Pellova jednadžba i verižni razlomci

Pretković, Petra

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Petra Pretković

PELLOVA JEDNADŽBA I VERIŽNI RAZLOMCI

Diplomski rad

Voditelj rada:
dr.sc. Vinko Petričević
Suvoditelj:
Izv.prof.dr.sc.
Matija Kazalicki

Zagreb, 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj diplomski rad posvećujem svojim roditeljima i sestri koji su me podržavali, vjerovali u mene i bili moj oslonac svih ovih godina.

Zahvaljujem mentoru dr.sc.Vinku Petričeviću na savjetima i vodstvu tijekom izrade ovog diplomskog rada.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

U ovom diplomskom radu bavit ćemo se Pellovom jednadžbom i njezinom vezom s verižnim razlomcima. Diofantska jednadžba oblika $x^2 - dy^2 = 1$, gdje je d prirodan broj koji nije potpuni kvadrat, naziva se Pellova jednadžba. Pellovom jednadžbom se često nazivaju i jednadžbe $x^2 - dy^2 = \pm 1, \pm 4$, no u ovom radu bavit ćemo se samo jednadžbom oblika $x^2 - dy^2 = 1$.
Jednadžba je dobila ime prema engleskom matematičaru Johnu Pellu[1]. Smatra se kako je Euler pomiješao Brounckerova i Pellova postignuća te je pogrešno Pellu pripisao zasluge za njezino rješavanje. Jedina poveznica između Pella i Pellove jednadžbe je knjiga *Teutsche Algebra* koja sadrži primjere Pellove jednadžbe. Objavio ju je 1658.godine J.Rahn[2], a Pell mu je pomogao u njezinu pisanju.
U prvom poglavlju govorit će se o diofantskim jednadžbama, linearnim i nelinearnim, te će se vidjeti njihova veza s Pellovom jednadžbom.
U drugom će poglavlju riječ biti o Pellovoj jednadžbi i verižnim razlomcima. Govorit ćemo o egzistenciji i strukturi rješenja Pellove jednadžbe, definirat ćemo verižne razlomke, navesti glavne tvrdnje vezane uz verižne razlomke te će biti dana veza rješenja Pellove jednadžbe s verižnim razlomcima.
U trećem, ujedno i posljednjem, poglavlju dan je povijesni pregled razvoja Pellove jednadžbe.

[1] John Pell (1611.-1685.), engleski matematičar i političar
[2] Johann Rahn (1622.-1676), švicarski matematičar

Poglavlje 1

Diofantske jednadžbe

Diofantske jednadžbe dobile su naziv po grčkom matematičaru Diofantu[1]. Diofant je prvi sustavno proučavao jednadžbe s više nepoznanica te je tražio njihova pozitivna racionalna rješenja. Danas pod diofantskim jednadžbama podrazumijevamo algebarske jednadžbe s više nepoznanica s cjelobrojnim koeficijentima kojima tražimo cjelobrojna rješenja.

Algebarska jednadžba s dvije ili više nepoznanica s cjelobrojnim koeficijentima, kojoj se traže cjelobrojna ili racionalna rješenja naziva se **diofantska jednadžba**.

Diofantske jednadžbe dijelimo na:

1. Linearne diofantske jednadžbe
2. Nelinearne diofantske jednadžbe (barem drugog stupnja).

1.1 Linearne diofantske jednadžbe

Diofantske jednadžbe oblika

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{1.1}$$

gdje su $a_1, a_2, \ldots a_n, b$ *cjelobrojni koeficijenti, a* $x_1, x_2, \ldots x_n$ *nepoznanice nazivamo* **linearne diofantske jednadžbe**.

Za početak promatrat ćemo uvjet rješivosti i strukturu rješenja najjednostavnije linearne diofantske jednadžbe s dvije nepoznanice $ax + by = c$, gdje su a, b i c cijeli brojevi, a x i y nepoznanice.

[1] Diofant Aleksandrijski (3.st.pr.Kr.), grčki matematičar

Teorem 1.1.1. *Neka su a, b, c cijeli brojevi i $d = nzd\,(a, b)$. Ako $d \nmid c$, onda jednadžba*

$$ax + by = c \tag{1.2}$$

nema cjelobrojnih rješenja. Ako $d \mid c$, onda jednadžba (1.2) *ima beskonačno mnogo cjelobrojnih rješenja. Ako je (x_1, y_1) jedno rješenje od* (1.2)*, onda su sva rješenja dana s $x = x_1 + \frac{b}{d} \cdot t, y = y_1 - \frac{a}{d} \cdot t$, gdje je $t \in \mathbb{Z}$.*

Napomena 1.1.2. *Cijeli broj d zovemo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$. Najveći među njima zove se* ***najveći zajednički djelitelj*** *od a i b i označava se s $nzd\,(a, b)$.*

Prije samog dokaza ovog teorema iskazat ćemo teorem koji će nam pomoći u njegovom dokazivanju (dokaz iskazanog teorema nalazi se u [5]):

Teorem 1.1.3. *Neka su a i m prirodni brojevi te b cijeli broj. Kongruencija $ax \equiv b\ (mod\ m)$ ima rješenja ako i samo ako $d = nzd\,(a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.*

Napomena 1.1.4. *Ako cijeli broj $m \neq 0$ dijeli razliku $a - b$, onda kažemo da je a kongruentan b modulo m i pišemo $a \equiv b\ (mod\ m)$.*

Sada možemo provesti dokaz Teorema 1.1.1.

Dokaz. Ako jednadžba (1.2) ima rješenje (x_1, y_1), onda $d \mid ax_1 + by_1$ pa $d \mid c$. Pretpostavimo da $d \mid c$ i promotrimo kongruenciju $ax \equiv c \pmod{b}$. Prema Teoremu 1.1.3. promatrana kongruencija ima rješenja i ako je x_1 neko rješenje, onda su sva rješenja kongruencije dana sa $x = x_1 + \frac{b}{d} \cdot k \pmod{b}$, gdje je $k = 0, 1, 2, \ldots, d - 1$. Stoga su sva rješenja jednadžbe (1.2) dana sa

$$x = x_1 + \frac{b}{d} \cdot t, t \in \mathbb{Z}. \tag{1.3}$$

Uvrstimo li (1.3) u (1.2) dobijemo: $by = c - ax_1 - \frac{ab}{d} \cdot t = by_1 - \frac{ab}{d} \cdot t$ pa je $y = y_1 - \frac{a}{d} \cdot t$. □

Teorem 1.1.5. *Neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi različiti od nule. Tada linearna diofantska jednadžba*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{1.4}$$

ima rješenja ako i samo ako $nzd\,(a_1, a_2, \ldots, a_n) \mid c$. Nadalje, ako jednadžba (1.4) *ima barem jedno rješenje, onda ih ima beskonačno mnogo.*

Dokaz. Pretpostavimo da jednadžba (1.4) ima rješenje.
Tada očito vrijedi $nzd\,(a_1, a_2, \ldots, a_n) \mid c$.
Drugi smjer implikacije, ako $nzd\,(a_1, a_2, \ldots, a_n) \mid c$ onda jednadžba (1.4) ima beskonačno

mnogo rješenja, dokazat ćemo matematičkom indukcijom. Za $n = 2$ tvrdnja vrijedi primjenom Teorema 1.1.1. Pretpostavimo da tvrdnja vrijedi za jednadžbe s $n - 1$ varijabli. Neka je $d = \text{nzd}\,(a_{n-1}, a_n)$. Prema pretpostavci, jednadžba $a_1x_1 + \cdots + a_{n-2}x_{n-2} + dy = c$ ima beskonačno mnogo rješenja $(x_1, \ldots, x_{n-2}, y)$. Za svako rješenje ove jednadžbe promotrimo jednadžbu

$$a_{n-1}x_{n-1} + a_nx_n = dy. \tag{1.5}$$

Budući da nzd $(a_{n-1}, a_n) \mid dy$, slijedi da jednadžba (1.5) ima beskonačno mnogo rješenja (x_{n-1}, x_n). Time smo dobili beskonačno mnogo rješenja $(x_1, \ldots, x_n)$ jednadžbe (1.4). □

1.2 Nelinearne diofantske jednadžbe

Jednadžbe s cjelobrojnim koeficijentima u kojima se nepoznanice ne pojavljuju u prvoj potenciji već sadrže i članove višeg reda nazivamo **nelinearne diofantske jednadžbe**.

Ne postoji univerzalna metoda rješavanja nelinearnih diofantskih jednadžbi, ali postoji niz metoda kojima rješavamo neke specijalne tipove tih jednadžbi. Najčešće korištene metode su:

1. metoda faktorizacije
2. metoda kvocijenta
3. metoda zbroja
4. metoda ostataka
5. metoda posljednje znamenke
6. metoda parnosti
7. metoda nejednakosti.

Poseban oblik nelinearnih diofantskih jednadžbi je **Pellova jednadžba** koju ćemo obraditi u nastavku ovog diplomskog rada.

Poglavlje 2

Pellova jednadžba

2.1 Općenito o Pellovoj jednadžbi

Definicija 2.1.1. *Diofantska jednadžba oblika*

$$x^2 - dy^2 = 1 \tag{2.1}$$

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

Pretpostavimo da je d potpun kvadrat, odnosno $d = \delta^2$. Tada iz $(x - \delta y)(x + \delta y) = 1$ slijedi $x - \delta y = x + \delta y = \pm 1$. Dakle, kad je d potpun kvadrat jednadžba (2.1) ima samo trivijalna rješenja $x = \pm 1$, $y = 0$ pa taj slučaj isključujemo.

U nastavku ćemo dokazati da Pellova jednadžba uvijek ima rješenje, štoviše dokazat ćemo da ima beskonačno mnogo rješenja u skupu prirodnih brojeva.
No najprije, iskažimo Dirichletov teorem i njegovu posljedicu koji će nam pomoći u dokazu (njihovi dokazi se nalaze u [5]).

Teorem 2.1.2. *(Dirichletov teorem)*
Neka su α *i* Q *realni brojevi i* $Q > 1$*. Tada postoje cijeli brojevi* p *i* q *takvi da je* $1 \leq q < Q$ *i* $\| \alpha q \| = | \alpha q - p | \leq \frac{1}{\mathbb{Q}}$.

Napomena 2.1.3. $S \| \alpha \|$ *označavamo udaljenost od* α *do najbližeg cijelog broja.*

Korolar 2.1.4. *Ako je* α *iracionalan broj, onda postoji beskonačno mnogo parova* p*,* q *relativno prostih cijelih brojeva takvih da je* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Lema 2.1.5. *Neka je* d *prirodni broj koji nije potpun kvadrat. Tada postoji cijeli broj* k*,* $0 < |k| < 1 + 2\sqrt{d}$*, sa svojstvom da jednadžba*

$$x^2 - dy^2 = k \tag{2.2}$$

ima beskonačno mnogo rješenja u prirodnim brojevima.

Dokaz. Prema Dirichletovom teoremu 2.1.2, postoji beskonačno mnogo parova prirodnih brojeva (x, y) sa svojstvom

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

Za svaki takav par (x, y) vrijedi

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

pa je

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

Budući da parova (x, y) s navedenim svojstvom ima beskonačno mnogo, a cijelih brojeva koji su po modulu manji od $1 + 2\sqrt{d}$ samo konačno mnogo, to postoji neki cijeli broj k, takav da je $|k| < 1 + 2\sqrt{d}$, za koji jednadžba (2.2) ima beskonačno mnogo rješenja. Budući da d nije potpun kvadrat, vrijedi da je $k \neq 0$. □

Sada možemo dokazati da Pellova jednadžba uvijek ima rješenje u skupu prirodnih brojeva.

Teorem 2.1.6. *Pellova jednadžba $x^2 - dy^2 = 1$ ima barem jedno rješenje u prirodnim brojevima x i y.*

Dokaz. Beskonačno mnogo rješenja jednadžbe (2.2) iz Leme 2.1.5. možemo podijeliti u k^2 klasa, stavljajući rješenja (x_1, y_1) i (x_2, y_2) u istu klasu ako i samo ako je $x_1 \equiv x_2 \pmod{k}$ i $y_1 \equiv y_2 \pmod{k}$. Tada neka od tih klasa sadržava barem dva različita rješenja (x_1, y_1) i (x_2, y_2) (x_1, x_2 su različiti prirodni brojevi). Stavimo

$$x = \frac{x_1x_2 - dy_1y_2}{k}, \qquad y = \frac{x_1y_2 - x_2y_1}{k}$$

("podijelimo rješenja" $x_2 + y_2\sqrt{d}$ i $x_1 + y_1\sqrt{d}$ i racionaliziramo nazivnik).
Tvrdimo da je $x, y \in \mathbb{Z}$, $y \neq 0$ i $x^2 - dy^2 = 1$. Imamo: $x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv k \equiv 0 \pmod{k}$, $x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{k}$, pa su $x, y \in \mathbb{Z}$. Pretpostavimo da je $y = 0$, tj. $x_1y_2 = x_2y_1$. Tada je

$$k = x_2^2 - dy_2^2 = x_2^2 - d \cdot \frac{x_2^2y_1^2}{x_1^2} = \frac{x_2^2}{x_1^2}\left(x_1^2 - dy_1^2\right) = \frac{x_2^2}{x_1^2} \cdot k,$$

tj. $x_1^2 = x_2^2$, što je u suprotnosti s pretpostavkom da su x_1 i x_2 različiti prirodni brojevi. Slijedi:

$$\begin{aligned} x^2 - dy^2 &= \frac{1}{k^2}\left[(x_1x_2 - dy_1y_2)^2 - d\,(x_1y_2 - x_2y_1)^2\right] \\ &= \frac{1}{k^2}\left(x_1^2x_2^2 + d^2y_1^2y_2^2 - dx_1^2y_2^2 - dx_2^2y_1^2\right) \\ &= \frac{1}{k^2}\left(x_1^2 - dy_1^2\right)\left(x_2^2 - dy_2^2\right) \\ &= \frac{1}{k^2}\cdot k \cdot k = 1 \end{aligned}$$

□

Definicija 2.1.7. *Najmanje rješenje u prirodnim brojevima Pellove jednadžbe nazivamo* ***fundamentalno rješenje****. Označavamo ga s* (x_1, y_1) *ili s* $x_1 + y_1\sqrt{d}$*.*

Ako znamo fundamentalno rješenje Pellove jednadžbe, onda iz njega možemo dobiti beskonačno mnogo rješenja te iste jednadžbe. O tome nam govori sljedeći teorem:

Teorem 2.1.8. *Pellova jednadžba* $x^2 - dy^2 = 1$ *ima beskonačno mnogo rješenja. Ako je* (x_1, y_1) *fundamentalno rješenje, onda su sva rješenja u prirodnim brojevima ove jednadžbe dana formulom*

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, \quad n \in \mathbb{N}, \tag{2.3}$$

tj.

$$\begin{aligned} x_n &= x_1^n + \binom{n}{2}dx_1^{n-2}y_1^2 + \binom{n}{4}d^2x_1^{n-4}y_1^4 + \cdots, \\ y_n &= nx_1^{n-1}y_1 + \binom{n}{3}dx_1^{n-3}y_1^3 + \binom{n}{5}d^2x_1^{n-5}y_1^5 + \cdots. \end{aligned}$$

Dokaz. Iz jednadžbe (2.3) slijedi $x_n - y_n\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)^n$, pa množenjem dobivamo

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

što znači da su (x_n, y_n) zaista rješenja i ima ih beskonačno mnogo.
Pretpostavimo sada da je (s, t) rješenje koje nije oblika $(x_n, y_n), n \in \mathbb{N}$.
Budući da je $x_1 + y_1\sqrt{d} > 1$ i $s + t\sqrt{d} > 1$, postoji $m \in \mathbb{N}$ takav da je

$$\left(x_1 + y_1\sqrt{d}\right)^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1} \tag{2.4}$$

Pomnožimo li (2.4) s $(x_1 + y_1\sqrt{d})^{-m} = (x_1 - y_1\sqrt{d})^m$, dobivamo

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

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

Primjer 2.1.9. *Nađimo sva rješenja Pellove jednadžbe* $x^2 - 2y^2 = 1$.

Rješenje:
Fundamentalno rješenje Pellove jednadžbe $x^2 - 2y^2 = 1$ *je* $(x_1, y_1) = (3, 2)$*, odnosno* $3 + 2\sqrt{2}$*. Prema Teoremu 2.1.8. sva rješenja zadane jednadžbe dana su sa*

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

Teorem 2.1.10. *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 redoslijedu. Uzmimo da je* $(x_0, y_0) = (1, 0)$.
Tada vrijedi:

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

Dokaz. Prema Teoremu 2.1.8. znamo da vrijedi $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$, $n \in \mathbb{N}$. Odavde slijedi

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

Množenjem i izjednačavanjem slobodnih članova dobivamo

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

odakle zbrajanjem slijedi $x_{n+2} = 2x_1x_{n+1} - x_n$.
Analogno, množenjem i izjednačavanjem članova uz $\sqrt{d}$ dobivamo

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

pa ponovnim zbrajanjem slijedi $y_{n+2} = 2x_1y_{n+1} - y_n$. □

Primjer 2.1.11. *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 ćemo provesti matematičkom indukcijom po m.
Uvrstimo $m = 1$ u prve dvije jednakosti te 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 dokazu prethodnog Teorema 2.1.10., izjednačavanjem slobodnih članove te članova uz $\sqrt{d}$, slijedi da gornje jednakosti vrijede za svaki prirodni broj n.
Pretpostavimo da jednakosti vrijede 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 $m = k + 1$. Primjenom rezultata 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 smo dokazali prvu jednakost, $x_{n+m} = x_m x_n + d y_m y_n$.
Analogno se dokazuje istinitost druge jednakosti, odnosno $y_{n+k+1} = x_{k+1} y_n + y_{k+1} x_n$.
Posljednju jednakost dobivamo dijeljenjem prve jednakosti drugom, uz uvjet $m = n$:

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

Na sljedeće dvije stranice dane su tablice u kojima su prikazana fundamentalna rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ za prirodni broj $d \leq 128$.

d	**x**	**y**	d	**x**	**y**
1	-	-	33	23	4
2	3	2	34	35	6
3	2	1	35	6	1
4	-	-	36	-	-
5	9	4	37	73	12
6	5	2	38	37	6
7	8	3	39	25	4
8	3	1	40	19	3
9	-	-	41	2049	320
10	19	6	42	13	2
11	10	3	43	3482	531
12	7	2	44	199	30
13	649	180	45	161	24
14	15	4	46	24335	3588
15	4	1	47	48	7
16	-	-	48	7	1
17	33	8	49	-	-
18	17	4	50	99	14
19	170	39	51	50	7
20	9	2	52	649	90
21	55	12	53	66249	9100
22	197	42	54	485	66
23	24	5	55	89	12
24	5	1	56	15	2
25	-	-	57	151	20
26	51	10	58	19603	2574
27	26	5	59	530	69
28	127	24	60	31	4
29	9801	1820	61	1766319049	226153980
30	11	2	62	63	8
31	1520	273	63	8	1
32	17	3	64	-	-

Tablica 2.1: Tablica fundamentalnih rješenja Pellove jednadžbe $x^2 - dy^2 = 1$

d	**x**	**y**	**d**	**x**	**y**
65	129	16	97	62809633	6377352
66	65	8	98	99	10
67	48842	5967	99	10	1
68	33	4	100	-	-
69	7775	936	101	201	20
70	251	30	102	101	10
71	3480	413	103	227528	22419
72	17	2	104	51	5
73	2281249	267000	105	41	4
74	3699	430	106	32080051	3115890
75	26	3	107	962	93
76	57799	6630	108	1351	130
77	351	40	109	158070671986249	15140424455100
78	53	6	110	21	2
79	80	9	111	295	28
80	9	1	112	127	12
81	-	-	113	1204353	113296
82	163	18	114	1025	96
83	82	9	115	1126	105
84	55	6	116	9801	910
85	285769	30996	117	649	60
86	10405	1122	118	306917	28254
87	28	3	119	120	11
88	197	21	120	11	1
89	500001		121	-	-
90	19	2	122	243	22
91	1574	165	123	122	11
92	1151	120	124	4620799	414960
93	12151	1260	125	930249	83204
94	2143295	221064	126	449	40
95	39	4	127	4730624	419775
96	49	5	128	577	51

Tablica 2.2: Tablica fundamentalnih rješenja Pellove jednadžbe $x^2 - dy^2 = 1$

2.2 Pellova jednadžba i verižni razlomci

Do sada smo dokazali da Pellova jednadžba $x^2 - dy^2 = 1$ uvijek ima rješenje, a Teoremi 2.1.8. i 2.1.10. nam pokazuju kako možemo dobiti sva njezina rješenja ako znamo njezino fundamentalno rješenje. Sada se postavlja pitanje kako pronaći fundamentalno rješenje Pellove jednadžbe.
Jedna je od metoda da uvršavamo redom $y = 1, 2, 3, \ldots$ i provjeravamo je li $dy^2 + 1$ kvadrat. Kod ove metode problem se javlja već za relativno male d-ove jer fundamentalno rješenje može biti vrlo veliko. Na primjer, za $d = 73$ fundamentalno rješenje je $(2281249, 267000)$, odnosno $2281249 + 267000\sqrt{73}$. Zbog toga se javlja potreba za pronalaskom efikasnije metode pomoću koje ćemo doći do fundamentalnog rješenja.
Efikasnija metoda pronalaska fundamentalnog rješenja, ujedno i metoda kojom ćemo se baviti u ovom diplomskom radu, je razvoj broja $\sqrt{d}$ u jednostavni verižni razlomak.

Stoga ćemo najprije definirati i upoznati se s osnovnim pojmovima vezanima uz verižne razlomke.

Napomena 2.2.1. *Najveći cijeli broj koji nije veći od α označavamo sa $\lfloor \alpha \rfloor$ i nazivamo najveće cijelo od α.*

Neka je $\alpha \in \mathbb{R}$. Definiramo:

$$a_0 := \lfloor \alpha \rfloor \in \mathbb{Z}.$$

Ako je $\alpha \neq a_0$, onda je $\alpha - a_0 \in \langle 0, 1 \rangle$ pa postoji $\alpha_1 > 1$ takav da je

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Kako je $\alpha_1 > 1$, definiramo

$$a_1 := \lfloor \alpha_1 \rfloor \in \mathbb{N}.$$

Ako je $\alpha_1 \neq a_1$, onda postoji $\alpha_2 > 1$ takav da je

$$\alpha_1 = a_1 + \frac{1}{\alpha_2},$$

odnosno

$$\alpha = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}.$$

Opisani postupak provodimo sve dok je $a_k = \lfloor \alpha_k \rfloor \neq \alpha_k, k \geq 2$.
Ako je $a_n = \alpha_n$ za neki $n \in \mathbb{N}$, tada je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}} \tag{2.5}$$

Izraz oblika (2.5) je **razvoj broja α u jednostavni konačni verižni razlomak.**
Jednostavni konačni verižni razlomak kraće zapisujemo u obliku $\alpha = [a_0, a_1, a_2, \ldots, a_n]$.

Napomena 2.2.2. *α ima razvoj u jednostavni konačni verižni razlomak ako i samo ako je α racionalan broj.*

Ako je $a_n \neq \alpha_n$ za svaki $n \in \mathbb{N}$, tada je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} \tag{2.6}$$

Izraz oblika (2.6) je **razvoj broja α u jednostavni beskonačni verižni razlomak.**
Jednostavni beskonačni verižni razlomak kraće zapisujemo u obliku $\alpha = [a_0, a_1, a_2, \ldots]$.

Napomena 2.2.3. *α ima razvoj u jednostavni beskonačni verižni razlomak ako i samo ako je α iracionalan broj.*

Brojevi $a_0, a_1, a_2, \ldots$ nazivaju se **parcijalni kvocijenti** verižnog razlomka.

Ako je $\alpha = \frac{a}{b}$, brojevi $a_0, a_1, a_2, \ldots$ su kvocijenti iz Euklidovog algoritma primijenjenog na brojeve a i b.

Početci verižnih razlomaka tradicionalno se vežu za vrijeme nastanka Euklidovog algoritma upravo zbog činjenice što do razvoja racionalnog broja u verižni razlomak možemo doći algebarskim manipulacijama s jednakostima u Euklidovom algoritmu.

Euklidov algoritam je metoda pomoću koje određujemo najveći zajednički djelitelj dvaju danih brojeva. Sada ćemo se prisjetiti Euklidovog algoritma te na konkretnom primjeru pokazati njegovu vezu s verižnim razlomcima. No najprije ćemo iskazati Teorem o dijeljenju s ostatkom (njegov dokaz se nalazi u [5]) kojeg ćemo primijeniti u Euklidovom algoritmu.

Teorem 2.2.4. *(Teorem o dijeljenju s ostatkom)*
Neka su a, b cijeli brojevi, $a > 0$. Tada postoje jedinstveni cijeli brojevi q i r takvi da je $b = aq + r$, $0 \leq r < a$.

Euklidov algoritam
Neka su a, b cijeli brojevi, $a > 0$. Uzastopnom primjenom Teorema 2.2.4 dobivamo niz jednakosti:

$$\begin{aligned}
b &= aq_0 + r_1, & 0 < r_1 < a \\
a &= r_1q_1 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2q_2 + r_3, & 0 < r_3 < r_2 \\
&\vdots & \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_n &
\end{aligned}$$

Primjer 2.2.5. *Razvijmo $\frac{47}{10}$ u jednostavni verižni razlomak.*

Odredimo najveći zajednički djelitelj brojeva 47 *i* 10 *pomoću Euklidovog algoritma:*

$$\begin{aligned}
47 &= \boldsymbol{4} \cdot 10 + 7 \\
10 &= \boldsymbol{1} \cdot 7 + 3 \\
7 &= \boldsymbol{2} \cdot 3 + 1 \\
3 &= \boldsymbol{3} \cdot 1
\end{aligned}$$

Svaki redak algoritma možemo zapisati i na sljedeći način:

$$\begin{aligned}
\frac{47}{10} &= 4 + \frac{7}{10} \\
\frac{10}{7} &= 1 + \frac{3}{7} \\
\frac{7}{3} &= 2 + \frac{1}{3}
\end{aligned}$$

Prvi redak Euklidovog algoritma možemo također zapisati i ovako: $\frac{47}{10} = 4 + \frac{7}{10} = 4 + \frac{1}{\frac{10}{7}}$. Na isti način zapišemo i preostale retke Euklidovog algoritma. Dobiveni niz jednakosti

možemo zapisati na sljedeći način:

$$\begin{aligned}
\frac{47}{10} &= 4 + \frac{7}{10} \\
&= 4 + \cfrac{1}{\cfrac{10}{7}} \\
&= 4 + \cfrac{1}{1 + \cfrac{3}{7}} \\
&= 4 + \cfrac{1}{1 + \cfrac{1}{\cfrac{7}{3}}} \\
&= \boldsymbol{4} + \cfrac{1}{\boldsymbol{1} + \cfrac{1}{\boldsymbol{2} + \cfrac{1}{\boldsymbol{3}}}}
\end{aligned}$$

ili $[4, 1, 2, 3]$. *Time smo dobili razvoj razlomka* $\frac{47}{10}$ *u jednostavni verižni razlomak.*

Zapis svakog razlomka kojemu je brojnik manji od nazivnika je oblika $[0, a_0, a_1, \ldots, a_n]$.
Na primjer: $\dfrac{69}{25} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6}}}$, dok je $\dfrac{25}{69} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{6}}}}$.

Napomena 2.2.6. *Euklidov algoritam funkcionira samo za razvoj racionalnih brojeva u verižni razlomak, odnosno onda kada je* $a_n = \alpha_n$, *za neki* $n \in \mathbb{N}$.

Definicija 2.2.7. *Neka je* $\alpha = [a_0, a_1, a_2, \ldots, a_n]$. *Svaki racionalan broj* $c_k = \frac{p_k}{q_k} = [a_0, a_1, a_2, \ldots, a_k]$ *za* $k \leq n$ *zovemo* ***k-ta konvergenta*** *od* α.
Ako u beskonačnom verižnom razlomku $\alpha = [a_0, a_1, a_2, \ldots]$ *uzmemo samo konačno mnogo članova,* $[a_0, a_1, a_2, \ldots, a_k]$, *onda takav izraz zovemo* ***k-ta konvergenta beskonačnog verižnog razlomka*** α.

Primjer 2.2.8. *Razvijmo $\frac{67}{29}$ u jednostavni verižni razlomak i odredimo njegove konvergente.*
Rješenje:

$$\begin{aligned} 67 &= \boldsymbol{2} \cdot 29 + 9 \\ 29 &= \boldsymbol{3} \cdot 9 + 2 \\ 9 &= \boldsymbol{4} \cdot 2 + 1 \\ 2 &= \boldsymbol{2} \cdot 1 \end{aligned}$$

$$\frac{67}{29} = 2 + \cfrac{1}{3 + \cfrac{1}{4 + \cfrac{1}{2}}}, \qquad tj. \qquad \frac{67}{29} = [2, 3, 4, 2]$$

Njegove konvergente su:

$$\begin{aligned} c_0 &= \frac{p_0}{q_0} = [2] = 2 \\ c_1 &= \frac{p_1}{q_1} = [2, 3] = 2 + \frac{1}{3} = \frac{7}{3} \\ c_2 &= \frac{p_2}{q_2} = [2, 3, 4] = 2 + \frac{1}{3 + \frac{1}{4}} = \frac{30}{13} \\ c_3 &= \frac{p_3}{q_3} = [2, 3, 4, 2] = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}} = \frac{67}{29} \end{aligned}$$

Lema 2.2.9. *Brojevi p_n, 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. Tvrdnju leme dokazat ćemo matematičkom indukcijom.
Za $n = 1$ vrijedi: $c_1 = \frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1}$.
Pretpostavimo da tvrdnja vrijedi za $n = m$. Tada imamo

$$c_m = [a_0, a_1, \ldots, a_m] = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}.$$

Sada trebamo pokazati da tvrdnja vrijedi i za $n = m + 1$, tj. da vrijedi

$$c_{m+1} = [a_0, a_1, \ldots, a_{m+1}] = \frac{p_{m+1}}{q_{m+1}} = \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}}.$$

Uočimo da je

$$c_{m+1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{m-1} + \cfrac{1}{\left(a_m + \cfrac{1}{a_{m+1}}\right)}}}}},$$

odnosno $c_{m+1} = [a_0, a_1, \ldots, a_m, a_{m+1}] = \left[a_0, a_1, \ldots, a_{m-1}, \left(a_m + \frac{1}{a_{m+1}}\right)\right]$. Na ovaj način dobili smo zapis od c_{m+1} pomoću m članova verižnog razlomka pa ako iskoristimo pretpostavku indukcije slijedi

$$\begin{aligned}
c_{m+1} &= [a_0, a_1, \ldots, a_m, a_{m+1}] = \left[a_0, a_1, \ldots, a_{m-1}, \left(a_m + \frac{1}{a_{m+1}}\right)\right] \\
&= \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) q_{m-1} + q_{m-2}} \\
&= \frac{(a_m a_{m+1} + 1) p_{m-1} + a_{m+1} p_{m-2}}{(a_m a_{m+1} + 1) q_{m-1} + a_{m+1} q_{m-2}} \\
&= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} \\
&= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}} \\
c_{m+1} &= \frac{p_{m+1}}{q_{m+1}}
\end{aligned}$$

Time je tvrdnja leme dokazana. □

Napomena 2.2.10. *Dogovorno uzimamo da je* $p_{-2} = 0, p_{-1} = 1, q_{-2} = 1, q_{-1} = 0$.

Nakon Leme 2.2.9. i Napomene 2.2.10. izračun uzastopnih konvergenti možemo sistematizirati tablicom. Pokažimo to na konkretnom primjeru.

Primjer 2.2.11. *Prisjetimo se Primjera 2.1.8 u kojem smo konvergente razlomka* $\frac{67}{29}$ *računali preko definicije. To je bio dulji način izračuna. U ovom primjeru ćemo pokazati kraći i*

brži način.
Razvoj broja $\frac{67}{29}$ *u jednostavni verižni razlomak jednak je*

$$\frac{67}{29} = [2, 3, 4, 2] = [a_0, a_1, a_2, a_3].$$

Sada kreiramo tablicu:

k	***-2***	***-1***	***0***	***1***	***2***	***3***
a_n			*2*	*3*	*4*	*2*
p_n	*0*	*1*	*2*	*7*	*30*	*67*
q_n	*1*	*0*	*1*	*3*	*13*	*29*

Za svaki $n = 0, \ldots, k$, p_n *dobijemo tako da* a_n *množimo s* p_{n-1} *te zbrojimo s* p_{n-2}. *Analogno dobijemo i* q_n. *Iščitavanjem iz ove tablice lako dobijemo* $c_n = \frac{p_n}{q_n}$. *Na primjer,* $c_2 = \frac{p_2}{q_2} = \frac{30}{13}$.

Uočimo da je

$$\begin{aligned} q_{-1}p_{-2} - p_{-1}q_{-2} &= 0 \cdot 0 - 1 \cdot 1 = -1 \\ q_0 p_{-1} - p_0 q_{-1} &= 1 \cdot 1 - 2 \cdot 0 = 1 \\ q_1 p_0 - p_1 q_0 &= 3 \cdot 2 - 7 \cdot 1 = -1 \\ q_2 p_1 - p_2 q_1 &= 13 \cdot 7 - 30 \cdot 3 = 1 \\ &\vdots \end{aligned}$$

Ovime dolazimo do sljedeće leme:

Lema 2.2.12. *Neka su* p_n *i* q_n *definirani kao u Lemi 2.2.9. Tada vrijedi:*

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n, \quad n \geq -1.$$

Dokaz. Tvrdnju leme dokazat ćemo matematičkom indukcijom.
Za $n = -1$ imamo $q_{-1}p_{-2} - p_{-1}q_{-2} = 0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{-1}$.
Pretpostavimo da tvrdnja vrijedi za $n - 1$. Tada imamo

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

□

Iz prethodne leme direktno slijedi da su p_n i q_n relativno prosti.

Lema 2.2.13. *Neka su $a_0, a_1, a_2 \ldots$ cijeli brojevi te neka su $a_1, a_2, \ldots$ pozitivni brojevi. Tada vrijedi:*

1. $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots$
2. $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots$
3. *Ako je n paran, a m neparan, onda je $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.*

Dokaz ove leme nalazi se u [5].

U sljedećem teoremu vidjet ćemo da su konvergente jako dobre racionalne aproksimacije iracionalnog broja α.

Teorem 2.2.14. *Neka su $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_n}{q_n}$ dvije uzastopne konvergente od α. Tada barem jedna od njih zadovoljava nejednakost*

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

Dokaz. Brojevi $\alpha - \frac{p_n}{q_n}$, $\alpha - \frac{p_{n-1}}{q_{n-1}}$ imaju suprotni predznak, pa je

$$\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q^2{}_{n-1}}.$$

Ako bi vrijedilo da je $\left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2}$ i $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \geq \frac{1}{2q_{n-1}^2}$, onda bi dobili da je

$$\frac{1}{q_n q_{n-1}} \geq \frac{1}{2q_n^2} + \frac{1}{2q^2{}_{n-1}},$$

a to je ekvivalentno s nejednakošću $(q_n - q_{n-1})^2 \leq 0$ što nije moguće.
Dakle, $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}$ ili $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q^2{}_{n-1}}$

□

Neku vrstu obrata upravo dokazanog teorema je dao Legendre i ona će se pokazati kao jako važan rezultat za određivanje fundamentalnog rješenja Pellove jednažbe.

Teorem 2.2.15. *(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. Možemo pretpostaviti da je $\alpha \neq \frac{p}{q}$ jer je inače tvrdnja teorema trivijalno zadovoljena. 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 možemo uvijek postići jer vrijedi $[a_0, a_1, \ldots, a_m] = [a_0, a_1, \ldots, a_{m-1}, 1]$.
Definirajmo ω sa

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

tako da je $\alpha = [b_0, b_1, \ldots, b_{n-1}, \omega]$. Sada prema formuli

$$q_n\alpha - p_n = q_n \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - p_n = \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}}$$

slijedi

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

pa je $\vartheta = \frac{q_{n-1}}{\omega q_{n-1} + q_{n-2}}$. Rješavanjem ove relacije po ω 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:

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

Budući da je $\omega > 1$, svi $b_j (j = n, n-1, \ldots)$ su prirodni brojevi. Stoga je

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

razvoj u verižni razlomak od α i

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

što je konvergenta od α, a to je i trebalo dokazati.

□

Definicija 2.2.16. *Za beskonačni verižni razlomak $[a_0, a_1, a_2, \ldots]$ kažemo da je **periodski** ako postoje cijeli brojevi $k \geq 0$, $m \geq 1$ takvi da je $a_{m+n} = a_n$, za sve $n \geq k$. U tom slučaju verižni razlomak pišemo u obliku*

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

gdje "crta" iznad brojeva $a_k, a_{k+1}, \ldots, a_{k+m-1}$ znači da se taj blok brojeva ponavlja unedogled. Broj m nazivamo duljina perioda. Ako je $k = 0$, onda kažemo da je verižni razlomak čisto periodski.

Definicija 2.2.17. *Za iracionalni broj α kažemo da je **kvadratna iracionalnost** ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Teorem 2.2.18. *(Euler, Lagrange)*
Razvoj u jednostavni verižni razlomak realnog broja α je periodski ako i samo ako je α kvadratna iracionalnost.

Iz dokaza izrečenog teorema (dokaz se nalazi u [5]) slijedi algoritam za razvoj kvadratnih iracionalnosti u verižni razlomak:

Neka je α kvadratna iracionalost. 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 $t_0 \mid (d - s_0^2)$. Ako je $\alpha = \sqrt{d}$ onda je $s_0 = 0$, $t_0 = 1$. Sada brojeve a_i računamo na sljedeći način:

$$a_i = \left\lfloor \frac{s_i + a_0}{t_i} \right\rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s^2{}_{i+1}}{t_i}. \tag{2.7}$$

Uočimo da iako je α iracionalan broj, ovaj algoritam radi samo s cijelim brojevima.

Teorem 2.2.19. *Ako prirodni broj d nije potpun kvadrat, onda razvoj u jednostavni verižni razlomak od $\sqrt{d}$ ima oblik*

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

gdje je $a_0 = \left\lfloor \sqrt{d} \right\rfloor$ te su $a_1, \ldots, a_{r-1}$ centralno simetrični, tj. $a_1 = a_{r-1}$, $a_2 = a_{r-2}$, ... Nadalje, u (2.7) *uz $\alpha_0 = \sqrt{d}$, $t_0 = 1$, $s_0 = 0$, imamo $t_i \neq -1$ te $t_i = 1$ ako i samo ako $r \mid i$ (ovdje r označava duljinu najmanjeg perioda u razvoju od $\sqrt{d}$).*

Napomena 2.2.20. *Budući da ne znamo unaprijed duljinu perioda u razvoju broja $\sqrt{d}$, algoritam* (2.7) *provodimo sve dok se vrijednosti s_1 i t_1 ne ponove. Ako je duljina perioda jednaka r, onda ćemo dobiti da je $(s_1, t_1) = (s_{r+1}, t_{r+1})$ što će nam biti znak da prestajemo s postupkom.*

Primjer 2.2.21. *Razvijmo broj $\sqrt{19}$ u jednostavni verižni razlomak.*

Rješenje:
Da bismo razvili $\sqrt{19}$ u jednostavni verižni razlomak koristimo algoritam (2.7) *i Teorem 2.2.19.*

$\sqrt{19} \approx 4.358898944$

$s_0 = 0,\ t_0 = 1,\ a_0 = \lfloor \sqrt{19} \rfloor = 4$

$s_1 = a_0t_0 - s_0 = 4 \cdot 1 - 0 = \boldsymbol{4}\,, \qquad t_1 = \frac{d-s_1^2}{t_0} = \frac{19-4^2}{1} = \boldsymbol{3}, \qquad a_1 = \left\lfloor \frac{s_1+a_0}{t_1} \right\rfloor = \left\lfloor \frac{4+4}{3} \right\rfloor = \boldsymbol{2}$

$s_2 = a_1t_1 - s_1 = 2 \cdot 3 - 4 = \boldsymbol{2}\,, \qquad t_2 = \frac{d-s_2^2}{t_1} = \frac{19-2^2}{3} = \boldsymbol{5}, \qquad a_2 = \left\lfloor \frac{s_2+a_0}{t_2} \right\rfloor = \left\lfloor \frac{2+4}{5} \right\rfloor = \boldsymbol{1}$

$s_3 = a_2t_2 - s_2 = 1 \cdot 5 - 2 = \boldsymbol{3}\,, \qquad t_3 = \frac{d-s_3^2}{t_2} = \frac{19-3^2}{5} = \boldsymbol{2}, \qquad a_3 = \left\lfloor \frac{s_3+a_0}{t_3} \right\rfloor = \left\lfloor \frac{3+4}{2} \right\rfloor = \boldsymbol{3}$

$s_4 = a_3t_3 - s_3 = 3 \cdot 2 - 3 = \boldsymbol{3}\,, \qquad t_4 = \frac{d-s_4^2}{t_3} = \frac{19-3^2}{2} = \boldsymbol{5}, \qquad a_4 = \left\lfloor \frac{s_4+a_0}{t_4} \right\rfloor = \left\lfloor \frac{3+4}{5} \right\rfloor = \boldsymbol{1}$

$s_5 = a_4t_4 - s_4 = 1 \cdot 5 - 3 = \boldsymbol{2}\,, \qquad t_5 = \frac{d-s_5^2}{t_4} = \frac{19-2^2}{5} = \boldsymbol{3}, \qquad a_5 = \left\lfloor \frac{s_5+a_0}{t_5} \right\rfloor = \left\lfloor \frac{2+4}{3} \right\rfloor = \boldsymbol{2}$

$s_6 = a_5t_3 - s_5 = 2 \cdot 3 - 2 = \boldsymbol{4}\,, \qquad t_6 = \frac{d-s_6^2}{t_5} = \frac{19-4^2}{3} = \boldsymbol{1}, \qquad a_6 = \left\lfloor \frac{s_6+a_0}{t_6} \right\rfloor = \left\lfloor \frac{4+4}{1} \right\rfloor = \boldsymbol{8}$

$s_7 = a_6t_6 - s_6 = 8 \cdot 1 - 4 = \boldsymbol{4}\,, \qquad t_7 = \frac{d-s_7^2}{t_6} = \frac{19-4^2}{1} = \boldsymbol{3},$

Sada uočimo da smo dobili $(s_7, t_7) = (s_1, t_1)$ *pa zaustavljamo algoritam i zapisujemo*

$$\sqrt{19} = [4, \overline{2, 1, 3, 1, 2, 8}].$$

Teorem 2.2.22. *Neka su* $\frac{p_n}{q_n}$ *konvergente, a r duljina perioda u razvoju u verižni razlomak od* $\sqrt{d}$.
Ako je r paran, onda su sva rješenja jednadžbe $x^2 - dy^2 = 1$ *dana s* $(x, y) = (p_{nr-1}, q_{nr-1}), n \in \mathbb{N}$. *Posebno, fundamentalno rješenje je* (p_{r-1}, q_{r-1}).
Ako je r neparan, onda su sva rješenja jednadžbe $x^2 - dy^2 = 1$ *dana s* $(x, y) = (p_{2nr-1}, q_{2nr-1}), n \in \mathbb{N}$. *Posebno, fundamentalno rješenje je* (p_{2r-1}, q_{2r-1}).

Pogledajmo sada na primjerima kako rješavamo Pellovu jednadžbu oblika $x^2 - dy^2 = 1$.

Primjer 2.2.23. *Nađimo fundamentalno rješenje jednadžbe* $x^2 - 14y^2 = 1$.

Rješenje:
Prvi korak u rješavanju zadane jednadžbe je razvoj broja $\sqrt{14}$ *u verižni razlomak.*
Za razvoj broja $\sqrt{14}$ *u verižni razlomak koristimo algoritam* (2.7) *i Teorem 2.2.19.*

$\sqrt{14} = 3.741657387$

$s_0 = 0,\ t_0 = 1,\ a_0 = \lfloor \sqrt{14} \rfloor = 3$

$s_1 = a_0t_0 - s_0 = 3 \cdot 1 - 0 = \boldsymbol{3}\,, \qquad t_1 = \frac{d-s_1^2}{t_0} = \frac{14-3^2}{1} = \boldsymbol{5}, \qquad a_1 = \left\lfloor \frac{s_1+a_0}{t_1} \right\rfloor = \left\lfloor \frac{3+3}{5} \right\rfloor = \boldsymbol{1}$

$s_2 = a_1t_1 - s_1 = 1 \cdot 5 - 3 = \boldsymbol{2}\,, \qquad t_2 = \frac{d-s_2^2}{t_1} = \frac{14-2^2}{5} = \boldsymbol{2}, \qquad a_2 = \left\lfloor \frac{s_2+a_0}{t_2} \right\rfloor = \left\lfloor \frac{2+3}{2} \right\rfloor = \boldsymbol{2}$

$s_3 = a_2t_2 - s_2 = 2 \cdot 2 - 2 = \boldsymbol{2}\,, \qquad t_3 = \frac{d-s_3^2}{t_2} = \frac{14-2^2}{2} = \boldsymbol{5}, \qquad a_3 = \left\lfloor \frac{s_3+a_0}{t_3} \right\rfloor = \left\lfloor \frac{2+3}{5} \right\rfloor = \boldsymbol{1}$

$s_4 = a_3t_3 - s_3 = 1 \cdot 5 - 2 = \boldsymbol{3}\,, \qquad t_4 = \frac{d-s_4^2}{t_3} = \frac{14-3^2}{5} = \boldsymbol{1}, \qquad a_4 = \left\lfloor \frac{s_4+a_0}{t_4} \right\rfloor = \left\lfloor \frac{3+3}{1} \right\rfloor = \boldsymbol{6}$

$s_5 = a_4t_4 - s_4 = 6 \cdot 1 - 3 = \mathbf{3}\,, \qquad t_5 = \frac{d-s_5^2}{t_4} = \frac{14-3^2}{1} = \mathbf{5},$

Uočimo da je $(s_5, t_5) = (s_1, t_1)$ *pa zaustavljamo algoritam te zapisujemo*

$$\sqrt{14} = [3, \overline{1, 2, 1, 6}].$$

Period $r = 4$ *je paran pa je prema Teoremu 2.2.22. fundamentalno rješenje jednadžbe* $x^2 - 14y^2 = 1$ *dano s* $(x, y) = (p_3, q_3)$. *Konvergente* (p_3, q_3) *pronaći ćemo koristeći Lemu 2.2.9., a njih ćemo prikazati u tablici.*

k	***-2***	***-1***	***0***	***1***	***2***	***3***	***4***
a_n			*3*	*1*	*2*	*1*	*6*
p_n	*0*	*1*	*3*	*4*	*11*	*15*	*101*
q_n	*1*	*0*	*1*	*1*	*3*	*4*	*27*

Iz tablice vidimo da je $(p_3, q_3) = (15, 4)$.
Dakle, fundamentalno rješenje zadane jednadžbe $x^2 - 14y^2 = 1$ *jednako je* $(x, y) = (15, 4)$.

Primjer 2.2.24. *Nađimo sva rješenja jednadžbe* $x^2 - 41y^2 = 1$ *za koja vrijedi* $0 < x < 10000000$.

Rješenje:
Prvi korak u rješavanju zadane jednadžbe je razvoj broja $\sqrt{41}$ *u verižni razlomak.*
Za razvoj broja $\sqrt{41}$ *u verižni razlomak koristimo algoritam* (2.7) *i Teorem 2.2.19.*

$\sqrt{41} \approx 6.403124237$

$s_0 = 0,\ t_0 = 1,\ a_0 = \lfloor \sqrt{41} \rfloor = 6$

$s_1 = a_0t_0 - s_0 = 6 \cdot 1 - 0 = \mathbf{6}\,, \qquad t_1 = \frac{d-s_1^2}{t_0} = \frac{41-6^2}{1} = \mathbf{5}, \qquad a_1 = \left\lfloor \frac{s_1+a_0}{t_1} \right\rfloor = \left\lfloor \frac{6+6}{5} \right\rfloor = \mathbf{2}$

$s_2 = a_1t_1 - s_1 = 2 \cdot 5 - 6 = \mathbf{4}\,, \qquad t_2 = \frac{d-s_2^2}{t_1} = \frac{41-4^2}{5} = \mathbf{5}, \qquad a_2 = \left\lfloor \frac{s_2+a_0}{t_2} \right\rfloor = \left\lfloor \frac{4+6}{5} \right\rfloor = \mathbf{2}$

$s_3 = a_2t_2 - s_2 = 2 \cdot 5 - 6 = \mathbf{6}\,, \qquad t_3 = \frac{d-s_3^2}{t_2} = \frac{41-6^2}{5} = \mathbf{1}, \qquad a_3 = \left\lfloor \frac{s_3+a_0}{t_3} \right\rfloor = \left\lfloor \frac{6+6}{1} \right\rfloor = \mathbf{12}$

$s_4 = a_3t_3 - s_3 = 12 \cdot 1 - 6 = \mathbf{6}\,, \qquad t_4 = \frac{d-s_4^2}{t_3} = \frac{41-6^2}{1} = \mathbf{5}$

Sada uočimo da smo dobili $(s_4, t_4) = (s_1, t_1)$ *pa zaustavljamo algoritam i zapisujemo*

$$\sqrt{41} = [6, \overline{2, 2, 12}].$$

Period $r = 3$ *je neparan pa je prema Teoremu 2.2.22. fundamentalno rješenje jednadžbe* $x^2 - 41y^2 = 1$ *dano s* $(x, y) = (p_5, q_5)$. *Konvergente* (p_5, q_5) *pronaći ćemo koristeći Lemu 2.2.9. te ćemo ih prikazati u tablici.*

k	***-2***	***-1***	***0***	***1***	***2***	***3***	***4***	***5***
a_n			*6*	*2*	*2*	*12*	*2*	*2*
p_n	*0*	*1*	*6*	*13*	*32*	*397*	*826*	*2049*
q_n	*1*	*0*	*1*	*2*	*5*	*62*	*129*	*320*

Iz tablice vidimo da je $(p_5, q_5) = (2049, 320)$.
Dakle, fundamentalno rješenje zadane jednadžbe $x^2 - 41y^2 = 1$ *jednako je* $(x, y) = (2049, 320)$.
Ostala rješenje $0 < x < 10000000$ *naći ćemo pomoću Teorema 2.1.10. Slijedi:*

$$x_2 = 2 \cdot 2049 \cdot 2049 - 1 = 8396801, \quad y_2 = 2 \cdot 2049 \cdot 320 - 0 = 1311360$$

$$x_3 = 2 \cdot 2049 \cdot 8396801 - 2049$$

Iz x_3 *zaključujemo da je* $x_n > 10000000$ *za* $n \geq 3$.
Konačno, sva rješenja jednadžbe $x^2 - 41y^2 = 1$ *za koja vrijedi* $0 < x < 10000000$ *su*

$$\begin{aligned} (x_1, y_1) &= (2049, 320) \\ (x_2, y_2) &= (8396801, 1311360). \end{aligned}$$

Poglavlje 3

Povijesni razvoj Pellove jednadžbe

3.1 Grčki matematičari i Pellova jednadžba

Prvo spominjanje Pellove jednadžbe pojavljuje se u radovima Teona iz Smirne[1]. Ako stavimo $s_1 = 1$ i $d_1 = 1$ i izračunamo

$$s_{n+1} = s_n + d_n, \quad d_{n+1} = 2s_n + d_n \quad (n = 1, 2, 3, \dots),$$

tada dobivamo

$$d_n^2 - 2s_n^2 = (-1)^n. \tag{3.1}$$

Teon nije koristio današnju navedenu notaciju niti je dokazao jednadžbu (3.1), jedino ju je provjerio za prvih nekoliko n-ova.
Na Teonova zapažanja nadovezao se Proklo[2]. Identitet koji je promatrao, u današnjoj notaciji izražen je kao

$$(2x + y)^2 + y^2 = 2x^2 + 2(x + y)^2. \tag{3.2}$$

Ako ovaj identitet zapišemo u obliku

$$(2x + y)^2 - 2(x + y)^2 = -(y^2 - 2x)$$

dobit ćemo dokaz Teonove jednadžbe (3.1), iako Proklo to nije izrekao. Većina povjesničara slaže se da su i Teon i Proklo koristili ranije pitagorejske izvore za svoje rezultate. Također, smatra se da su Pitagorejci koristili vrijednost $\frac{d_n}{s_n}$ kako bi došli do što bolje aproksimacije $\sqrt{2}$. Kako su grčki matematičari bili zainteresirani za problem iracionalnosti, moguće je da su iskoristili vrijednosti $\frac{d_n}{s_n}$, koja se približava, ali ne dostiže vrijednost $\sqrt{2}$, kao dokaz (ali netočan dokaz) iracionalnosti $\sqrt{2}$.

[1] Teon iz Smirne (70.-135.), grčki matematičar, filozof i astronom
[2] Proklo (412.-485.), grčki filozof

Zapravo, moguće je upotrijebiti (3.1) kako bismo došli do točnog dokaza iracionalnosti $\sqrt{2}$, ali nije vjerojatno da su ga Pitagorejci otkrili.
Pretpostavimo da je $\sqrt{2}$ racionalan broj. Tada je $\sqrt{2} = \frac{a}{b}$, gdje su $a, b \in \mathbb{N}$. Sada (3.1) možemo zapisati kao

$$bd_n + as_n = \frac{b^2}{|bd_n - as_n|}.$$

Kako je $bd_n - as_n \neq 0$ slijedi $|bd_n - as_n| \geq 1$

$$0 < bd_n + as_n < b^2. \tag{3.3}$$

Primijetimo, kako d_n i s_n teže u beskonačnost (3.3) nemoguće je za sve $n \in \mathbb{N}$. No, unatoč tome čini se da su Grci znali riješiti Pellovu jednadžbu za $d = 2$.
Nadalje, Pellovu jednadžbu spominje i Diofant u svojem djelu *Aritmetika*. U njoj je dao rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ za $d = 26$ i $d = 30$.
Za razliku od danas, kada tražimo samo cjelobrojna rješenja Pellove jednadžbe, stari su Grci svojim metodama, generalno gledano, dobivali samo racionalna rješenja.
Sljedeći grčki matematičar koji se bavio rješavanjem Pellove jednadžbe bio je Arhimed[3]. Već su i stari Grci znali da što je d veći, to je teže riješiti Pellovu jednadžbu. To može objasniti Arhimedovo razmišljanje kod postavljanja problema sa stokom.

Arhimedov problem stoke

Proučavajući i prevodeći brojne rukopise i djela pisana na grčkom i latinskom jeziku, u poznatoj Herzogovoj biblioteci u Wolfenbüttelu, 1773. godine Gotthold Ephraim[4] naišao je na problem stoke. Danas je taj problem poznat kao Arhimedov problem stoke, 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.

[3] Arhimed iz Sirakuze (287.-212.pr.Kr.), grčki matematičar, fizičar i astronom
[4] Gotthold Ephraim (1729.-1781.), njemački pisac i knjižničar

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.

Napisan je u formi epigrama u 44 retka. Epigram je kratka pjesnička forma, obično pisana u elegijskom distihu. Izrazito je prisutna u starogrčkoj književnosti, a rabljena je i kao javna ili prigodna poruka (čestitka, poslanica, iskaz sućuti, molba) te kao rugalica nekim osobama ili zbivanjima u piščevoj okolini.
Arhimedov epigram nastao je kao svojevrstan odgovor na Apolonijeva[5] zanovijetanja. Apolonije je Arhimedu predbaciovao da je sklon matematičkim problemima čije rješavanje zahtijeva naporna i dugotrajna računanja. Arhimed je zatim osmislio numerički uistinu zahtjevan problem te ga uputio Eratostenu[6].
Opće rješenje problema dao je 1880. godine njemački matematičar A. Amthor[7] koji je pokazao da je rezultat približno jednak $7.76 \cdot 10^{206544}$, što je broj s 206545 znamenki, čije su prve četiri znamenke jednake 7760.
The Hillsboro Mathematical Club, neformalna skupina koju su činili matematičari E. Fish, G. H. Richards i A. H. Bell, od 1889. do 1893. godine izračunala je prvih 31 i posljednjih 12 znamenki najmanjeg rješenja problema. Rezultat je objavljen u časopisu *American Mathematical Montly*:

$$7760271406486818269530232833209 \ldots\ldots 719455081800$$

Iz teksta objavljenog 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." vidljiva je složenost problema i njegovog računanja prije pojave računala. No, ipak svijet je dočekao rješenje 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. Stroju je za izračun trebalo 7 sati i 49 minuta.
Provjeru tog rezultata proveo je 16 godina kasnije Harry L. Nelson na računalu Cray-1, a broj s 206545 znamenki ispisan je na 47 listova papira. Računanje, zajedno s provjerom točnosti, trajalo je desetak minuta.

[5] Apolonije iz Perge (260.-190.pr.Kr.), grčki matematičar
[6] Eratosten iz Kirene (275.-195.pr.Kr.), grčki matematičar
[7] Carl Ernst August Amthor (1845.–1916.), njemački matematičar

Riješimo sada zadani Arhimedov problem stoke.

Zamislimo stado koje se sastoji od krava i bikova bijele, crne ili žute boje te onih koji su šareni. Brojevi pojedine podskupine međusobno su povezani uvjetima. Uvodimo 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 navedene oznake, uvjete iz problema zapisujemo u 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. $z = \left(\frac{1}{6} + \frac{1}{7}\right) \cdot (B + b)$.

   Postavljena su još dva uvjeta:

8. B+C je potpuni kvadrat
9. Z+S je broj oblika $\frac{n(n+1)}{2}$

Prvih sedam jednadžbi čine homogeni linearni sustav s osam nepoznanica. Nije velik problem riješiti takav linearni sustav nekim od računalnih programa, ali pogledajmo kako bismo ga riješili "pješice".
Pomnožimo li redom, prvu jednadžbu s 336, drugu s 280 i treću s 126 dobit ćemo:

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

Zbrojimo sada ove tri jednadžbe i dobivamo

$$297\,B = 742\,Z$$

odnosno

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

Iz druge i treće jednadžbe nalazimo

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

odnosno

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

Analognim postupkom primjenjenim na sljedeće četiri jednadžbe sustava, gdje prvu množimo s 4800, drugu s 2800, treću s 1260 i četvrtu s 462, dobit ćemo:

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

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 zapisati:

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

Ovim postupcima došli smo do općeg rješenja sustava sedam linearnih jednadžbi uz uvjet da su ta rješenja prirodni brojevi:

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

pri čemu je k prirodni broj. Ukupno je to $50389082 \cdot k$ komada stoke.
Prvi od dodatnih uvijeta kaže da je $B + C$ potpuni kvadrat, odnosno da je $B + C = m^2$, gdje je m prirodan broj. Iz toga slijedi:

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

Očito je $k = 3 \cdot 11 \cdot 29 \cdot 4657 \cdot t^2$, $t \in \mathbb{Z}$.
Sada imamo rješenje sustava što ga čini sedam jednadžbi uz dodatni uvjet da je $B + C$ potpuni kvadrat:

$$\begin{aligned}
B &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 29 \cdot 53 \cdot 4657^2 \cdot t^2 = 46200808287018 \cdot t^2 \\
C &= 2 \cdot 3^3 \cdot 11 \cdot 29 \cdot 89 \cdot 4657^2 \cdot t^2 = 33240638308986 \cdot t^2 \\
Z &= 3^5 \cdot 11^2 \cdot 29 \cdot 4657^{22} = 18492776362863 \cdot t^2 \\
S &= 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 29 \cdot 79 \cdot 4657^2 \cdot t^2 = 32793026546940 \cdot t^2 \\
b &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 \cdot 29 \cdot 373 \cdot 4657 \cdot t^2 = 32116937723640 \cdot t^2 \\
c &= 2 \cdot 3^3 \cdot 11 \cdot 17 \cdot 29 \cdot 4657 \cdot 15991 \cdot t^2 = 21807969217254 \cdot t^2 \\
z &= 3^3 \cdot 11 \cdot 13 \cdot 29 \cdot 4657 \cdot 46489 \cdot t^2 = 24241207098537 \cdot t^2 \\
s &= 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11^2 \cdot 29 \cdot 761 \cdot 4657 \cdot t^2 = 15669127269180 \cdot t^2.
\end{aligned}$$

Drugi, i posljednji, od dodatnih uvjeta kaže da je $Z + S$ broj oblika $\frac{n(n+1)}{2}$, tj. trokutni broj. Primjetimo da je $Z + S = \frac{n(n+1)}{2}$ ekvivalentno s $8(Z + S) + 1 = (2n + 1)^2$. Kako je $Z + S = 4149387 \cdot k + 7358060 \cdot k = 11507447 \cdot k$ slijedi

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

Uvrstimo li sada nađenu vrijednost za k dobivamo jednadžbu

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

Zapišimo ovu jednadžbu u obliku

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

i nađimo joj cjelobrojna rješenja. Uvrstimo sada $2n+1 = x$ i $2 \cdot 4657 \cdot t = y$, dobivamo jednadžbu oblika $x^2 - 4729494y^2 = 1$ koja je zapravo Pellova jednadžba. Najmanja rješenja dane Pellove jednadžbe su:

$$\begin{aligned} x &= 109931986732829734979866232821433543901088049 \\ y &= 50549485234315033074477819735540408863 40 \end{aligned}$$

Zbog velikog fundamentalnog rješenja dane Pellove jednadžbe nećemo se upuštati u njezino rješavanje.
Ilan Vardi[8] kaže: "Teško je povjerovati da je Arhimed mogao riješiti problem.". Upravo zbog težine računanja i velikih rješenja teško je povjerovati da je Arhimed mogao riješiti problem, a nije niti izgledno da bi znao postoji li njegovo rješenje.
Arhimedov problem stoke možemo zaključiti 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.".

3.2 Indijski matematičari i Pellova jednadžba

Indijski matematičari znali su rješavati linearne diofantske jednadžbe. Aryabhata I.[9] razvio je metodu rješavanja linearne diofantske jednadžbe

$$ax - by = c$$

gdje su a, b, c dani prirodni brojevi, a x, y traženi cijeli brojevi.

Na razvoj Pellove jednadžbe poseban utjecaj imali su indijski matematičari Brahmagupta[10] i Bhaskara II.[11]
Krenut ćemo s pregledom Brahmaguptinog doprinosa razvoju Pellove jednadžbe.

[8] Ilan Vardi (1957.-), američki matematičar
[9] Aryabhata I. (476.-550.), indijski matematičar i astronom
[10] Brahmagupta (598.-670), indijski matematičar i astronom
[11] Bhaskara II. (1114.-1185.), indijski matematičar

628.godine Brahmagupta dolazi do važne metode kojom se iz jednog poznatog rješenja dane Pellove jednadžbe mogu dobiti i njezina ostala rješenja. Indijski matematičari su Brahmaguptinu metodu nazivali *samasa*, a mi je danas nazivamo *metoda kompozicije*.
Kako djeluje Brahmaguptina metoda?
Neka su dane dvije jednadžbe $a^2 - db^2 = q$ i $p^2 - dr^2 = s$. Njihovim množenjem slijedi

$$(a^2 - db^2) \cdot (p^2 - dr^2) = qs$$

$$a^2p^2 - da^2r^2 - db^2p^2 + d^2b^2r^2 = qs$$
$$a^2p^2 + d^2b^2r^2 - d(a^2r^2 + b^2p^2) = qs$$
$$(ap + dbr)^2 - d(ar + bp)^2 = qs$$

Uzmimo da vrijedi: $q = s = 1$, $a = p$ te $b = r$. Tada dobivamo jednadžbu $(a^2 + db^2)^2 - d(2ab)^2 = 1$. Ako je (a, b) rješenje jednadžbe $a^2 - db^2 = 1$ onda je i $(a^2 + db^2, 2ab)$ njezino rješenje jer smo primijenili metodu kompozicije na (a, b) i (a, b). Nadalje, ako primijenimo metodu kompozicije na (a, b) i $(a^2 + db^2, 2ab)$ također ćemo dobiti cjelobrojno rješenje Pellove jednadžbe $a^2 - db^2 = 1$.
Brahmagupta nije koristio metodu kompozicije samo za Pellovu jednadžbu $x^2 - dy^2 = 1$, već i za Pellove jednadžbe $x^2 - dy^2 = k$, $k = \pm 1, \pm 2, \pm 4$.
Koristeći prethodno napisana svojstva, ako je (a, b) rješenje jednadžbe $x^2 - dy^2 = k$, primjenom metode kompozicije na (a, b) i (a, b) dobivamo $(a^2 + db^2, 2ab)$ kao rješenje jednadžbe $x^2 - dy^2 = k^2$. Podijelimo li dobivenu jednadžbu $(a^2 + db^2)^2 - d(2ab)^2 = k^2$ s k^2 dobivamo jednadžbu

$$\left(\frac{a^2 + db^2}{k}\right)^2 - d\left(\frac{2ab}{k}\right) = 1.$$

gdje su

$$x = \frac{a^2 + db^2}{k}, \quad y = \frac{2ab}{k} \tag{3.4}$$

njezina rješenja.
Na primjer, promatrajmo jednadžbu $x^2 - dy^2 = k$ za $k = 2$. Ako je (a, b) njezino rješenje, onda iz $a^2 - db^2 = 2$ slijedi $db^2 = a^2 - 2$. Iz (3.4) slijedi

$$x = \frac{a^2 + db^2}{2} = \frac{a^2 + a^2 - 2}{2} = \frac{2a^2 - 2}{2} = a^2 - 1$$

$$y = \frac{2ab}{2} = ab. \tag{3.5}$$

Analogno se rješava slučaj kada je $k = -2$, a ako je $k = \pm 4$ na malo kompliciraniji način se metodom kompozicije također može doći do rješenja.

Kasnije ćemo ovaj Brahmaguptin rezultat koristiti i kod Bhaskare II.

Sada ćemo iskazati i dokazati metodu kompozicije te ju primijeniti na konkretnom primjeru.

Teorem 3.2.1. *(Brahmaguptino kompoziciono pravilo)*
Ako su (x_1, y_1) *i* (x_2, y_2) *rješenja Pellove jednadžbe* $x^2 - dy^2 = 1$*, tada je i* $(x_3, y_3) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)$ *također rješenje.*

Dokaz. Primijetimo da vrijedi $(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 + dy_1y_2 + \sqrt{d}(x_1y_2 + x_2y_1)$. Kako su (x_1, y_1) i (x_2, y_2) rješenja Pellove jednadžbe $x^2 - dy^2 = 1$, očito je $1 = (x_1^2 + y_1^2d)(x_2^2 + y_2^2d)$. Redom dobivamo

$$\begin{aligned} 1 &= (x_1 - y_1\sqrt{d})(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})(x_2 + y_2\sqrt{d}) \\ &= (x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d})(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) \\ &= (x_1x_2 + dy_1y_2 - \sqrt{d}(x_1y_2 + x_2y_1))(x_1x_2 + dy_1y_2 + \sqrt{d}(x_1y_2 + x_2y_1)) \\ &= (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2 \\ &= x_3^2 - dy_3^2 \end{aligned}$$

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

Primjer 3.2.2. *Primjenom Brahmaguptinog kompozicionog pravila iz fundamentalnog rješenja* $(x, y) = (2, 1)$ *pronađimo još nekoliko rješenja Pellove jednadžbe* $x^2 - 3y^2 = 1$.

Rješenje:
Prvo primijenimo kompoziciono pravilo na $(x_1, y_1) = (2, 1)$ *i* $(x_1, y_1) = (2, 1)$ *:*

$$(x_2, y_2) = (x_1^2 + dy_1^2, 2x_1y_1) = (4 + 3, 4) = (7, 4).$$

Sada primijenimo kompoziciono pravilo na $(x_1, y_1) = (2, 1)$ *i* $(x_2, y_2) = (7, 4)$*:*

$$(x_3, y_3) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1) = (14 + 12, 8 + 7) = (26, 15).$$

Kako bismo dobili sljedeće rješenje primijenimo kompoziciono pravilo na $(x_1, y_1) = (2, 1)$ *i* $(x_3, y_3) = (26, 15)$*:*

$$(x_4, y_4) = (x_1x_3 + dy_1y_3, x_1y_3 + x_3y_1) = (52 + 45, 30 + 26) = (97, 56).$$

Dakle, primjenom kompozicionog pravila iz fundamentalnog rješenja $(x, y) = (2, 1)$ *Pellove jednadžbe* $x^2 - 3y^2 = 1$ *dobili smo njezina sljedeća rješenja* $(7, 4)$*,* $(26, 15)$*,* $(97, 56)$*.*

Sljedeće važno otkriće u rješavanju Pellove jednadžbe bio je razvoj cikličke metode. Cikličku metodu, koju su indijski matematičari nazivali *chakravala*, opisao je 1150.godine Bhaskara II. Ova je metoda algoritam za rješavanje jednadžbe $x^2 - dy^2 = k$, gdje su $x, y \in \mathbb{Z}$ i $k = \pm 1, \pm 2, \pm 4$. Bhaskara II. nije dokazao da njegova ciklička metoda uvijek radi, prvi je to pokazao Lagrange 1768. godine.
Opisat ćemo cikličku metodu i prikazati je na konkretnom primjeru.

Kako bismo dobili rješenje jednadžbe $x^2 - dy^2 = 1$ krećemo od jednadžbe $a^2 - db^2 = k$, $a, b, k \in \mathbb{Z}$, gdje su (a, b) njezina rješenja. Pretpostavimo da je najveći zajednički djelitelj brojeva a i b jednak 1, odnosno da su a i b relativno prosti brojevi. Tada su i b i k također relativno prosti brojevi. Sada biramo $m > 0$ tako da za svaki m, $(m, 1)$ zadovoljava jednadžbu $m^2 - d \cdot 1^2 = (m^2 - d)$. Sada Bhaskara II. primjenjuje Brahmaguptinu metodu kompozicije na (a, b) i $(m, 1)$ te dobiva jednadžbu

$$(am + db)^2 - d(bm + a)^2 = (m^2 - d)k.$$

Dijeljenjem dobivene jednadžbe s k^2 dobivamo

$$\left(\frac{am + db}{k}\right)^2 - d\left(\frac{bm + a}{k}\right)^2 = \frac{m^2 - d}{k}.$$

Budući da je izraz unutar kvadrata uvijek pozitivan, moguća je sljedeća supstitucija:

$$\frac{am + db}{|k|} \to a, \quad \frac{bm + a}{|k|} \to b, \quad \frac{m^2 - d}{k} \to k. \tag{3.6}$$

Broj $m > 0$ odabrat ćemo tako da zadovoljava sljedeća dva uvjeta:

1. $k \mid bm + a$
2. $|m^2 - d|$ ima minimalnu vrijednost.

Iz prvog uvjeta slijedi: $k \mid am + db$ i $k \mid m^2 - d$. Takvim izborom broja m Pellova jednadžba ima cjelobrojna rješenja.
Ako je $\frac{m^2-d}{k}$ jedna od vrijednosti $1, -1, 2, -2, 4, -4$ tada možemo koristiti Brahmaguptinu metodu kompozicije kako bismo pronašli rješenje jednadžbe $x^2 - dy^2 = 1$.

Pogledajmo sada primjenu cikličke metode na konkretnom primjeru.

Primjer 3.2.3. *Riješimo jednadžbu* $x^2 - 67y^2 = 1$.

Rješenje:

Prvi korak u rješavanju zadane jednadžbe je pronalazak bilo kojeg para brojeva (a, b) *za koje vrijedi* $a^2 - 67b^2 = k$*, za bilo koji* $k \in \mathbb{Z}$ *do kojeg dođemo odabirom brojeva a i b. Ako uzmemo* $(a, b) = (8, 1)$ *dobijemo jednadžbu* $8^2 - 67 \cdot 1^2 = -3$*. Primijetimo da su odabrani a i b, odnosno* 8 *i* 1 *relativno prosti brojevi kao i brojevi* 1 *i* -3*.*
Drugi korak je primjena metode kompozicije na $(8, 1)$ *i* $(m, 1)$ *iz koje slijedi jednadžba* $(8m + 67)^2 - 67(m + 8)^2 = (m^2 - 67) \cdot -3$*. Dijeljenjem s* $(-3)^2$ *dobivamo jednadžbu*

$$\left(\frac{8m + 67}{-3}\right)^2 - 67\left(\frac{m + 8}{-3}\right)^2 = \frac{m^2 - 67}{-3}$$

iz koje prema (3.6) *slijedi:*

$$\frac{8m + 67}{3} \to a, \quad \frac{m + 8}{3} \to b, \quad \frac{m^2 - 67}{-3} \to k. \tag{3.7}$$

U sljedećem koraku biramo m. Uvjeti koje m mora zadovoljiti su:

1. $3 \mid m + 8$
2. $|m^2 - 67|$ *ima minimalnu vrijednost.*

Iz prvog uvjeta slijedi da je m oblika $3t + 1$*,* $t \in \mathbb{Z}$*, odnosno* $m \in \{1, 4, 7, 10, \dots\}$*, a među takvim m minimalna vrijednost iz drugog uvjeta postiže se za* $m = 7$*. Dobiveni m uvrstimo u* (3.7) *odakle dobijemo* $a_1 = 41$*,* $b_1 = 5$*,* $k_1 = 6$*.*
Sada smo dobili novu jednažbu $a_1^2 - 67b_1^2 = k_1$*, odnosno* $41^2 - 67 \cdot 5^2 = 6$*.*
Vidimo da je novi $k = 6$*, a mi tražimo* $k = 1$ *pa nastavljamo postupak.*

Sada krećemo od jednadžbe $41^2 - 67 \cdot 5^2 = 6$*.*
Primijetimo, sada su naši početni a i b jednaki 41 *i* 5*, a* $k = 6$ *te su* 41 *i* 5 *relativno prosti brojevi kao i* 5 *i* 6*.*
Primjenom metode kompozicije na $(41, 5)$ *i* $(m, 1)$ *dobivamo jedandžbu* $(41m + 335)^2 - 67(5m + 41)^2 = (m^2 - 67) \cdot 6$*. Dobivenu jednadžbu dijelimo s* 6^2*,*

$$\left(\frac{41m + 335}{6}\right)^2 - 67\left(\frac{5m + 67}{6}\right)^2 = \frac{m^2 - 67}{6},$$

iz koje zatim prema (3.6) *slijedi:*

$$\frac{41m + 335}{6} \to a, \quad \frac{5m + 41}{6} \to b, \quad \frac{m^2 - 67}{6} \to k. \tag{3.8}$$

Tražimo $m > 0$ *tako da:*

1. $6 \mid 5m + 41$
2. $|m^2 - 67|$ *ima minimalnu vrijednost.*

Iz prvog uvjeta slijedi da je m *oblika* $6t + 5$, $t \in \mathbb{Z}$, *odnosno* $m \in \{5, 11, 17, \dots\}$, *a među takvim* m *minimalna vrijednost iz drugog uvjeta postiže se za* $m = 5$. *Dobiveni* m *uvrstimo u* (3.8) *odakle dobijemo* $a_2 = 90$, $b_2 = 11$, $k_2 = -7$.
Dobili smo novu jednažbu $a_2^2 - 67b_2^2 = k_2$, *odnosno* $90^2 - 67 \cdot 11^2 = -7$. *Vidimo da je novi* $k = -7$, *a mi tražimo* $k = 1$ *pa nastavljamo postupak.*

Krećemo od jednadžbe $90^2 - 67 \cdot 11^2 = -7$. *Primijetimo, sada su naši početni* a *i* b *jednaki* 90 *i* 11, $k = -7$, 90 *i* 11 *su relativno prosti brojevi kao i* 11 *i* -7.
Primjenom metode kompozicije na $(90, 11)$ *i* $(m, 1)$ *dobivamo jedandžbu* $(90m + 737)^2 - 67(11m + 90)^2 = (m^2 - 67) \cdot -7$. *Dobivenu jednadžbu dijelimo s* $k = -7$,

$$\left(\frac{90m + 737}{-7}\right)^2 - 67\left(\frac{11m + 90}{-7}\right)^2 = \frac{m^2 - 67}{-7},$$

iz koje zatim prema (3.6) *slijedi:*

$$\frac{90m + 737}{7} \to a, \quad \frac{11m + 90}{7} \to b, \quad \frac{m^2 - 67}{-7} \to k. \tag{3.9}$$

Tražimo $m > 0$ *tako da:*

1. $7 \mid 11m + 90$
2. $|m^2 - 67|$ *ima minimalnu vrijednost.*

Iz prvog uvjeta slijedi da je m *oblika* $7t + 2$, $t \in \mathbb{Z}$, *odnosno* $m \in \{2, 9, 16, \dots\}$, *a među takvim* m *minimalna vrijednost iz drugog uvjeta postiže se za* $m = 9$. *Dobiveni* m *uvrstimo u* (3.9) *odakle dobijemo* $a_3 = 221$, $b_3 = 27$, $k_3 = -2$.
Sada smo dobili novu jednažbu $a_3^2 - 67b_3^2 = k_3$, *odnosno* $221^2 - 67 \cdot 27^2 = -2$.
Kako je novi $k = -2$, *a mi tražimo* $k = 1$ *možemo nastaviti dosadašnji postupak. Ako nastavimo postupak, do rješenja ćemo doći nakon što ga ponovimo još četiri puta.*
No primijetimo, kako je dobiveni $k = -2$ *možemo nastaviti i sa Brahmaguptinim kompozicionim pravilom.*
Primijenimo metodu kompozicije na $(221, 27)$ *i* $(221, 27)$ *odakle analogno postupku iz* (3.5) *slijedi*

$$(x, y) = \left(\frac{221^2 + 67 \cdot 27^2}{2}, \frac{2 \cdot 221 \cdot 27}{2}\right) = (48842, 5967).$$

Uvrstimo li dobivene x *i* y *u početnu zadanu jednažbu* $x^2 - 67y^2 = 1$ *vidimo da je zadovoljavaju.*
Dakle, $x = 48842$ *i* $y = 5967$ *traženo je rješenje polazne jednadžne* $x^2 - 67y^2 = 1$.

3.3 Fermat i Pellova jednadžba

Europski interes za proučavanje Pellove jednadžbe javlja se u 17. stoljeću. Vjeruje se da je Fermat[12] proučavajući Bachetove jednadžbe[13], posebno jednadžbu $x^2 + 2 = y^3$, počeo proučavati Pellovu jednadžbu $x^2 - dy^2 = 1$ te je došao do tvrdnje, bez dokaza, da za prirodan broj d koji nije potpun kvadrat jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo cjelobrojnih rješenja. Ovu Fermatovu tvrdnju dokazao je Lagrange 1770.godine. Fermata je posebno intrigiralo to što fundamentalno rješenje Pellove jednadžbe može biti izuzetno veliko. Stoga je 1657.godine poslao pisma Bessyju [14], Wallisu [15] i Brounckeru [16] u kojima ih izaziva da pronađu fundamentalno rješenje za konkretne vrijednosti broja d, tj. $d = 109, 149, 433$.
Broucknerova metoda rješavanja Pellove jednadžbe bila je slična današnjoj metodi verižnih razlomaka, koju je kasnije usavršio Lagrange.
Promotrimo sada Broucknerovu metodu.
Neka su $P, Q, R \in \mathbb{Z}$, $Q \neq 0$, $P^2 - QR = D > 0$ i D nije potpun kvadrat. Stavimo

$$F(X, Y) = QX^2 - 2PXY + RY^2 \tag{3.10}$$

te neka ρ i ρ' označavaju nultočke od $F(x, 1)$. Kako D nije potpun kvadrat, znamo da vrijedi $\rho, \rho' \notin \mathbb{Q}$. Brouncher je koristio sljedeći rezultat, ali bez dokaza.

Propozicija 3.3.1. *Pretpostavimo da je $\rho > 1$ i $\rho' < 0$. Ako je $F(X, Y) = 1$, gdje su $X, Y \in \mathbb{Z}$ i $X > Y > 1$, onda $\lfloor \rho \rfloor < \frac{X}{Y} < \lfloor \rho \rfloor + 1$.*

Uvođenjem supstitucije $X = qY + Z$ u (3.10) dobivamo

$$F'(Y, Z) = Q'Y^2 - 2P'YZ + R'Z^2,$$

gdje je $Q' = q^2Q - 2qP + R$, $P' = P - qQ$, $R' = Q$ i

$$P'^2 - Q'R' = D \tag{3.11}$$

Pretpostavimo sada da su x, y rješenja jednadžbe $x^2 - dy^2 = 1$ te stavimo $Q_0 = 1$, $P_0 = 0$, $R_0 = -D$, $X_0 = x$ i $X_1 = y$. Na temelju prethodnog računa imamo $F_0(X_0, X_1) = Q_0X_0^2 - 2P_0X_0X_1 + R_0X_1^2 = 1$ i $\rho = \sqrt{D}$, $\rho' = -\sqrt{D}$ su nule od $F_0 = (z, 1)$. Stavimo li $q_0 = \lfloor \rho_0 \rfloor$ i uvedemo supstituciju $X_0 = q_0X_1 + X_2$ u $F_0(X_0, X_1)$ dobivamo $F_1(X_1, X_2) = 1$ $(0 < X_2 < X_1)$. Ovdje vrijedi $Q_1 = q_0^2Q_0 - 2q_0P_0 + R_0$, $P_1 = P_0 - q_0Q_0$, $R_1 = Q_0$. Nadalje, stavimo

[12] Pierre de Fermat (1601.-1665.), francuski pravnik i matematičar
[13] Bachetove jednadžbe su jednadžbe oblika $x^2 + k = y^3$.
[14] Frenicle de Bessy (1604.-1674.), francuski matematičar-amater
[15] John Wallis (1616.-1703.), engleski matematičar
[16] William Brouncker (1620.-1684.), irski matematičar

$\rho_1 = \frac{1}{\rho_0 - q_0}$, $q_1 = \lfloor \rho_1 \rfloor$ te $X_1 = q_1 X_2 + X_3$ $(0 < X_3 < X_2)$ te krećemo u računanje $F_2(x_2, X_3)$ i nastavljamo opisani postupak.
Dakle, ako je $F_i(X_i, X_{i+1}) = 1$ $(0 < X_{i+1} < X_i)$, stavljamo

$$\rho_i = \frac{1}{\rho_{i-1} - q_{i-1}}, \tag{3.12}$$

$q_i = \lfloor \rho_i \rfloor$ i

$$X_i = q_i X_{i+1} + X_{i+2} \tag{3.13}$$

u F_i kako bismo dobili $F_{i+1}(X_{i+}1, X_{i+2}) = 1$ gdje je $Q_{i+1} = \frac{P_{i+1}^2 - D}{Q_i}$, $P_{i+1} = P_i - q_i Q_i$, $R_{i+1} = Q_i$ prema (3.11).
Kako je niz X_i strogo padajuć niz pozitivnih cijelih brojeva, gore opisani algoritam zaustavljamo kada je $X_j = 1$, $X_{j+1} = 0$, za neki $j \geq 0$. Kada su nam poznate vrijednosti $q_0, q_1, q_2, \ldots, q_{j-1}$, vraćamo se unazad koristeći (3.13) kako bismo pronašli x, y, odnosno tražena rješenja jednadžbe $x^2 - dy^2 = 1$.
Pogledajmo sada primjenu ovog algoritma na konkretnom primjeru.

Primjer 3.3.2. *Riješimo jednadžbu* $x^2 - 22y^2 = 1$.

Rješenje:
Primijenjući opisani algoritam slijedi:

$$\begin{aligned}
F_0(X_0, X_1) &= X_0^2 - 22X_1^2, & q_0 &= \left\lfloor \sqrt{22} \right\rfloor = 4 \\
F_1(X_1, X_2) &= -6X_1^2 + 8X_1X_2 + X_2^2, & q_1 &= \left\lfloor \frac{4 + \sqrt{22}}{6} \right\rfloor = 1 \\
F_2(X_2, X_3) &= 3X_2^2 - 4X_2X_3 - 6X_3^2, & q_2 &= \left\lfloor \frac{2 + \sqrt{22}}{3} \right\rfloor = 2 \\
F_3(X_3, X_4) &= -2X_3^2 + 8X_3X_4 + 3X_4^2, & q_3 &= \left\lfloor \frac{4 + \sqrt{22}}{2} \right\rfloor = 4 \\
F_4(X_4, X_5) &= 3X_4^2 - 8X_4X_5 - 2X_5^2, & q_4 &= \left\lfloor \frac{4 + \sqrt{22}}{3} \right\rfloor = 2 \\
F_5(X_5, X_6) &= -6X_5^2 + 4X_5X_6 + 3X_6^2, & q_5 &= \left\lfloor \frac{2 + \sqrt{22}}{6} \right\rfloor = 1 \\
F_6(X_6, X_7) &= X_6^2 - 8X_6X_7 - 6X_7^2.
\end{aligned}$$

Primijetimo da je $F_6(X_6, X_7) = 1$ *za* $X_6 = 1$ *i* $X_7 = 0$*. Sada primijenjući* (3.13) *dobivamo:*

$$\begin{aligned} X_5 &= 1 \\ X_4 &= 3 \\ X_3 &= 13 \\ X_2 &= 29 \\ X_1 &= 42 \\ X_0 &= 197 \end{aligned}$$

iz čega slijedi da je rješenje tražene jednadžbe $x^2 - 22y^2 = 1$ *jednako* $x = 197$*,* $y = 42$*.*

Brouncker je ovom metodom našao rješenja nekoliko težih Pellovih jednadžbi, uključujući i jednadžbu $x^2 - 433y^2 = 1$ koju je zadao Fermat u svojem pismu. Fermat je izabrao određene vrijednosti za d zato što odgovarajuće Pellove jednadžbe imaju velike vrijednosti za x i y. Na primjer, kod Brounckerove jednadžbe $x^2 - 433y^2 = 1$ vrijednost broja y je devetnaesteroznamenkasti broj. Brouncker, kao niti Wallis ni Bessy, nije dokazao da se Pellova jednadžba može uvijek riješiti (netrivijalno) za bilo koju pozitivnu nekvadratnu vrijednost broja d. Fermat je tvrdio kako ima dokaz za tu tvrdnju, ali nikada ga nije pokazao ili objavio.
Brounckerovu metodu modificirao je i proširio Euler. Euler je iz (3.12) shvatio kako bi se korištenjem verižnih razlomaka mogla razviti efikasnija metoda rješavanja Pellovih jednadžbi. Jedini Eulerov propust bio je što nije dokazao da metoda korištenja verižnih razlomaka daje rješenje za bilo koji d koji nije potpuni kvadrat. Kao što je već spomenuto, za taj dokaz zaslužan je Lagrange.

Bibliografija

[1] Krešimir Burazin, *Nelinearne diofantske jednadžbe*, Osječki matematički list **7** (2007), br. 1, 11–21.

[2] Branimir Dakic, *Arhimedov problem stoke*, Matematika i škola **51** (2009), 34–37.

[3] Andrej Dujella, *Uvod u teoriju brojeva*, PMF-Matematicki odjel, Sveucilište u Zagrebu (skripta) (2003).

[4] Andrej Dujella, *Diofantske jednadzbe*, Skripta, PMF-matematicki odjel, Sveucilište u Zagrebu (2006).

[5] Andrej Dujella, *Teorija brojeva*, Školska knjiga, 2019.

[6] Michael J Jacobson i Hugh C Williams, *Solving the Pell equation*, Springer, 2009.

[7] Ivona Mandic i Ivan Soldo, *Pellova jednadzba*, Osjecki matematicki list **8** (2008), 29–36.

[8] Goran Perišić, *Teorija brojeva u Aziji*, Sveučilište J. J. Strossmayera u Osijeku (završni rad), 2013.

[9] Ivana Tržić, *Verižni razlomci*, Sveučilište J. J. Strossmayera u Osijeku (diplomski rad), 2011.

Sažetak

U ovom diplomskom radu glavnu ulogu imao je poseban oblik nelinearnih diofantskih jednadžbi, odnosno Pellova jednadžba.
Cilj rada bio je definirati Pellovu jednadžbu, navesti teoreme, nužne i dovoljne, za egzistenciju i strukturu njezina rješenja, vidjeti vezu između rješenja Pellove jednadžbe i verižnih razlomaka te dati uvid u njezin povijesni razvoj.

Summary

In this thesis, the main role had special form of nonlinear diophantine equation, Pell's equation.
The aim of the study was to define Pell's equation, state theorems, necessary and sufficient, for the existence and structure of its solution, see the connection between the solution of Pell's equation and continued fractions and give an insight into its historical development.

Životopis

Zovem se Petra Pretković i rođena sam 29. srpnja 1996. u Zagrebu. Godine 2003. upisala sam Osnovnu školu Ante Kovačića u Zlataru. Srednju školu upisala sam 2011. godine. Pohađala sam Srednju školu Zlatar, smjer opća gimnazija. U rujnu 2015. godine upisala sam Preddiplomski sveučilišni studij matematike, smjer nastavnički na Prirodoslovno-matematičkom fakultetu u Zagrebu. Godine 2018. nastavljam studij upisom Diplomskog sveučilišnog studija Matematika, smjer nastavnički.