# Pellova jednadžba

**Balog, Karla**

**Master's thesis / Diplomski rad**

**2023**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:126:617315

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
Smjer: Financijska matematika i statistika

**Karla Balog**

# Pellova jednadžba

Diplomski rad

Osijek, 2023.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike
Smjer: Financijska matematika i statistika

**Karla Balog**

# Pellova jednadžba

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Soldo

Osijek, 2023.

# Sadržaj

# Uvod

Pellova jednadžba jedna je od najstarijih i najvažnijih oblika diofantski jednadžbi drugog reda čijim se proučavanjem bave matematičari diljem svijeta već više od 2 tisuće godina. Ta jednadžba, oblika

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

gdje je $d$ prirodan broj različit od potpunog kvadrata, naziv je dobila, nezasluženo, po engleskom matematičaru Johnu Pellu za kojeg je Euler smatrao da je bio prvi koji je promatrao njezina netrivijalna rješenja. Ako je $d$ potpun kvadrat, onda se lako pokaže da ta Pellova jednadžba ima samo trivijalna rješenja $(x, y) \in \{(-1, 0), (1, 0)\}$. Prva spominjanja te jednadžbe sežu još u doba antičke grčke kada su starogrčki matematičari pomoću jednadžbe $x^2 - 2y^2 = 1$ aproksimirali broj $\sqrt{2}$ brojem $\frac{x}{y}$. Osim njih, proučavanjem jednadžbi ovakvog oblika bavili su se i indijski matematičari Brahmagupta i Bhaskara II te razni europski matematičari poput Fermata, Eulera i Lagrangea.

U prvom poglavlju ovoga rada ćemo navesti definiciju, neke osnovne rezultate te primjere linearnih i nelinearnih diofantskih jednadžbi. U drugom poglavlju najprije ćemo kratko proći kroz povijest jednadžbe $x^2 - dy^2 = k$, $k \in \mathbb{Z} \setminus \{0\}$ nakon čega ćemo proučiti Pellovu jednadžbu $x^2 - dy^2 = 1$, a zatim i pelovske jednadžbe $x^2 - dy^2 = -1$ te $x^2 - dy^2 = \pm 4$. Dat ćemo njihove definicije, uvjete egzistencije njihovih rješenja, opisati strukturu rješenja te sve potkrijepiti primjerima. U trećem i posljednjem poglavlju objasnit ćemo kako pomoću razvoja $\sqrt{d}$ u verižni razlomak i pomoću cikličke *Chakravala* metode pronaći rješenja ovakvih tipova diofantskih jednadžbi.

# 1 Linearne i neke nelinearne diofantske jednadžbe

Proučavanje diofantskih jednadžbi, nazvanih po grčkom matematičaru Diofantu iz Aleksandrije, ima dugu povijest koja seže još u antičko doba. Diofant je bio jedan od prvih matematičara koji je sustavno proučavao ove vrste jednadžbi. Najpoznatiji je po svom djelu *Arithmetica*, zbirci od 13 knjiga od kojih je sačuvano samo šest. U svojim je djelima Diofant uveo simbole, koji su zamijenili dotadašnji način pisanja algebarskih problema riječima. Osim toga, proučavao je algebarske jednadžbe i njihova racionalna rješenja te se on smatra ocem algebre.

Diofant je uvelike utjecao na druge svjetski poznate matematičare poput Vietea, Fermata i Eulera. Mnogi matematičari dali su značajan doprinos ovom području matematike kroz povijest, a proučavanje diofantskih jednadžbi i danas je aktivno područje istraživanja.

U iduća dva potpoglavlja navodimo definicije i neke osnovne pojmove vezane uz diofantske jednadžbe, a u ostatku rada usmjerit ćemo se na proučavanje specijalnog tipa diofantskih jednadžbi: Pellovu jednadžbu.

**Definicija 1.** *Diofantskom jednadžbom obično nazivamo polinomnu jednadžbu s dvije ili više nepoznanica čiji su koeficijenti i rješenja cijeli brojevi.*

Dijelimo ih u dvije skupine, linearne i nelinearne diofantske jednadžbe.

## 1.1 Linearne diofantske jednadžbe

U ovom dijelu rada navest ćemo definiciju linearne diofantske jednadžbe, njezina osnovna svojstva te proći kroz nekoliko primjera.

**Definicija 2.** *Linearne diofantske jednadžbe su jednadžbe oblika*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

*pri čemu su* $a_1, \ldots, a_n, b \in \mathbb{Z} \setminus \{0\}$, *a* $x_1, \ldots, x_n$ *nepoznanice.*

Radi jednostavnosti, najprije ćemo promotriti slučaj linearne diofantske jednadžbe s dvije nepoznanice, $x$ i $y$:

$$ax + by = c, \quad a, b, c \in \mathbb{Z}. \tag{1.1}$$

Jedno od najpoznatijih svojstava linearnih diofantskih jednadžbi ovakvog tipa je da uvijek imaju rješenje ako najveći zajednički djelitelj brojeva $a$ i $b$ dijeli $c$, o čemu

govori idući teorem. Njegov dokaz, kao i dokazi svih ostalih tvrdnji koje ćemo navesti u ovom poglavlju, mogu se pronaći u [1].

**Teorem 1** (vidjeti [1, Teorem 10.1]). *Neka su $a, b, c$ cijeli brojevi i $d$ najveći zajednički djelitelj od $a$ i $b$.*

(a) *Ako $d \nmid c$, onda jednadžba (1.1) nema cjelobrojnih rješenja.*

(b) *Ako $d \mid c$, onda jednadžba (1.1) ima beskonačno mnogo cjelobrojnih rješenja.*

(c) *Ako je $(x_1, y_1)$ jedno rješenje od (1.1), onda su sva rješenja dana s*

$$x = x_1 + \frac{b}{d} \cdot t, \quad y = y_1 - \frac{a}{d} \cdot t, \quad t \in \mathbb{Z}.$$

Postoji nekoliko načina za rješavanje linearnih diofantskih jednadžbi. Mi ćemo u idućem primjeru pokazati kako pronaći rješenje koristeći Euklidov algoritam.

**Primjer 1.** *Pronađimo sva cjelobrojna rješenja jednadžbe*

$$113x + 130y = 15.$$

*Znamo da rješenje postoji jer je $(113, 130) = 1$. Stoga primjenjujemo Euklidov algoritam na brojeve 113 i 130:*

$$\begin{aligned} 130 &= 1 \cdot 113 + 17 \\ 113 &= 17 \cdot 6 + 11 \\ 17 &= 11 \cdot 1 + 6 \\ 11 &= 6 \cdot 1 + 5 \\ 6 &= 1 \cdot 5 + 1 \\ 5 &= 1 \cdot 5. \end{aligned}$$

*Povratnim supstitucijama dobivamo:*

$$\begin{aligned} 1 &= 1 \cdot 6 - 1 \cdot 5 = 17 - 11 - (11 - 6) = 17 - 2 \cdot 11 + 17 - 11 \\ &= 2 \cdot 17 - 3 \cdot 11 = 2 \cdot (130 - 113) - 3 \cdot (113 - 17 \cdot 6) \\ &= 2 \cdot 130 - 2 \cdot 113 - 3 \cdot 113 + 3 \cdot 6 \cdot (130 - 113) \\ &= 2 \cdot 130 - 5 \cdot 113 + 18 \cdot 130 - 18 \cdot 113 \\ &= 20 \cdot 130 - 23 \cdot 113. \end{aligned}$$

*Sada posljednju jednakost,* $1 = 20 \cdot 130 - 23 \cdot 113$*, pomožimo sa 15 i dobivamo jedno rješenje početne jednadžbe:* $(x_0, y_0) = (-345, 300)$*. Prema tvrdnji* $(c)$ *Teorema 1, sva su njena rješenja dana s:*

$$x = -345 + 130t, \quad y = 300 - 113t, \quad t \in \mathbb{Z}.$$

Sljedeći teorem poopćenje je Teorema 1 na slučaj linearne diofantske jednadžbe s $n$ nepoznanica.

**Teorem 2** (vidjeti [1, Teorem 10.2])**.** *Neka su* $a_1, a_2, \ldots, a_n$ *cijeli brojevi različiti od nule. Tada linearna diofantska jednadžba*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{1.2}$$

*ima rješenja ako i samo ako* $(a_1, a_2, \ldots, a_n) \mid c$*. Nadalje, ako jednadžba (1.2) ima barem jedno rješenje, onda ih ima beskonačno mnogo.*

Pogledajmo primjenu ovog teorema na sljedećem primjeru.

**Primjer 2.** *Odredimo sva cjelobrojna rješenja linearne diofantske jednadžbe* $3x + 2y + 5z = 73$*. Najprije primjećujemo da vrijedi* $(3, 2, 5) = 1$*, što prema prethodnom teoremu znači da jednadžba ima rješenje. Primjer ćemo riješiti korištenjem modularne aritmetike. Djelujemo li na početnu jednadžbu, redom, modulo 2, a zatim modulo 3, dobivamo kongruencije:*

$$\begin{aligned} x + z &\equiv 1 \pmod 2 \\ -y + 2z &\equiv 1 \pmod 3, \end{aligned}$$

*što još možemo zapisati i u obliku*

$$\begin{aligned} x + z &= 1 + 2k, \quad k \in \mathbb{Z} \\ -y + 2z &= 1 + 3m, \quad m \in \mathbb{Z}. \end{aligned}$$

*Iz prethodne dvije jednakosti izrazimo* $x$ *i* $y$ *preko ostalih nepoznanica. Zatim to uvrstimo u početnu diofantsku jednadžbu i sređivanjem dobivamo:*

$$x = 1 + 2k - z \tag{1.3}$$

$$y = 2z - 1 - 3m \tag{1.4}$$

$$z = 12 - k + m. \tag{1.5}$$

*Uvrštavanjem (1.5) u (1.3) i (1.4) dobivamo sva cjelobrojna rješenja početne jednadžbe:*

$$(x, y, z) = (3k - m - 11, 23 - 2k - m, 12 - k + m), \quad k, m \in \mathbb{Z}.$$

## 1.2 Neke nelinearne diofantske jednadžbe

Najprije ćemo navesti definiciju nelinearnih diofantskih jednadžbi, a zatim kroz nekoliko primjera pokazati kako pronaći njezina cjelobrojna rješenja.

**Definicija 3.** *Nelinearne diofantske jednadžbe su jednadžbe s cjelobrojnim koeficijentima i nepoznanicama u članovima višeg reda, a kojima rješenja najčešće tražimo u skupu cijelih brojeva.*

Mogu se riješiti različitim metodama ili kombiniranjem više metoda istovremeno. Prvi korak u rješavanju je zapisati jednadžbu u odgovarajući oblik kako bi se pronašla odgovarajuća metoda. Pogledajmo kako to funkcionira na sljedećem primjeru.

**Primjer 3.** *Pronađimo sva cjelobrojna rješenja $x$ i $y$ kvadratne diofantske jednadžbe*

$$x^2 + 3x + 9 = 9y^2.$$

*Prvi korak u rješavanju je prebacivanje cijelog izraza na lijevu stranu pri čemu ćemo $x$ promatrati kao nepoznanicu, a $y$ kao konstantu:*

$$x^2 + 3x + 9 - 9y^2 = 0.$$

*Pomoću formule za rješenje kvadratne jednadžbe dobivamo*

$$\begin{aligned} x_{1,2} &= \frac{-3 \pm \sqrt{9 - 4(9 - 9y^2)}}{2} = \frac{-3 \pm \sqrt{9 - 36 - 36y^2)}}{2} \\ &= \frac{-3 \pm \sqrt{36y^2 - 27)}}{2} = \frac{-3 \pm 3\sqrt{4y^2 - 3}}{2}. \end{aligned}$$

*S obzirom da tražimo cjelobrojna rješenja, trebamo osigurati da i $\sqrt{4y^2 - 3}$ bude cijeli broj, što znači da $4y^2 - 3$ treba biti potpun kvadrat, odnosno:*

$$\begin{aligned} 4y^2 - 3 &= k^2 \\ 4y^2 - k^2 &= 3 \\ (2y + k)(2y - k) &= 3. \end{aligned}$$

*Kako su $i$ $y$ $i$ $k$ cijeli brojevi, imamo sljedeća 4 slučaja:*

$$\begin{aligned} 2y+k=3 \quad i \quad 2y-k=1 \quad &\Longrightarrow \quad y=1 \\ 2y+k=1 \quad i \quad 2y-k=3 \quad &\Longrightarrow \quad y=1 \\ 2y+k=-3 \quad i \quad 2y-k=-1 \quad &\Longrightarrow \quad y=-1 \\ 2y+k=-1 \quad i \quad 2y-k=-3 \quad &\Longrightarrow \quad y=-1. \end{aligned}$$

*Uočimo da nam nije važno koliko $k$ iznosi jer možemo $y$ direktno uvrstiti u početnu jednadžbu i dobiti $x$:*

$$\begin{aligned} y=-1 \quad &\Longrightarrow \quad x^2+3x=0 \quad \Longrightarrow \quad x_1=0, x_2=-3 \\ y=1 \quad &\Longrightarrow \quad x^2+3x=0 \quad \Longrightarrow \quad x_1=0, x_2=-3. \end{aligned}$$

*Dakle, sva cjelobrojna rješenja početne jednadžbe dana su s:*

$$(x,y) \in \{(0,-1),(-3,-1),(0,1),(-3,1)\}.$$

Metoda koju smo koristili u prethodnom primjeru zove se *metoda faktorizacije*. Slična ovoj metodi je *metoda kvocijenta* u kojoj se jedna strana jednadžbe zapisuje u obliku kvocijenta dvaju cjelobrojnih vrijednosti, dok je s druge strane također cjelobrojna vrijednost pa opet promatramo moguće slučajeve. Osim ove dvije metode, postoje još i *metoda zbroja*, *metoda parnosti* i druge. Pogledajmo kako bi se primjenom *metode zbroja* riješila nelinearna diofantska jednadžba iz sljedećeg primjera.

**Primjer 4.** *Odredimo cijele brojeve $x$ i $y$ za koje vrijedi*

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

*Najprije nepoznanice prebacujemo na lijevu stranu i sređujemo izraz:*

$$\begin{aligned} x^2-2x+y^2-2y &= 0 \\ x^2-2x+y^2-2y+2 &= 2 \\ (x-1)^2+(y-1)^2 &= 2. \end{aligned}$$

*Jedini način da se broj 2 napiše kao suma kvadrata dvaju cijelih brojeva je kao suma dvaju jedinica pa slijedi da je*

$$(x-1)^2=1,\ (y-1)^2=1 \quad \Longrightarrow \quad x-1=\pm 1,\ y-1=\pm 1.$$

*Sada dobivamo da su $x$ i $y$ jednaki 0 ili 2, tj. sva rješenja u cijelim brojevima početne jednadžbe dana su s*

$$(x,y) \in \{(0,0),(0,2),(2,0),(2,2)\}.$$

Najvažniji tip jednadžbe iz skupine nelinearnih diofantskih jednadžbi je Pellova jednadžba s kojom ćemo se detaljnije baviti u nastavku ovoga rada.

# 2 Pellova i neke pelovske jednadžbe

Kada govorimo o Pellovoj jednadžbi mislimo na jednadžbu oblika

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

pri čemu je $d$ prirodan broj različit od potpunog kvadrata. Slučaj kada je $d$ potpun kvadrat ne promatramo jer tada dobivamo trivijalna rješenja te jednadžbe, $(x, y) = (-1, 0)$ i $(x, y) = (1, 0)$. Fundamentalnim rješenjem jednadžbe zovemo njezino najmanje rješenje $(x_1, y_1)$ u prirodnim brojevima, a preciznije će biti definirano u Poglavlju 2.1. Jednadžbe oblika

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

gdje je $d$ prirodan broj različit od potpunog kvadrata, a $k$ cijeli broj različit od 0 i 1 zovemo *pelovskim jednadžbama.* Osim Pellove jednadžbe (2.1), u radu ćemo se također baviti i pelovskim jednadžbama $x^2 - dy^2 = -1$ te $x^2 - dy^2 = \pm 4$.

Istina je da je jednadžba (2.1) dobila naziv po engleskom matematičaru Johnu Pellu koji je živio u 17. stoljeću, ali početci proučavanja ove jednadžbe sežu još do antičke grčke, otprilike 250 godina pr. Kr., kada se njome bavio Arhimed. Najpoznatiji primjer Pellove jednadžbe veže se uz Arhimedov problem stoke, koji je originalno zapisan u obliku epigrama od 44 retka, a nastao je kao odgovor na zanovijetanja Apolonija iz Perga na činjenicu da je Arhimed volio matematičke probleme čije rješavanje zahtijeva dugotrajna računanja. U problemu stoke u središtu pozornosti nalaze se krave i bikovi, svaki od njih raspoređen u četiri grupe po bojama. Cilj je izračunati ukupan broj stoke uz određene uvjete. Rješavanje problema svodi se na rješavanje homogenog lineranog sustava od sedam jednadžbi s osam nepoznanica, a sređivanjem tog sustava dobije se Pellova jednadžba

$$x^2 - 4729494y^2 = 1. \tag{2.3}$$

U današnje vrijeme rješenje ovog problema nije toliko kompliciranо pronaći, pogotovo korištenjem računala. S obzirom da fundamentalno rješenje jednadžbe (2.3) iznosi

$$x = 109931986732829734979866232821433543901088049,$$
$$y = 50549485234315033074477819735540408863 40$$

nije poznato je li ga Arhimed uopće znao izračunati. Prvo rješenje dao je 1880. godine njemački matematičar A. Amthor. Nije uspio odrediti sve znamenke rješenja i time ga potpuno odrediti, ali je dao djelomično rješenje pokazavši da se ono sastoji od 206 545 znamenki te da počinje sa brojevima 7760. Između 1889. i 1893. godine, tri člana matematičkog kluba *The Hillsboro Mathematical Club* (Edmund Fish, Geo. H. Richards, and A. H. Bell) izračunali su prvih 31 i posljednjih 13 znamenki rješenja. 1965. godine prvo potpuno rješenje izračunali su na računalu IBM 7040 matematičari H. C. Williams, R. A. German i C.R. Zarnke. Računalu je trebalo 7 sati i 49 minuta da izračuna rješenje. 1981. godine, Harry L. Nelson je na računalu Cray 1, kojemu je za izračun trebalo otprilike 10 minuta, izračunao ne samo najmanje, nego i dodatnih 5 rješenja, pri čemu se najveće rješenje sastoji od više od milijun znamenaka.

Osim Arhimeda, približno 1000 godina prije nego što se Pellova jednadžba počela proučavati u Europi, indijski matematičari Brahmagupta i Bhaskara II bavili su se jednadžbama oblika (2.2). Oni su otkrili metodu rješavanja jednadžbi ovog oblika, *Chakravala* metodu, pomoću koje su pronalazili rješenja spomenutih jednadžbi za $k = \pm 1, \pm 2, \pm 4$.

Pellovu jednadžbu su tek u 17. stoljeću počeli proučavati matematičari u Europi, ali njima nije bila poznata prethodno otkrivena ciklička metoda pronalaženja rješenja. Pierre de Fermat prvi je postavio izazov svim europskim matematičarima da pronađu dokaz sljedeće tvrdnje:

> *Za svaki (pozitivan) broj d različit od potpunog kvadrata postoji beskonačan broj kvadrata takvih da taj kvadrat pomnožen s d i zbrojen s jedinicom daje potpun kvadrat.* [1]

Osim toga, zatražio je i rješenja za neke određene $d$. Nekoliko je matematičara, uključujući de Bessyja, Brounckera i Wallisa, sudjelovalo u tom izazovu. Brouncker je pronašao metodu rješavanja jednadžbe koju je postavio Fermat, sličnu metodi verižnih razlomaka, ali ju nije uspio dokazati. Nedugo nakon toga, švicarski matematičar Rahn objavio je knjigu iz algebre koja je sadržavala primjer Pellove jednadžbe. Knjiga je napisana uz Pellovu pomoć, ali je to jedina poznata veza između Pella i Pellove jednadžbe. Leonard Euler je bio taj koji je greškom proglasio kako je Pell bio prvi koji je proučavao netrivijalna rješenja jednadžbe. U 18. stoljeću je Joseph-Louis Lagrange dokazao vezu između verižnih razlomaka i pronalaženja rješenja Pellove jednadžbe.

[1] slobodni prijevod s engleskog jezika, vidjeti [2]

Kroz povijest, pa i danas, Pellova jednadžba ima široke primjene - koristi se u teoriji brojeva, kriptografiji, geometriji, fizici, inženjerstvu i slično.

## 2.1 Pellova jednadžba

Poglavlje započinjemo navođenjem potpune definicije Pellove jednadžbe, a zatim ćemo pokazati da njezino rješenje uvijek postoji te kakva je njegova struktura.

**Definicija 4.** *Nelinearna diofantska jednadžba oblika*

$$x^2 - dy^2 = 1, \tag{2.4}$$

*gdje je $d$ prirodan broj različit od potpunog kvadrata, zove se Pellova jednadžba.*

Slučaj kada je $d$ potpuni kvadrat ne promatramo jer tada dobivamo trivijalna rješenja u cijelim brojevima:

$$\begin{aligned} d = k^2 \quad &\Longrightarrow \quad x^2 - k^2y^2 = (x + ky)(x - ky) = 1 \\ &\Longrightarrow \quad x + ky = x - ky = 1 \text{ ili } x + ky = x - ky = -1 \\ &\Longrightarrow \quad (x, y) \in \{(-1, 0), (1, 0)\}. \end{aligned}$$

Kada bi dopustili $x = 0$, cjelobrojnih rješenja ne bismo imali osim u slučaju $d = -1$ (dobili bismo $y = \pm 1$, što su opet trivijalna rješenja). Ovo je također jedini slučaj u kojem rješenja postoje za $d < 0$.

**Napomena 1.** *Za rješenja Pellove jednadžbe uvijek uzimamo prirodne brojeve jer ako je $(x_1, y_1)$ jedno rješenje, onda su to i $(x_1, -y_1), (-x_1, y_1)$ te $(-x_1, -y_1)$.*

Problem rješavanja Pellove jednadžbe može se svesti na problem aproksimacije broja $\sqrt{d}$ nekim racionalnim brojem. Općenito za neki racionalan broj $\frac{a}{b}$ kažemo da je dobra aproksimacija iracionalnog broja $\alpha$ ako vrijedi

$$\left|\alpha - \frac{a}{b}\right| = min\left\{\left|\alpha - \frac{u}{v}\right| : u, v \in \mathbb{Z}, 0 < v \leq b\right\}.$$

Ako je $\sqrt{d}$ iracionalan broj i $\frac{a}{b}$ aproksimacija od $\sqrt{d}$, tada je $\frac{a^2}{b^2}$ aproksimacija od $d$. Pretpostavimo da imamo:

$$\frac{a^2}{b^2} - d = \frac{c}{b^2} \neq 0$$

Množenjem s $b^2$ dobivamo

$$a^2 - db^2 = c \neq 0$$

Ono što znamo je da, ako želimo da $\frac{a}{b}$ bude u nekom smislu dobra aproksimacija od $d$, tada $c$ treba biti mali broj. Posebno, ako je $c = 1$, imamo Pellovu jednadžbu te je $\frac{a}{b}$ dobra aproksimacija od $\sqrt{d}$. Kasnije ćemo ovo malo bolje objasniti kroz primjenu verižnih razlomaka u procjeni od $\sqrt{d}$.

Kako bismo dokazali egzistenciju rješenja jednadžbe $x^2 - dy^2 = 1$ potrebne su nam sljedeće leme:

**Lema 1** (vidjeti [1, Korolar 8.2]). *Za svaki iracionalan broj $\alpha$ postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je*

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

**Lema 2** (vidjeti [1, Lema 10.9]). *Ako je $d$ prirodan broj različit od potpunog kvadrata, tada postoji $k \in \mathbb{Z}$, $0 < |k| < 1 + 2\sqrt{d}$ i beskonačno mnogo parova $(x, y) \in \mathbb{N}^2$ koji zadovoljavaju jednakost*

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

*Dokaz.* Kako je $d$ različit od potpunog kvadrata, odnosno $\sqrt{d}$ iracionalan, prema Lemi 1 postoji beskonačno mnogo racionalnih brojeva $(x, y)$ takvih da je

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

Nadalje, vrijedi

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

Stoga je

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

S obzirom da postoji beskonačno mnogo parova $(x, y)$ s prethodnim svojstvom i konačno mnogo cijelih brojeva koji su po apsolutnoj vrijednosti manji od $1 + 2\sqrt{d}$, to znači da postoji $k \in \mathbb{Z}$ takav da je $|k| < 1 + 2\sqrt{d}$ i za koji jednadžba $x^2 - dy^2 = k$ ima beskonačno mnogo rješenja. S obzirom na pretpostavku da je $d$ različit od potpunog kvadrata, tada ne može biti ni $k = 0$.

□

Sada možemo dokazati egzistenciju rješenja Pellove jednadžbe $x^2 - dy^2 = 1$.

**Teorem 3** (vidjeti [1, Teorem 10.10]). *Ako je $d$ prirodan broj različit od potpunog kvadrata, tada postoji barem jedan par $(x, y) \in \mathbb{N}^2$ koji zadovoljava Pellovu jednadžbu $x^2 - dy^2 = 1$.*

*Dokaz.* Prema Lemi 2, jednadžba $x^2 - dy^2 = k$ ima beskonačno mnogo rješenja koja možemo podijeliti u klase, pri čemu su $(x_1, y_1)$ i $(x_2, y_2)$ u istoj klasi ako i samo ako je $x_1 \equiv x_2 \pmod{k}$ i $y_1 \equiv y_2 \pmod{k}$. Tada barem jedna od tih klasa sadrži barem dva različita rješenja $(x_1, y_1)$ i $(x_2, y_2)$ takva da je:

$$x_1^2 - dy_1^2 = k \quad \text{i} \quad x_2^2 - dy_2^2 = k, \quad x_i, y_i > 0, i = 1, 2.$$

Sada podijelimo $x_1 + y_1\sqrt{d}$ s $x_2 + y_2\sqrt{d}$ i racionaliziramo te dobivamo

$$\frac{x_1 + y_1\sqrt{d}}{x_2 + y_2\sqrt{d}} \cdot \frac{x_2 - y_2\sqrt{d}}{x_2 - y_2\sqrt{d}} = \frac{x_1x_2 - y_1y_2d}{k} - \sqrt{d}\left(\frac{x_1y_2 - x_2y_1}{k}\right),$$

pri čemu je $k = x_1^2 - dy_1^2$. Definiramo $x$ i $y$ kao:

$$x = \frac{x_1x_2 - y_1y_2d}{k} \quad \text{i} \quad y = \frac{x_1y_2 - x_2y_1}{k}. \tag{2.5}$$

Ono što sada trebamo napraviti je pokazati da su ovako definirani $x$ i $y$ rješenja jednadžbe $x^2 - dy^2 = 1$, a to radimo u dva koraka: dokazujemo da su $x$ i $y$ cijeli brojevi te da zadovoljavaju jednadžbu $x^2 - dy^2 = 1$. Ako bismo dopustili $y = 0$, tj. $x_1y_2 = x_2y_1$, tada bismo imali:

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

iz čega slijedi $x_1^2 = x_2^2$, što je kontradikcija s pretpostavkom da su $x_1$ i $x_2$ različiti prirodni brojevi. Nadalje pretpostavljamo da je $y \neq 0$. Znamo da vrijedi:

$$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv k \equiv 0 \pmod{k}$$
$$x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{k}$$

pa zaključujemo da su $x$ i $y$ zaista cijeli brojevi. Naposljetku treba dokazati da oni zadovoljavaju Pellovu jednadžbu, a to lako radimo direktnom provjerom:

$$\begin{aligned} x^2 - dy^2 &= \left(\frac{x_1x_2 - dy_1y_2}{k}\right)^2 - d\left(\frac{x_1y_2 - x_2y_1}{k}\right)^2 \\ &= \frac{1}{k^2}\left[x_1^2x_2^2 - 2dx_1x_2y_1y_2 + y_1^2y_2^2d^2 - d(x_1^2y_2^2 - 2x_1x_2y_1y_2 + x_2^2y_1^2)\right] \\ &= \frac{1}{k^2}\left[x_1^2(x_2^2 - dy_2^2) - y_1^2d(x_2^2 - dy_2^2)\right] \\ &= \frac{1}{k^2}(x_1^2 - y_1^2d)(x_2^2 - dy_2^2) = \frac{1}{k^2} \cdot k \cdot k = 1. \end{aligned}$$

□

Preostalo nam je još pokazati strukturu rješenja Pellove jednadžbe $x^2 - dy^2 = 1$. Za neke $d$ je poprilično jednostavno pronaći rješenje. Primjerice, jedno cjelobrojno rješenje jednadžbe $x^2 - 2y^2 = 1$ je očito $(x, y) = (3, 2)$ te je ono i njezino najmanje rješenje u prirodnim brojevima. Takva rješenja imaju poseban naziv, a u ostatku poglavlja ćemo se detaljnije njima pozabaviti.

**Definicija 5.** *Ako sa* $S = \{(x_n, y_n) \ : \ x_n, y_n \in \mathbb{N}\}$ *označimo skup svih rješenja Pellove jednadžbe, tada njezinim fundamentalnim rješenjem nazivamo uređeni par* $(x_1, y_1)$, $x_1 = min\{x_n \ : \ x_n \in \mathbb{N}\}$, $y_1 = min\{y_n \ : \ y_n \in \mathbb{N}\}$ *koji zadovoljava (2.4). Fundamentalno rješenje često zapisujemo i kao* $x_1 + y_1\sqrt{d}$.

Fundamentalno rješenje se s razlogom tako i zove - pomoću njega možemo zapisati i sva ostala prirodna rješenja o čemu govori idući teorem.

**Teorem 4** (vidjeti [1, Teorem 10.11])**.** *Pellova jednadžba (2.4) ima beskonačno mnogo rješenja, a ako je* $(x_1, y_1) \in \mathbb{N}^2$ *njezino fundamentalno rješenje, onda su sva rješenja u prirodnim brojevima dana s*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}. \tag{2.6}$$

*Dokaz.* Najprije dokazujemo da jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Znamo da iz $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ slijedi da je $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ pa množenjem ta dva izraza dobivamo:

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

iz čega zaključujemo da $x_n + y_n\sqrt{d}$ jest rješenje te da ih ima beskonačno mnogo. Dokaz drugog dijela tvrdnje je malo kompliciraniji. Kako bismo dokazali da su rješenja oblika (2.6), pretpostavit ćemo suprotno - da postoji rješenje $(u, v) \in \mathbb{N}^2$ koje nije oblika kao $(x_n, y_n), n \in \mathbb{N}$. Iz pretpostavke da su $(x_n, y_n), (u, v) \in \mathbb{N}^2$ vrijedi

$$x_1 + y_1\sqrt{d} > 1 \quad \text{i} \quad u + v\sqrt{d} > 1$$

pa onda postoji $m \in \mathbb{N}$ takav da je

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

Množenjem prethodnog izraza sa $(x_1 + y_1\sqrt{d})^{-m} = (x_1 - y_1\sqrt{d})^m$ slijedi

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

Sada, ako uzmemo $a, b \in \mathbb{Z}$ i definiramo

$$a + b\sqrt{d} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^m$$
$$a - b\sqrt{d} = (u - v\sqrt{d})(x_1 + y_1\sqrt{d})^m,$$

množenjem ta dva izraza dobivamo

$$a^2 - db^2 = (u^2 - dv^2)(x_1^2 - dy_1^2)^m = 1.$$

Kako je $a + b\sqrt{d} > 1$, imamo

$$0 < a - b\sqrt{d} < 1 \quad \Longrightarrow \quad a > 0 \text{ i } b > 0, \text{ tj. } a, b \in \mathbb{N}.$$

Iz prethodnog zaključujemo kako je $a + b\sqrt{d}$ rješenje u prirodnim brojevima Pellove jednadžbe $x^2 - dy^2 = 1$, ali i da je $a + b\sqrt{d} < x_1 + y_1\sqrt{d}$ što je kontradikcija s pretpostavkom da je $(x_1, y_1)$ fundamentalno rješenje. Dakle, početna pretpostavka je točna: sva rješenja u prirodnim brojevima Pellove jednadžbe $x^2 - dy^2 = 1$ dana su s (2.6). □

Više riječi o pronalasku fundamentalnog rješenja bit će u posljednjem poglavlju ovoga rada, u idućem će primjeru ono samo biti navedeno radi ilustracije korištenja prethodnog teorema.

**Primjer 5.** *Fundamentalno rješenje Pellove jednadžbe*

$$x^2 - 7y^2 = 1$$

*je uređeni par* $(x_1, y_1) = (8, 3)$ *pa su, prema prethodnom teoremu, sva njezina rješenja dana s*

$$x_n + y_n\sqrt{7} = (8 + 3\sqrt{7})^n, \quad n \in \mathbb{N}.$$

Osim kao skup, sva rješenja Pellove jednadžbe možemo zapisati i kao rastući niz $(x_n, y_n), n \in \mathbb{N}$. Ako izraz (2.6) promatramo za $n+1$ umjesto za $n$ te ga najprije pomožimo s $x_1 + y_1\sqrt{d}$, zatim s $x_1 - y_1\sqrt{d}$, dobivamo jednadžbe:

$$(x_{n+1} + y_{n+1}\sqrt{d})(x_1 + y_1\sqrt{d}) = (x_1 + y_1\sqrt{d})^{n+2} \overset{(2.6)}{=} x_{n+2} + y_{n+2}\sqrt{d} \tag{2.7}$$
$$(x_{n+1} + y_{n+1}\sqrt{d})(x_1 - y_1\sqrt{d}) = (x_1 + y_1\sqrt{d})^n(x_1^2 - dy_1^2) \overset{(2.4)}{=} x_n + y_n\sqrt{d}. \tag{2.8}$$

Sada iz (2.7) slijedi:

$$x_{n+2} = x_1 x_{n+1} + d y_1 y_{n+1} \tag{2.9}$$

$$y_{n+2} = x_1 y_{n+1} + y_1 x_{n+1} \tag{2.10}$$

te analogno iz (2.8):

$$x_n = x_1 x_{n+1} - d y_1 y_{n+1} \tag{2.11}$$

$$y_n = x_1 y_{n+1} - y_1 x_{n+1}. \tag{2.12}$$

Zbrajanjem (2.9) i (2.11) te (2.10) i (2.12) dobivamo rekurzivne formule za rješenja Pellove jednadžbe, pri čemu je $(x_1, y_1)$ fundamentalno, $(x_0, y_0) = (1, 0)$ trivijalno rješenje:

$$x_{n+2} = 2x_1 x_{n+1} - x_n \tag{2.13}$$

$$y_{n+2} = 2x_1 y_{n+1} - y_n. \tag{2.14}$$

Pokažimo primjenu prethodno izvedenih rekurzivnih formula na idućem primjeru.

**Primjer 6.** *Odredimo prvih 5 rješenja Pellove jednadžbe*

$$x^2 - 23y^2 = 1.$$

*Njezino je fundamentalno rješenje* $(x_1, y_1) = (24, 5)$ *pa pomoću formula (2.13) i (2.14) lako izračunamo iduća četiri rješenja:*

- $(x_2, y_2) = (2x_1 x_1 - x_0, 2x_1 y_1 - y_0) = (1151, 240)$
- $(x_3, y_3) = (2x_1 x_2 - x_1, 2x_1 y_2 - y_1) = (55224, 11515)$
- $(x_4, y_4) = (2x_1 x_3 - x_2, 2x_1 y_3 - y_2) = (2649601, 552480)$
- $(x_5, y_5) = (2x_1 x_4 - x_3, 2x_1 y_4 - y_3) = (127125624, 26507525).$

Rješenje $(x_n, y_n)$ možemo, osim preko formule iz Teorema 4 i prethodno izvedenih rekurzivnih formula, zapisati pomoću sljedećih formula:

$$x_n = \frac{1}{2}\left[(x_1 + y_1\sqrt{d})^n + (x_1 - y_1\sqrt{d})^n\right] \tag{2.15}$$

$$y_n = \frac{1}{2\sqrt{d}}\left[(x_1 + y_1\sqrt{d})^n - (x_1 - y_1\sqrt{d})^n\right]. \tag{2.16}$$

Zaista, ako pomnožimo (2.16) sa $\sqrt{d}$ i oduzemo taj izraz od (2.15), dobivamo

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n. \tag{2.17}$$

Prema razlici kvadrata vrijedi

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) \\ &\overset{(2.17),(2.6)}{=} (x_1 - y_1\sqrt{d})^n(x_1 + y_1\sqrt{d})^n \\ &= (x_1^2 - dy_1^2)^n = 1. \end{aligned}$$

Dakle, (2.15) i (2.16) su rješenja Pellove jednadžbe (2.4).

## 2.2 Pelovska jednadžba $x^2 - dy^2 = -1$

U ovom poglavlju navodimo rezultate vezane za pelovsku jednadžbu

$$x^2 - dy^2 = -1. \tag{2.18}$$

Kao i kod obične Pellove jednadžbe, $d$ je prirodan broj različit od potpunog kvadrata, a fundamentalno rješenje ove jednadžbe je najmanji uređeni par prirodnih brojeva $(x_1, y_1)$ koji ju zadovoljava. Za početak pogledajmo nekoliko primjera.

**Primjer 7.** *Za jednadžbu $x^2 - 5y^2 = -1$ i bez poznavanja metoda za rješavanje možemo lako zaključiti da je njezino fundamentalno rješenje $(x_1, y_1) = (2, 1)$.*

**Primjer 8.** *Za razliku od Pellove jednadžbe, jednadžba $x^2 - dy^2 = -1$ ne mora imati cjelobrojna rješenja. Primjerice, jednadžba*

$$x^2 - 7y^2 = -1$$

*nema cjelobrojnih rješenja. Kako bismo to pokazali, pretpostavljamo suprotno, odnosno da rješenje postoji. Tada od iduća četiri slučaja mora vrijediti jedan:*

(1) *$x$ i $y$ su oba parni:*
*Neka je $x = 2u$ i $y = 2v$ za neke $u, v \in \mathbb{N}$. Tada je*

$$x^2 - 7y^2 = 4u^2 - 28v^2 = 4(u^2 - 7v^2).$$

*Kako je po pretpostavci $x^2 - 7y^2 = -1$, moralo bi biti $u^2 - 7v^2 = -\frac{1}{4}$, što nije moguće jer su $u, v \in \mathbb{N}$, pa je i $u^2 - 7v^2 \in \mathbb{Z}$. Dakle, $x$ i $y$ ne mogu oba biti parni.*

(2) *$x$ i $y$ su oba neparni:*
*Neka je $x = 2u - 1$ i $y = 2v - 1$ za neke $u, v \in \mathbb{N}$. Tada je*

$$\begin{aligned} x^2 - 7y^2 &= (2u-1)^2 - 7(2v-1)^2 \\ &= 4u^2 - 4u + 1 - 28v^2 + 28v - 7 \\ &= 2(2u^2 - 2u - 14v^2 + 14v - 3). \end{aligned}$$

*Iz ovoga slijedi da je izraz u zagradi jednak $-\frac{1}{2}$, što nije moguće jer su $u, v \in \mathbb{N}$ pa zaključujemo da ovaj slučaj također nije mogući.*

(3) *$x$ je paran, a $y$ neparan:*
*Neka je $x = 2u$, a $y = 2v - 1$ za neke $u, v \in \mathbb{N}$. Tada je*

$$\begin{aligned} x^2 - 7y^2 &= (2u)^2 - 7(2v-1)^2 \\ &= 4u^2 - 28v^2 + 28v - 7 \\ &= 4(u^2 - 7v^2 + 7v - 1) - 3. \end{aligned}$$

*pa bi moralo biti $u^2 - 7v^2 + 7v - 1 = \frac{1}{2}$, što opet nije moguće jer su $u, v \in \mathbb{N}$. Opet zaključujemo da ni ovakva kombinacija $x$ i $y$ nije moguća.*

(4) *$x$ je neparan, a $y$ paran:*
*Neka je $x = 2u - 1$, a $y = 2v$ za neke $u, v \in \mathbb{N}$. Tada je*

$$\begin{aligned} x^2 - 7y^2 &= (2u-1)^2 - 7(2v)^2 \\ &= 4u^2 - 4u + 1 - 28v^2 \\ &= 4(u^2 - u - 7v^2) + 1. \end{aligned}$$

*pa bi moralo biti $u^2 - u - 7v^2 = -\frac{1}{2}$, što je kontradikcija s pretpostavkom da su $u, v \in \mathbb{N}$. Dakle, nije moguće ni da je $x$ neparan, a $y$ paran.*

*Kako smo u sva četiri slučaja dobili kontradikciju, zaključujemo da jednadžba $x^2 - 7y^2 = -1$ nema cjelobrojnih rješenja.*

Jednako kao Pellova jednadžba i jednadžba (2.18) može se riješiti pomoću verižnih razlomaka (o tome će više riječi biti u Poglavlju 3.1, Teorem 10). Međutim, ni metoda verižnih razlomaka nam ne govori o tome ima li jednadžba (2.18) rješenja. Jedini nužan uvjet njezine rješivosti u cijelim brojevima leži u činjenici da $-1$ mora biti kvadratni ostatak modulo $d$, odnosno da $d$ nije djeljiv s 4 niti s bilo kojim prostim brojem oblika $4k + 3$. Sljedeći teorem govori nam koji je dovoljan uvjet za postojanje rješenja jednadžbe $x^2 - dy^2 = -1$.

**Teorem 5** (vidjeti [1, Teorem 10.14]). *Neka je $d$ prirodan broj različit od potpunog kvadrata. Ako pretpostavimo da postoji rješenje pelovske jednadžbe $x^2 - dy^2 = -1$ i da je njezino fundamentalno rješenje*

$$x_1 + y_1\sqrt{d},$$

*tada je fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$ dano s*

$$(x_1 + y_1\sqrt{d})^2.$$

*Dodatno, ako stavimo*

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

*tada su u nizu rješenja $(x_n, y_n)$ na neparnim mjestima sva rješenja jednadžbe $x^2 - dy^2 = -1$, a na parnim mjestima sva rješenja Pellove jednadžbe $x^2 - dy^2 = 1$.*

*Dokaz.* Drugi dio tvrdnje teorema je puno jednostavniji za pokazati pa ćemo najprije to napraviti. Po pretpostavci je $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ pa je tada i $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$. Množenjem ta dva izraza dobivamo:

$$x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = (-1)^n = \begin{cases} 1, & n \text{ paran} \\ -1, & n \text{ neparan,} \end{cases}$$

odnosno, vrijedi:

$$x_{2n} + y_{2n}\sqrt{d} \text{ je rješenje jednadžbe } x^2 - dy^2 = 1,$$
$$x_{2n+1} + y_{2n+1}\sqrt{d} \text{ je rješenje jednadžbe } x^2 - dy^2 = -1.$$

Prvi dio teorema, da je $(x_1 + y_1\sqrt{d})^2$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$, dokazat ćemo kontradikcijom. Pretpostavimo da je $u + v\sqrt{d}$ njezino fundamentalno rješenje za koje vrijedi:

$$1 < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^2.$$

Kako je $(x_1 + y_1\sqrt{d})(-x_1 + y_1\sqrt{d}) = -x_1^2 + dy_1^2 = 1$, slijedi da je $0 < -x_1 + y_1\sqrt{d} < 1$ pa je zato

$$-x_1 + y_1\sqrt{d} < (u + v\sqrt{d})(-x_1 + y_1\sqrt{d}) = s + t\sqrt{d} < x_1 + y_1\sqrt{d},$$

pri čemu je $s = -ux_1 + dvy_1$, $t = uy_1 - vx_1$ i $s^2 - dt^2 = -1$. Iz $s + t\sqrt{d} > 0$ i $s - t\sqrt{d} < 0$ mora biti $t > 0$. Kada bi vrijedilo da je $s < 0$, iz

$$-x_1 + y_1\sqrt{d} < s + t\sqrt{d}$$

bismo dobili

$$x_1 + y_1\sqrt{d} > -s + t\sqrt{d}$$

iz čega zaključujemo da je $|s| + t\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = -1$ manje od fundamentalnog rješenja, što je kontradikcija s početnom pretpostavkom.

Ako bismo pretpostavili da je $w + z\sqrt{d}$ neko rješenje od $x^2 - dy^2 = -1$ koje nije sadržano u nizu $(x_{2n+1} + y_{2n+1}\sqrt{d})$, tada bi postojao neki $m \in \mathbb{N}$ takav da je

$$(x_1 + y_1\sqrt{d})^{2m-1} < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{2m+1}.$$

Pomnožimo li prethodnu nejednakost s $(x_1 - y_1\sqrt{d})^{2m}$, dobivamo

$$-x_1 + y_1\sqrt{d} < \sigma + \tau\sqrt{d} < x_1 + y_1\sqrt{d},$$

pri čemu je $\sigma^2 - d\tau^2 = -1$, ali već smo pokazali da takvi $\sigma$ i $\tau$ ne mogu postojati. □

Pokažimo kroz primjer kako prethodni teorem možemo iskoristiti da bismo provjerili ima li jednadžba $x^2 - dy^2 = -1$ cjelobrojnih rješenja.

**Primjer 9.** *Neka je zadano fundamentalno rješenje $(x, y) = (19, 3)$, tj. $x + y\sqrt{40} = 19 + 3\sqrt{40}$ jednadžbe*

$$x^2 - 40y^2 = 1.$$

*Zanima nas ima li jednadžba $x^2 - 40y^2 = -1$ rješenje. Pretpostavimo da ono postoji, i označimo njezino fundamentalno rješenje s $x_1 + y_1\sqrt{40}$. Prema prethodnom bi teoremu za to rješenje trebalo vrijediti*

$$(x_1 + y_1\sqrt{40})^2 = 19 + 3\sqrt{40},$$

*odnosno*

$$x_1^2 + 40y_1^2 = 19, \quad 2x_1y_1 = 3.$$

*S obzirom da ovaj sustav nema cjelobrojnih rješenja, zaključujemo da ih nema ni jednadžba $x^2 - 40y^2 = -1$.*

Iduća propozicija daje nam dovoljan uvjet postojanja rješenja jednadžbe (2.18) za specijalan oblik broja $d$.

**Propozicija 1** (vidjeti [1, Propozicija 10.15])**.** *Ako je $p$ prost broj takav da je $p \equiv 1 \pmod 4$, tada jednadžba $x^2 - py^2 = -1$ ima rješenja.*

*Dokaz.* Ako s $(x_1, y_1)$ označimo fundamentalno rješenje jednadžbe $x^2 - py^2 = 1$, vrijedi da je $x_1^2 - y_1^2 \equiv 1 \pmod 4$ iz čega slijedi da je $x_1$ neparan, a $y_1$ paran. Nadalje, s obzirom da je $NZD(\frac{x_1-1}{2}, \frac{x_1+1}{2}) = 1$ i

$$\frac{x_1 - 1}{2} \cdot \frac{x_1 + 1}{2} = \frac{1}{4}(x_1^2 - 1) = \frac{1}{4}py_1^2 = p\left(\frac{y_1}{2}\right)^2,$$

znači da postoje prirodni brojevi $u$ i $v$ takvi da je

$$\frac{x_1 \pm 1}{2} = pv^2, \quad \frac{x_1 \mp 1}{2} = u^2 \quad \text{i} \quad \frac{y_1}{2} = uv.$$

Iz prethodnog slijedi da je $u^2 - pv^2 = \mp 1$, ali kako je $(x_1, y_1)$ po pretpostavci fundamentalno, pa stoga i minimalno rješenje, i $v < y_1$, mora vrijediti $u^2 - pv^2 = -1$. odnosno $(u, v)$ je rješenje jednadžbe $x^2 - py^2 = -1$. Također, prema Teoremu 4, rješenje $u + v\sqrt{p}$ je fundamentalno rješenje jednadžbe $x^2 - py^2 = -1$ i vrijedi

$$(u + v\sqrt{p})^2 = u^2 + pv^2 + 2uv\sqrt{p} = x_1 + y_1\sqrt{p}.$$

□

Pogledajmo primjenu Propozicije 1 na idućem primjeru.

**Primjer 10.** *Znamo da jednadžbe $x^2 - 5y^2 = -1$ i $x^2 - 13y^2 = -1$ imaju rješenje jer je $5 \equiv 1 \pmod 4$ i $13 \equiv 1 \pmod 4$. Posebno, fundamentalno rješenje prve jednadžbe je $(x_1, y_1) = (2, 1)$, a druge $(x_1, y_1) = (18, 5)$.*

## 2.3 Pelovske jednadžbe $x^2 - dy^2 = \pm 4$

U ovom dijelu rada navest ćemo primjere i neke specijalne rezultate vezane uz pelovske jednadžbe

$$x^2 - dy^2 = \pm 4,$$

pri čemu je $d$, kao i dosada, prirodan broj različit od potpunog kvadrata. Primijetimo da jednadžba

$$x^2 - dy^2 = 4 \tag{2.19}$$

uvijek ima rješenje jer ako je $(u, v)$ rješenje jednadžbe $x^2 - dy^2 = 1$ onda je $(2u, 2v)$ očigledno rješenje jednadžbe (2.19). Analogno, ako rješenje pelovske jednadžbe $x^2 - dy^2 = -1$ postoji i ako ga označimo s $(u, v)$, tada je $(2u, 2v)$ rješenje jednadžbe

$$x^2 - dy^2 = -4.$$

Sljedeći teorem daje nam dodatnu karakterizaciju rješenja jednadžbe (2.19).

**Teorem 6** (vidjeti [1, Teorem 10.16.]). *Sva rješenja jednadžbe* $x^2 - dy^2 = 4$ *u prirodnim brojevima dana su s*

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

*pri čemu je* $(x_1, y_1)$ *njezino fundamentalno rješenje.*

Teorem se dokazuje analogno kao i Teorem 4 stoga ga nećemo dokazati. Nadalje ćemo promotriti kakvog su oblika rješenja jednadžbe (2.19) u ovisnosti o parnosti ili neparnosti od $x_1$ i $y_1$. Dakle, imamo četiri slučaja:

(1) $x_1$ neparan i $y_1$ paran:
Stavimo da je $x_1 = 2u + 1$ i $y_1 = 2v$, $u, v \in \mathbb{N}$. Tada je

$$x_1^2 - dy_1^2 = (2u+1)^2 - d(2v)^2 = 4k^2 + 4k + 1 - 4dl^2 \neq 4.$$

Dakle, jasno je da slučaj u kojem je $x_1$ neparan, a $y_1$ paran nije moguć.

(2) $x_1$ paran i $y_1$ paran:
Zbog prethodnog su teorema u ovom slučaju tada i $x_n$ i $y_n$ također parni za svaki $n$ te je $\frac{x_1+y_1\sqrt{d}}{2}$ fundamentalno rješenje Pellove jednadžbe $x^2 - dy^2 = 1$.

(3) $x_1$ paran i $y_1$ neparan:
Stavimo $x_1 = 2u$ i $y_1 = 2v + 1$, $u, v \in \mathbb{N}$. Tada mora vrijediti

$$(2u)^2 - d(2v+1)^2 = 4u^2 - 4dv^2 - 4dv - d = 4,$$

odnosno $d$ mora biti djeljiv s 4. Dakle, postoji $d' \in \mathbb{N}$ takav da je $d = 4d'$ te je $\frac{x_1}{2} + y_1\sqrt{d'}$ fundamentalno rješenje Pellove jednadžbe $x^2 - d'y^2 = 1$.

(4) $x_1$ neparan i $y_1$ neparan:
Pod ovom pretpostavkom mora vrijediti

$$d \equiv dy_1^2 \equiv x_1^2 - 4 \equiv 5 \pmod 8$$

što znači da je uvjet da je $d \equiv 5 \pmod 8$ nužan da jednadžba (2.19) ima rješenja u neparnim brojevima. No taj uvjet nije i dovoljan, što možemo vidjeti u idućem primjeru.

**Primjer 11.** *Promotrimo sljedeće dvije jednadžbe:*

$$x^2 - 37y^2 = 4 \tag{2.20}$$

$$x^2 - 45y^2 = 4. \tag{2.21}$$

*Za obje jednadžbe vrijedi da je* $d \equiv 5 \pmod 8$, *ali nemaju obje jednadžbe rješenja u nepranim brojevima. Jednadžba (2.21) ima rješenja u neparnim brojevima i njezino je fundamentalno rješenje* $(x_1, y_1) = (7, 1)$, *dok je fundamenalno rješenje jednadžbe (2.20) dano s* $(x_1, y_1) = (146, 24)$ *i njezina su sva rješenja parna.*

Iduća propozicija daje nam konkretnu vezu između rješenja pelovske jednadžbe $x^2 - dy^2 = 4$ i njoj pripadne Pellove jednadžbe $x^2 - dy^2 = 1$ u slučaju kada su i $x_1$ i $y_1$ neparni.

**Propozicija 2** (vidjeti [1, Propozicija 10.17.])**.** *Ako jednadžba* $x^2 - dy^2 = 4$ *ima rješenja u neparnim brojevima i ako je* $x_1 + y_1\sqrt{d}$ *njezino fundamentalno rješenje, tada je*

$$\left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^3 = \frac{1}{8}(x_1^3 + 3dx_1y_1^2) + \frac{1}{8}(3x_1^2y_1 + dy_1^3)\sqrt{d}$$

*fundamentalno rješenje jednadžbe* $x^2 - dy^2 = 1$.

Za kraj ovog dijela dodatno ćemo još promotriti jednadžbu

$$x^2 - dy^2 = -4. \tag{2.22}$$

Već smo zaključili da ona ima rješenja ako ih ima i pripadna pelovska jednadžba $x^2 - dy^2 = -1$ i da su ta rješenja u parnim brojevima. No jednadžba (2.22) može imati rješenja i u neparnim brojevima te je, analogno kao i kod jednadžbe $x^2 - dy^2 = 4$, nužan uvjet za to da je $d \equiv 5 \pmod 8$. Vrijedi sljedeći teorem:

**Teorem 7** (vidjeti [1, Teorem 10.18.])**.** *Ako jednadžba* $x^2 - dy^2 = -4$ *ima rješenja i ako je njezino fundamentalno rješenje* $x_1 + y_1\sqrt{d}$, *tada su sva rješenja te jednadžbe dana s*

$$\frac{x_n + y_n\sqrt{d}}{2} = \left(\frac{x_1 + y_1\sqrt{d}}{2}\right)^n,$$

*pri čemu je* $n$ *neparan i* $(\frac{x_1+y_1\sqrt{d}}{2})^2$ *fundamentalno rješenje jednadžbe* $x^2 - dy^2 = 4$.

Pogledajmo na primjeru kako iskoristiti prethodno navedene tvrdnje kako bismo odredili fundamentalno rješenje Pellove jednadžbe $x^2 - dy^2 = 1$.

**Primjer 12.** *Neka je dana Pellova jednadžba*

$$x^2 - 29y^2 = 1$$

*i fundamentalno rješenje* $x_1 + y_1\sqrt{29} = 5 + \sqrt{29}$ *pripadne pelovske jednadžbe*

$$x^2 - 29y^2 = -4.$$

*Najprije pomoću Teorema 7 za fundamentalno rješenje jednadžbe*

$$x^2 - 29y^2 = 4$$

*dobivamo* $x_1 + y_1\sqrt{29} = 27 + 5\sqrt{29}$*, a zatim korištenjem Propozicije 2 dobivamo da je fundamentalno rješenje početne Pellove jednadžbe* $x_1 + y_1\sqrt{29} = 9801 + 1820\sqrt{29}$.

# 3 Neke metode rješavanja Pellove i pelovskih jednadžbi

Postoji više načina za pronalaženje fundamentalnog rješenja jednadžbe $x^2 - dy^2 = k$, $k \in \mathbb{Z} \setminus \{0\}$. Uvijek možemo probati "nabadanjem", tako da za $y$ uvrštavamo redom sve prirodne brojeve dok za $x$ ne dobijemo prirodan broj. Primjerice, ako imamo $x^2 - 2y^2 = 1$, možemo tu jednadžbu gledati kao $x^2 = 1 + 2y^2$. Dakle, ako za $y$ uvrštavamo, redom, $y = 1, 2, 3 \ldots$ već za $y = 2$ ćemo dobiti da je $x = 3$. No, ovaj pristup će u većini slučajevi biti previše vremenski zahtjevan. Recimo, fundamentalno rješenje jednadžbe $x^2 - 13y^2 = 1$ je $(x_1, y_1) = (180, 649)$, dok je fundamentalno rješenje jednadžbe $x^2 - 85y^2 = 1$ dano s $(x_1, y_1) = (285769, 30996)$. To bi značilo da smo u prvom slučaju uvrštavanjem morali napraviti 180, a u drugom slučaju 30996 iteracija kako bismo pronašli najmanje prirodno rješenje te su iz tog razloga razvijene druge efikasnije metode pronalaženja fundamentalnog rješenja.

U ovom poglavlju opisat ćemo dvije metode spomenute u Poglavlju 2, metodu verižnih razlomaka i *Chakravala* metodu. Međutim, prije toga navest ćemo i primjerom potkrijepiti još jedan rezultat koji nam govori kako pronaći fundamentalno rješenje Pellove jednadžbe.

**Propozicija 3** (vidjeti [1, Propozicija 10.13])**.** *Ako je $a+b\sqrt{d}$ rješenje jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima i vrijedi da je $a > \frac{1}{2}b^2 - 1$, onda je to fundamentalno rješenje. Posebno, ako su $u, v$ prirodni brojevi i $d = u(uv^2+2)$, onda je $1+uv^2+v\sqrt{d}$ fundamentalno rješenje jednadžbe $x^2 - dy^2 = 1$.*

**Primjer 13.** *Odredimo fundamentalno rješenje Pellove jednadžbe*

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

*Kako je*

$$8 = 2(2 \cdot 1^2 + 2),$$

*prema prethodnoj propoziciji je $1 + 2 \cdot 1^2 + \sqrt{8} = 3 + \sqrt{8} = x_1 + y_1\sqrt{8}$ fundamentalno rješenje početne jednadžbe. Dodatno, prema Teoremu 4 sva su njezina rješenja u prirodnim brojevima dana s*

$$x_n + y_n\sqrt{d} = (3 + \sqrt{8})^n, \quad n \in \mathbb{N}.$$

## 3.1 Korištenje verižnih razlomaka pri rješavanju pelovskih jednadžbi

Kao što smo već objasnili u Poglavlju 2.1, svako netrivijalno rješenje jednadžbe $x^2 - dy^2 = 1$ daje jako dobru racionalnu aproksimaciju iracionalnog broja $\sqrt{d}$, a dobre racionalne aproksimacije realnog broja dobivaju se pomoću razvoja tog broja u verižni razlomak. Najprije navodimo u obliku definicije što znači razviti redom broj u verižni razlomak.

**Definicija 6.** *Neka je $\alpha \in \mathbb{R}$. Stavimo $a_0 = \lfloor \alpha \rfloor$. Ako je $a_0 \neq \alpha$ napišemo $\alpha = a_0 + \frac{1}{\alpha_1}$, tj. $\alpha_1 = \frac{1}{\alpha - a_0} > 1$ i stavimo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $a_1 \neq \alpha_1$ napišemo $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tj. $\alpha_2 = \frac{1}{\alpha_1 - a_1} > 1$ i analogno stavimo $a_2 = \lfloor \alpha_2 \rfloor$. Taj postupak ponavljamo i on staje ako je za neki $m \in \mathbb{N}$ $a_m = \alpha_m$. Tada je*

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

*i vrijedi $\alpha \in \mathbb{Q}$. Uočimo da je $a_0 \in \mathbb{Z}$ i $a_i \in \mathbb{N}$, za svaki $i = 1, \ldots, m$. Takav $\alpha$ pišemo u obliku $\alpha = [a_0, a_1, \ldots, a_m]$ i kažemo da je to razvoj broja $\alpha$ u jednostavan verižni razlomak. Ako je $\alpha_m \neq a_m$ za svaki $m$, onda je $\alpha \in \mathbb{I}$ i imamo razvoj oblika $\alpha = [a_0, a_1, \ldots]$.*

Pogledajmo primjenu prethodne definicije na idućem primjeru.

**Primjer 14.** *Odredimo razvoj od $\alpha \in \mathbb{R}$ u jednostavan verižni razlomak ako je:*

(a) $\alpha = \frac{193}{25}$

*Rješenje: Primjenom Euklidovog algoritma lako dobijemo razvoj od $\alpha$ u jednostavan verižni razlomak. Imamo:*

$$\begin{aligned} 193 &= 7 \cdot 25 + 18 \\ 25 &= 1 \cdot 18 + 7 \\ 18 &= 2 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned}$$

*Dakle,* $\alpha = \frac{193}{25} = [7, 1, 2, 1, 1, 3]$.

(*b*) $\alpha = \frac{53}{37}$

*Rješenje: Analogno kao u prethodnom dobijemo sljedeći razvoj:*

$$\alpha = \frac{53}{37} = [1, 2, 3, 5].$$

**Definicija 7.** *Za beskonačni verižni razlomak*

$$[a_0, a_1, a_2, \dots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}$$

*kažemo da je periodski ako postoje cijeli brojevi* $k \geq 0$, $m \geq 1$ *takvi da je* $a_{m+n} = a_n$ *za sve* $n \geq k$. *U tom slučaju verižni razlomak pišemo u obliku*

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

*Broj* $m$ *nazivamo duljina perioda.*

**Napomena 2.** *Racionalni broj* $\frac{p_n}{q_n} = [a_0, a_1, \dots, a_n]$ *je* $n$*-ta konvergenta u razvoju broja* $\alpha$ *u verižni razlomak. Za* $n \geq 0$, *brojevi* $p_n$ *i* $q_n$ *zadovoljavaju rekurzivne relacije (vidjeti [1, Lema 8.13.]):*

$$p_n = a_n p_{n-1} + p_{n-2}, \quad p_{-2} = 0, p_{-1} = 1,$$
$$q_n = a_n q_{n-1} + q_{n-2}, \quad q_{-2} = 1, p_{-1} = 0.$$

**Definicija 8.** *Za iracionalni broj* $\alpha$ *kažemo da je kvadratna iracionalnost ako je* $\alpha$ *korijen kvadratne jednadžbe s racionalnim koeficijentima.*

Svaka kvadratna iracionalnost je oblika $\frac{s \pm \sqrt{d}}{t}$, $s \in \mathbb{Z}$, $d \in \mathbb{N}$, $d$ različit od potpunog kvadrata, $t \in \mathbb{Z} \setminus \{0\}$. Vrijedi sljedeći teorem:

**Teorem 8** (Euler, Lagrange, vidjeti [1, Teorem 8.39.])**.** *Razvoj realnog broja* $\alpha$ *u verižni razlomak je periodski ako i samo ako je* $\alpha$ *kvadratna iracionalnost.*

**Napomena 3.** *Ako je* $d$ *prirodan broj različit od potpunog kvadrata, razvoj broja* $\alpha = \frac{s_0 + \sqrt{d}}{t_0}$ *u verižni razlomak može se dobiti sljedećim algoritmom:*

$$a_i = \left\lfloor \frac{s_i + \sqrt{d}}{t_i} \right\rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, \quad i \in \mathbb{N}_0.$$

**Teorem 9** (vidjeti [1, Teorem 8.41.]). *Ako je $d$ prirodan broj različit od potpunog kvadrata, onda razvoj u verižni razlomak broja $\sqrt{d}$ ima oblik*

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

*gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, $r$ duljina najmanjeg perioda u razvoju od $\sqrt{d}$ te su $a_1, \ldots, a_{r-1}$ centralno simetrični, tj. $a_1 = a_{r-1}, a_2 = a_{r-2}$, itd.*

Pokažimo sada na primjeru kako razviti kvadratnu iracionalnost u verižni razlomak.

**Primjer 15.** *Odredimo razvoj od $\alpha \in \mathbb{R}$ u verižni razlomak ako je:*

(a) $\alpha = \sqrt{21}$

*Rješenje: Prema algoritmu iz Napomene 3 dobivamo*

- $s_0 = 0,\ t_0 = 1 \implies a_0 = \lfloor \sqrt{21} \rfloor = 4,$
- $s_1 = a_0 t_0 - s_0 = 4,\ t_1 = \frac{21 - s_1^2}{t_0} = 5 \implies a_1 = \left\lfloor \frac{s_1 + \sqrt{21}}{t_1} \right\rfloor = 1,$
- $s_2 = a_1 t_1 - s_1 = 1,\ t_2 = \frac{21 - s_2^2}{t_1} = 4 \implies a_2 = \left\lfloor \frac{s_2 + \sqrt{21}}{t_2} \right\rfloor = 1,$
- $s_3 = a_2 t_2 - s_2 = 3,\ t_3 = \frac{21 - s_3^2}{t_2} = 3 \implies a_3 = \left\lfloor \frac{s_3 + \sqrt{21}}{t_3} \right\rfloor = 2,$
- $s_4 = a_3 t_3 - s_3 = 3,\ t_4 = \frac{21 - s_4^2}{t_3} = 4 \implies a_4 = \left\lfloor \frac{s_4 + \sqrt{21}}{t_4} \right\rfloor = 1,$
- $s_5 = a_4 t_4 - s_4 = 1,\ t_5 = \frac{21 - s_5^2}{t_4} = 5 \implies a_5 = \left\lfloor \frac{s_5 + \sqrt{21}}{t_5} \right\rfloor = 1,$
- $s_6 = a_5 t_5 - s_5 = 4,\ t_6 = \frac{21 - s_6^2}{t_5} = 1 \implies a_6 = \left\lfloor \frac{s_6 + \sqrt{21}}{t_6} \right\rfloor = 8,$
- $s_7 = a_6 t_6 - s_6 = 4,\ t_7 = \frac{21 - s_7^2}{t_6} = 5 \implies a_7 = a_1 = 1.$

*Odavde je $\sqrt{21} = [4, \overline{1, 1, 2, 1, 1, 8}]$. Uočimo da teorijski rezultat dan u Teoremu 9 možemo iskoristiti u sljedećem smislu: ukoliko dobivamo razvoj koji nije oblika navedenog u tom teoremu, jasno je da smo nešto krivo izračunali.*

(b) $\alpha = \sqrt{17}$

*Rješenje: Analogno kao i u prethodnom dobivamo sljedeći razvoj:*

$$\sqrt{17} = [4, \overline{8}].$$

Kako bismo pokazali vezu između verižnih razlomaka i određivanja rješenja Pellove jednadžbe navodimo sljedeći rezultat čiji se dokaz može vidjeti u [5].

**Teorem 10** (vidjeti [1, Teorem 10.20.]). *Neka je $l$ duljina perioda u razvoju od $\sqrt{d}$ u verižni razlomak. Tada vrijedi:*

(a) *Ako je $l$ paran, tada jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva su pozitivna rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ dana s*

$$(x, y) = (p_{kl-1}, q_{kl-1}), \quad k \in \mathbb{N}.$$

*Dodatno, njezino fundamentalno rješenje je $(p_{l-1}, q_{l-1})$.*

(b) *Ako je $l$ neparan, sva pozitivna rješenja jednadžbe $x^2 - dy^2 = -1$ dana su s*

$$(x, y) = (p_{(2k-1)l-1}, q_{(2k-1)l-1}), \quad k \in \mathbb{N},$$

*dok su sva pozitivna rješenja Pellove jednadžbe $x^2 - dy^2 = 1$ dana s*

$$(x, y) = (p_{2kl-1}, q_{2kl-1}), \quad k \in \mathbb{N}.$$

*Dodatno, njezino fundamentalno rješenje je $(p_{2l-1}, q_{2l-1})$.*

U idućem ćemo primjeru pokazati kako pronaći rješenje Pellove jednadžbe korištenjem prethodnog teorema.

**Primjer 16.** *Pronađimo korištenjem verižnih razlomaka prvih nekoliko rješenja jednadžbe*

$$x^2 - 17y^2 = 1.$$

*Najprije je potrebno razviti $\sqrt{17}$ u verižni razlomak, što smo mi već napravili u Primjeru 15 i dobili $\sqrt{17} = [4, \overline{8}]$. Sada, s obzirom da je period neparan, iz tvrdnje pod b) prethodnog teorema znamo da su sva rješenja početne jednadžbe dana s*

$$(x, y) = (p_{2k-1}, q_{2k-1}), \quad k \in \mathbb{N},$$

*pri čemu je fundamentalno rješenje $(p_1, q_1)$. Računamo*

$$\frac{p_1}{q_1} = 4 + \frac{1}{8} = \frac{33}{8}$$

*i dobivamo za fundamentalno rješenje $(x, y) = (33, 8)$. Iduće rješenje dobivamo za $k = 2$ odnosno računajući treću konvergentu*

$$\frac{p_3}{q_3} = 4 + \cfrac{1}{8 + \cfrac{1}{8 + \cfrac{1}{8}}} = \frac{2177}{528}$$

*pa je iduće najmanje rješenje* $(x, y) = (2177, 528)$. *Time smo odredili prva dva rješenja, dok ostala možemo dobiti računajući dalje konvergente za* $k = 3, 4, 5 \ldots$ *Primijetimo da, s obzirom da je period* $l$ *neparan, prema prethodnom teoremu i jednadžba* $x^2 - 21y^2 = -1$ *ima rješenja i da su sva njezina rješenja dana s*

$$(x, y) = (p_{2k-2}, q_{2k-2}), \quad k \in \mathbb{N}.$$

*Dakle, računajući redom sve konvergente u razvoju od* $\sqrt{17}$ *u verižni razlomak bismo na neparnim mjestima dobili rješenja jednadžbe* $x^2 - 17y^2 = 1$, *a na parnim mjestima rješenja jednadžbe* $x^2 - 17y^2 = -1$.

Sljedeća propozicija može se koristiti pri rješavanju pelovskih jednadžbi oblika $x^2 - dy^2 = k$, $k \in \mathbb{Z} \setminus \{0\}$. Iskazat ćemo ju u općenitom obliku, a pokazati njenu primjenu u slučaju $k = 4$.

**Propozicija 4** (vidjeti [1, Propozicija 10.22.]). *Ako je* $|k| < \sqrt{d}$ *i* $u + v\sqrt{d}$ *rješenje jednadžbe* $x^2 - dy^2 = k$, *onda je* $\frac{u}{v}$ *neka konvergenta u razvoju od* $\sqrt{d}$ *u verižni razlomak.*

Propoziciju ćemo i dokazati no za to su nam potrebne još dvije tvrdnje.

**Teorem 11** (Legendrov, vidjeti [1, Teorem 8.26.]). *Ako su* $p$ *i* $q$ *cijeli brojevi takvi da vrijedi*

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

*tada je* $\frac{p}{q}$ *neka konvergenta od* $\alpha$.

**Teorem 12** (vidjeti [5, Teorem 11, str. 190.]). *Ako je* $\alpha$ *iracionalan broj, tada je* $(k+1)$*-a konvergenta u razvoju od* $\frac{1}{\alpha}$ *recipročna vrijednost* $k$*-te konvergente u razvoju od* $\alpha$ *u verižni razlomak.*

Vratimo se sada na dokaz Propozicije 4.

*Dokaz.* Prvo ćemo tvrdnju dokazati za $k > 0$. Iz te pretpostavke odmah slijedi da je $u^2 - dv^2 > 0$, tj. $u > v\sqrt{d}$ pa je

$$\begin{aligned} 0 < \frac{u}{v} - \sqrt{d} &= \left(\frac{u - v\sqrt{d}}{v}\right)\left(\frac{u + v\sqrt{d}}{u + v\sqrt{d}}\right) \\ &= \frac{u^2 + uv\sqrt{d} - uv\sqrt{d} - dv^2}{v(u + v\sqrt{d})} \\ &= \frac{k}{v(u + v\sqrt{d})}. \end{aligned}$$

Kako je $u > v\sqrt{d}$, tada vrijedi

$$\begin{aligned} u > v\sqrt{d} &\implies u + v\sqrt{d} > 2v\sqrt{d} \\ &\implies v(u + v\sqrt{d}) > 2v^2\sqrt{d} \\ &\implies \frac{1}{v(u + v\sqrt{d})} < \frac{1}{2v^2\sqrt{d}}. \end{aligned}$$

Dodatno, iz pretpostavki da je $|k| < \sqrt{d}$ i $k > 0$, znamo da je $\frac{1}{\sqrt{d}} < \frac{1}{k}$ pa imamo

$$0 < \frac{u}{v} - \sqrt{d} = \frac{k}{v(u + v\sqrt{d})} < \frac{k}{2v^2\sqrt{d}} < \frac{k}{2v^2 k} = \frac{1}{2v^2}.$$

Iz Teorema 11 znamo da je $\frac{u}{v}$ neka konvergenta u razvoju od $\sqrt{d}$ u verižni razlomak.

Ako sada pretpostavimo da je $k < 0$, slijedi da je $u < v\sqrt{d}$, odnosno

$$\begin{aligned} 0 < \frac{v}{u} - \frac{1}{\sqrt{d}} &= \left(\frac{v\sqrt{d} - u}{u\sqrt{d}}\right)\left(\frac{u + v\sqrt{d}}{u + v\sqrt{d}}\right) \\ &= \frac{uv\sqrt{d} - u^2 + v^2 d - uv\sqrt{d}}{u\sqrt{d}(u + v\sqrt{d})} \\ &= \frac{-k}{u\sqrt{d}(u + v\sqrt{d})}. \end{aligned}$$

S obzirom da je $|k| < \sqrt{d}$ i $k < 0$, imamo $\frac{1}{\sqrt{d}} < \frac{1}{|k|}$. Nadalje, iz $u < v\sqrt{d}$ imamo

$$\begin{aligned} u < v\sqrt{d} &\implies 2u < u + v\sqrt{d} \\ &\implies 2u^2\sqrt{d} < u\sqrt{d}(u + v\sqrt{d}) \\ &\implies \frac{1}{u\sqrt{d}(u + v\sqrt{d})} < \frac{1}{2u^2\sqrt{d}} \end{aligned}$$

te je tada

$$0 < \frac{v}{u} - \frac{1}{\sqrt{d}} = \frac{|k|}{u\sqrt{d}(u + v\sqrt{d})} < \frac{|k|}{2u^2\sqrt{d}} < \frac{|k|}{2u^2|k|} < \frac{1}{2u^2}.$$

Ponovno iskorištavamo Legendreov teorem i zaključujemo da je $\frac{v}{u}$ neka konvergenta u razvoju od $\frac{1}{\sqrt{d}}$ pa je, zbog Teorema 12, $\frac{u}{v}$ neka konvergenta u razvoju od $\sqrt{d}$ u verižni razlomak. Točnije, ako je $\frac{v}{u}$ $(i+1)$-va konvergenta u razvoju od $\frac{1}{\sqrt{d}}$, tada je $\frac{u}{v}$ $i$-ta konvergenta u razvoju od $\sqrt{d}$. □

Za kraj ovog dijela kroz primjer navodimo kako pronaći rješenje pelovske jednadžbe za $k = 4$ korištenjem Propozicije 4.

**Primjer 17.** *Pronađimo barem jedno rješenje jednadžbe*

$$x^2 - 21y^2 = 4.$$

*Ranije smo već pokazali da pelovska jednadžba $x^2 - dy^2 = 4$ uvijek ima rješenja u parnim brojevima. Kako je $|4| < \sqrt{21}$, zbog Propozicije 4 znamo da razvojem $\sqrt{21}$ u verižni razlomak i računanjem konvergenti možemo odrediti neka od tih rješenja. Iz Primjera 15 znamo da je*

$$\sqrt{21} = [4, \overline{1, 1, 2, 1, 1, 8}].$$

*Izračunamo li, redom, konvergente $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \ldots, \frac{p_6}{q_6}$ i provjeravamo zadovoljavaju li neke od njih početnu jednadžbu, dobit ćemo sljedeća dva rješenja:*

$$(p_1, q_1) = (5, 1) \text{ i } (p_3, q_3) = (23, 5).$$

## 3.2 Chakravala metoda

Kao što smo već rekli, prije nego što se Pellova jednadžba počela proučavati u Europi, prije Pella, Eulera i Fermata, jednadžbe oblika $x^2 - dy^2 = k$ proučavali su indijski matematičari, od kojih je prvi bio Brahmagupta. Njegovo je proučavanje Pellove jednadžbe dovelo do metode koja je nazvana *Chakravala* zbog svoje cikličke prirode ('chakra' = kotač), a nama je ista danas poznata kao *metoda kompozicije*.

U ovom poglavlju opisat ćemo kako *Chakravala* metoda funkcionira, ali to nećemo dokazivati (detaljnije se može pronaći u [6] i [7]). Započinjemo s navođenjem Brahmaguptinog identiteta:

$$(a^2 - nb^2)(c^2 - nd^2) = (ac + nbd)^2 - n(ad + bc)^2$$
$$(a^2 - nb^2)(c^2 - nd^2) = (ac - nbd)^2 - n(ad - bc)^2,$$

pri čemu su $a, b, c, d, n \in \mathbb{N}$. Ono što ovdje možemo primijetiti je da, ako vrijedi

$$a^2 - nb^2 = 1 \quad \text{i} \quad c^2 - nd^2 = 1$$

tada je

$$(ac + nbd)^2 - n(ad + bc)^2 = 1,$$
$$(ac - nbd)^2 - n(ad - bc)^2 = 1.$$

Drugim riječima, ako su $(a, b)$ i $(c, d)$ rješenja Pellove jednadžbe $x^2 - ny^2 = 1$, tada su to i $(ac + nbd, ad + bc)$ te $(ac - nbd, ad - bc)$. Analogno se dokaže da isto vrijedi i ako pretpostavimo da je

$$a^2 - nb^2 = -1 \quad \text{i} \quad c^2 - nd^2 = -1.$$

Sljedeća važna tvrdnja generalizacija je Brahmaguptinog identiteta, a iskazat ćemo ju u obliku teorema.

**Teorem 13** (Brahmaguptino pravilo kompozicije, vidjeti [6])**.** *Neka su $k_1$ i $k_2$ cijeli brojevi različiti od 0. Ako je $(a, b)$ cjelobrojno rješenje jednadžbe $x^2 - ny^2 = k_1$ i $(c, d)$ cjelobrojno rješenje jednadžbe $x^2 - ny^2 = k_2$, tada je $(ac + nbd, ad + bc)$ cjelobrojno rješenje jednadžbe $x^2 - ny^2 = k_1k_2$.*

*Dokaz.*

$$\begin{aligned}(ac + nbd)^2 - n(ad + bc)^2 &= a^2c^2 + 2abcdn + n^2b^2d^2 - n(a^2d^2 + 2abcd + b^2c^2)\\ &= a^2c^2 + n^2b^2d^2 - na^2d^2 - nb^2c^2)\\ &= a^2(c^2 - nd^2) - nb^2(c^2 - nd^2)\\ &= (a^2 - nb^2)(c^2 - nd^2) = k_1k_2.\end{aligned}$$

□

Pogledajmo kroz nekoliko primjera primjenu Brahmaguptinog pravila kompozcije u rješavanju pelovskih jednadžbi.

**Primjer 18.** *Odredimo jedno rješenje jednadžbe $x^2 - ny^2 = k$ ako je:*

(a) $n = 13$, $k = -4$
*Rješenje: Tražimo rješenje jednadžbe*

$$x^2 - 13y^2 = -4 = -1 \cdot 4.$$

*Iz Primjera 10 i 17 znamo da je $(a, b) = (11, 3)$ rješenje jednadžbe $x^2 - 13y^2 = 4$, a $(c, d) = (18, 5)$ rješenje jednadžbe $x^2 - 13y^2 = -1$. Sada primjenom Teorema 13 lako dolazimo do rješenja početne jednadžbe:*

$$(ac + nbd, ad + bc) = (18 \cdot 11 + 13 \cdot 5 \cdot 3, 18 \cdot 3 + 5 \cdot 11) = (393, 109).$$

(*b*) $n = 13,\ k = -16$

*Rješenje: Želimo pronaći jedno rješenje jednadžbe*

$$x^2 - 13y^2 = -16 = -4 \cdot 4.$$

*S obzirom da znamo rješenja jednadžbi* $x^2 - 13y^2 = \pm 4$*, analogno kao i u prethodnom primijenimo Teorem 13 i dobivamo da je jedno rješenje početne jednadžbe*

$$(393 \cdot 11 + 13 \cdot 109 \cdot 3, 393 \cdot 3 + 109 \cdot 11) = (8574, 2378).$$

Idući indijski matematičar koji se bavio Pellovim jednadžbama bio je Bhaskara II., koji je dao treći identitet važan za *Chakravala* algoritam.

**Lema 3** (Bashkarina lema, vidjeti [6])**.** *Ako je* $a^2 - nb^2 = k$*, tada je*

$$\left(\frac{ma + nb}{k}\right)^2 - n\left(\frac{a + bm}{k}\right)^2 = \frac{m^2 - n}{k}, \quad m \in \mathbb{Z}.$$

*Dokaz.*

$$\begin{aligned}
\left(\frac{ma + nb}{k}\right)^2 - n\left(\frac{a + bm}{k}\right)^2 &= \frac{1}{k^2}\left[m^2a^2 + 2abmn + n^2b^2 - n(a^2 - 2abm + b^2m^2)\right] \\
&= \frac{1}{k^2}\left[m^2a^2 + n^2b^2 - na^2 + m^2b^2\right] \\
&= \frac{1}{k^2}\left[m^2(a^2 - nb^2) - n(a^2 - nb^2)\right] \\
&= \frac{1}{k^2}(m^2 - n)(a^2 - nb^2) = \frac{m^2 - n}{k}.
\end{aligned}$$

□

Dalje ćemo pretpostaviti da je $n$ fiksan prirodan broj različit od potpunog kvadrata, a s $(x, y, k)$ ćemo označiti rješenje jednadžbe

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

pri čemu je $k$ cijeli broj različit od 0. Iz Teorema 13 znamo da za svake dvije uređene trojke cijelih brojeva $(a, b, k_1)$ i $(a, b, k_2)$ postoji uređena trojka $(ac + nbd, ad + bc, k_1k_2)$. Kompoziciju te dvije trojke je Brahmagupta nazvao *Bhavana*:

$$(a, b, k_1) * (c, d, k_2) := (ac + nbd, ad + bc, k_1k_2).$$

Pretpostavimo da imamo $a^2 - nb^2 = k$, tj. imamo uređenu trojku $(a, b, k)$. Ako bismo, dodatno, uzeli da je $a = m$, dobili bismo trivijalno rješenje, tj. uređenu trojku $(m, 1, m^2 - n)$. Sada, ako iskoristimo *Bhavanu*, dobijemo

$$(a, b, k) * (m, 1, m^2 - n) = (ma + nb, a + bm, k(m^2 - n)).$$

Dakle, ako znamo da je $a^2 - nb^2 = k$, tada je

$$(ma + nb)^2 - n(a + bm)^2 = k(m^2 - n)$$

te dijeljenjem s $k^2$ dobijemo Bhaskarinu lemu.

*Chakravala* metodom tražimo rješenja jednadžbi $x^2 - ny^2 = \pm 1$. Ideja metode temelji se na uzastopnoj primjeni pravila kompozicije, pri čemu se sve tri koordinate u svakom ponavljanju povećavaju. Iz toga razloga se u algoritmu primjenjuje Bhaskarina lema - uvodi se dijeljenje jer želimo da se $k$ smanjuje, a ne povećava. Algoritam se provodi na sljedeći način: najprije odabiremo uređenu trojku cijelih brojeva $(a_0, b_0, k_0)$ takvu da je

$$a_0 < \sqrt{n} < a_0 + 1, \quad b_0 = 1, \quad k_0 = a_0^2 - n \quad (k_0 < 0 \text{ uvijek}),$$

a zatim za $i = 1, 2, 3, \ldots$ ponavljamo iduće korake:

1. Tražimo $m_i$ takav da je $a_{i-1} \equiv -b_{i-1}m_i \pmod{k_{i-1}}$ i $|m_i^2 - n|$ minimalno.

2. Računamo

$$a_i = \frac{a_{i-1}m_i + nb_{i-1}}{|k_{i-1}|}, \quad b_i = \frac{a_{i-1} + b_{i-1}m_i}{|k_{i-1}|}, \quad k_i = \frac{m_i^2 - n}{k_{i-1}}.$$

Algoritam, odnosno korake 1 i 2 ponavljamo sve dok za neki $i = l$ ne dobijemo $k_l = 1$ ako tražimo rješenje jednadžbe $x^2 - ny^2 = 1$, odnosno $k_l = -1$ ako tražimo rješenje jednadžbe $x^2 - ny^2 = -1$ (ako ono postoji). Fundamentalno rješenje je tada dano s $(a_l, b_l)$. Pogledajmo primjenu algoritma na sljedećem primjeru:

**Primjer 19.** *Pronađimo rješenje Pellove jednadžbe*

$$x^2 - 17y^2 = 1.$$

*Prvo stavljamo da je* $b_0 = 1$ *i tražimo* $a_0$ *tako da je* $a_0 < \sqrt{17} < a_0 + 1$ *i* $k_0 = a_0^2 - n$. *Dakle, krećemo s trojkom* $(4, 1, -1)$.

- $i = 1$ :

  1. *Tražimo* $m_1$ *takav da* $k_0|(a_0 + b_0 m_1)$, *tj.* $-1|(4 + m_1)$, *što vrijedi za svaki prirodan broj* $m_1$. *S obzirom da je dodatni uvjet da* $|m_1^2 - 17|$ *bude minimalno, uzimamo da je* $m_1 = 3$.

  2. *Računamo* $a_1, b_1$ *i* $k_1$*:*

$$a_1 = \frac{a_0 \cdot m_1 + n b_0}{|k_0|}, \quad b_1 = \frac{a_0 + b_0 m_1}{|k_0|}, \quad k_1 = \frac{m_1^2 - n}{k_0}.$$

  *i dobivamo*

$$a_1 = 29, \quad b_1 = 7, \quad k_1 = 8.$$

  *Kako je* $k_1 \neq 1$, *nastavljamo s algoritmom.*

- $i = 2$ :

  1. *Tražimo* $m_2$ *takav da* $8|(29 + 7m_2)$, *dakle* $m_2 \in \{5, 13, 21, \dots\}$. *Zbog dodatnog uvjeta da* $|m_2^2 - 17|$ *bude minimalno, uzimamo da je* $m_2 = 5$ *i prelazimo na korak 2.*

  2. *Računamo nove* $a_2, b_2$ *i* $k_2$*:*

$$a_2 = \frac{29 \cdot 5 + 17 \cdot 7}{8} = 33, \quad b_2 = \frac{29 + 7 \cdot 5}{8} = 8, \quad k_2 = \frac{5^2 - 17}{-1} = 1.$$

  *Kako je* $k_2 = 1$ *to je* $(a_2, b_2) = (33, 8)$ *rješenje jednadžbe* $x^2 - 17y^2 = 1$.

Što se dogodi ako nastavimo s provođenjem algoritma? Konkretno, u prethodnom primjeru bismo u iduća 4 koraka dobili iduće:

- $i = 3$ : $\quad m_3 = 3, \quad (a_3, b_3, k_3) = (235, 57, -8)$
- $i = 4$ : $\quad m_4 = 5, \quad (a_4, b_4, k_4) = (268, 65, -1)$
- $i = 5$ : $\quad m_5 = 3, \quad (a_5, b_5, k_5) = (1909, 463, 8)$
- $i = 6$ : $\quad m_6 = 5, \quad (a_6, b_6, k_6) = (2177, 528, 1).$

Dakle, nastavkom provođenja algoritma dolazimo do još jednog rješenja, odnosno ponavljanjem algoritma dobit ćemo sva rješenja. Osim toga, uvjet da algoritam započinjemo odabiranjem trojke $(a_0, b_0, k_0)$ takve da je

$$a_0 < \sqrt{n} < a_0 + 1, \quad b_0 = 1, \quad k_0 = a_0^2 - n,$$

osigurava nam da do prvog rješenja dođemo u što manje iteracija.

Primijetimo da *Chakravala* metoda ne služi samo za rješavanje jednadžbi $x^2 - ny^2 = \pm 1$, nego i za rješavanje pelovskih jednadžbi, odnosno jednadžbi kod kojih umjesto $\pm 1$ stoji neki drugi cijeli broj različit od 0. Konkretno, u prethodnom smo primjeru za $i = 1$ u koraku 2 dobili uređenu trojku $(a_1, b_1, k_1) = (29, 7, 8)$ i lako se provjeri da je

$$(a_1, b_1) = (29, 7)$$

fundamentalno rješenje jednadžbe

$$x^2 - 17y^2 = 8.$$

Dakle, *Chakravala* algoritmom možemo računati rješenja (naravno, ukoliko ona postoje) svih jednadžbi oblika

$$x^2 - ny^2 = k, \quad k \in \mathbb{Z}\backslash\{0\}, \tag{3.1}$$

pri čemu korake 1 i 2 ponavljamo dok za neki $i = l$ ne dobijemo $k_l = k$.

# Literatura

[1] A. Dujella, *Teorija brojeva*, Školska knjiga d.d., Zagreb, 2019.

[2] M. J. Jacobson, Jr., H. C. Williams, *Solving the Pell equation*, Springer Science+Business Media, New York, 2009.

[3] H. L. Keng, *Introduction to Number Theory*, Springer-Verlag Berlin Heidelberg, Wurzburg, 1982.

[4] W. Sierpinski, *Elementary Theory of Numbers*, PWN - Polish Scientific Publishers, Varšava, vol. 31, 1988.

[5] J. E. Shockley, *Introduction to Number Theory*, Holt, Rinehart and Winston, Inc., New York, 1967.

[6] S. Birbrower, *Pell's Equation and the Chakravala Method*, članak, 2021., web izvor dostupan na https://medium.com/

[7] B.Sury, *Chakravala - a modern Indian method*, Indian Statistical Institute Bangalore, India, 2010., web izvor dostupan na https://www.isibang.ac.in/

[8] J. Unger, *Solving Pell's equation with Continued Fractions*, University of Canterbury, 2009., web izvor dostupan na https://ir.canterbury.ac.nz/

[9] Wikiwand, web izvor dostupan na https://www.wikiwand.com/

# Sažetak

U ovom diplomskom radu najprije smo naveli definicije te neke općenite rezultate vezane uz neke oblike diofantskih jednadžbi, a zatim se u ostatku rada usmjerili na specijalan oblik nelinearne diofantske jednadžbe: Pellovu jednadžbu. Osim toga, proučili smo pelovske jednadžbe $x^2 - dy^2 = \pm 1, \pm 4$. Naveli smo dokaze o nužnim i dovoljnim uvjetima postojanja njihovih rješenja, pokazali strukturu rješenja te naposlijetku pokazali kako te jednadžbe riješiti korištenjem verižnih razlomaka i drevne indijske *Chakravala* metode.

# Ključne riječi

linearne diofantske jednadžbe, nelinearne diofantske jednadžbe, Pellova jednadžba, pelovska jednadžba, fundamentalno rješenje, verižni razlomci, *Chakravala* metoda

# Pell's equation

## Summary

In this final paper, we first stated the definitions and some general results related to some types of Diophantine equations. After that, we focused on a special type of nonlinear Diophantine equation: Pell's equation. Additionally, we studied the equations $x^2 - dy^2 = \pm 1, \pm 4$. We presented the necessary and sufficient conditions for the existence of their solutions, showed the structure of the solutions and finally showed how to solve these equations using the continued fractions method and the ancient Indian *Chakravala* method.

## Keywords

linear Diophantine equations, nonlinear Diophantine equations, Pell's equation, generalized Pell's equation, Pellian equation, continued fractions, *Chakravala* method

# Životopis

Rođena sam u Osijeku, 28.9.1997. godine, gdje sam i živjela do 2000. godine kada se selim u Bilje i ondje završavam osnovnu školu. Ostajem živjeti u Bilju, ali u Osijeku upisujem II. gimnaziju i završavam svoje srednjoškolsko obrazovanje 2016. godine. Iste godine upisujem preddiplomski studij matematike na Sveučilištu J.J. Strossmayera u Osijeku na Odjelu za matematiku koji završavam 2020. godine s temom završnog rada *Korisne metode opisa skupova podataka*, izrađenog pod mentorstvom prof. dr. sc. Mirte Benšić. Na istom fakultetu upisujem i diplomski studij, smjer *Financijska matematika i statistika*.