \lfloor \sqrt{d} \rfloor$, pa je $\beta_i = \beta$, što povlači da $r \mid i$.

Neka je sada $t_i = -1$. Onda je $\beta = -s_i - \sqrt{d}$, pa Teorem 2.7 povlači da je $-s_i - \sqrt{d} > 1$ i $-1 < -s_i + \sqrt{d} < 0$, pa je $\sqrt{d} < s_i < -\sqrt{d} - 1$, što je očito nemoguće. □

Teorem 3.2.

$$p_n^2 - dq_n^2 = (-1)^{n+1} t_{n+1}, \quad \textit{za sve} \quad n \geq -1.$$

Dokaz. Iz (3) imamo:

$$\sqrt{d} = \alpha_0 = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} = \frac{(s_{n+1} + \sqrt{d}) p_n + t_{n+1} p_{n-1}}{(s_{n+1} + \sqrt{d}) q_n + t_{n+1} q_{n-1}}.$$

Budući da je $\sqrt{d}$ iracionalan, slijedi

$$s_{n+1} q_n + t_{n+1} q_{n-1} - p_n = 0, \quad s_{n+1} p_n + t_{n+1} p_{n-1} - d q_n = 0.$$

Eliminirajući s_{n+1}, dobivamo

$$p_n^2 - dq_n^2 = (p_n q_{n-1} - p_{n-1} q_n) t_{n+1} = (-1)^{n-1} t_{n+1}.$$

□

Teorem 3.3. *Neka je d prirodan broj koji nije potpun kvadrat, te neka su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je N cijeli broj, $|N| < \sqrt{d}$. Tada svako pozitivno rješenje $x = u, y = v$ jednadžbe $x^2 - dy^2 = N$, takvo da je $(u, v) = 1$, zadovoljava $u = p_n, v = q_n$ za neki $n \in \mathbb{N}$.*

Dokaz. Neka su $E, M \in \mathbb{N}$ takvi da je $(E, M) = 1$ i $E^2 - \varrho M^2 = \sigma$, gdje je $\sqrt{\varrho}$ iracionalan i $0 < \sigma < \sqrt{\varrho}$, σ i ϱ su realni brojevi, ne nužno cijeli. Tada je $\frac{E}{M} - \sqrt{\varrho} = \frac{\sigma}{M(E+M\sqrt{\varrho})}$ pa je

$$0 < \frac{E}{M} - \sqrt{\varrho} < \frac{\sqrt{\varrho}}{M(E + M\sqrt{\varrho})} = \frac{q}{M^2(\frac{E}{M\sqrt{\varrho}} + 1)} < \frac{1}{2M^2}.$$

Po Teoremu 2.5, $\frac{E}{M}$ je konvergenta u razvoju od $\sqrt{\varrho}$.

Ako je $N > 0$, uzmimo $\sigma = N, \varrho = d, E = u, M = v$, pa dobivamo tvrdnju teorema u ovom slučaju.

Ako je $N < 0$, onda je $v^2 - \frac{1}{d}u^2 = -\frac{N}{d}$, pa možemo uzeti $\sigma = -\frac{N}{d}, \varrho = \frac{1}{d}, E = v, M = u$. Dobivamo da je $\frac{v}{u}$ konvergenta u razvoju od $\frac{1}{\sqrt{d}}$. No, ako je $\frac{v}{u}$ n-ta konvergenta od $\frac{1}{\sqrt{d}}$, onda je $\frac{u}{v}(n-1)$-va konvergenta od $\sqrt{d}$, pa je teorem dokazan i u ovom slučaju. □

Iz Teorema 3.1, 3.2 i 3.3 neposredno slijedi:

Teorem 3.4. *Sva rješenja u prirodnim brojevima jednadžbi $x^2 - dy^2 = \pm 1$ nalaze se među $x = p_n, y = q_n$, gdje su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je r duljina perioda u razvoju od $\sqrt{d}$.*

Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana s $x = p_{nr-1}, y = q_{nr-1}$ za $n \in \mathbb{N}$.

Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana s $x = p_{nr-1}, y = q_{nr-1}$ za n neparan, dok su sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana s $x = p_{nr-1}, y = q_{nr-1}$ za n paran.

Teorem 3.5. *Ako je (x_1, y_1) najmanje rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$, onda su sva rješenja ove jednadžbe dana s (x_n, y_n) za $n \in \mathbb{N}$, gdje su x_n i y_n prirodni brojevi definirani s*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{9}$$

Dokaz. Iz (9) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je

$$x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = 1,$$

što znači da su (x_n, y_n) zaista rješenja.

Pretpostavimo sada da je (s, t) rješenje koje se ne nalazi u familiji

$$\{(x_n, y_n) : n \in \mathbb{N}\}.$$

Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, postoji $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{10}$$

Pomnožimo li (10) s $(x_1 - y_1\sqrt{d})^m$, dobivamo

$$1 < (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m < x_1 + y_1\sqrt{d}.$$

Definirajmo $a, b \in \mathbb{Z}$ s $a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m$. Imamo: $a^2 - db^2 = (s^2 - dt^2)(x_1^2 - dy_1^2)^m = 1$. Iz $a + b\sqrt{d} > 1$ slijedi $0 < a - b\sqrt{d} < 1$, pa je

$$\begin{aligned} 2a &= (a + b\sqrt{d}) + (a - b\sqrt{d}) > 0, \\ 2b\sqrt{d} &= (a + b\sqrt{d}) - (a - b\sqrt{d}) > 0. \end{aligned}$$

Stoga je (a, b) rješenje u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ i $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$, što je kontradikcija s pretpostavkom da je (x_1, y_1) najmanje rješenje. □

Teorem 3.6. *Neka je $(x_n, y_n), n \in \mathbb{N}$ niz svih rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima, zapisan u rastućem redosljedu. Uzmimo da 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. Vrijedi $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$. Odavde je

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

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 $x_{n+2} = 2x_1x_{n+1} - x_n$.
Analognim računom, tj. izjednačavanjem članova uz $\sqrt{d}$ imamo

$$\begin{aligned} y_{n+2} &= x_1y_{n+1} + y_1y_{n+1}, \\ y_n &= x_1y_{n+1} - y_1x_{n+1}, \end{aligned}$$

pa ponovo zbrajanjem dobivamo $y_{n+2} = 2x_1y_{n+1} - y_n$.

□

3.2 Primjeri

Proučimo sada neke primjere i probleme koji se se svode na analizu skupa rješenja Pellove jednadžbe.

Primjer 3.1. *Nađimo najmanja rješenja jednadžbi $x^2 - 29y^2 = -1$ i $x^2 - 29y^2 = 1$ u prirodnim brojevima (ako postoje).*

Rješenje. Razvijmo broj $\sqrt{29}$ u verižni razlomak koristeći postupak (3).

i	s_i	t_i	α_i	a_i
0	0	1	$\sqrt{29}$	5
1	5	4	$\frac{5+\sqrt{29}}{4}$	2
2	3	5	$\frac{3+\sqrt{29}}{5}$	1
3	2	5	$\frac{2+\sqrt{29}}{5}$	1
4	3	4	$\frac{3+\sqrt{29}}{4}$	2
5	5	1	$\frac{5+\sqrt{29}}{1}$	10
6	5	4		

Kako je $s_1 = s_6, t_1 = t_6$ razvoj od $\sqrt{29}$ u verižni razlomak je oblika $\sqrt{29} = [5, \overline{2, 1, 1, 2, 10}]$, iz čega vidimo da je period $r = 5$ neparan. Tada je prema Teoremu 3.4 najmanje rješenje od $x^2 - 29y^2 = -1$ dano s $(p_{1\cdot 5-1}, q_{1\cdot 5-1}) = (p_4, q_4)$, a najmanje rješenje od $x^2 - 29y^2 = 1$ s $(p_{2\cdot 5-1}, q_{2\cdot 5-1}) = (p_9, q_9)$. Sada prema Teoremu 2.1 računamo p_i, q_i, za $i = -1, 0, 1, \ldots, 9$.

i	a_i	p_i	q_i
-1		1	0
0	5	5	1
1	2	11	2
2	1	16	3
3	1	27	5
4	2	70	13
5	10	727	135
6	2	1524	283
7	1	2251	418
8	1	3775	701
9	2	9801	1820

Dakle, $(p_4, q_4) = (70, 13), (p_9, q_9) = (9801, 1820)$.
Uočimo da je $(70 + 13\sqrt{29})^2 = 9801 + 1820\sqrt{29}$. □

Primjer 3.2. *Neka je (x_n, y_n) rastući niz rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima. Pokažimo 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 provodimo indukcijom po m. Uvrštavanjem $m = 1$ u prve dvije jednakosti dobivamo

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

Prema računu kojeg smo koristili u dokazu Teorema 3.6, izjednačavanjem slobodnih članova i članova uz $\sqrt{d}$, gornje jednakosti vrijede za svaki prirodni broj n.
Pretpostavimo da jednakost vrijedi za $m = k$, tj.

$$\begin{aligned} x_{n+k} &= x_k x_n + d y_k y_n, \\ y_{n+k} &= x_k y_n + y_k x_n. \end{aligned}$$

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 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 $m = n$.

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

□

Primjer 3.3. *Neka su m i d proizvoljni prirodni brojevi i d nije potpun kvadrat. Pokažimo 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

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

Kvadriranjem i grupiranjem imamo

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

Označimo li dk^2 s d', dobivamo jednadžbu

$$x^2 - d'm^2 = 1,$$

d' nije potpun kvadrat (jer d nije potpun kvadrat), koja prema Teoremu 3.5 ima beskonačno mnogo rješenja u prirodnim brojevima. Time je tvrdnja pokazana. □

Primjer 3.4. *Pokažimo da postoji beskonačno mnogo prirodnih brojeva n sa svojstvom da je suma prvih n prirodnih brojeva jednaka kvadratu nekog prirodnog broja. Nađimo barem dva prirodna broja s tim svojstvom.*

Rješenje. Neka su $m, n \in \mathbb{N}$ takvi da vrijedi

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

tj.

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

Množenjem s 8 dobivamo

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

Sada, svođenjem na potpuni kvadrat imamo

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

odnosno

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

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

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

Prema Teoremu 3.5 jednadžba ima beskonačno mnogo rješenja u $\mathbb{N}$. Najmanje rješenje je očito $(x_1, y_1) = (3, 1)$. Stoga iz $2n_1 + 1 = x_1$ slijedi $n_1 = 1$, a $m_1 = 1$. Zaista, vrijedi $1 = 1^2$. Sva rješenja jednadžbe $x^2 - 8y^2 = 1$ dana su s

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

Neka je npr. $k = 2$. Sada je

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

Stoga je $2n_2 + 1 = x_2 = 17$, odakle slijedi $n_2 = 8$, a $m_2 = 6$. Zaista vrijedi $\sum_{i=1}^{8} i = 6^2$.

Analogno, možemo pronaći beskonačno mnogo parova (n, m) tako da je $\sum_{i=1}^{n} i = m^2$.

□

4 Arhimedov problem stoke

U ovom poglavlju proučit ćemo zanimljiv problem kojem se rješenje nalazi pomoću Pellove jednadžbe, a to je problem poznat kao Arhimedov problem stoke.

Arhimedov problem stoke je napisan u formi epigrama u 44 retka. Epigram je kratka pjesnička forma koja je bila izrazito prisutna u starogrčkoj književnosti, pomoću koje su se izražavale javne ili prigodne poruke (čestitke, iskaz sućuti, molba), ili pak rugalice, bilo nekim osobama, bilo zbivanjima u piščevoj okolini. Tako je i Arhimedov epigram nastao kao njegov odgovor na zanovijetanja Apolonija iz Perga (262.–190. g. pr. Kr.) koji je Arhimedu predbacivao da je sklon matematičkim problemima čije rješavanje zahtijeva naporna i dugotrajna računanja. Arhimed je inspiraciju za pisanje epigrama vrlo vjerojatno našao u Homerovoj *Odiseji*, a ovdje je dan njegov slobodan prijevod:

Ako si marljiv i mudar, stranče, izračunaj broj
Sunčevih goveda što su nekoć pasla na poljima
Trinakije na otoku Siciliji, podijeljenih u četiri stada
različitih boja: jednog bijelog kao snijeg, drugog
blještavo crnog, trećeg žutog i četvrtog šarenog.

U svakom je stadu bilo mnoštvo bikova:

Broj bijelih bio je jednak zbroju polovine i trećine
crnih i još k tome valja dodati sve žute.

Broj crnih dobije se kad četvrtini i petini šarenih
pridodamo i opet sve žute.

Znaj da je šarenih bilo koliko je zbroj šestine
bijelih i njihove sedmine, a i ovima valja pridodati
sve žute.

A evo koliko krava bijaše:

Bijelih je bilo točno onoliko koliko iznosi trećina i
četvrtina cjelokupnog krda crnih.

Broj crnih bio je jednak zbroju četvrtine i petine
sve šarene stoke.

Šarenih je krava bilo onoliko koliki je zbroj petine i
šestine sve žute stoke u stadu.

Naposljetku, žute su krave po broju bile jednake
zbroju šestine i sedmine bijeloga krda.

Mogneš li, stranče, točno reći broj Sunčevih
goveda, utvrdivši ponaosob broj gojnih bikova i k
tome broj krava prema njihovoj boji, neću te držati

nevježom i neznalicom po pitanju brojeva, no još uvijek te neću ubrojiti niti među mudre.

No, hajde razmisli još i o ovim uvjetima koji se odnose na Sunčeva goveda:

Kad se bijeli volovi izmiješaju s crnima te rasporede tako da u širinu stane jednako kao u dubinu, ispunit će se dolina Trinakije njihovim mnoštvom.

A ako se žuti i šareni bikovi skupe u jedno krdo tako da među njima ne bude nijednog vola druge boje niti ijedan od žutih ili šarenih ne uzmanjka, oni će se moći rasporediti tako da im broj po redovima raste, počev od broja jedan, te se tako napuni triangularni broj.

Uzmogneš li, stranče, riješiti sve ovo, završit ćeš okrunjen slavom i smatrat će te nenadmašnim u mudrosti.

Sam problem se pojavio 1773. godine u prijevodu njemačkog pisca Gottholda Ephraima Lessinga. On je, proučavajući i prevodeći rukopise i djela pisana na grčkom i latinskom jeziku, naišao na problem stoke. Opće rješenje problema dao je 1880. godine njemački matematičar A. Amthor koji je pokazao da je rezultat približno jednak $7.76 \cdot 10^{206544}$, što je broj s 206545 znamenki, kojemu su prve četiri znamenke 7760.
Grupa matematičara pod nazivom The Hillsboro Mathematical Club koju su činili matematičari E. Fish, G. H. Richards i A. H. Bell u godinama od 1889. do 1893. izračunali su prvu 31 i posljednjih 12 znamenki najmanjeg rješenja problema:

$$7760271406486818269530232833209\ldots$$
$$\ldots 719455081800$$

O složenosti ovog problema i o tome kako je računanje prije pojave računala bilo složeno, lijepo se vidi u tekstu objavljenom u *The New York Timesu* 18. siječnja 1931.: *"Budući da bi izračun zahtijevao tisuću ljudi i tisuću godina, jasno je da svijet nikad neće dočekati cjelokupno rješenje."*. No, ipak su ga dočekali i to 1965. godine. Matematičari H. C. Williams, R. A. German i C. R. Zarnke, s kanadskog Sveučilišta Waterloo, primjenom računala IBM 7040 odredili su točan broj, sve njegove znamenke. Računalu je za izračun trebalo 7 sati i 49 minuta. Provjeru tog rezultata proveo je 16 godina kasnije Harry L. Nelson na glasovitom računalu Cray-1, a broj s 206545 znamenki ispisan je na 47 listova papira. Ovdje je zapravo bila riječ o testiranju novoproizvedenog računalnog čuda. Račun je, zajedno s provjerom točnosti, trajao desetak minuta. Nelson je uz najmanje našao i pet sljedećih rješenja od kojih je posljednje imalo više od milijun znamenki.

Prihvatimo se sada rješavanja samog problema. Zamislimo stado koje se sastoji od krava i bikova bijele, crne i žute boje, a neki su i šareni. Brojevi pojedine skupine su međusobno povezani određenim uvjetima, stoga za njihov lakši zapis uvedimo sljedeće oznake:

B – broj bijelih bikova,

b – broj bijelih krava,

C – broj crnih bikova,

c – broj crnih krava,

Z – broj žutih bikova,

z – broj žutih krava,

S – broj šarenih bikova,

s – broj šarenih krava.

Uz ove oznake problem svodimo na sljedeći sustav jednadžbi:

1. $B = \left(\frac{1}{2} + \frac{1}{3}\right) \cdot C + Z$,
2. $C = \left(\frac{1}{4} + \frac{1}{5}\right) \cdot S + Z$,
3. $S = \left(\frac{1}{6} + \frac{1}{7}\right) \cdot B + Z$,
4. $b = \left(\frac{1}{3} + \frac{1}{4}\right) \cdot (C + c)$,
5. $c = \left(\frac{1}{4} + \frac{1}{5}\right) \cdot (S + s)$,
6. $s = \left(\frac{1}{5} + \frac{1}{6}\right) \cdot (Z + z)$,
7. $z = \left(\frac{1}{6} + \frac{1}{7}\right) \cdot (B + b)$.

Uz to su postavljena još dva uvjeta:

8. $B + C$ je potpuni kvadrat,
9. $Z + S$ je oblika $\frac{n(n+1)}{2}$, tj. suma prvih n prirodnih brojeva (ukupan broj točaka koje se mogu razmjestiti u obliku trokuta).

Prvih sedam jednadžbi čine homogeni linearni sustav s osam nepoznanica, njega nije problem riješiti nekim od računalnih programa, no pogledajmo kako to izgleda ako ga riješimo "pješice".
Pomnožimo redom, prvu jednadžbu s 336, drugu s 280, treću s 126. Dobivamo:

$$\begin{aligned} 336B &= 280C + 336Z, \\ 280C &= 126S + 280Z, \\ 126S &= 39B + 126Z. \end{aligned}$$

Zbrojimo li te tri jednadžbe dobivamo:

$$297B = 742Z,$$

odnosno

$$3^3 \cdot 11B = 2 \cdot 7 \cdot 53Z.$$

Zatim iz druge i treće nalazimo

$$3^4 \cdot 11S = 2^2 \cdot 5 \cdot 79Z,$$

odnosno

$$3^2 \cdot 11C = 2 \cdot 89Z.$$

Analogno postupimo sa sljedeće četiri jednadžbe, prvu množimo s 4800, drugu s 2800, treću s 1260, četvrtu s 462 i dobivamo:

$$\begin{aligned} 3^3 \cdot 11 \cdot 4657b &= 2^3 \cdot 5 \cdot 7 \cdot 23 \cdot 373Z, \\ 3^2 \cdot 11 \cdot 4657z &= 13 \cdot 46489Z, \\ 3^3 \cdot 4657s &= 2^2 \cdot 5 \cdot 7 \cdot 761Z, \\ 3^2 \cdot 11 \cdot 4657c &= 2 \cdot 17 \cdot 15991Z. \end{aligned}$$

Kako rješenja moraju biti cijeli brojevi, promatrajući gornje jednakosti zaključujemo da broj Z mora biti djeljiv s $3^4 \cdot 11 \cdot 4657$, tj. možemo pisati:

$$Z = 3^4 \cdot 11 \cdot 4657 \cdot k = 4149387 \cdot k.$$

Na ovaj način smo došli do općeg rješenja sustava sedam linearnih jednadžbi sa osam nepoznanica, uz uvjet da su ta rješenja prirodni brojevi:

$$\begin{aligned} B &= 2 \cdot 3 \cdot 7 \cdot 53 \cdot 4657k = 10366482 \cdot k, \\ C &= 2 \cdot 3^2 \cdot 89 \cdot 4657k = 7460514 \cdot k, \\ Z &= 3^4 \cdot 11 \cdot 4657 \cdot k = 4149387 \cdot k, \\ S &= 2^2 \cdot 5 \cdot 79 \cdot 4657 \cdot k = 7358060 \cdot k, \\ b &= 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 23 \cdot 373k = 7206360 \cdot k, \\ c &= 2 \cdot 3^2 \cdot 17 \cdot 15991k = 4893246 \cdot k, \\ z &= 3^2 \cdot 13 \cdot 46489k = 5439213 \cdot k, \\ s &= 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 761k = 3515820 \cdot k, \end{aligned}$$

gdje je $k \in \mathbb{N}$. Ako ih sada sve pozbrajamo, dobijemo da je to ukupno $50389082 \cdot k$ komada stoke.

Jedan od dodatnih uvjeta kaže da je broj $B + C$ potpun kvadrat, tj. $B + C = m^2, m \in \mathbb{N}$. Odnosno:

$$\begin{aligned} m^2 &= 2 \cdot 3 \cdot (7 \cdot 53 + 3 \cdot 89) \cdot 4657 \cdot k \\ &= 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657 \cdot k. \end{aligned}$$

Očigledno je $k = 3 \cdot 11 \cdot 29 \cdot 4657 \cdot t^2, t \in \mathbb{Z}$.

Tada je rješenje sustava što ga čini sedam jednadžbi uz dodatni uvjet da je $B + C$ potpun kvadrat dano s:

$$\begin{aligned} B &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 29 \cdot 53 \cdot 4657^2t^2 = 462008082870 18t^2, \\ C &= 2 \cdot 3^3 \cdot 11 \cdot 29 \cdot 89 \cdot 4657^2t^2 = 33240638308986 \cdot t^2, \\ Z &= = 3^5 \cdot 11^2 \cdot 29 \cdot 4657^2t^2 = 18492776362863 \cdot t^2, \\ S &= 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 29 \cdot 79 \cdot 4657^2t^2 = 32793026546940 \cdot t^2, \\ b &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 \cdot 29 \cdot 373 \cdot 4657t^2 = 32116937723640 \cdot t^2, \\ c &= 2 \cdot 3^3 \cdot 11 \cdot 17 \cdot 29 \cdot 4657 \cdot 15991t^2 = 21807969217254 \cdot t^2, \\ z &= 3^3 \cdot 11 \cdot 13 \cdot 29 \cdot 4657 \cdot 46489t^2 = 24241207098537 \cdot t^2, \\ s &= 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2 \cdot 29 \cdot 761 \cdot 4657t^2 = 15669127269180 \cdot t^2. \end{aligned}$$

Posljednji uvjet zahtijeva da je $Z+S$ trokutni broj, tj. $Z+S=\frac{n(n+1)}{2}$. Primijetimo da je broj trokutni ako i samo ako je $8(Z+S)+1=(2n+1)^2$, a kako je $Z+S=4149387\cdot k+7358060\cdot k=11507447\cdot k$, imamo

$$8(11507447k)+1=(2n+1)^2.$$

Ako sada uvrstimo nađenu vrijednost za k imamo jednadžbu:

$$8(11507447\cdot 3\cdot 11\cdot 29\cdot 4657t^2)+1=(2n+1)^2,$$

koju ćemo zapisati u obliku:

$$(2n+1)^2-2\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353\cdot(2\cdot 4657t)^2=1,$$

i kojoj trebamo naći sva cjelobrojna rješenja. Uvrstimo li sada da je $2n+1=x$ i $2\cdot 4567t=y$, dobivamo jednadžbu oblika:

$$x^2-4729494y^2=1,$$

koja je zapravo Pellova jednadžba. Upravo na ovaj način je Amthor došao do rješenja problema, tj. do rezultata koji iskazuje najmanji mogući ukupan broj stoke.
Najmanja rješenja dane Pellove jednadžbe su:

$$\begin{aligned} x &= 109931986732829734979866232821433543901088049 \\ y &= 50549485234315033074477819735540408986340 \end{aligned}$$

Zbog ogromnih brojeva nećemo se upuštati u njezino rješavanje.
Američki matematičar Vardi kaže: "Teško je povjerovati da je Arhimed mogao riješiti ovaj problem", a nije čak niti izgledno da bi znao postoji li njegovo rješenje. On je također izračunao najmanji mogući broj stoke:

$$\left\lceil \frac{25194541}{184119152}\cdot[109931986732897349798662328214335439010880 49+ \right.$$
$$\left. 50549485234331503307447781973554040898634 0\cdot\sqrt{4729494}]^{4658}\right\rceil$$

Teško je uopće zamisliti da toliki broj stoke stane na otok Siciliju, no bog Sunca Helios, kome pripada"Sunčeva stoka", bi se već nekako nosio s time. Za kraj se možemo složiti s Vardijevom rečenicom: "Jednostavnost problema i složenost rješenja sjajan su izazov, a sam je problem još jedan prilog tvrdnji da je Arhimed jedan od najvećih matematičara svih vremena."

Literatura

[1] B. Dakić, Arhimedov problem stoke, Matematika i škola, 51(2009), 34-37

[2] A. Dujella, Uvod u teoriju brojeva, Skripta, PMF - matematički odjel, Sveučilište u Zagrebu, 2003

[3] A. Dujella, Diofantske jednadžbe, Skripta, PMF - matematički odjel, Sveučilište u Zagrebu, 2006

[4] I. Mandić, I. Soldo, Pellova jednadžba, Osječki matematički list, 8(2008), 29-36

[5] I. Matić, Uvod u teoriju brojeva, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, 2015

[6] V. Petričević, Periodski verižni razlomci, Magistarski rad, PMF - matematički odjel, Sveučilište u Zagrebu, 2009