SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Jasna Bagović

METODE RJEŠAVANJA PELLOVE JEDNADŽBE

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Alan Filipin

Zagreb, rujan, 2015.

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. ____________________________

Sadržaj

Uvod

Još od davne prošlosti Diofant se počeo baviti problemom rješenja raznih jednadžbi čija je rješenja tražio u skupu cjelobrojnih ili racionalnih brojeva. Poznat je po svom radu *Arithmetica* koji se sastoji od 13 knjiga u kojima se nalazi oko 130 takvih problema, dajući njihova numerička rješenja. Za ovaj rad je bitna jednadžba koja je specijalan oblik diofantske jednadžbe, a koja se zove Pellova jednadžba.
John Pell, engleski matematičar, rođen je 1611. u Southwicku u Engleskoj, a umro 1685. godine u Londonu. U dobi od 13 godina je upisao studij na "Trinity college, Cambridge" na kojem je diplomirao 1628. godine, dok je 1630. godine na istom studiju magistrirao. Predavao je matematiku u Londonu i Amsterdamu. Bavio se algebrom i teorijom brojeva. Godine 1672. izdaje tablicu kvadratnih brojeva do 10000. Dio njegovih poznatih djela je: *Eliptica prognostica*, *Un idea of the mathematcis*, *A table of ten thounshand of square numbers* i mnoga druga.
Danas se Pell najviše pamti po jednadžbi koja je po njemu dobila ime. Jednadžbu oblika $x^2 - dy^2 = \pm 1$ zovemo Pellova jednadžba. Navedena jednadžba ima današnji naziv jer je švicarski matematičar Leonard Euler u 18.st., nakon susreta s djelom *Opera Mathematica*, greškom proglasio kako je prvi koji je ozbiljnije proučavao netrivijalna rješenja iste jednadžbe upravo John Pell. Ipak, ne postoje dokazi da se Pell ikada bavio jednadžbama ovog tipa. Cilj ovog diplomskog rada je dati uvid u Pellove jednadžbe te pokazati neke od metoda pomoću kojih se na zahvalan način dolazi do rješenja navedenih jednadžbi.
U prvom poglavlju rada će biti riječ o diofantskim jednadžbama, jer kao što je već u uvodu rečeno, Pellove jednadžbe su zapravo specijalan slučaj diofantskih jednadžbi. Nakon nekoliko važnih činjenica o diofantskim jednadžbama se prebacujemo na Pellove jednadžbe. Navest će se njihova definicija, uvjeti za egzistenciju njihovih rješenja, kao i struktura skupa rješenja.
Da bismo mogli odrediti rješenja Pellovih jednadžbi, potrebno je naći efikasne metode i alogritme njihova rješavanja. U radu će se navesti i obraditi četiri metode:

- Metoda verižnih razlomaka
- Rekurzivna metoda

- Eulerova metoda
- Metoda unimodularne transformacije ravnine

što će biti tema drugog poglavlja.
Treće poglavlje ćemo posvetiti Arhimedovom problemu stoke u kojem ćemo probati približiti i pojasniti povezanost Pellove jednadžbe sa ovim problemom iz antičke Grčke.

Poglavlje 1

Pellova jednadžba

1.1 Diofantske jednadžbe

Diofantske jednadžbe su dobile naziv po grčkom matematičaru Diofantu, koji je proučavao razne jednadžbe s dvije ili više nepoznanica čija rješenja pripadaju skupu racionalnih ili cijelih brojeva.

Definicija 1.1.1. ***Diofantskim jednadžbama*** *nazivamo općenito neodređenu polinomnu jednadžbu ili neodređenu jednadžbu nekog drugog oblika koja nalazi rješenja u domeni cijelih ili racionalnih pozitivnih brojeva.*

Posebno zanimljive su nam polinomne diofantske jednadžbe, pa ćemo koristiti sljedeću definiciju:

Definicija 1.1.2. *Polinomska jednadžba oblika $f(x_1, x_2, ..., x_n) = b$, gdje je f zadan polinom s cjelobrojnim koeficijentima u varijablama $x_1, x_2, ..., x_n$, a $b \in \mathbb{Z}$ zadan broj, i čija su rješenja također cijeli brojevi $x_1, x_2, ..., x_n$ zove se* ***diofantska jednadžba****.*

Dijele se na dvije kategorije:

- Linearne diofantske jednadžbe
- Nelinearne diofantske jednadžbe koje su barem drugog stupnja te imaju dvije ili više nepoznanica.

Linearne diofantske jednadžbe

Za početak ćemo navesti definiciju linearnih diofantskih jednadžbi, a zatim neke važnije rezultate koji daju nužne i dovoljne uvjete za egzistenciju i oblik rješenja diofantskih jednadžbi.

Definicija 1.1.3. *Diofantske jednadžbe oblika*

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

gdje su $a_1, a_2, \ldots, a_n$ *cjelobrojni koeficijenti,* $b \in \mathbb{Z}$ *zadan broj, a* $x_1, x_2, \ldots, x_n$ *nepoznanice nazivamo* ***linearne diofantske jednadžbe****.*

U sljedećem teoremu promatramo diofantske jednadžbe sa dvije nepoznanice, odnosno jednadžbe oblika:

$$ax + by = c, \ a, b, c \in \mathbb{Z}. \tag{1.2}$$

Teorem 1.1.4. *Neka su a,b,c cijeli brojevi i neka je d najveći zajednički djelitelj od a i b. Ako* $d \nmid c$*, onda jednadžba* $ax+by = c$ *nema cjelobrojnih rješenja. Ako* $d|c$*, onda jednadžba ima beskonačno mnogo cjelobrojnih rješenja. Ako je* (x_1, y_1) *jedno rješenje, onda su sva rješenja dana sa* $x = x_1 + \frac{b}{d} \cdot t$*,* $y = y_1 - \frac{a}{d} \cdot t$*, gdje je* $t \in \mathbb{Z}$*.*

U dokazu iskazanog teorema se pozivamo na tvrdnju teorema:

Teorem 1.1.5. *Neka su a i m prirodni, te b cijeli broj. Kongruencija*

$$ax \equiv b \pmod{m} \tag{1.3}$$

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.*

Sada možemo krenuti s dokazom Teorema 1.1.4.

Dokaz. U slučaju da jednadžba (1.2) ima rješenja, tada očito vrijedi $d|c$. Pretpostavimo da vrijedi $d|c$. Nadalje, za kongruenciju

$$ax \equiv b \pmod{m}$$

postoje rješenja po Teoremu 1.1.5. Nadalje ako je x_1 neko rješenje, onda su sva rješenja od promatrane kongruencije dana sa $x \equiv x_1 + \frac{b}{d} \cdot k \pmod{b}$, gdje je $k = 0, 1, \ldots, d-1$. Stoga su sva rješenja od (1.2) oblika

$$x = x_1 + \frac{b}{d} \cdot t, \ t \in \mathbb{Z}. \tag{1.4}$$

Uvrstimo li (1.4) u (1.2), dobijemo sljedeće:

$$by = c - ax_1 - \frac{ab}{d} \cdot t = by_1 - \frac{ab}{d} \cdot t,$$

pa je na kraju

$$y = y_1 - \frac{a}{d} \cdot t.$$

□

Teorem 1.1.6. *Neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi različiti od nule. Tada linearna diofantska jednadžba*

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c \tag{1.5}$$

ima rješenja ako i samo ako $(a_1, a_2, ..., a_n)|c$. Nadalje, ako jednadžba ima barem jedno rješenje, onda ih ima beskonačno.

Dokaz. Činjenica da postoji beskonačno mnogo rješenja linearne jednadžbe (1.5) rezultira sljedećim rezultatom:

$$(a_1, a_2, \ldots, a_n)|c$$

čime je dokazana jedna implikacija teorema. Suprotni smjer implikacije dokazujemo matematičkom indukcijom. Pretpostavimo da

$$(a_1, a_2, \ldots, a_n)|c,$$

onda (1.5) ima beskonačno mnogo rješenja.

Neka je $n = 2$, tada primjenjujući Teorem 1.1.4 tvrdnja vrijedi.

Pretpostavka indukcije je da tvrdnja vrijedi za jednadžbe s $n - 1$ varijabli.

Neka je $d = (a_{n-1}, a_n)$. Jednadžba $a_1x_1 + \cdots + a_{n-2}x_{n-2} + dy = c$ ima beskonačno mnogo rješenja $(x_1, \ldots, x_{n-2}, y)$ (vrijedi po pretpostavci indukcije). Za svako rješenje ove jednadžbe promatramo:

$$a_{n-1}x_{n-1} + a_nx_n = dy. \tag{1.6}$$

Zbog činjenice da $(a_{n-1}, a_n)|dy$ slijedi da ova jednadžba ima beskonačno mnogo rješenja oblika (x_{n-1}, x_n). S time smo dokazali da jednadžba (1.5) ima beskonačno mnogo rješenja $(x_1, \ldots, x_n)$. □

Primjer 1.1.7. *Neka je $3x + 5y = 8$ diofantska jednadžba. Provjerimo njenu rješivost. Najveći zajednički djelitelj brojeva $(3, 5)$ je 1, tj. $nzd(3, 5) = 1$, tada vrijedi da $1|8$ pa slijedi da diofantska jednadžba ima cjelobrojna rješenja. Partikularno rješenje ove jednadžbe je dano sa $(x_1, y_1) = (1, 1)$. Rješenje pridružene homogene jednadžbe $3x + 5y = 0$ je $x_H = 5k$, $y_H = -3k$, $k \in Z$.*

Opće rješenje jednadžbe je dano sa:

$$x = 1 + 5k, \ y = 1 - 3k, \ k \in \mathbb{Z}. \tag{1.7}$$

Nelinearne diofantske jednadžbe

U ovom dijelu ćemo navesti neke od metoda rješavanja nelinearnih diofantskih jednadžbi, no prvo krećemo s definicijom:

Definicija 1.1.8. ***Nelinearnim diofantskim jednadžbama*** *zovemo jednadžbe s cjelobrojnim koeficijentima u kojima se nepoznanice ne pojavljuju u prvoj potenciji već one sadrže i članove višeg reda, kao npr.* x^2, xy, y^3*, itd.*

Kod nelinearnih diofantskih jednadžbi ne postoji univerzalna metoda rješavanja, već postoje razni načini na koje se takve jednadžbe mogu rješavati:

- metoda faktorizacije - cilj je jednu stranu jednadžbe zapisati u obliku produkta cjelobrojnih vrijednosti te zatim promatramo moguće slučajeve, uzimajući u obzir drugu stranu jednadžbe,
- metoda kvocijenta - kod ove metode zapisujemo jednu stranu jednadžbe u obliku kvocijenta dviju cjelobrojnih vrijednosti. Na drugoj strani jednadžbe imamo, također, cjelobrojnu vrijednost. Zbog toga nazivnik tog razlomka mora dijeliti brojnik, što nam daje raznolike slučajeve kao potencijalna rješenja,
- metoda posljednje znamenke - metoda koja koristi ispitivanje ostataka pri dijeljenju s brojem 10,
- metoda kongruencija - metoda koja razlikovanje slučajeva vrši ispitivanjem ostataka koje daju dijelovi jednadžbe pri dijeljenju s nekim cijelim brojem, te njihovim uspoređivanjem,

i druge metode.
Nama najvažnija jednadžba koja pripada ovoj skupini je **Pellova jednadžba**. U nastavku rada ćemo dati njenu preciznu definiciju kao i metode kojima se ona rješava.

1.2 Pellova jednadžba $x^2 - dy^2 = 1$

Specijalni oblik diofantske jednadžbe drugog stupnja je Pellova jednadžba.

Definicija 1.2.1. *Diofantska jednadžba*

$$x^2 - dy^2 = 1 \tag{1.8}$$

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

$$x^2 - dy^2 = N \tag{1.9}$$

gdje je $d \in \mathbb{N}$*,* d *nije potpuni kvadrat i* $N \in \mathbb{N}$ *zovemo* ***pellovska jednadžba****.*

U slučaju kad je $d < 0$ ili je d potpun kvadrat, tada jednadžba (1.8) ima konačno mnogo rješenja, odnosno (1.8) ima beskonačno mnogo rješenja kada d nije potpuni kvadrat.

Egzistencija rješenja Pellove jednadžbe

Teorem 1.2.2. *Neka je d prirodni broj koji nije potupun kvadrat. Postoji bar jedan par prirodnih brojeva (x, y) koji zadovoljava Pellovu jednadžbu.*

Za dokaz iskazanog teorema su nam potrebne dvije tvrdnje:

Lema 1.2.3. *Ako je α iracionalan broj, onda postoji beskonačno mnogo relativno prostih cijelih brojeva p i q takvih da je*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.10}$$

Iskazana lema je poznata kao Dirichletov teorem.

Korolar 1.2.4. *Neka je d prirodan broj koji nije potpun kvadrat. Postoji beskonačno mnogo parova prirodnih brojeva (x, y) koji zadovoljavaju nejednakost*

$$\left|x^2 - dy^2\right| < 1 + 2\sqrt{d}. \tag{1.11}$$

Dokaz. Broj $\sqrt{d}$ je iracionalan te koristeći Lemu 1.2.3 postoji beskonačno mnogo parova (x, y) takvih da vrijedi nejednakost

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

Odnosno, vrijedi:

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

Te je na kraju

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

Što znači da nejednakost (1.11) ima beskonačno mnogo cjelobrojnih rješenja x i y. □

Sada možemo dokazati Teorem 1.2.2.

Dokaz. Po Korolaru 1.2.4, znamo da postoji cijeli broj $k \neq 0$ takav da vrijedi da je $x^2 - dy^2 = k$ za beskonačno parova brojeva (x, y), gdje su $x, y \in \mathbb{Z}$. Tada sigurno postoje barem dva para (x_1, y_1) i (x_2, y_2) za koje je

$$x_1 \equiv x_2 \pmod{|k|},\ y_1 \equiv y_2 \pmod{|k|}. \tag{1.12}$$

Sada je

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

Iz (1.12) i $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k$ vrijede i sljedeće kongruencije:

$$x_1x_2 - y_1y_2d \equiv x_1^2 - dy_1^2 \equiv 0 \pmod{|k|},\ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}.$$

Prema tome,

$$x_1x_2 - y_1y_2d = ku,\ x_1y_2 - x_2y_1 = kv,$$

za neke $u, v \in \mathbb{Z}$. Te, vrijedi

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

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

Kada ove dvije jednadžbe pomnožimo, dobijemo sljedeće

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = k^2 = k^2(u^2 - dv^2)$$

Odnosno, vrijedi da je $u^2 - dv^2 = 1$.
Potrebno je dokazati da je $v \neq 0$. Pretpostavimo da je $v = 0$. Tada vrijedi $x_1y_2 = x_2y_1$, $u = 1$ ili $u = -1$, pa imamo

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

Kad podijelimo jednakost sa k, dobivamo $x_1 - y_1\sqrt{d} = \pm(x_2 - y_2\sqrt{d})$, iz čega slijedi da je $x_1 = \pm x_2$ i $y_1 = \pm y_2$. Obzirom da možemo birati proizvoljne $|x_1| \neq |x_2|$, slijedi da je $v \neq 0$. □

Ovim smo dokazali postojanje rješenja Pellove jednadžbe u skupu prirodnih brojeva.

Struktura rješenja Pellove jednadžbe

Teoremom 1.2.2 smo ustanovili da Pellova jednadžba ima rješenje (u, v) u skupu prirodnih brojeva. Označimo to rješenje na sljedeći način:

$$u + v\sqrt{d} \tag{1.13}$$

odnosno, označili smo ga kao element polja $\mathbb{Q}(\sqrt{d})$. Možemo reći da je rješenje $u + v\sqrt{d}$ veće od rješenja $u' + v'\sqrt{d}$, ako vrijedi numerička nejednakost $u + v\sqrt{d} > u' + v'\sqrt{d}$. Obzirom na to, možemo izdvojiti i najmanje rješenje.

Definicija 1.2.5. *Najmanje rješenje pellove jednadžbe ili pellovske jednadžbe naziva se **fundamentalno rješenje** i označava s* $x_1 + y_1\sqrt{d}$.

Teorem 1.2.6. *Neka je* $x_1 + y_1\sqrt{d}$ *fundamentalno rješenje Pellove jednadžbe* (1.8)*. Tada su sva rješenja u skupu prirodnih brojeva dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{1.14}$$

Tj., vrijedi

$$x_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} x_1^{n-2k} y_1^{2k} d^k,$$

$$y_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} x_1^{n-2k-1} y_1^{2k+1} d^k.$$

Dokaz. Koristeći (1.14) slijedi $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, pa je

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

iz čega slijedi da su (x_n, y_n) zaista rješenja.
Nadalje, pretpostavimo da je (s, t) rješenje jednadžbe koje se ne nalazi u skupu

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

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

$$(x_1 + y_1\sqrt{d})^m < s + t\sqrt{d} < (x_1 + y_1\sqrt{d})^{m+1}. \tag{1.15}$$

Ukoliko pomnožimo (1.15) sa $(x_1 - y_1\sqrt{d})^m$ dobijemo sljedeće

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

Neka su $a, b \in \mathbb{Z}$ takvi da vrijedi

$$a + b\sqrt{d} = (s + t\sqrt{d})(x_1 - y_1\sqrt{d})^m.$$

Imamo:

$$a^2 - db^2 = (s^2 - dt^2)(x_1^2 - dy_1^2)^2 = 1.$$

Iz $a + b\sqrt{d} > 1$ slijedi $0 < a - b\sqrt{d} < 1$, pa vrijedi da je $a > 0$ i $b > 0$. Sada možemo zaključiti da 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. □

Napomena 1.2.7. *Iz jednadžbe* (1.15) *se može dobiti da nizovi* (x_n) *i* (y_n) *zadovoljavaju rekurzije*

$$x_{n+2} = 2x_1 x_{n+1} - x_n,$$

$$y_{n+2} = 2x_1 y_{n+1} - y_n,$$

za svaki $n \geq 0$ *gdje je* (x_1, y_1) *fundamentalno rješenje od* (1.8)*, dok je* $(x_0, y_0) = (1, 0)$ *trivijalno rješenje.*

1.3 Pellovska jednadžba $x^2 - dy^2 = N$

Definicija 1.3.1. *Jednadžba oblika*

$$x^2 - dy^2 = N \tag{1.16}$$

gdje je $d \in \mathbb{N}$, d nije potpuni kvadrat i $N \in \mathbb{N}$ zovemo ***pellovska jednadžba****.*

Pellovska jednadžba ne mora imati rješenje, no međutim u slučaju da je $x + y\sqrt{d}$ jedno njezino rješenje, a $u + v\sqrt{d}$ proizvoljno rješenje jednadžbe (1.12), tada je i

$$(x + y\sqrt{d})(u + v\sqrt{d}) = xu + yud + (yu + xv)\sqrt{d} \tag{1.17}$$

rješenje jednadžbe (1.3.1). Za takvo rješenje kažemo da je asocirano rješenjem $x + y\sqrt{d}$. Možemo reći da skup svih asociranih rješenja tvori jednu klasu rješenja. Rješenja su asocirana ako i samo ako vrijedi

$$xx' \equiv dyy' \pmod{N}, xy' \equiv x'y \pmod{N}. \tag{1.18}$$

Ako se klasa **K** sastoji od rješenja $x_i + y_i\sqrt{d}$, za $i = 1, 2, \ldots$, tada rješenja oblika $x_i - y_i\sqrt{d}$, za $i = 1, 2, 3, \ldots$ čine također klasu rješenja u oznaci $\bar{\mathbf{K}}$. Klase **K** i $\bar{\mathbf{K}}$ su konjugirane.

Definicija 1.3.2. *Kažemo da je klasa* **K** ***dvoznačna*** *ukoliko vrijedi da je*

$$K = \bar{K}.$$

Iz klase **K** biramo jedno od rješenja $x^* + y^*\sqrt{d}$ na sljedeći način:
y^* je najmanja nenegativna vrijednost od y koja se pojavljuje u klasi **K**. Ako je **K** dvoznačna tada je x^* jednoznačno određen pod uvjetom da tražimo $x^* \geq 0$. No, ako klasa **K** nije dvoznačna, tada je x^* jedinstveno određen. Tako konstruirano rješenje je ujedno i fundamentalno rješenje pellovske jednadžbe.

Teorem 1.3.3. *Neka je $N > 0$ i neka je $u+v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2-dy^2 =$ 1. Tada za svako fundamentalno rješnje $x^* + y^*\sqrt{d}$ jednadžbe $x^2 - dy^2 = N$, vrijede sljedeće nejednakosti*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+1)}}. \sqrt{N}, 0 < |x^*| \leq \sqrt{\frac{1}{2}(u+1)N}. \tag{1.19}$$

Dokaz. Pretpostavimo da je x^* pozitivan. Očito onda vrijedi:

$$x^*u - dy^*v = x^*u - \sqrt{(x^{*2} - N)(u^2 - 1)} > 0.$$

Pogledajmo rješenje

$$(x^* + y^* \sqrt{d})(u - v\sqrt{d}) = x^*u - dy^*v + (ux^* - vy^*)\sqrt{d},$$

koje pripada istoj klasi kao i $x^* + y^* \sqrt{d}$. Rješenje $x^* + y^* \sqrt{d}$ je fundamentalno rješenje te klase i zato što je

$$x^*u - dy^*v > 0$$

mora vrijediti

$$x^*u - dy^*v \geq x^*.$$

Iz toga slijedi

$$x^{*2}(u-1)^2 \geq d^2y^{*2}v^2 = (x^{*2} - N)(u^2 - 1),$$

odnosno

$$\frac{u-1}{u+1} \geq 1 - \frac{N}{x^{*2}}$$

te je na kraju

$$x^{*2} \leq \frac{1}{2}(u+1)N.$$

Iz ove ocjene, lako se izvede ocjena za y^*. □

U slučaju $N < 0$ vrijedi i sljedeći teorem, analogan Teoremu 1.3.3:

Teorem 1.3.4. *Neka je $u + v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$. Tada za svako fundamentalno rješenje $x^* + y^* \sqrt{d}$ jednadžbe $x^2 - dy^2 = N$, vrijede sljedeće nejednakosti*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+1)}}. \sqrt{N}, 0 < |x^*| \leq \sqrt{\frac{1}{2}(u+1)N}. \tag{1.20}$$

Napomena 1.3.5. *Ukoliko je $x^* + y^* \sqrt{d}$ fundamentalno rješenje pellovske jednadžbe* (1.3.1) *koje pripada klasi* **K***, onda su sva rješenja klase oblika:*

$$x_n + y_n\sqrt{d} = \pm(x^* + y^* \sqrt{d})(u + v\sqrt{d})^n, \ n \in \mathbb{Z},$$

gdje je $u + v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.

Ovisno o broju N može se dati dovoljno dobra ocjena za broj klasa, ta ocjena je dana u sljedećoj propoziciji.

Propozicija 1.3.6. *Neka je N kvadratno slobodan cijeli broj, tada je broj klasa rješenja jednadžbe $x^2 - dy^2 = N$ najviše $2^{\omega(N)}$ gdje je $\omega(N)$ broj prostih faktora od N.*

Nadalje, sljedeća propozicija daje način traženja rješenja pellovske jednadžbe ako je $|N| < \sqrt{d}$.

Propozicija 1.3.7. *Pretpostavimo da je* $|N| < \sqrt{d}$*. Ako je* $x + y\sqrt{d}$ *rješenje jednadžbe* $x^2 - dy^2 = N$ *u prirodnim brojevima, onda je* $\frac{x}{y}$ *neka konvergenta u razvoju u verižni razlomak od* $\sqrt{d}$*.*

Verižne razlomke ćemo detaljnije obraditi u idućem poglavlju.

Primjer 1.3.8. *Primjenjujući dosadašnje rezultate želimo naći fundamentalna rješenja jednadžbe*

$$x^2 - 2y^2 = 119$$

Fundamentalno rješenje jednadžbe $x^2 - 2y^2 = 1$ *dano je sa* $3 + 2\sqrt{2}$*. Sada sva fundamentalna rješenja moraju zadovoljavati sljedeće nejednakosti*

$$0 \leq y^* \leq \frac{2}{\sqrt{2 \cdot 4}} \cdot \sqrt{119} < 8, 0 < |x^*| \leq \sqrt{\frac{1}{2} \cdot 4 \cdot 119} < 16.$$

Sada se vidi da rješenja koja zadovoljavaju tražene nejednakosti su:

$$11 + \sqrt{2}, -11 + \sqrt{2}, 13 + 5\sqrt{2}, -13 + 5\sqrt{2}.$$

Poglavlje 2

Metode rješavanja Pellove jednadžbe

2.1 Metoda verižnih razlomaka

Teorem 1.2.6 i Napomena 1.2.7 nam pokazuju na koji način možemo generirati sva rješenja Pellove jednadžbe (1.8) ukoliko znamo njeno fundamentalno rješenje. No, problem se javlja u trenu kada treba naći to fundamentalno rješenje. Jedna od efikasnih metoda za pronalaženje rješenja Pellovih jednadžbi je upravo **metoda verižnih ralomaka**. Svako netrivijalno rješenje jednadžbe (1.8) daje jako dobru racionalnu aproksimaciju iracionalnog broja $\sqrt{d}$. Dobre racionalne aproksimacije realnog broja se dobivaju pomoću njegovog razvoja u verižni razlomak.

Definicija 2.1.1. *Neka je $\alpha \in \mathbb{R}$. Izraz oblika*

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} \tag{2.1}$$

*gdje je $a_0 \in \mathbb{Z}$, te $a_1, a_2, \ldots \in \mathbb{N}$, zove se **razvoj broja α u jednostavni verižni razlomak**. Kraće to zapisujemo kao $\alpha = [a_0, a_1, a_2, \ldots]$. Aproksimaciju broja α danu sa*

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n] \tag{2.2}$$

*nazivamo **n-tom konvergentom broja** α.*

U sljedećem teoremu će se vidjeti da su konvergente jako dobre racionalne aproksimacije iracionalnog broja α.

Teorem 2.1.2. *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*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \tag{2.3}$$

Dokaz. Kako su $\alpha - \frac{p_n}{q_n}$ i $\alpha - \frac{p_{n-1}}{q_{n-1}}$ suprotnog predznaka tako vrijedi sljedeće:

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

Pa na samom kraju vrijedi:

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2}$$

ili

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}$$

Očito je da vrijedi da barem jedna od konvergenti zadovoljava tvrdnju teorema. □

Obrat upravo dokazanog teorema je dao Legendre i taj teorem će se pokazati kao jako važan rezultat za određivanje fundamentalnih rješenja Pellove jednadžbe.

Teorem 2.1.3. *Neka su p i q cijeli brojevi takvi da vrijedi*

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

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

Za dokaz iskazanog teorema potrebna nam je sljedeća lema:

Lema 2.1.4. *Neka je α iracionalan broj i neka su $c_k = \frac{p_k}{q_k}$ gdje je $k \geq 0$ konvergente razvoja u verižni razlomak broja α. Ako su $p, q \in \mathbb{Z}$ tako da je $q > 0$ i $k \in \mathbb{N}$ tako da vrijedi*

$$\left|q\alpha - p\right| < \left|q_k\alpha - p_k\right|,$$

onda je $q \geq q_{k+1}$.

Slijedi dokaz Teorema 2.1.3.

Dokaz. Za početak ćemo pretpostaviti da je $\alpha \neq \frac{p}{q}$, jer inače je tvrdnja trivijalno zadovoljena. Neka je k najveći prirodan broj takav da je $q \geq q_k$. Takav k sigurno postoji jer je $q_0 = 1$, a $\lim_{k\to\infty} q_k = \infty$. Znamo da je $q_k \leq q < q_{k+1}$ po Lemi 2.1.4 možemo zaključiti da vrijedi

$$\left|q_k\alpha - p_k\right| \leq \left|q\alpha - p\right| = q\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q},$$

odnosno

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2qq_k}.$$

Znamo da je $\frac{p}{q} \neq \frac{p_k}{q_k}$ imamo $\left|qp_k - pq_k\right| \geq 1$, iz čega slijedi da je

$$\frac{1}{qq_k} \leq \frac{\left|qp_k - pq_k\right|}{qq_k} = \left|\frac{p_k}{q_k} - \frac{p}{q}\right| \leq \left|\frac{p_k}{q_k} - \alpha\right| + \left|\alpha - \frac{p}{q}\right| < \frac{1}{2qq_k} + \frac{1}{2q^2},$$

tj.

$$\frac{1}{2qq_k} < \frac{1}{2q^2},$$

što povlači $q_k > q$, što je u kontradikciji sa $q \geq q_k$.

□

Teorem 2.1.5. *Neka je $(u, v) \in \mathbb{N}^2$ rješenje Pellove jednadžbe $x^2 - dy^2 = 1$. Onda je $\frac{u}{v}$ neka konvergenta razvoja $\sqrt{d}$ u verižni razlomak.*

Dokaz. Iz Pellove jednadžbe (njenom faktorizacijom), imamo:

$$(u - v\sqrt{d})(u + v\sqrt{d}) = 1. \tag{2.4}$$

Odavde možemo zaključiti da je $u - v\sqrt{d} > 0$ i da je onda $\frac{u}{v} > \sqrt{d}$. Jednakost (2.4) je ekvivalentna sljedećoj:

$$u - v\sqrt{d} = \frac{1}{u + v\sqrt{d}}$$

Sada imamo

$$\frac{u}{v} - \sqrt{d} = \frac{1}{v(u + v\sqrt{d})} = \frac{1}{u^2(\frac{u}{v} + \sqrt{d})} < \frac{1}{2v^2\sqrt{d}} < \frac{1}{2v^2}.$$

Zato što je $\frac{u}{v} - \sqrt{d}$ pozitivan, vrijedi svakako $\left|\frac{u}{v} - \sqrt{d}\right| < \frac{1}{2v^2}$. Primjenimo li sada Teorem 2.1.3 slijedi da je $\frac{u}{v}$ konvergenta razvoja $\sqrt{d}$ u verižni razlomak. □

Iskazat ćemo još jedan teorem vezan za duljinu perioda, a koristi se često u dokazima.

Teorem 2.1.6. *Sva rješenja u prirodnim brojevima jednadžbi $x^2 - dy^2 = 1$ nalaze se među $x = p_n$, $y = q_n$, gdje su $\frac{p_n}{q_n}$ konvergente u razvoju od $\sqrt{d}$. Neka je l duljina perioda u razvoju od $\sqrt{d}$.*

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

Primjer 2.1.7. *Nađite sva rješenja jednadžbe* $x^2 - 15y^2 = 1$ *za koja je* $1 < x < 1000$.

Rješenje

Prvo razvijemo $\sqrt{15}$ u verižni razlomak sa rješenjem $\sqrt{15} = [3, \overline{1, 6}]$.
Iz toga vidimo da je period paran. Po prethodnom teoremu vrijedi da je najmanje rješenje jednadžbe $x^2 - 15y^2 = 1$ jednako $(x_1, y_1) = (4, 1)$. Potom slijedi

$$x_2 = 8 \cdot 4 - 1 = 31, y_2 = 8$$

$$x_3 = 8 \cdot 31 - 4 = 244, y_3 = 63$$

Već x_4 nam prestiže vrijednost 1000 pa vrijedi da su rješenja jednadžbe

$$(x, y) = (4, 1), (31, 8), (244, 63).$$

2.2 Rekurzivna metoda

Teorem 2.2.1. *Rješenje Pellove jednadžbe 1.8 u skupu prirodnih brojeva* (x_n, y_n) *zadovoljavaju rekurzivne relacije*

$$\begin{aligned} x_n &= x_1 x_{n-1} + d y_1 y_{n-1}, \\ y_n &= y_1 x_{n-1} + x_1 y_{n-1}, n \geq 1, \end{aligned} \tag{2.5}$$

pri čemu je (x_1, y_1) *fundamentalno, a* $(x_0, y_0) = (1, 0)$ *trivijalno rješenje od 1.8 .*
Nadalje, uz iste početne uvjete vrijede i relacije

$$\begin{aligned} x_n &= 2x_1 x_{n-1} - x_{n-2}, \\ y_n &= 2x_1 y_{n-1} - y_{n-2}, n \geq 2. \end{aligned} \tag{2.6}$$

Dokaz. Rekurzije iz 2.5 direktno slijede prema 1.14, vrijedi

$$(x_{n-1} + y_{n-1})(x_1 + y_1 \sqrt{d}) = x_n + y_n \sqrt{d}.$$

Kako je $x_1 - y_1 \sqrt{d} = (x_1 + y_1 \sqrt{d})^{-1}$ imamo

$$(x_{n-1} + y_{n-1})(x_1 - y_1 \sqrt{d}) = x_{n-2} + y_{n-2} \sqrt{d},$$

Raspišemo li gornje jednakosti, dobivamo

$$x_1 x_{n-1} + y_1 x_{n-1} \sqrt{d} + x_1 y_{n-1} \sqrt{d} + y_1 y_{n-1} d = x_n + y_n \sqrt{d},$$

$$x_1 x_{n-1} - y_1 x_{n-1} \sqrt{d} + x_1 y_{n-1} \sqrt{d} - y_1 y_{n-1} d = x_{n-2} + y_{n-2} \sqrt{d}$$

te njihovim zbrajanjem slijedi 2.6 □

Spomenimo još dva korolara vezana za rekurzije a u kojima se spominju identiteti zbroja te dvostrukog kuta.

Korolar 2.2.2. *Neka je* (x_n, y_n) *niz rješenja Pellove jednadžbe. Vrijede sljedeći identiteti zbroja, odnosno razlike:*

$$x_{m\pm n} = x_m x_n \pm d y_m y_n,$$

$$y_{m\pm n} = x_n y_m \pm x_m y_n, m \geq n.$$

Korolar 2.2.3. *Neka je* (x_n, y_n) *niz rješenja Pellove jednadžbe. Vrijedi sljedeći identitet dvostrukog kuta:*

$$x_{2n} = 2x_n^2 - 1,$$

$$y_{2n} = 2x_n y_n, n \geq 0.$$

Primjer 2.2.4. *Odredite prirodne brojeve* $n \in \mathbb{N}$ *za koje je* $1 + 11n^2$ *kvadratni broj.*

Rješenje

Dakle, trebamo takav prirodni broj n za koji izraz $1 + 11n^2$ možemo napisati u obliku

$$x^2 = 1 + 11n^2.$$

Supstituiramo li $n = y$, prepoznajemo Pellovu jednadžbu

$$x^2 - 11y^2 = 1$$

s fundamentalnim rješenjem $x_1 = 10$, $y_1 = 3$. Rekurzija za niz (y_n) sada izgleda

$$y_{n+2} = 20y_{n+1} - y_n, (y_0 = 0, y_1 = 3)$$

iz čega dobivamo konačna rješenja za n, n= 3, 60, 1197, ...

2.3 Eulerova metoda

Pitagora iz Samosa, poznat kao prvi *pravi* matematičar, premda premalo znamo o njegovom radu, jedna je od vrlo važnih osoba u razvoju matematike. Upravo njegove trojke(*Pitagorine tojke)* ćemo koristiti u Eulerovoj metodi, pa definirajmo ih:

Definicija 2.3.1. *Uređenu trojku prirodnih brojeva (x ,y, z) zovemo Pitagorina trojka ako su x, y katete, a z hipotenuza nekog pravokutnog trokuta, tj. ako vrijedi*

$$x^2 + y^2 = z^2. \tag{2.7}$$

Ako su x, y, z relativno prosti, onda kažemo da je $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ ***primitivna Pitagorina trojka****.*

A kakve veze ima Pellova jednadžba sa Pitagorinom trojkom dajemo primjerom. Neka je trojka $(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$ Pitagorina i uzmimo da je $a - b = 1$. Uvrstimo li to u formulu, dobivamo:

$$m^2 - 2mn - n^2 = 1(m - n)^2 - 2n^2 = 1.$$

Supstitucijom $m - n = x$ i $n = y$ dobivamo:

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

Dakle, cjelobrojna rješenja $(x,\ y)$ ove Pellove jednadžbe nam daju rješenja za (m,n). No, ono što nas zanima je kako iz Pitagorine trojke doći do rješenja Pellovih jednadžbi. Rješenje za to nam je dao Leonard Euler koji je generirao Pitagorine trojke i njene analogone za dobivanje rješenja različitih Pellovih jednadžbi, uključujući i one oblika $x^2 - dy^2 = -1$ jer su one generalizirane Pellove jednadžbe.

Propozicija 2.3.2. *Neka je (x,y)=(p,q) rješenje od $x^2 - dy^2 = -1$. Tada je (x,y)=($2p^2 + 1$, $2pq$) rješenje od $x^2 - dy^2 = 1$.*

Dokaz.

$$\begin{aligned}(2p^2 + 1)^2 - d(2pq)^2 &= 4p^4 + 4p^2 + 1 - d4p^2q^2 \\ &= 4p^2(p^2 - dq^2) + 4p^2 + 1 \\ &= 4p^2(-1) + 4p^2 + 1 \\ &= 1\end{aligned} \tag{2.8}$$

□

Dakle, možemo generirati rješenja $x^2 - dy^2 = 1$ it p i q koji zadovoljavaju $p^2 = dq^2 - 1$. Fiksiramo li vrijednost za q, imamo $q^2 = \frac{p2+1}{d} \cdot p^2 + 1$ je trivijalna suma dvaju kvadrata, pa to zahtjevamo i od q^2. Pretpostavimo da je q najveći broj u Pitagorinoj trojci($q^2 = b^2 + c^2$). Kako bi $d = \frac{p^2+1}{q^2}$ bio cijeli broj, mora vrijediti

$$\begin{aligned}p^2 + 1 &= (b^2 + c^2)(f^2 + g^2) \\ &= (bf + cg)^2 + (bf - cg)^2.\end{aligned}$$

Uz dobivene p,b,c odredimo rješenja $(g,\ f)$.

Pogledajmo to sada na primjeru:

Primjer 2.3.3. *Uzmimo q=13 i koristeći Eulerovu metodu odredimo rješenja nekih Pellovih jednadžbi.*

Rješenje

Krenimo s nekom Pitagorinom trojkom, $(5, 12, 13)$, $5^2 + 12^2 = 12^2$.

$$q = 13, b = 5, c = 12$$

pa je

$$bg - cf = \pm 1$$

$$5g - 12f = \pm 1 \tag{2.9}$$

Sada iz (2.12) imamo rješenja $(g, f) = (5, 2), (7, 3), (17, 7), (9, 8)$.
Vrijednosti od p dobivamo $p = 5f + 12g$.
Tablicu rješenja dobivamo uz fiksni $q = 13$, formule $d = \frac{p^2+1}{q^2}$, $x = 2p^2 + 1$, $y = 2pq$.
Tablica izgleda kao

f	2	3	7	8
g	5	7	17	9
d	29	58	338	425
p	70	99	239	268
x	9801	19603	114243	143649
y	1820	2574	6214	6968

Moguća rješenja očitamo iz tablice.

2.4 Metoda unimodularne transformacije ravnine

Rješenja Pellove jednadzbe 1.8 gdje d nije potpuni kvadrat u geometriji određuju hiperbolu u pravokutnom koordinatnom sustavu. Metoda unimodularne transformacije ravnine je metoda pronalaženja rješenja Pellove jednadžbe na osnovi poznavanja prethodnog rješenja.

Definicija 2.4.1. *Ako je u ravnini zadan Kartezijev pravokutni koordinatni sustav, onda u svakoj točki (x, y) te ravnine možemo pridružiti točku (x', y') te iste ravnine određenu jednakostima*

$$x' = ax + by \tag{2.10}$$

$$y' = cx + dy,$$

gdje su a, b, c i d zadani cijeli brojevi takvi da vrijedi

$$ad - bc = 1. \tag{2.11}$$

Svako preslikavanje 2.10 koje zadovoljava uvjet 2.11 zovemo unimodularnom transformacijom ravnine.

Očito imamo trivijalno rješenje $(x', y') = (1, 0)$.
Za $x_1, x_2 \in \mathbb{N} \cup \{0\}$ točka (x_1, x_2) je na desnoj polugrani hiperbole koja je najbliža točki $(1, 0)$. Treba pokazati da postoji unimodularna transformacija 2.11 koja desnu gornju granu hiperbole preslikava samu u sebe, a točku $(1, 0)$ u (x_1, y_2). Iz tog preslikavanja slijedi da je $a = x_1$ a $c = y_1$. Sada je transformacija oblika

$$x' = x_1 x + by \tag{2.12}$$

$$y' = y_1 x + dy,$$

pa mora vrijediti

$$x_1 d - y_1 b = 1 \tag{2.13}$$

Hiperbola $x^2 - dy^2 = 1$ se translacijom 2.12 preslikava u

$$x^2 + 2(x_1 b - ky_1 d)xy + (b^2 - kd^2)y^2 = 1.$$

Dakle, ako i samo ako vrijedi da je $x_1 b - ky_1 d = 0$ te $b^2 - kd^2 = -k$, hiperbola će se preslikati u samu sebe.

Sada, iz 2.13 i $x_1 b - ky_1 d = 0$ slijedi

$$b = ky_1, \ d = x_1.$$

Tansformacija 2.10 uz vrijednosti poviše sada izgleda ovako:

$$x' = x_1 x + ky_1 y,$$

$$y' = y_1 x + x_1 y$$

No, budući da vrijedi

$$x_1{}^2 - ky_1{}^2 = 1$$

što povlači

$$k = \frac{x_1{}^2 - 1}{y_1{}^2},$$

konačno imamo transformaciju koja glasi

$$x' = x_1 x + \frac{{x_1}^2 - 1}{y_1} y,$$

$$y' = y_1 x + x_1 y.$$

Sada možemo reći da Pellovoj jednadžbi oblika $x^2 - ky^2 = 1$ s fundamentalnim rješenjem (x_1, y_1) odgovara unimodularna matrica i transformacija:

$$M = \begin{bmatrix} x_1 & \frac{{x_1}^2-1}{y_1} \\ y_1 & x_1 \end{bmatrix},$$

$$x_{n+1} = x_1 x_n + \frac{{x_1}^2 - 1}{y_1} y_n,$$

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

Dobivamo konačno rješenje Pellove jednadžbe $x^2 - ky^2 = 1$ nizom (x_1, y_1), (x_2, y_2),...,(x_n, y_n), (x_{n+1}, y_{n+1}),...

Primjer 2.4.2. *Riješiti Pellovu jednadžbu $x^2 - 5y^2 = 1$ koristeći gore navedenu metodu.*

Rješenje

Fundamentalno rješenje dane jednadžbe je $x_1 = 9$, $y_1 = 4$.
Unimodularna transformacija za danu jednadžbu izgleda:

$$x_{n+1} = 9x_n + 20y_n,$$

$$y_{n+1} = 4x_n + 9y_n,$$

s matricom

$$M = \begin{bmatrix} 9 & 20 \\ 4 & 9 \end{bmatrix},$$

pa su rješenja:

$$(9, 4), (161, 72), (2889, 1292), (51841, 23184), ...$$

Poglavlje 3

Arhimedov problem stoke

3.1 O Arhimedovom problemu stoke

Zanimljiv primjer Pellove jednadžbe nam donosi Arhimedov problem stoke (*The cattle problem*). Rukopis u kom je sadržan ovaj problem je otkrio zaposelnik čuvene Herzogove biblioteke u Wolfenbuttelu, Gotthod E. Lessing(1729.-1781.)
Navodimo hrvatski prijevod autora Tome Maretića, a problem glasi:

> Ako si marljiv i mudar, stranče, izračunaj broj Sunčevih goveda što su nekoć pasla na poljima Trinakije na otoku Siciliji, podijeljenih u četiri s tada 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 pridodat i 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, strančе, riješiti sve ovo, završit ćeš okrunjen slavom i smatrat će te nenadmašnim u mudrosti.

Napisan u formi epigrama u 44 retka, ovdje u slobodnom prijevodu, napisan je Arhimedov problem stoke. Epigram je korišten kao javna ili prigodna poruka, no isti oblik su nerijetko imale i rugalice. Ovaj epigram je nastao kao svojevrstan Arhimedov odgovor na zanovijetanja Apolonija iz Perga (262.-190. g. pr. Kr.) koji je podbadao Arhimeda kako je sklon matematičkim problemima za čija rješenja je potrebno naporno i dugotrajno računanje. Potaknut time, Arhimed osmišljava ovaj zahtjevan problem te ga upućuje Erastotenu iz Kirene (275.-195. g. pr. Kr.). Krenimo sada na rješavanje problema.

Stado, odnosno karakteristike životinja, označimo varijablama. Imamo krave i bikove bijele, crne ili žute boje, a neki su i šareni. Također, postoje i određene veze između broja istih pa krenimo redom:
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.

Veze, odnosno uvjeti zadatka su:

$$B = (\frac{1}{2} + \frac{1}{3}) \cdot C + Z$$

$$C = (\frac{1}{4} + \frac{1}{5}) \cdot S + Z$$

$$S = (\frac{1}{6} + \frac{1}{7}) \cdot B + Z$$

$$b = (\frac{1}{3} + \frac{1}{4}) \cdot (C + c)$$

$$c = (\frac{1}{4} + \frac{1}{5}) \cdot (S + s)$$
$$s = (\frac{1}{5} + \frac{1}{6}) \cdot (Z + z)$$
$$z = (\frac{1}{6} + \frac{1}{7}) \cdot (B + b)$$

Postavljena su još dva uvjeta u tekstu:

$B + C$ je potpuni kvadrat,

$Z + S$ je broj oblika $\frac{n(n+1)}{2}$.

Dakle, imamo 8 nepoznanica u 7 jednadžbi koje čine homogeni linearni sustav. Možemo ga računati suvremenim softverskim alatom poput *Mathematica*, no rješavamo li sustav klasično, imamo:

Množimo redom jednadžbe, prvu s 336, drugu s 280, treću s 126:

$$336B = 280C + 336Z$$
$$280C = 126S + 280Z$$
$$126S = 39B + 126Z$$

Zbrojimo li jednadžbe, dobivamo:

$$297B = 742Z$$

tj, $3^3 \cdot 11B = 2 \cdot 7 \cdot 53Z$. Napravimo li isto s ostalima, dobivamo:

$$3^4 \cdot 11S = 2^2 \cdot 5 \cdot 79Z$$
$$3^2 \cdot 11C = 2 \cdot 89Z$$

Radimo li isto sa sljedeće četiri jednadžbe, množeći s brojevima, redom, 4800, 2800, 1260 i 462:

$$3^3 \cdot 11 \cdot 4657b = 2^3 \cdot 5 \cdot 7 \cdot 23 \cdot 373Z$$
$$3^2 \cdot 11 \cdot 4657z = 13 \cdot 46489Z$$
$$3^3 \cdot 4657s = 2^2 \cdot 5 \cdot 7 \cdot 761Z$$
$$3^2 \cdot 11 \cdot 4657c = 2 \cdot 17 \cdot 15991Z$$

Rješenja su cijeli brojevi pa shodno tome Z mora biti djeljiv s $3^4 \cdot 11 \cdot 4657$, što znači da to možemo zapisati kao:

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

ostala opća rješenja zapisujemo kao:

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

pri čemu je $k \in \mathbb{N}$. Zbrojimo li svu stoku, ukupan broj je $50389082 \cdot k$ komada.
Ograničenje ovog prvog dijela računanja je red veličine brojeva, a ograničenje drugog dijela problema je jednostavni slučaj Pellove jednadžbe. Prvo imamo jednadžbu iz uvjeta da je $C + B$ potpuni kvadrat pa koristeći vrijednosti iznad imamo:

$$C + B = 7460514k + 10366482k = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657k.$$

Prema tome, supstituirat ćemo $k = 3 \cdot 11 \cdot 29 \cdot 4657y^2$ za neki cijeli broj y. To će nam dati rješenje prvog uvjeta. Pogledajmo sada drugu jednadžbu koja nije bila iz skupa linearnih jednadžbi:

$$Z + S = \frac{n(n+1)}{2}.$$

Pa imamo

$$n = \frac{-1 \pm \sqrt{1 + 8(Z + S)}}{2}$$

Supstituiramo sada $Z + S$ i k brojem y tako da je diskriminanta ove kvadratne jednadžbe potpuni kvadrat x^2 što sa sobom sada povlači Pellovu jednadžbu

$$x^2 - 8 \cdot 2471 \cdot 957 \cdot 4657^2 y^2 = 1. \tag{3.1}$$

3.2 Veza Arhimedovog problema i Pellove jednadžbe

Za riješiti jednadžbu 3.1 oblika

$$x^2 - Cy^2 = 1$$

gdje je $C = 410286423278424 = 8 \cdot 2471 \cdot 957 \cdot 4657^2 = 2 \cdot 2471 \cdot 957 \cdot (2 \cdot 2471)^2 = 4729494 \cdot (2942)^2$ koristit ćemo se metodom verižnih razlomaka. Rješavat ćemo jednadžbu u dva dijela. U prvom dijelu ćemo rješavati Pellovu jednadžbu $x^2 - C'y^2 = 1$ gdje je $C' = 4729494$, a u drugom dijelu rješenja ćemo pronaći one y iz prvog dijela koji su djeljivi sa 2942.

Pellova jednadžba i verižni razlomci

Ono što sada trebamo je razvoj broja $\sqrt{C'} = \sqrt{4729494}$, što je 2174.7399844579, u jednostavni verižni razlomak.
Ovako to izračunavamo:

$$\begin{aligned}
2174.7399844579 &= 2174 + 1/1.35137973413856\\
1.35137973413856 &= 1 + 1/2.84592394735536\\
2.84592394735536 &= 1 + 1/1.18213936740570\\
1.1821393674057 &= 1 + 1/5.49030126898696\\
5.4903012689870 &= 5 + 1/2.03956233290230\\
2.0395623329023 &= 2 + 1/25.2765805450719\\
25.276580545072 &= 25 + 1/3.61574659004589\\
3.6157465900460 &= 3 + 1/1.62404472256270\\
1.6240447225627 &= 1 + 1/1.60244925378649\\
1.6024492537865 &= 1 + 1/1.65989084344423\\
1.6598908434442 &= 1 + 1/1.51540214557397\\
1.5154021455740 &= 1 + 1/1.94023251278156\\
1.9402325127816 &= 1 + 1/1.06356670972973\\
1.0635667097297 &= 1 + 1/15.7315048120601\\
15.731504812060 &= 15 + 1/1.36704500573790
\end{aligned}$$

Prema tome,

$$\begin{aligned}\sqrt{4729494} = [2174,&\overline{1,2,1,5,2,25,3,1,1,1,1,1,1,15,1,2,16,1,2,1,1,8,6,1,21,}\\&\overline{1,1,3,1,1,1,2,2,6,1,1,5,1,17,1,1,47,3,1,1,6,1,1,3,47,1,}\\&\overline{1,17,1,5,1,1,6,2,2,1,1,1,3,1,1,21,1,6,8,1,1,2,1,16,2,1,}\\&\overline{15,1,1,1,1,1,1,3,25,2,5,1,2,1,4348}]\end{aligned}$$

Idemo sada izračunati prvih par aproksimacija od $\sqrt{C}$.

	x	**y**
	0	1
	1	0
2174	2174	1
1	2175	1
2	6524	3
1	8699	4
5	50019	23

Najmanje rješenje Pellove jednadžbe $x^2 - Cy^2 = 1$ će biti ono u redu gdje je $x = 81022113$, a $y = 4$ što nam daje jednadžbu

$$81022113^2 - 410286423278424 \cdot 4^2 = 1.$$

Opće rješenje ovog problema dao je njemački matematičar A. Amthor još 1880. godine. Pokazao je da je rezultat približno jednak $7.76 \cdot 10^{206544}$ i da su prve četiri njegove znamenke 7760. Kroz sljedeća dva desetljeća matematičari E. Fish, G. H. Richards i A. H. Bell (članovi skupine *The Hillsboro Mathematical Club*) su izračunali prvih 31 i posljednjih 12 znamenki rješenja. Kako čitavo rješenje ima 206545 znamenki, čitavo računanje bez upotrebe računala je bilo složeno. O tome govori članak iz *New York Timesa* iz 1931. godine u kom stoji: *Budući da bi izračun zahtijevao tisuću ljudi i tisuću godina, jasno je da svijet nikad neće dočekati cjelokupno rješenje*. No, pojavom računala, već 1965. godine, za vrijeme od 7 sati i 49 minuta, matematičari H. C. Williams, R. A. German i C. R. Zarnke dobili rezultat na računalu IBM 7040. Koliko tehnika ide naprijed svjedoči i rezultat Harryja L. Nelsona iz 1981.godine koji je provjeru prethodnog rezultata provjerio i ispisao na računalu Cray-1 za desetak minuta, a broj od 206 545 znamenki je ispisan na 47 listova papira.

Bibliografija

[1] Branimir Dakić, *Arhimedov problem stoke*, Matematika i kola **51** (2009), 34–37.

[2] Andrej Dujella, *Uvod u teoriju brojeva*, PMF-Matematicki odjel, Zagreb, skripta (2006).

[3] ______, *Diofantske jednadžbe*, (2007).

[4] Alan Filipin, *Linearne forme u logaritmima i diofantska analiza*, (2010).

[5] Hendrik W Lenstra Jr, *Solving the Pell equation*, Notices of the AMS **49** (2002), br. 2, 182–192.

[6] Ivan Matić, *Uvod u teoriju brojeva*.

[7] Nina Mikolaj, *Pellova jednadžba i Pitagorine trojke*, (2008).

[8] Zahid Raza i Hafsa Masood Malik, *Solution of Certain Pell Equations*, arXiv preprint arXiv:1402.5206 (2014).

[9] Željko Zrno, *Some reviews on the Pell equation*, Osječki matematički list **12** (2013), br. 2, 127–137.

Sažetak

U ovom diplomskom radu, glavnu ulogu je imao Pell, odnosno njegove jednadžbe. Cilj rada je bio definirati i dati efikasne načine rješavanja Pellovih jednadžbi. Na samom početku rada su navedeni neki važniji rezultati koji se tiču diofantskih jednadžbi jer je Pellova jednadžba zapravo specijalan slučaj diofantske jednadžbe. Nadalje, dane su definicije Pellove i pellovske jednadžbe, kao i teoremi koji daju nužne i dovoljne uvjete za egzistenciju i strukturu tih rješenja. Kroz drugo poglavlje su opisane metode kojima se određuju rješenja tih jednadžbi, dok je u trećem poglavlju opisan takozvani Arhimedov problem stoke, te je dana veza tog problema s Pellovim jednadžbama.

Summary

In this thesis, the main role had Pell, in fact his equations. The aim of the study was to define and provide efficient ways of solving Pell's equations. At the very beginning of this thesis are some important results concerning diophantine equations because Pell's equation is a special case of diophantine equation. Further,there are also definitions of Pell's and generalized Pell equations as well as theorems which are giving necessary and sufficient conditions for existence and structure of such solutions. The second chapter describes methods for determining solutions of these equations,while the third chapter describes the so-called Archimede's cattle problem and finds connection between that problem and Pell's equation.

Životopis

Rođena sam u Dubrovniku 1988. godine odakle se selim, tokom Domovinskog rata, u Kaštela gdje 2002. godine završavam osnovnu školu, a potom upisujem Srednju školu *Braća Radić*, smjer opća gimnazija. Maturirala sam na temu *Povijest Kaštela na prijelazu iz XIX. u XX. stoljeće* 2006. godine s odličnim uspjehom. Iste godine sam upisala Preddiplomski sveučilišni studij matematike na *Prirodoslovno-matematičkom fakultetu u Zagrebu*, godinu nakon upisujem na istom fakultetu nastavnički smjer. Godine 2011. nastavljam studij upisom Diplomskog sveučilišnog studija *Računarstvo i matematika*, a 2014. upisujem i razlikovnu skupinu predmeta za nastavnički profil na *Prirodoslovno-matematičkom fakultetu u Splitu*. Od 2015. radim kao profesorica matematike u *Turističkoj i ugostiteljskoj školi Dubrovnik*.