Diofantske jednadžbe višeg stupnja

Sučić, Dora

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Dora Sučić

DIOFANTSKE JEDNADŽBE VIŠEG STUPNJA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, rujan, 2019.

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. _____

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

Sadržaj

Uvod

Diofantska jednadžba je polinomijalna jednadžba u jednoj ili više nepoznanica čija se rješenja traže u prstenu cijelih brojeva $\mathbb{Z}$. Dakle,

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

gdje je f polinom sa cjelobrojnim koeficijentima, tj. $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Za jednadžbu (1) reći ćemo da je rješiva ako postoji uređena n-torka cijelih brojeva $(a_1, a_2, \ldots, a_n)$ takva da vrijedi jednakost $f(a_1, a_2, \ldots, a_n) = 0$. Među najpoznatije diofantske jednadžbe spadaju:

- linearna diofantska jednadžba

  $$ax + by = c,$$

  gdje su $a, b, c \in \mathbb{Z}$,

- Pitagorina jednadžba

  $$x^2 + y^2 = z^2,$$

- Fermatova jednadžba

  $$x^n + y^n = z^n,$$

  gdje je $n \in \mathbb{N}$ i $n > 2$,

- Pellova jednadžba

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

  gdje je $d \in \mathbb{N}$ i d nije potpun kvadrat.

Linearna diofantska jednadžba, uz uvjet da $\gcd(a, b) \mid c$, Pitagorina jednadžba i Pellova jednadžba imaju beskonačno mnogo rješenja u prstenu cijelih brojeva. Fermatova jednadžba nema rješenja u skupu prirodnih brojeva. Slutnju za tu tvrdnju postavio je Fermat u 17. stoljeću, a za konačan dokaz trebalo je više od 350 godina (A. Wiles).

Jednadžbe oblika (1) ime su dobile po grčkom matematičaru Diofantu iz Aleksandrije koji je živio u 3. stoljeću. O Diofantovom životu ne zna se mnogo, ali ga se smatra najznačajnijim matematičarom postklasičnog razdoblja grčke matematike i posljednjim velikim europskim matematičarom prije Fibonaccija. Diofant je najpoznatiji po svom djelu *Arithmetica* čije su kopije i prijevodi imali velik utjecaj na druge značajne matematičare. *Arithmetica* se razlikuje po stilu i sadržaju od ostalih djela iz toga doba koja su se bavila teorijom brojeva zbog simboličkih zapisa. Naime, Diofant je za oznake nepoznanica, potencija, suprotnih brojeva, jednakosti i oduzimanja koristio skraćeni zapis riječi, što je bio prijelazni oblik na čisto simboličku algebru. Stoga Diofanta nazivamo *ocem algebre*.

U ovom radu bavimo se jednadžbama oblika (1) u kojima je stupanj polinoma f veći od 1. Vezano uz rješavanje diofantskih jednadžbi možemo istaknuti sljedeća pitanja, odnosno probleme:

- Je li jednadžba (1) rješiva?
- Ako je jednadžba (1) rješiva, je li skup rješenja konačan ili beskonačan?
- Ako je jednadžba (1) rješiva, možemo li odrediti sva njena rješenja?

U prvom poglavlju opisujemo neke elementarne metode rješavanja kao što su metoda faktorizacije, metoda matematičke indukcije i parametarska metoda, te opisujemo nešto naprednije metode koje uključuju Gaussove cijele brojeve, odnosno općenito kvadratna polja.

U drugom poglavlju bavimo se nekim klasičnim diofantskim jednadžbama drugog stupnja: Pitagorinom jednadžbom, njenom poopćenom jednadžbom $ax^2 + by^2 = z^2$ i Pellovom jednadžbom te opisujemo njihov skup rješenja.

Poglavlje 1

Metode rješavanja diofantskih jednadžbi

1.1 Metoda faktorizacije

Neka je zadana jednadžba

$$f(x_1, x_2, \ldots, x_n) = 0,$$

za $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$. Ideja ove metode je zapisati danu jednadžbu u ekvivalentnom obliku

$$f_1(x_1, x_2, \ldots, x_n) \cdot f_2(x_1, x_2, \ldots, x_n) \cdots f_k(x_1, x_2, \ldots, x_n) = a$$

gdje su f_1,f_2,...,$f_k \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ i $a \in \mathbb{Z}$. Broj a se na konačno mnogo načina može zapisati kao umnožak k faktora, odnosno k cijelih brojeva $a_1, a_2, \ldots, a_k$. Iz svakog takvog rastava dobivamo po jedan sustav jednadžbi

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = a_1, \\ f_2(x_2, x_2, \ldots, x_n) = a_2, \\ \vdots \\ f_k(x_1, x_2, \ldots, x_n) = a_k. \end{cases}$$

Rješavanjem svih takvih sustava dobivamo sva rješenja početne jednadžbe. Pokažimo primjenu ove metode na nekoliko primjera.

Primjer 1.1. *Odredimo sva cjelobrojna rješenja jednadžbe*

$$x^6 + 3x^3 + 1 = y^4.$$

Rješenje. Prvo želimo početnu jednadžbu zapisati u ekvivalentnom obliku takvom da s lijeve strane jednakosti imamo umnožak funkcija koje ovise o x i y, a s desne cijeli broj. Množenjem početne jednadžbe s 4, te dodavanjem jedinice dobivamo

$$4x^6 + 12x^3 + 5 = 4y^4 + 1.$$

Dobivena jednadžba ekvivalentna je

$$4x^6 + 12x^3 + 9 - 4y^4 = 5,$$

odnosno

$$(2x^3 + 3)^2 - 4y^4 = 5.$$

Uočimo da smo ovime dobili razliku kvadrata, pa imamo

$$(2x^3 + 3 - 2y^2)(2x^3 + 3 + 2y^2) = 5.$$

Za broj 5 imamo četiri moguća rastava na dva faktora, pa dobivamo sustave:

$$\begin{cases} 2x^3 + 3 - 2y^2 = 5 \\ 2x^3 + 3 + 2y^2 = 1, \end{cases} \qquad \begin{cases} 2x^3 + 3 - 2y^2 = 1 \\ 2x^3 + 3 + 2y^2 = 5, \end{cases}$$

$$\begin{cases} 2x^3 + 3 - 2y^2 = -5 \\ 2x^3 + 3 + 2y^2 = -1, \end{cases} \qquad \begin{cases} 2x^3 + 3 - 2y^2 = -1 \\ 2x^3 + 3 + 2y^2 = -5. \end{cases}$$

Njihovim rješavanjem dobivamo sva rješenja početne jednadžbe, a to su $(0, 1)$ i $(0, -1)$. ♢

Primjer 1.2. *Nađimo sve parove prirodnih brojeva (x, y) koji zadovoljavaju jednadžbu*

$$x^3 - y^3 = xy + 61.$$

Rješenje. Riješimo danu jednadžbu na dva načina.

1. način

Množenjem početne jednadžbe s 27 i oduzimanjem jedinice dobivamo

$$27x^3 - 27y^3 - 1 = 27xy + 1646.$$

Kako s lijeve strane jednakosti želimo umnožak, jednadžbu trebamo transformirati. Zapišimo ju u ekvivalentnom obliku

$$(3x)^3 + (-3y)^3 + (-1)^3 - 3(3x)(-3y)(-1) = 1646. \tag{1.1}$$

Budući da vrijedi

$$a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ac), \tag{1.2}$$

jednadžba (1.1) je ekvivalentna

$$(3x-3y-1)(9x^2+9y^2+1+9xy-3y+3x)=1646.$$

Desnu stranu u skupu prirodnih brojeva, do na poredak faktora, možemo zapisati kao $1646=1\cdot 1646=2\cdot 823$. Stoga bi, ako uključimo i predznake, imali osam mogućih sustava. No, budući da vrijedi

$$\begin{aligned} 3x-3y-1 &\equiv 2 \pmod 3,\\ 9x^2+9y^2+1+9xy-3y+3x &\equiv 1 \pmod 3,\end{aligned}$$

u obzir uzimamo četiri sustava:

$$\begin{cases} 3x-3y-1=2\\ 9x^2+9y^2+1+9xy+3x-3y=823, \end{cases} \qquad \begin{cases} 3x-3y-1=-823\\ 9x^2+9y^2+1+9xy+3x-3y=-2. \end{cases}$$

$$\begin{cases} 3x-3y-1=1646\\ 9x^2+9y^2+1+9xy+3x-3y=1, \end{cases} \qquad \begin{cases} 3x-3y-1=-1\\ 9x^2+9y^2+1+9xy+3x-3y=-1646. \end{cases}$$

Prvi sustav je ekvivalentan sustavu

$$\begin{cases} x-y=1\\ 3x^2+3y^2+3xy+x-y=274 \end{cases}$$

čija su rješenja $(6,5)$ i $(-5,-6)$, dok ostali sustavi nemaju realnih rješenja. Kako nas zanimaju samo prirodni brojevi koji su rješenja početne jednadžbe, zaključujemo da je jedino rješenje $(x,y)=(6,5)$.

2.način

Uočimo da mora vrijediti $x>y$. Neka je $x-y=d, d\in\mathbb{N}$. Uvrštavanjem $x=y+d$ u početnu jednadžbu dobivamo

$$3y^2d+3yd^2+d^3=y^2+yd+61,$$

odnosno

$$(3d-1)y^2+(3d^2-d)y+d^3=61. \tag{1.3}$$

Uočimo da vrijedi $d^3<61$ iz čega slijedi da je $d=1$, $d=2$ ili $d=3$.

Ako je $d = 1$, iz (1.3) dobivamo kvadratnu jednadžbu

$$y^2 + y - 30 = 0$$

čija su rješenja $y = 5$ i $y = -6$. Kako y mora biti prirodan broj i vrijedi $x = y + d$, dobivamo rješenje početne jednadžbe $(x, y) = (6, 5)$.

Ako je $d = 2$ ili $d = 3$ iz (1.3) dobivamo redom jednadžbe

$$5y^2 + 10y - 53 = 0,$$

$$4y^2 + 12y - 17 = 0$$

koje nemaju cjelobrojnih rješenja. Dakle, jedino rješenje početne jednadžbe je $(6, 5)$. ♢

Primjer 1.3. *Odredimo sve parove brojeva $x, y \in \mathbb{Z} \setminus \{0\}$ koji zadovoljavaju*

$$(x^2 + y)(x + y^2) = (x - y)^3.$$

Rješenje. Iz početne jednadžbe raspisivanjem dobivamo

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

Uočimo da svaki član sadrži y, pa podijelimo jednadžbu s njim (što smijemo zbog uvjeta $y \neq 0$). Zatim grupiranjem članova dobivamo kvadratnu jednadžbu

$$2y^2 + (x^2 - 3x)y + (x + 3x^2) = 0.$$

Jednadžba ima cjelobrojna rješenja ako i samo ako je njena diskriminanta jednaka broju koji je potpun kvadrat. Dobivamo $D = x(x+1)^2(x-8)$, iz čega slijedi $x(x-8) = z^2$. Zapisivanjem te jednadžbe u ekvivalentnom obliku

$$(x - 4)^2 - z^2 = 16$$

uočavamo razliku kvadrata, pa slijedi

$$(x - 4 - z)(x - 4 + z) = 16.$$

Stoga je

$$\begin{cases} x - 4 - z = d_1 \\ x - 4 + z = d_2, \end{cases}$$

gdje su d_1 i d_2 cijeli brojevi takvi da je $d_1 d_2 = 16$. Slijedi

$$x = \frac{d_1 + d_2}{2} + 4.$$

Kako je x cjelobrojan, tražimo samo one cjelobrojne djelitelje od 16, do na poredak, koji imaju paran zbroj i umnožak im je 16:

$$(d_1, d_2) \in \{(2,8), (-2,-8), (4,4), (-4,-4)\}.$$

Zbog uvjeta $x \neq 0$, konačno dobivamo da je $x \in \{-1, 8, 9\}$. Iz toga slijedi da su rješenja početne jednadžbe $(-1,-1), (8,-10), (9,-6)$ i $(9,-21)$. ♢

Primjer 1.4. *Odredimo sve cijele brojeve n za koje jednadžba*

$$x^3 + y^3 + z^3 - 3xyz = n$$

ima rješenja u prirodnim brojevima.

Rješenje. Prvo uočimo da jednadžba ima rješenja za $n = 0$ (u slučaju $x = y = z$).

Ponovno koristimo jednakost (1.2) koju možemo zapisati kao

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z) \cdot \frac{1}{2}((x-y)^2 + (y-z)^2 + (z-x)^2) \tag{1.4}$$

i

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)^3 - 3(x + y + z)(xy + yz + xz) \tag{1.5}$$

Razlikujemo slučajeve s obzirom na ostatke pri dijeljenju s 3:

Slučaj I. Neka je $n = 3k + 1, k \in \mathbb{Z}$. Iz (1.4) dobivamo sustav jednadžbi

$$\begin{cases} \frac{1}{2}((x-y)^2 + (y-z)^2 + (z-x)^2) = 1 \\ x + y + z = 3k + 1. \end{cases}$$

Uvođenjem supstitucije $x = 3k + 1 - y - z$ i sređivanjem dobivamo

$$3k^2 + y^2 + z^2 - 3ky - 3kz - y - z + yz + 2k = 0.$$

Neka je $z = k, k \geq 1$. Iz toga slijedi da su trojke oblika $(k+1, k, k)$ i $(k, k+1, k)$ za $k \geq 1$ rješenja dane jednadžbe.

Slučaj II. Neka je $n = 3k + 2, k \in \mathbb{Z}$. Analognim postupkom kao u prethodnom slučaju dobivamo da su trojke oblika $(k+1, k+1, k)$ za $k \geq 1$ rješenja početne jednadžbe.

Slučaj III. Neka je n djeljiv s 3. Tada iz (1.5) slijedi da je izraz $x + y + z$ djeljiv s 3, pa je $n = x^3 + y^3 + z^3 - 3xyz$ djeljiv s 9, odnosno $n = 9k, k \in \mathbb{Z}$. Iz sustava jednadžbi

$$\begin{cases} \frac{1}{2}((x-y)^2 + (y-z)^2 + (z-x)^2) = 3 \\ x + y + z = 3k \end{cases}$$

analognim postupkom dobivamo da trojke oblika $(k+1, k-1, k)$ i $(k-1, k+1, k), k \geq 2$ zadovoljavaju početnu jednadžbu.

Dakle, traženi cijeli brojevi n su $n = 3k+1, k \geq 1$, $n = 3k+2, k \geq 1$ i $n = 9k$, $k = 0$ ili $k \geq 2$. $\diamondsuit$

1.2 Metoda matematičke indukcije

Metoda matematičke indukcije ima široku primjenu u različitim područjima matematike, pa tako i u teoriji brojeva. Možemo ju koristiti ako varijabla o kojoj tvrdnja ovisi poprima vrijednosti iz skupa prirodnih brojeva. Odnosno, primjenjujemo ju ako želimo dokazati da je tvrdnja $P(n)$ istinita za sve $n \geq n_0$, $n_0 \in \mathbb{N}$. Ova metoda se zasniva na *Peanovom aksiomu* koji glasi:

Neka je $M \subseteq \mathbb{N}$. Ako vrijedi

1. $1 \in M$,
2. za svaki $n \in \mathbb{N}$, $n \in M$ povlači da je $n+1 \in M$,

onda je $M = \mathbb{N}$.

Navedeni Peanov aksiom naziva se još *princip matematičke indukcije* koji se u konkretnoj primjeni pojavljuje u nekoliko oblika. Najčešće se koristi sljedeći:

Neka je $n_0 \in \mathbb{N}$. Ako za tvrdnju $P(n)$ vrijedi

(i) da je istinita za $n = n_0$,

(ii) da iz istinosti tvrdnje $P(n)$ za $n \geq n_0$ slijedi istinitost tvrdnje $P(n+1)$,

onda je tvdnja $P(n)$ istinita za svaki prirodni broj $n \geq n_0$. Obično ističemo tzv. tri koraka u primjeni principa matematičke indukcije:

(a) *baza indukcije*: provjera istinitosti tvrdnje $P(n_0)$,

(b) *pretpostavka indukcije*: pretpostavimo da je tvrdnja $P(i)$ istinita za $i \geq n_0$,

(c) *korak indukcije*: uz pretpostavku (b) dokazujemo istinitost tvrdnje $P(i+1)$.

Koristan je i sljedeći oblik principa matematičke indukcije s tzv. većim korakom, odnosno s korakom $k \in \mathbb{N}$:

(a) *baza indukcije*: provjera istinitosti tvrdnji $P(n_0)$, $P(n_0+1)$, ..., $P(n_0+k-1)$,

(b) *pretpostavka indukcije*: pretpostavimo da je tvrdnja $P(i)$ istinita za $i \geq n_0$,

(c) *korak indukcije*: uz pretpostavku (b) dokazujemo istinitost tvrdnje $P(i+k)$.

Primjenu principa matematičke indukcije u rješavanju diofantskih jednadžbi ilustrirat ćemo na nizu primjera.

Primjer 1.5. *Dokažimo da za sve prirodne brojeve $k \geq 3$ postoje neparni prirodni brojevi x, y koji zadovoljavaju jednadžbu*

$$7x^2 + y^2 = 2^k. \tag{1.6}$$

Rješenje. Za dani $n \in \mathbb{N}$ i $k = n$, označimo rješenje od (1.6) s (x_n, y_n).

Baza indukcije: Za $k = 3$ jednadžba (1.6) glasi

$$7x_3^2 + y_3^2 = 8.$$

Lako se provjeri da je $(x_3, y_3) = (1, 1)$ njeno rješenje.

Pretpostavka indukcije: Pretpostavimo sada da za neki $n \geq 3$ tvrdnja vrijedi za $k = n$, odnosno postoji rješenje (x_n, y_n) jednadžbe (1.6) takvo da su x_n i y_n neparni prirodni brojevi.

Korak indukcije: Vrijedi

$$7\left(\frac{x_n \pm y_n}{2}\right)^2 + \left(\frac{7x_n \mp y_n}{2}\right)^2 = \frac{1}{4}(56x_n^2 + 8y_n^2) = 2(7x_n^2 + y_n^2) = 2^{n+1}.$$

Stoga su

$$\left(\frac{x_n + y_n}{2}, \frac{|7x_n - y_n|}{2}\right), \left(\frac{|x_n - y_n|}{2}, \frac{7x_n + y_n}{2}\right)$$

rješenja u skupu prirodnih brojeva jednadžbe

$$7x^2 + y^2 = 2^{n+1}.$$

Još treba pokazati da su u barem jednoj od mogućnosti obje komponente rješenja neparni brojevi. Imamo dvije mogućnosti.

(i) Prepostavimo da je $\frac{x_n+y_n}{2}$ neparan broj. Tada je

$$(x_n, y_n) \equiv (1, 1) \pmod 4 \text{ ili } (x_n, y_n) \equiv (3, 3) \pmod 4.$$

Otuda je

$$7x_n - y_n \equiv 2 \pmod 4$$

u oba slučaja. Dakle, $\frac{|7x_n-y_n|}{2}$ je neparan broj, odnosno

$$(x_{n+1}, y_{n+1}) = \left(\frac{x_n + y_n}{2}, \frac{|7x_n - y_n|}{2}\right)$$

je rješenje od (1.6) za $k = n + 1$ takvo da su x_{n+1} i y_{n+1} neparni.

(ii) Prepostavimo da je $\frac{x_n+y_n}{2}$ paran broj. Tada je

$$(x_n, y_n) \equiv (1,3) \pmod 4 \text{ ili } (x_n, y_n) \equiv (3,1) \pmod 4.$$

Otuda je

$$x_n - y_n \equiv 2 \pmod 4,\ 7x_n + y_n \equiv 2 \pmod 4$$

pa su $\frac{|x_n-y_n|}{2}$, $\frac{7x_n+y_n}{2}$ neparni brojevi. Dakle,

$$(x_{n+1}, y_{n+1}) = \left(\frac{|x_n - y_n|}{2}, \frac{7x_n + y_n}{2}\right)$$

je rješenje od (1.6) za $k = n+1$ takvo da su x_{n+1} i y_{n+1} neparni.

Stoga prema principu matematičke indukcije jednadžba (1.6) ima rješenje u skupu neparnih prirodnih brojeva za svaki prirodan broj $k \geq 3$. ♢

Primjer 1.6. *Dokažimo da za sve prirodne brojeve n jednadžba*

$$x^2 + y^2 + z^2 = 59^n \tag{1.7}$$

ima rješenja u prirodnim brojevima.

Rješenje. U ovom primjeru koristit ćemo princip matematičke indukcije s korakom $k = 2$. Za fiksan $n \in \mathbb{N}$ označimo rješenje od (1.7) u skupu prirodnih brojeva s (x_n, y_n, z_n).

Baza indukcije: Jednadžbe

$$x^2 + y^2 + z^2 = 59, \quad x^2 + y^2 + z^2 = 59^2$$

imaju redom rješenja $(x_1, y_1, z_1) = (1, 3, 7)$ i $(x_2, y_2, z_2) = (14, 39, 42)$. Stoga tvrdnja vrijedi za $n = 1$ i $n = 2$.

Pretpostavka indukcije: Pretpostavimo sada da za neki $n \geq 1$ postoji rješenje $(x_n, y_n, z_n) \in \mathbb{N}^3$ jednadžbe (1.7).

Korak indukcije: Prema pretpostavci indukcije je

$$x_n^2 + y_n^2 + z_n^2 = 59^n.$$

Množenjem prethodne jednakosti s 59^2 slijedi

$$(59x_n)^2 + (59y_n)^2 + (59z_n)^2 = 59^{n+2}$$

pa je

$$(x_{n+2}, y_{n+2}, z_{n+2}) = (59x_n, 59y_n, 59z_n)$$

rješenje jednadžbe $x^2 + y^2 + z^2 = 59^{n+2}$ u skupu prirodnih brojeva.

Prema principu matematičke indukcije, s korakom 2, pokazali smo da za svaki $n \in \mathbb{N}$ jednadžba (1.7) ima rješenje u skupu prirodnih brojeva. Štoviše, za $n = 2k-1$, $k \in \mathbb{N}$, rješenje od (1.7) glasi:

$$(x_{2k-1}, y_{2k-1}, z_{2k-1}) = (1 \cdot 59^{k-1}, 3 \cdot 59^{k-1}, 7 \cdot 59^{k-1}),$$

a za $n = 2k$:

$$(x_{2k}, y_{2k}, z_{2k}) = (14 \cdot 59^{k-1}, 39 \cdot 59^{k-1}, 42 \cdot 59^{k-1}).$$

♢

Primjer 1.7. *Dokažimo da jednadžba*

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = \frac{n+1}{x_{n+1}^2} \tag{1.8}$$

ima rješenja u prirodnim brojevima ako i samo ako $n \geq 3$.

Rješenje. Pokažimo prvo da jednadžba (1.8) nema rješenja za $n = 1$ i $n = 2$. Za $n = 1$ imamo

$$\frac{1}{x_1^2} = \frac{2}{x_2^2},$$

odnosno $\sqrt{2}x_1 = x_2$, što nema rješenja jer je $\sqrt{2}$ iracionalan broj a $\frac{x_2}{x_1}$ je racionalan.

Neka je sada $n = 2$. Tada imamo

$$(x_2x_3)^2 + (x_1x_3)^2 = 3(x_1x_2)^2.$$

Za $1 \leq i \leq 3$, neka je $x_i = 3^{n_i}y_i$, gdje je y_i prirodan broj koji nije djeljiv s 3. Imamo

$$3^{2(n_2+n_3)}(y_2y_3)^2 + 3^{2(n_1+n_3)}(y_1y_3)^2 = 3^{2(n_1+n_2)+1}(y_1y_2)^2.$$

Bez smanjenja općenitosti, pretpostavimo da je $n_1 \geq n_2$ pa dobivamo

$$3^{2(n_2+n_3)}((y_2y_3)^2 + 3^{2(n_1-n_2)}(y_1y_3)^2) = 3^{2(n_1+n_2)+1}(y_1y_2)^2. \tag{1.9}$$

Znamo da je 1 jedini kvadratni ostatak modulo 3, pa iz toga slijedi

$$(y_2y_3)^2 + 3^{2(n_1-n_2)}(y_1y_3)^2 \equiv 1 \quad \text{ili} \quad 2 \pmod 3.$$

S druge strane je

$$3^{2(n_1+n_2)+1}(y_1y_2)^2 \equiv 0 \pmod 3,$$

pa jednadžba (1.8) nema rješenja za $n = 2$.

Sada metodom matematičke indukcije pokazujemo da je jednadžba (1.8) rješiva u skupu prirodnih brojeva za sve $n \geq 3$.

Baza indukcije: Neka je $n = 3$. U ovom slučaju želimo pronaći barem jedno rješenje početne jednadžbe. Počnimo od jednakosti $4^2 + 3^2 = 5^2$. Dijeljenjem s $3^2 4^2 5^2$, a zatim množenjem s $\frac{1}{12^2}$ dobivamo

$$\frac{1}{12^2 \cdot 15^2} + \frac{1}{12^2 \cdot 20^2} = \frac{1}{12^4}.$$

Kako bismo odredili tražena rješenja, uočimo da obje strane dobivene jednakosti moramo transformirati. Imamo

$$\frac{1}{12^2 \cdot 15^2} + \left(\frac{1}{15^2} + \frac{1}{20^2}\right)\frac{1}{20^2} = \frac{4}{4 \cdot 12^4},$$

odnosno

$$\frac{1}{(12 \cdot 15)^2} + \frac{1}{(15 \cdot 20)^2} + \frac{1}{(20 \cdot 20)^2} = \frac{4}{(2 \cdot 12^2)^2}.$$

Dakle, dobili smo da za $n = 3$ jednadžba (1.8) ima rješenje

$$(x_1, x_2, x_3, x_4) = (12 \cdot 15, 15 \cdot 20, 20 \cdot 20, 2 \cdot 12^2).$$

Pretpostavka indukcije: Neka je $k \in \mathbb{N}$ i $k \geq 3$. Pretpostavimo da je $(a_1, a_2, \ldots, a_{k+1}) \in \mathbb{N}^{k+1}$ rješenje jednadžbe (1.8) za $n = k$, odnosno

$$\frac{1}{a_1^2} + \frac{1}{a_2^2} + \cdots + \frac{1}{a_k^2} = \frac{k+1}{a_{k+1}^2}. \tag{1.10}$$

Korak indukcije: Pribrajanjem $\frac{1}{a_{k+1}^2}$ jednakosti (1.10) dobivamo

$$\frac{1}{a^2} + \cdots + \frac{1}{a_k^2} + \frac{1}{a_{k+1}^2} = \frac{k+1}{a_{k+1}^2} + \frac{1}{a_{k+1}^2} = \frac{k+2}{a_{k+1}^2},$$

čime smo pokazali da je

$$(x_1, x_2, \ldots, x_k, x_{k+1}, x_{k+2}) = (a_1, a_2, \ldots, a_k, a_{k+1}, a_{k+1})$$

rješenje jednadžbe (1.8) za $n = k + 1$. ♢

Napomena 1.8. Dokaz da jednadžba (1.8) za $n = 2$ nema rješenja mogli smo provesti i na drugi način. Naime, jednadžbu $(x_2 x_3)^2 + (x_1 x_3)^2 = 3(x_1 x_3)^2$ možemo zapisati kao

$$a^2 + b^2 = 3c^2.$$

Uz pretpostavku da su a, b i c različiti od nule i relativno prosti, znamo da kvadrat cijelog broja daje ostatak 0 ili 1 pri dijeljenju s 3, iz čega zaključujemo da su i a i b djeljivi s 3. S obzirom da u jednadžbi imamo njihove kvadrate, slijedi da je i c djeljiv s 3, što je u kontradikciji s pretpostavkom.

Napomena 1.9. Uočimo da je

$$(x_1, x_2, x_3, x_4) = (3, 3, 6, 4)$$

rješenje jednadžbe (1.8) za $n = 3$, odnosno vrijedi

$$\frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{6^2} = \frac{4}{4^2}.$$

Ako prethodnoj jednakosti $n-3$ puta pribrojimo $\frac{1}{4^2}$, za proizvoljan $n > 3$, dobivamo

$$\frac{1}{3^2} + \frac{1}{3^2} + \frac{1}{6^2} + \underbrace{\frac{1}{4^2} + \cdots + \frac{1}{4^2}}_{n-3} = \frac{4}{4^2} + \frac{n-3}{4^2} = \frac{n+1}{4^2}.$$

To znači da je

$$(x_1, x_2, x_3, x_4, x_5, \ldots, x_{n+1}) = (3, 3, 6, 4, \underbrace{4, \ldots, 4}_{n-3})$$

jedno rješenje u skupu $\mathbb{N}$ od (1.8), za $n \geq 4$.

Za rješavanje sljedećeg primjera potrebna nam je sljedeća pomoćna tvrdnja koju ćemo također pokazati primjenom principa matematičke indukcije.

Lema 1.10. *Ako je $a_1, a_2, \ldots$ niz različitih prirodnih brojeva, tada za sve prirodne brojeve n vrijedi*

$$a_1^3 + \cdots + a_n^3 \geq (a_1 + \cdots + a_n)^2.$$

Dokaz. Bez smanjenja općenitosti, pretpostavimo da vrijedi $a_1 < a_2 < \cdots < a_n$.

Baza indukcije: Za $n = 1$ je $a_1^3 \geq a_1^2$, što je ekvivalentno $a_1^2(a_1 - 1) \geq 0$ i očito vrijedi jer je $a_1 \geq 1$.

Pretpostavka indukcije: Pretpostavimo da tvrdnja propozicije vrijedi za neki $n = k$, te da su $a_1 < a_2 < \cdots < a_k < a_{k+1}$ različiti prirodni brojevi.

Korak indukcije: Kako je $a_{k+1} > a_k$ te stoga i $a_{k+1} \geq a_k + 1$, vrijedi nejednakost

$$\frac{(a_{k+1} - 1)a_{k+1}}{2} \geq \frac{a_k(a_k + 1)}{2} = 1 + 2 + \cdots + a_k.$$

Uočimo da suma $1 + 2 + \cdots + a_k$ sadrži sve prirodne brojeve manje ili jednake a_k, te da je ona veća ili jednaka sumi $a_1 + a_2 + \cdots + a_k$ koja sadrži različite prirodne brojeve manje ili jednake a_k. Iz toga slijedi

$$\frac{(a_{k+1} - 1)a_{k+1}}{2} \geq a_1 + a_2 + \cdots + a_k.$$

Množenjem s $2a_{k+1}$ i sređivanjem dobivamo

$$a_{k+1}^3 \geq 2(a_1 + a_2 + \cdots + a_k)a_{k+1} + a_{k+1}^2.$$

S druge strane, pretpostavili smo da vrijedi

$$a_1^3 + a_2^3 + \cdots + a_k^3 \geq (a_1 + a_2 + \cdots + a_k)^2.$$

Iz toga slijedi

$$a_1^3 + a_2^3 + \cdots + a_k^3 + a_{k+1}^3 \geq (a_1 + a_2 + \cdots + a_{k+1})^2.$$

□

Primjer 1.11. *Odredimo sva rješenja jednadžbe*

$$x_1^3 + x_2^3 + \cdots + x_m^3 = (x_1 + x_2 + \cdots + x_m)^2,$$

gdje su $x_1, \ldots, x_m$ različiti prirodni brojevi.

Rješenje. Pretpostavimo, najprije, da vrijedi $x_1 < x_2 < \cdots < x_m$. Otuda, kako su rješenja jednadžbe različiti prirodni brojevi, slijedi da je $x_1 \geq 1, x_2 \geq 2, \ldots, x_m \geq m$. Mi ćemo pokazati da je $x_1 = 1, x_2 = 2, \ldots, x_m = m$.

Iz svega pretpostavljenog, očito je da vrijedi

$$x_{m-1} \leq x_m - 1, x_{m-2} \leq x_m - 2, \ldots, x_1 \leq x_m - (m-1),$$

iz čega dobivamo

$$x_1 + x_2 + \cdots + x_{m-1} \leq (m-1)x_m - \frac{(m-1)m}{2}. \tag{1.11}$$

Iz Leme 1.10 slijedi

$$x_1^3 + x_2^3 + \cdots + x_{m-1}^3 \geq (x_1 + x_2 + \cdots + x_{m-1})^2. \tag{1.12}$$

S druge strane, početnu jednadžbu možemo zapisati u obliku

$$x_1^3+x_2^3+\cdots+x_{m-1}^3+x_m^3 = (x_1+x_2+\cdots+x_{m-1})^2+2(x_1+x_2+\cdots+x_{m-1})x_m+x_m^2. \tag{1.13}$$

Koristeći (1.12) dobivamo

$$x_m^3 \leq 2(x_1 + x_2 + \cdots + x_{m-1})x_m + x_m^2.$$

dijeljenjem prethodne relacije s x_m, $x_m \in \mathbb{N}$, dobivamo

$$x_m^2 \leq 2(x_1 + x_2 + \cdots + x_{m-1}) + x_m.$$

Iz (1.11) slijedi

$$x_m^2 \leq 2(m-1)x_m - (m-1)m + x_m$$

odnosno

$$(x_m - m)(x_m - (m-1)) \leq 0.$$

Znamo da vrijedi $x_m > m-1$, pa iz prethodne nejednakosti slijedi da je $x_m \leq m$. Kako tražimo različite prirodne brojeve $x_1, x_2, \ldots, x_m$, zaključujemo da vrijedi $x_m = m$, odnosno

$$x_1 = 1, x_2 = 2, \ldots, x_m = m.$$

Dakle, sva rješenja početne jednadžbe su oblika $(p(1), p(2), \ldots, p(m))$, gdje je p permutacija skupa $\{1, 2, \ldots, m\}$. ♢

1.3 Parametarska metoda

U nekim slučajevima cjelobrojna rješenja diofantske jednadžbe

$$f(x_1, x_2, \ldots, x_n) = 0$$

mogu se zapisati parametarski kao

$$x_1 = g_1(k_1, \ldots, k_l), \quad x_2 = g_2(k_1, ..., k_l), \ldots, x_n = g_n(k_1, \ldots, k_l)$$

gdje su $g_1, g_2, \ldots, g_n$ cjelobrojne funkcije više varijabli. Parametarski zapis rješenja diofantske jednadžbe ne mora biti jedinstven.

Ovom metodom često ne tražimo sva rješenja danih jednadžbi eksplicitno, već dokazujemo postojanje beskonačno mnogo rješenja. Prikažimo kako se ona koristi na primjerima.

Primjer 1.12. .

a) Neka su m i n različiti prirodni brojevi. Dokažimo da postoji beskonačno mnogo trojki (x, y, z) prirodnih brojeva koje zadovoljavaju

$$x^2 + y^2 = (m^2 + n^2)^z$$

gdje je

i) z neparan,

ii) z paran.

b) Dokažimo da postoji beskonačno mnogo trojki (x, y, z) prirodnih brojeva koje zadovoljavaju jednadžbu

$$x^2 + y^2 = 13^z.$$

Rješenje. a) Razlikujemo dva slučaja za z neparan, odnosno paran.

i) Neka je $z = 2k + 1, k \in \mathbb{N}_0$. Uvrštavanjem u početnu jednadžbu dobivamo

$$x^2 + y^2 = m^2(m^2 + n^2)^{2k} + n^2(m^2 + n^2)^{2k},$$

iz čega slijedi $x^2 = \left(m(m^2 + n^2)^k\right)^2$ i $y^2 = \left(n(m^2 + n^2)^k\right)^2$. Kako su x i y prirodni brojevi, zaključujemo da postoji beskonačno mnogo rješenja početne jednadžbe oblika

$$(x, y, z) = (m(m^2 + n^2)^k, n(m^2 + n^2)^k, 2k + 1), k \in \mathbb{N}_0.$$

ii) Neka je $z = 2k, k \in \mathbb{N}$. Ponovno, uvrštavanjem u početnu jednadžbu i sređivanjem dobivamo

$$x^2 + y^2 = \left((m^2 + n^2)^{k-1}\right)^2 (m^2 - n^2)^2 + \left((m^2 + n^2)^{k-1}\right)^2 4m^2n^2$$

iz čega slijedi da i u ovom slučaju postoji beskonačno mnogo rješenja početne jednadžbe, a ona su oblika

$$(x, y, z) = (|m^2 - n^2|(m^2 + n^2)^{k-1}, 2mn(m^2 + n^2)^{k-1}, 2k), k \in \mathbb{N}.$$

b) Usporedimo li ovu jednadžbu s jednadžbom u a) dijelu zadatka, možemo uočiti $m^2 + n^2 = 13$, što vrijedi za $m = 2$ i $n = 3$. Kako smo već odredili trojke koje su rješenja dane jednadžbe, uvrštavanjem odabranih m i n dobivamo

$$(x', y', z') = (2 \cdot 13^k, 3 \cdot 13^k, 2k + 1), k \in \mathbb{N}_0$$

za z neparan, te

$$(x'', y'', z'') = (5 \cdot 13^{k-1}, 12 \cdot 13^{k-1}, 2k), k \in \mathbb{N}$$

za z paran. Time smo dokazali da zadana jednadžba ima beskonačno mnogo rješenja u prirodnim brojevima.

♢

Primjer 1.13. *Dokažimo da postoji beskonačno mnogo trojki (x, y, z) cijelih brojeva takvih da vrijedi*

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

Rješenje. Kako ne tražimo sva rješenja dane jednadžbe, možemo staviti $z = -y$ kako bismo eliminirali nepoznanicu z. Tada početna jednadžba glasi

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

Neka je sada $y = mx, m \in \mathbb{Z}$, te $x \neq 0$ iz čega dobivamo

$$x = 1 + 2m^2.$$

Time smo dobili beskonačno mnogo rješenja početne jednadžbe, a to su

$$(x, y, z) = (2m^2 + 1, m(2m^2 + 1), -m(2m^2 + 1)), m \in \mathbb{Z}.$$

♢

Primjer 1.14. *Dokažimo da postoji beskonačno mnogo trojki (x, y, z) prirodnih brojeva koji zadovoljavaju*

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}. \tag{1.14}$$

Rješenje. Početna jednadžba (1.14) ekvivalentna je

$$z = \frac{xy}{x + y}.$$

Neka je $\gcd(x, y) = d$. Tada je $x = dm, y = dn$, gdje je $\gcd(m, n) = 1$. Iz toga slijedi $\gcd(mn, m + n) = 1$, te

$$z = \frac{dmn}{m + n}.$$

Uočimo da tada vrijedi $(m + n)|d$, odnosno $d = k(m + n), k \in \mathbb{N}$. Dakle, jednadžba (1.14) ima beskonačno mnogo rješenja i to su

$$(x, y, z) = (km(m + n), kn(m + n), kmn), k, m, n \in \mathbb{N}.$$

♢

Napomenimo da je jednadžba (1.14) ekvivalentna polinomijalnoj, odnosno diofantskoj jednadžbi drugog stupnja

$$yz + xz = xy,$$

za $x, y, z \neq 0$.

1.4 Gaussovi cijeli brojevi

Skup Gaussovih cijelih brojeva najjednostavnije možemo opisati kao proširenje skupa cijelih brojeva $\mathbb{Z}$. Zapisujemo ga kao

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

gdje je $i^2 = -1$ *imaginarna jedinica*. Skup $\mathbb{Z}[i]$ je komutativan prsten s jedinicom, 1, uz operacije zbrajanja i množenja definiranih s

$$(a + bi) + (c + di) = a + c + (b + d)i,$$

$$(a + bi) \cdot (c + di) = ac - bd + (ad + bc)i,$$

za $a, b, c, d \in \mathbb{Z}$. Gaussove cijele brojeve koristimo za proučavanje sume dvaju kvadrata, jer ju u skupu $\mathbb{Z}[i]$ možemo faktorizirati na sljedeći način

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

Za $\alpha = a + bi \in \mathbb{Z}[i]$, definiramo normu od α kao

$$N(\alpha) = a^2 + b^2$$

što je očito nenegativan cijeli broj. Navedena norma ima svojstvo multiplikativnosti, odnosno $N(\alpha\beta) = N(\alpha)N(\beta)$.

Već smo spomenuli faktorizaciju Gaussovih cijelih brojeva. Za nju najprije trebamo definirati što je prost Gaussov cijeli broj, a za to trebamo poznavati skup invertibilnih elemenata u $\mathbb{Z}[i]$.

Definicija 1.15. *Kažemo da je $\alpha \in \mathbb{Z}[i]$* invertibilni element *ako postoji $\beta \in \mathbb{Z}[i]$ takav da vrijedi $\alpha\beta = \beta\alpha = 1$. Pišemo, $\beta = \alpha^{-1}$ i nazivamo ga inverzom od α.*

Napominjemo da ako je neki element, općenito, monoida invertibilan, onda je njegov inverz jedinstven.

Teorem 1.16. *Skup svih invertibilnih elemenata u prstenu $\mathbb{Z}[i]$ je $\{1, -1, i, -i\}$. Element iz $\mathbb{Z}[i]$ je invertibilan ako i samo mu je norma jednaka 1.*

Dokaz. Očito je svaki od elemenata iz $\{1, -1, i, -i\}$ invertibilan i ima normu 1. Neka je $u \in \mathbb{Z}[i]$ invertibilan element. Tada postoji $v \in \mathbb{Z}[i]$ takav da vrijedi $uv = 1$, što zbog multiplikativnosti norme povlači da je $N(u)N(v) = 1$. Kako je norma nenegativna, zaključujemo $N(u) = N(v) = 1$, odnosno ako je $u = a + bi$, slijedi $a^2 + b^2 = 1$. Jedina rješenja ove jednadžbe u $\mathbb{Z}$ su $(a, b) = (\pm 1, 0)$ i $(a, b) = (0, \pm 1)$. Dakle, jedini invertibilni elementi u skupu $\mathbb{Z}[i]$ su $\pm 1, \pm i$. □

Općenito ćemo invertibilni element skupa $\mathbb{Z}[i]$ odnosno tzv. *jedinicu* označavati s u. Skup svih invertibilnih elemenata u $\mathbb{Z}[i]$ (odnosno općenito u monoidu) čini multiplikativnu grupu koju nazivamo *grupa jedinica*.

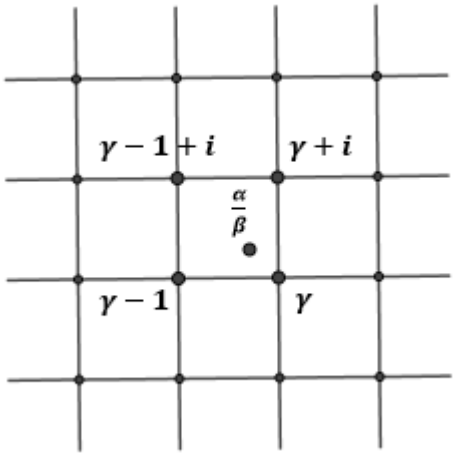
Kao i u prstenu $\mathbb{Z}$, u prstenu $\mathbb{Z}[i]$ postoji analogan Teorem o dijeljenju s ostatkom.

Teorem 1.17. *Za sve $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, postoje γ i ρ iz skupa $\mathbb{Z}[i]$ takvi da vrijedi*

$$\alpha = \beta\gamma + \rho, \quad N(\rho) \leq \frac{1}{2}N(\beta) < N(\beta).$$

Dokaz. Norma u $\mathbb{Z}[i]$ je blisko povezana sa apsolutnom vrijednosti kompleksnih brojeva, točnije $N(a + bi) = |a + bi|^2$. Apsolutnom vrijednosti kompleksnih brojeva mjerimo udaljenosti, te ćemo tu činjenicu iskoristiti u ovom dokazu. Uočimo da za svaki kompleksan broj z postoji neki $w \in \mathbb{Z}[i]$ takav da udaljenost među njima nije veća od $\frac{\sqrt{2}}{2}$, odnosno $|z - w| \leq \frac{\sqrt{2}}{2}$. Naime, točke iz $\mathbb{Z}[i]$ čine u kompleksnoj ravnini kvadratnu rešetku. Svaki od kvadratića iz rešetke je dimenzije 1×1, a točka koja je najviše udaljena (za $\frac{\sqrt{2}}{2}$) nekom od vrhova nalazi se u središtu kvadratića.

Promotrimo omjer $\frac{\alpha}{\beta}$ kao kompleksan broj, odnosno točku kompleksne ravnine. Tada postoji jedinični kvadratić čiji su vrhovi iz $\mathbb{Z}[i]$ koji ju sadrži. Pretpostavimo da je $\gamma \in \mathbb{Z}[i]$ vrh kvadrata koji je najbliži točki $\frac{\alpha}{\beta}$.



Slika 1.1: Gaussovi cijeli brojevi

Tada vrijedi

$$\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{\sqrt{2}}{2}.$$

Množenjem sa $|\beta|$, te kvadriranjem dobivamo

$$N(\alpha - \beta\gamma) \leq \frac{1}{2}N(\beta).$$

Stavimo još $\rho = \alpha - \beta\gamma$, čime je tvrdnja dokazana. □

Uočimo da u skupu Gaussovih cijelih brojeva γ i ρ nisu jedinstveni. Na primjer, za $\alpha = 37 + 2i$ i $\beta = 11 + 2i$ imamo

$$\alpha = \beta \cdot 3 + (4 - 4i) = \beta \cdot (3 - i) + (2 + 7i).$$

U ovom slučaju oba ostatka imaju normu manju od $\frac{1}{2}N(\beta)$. Također, iz prethodnog teorema možemo uočiti geometrijsko objašnjenje zašto γ i ρ nisu jedinstveni.

Uočimo da za svaki $a \in \mathbb{Z}[i]$, $a \neq 0$, postoje djelitelji koji se lako mogu odrediti. To su jedinice, te elementi dobiveni množenjem a sa svakom od jedinica. Te djelitelje, norme 1 i norme $N(a)$ nazivamo *trivijalnim djeliteljima* ili *trivijalnim faktorima* od a. Dakle, točno je osam trivijalnih faktora od a i to su $\pm 1, \pm i, \pm a, \pm ia$. Ostale faktore, odnosno djelitelje od a nazivamo *netrivijalnim*. Ako je b netrivijalni djelitelj od a, onda vrijedi da je $1 < N(b) < N(a)$.

Definicija 1.18. *Za Gaussov cijeli broj a, $N(a) > 1$, kažemo da je* prost Gaussov cijeli broj *ako su jedini njegovi djelitelji trivijalni. U suprotnom, a je* složen Gaussov cijeli broj.

Navedimo nekoliko prostih Gaussovih cijelih brojeva:

$$1 + i, \quad 1 - i, \quad 3, \quad 1 - 2i, \quad 7, \quad 2 + 3i$$

Uočimo da npr. broj 2 nije prost Gaussov cijeli broj jer vrijedi

$$2 = (1 + i)(1 - i).$$

Definicija 1.19. *Kažemo da su $a, b \in \mathbb{Z}[i]$* relativno prosti *ako su im jedini zajednički djelitelji invertibilni elementi.*

Teorem 1.20. *Svaki $\alpha \in \mathbb{Z}[i], \alpha \neq 0, N(\alpha) > 1$, ima jedinstven rastav na proste faktore do na poredak i množenje invertibilnim elementima.*

Dokaz. Pretpostavimo da α ima dvije različite faktorizacije

$$\alpha = \beta_1 \cdot \beta_2 \cdots \beta_r$$

$$\alpha = \beta_1' \cdot \beta_2' \cdots \beta_s'$$

gdje su $\beta_1, \beta_2, \ldots, \beta_r$ i $\beta_1', \beta_2', \ldots, \beta_s'$ prosti Gaussovi cijeli brojevi, te da vrijedi

$$\beta_1 \cdot \beta_2 \cdots \beta_r = \beta_1' \cdot \beta_2' \cdots \beta_s'$$

uz uvjet $\beta_i \neq u\beta_j'$, za sve $i \in \{1, 2, \ldots, r\}, j \in \{1, 2, \ldots, s\}$, gdje je u invertibilni element. Očito $\beta_1 | \alpha$ iz čega slijedi $\beta_1 | \beta_1' \cdot \beta_2' \cdots \beta_s'$. Iz činjenice da je β_1 prost slijedi $\beta_1 | \beta_1'$ ili $\beta_1 | \beta_2' \cdot \beta_3' \cdots \beta_s'$. Pretpostavimo da vrijedi $\beta_1 | \beta_1'$ iz čega dobivamo kontradikciju s pretpostavkom $\beta_i \neq u\beta_j'$. Ponavljanjem ovog postupka u svim slučajevima dobivamo kontradikciju, pa zaključujemo da je rastav Gaussovih cijelih brojeva na proste faktore jedinstven do na poredak i množenje invertibilnim elementima. □

Kroz nekoliko primjera pokazat ćemo se kako se pri rješavanju diofantskih jednadžbi pojavljuju Gaussovi cijeli brojevi.

Primjer 1.21. *Odredimo sva rješenja Pitagorine jednadžbe*

$$x^2 + y^2 = z^2.$$

Rješenje. Za rješavanje dane jednadžbe koristimo jedinstvenost rastava na proste faktore u skupu $\mathbb{Z}[i]$. Pretpostavimo da je (x, y, z) rješenje početne jednadžbe takvo da vrijedi $\gcd(x, y) = 1$. Iz toga slijedi da je jedan od brojeva x, y neparan iz čega zaključujemo da je z također neparan. Početnu jednadžbu možemo zapisati kao

$$(x + yi)(x - yi) = z^2.$$

Želimo pokazati $\gcd(x + yi, x - yi) = 1$. Neka je $d \in \mathbb{Z}[i]$ takav da dijeli $x + yi$ i $x - yi$. Iz toga slijedi da $d|2x$ i $d|2y$. Kako je z neparan broj, slijedi da d ne dijeli 2, pa zaključujemo $d|x$ i $d|y$. Stoga za norme vrijedi da $N(d)|x$ i $N(d)|y$. Zbog $\gcd(x, y) = 1$ slijedi da je $N(d) = 1$, odnosno da je d jedinica. Stoga zaključujemo da su $x + yi$ i $x - yi$ relativno prosti, odnosno jedini njihov zajednički djelitelj je invertibilan element skupa $\mathbb{Z}[i]$. Dakle, dobivamo

$$x + yi = u(a + bi)^2,$$

gdje je $u = d$ invertibilan element u $\mathbb{Z}[i]$, $a, b \in \mathbb{Z}$. Ako uzmemo $u = 1$, te izjednačimo realni i imaginarni dio dobivamo

$$x = a^2 - b^2, \quad y = 2ab$$

Iz toga slijedi $z = a^2 + b^2$. Kako je z neparan, a i b su različite parnosti. Uzmemo li neku drugu vrijednost za u, dobit ćemo slične izraze. Npr., za $u = i$ dobivamo $x = -2ab, y = a^2 - b^2, z = a^2 + b^2$.

Dakle, rješenja početne jednadžbe su

$$(x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2),$$

za $a, b \in \mathbb{Z}$ različite parnosti. ♢

Napomenimo da će više o Pitagorinoj jednadžbi biti u odjeljku 2.1.

Primjer 1.22. *Riješimo jednadžbu*

$$x^2 + y^2 = z^n,$$

gdje je n prirodan broj, $n > 1$.

Rješenje. Za $n = 2$ rješenja jednadžbe su Pitagorine trojke, a taj slučaj smo riješili u prethodnom primjeru. Neka je $n \geq 3$. U ovom primjeru koristit ćemo jedinstvenost rastava na proste faktore u skupu $\mathbb{Z}[i]$. Bez smanjenja općenitosti, pretpostavimo da su x i y relativno prosti, te zapišimo jednadžbu u ekvivalentnom obliku

$$(x + yi)(x - yi) = z^n.$$

Želimo pokazati $\gcd(x + yi, x - yi) = 1$ u $\mathbb{Z}[i]$. Uočimo da $\gcd(x + yi, x - yi)$ dijeli $\gcd(2x, 2y) = 2$. Međutim, u skupu Gaussovih cijelih brojeva vrijedi $2 = -i(1 + i)^2$. Ako $1 + i$ dijeli oba faktora, tada $2|z$, čime bi dobili kontradikciju modulo 8. Dakle, $x + yi$ i $x - yi$ su relativno prosti. Slijedi

$$x + yi = (a + bi)^n,$$

gdje su $a, b \in \mathbb{Z}$, te vrijedi $a^2 + b^2 = z$. Neka je $x = A_n$ i $y = B_n$. Izjednačavanjem realnog i imaginarnog dijela dobivamo

$$A_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k \binom{n}{2k} a^{n-2k} b^{2k},$$

$$B_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (-1)^k \binom{n}{2k+1} a^{n-2k-1} b^{2k+1}.$$

Dakle, rješenja početne jednadžbe su trojke

$$(d^n A_n, d^n B_n, d^2(a^2 + b^2))$$

gdje su $a, b, d \in \mathbb{Z}$. ♢

Primjer 1.23. *Riješimo jednadžbu*

$$x^2 + 4 = y^3.$$

Rješenje. Promatramo dva slučaja.
Slučaj I. Neka je x neparan. Početnu jednadžbu možemo zapisati kao

$$(2 + xi)(2 - xi) = y^3. \tag{1.15}$$

Želimo pokazati da su $2 + xi$ i $2 - xi$ relativno prosti Gaussovi cijeli brojevi. Neka je $\gcd(2 + xi, 2 - xi) = z, z = c + di \in \mathbb{Z}[i]$. Tada z dijeli $(2 + xi) + (2 - xi) = 4$ iz čega slijedi da i $\bar{z}$ dijeli 4. Kako vrijedi $z \cdot \bar{z} = c^2 + d^2$, zaključujemo

$$c^2 + d^2 \mid 16 \tag{1.16}$$

S druge strane, iz $z|2 + xi$ slijedi $\bar{z}|2 - xi$, pa imamo

$$c^2 + d^2 \mid x^2 + 4. \tag{1.17}$$

Uspoređivanjem (1.16) i (1.17), te uzimajući u obzir da je x neparan, zaključujemo da je $c^2 + d^2 = 1$, odnosno z je invertibilan element skupa $\mathbb{Z}[i]$ (jer mu je norma jednaka 1), što znači da su $2 + xi$ i $2 - xi$ relativno prosti. Tada iz (1.15) slijedi

$$2 + xi = (a + bi)^3,$$

gdje su $a, b \in \mathbb{Z}$, te smo uzeli $u = 1$, kao i u prethodnim primjerima. Izjednačavanjem realnog i imaginarnog dijela dobivamo

$$\begin{cases} a(a^2 - 3b^2) = 2 \\ 3a^2b - b^3 = x \end{cases}.$$

Prvu jednadžbu dobivenog sustava riješit ćemo koristeći metodu faktorizacije. Dobivamo sustave

$$\begin{cases} a = 1 \\ a^2 - 3b^2 = 2, \end{cases} \qquad \begin{cases} a = -1 \\ a^2 - 3b^2 = -2, \end{cases}$$

$$\begin{cases} a = 2 \\ a^2 - 3b^2 = 1, \end{cases} \qquad \begin{cases} a = -2 \\ a^2 - 3b^2 = -1, \end{cases}$$

čija su rješenja $(a, b) = (-1, \pm 1)$, te $(a, b) = (2, \pm 1)$. Uvrštavanjem dobivamo $x = \pm 2, \pm 11$. Kako je u ovom slučaju x neparan, zaključujemo da su rješenja početne jednadžbe $(x, y) = (\pm 11, 5)$.

Slučaj II. Neka je sada x paran. Iz toga slijedi da je i y paran. Neka je $x = 2u, y = 2v$. Tada početnu jednadžbu možemo zapisati kao

$$u^2 + 1 = 2v^3,$$

odnosno

$$(u + i)(u - i) = 2v^3.$$

Na sličan način kao i u prethodnom slučaju, dobivamo $\gcd(u+i, u-i) = 1$. Koristeći činjenicu da je $2 = (1 + i)(1 - i)$, te jedinstvenost rastava na proste faktore u skupu $\mathbb{Z}[i]$ dobivamo

$$u + i = (1 + i)(a + bi)^3,$$

gdje su $a, b \in \mathbb{Z}$. Izjednačavanjem realnog i imaginarnog dijela dobivamo sustav

$$\begin{cases} a^3 - 3a^2b - 3ab^2 + b^3 = u \\ a^3 + 3a^2b - 3ab^2 - b^3 = 1. \end{cases}$$

Drugu jednadžbu možemo zapisati u ekvivalentnom obliku $(a-b)(a^2+4ab+b^2) = 1$, pa kao i u prethodnom slučaju koristimo metodu faktorizacije kojom dobivamo dva sustava jednadžbi

$$\begin{cases} a - b = 1 \\ a^2 + 4ab + b^2 = 1, \end{cases} \qquad \begin{cases} a - b = -1 \\ a^2 + 4ab + b^2 = -1. \end{cases}$$

Rješenja prvog sustava su $(a, b) = (1, 0)$ i $(a, b) = (0, -1)$, dok drugi sustav nema rješenja jer vrijedi $(a + 2b)^2 - 3b^2 \equiv 0, 1 \pmod 3$, što je u kontradikciji s drugom jednadžbom sustava. Uvrštavanjem dobivamo $(u, v) = (1, 1)$ i $(u, v) = (-1, 1)$, pa slijedi da su u ovom slučaju rješenja početne jednadžbe $(x, y) = (2, 2)$ i $(x, y) = (-2, 2)$. Dakle, sva rješenja zadane jednadžbe su $(-11, 5), (11, 5), (-2, 2)$, te $(2, 2)$. ♢

1.5 Kvadratna polja

Neka je d kvadratno slobodan cijeli broj i $d \neq 1$. Označimo skup

$$\mathbb{Q}(\sqrt{d}) = \{u + v\sqrt{d} \,|\, u, v \in \mathbb{Q}\}.$$

Uz standardne operacije zbrajanja i množenja u $\mathbb{R}$, skup $\mathbb{Q}(\sqrt{d})$ ima strukturu polja i zovemo ga *kvadratno polje*. Zaista, za to je ključno ustanoviti da su operacije zbrajanja i množenja zatvorene u $\mathbb{Q}(\sqrt{d})$, odnosno da su

$$(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d},$$

$$(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) = a_1a_2 + b_1b_2d + (a_1b_2 + b_1a_2)\sqrt{d}$$

elementi skupa $\mathbb{Q}(\sqrt{d})$ za sve racionalne brojeve a, b, c, d. Nadalje, multiplikativni inverz od proizvoljnog elementa $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})\setminus\{0\}$:

$$(a + b\sqrt{d})^{-1} = \frac{a}{a^2 - db^2} - \frac{b}{a^2 - db^2}\sqrt{d}$$

je također iz istog skupa $\mathbb{Q}(\sqrt{d})$.

Za $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ definiramo *normu* od α kao

$$N(\alpha) = a^2 - db^2.$$

Dakle, $N(\alpha) = \alpha\overline{\alpha}$, gdje je $\overline{\alpha} = a - b\sqrt{d}$ *konjugat* od α. Navedena norma ima svojstvo multiplikativnosti, odnosno $N(\alpha\beta) = N(\alpha)N(\beta)$.

Uočimo da je svaki $\alpha \in \mathbb{Q}(\sqrt{d})$ nultočka polinoma s racionalnim koeficijentima

$$f(X) = X^2 - (\alpha + \overline{\alpha})X + \alpha\overline{\alpha}. \tag{1.18}$$

Definicija 1.24. *Kažemo da je* $\alpha \in \mathbb{Q}(\sqrt{d})$ cijeli broj *(odnosno algebarski cijeli broj) ako polinom* (1.18) *ima cjelobrojne koeficijente, tj. ako su* $\alpha + \overline{\alpha}, \alpha\overline{\alpha} \in \mathbb{Z}$.

Skup svih cijelih brojeva u $\mathbb{Q}(\sqrt{d})$ čini komutativan prsten s jedinicom. Sljedeći teorem opisuje kako izgledaju cijeli brojevi u $\mathbb{Q}(\sqrt{d})$, ovisno o vrijednosti broja d.

Teorem 1.25. *Ako je* $d \equiv 2$ ili $3 \pmod 4$*, tada su svi cijeli brojevi u* $\mathbb{Q}(\sqrt{d})$ *oblika*

$$a + b\sqrt{d}, a, b \in \mathbb{Z}.$$

Ako je $d \equiv 1 \pmod 4$*, tada su svi cijeli brojevi u* $\mathbb{Q}(\sqrt{d})$ *oblika*

$$a + b\frac{1 + \sqrt{d}}{2},\ a, b \in \mathbb{Z}.$$

Dokaz. Neka su $a, b \in \mathbb{Z}$. Ako je $\alpha = a + b\sqrt{d}$, onda su

$$\alpha + \overline{\alpha} = 2a, \alpha\overline{\alpha} = a^2 - db^2$$

iz $\mathbb{Z}$, pa je α cijeli broj u $\mathbb{Q}(\sqrt{d})$. Analogno, za $\alpha = a + b\frac{1+\sqrt{d}}{2} = a + \frac{b}{2} + \frac{b}{2}\sqrt{d}$ je

$$\alpha + \overline{\alpha} = 2a + b, \alpha\overline{\alpha} = a^2 + ab - (d - 1)\frac{b^2}{4}.$$

Uz pretpostavku $d \equiv 1 \pmod 4$ imamo da je $\alpha\overline{\alpha} \in \mathbb{Z}$ te je u tom slučaju i α cijeli broj u $\mathbb{Q}(\sqrt{d})$.

Sada pokažimo obratno. Neka je $\alpha = u + v\sqrt{d}$, $u, v \in \mathbb{Q}$, cijeli broj iz $\mathbb{Q}(\sqrt{d})$. Tada je

$$\alpha + \overline{\alpha} = 2u \in \mathbb{Z}, \quad \alpha\overline{\alpha} = u^2 - dv^2 \in \mathbb{Z}.$$

Iz toga slijedi da je $u = \frac{1}{2}(2u)$, odnosno $u \in \mathbb{Z}$ ili je u polovina neparnog cijelog broja. Označimo $a = 2u$, $b = 2v$ i $u^2 - dv^2 = c$. Prema pretpostavci su $a, c \in \mathbb{Z}$ pa je stoga i $db^2 = a^2 - 4c \in \mathbb{Z}$. Kako je d kvadratno slobodan, zaključujemo da je i $b \in \mathbb{Z}$.

Neka je $d \equiv 2$ ili $3 \pmod 4$. Iz

$$a^2 \equiv b^2 d \pmod 4, \quad a^2 \equiv 0 \text{ ili } 1 \pmod 4, \quad b^2 d \equiv 0, 2 \text{ ili } 3 \pmod 4$$

slijedi da su a i b parni brojevi, pa su $u, v \in \mathbb{Z}$.

Neka je $d \equiv 1 \pmod 4$. Iz $a^2 \equiv b^2 \pmod 4$ slijedi da su brojevi a i b iste parnosti. Tada je $u - v = \frac{a-b}{2}$ cijeli broj, odnosno

$$u + v\sqrt{d} = u - v + v(1 + \sqrt{d}) = \underbrace{u - v}_{\in\mathbb{Z}} + \underbrace{2v}_{=b\in\mathbb{Z}} \frac{1 + \sqrt{d}}{2},$$

što daje traženi oblik. □

Skup, odnosno prsten cijelih brojeva u $\mathbb{Q}(\sqrt{d})$ za $d \equiv 2, 3 \pmod 4$, označavamo sa

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,|\, a, b \in \mathbb{Z}\},$$

a za $d \equiv 1 \pmod 4$ sa

$$\mathbb{Z}\left[\frac{1 + \sqrt{d}}{2}\right] = \{a + b\frac{1 + \sqrt{d}}{2} \,|\, a, b \in \mathbb{Z}\}.$$

Napomenimo da direktno iz Definicije 1.24 slijedi da je $N(\alpha) \in \mathbb{Z}$ za svaki cijeli broj α iz kvadratnog polja. No, obrat ne vrijedi. Na primjer, za $\alpha = \frac{1}{3} + \frac{2}{3}\sqrt{-2} \in \mathbb{Q}(\sqrt{-2})$ vrijedi da je $N(\alpha) = \frac{1}{9} + \frac{8}{9} = 1 \in \mathbb{Z}$, no α nije cijeli broj u polju $\mathbb{Q}(\sqrt{-2})$.

Kao i u prstenu Gaussovih cijelih brojeva, zanimaju nas invertibilni elementi u prstenima cijelih brojeva kvadratnog polja, tj. u $\mathbb{Z}[\sqrt{d}]$, odnosno u $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Invertibilan element prstena cijelih brojeva i ovdje je uobičajeno zvati *jedinicom*. Skup invertibilnih elemenata i ovdje čini grupu, *grupu jedinica*.

Vrijedi slična tvrdnja Teoremu 1.16.

Teorem 1.26. *Cijeli broj $\alpha \in \mathbb{Q}(\sqrt{d})$ je jedinica ako i samo ako je α cijeli broj takav da je $N(\alpha) = \pm 1$.*

Dokaz. Ako je α jedinica, onda postoji cijeli broj $\beta \in \mathbb{Q}(\sqrt{d})$ takav da je $\alpha\beta = 1$. Iz toga slijedi $N(\alpha)N(\beta) = N(1) = 1$. Kako su $N(\alpha)$ i $N(\beta)$ cijeli brojevi, zaključujemo da je $N(\alpha) = \pm 1$.

S druge strane, ako je α cijeli broj takav da je $N(\alpha) = \pm 1$, onda je $\alpha\overline{\alpha} = \pm 1$, odnosno imamo $\alpha\overline{\alpha} = 1$ ili $\alpha(-\overline{\alpha}) = 1$. U oba slučaja, kao su $\pm\overline{\alpha}$ cijeli brojevi, slijedi da je α jedinica. □

Pogledajmo, na primjer, invertibilne elemente za $d = -2$. Tada su cijeli brojevi u $\mathbb{Q}(\sqrt{d})$ oblika $u + v\sqrt{-2}, u, v \in \mathbb{Z}$. Neka je $\alpha = a + b\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$ takav da vrijedi $N(\alpha) = \pm 1$. Iz toga slijedi

$$a^2 + 2b^2 = \pm 1$$

pa zaključujemo da je $\alpha = \pm 1$, odnosno invertibilni elementi za $d = -2$ su $1, -1$.

Definicija 1.27. *Kažemo da su $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$* relativno prosti *ako su im jedini zajednički djelitelji invertibilni elementi.*

Postavlja se pitanje za koje vrijednosti od d kvadratno polje $\mathbb{Q}(\sqrt{d})$ ima svojstvo jedinstvene faktorizacije. Gauss (19. st.) je pokazao da za

$$d = -1, -2, -3 - 7, -11, -19, -43, -67, -163,$$

prsten cijelih brojeva u $\mathbb{Q}(\sqrt{d})$ ima svojstvo jedinstvene faktorizacije te pretpostavio da su jedina imaginarna kvadratna polja za koja to vrijedi. To su puno godina kasnije pokazali Heegner and Stark (1966.). Zanimljivo je da je u realnim kvadratnim poljima, tj. u $\mathbb{Q}(\sqrt{d})$, $d > 0$ problem još otvoren. Nije čak poznato ima li konačno ili beskonačno mnogo realnih kvadratnih polja čiji prsteni cijelih brojeva imaju svojstvo jedinstvene faktorizacije.

Na sljedećem primjeru pokažimo korištenje kvadratnih polja u rješavanju diofantskih jednadžbi.

Primjer 1.28. *Odredimo sva cjelobrojna rješenja jednadžbe*

$$x^3 - 2 = y^2.$$

Rješenje. Zapišimo danu jednadžbu u ekvivalentnom obliku

$$x^3 = y^2 + 2 = (y + \sqrt{-2})(y - \sqrt{-2}). \tag{1.19}$$

Uočimo da y ne može biti paran jer bi tada vrijedilo

$$y^2 + 2 \equiv 2 \pmod 4,$$

a niti jedan kub ne daje ostatak 2 modulo 4. Dakle, y je neparan. Neka je

$$\gcd(y+\sqrt{-2}, y-\sqrt{-2}) = \gamma,$$

te označimo $\gamma = u + v\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$. Tada γ dijeli $y+\sqrt{-2}-(y-\sqrt{-2}) = 2\sqrt{-2}$ iz čega slijedi da $\overline{\gamma}$ dijeli $-2\sqrt{-2}$. Znamo da vrijedi $\gamma\overline{\gamma} = u^2+2v^2$, pa iz toga slijedi

$$u^2 + 2v^2 \mid 8.$$

S druge strane, $\gamma \mid y+\sqrt{-2}$ iz čega slijedi $\overline{\gamma} \mid y-\sqrt{-2}$, pa dobivamo

$$u^2 + 2v^2 \mid y^2 + 2.$$

Znamo da je y neparan, pa zaključujemo da je $u^2+2v^2 = 1$, odnosno γ je jedinica. Dakle, $y+\sqrt{-2}$ i $y-\sqrt{-2}$ su relativno prosti, te je njihov umnožak kub cijelog broja. Kako u prstenu cijelih brojeva polja $\mathbb{Q}(\sqrt{-2})$ vrijedi svojstvo jedinstvene faktorizacije, slijedi da je svaki od faktora, $y+\sqrt{-2}$ i $y-\sqrt{-2}$, jednak kubu nekog cijelog broja do na jedinice iz prstena $\mathbb{Z}[\sqrt{-2}]$. Jedinice u $\mathbb{Z}[\sqrt{-2}]$ su ± 1, što su također kubovi. Slijedi

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3,$$

za $a, b \in \mathbb{Z}$. Raspisivanjem desne strane jednakosti, te izjednačavanjem realnog i imaginarnog dijela dobivamo sustav

$$\begin{cases} y = a^3 - 6ab^2 \\ 1 = 3a^2b - 2b^3 \end{cases}$$

Drugu jednadžbu sustava možemo zapisati kao $1 = b(3a^2 - 2b^2)$, pa zaključujemo $b = \pm 1$. Iz toga slijedi $a = \pm 1$, pa uvrštavanjem u prvu jednadžbu sustava dobivamo $y = \pm 5$. Zatim uvrštavanjem u (1.19) dobivamo $x = 3$. Dakle, sva cjelobrojna rješenja početne jednadžbe su $(x, y) = (3, \pm 5)$. ♢

Vrlo korisnu i praktičnu primjenu kvadratnih polja pokazat ćemo u sljedećem poglavlju, u odsječku 2.3.

Poglavlje 2

Klasične diofantske jednadžbe drugog stupnja

2.1 Pitagorina jednadžba

Jednadžba oblika

$$x^2 + y^2 = z^2 \tag{2.1}$$

predstavlja jednu od najjednostavnijih kvadratnih diofantskih jednadžbi i njeno proučavanje seže daleko u prošlost. Naime, na staroj babilonskoj ploči iz oko 1700. godine pr. Kr. nalazi se opsežan popis njenih rješenja od kojih su neka prilično velika. Jednadžba je bila i od značajnog interesa za starogrčke matematičare, a zbog njezine povezanosti s Pitagorinim teoremom nazvana je *Pitagorina jednadžba*. Njeno opće rješenje može se naći u X. knjizi Euklidovih *Elemenata*.

Iako smo u Primjeru 1.21 već opisali rješenja Pitagorine jednadžbe, u onom što slijedi opisat ćemo jednu klasičnu metodu rješavanja koja će nam omogućiti da riješimo i poopćenu Pitagorinu jednadžbu. Uočimo kako je smisleno odrediti sva rješenja u skupu prirodnih brojeva jer ako je (a, b, c) neko rješenje jednadžbe (2.1), onda su to i $(\pm a, \pm b, \pm c)$ sa svim kombinacijama predznaka. Nadalje, lako je odrediti tzv. trivijalna rješenja $(0, 0, 0)$, $(0, \pm 1, \pm 1)$, $(\pm 1, 0, \pm 1)$.

Definicija 2.1. *Uređenu trojku prirodnih brojeva* (x, y, z) *zovemo* Pitagorina trojka *ako vrijedi*

$$x^2 + y^2 = z^2.$$

Ako su x, y, z *relativno prosti, onda kažemo da je* (x, y, z) primitivna Pitagorina trojka.

Dijeljenjem jednadžbe (2.1) sa z^2 dobivamo

$$X^2 + Y^2 = 1 \tag{2.2}$$

gdje je $X = \frac{x}{z}$ i $Y = \frac{y}{z}$. Time smo problem sveli na traženje rješenja $(X, Y) \in \mathbb{Q}^2$ jednadžbe (2.2). Izrazimo Y^2:

$$Y^2 = 1 - X^2 \ = (1 - X)(1 + X)$$

i podijelimo s $(1 + X)^2$, što možemo jer bi iz $X + 1 = 0$ slijedilo da je $y = 0$,

$$\left(\frac{Y}{1+X}\right)^2 = \frac{1-X}{1+X}.$$

Označimo $t = \frac{Y}{1+X}$, odnosno $t^2 = \frac{1-X}{1+X}$. Tada je

$$(X, Y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right), \tag{2.3}$$

čime smo prikazali X i Y kao racionalne funkcije od t. Dakle, za svaki $t \in \mathbb{Q}$ dobivamo odgovarajuće rješenje $(X, Y) \in \mathbb{Q}^2$ od (2.2), osim trivijalnog $(-1, 0)$. Obratno, svako racionalno rješenje $(X, Y) \neq (-1, 0)$ jednadžbe (2.2) određuje neki, ne nužno jedinstven, $t \in \mathbb{Q}$.

Napomenimo da trivijalnom rješenju $(-1, 0)$ jednadžbe (2.2) možemo dati i geometrijsku interpretaciju. Pravac iz točke $(-1, 0)$ s koeficijentom smjera t, $y = tx + t$, siječe kružnicu $x^2 + y^2 = 1$ u točkama $(x_1, y_1) = (-1, 0)$ i (x_2, y_2)

$$x_2 = \frac{1-t^2}{1+t^2}, \ y_2 = \frac{2t}{1+t^2}.$$

Budući da pravac $y = tx + t$ ne može biti tangenta kružnice $x^2 + y^2 = 1$ (koja glasi $x = -1$) i ima zajedničku točku s kružnicom, $(-1, 0)$, onda on može biti samo njena sekanta pa je

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \neq (-1, 0),$$

za sve $t \in \mathbb{R}$.

Dakle, za proizvoljan $t \in \mathbb{Q}$, (2.3) predstavlja opće rješenje jednadžbe (2.2) u skupu racionalnih brojeva. Sada nam slijedi opis postupka kojim od racionalnih rješenja jednadžbe (2.2) dobivamo cjelobrojna, odnosno prirodna rješenja jednadžbe (2.1). Neka je

$$t = \frac{q}{p},$$

gdje su p i q relativno prosti prirodni brojevi. Tada iz (2.3) slijedi

$$\frac{x}{z} = \frac{p^2 - q^2}{p^2 + q^2}, \ \frac{y}{z} = \frac{2pq}{p^2 + q^2} \tag{2.4}$$

Očito je da uređena trojka

$$(p^2 - q^2, 2pq, p^2 + q^2) \tag{2.5}$$

predstavlja jedno cjelobrojno rješenje jednadžbe (2.1). No, i svaka uređena trojka čiji su elementi višekratnici tih brojeva ili čiji su elementi nastali dijeljenjem njihovim zajedničkim višekratnikom također predstavlja cjelobrojno rješenje od(2.1). S obzirom da bismo htjeli „popisati" sva rješenja bez ponavljanja, trebamo najprije opisati skup svih rješenja čiji su elementi relativno prosti, odnosno trebamo opisati skup svih *primitivnih* Pitagorinih trojki.

Ako bi brojevi p i q bili iste parnosti, onda bi svaki od brojeva p^2-q^2, $2pq$, p^2+q^2 bio paran, tj. djeljiv s 2. Zato pretpostavimo da su p i q različite parnosti i relativno prosti. Ako bi postojao djelitelj $d > 1$ koji dijeli p^2-q^2 i p^2+q^2, onda bi d morao biti neparan (jer su p^2-q^2 i p^2+q^2 neparni) i d bi morao dijeliti i $(p^2-q^2)+(p^2+q^2) = 2p^2$ i $(p^2 + q^2) - (p^2 - q^2) = 2q^2$ što je nemoguće jer su p i q relativno prosti. Dakle, uz pretpostavke da su $p, q \in \mathbb{N}$, $p > q$, relativno prosti brojevi različite parnosti , (2.5) predstavlja jednu primitivnu Pitagorinu trojku. Skup svih primitivnih Pitagorinih trojki (x, y, z), u kojima je y paran, je skup

$$\{(p^2 - q^2, 2pq, p^2 + q^2) \mid p, q \in \mathbb{N},\, p > q, \gcd(p, q) = 1,\, p \not\equiv q \pmod 2\}.$$

Sada lako možemo doći do svih rješenja jednadžbe (2.1). To je unija skupa

$$\{(m(p^2 - q^2), 2mpq, m(p^2 + q^2)) \mid m, p, q \in \mathbb{N},\, p > q, \gcd(p, q) = 1,\, p \not\equiv q \pmod 2\}$$

i skupa

$$\{(2mpq, m(p^2 - q^2), m(p^2 + q^2)) \mid m, p, q \in \mathbb{N},\, p > q, \gcd(p, q) = 1,\, p \not\equiv q \pmod 2\}$$

kojeg smo dobili zamjenom varijabli x i y. (Isto bi dobili ako krenemo od prepostavke da su p i q neparni relativno prosti brojevi. Tada, ako stavimo $p+q = 2P$ i $p-q = 2Q$ slijedi da su P i Q relativno prosti brojevi, različite parnosti jer je $P+Q = p$ neparan. Nadalje, zamijenimo li p i q sa P i Q u (2.4) dobivamo

$$\frac{x}{z} = \frac{2PQ}{P^2 + Q^2}, \frac{y}{z} = \frac{P^2 - Q^2}{P^2 + Q^2},$$

što upravo odgovara zamjeni varijabli x i y).

Iz svega prethodno dokazanog slijedi teorem.

Teorem 2.2. *Sve Pitagorine trojke (x, y, z) u kojima je y paran, dane su formulama*

$$x = m(p^2 - q^2),\ y = 2mpq,\ z = m(p^2 + q^2), \tag{2.6}$$

gdje su p i q relativno prosti prirodni brojevi različite parnosti te m prirodan broj.

Primjer 2.3. *Odredite sve Pitagorine trojke (x, y, z) čiji su svi elementi manji ili jednaki od 30.*

Rješenje. Kako je $x < z$ i $y < z$, prema Teoremu 2.2 slijedi da trebamo odrediti sve prirodne m, p, q takve da je $m(p^2 + q^2) \leq 30$ pri čemu su p i q relativno prosti brojevi različite parnosti. Neka je $p > q$. Za $m = 1$, iz $p^2 + q^2 \leq 30$ dobivamo sljedeće parove brojeva (p, q):

$$(2, 1), \quad (3, 2), \quad (4, 1), \quad (4, 3), \quad (5, 2).$$

Sada prema (2.6) slijedi da su

$$(3, 4, 5), \quad (5, 12, 13), \quad (15, 8, 17), \quad (7, 24, 25), \quad (21, 20, 29)$$

sve primitivne Pitagorine trojke. Ostale Pitagorine trojke dobivamo za vrijednosti $(m, p, q) = (m, 2, 1)$, $2 \leq m \leq 6$ i za $(m, p, q) = (2, 3, 2)$, a to su

$$(6, 8, 10), \quad (10, 24, 26), \quad (9, 12, 15), \quad (12, 16, 20), \quad (15, 20, 25), \quad (18, 24, 30).$$

Dakle, dobili smo točno 11 Pitagorinih trojki, s parnim y, čiji su elementi ≤ 30. $\diamondsuit$

Primjer 2.4. *Odredite sve Pitagorine trojke (x, y, z) u kojima je jedan element jednak 2019.*

Rješenje. Djelitelji broja 2019, osim njega samog, su $1, 3$ i 673. Iz toga slijedi da je $m = 1, m = 3$ ili $m = 673$.

Neka je $m = 1$. Određujemo sve primitivne Pitagorine trojke sa stranicom 2019. Kako se 2019 ne može prikazati kao suma kvadrata, ostaje za ispitati može li biti $p^2 - q^2 = 2019$, odnosno $(p - q)(p + q) = 2019$. Iz toga slijedi

$$\begin{cases} p - q = 1 \\ p + q = 2019 \end{cases} \quad \text{ili} \quad \begin{cases} p - q = 3 \\ p + q = 673. \end{cases}$$

Rješenja gornjih sustava su $(p, q) = (1010, 1009)$, odnosno $(p, q) = (338, 335)$. Budući da su p i q različitih parnosti i relativno prosti, uvrštavanjem u (2.6) dobivamo sljedeće primitivne Pitagorine trojke sa stranicom 2019:

$$(2019, 2038180, 2038181),\ (2019, 226460, 226469).$$

Neka je $m = 3$. Određujemo sve primitivne Pitagorine trojke sa stranicom $2019/3 = 673$. Rješenje jednadžbe $p^2 + q^2 = 673$ je $(p, q) = (23, 12)$, a jednadžbe $p^2 - q^2 = 673$, $(p, q) = (337, 336)$. Prema (2.6) dobivamo trojke:

$$(1155, 1656, 2019), \ (2019, 679392, 679395).$$

Ako je $m = 673$, onda tražimo sve primitivne Pitagorine trojke sa stranicom 3. Jedino je moguće $p^2 - q^2 = 3$ za $(p, q) = (2, 1)$, čime smo dobili Pitagorinu trojku

$$(2019, 2692, 3365).$$

$\diamondsuit$

2.2 Jednadžba $ax^2 + by^2 = z^2$

Metodu koju smo koristili na primjeru Pitagorine jednadžbe možemo primijeniti i na jednadžbu

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

Pokazat ćemo da jednadžba (2.7) ima beskonačno mnogo primitivnih rješenja u skupu prirodnih brojeva, odnosno rješenja za koja su x, y, z relativno prosti brojevi. Zapišimo jednadžbu(2.7) u ekvivalentnom obliku $z^2 - y^2 = ax^2$ te ju podijelimo s y^2. Dobivamo

$$X^2 - 1 = aY^2 \tag{2.8}$$

gdje je $X = \frac{z}{y}, Y = \frac{x}{y}$. Dakle, tražimo rješenja $(X, Y) \in \mathbb{Q}^2$ jednadžbe (2.8). Množenjem jednadžbe sa $\frac{a}{(X+1)^2}$ dobivamo

$$\frac{a(X-1)}{X+1} = \left(\frac{aY}{X+1}\right)^2.$$

Označimo $t = \frac{aY}{X+1}$, odnosno $t^2 = \frac{a(X-1)}{X+1}$. Iz toga slijedi

$$(X, Y) = \left(\frac{a + t^2}{a - t^2}, \frac{2t}{a - t^2}\right).$$

Neka je $t = \frac{q}{p}$, gdje su p i q relativno prosti prirodni brojevi. Tada imamo

$$\frac{x}{y} = \frac{2pq}{ap^2 - q^2}, \frac{z}{y} = \frac{ap^2 + q^2}{ap^2 - q^2}.$$

Dakle, dobili smo uređenu trojku

$$(x, y, z) = d(2pq, ap^2 - q^2, ap^2 + q^2), d \in \mathbb{N}$$

koja predstavlja sva rješenja jednadžbe (2.7) u skupu prirodnih brojeva za x paran.

Istu metodu ne možemo primijeniti na jednadžbu

$$ax^2 + by^2 = z^2, \tag{2.9}$$

gdje su $a, b \in \mathbb{N}$, te niti jedan od njih nije potpun kvadrat. Uočimo da, osim trivijalnog rješenja $(0, 0, 0)$, takva jednadžba možda nema rješenja. U onom što slijedi ćemo pod pojmom da jednadžba *ima rješenja* misliti na to da jednadžba ima i *netrivijalnih* rješenja.

Primjer 2.5. *Jednadžba $2x^2 + 3y^2 = z^2$ nema netrivijalnih rješenja.*

Rješenje. Bez smanjenja općenitosti pretpostavimo da x, y, z nemaju zajedničkog djelitelja većeg od 1, tj. $\gcd(x, y, z) = 1$. Otuda slijedi da niti x niti z nisu djeljivi sa 3. Nadalje, iz

$$2x^2 \equiv z^2 \pmod 3 \tag{2.10}$$

dobivamo kontradikciju jer je 2 kvadratni neostatak modulo 3. ♢

Ideja iz Primjera (2.5), tj. uspostavljanje određenih kongruencija može se primijeniti i na traženje općeg rješenja jednadžbe (2.9). Bez smanjenja općenitosti pretpostavimo da su a i b kvadratno slobodni, tj. da nisu djeljivi kvadratima prirodnih brojeva većih od 1. Ako bi, na primjer, c^2, $c \in \mathbb{N}$, $c > 1$, dijelio broj a, onda umjesto (2.9) rješavamo jednadžbu $a'x'^2 + by^2 = 1$, gdje su $a' = a/c^2$ i $x' = xc$. Nadalje, možemo pretpostaviti da tražimo rješenja (x, y, z) tako da je $\gcd(x, y, z) = 1$.

Iz (2.9) slijedi

$$ax^2 \equiv z^2 \pmod b. \tag{2.11}$$

Uočimo da x i b moraju biti relativno prosti. U suprotnom, kada bi oni imali zajednički prosti faktor, on bi dijelio x i z, a njegov kvadrat bi dijelio by^2. S obzirom da je b kvadratno slobodan slijedi da bi taj broj dijelio y, što je u kontradikciji s $(x, y, z) = 1$.

Pomnožimo kongruenciju (2.11) s x'^2, $x' \in \mathbb{Z}$, takvim da je $xx' \equiv 1 (\mathrm{mod}\ b)$:

$$a \equiv \alpha^2 \pmod b, \tag{2.12}$$

gdje je $\alpha = x'z$. Slično, dobivamo

$$b \equiv \beta^2 \pmod{a}, \tag{2.13}$$

za $\beta \in \mathbb{Z}$. Dakle, a mora biti kvadratni ostatak modulo b, a b kvadratni ostatak modulo a.

Ako a i b nisu relativno prosti, onda rješivost jednadžbe (2.9) povlači još jednu kongruenciju. Dakle, neka je $a = ha_1$ i $b = hb_1$ tako da su a_1 i b_1 u relativno prosti. Nadalje, jer su a i b kvadratno slobodni slijedi da je h je kvadratno slobodan i da su a_1, b_1, h u parovima relativno prosti. Tada z mora biti djeljiv sa h pa slijedi da izraz $a_1x^2 + b_1y^2$ mora biti djeljiv s h. Množenjem tog izraza s $b_1x'^2$ dobivamo

$$a_1b_1(x'x)^2 + b_1^2x'^2y^2 \equiv a_1b_1 + (b_1x'y)^2 \equiv 0 \pmod{h},$$

tj. postoji $\gamma \in \mathbb{Z}$ za koji je

$$a_1b_1 \equiv -\gamma^2 \pmod{h}. \tag{2.14}$$

Do sada smo pokazali, ako jednadžba (2.9) ima rješenja, onda vrijede kongruencije (2.12), (2.13) i (2.14). Dakle, ako jedna od navedenih konkruencija ne vrijedi, onda jednadžba (2.9) ima samo trivijalno rješenje.

Sada želimo pokazati obrat prethodne tvrdnje, ako vrijede (2.12), (2.13) i (2.14), onda je jednadžba (2.9) rješiva. Promotrit ćemo nekoliko slučajeva.

Slučaj I. Neka je $a = 1$ ili $b = 1$. Već smo pokazali da u ovom slučaju jednadžba ima rješenja.

Slučaj II. Neka je $a = b$. Tada iz (2.14) dobivamo

$$1 \equiv -\gamma^2 \pmod{a}$$

Otuda slijedi da a dijeli zbroj kvadrata $1 + \gamma^2$ pa je i sam jednak zbroju kvadrata, tj. $a = p^2+q^2$. Uočimo da je $(x, y, z) = (p, q, p^2+q^2)$ jedno (netrivijalno) rješenje od (2.9).

Slučaj III. Pretpostavimo $a > b > 1$. Ideja dokaza je u jednadžbi (2.9) zamijeniti a s A, gdje je $0 < A < a$, te A i b zadovoljavaju odgovarajuće analogne kongruencije. Ponavljanjem postupka želimo dobiti da je jedan od koeficijenata A, odnosno b jednak 1 ili da su oni međusobno jednaki, te bismo time ovaj slučaj sveli na jedan od prethodna dva.

Iz uvjeta (2.13) slijedi je $\beta^2 - b$ višekratnik od a. Biramo $\beta \in \mathbb{Z}$ takav da $|\beta| \leq \frac{1}{2}a$ i

$$\beta^2 - b = aAk^2, \tag{2.15}$$

gdje su $k, A \in \mathbb{Z}$, A kvadratno slobodan, k i b relativno prosti (jer je b kvadratno slobodan). Uočimo da je A pozitivan jer

$$aAk^2 = \beta^2 - b > -b > -a.$$

Slijedi $Ak^2 \geq 0$, odnosno $Ak^2 > 0$ jer b nije potpun kvadrat. Supstitucijom $z - y\sqrt{b} = (\beta - \sqrt{b})(Z - Y\sqrt{b})$ dobivamo

$$z = bY + \beta Z, y = \beta Y + Z, \tag{2.16}$$

odnosno

$$z^2 - by^2 = (\beta^2 - b)(Z^2 - bY^2).$$

Tada jednadžba (2.9) glasi

$$ax^2 = aAk^2(Z^2 - bY^2)$$

Neka je $x = kAX$. Dobivamo

$$AX^2 + bY^2 = Z^2.$$

Ako ova jednadžba ima cjelobrojna rješenja, onda ih ima i jednadžba (2.9), uz supstituciju (2.16) i $x = kAX$. Dakle, novi koeficijent A je pozitivan i kvadratno slobodan, te zadovoljava

$$A = \frac{1}{ak^2}(\beta^2 - b) < \frac{\beta^2}{ak^2} \leq \frac{\beta^2}{a} \leq \frac{1}{4}a$$

iz čega slijedi $A < a$. Preostaje dokazati da koeficijenti A i b zadovoljavaju postavljene uvjete (2.12), (2.13) i (2.14).

Uvjet (2.13) glasi $b \equiv \beta^2 (\text{mod } A)$ zbog (2.15). Kako bismo pokazali analognu kongruenciju kongruenciji (2.12), podijelimo (2.15) s h:

$$h\beta_1^2 - b_1 = a_1 Ak^2, \tag{2.17}$$

gdje smo bili označili $a = ha_1$ i $b = hb_1$, odnosno $h = \gcd(a, b)$, te $\beta = h\beta_1$. Relacija (2.12) povlači $hb_1 \mid a_1 h - \alpha^2$ pa $h \mid \alpha^2$. Stoga je $\alpha = h\alpha_1$ (jer je h kvadratno slobodan) i $b_1 \mid a_1 - h\alpha_1^2$, tj.

$$a_1 \equiv h\alpha_1^2 \pmod{b_1}. \tag{2.18}$$

Kombiniranjem (2.17) i (2.18) dobivamo

$$h\beta_1^2 \equiv a_1 Ak^2 \equiv hA(\alpha_1 k)^2 \pmod{b_1}$$

Kako su h, k, α_1 relativno prosti s b_1, slijedi da je A kongruentan kvadratu modulo b_1. Također, množenjem kongruencije $-a_1 Ak^2 \equiv b_1 (\text{mod } h)$ s b_1 i prema (2.14) slijedi

$$A(k\gamma)^2 \equiv b_1^2 \pmod{h},$$

što znači da je A kongruentan kvadratu modulo h. Konačno, zaključujemo da je A kongruentan kvadratu modulo $hb_1 = b$.

Kako bismo dokazali da vrijedi (2.14), označimo s H najveći zajednički djelitelj brojeva A i b i stavimo $A = HA_2$, $b = Hb_2$. Jednadžbu (2.15) podijelimo s H pa imamo:

$$H\beta_2^2 - b_2 = aA_2k^2.$$

Sada slijedi

$$-A_2b_2 \equiv a(A_2k)^2 \pmod{H}.$$

Iz $a \equiv \alpha^2 (\mathrm{mod}\ H)$ slijedi da je $-A_2b_2$ kongruentno kvadratu modulo H, što je analogno (2.14). Time smo pokazali da koeficijenti A i b zadovoljavaju uvjete analogne onima koji vrijede za koeficijente a i b.

Daljnjim ponavljem postupka smanjivanja koeficijenta uz prvu nepoznanicu (x) jednadžbu bi u konačno mnogo koraka sveli na onu iz slučaja I, odnosno slučaja II, tj. na rješivu jednadžbu. Ta se metoda naziva *metoda spusta* a prvi ju je u 17. stoljeću primjenjivao Pierre de Fermat. Konačno, možemo zaključiti da su uvjeti dani kongruencijama (2.12), (2.13) i (2.14) nužni i dovoljni za rješivost jednadžbe (2.9) uz pretpostavku da su a i b kvadratno slobodni.

Kako bismo ilustrirali gornji dokaz, primijenimo postupak na primjeru.

Primjer 2.6. *Ispitajmo rješivost jednadžbe*

$$41x^2 + 31y^2 = z^2. \tag{2.19}$$

Rješenje. Koeficijenti su relativno prosti, pa imamo samo dva uvjeta:

$$41 \equiv \alpha^2 \pmod{31},\ 31 \equiv \beta^2 \pmod{41}$$

Obje kongruencije imaju rješenja, i to $\alpha \equiv \pm 14 \pmod{31}$ i $\beta \equiv \pm 20 \pmod{41}$. Zaista, u ovom slučaju rješivost jedne kongruencije povlači rješivost druge zbog Gaussovog kvadratnog zakona reciprociteta, jer su 31 i 41 različiti neparni prosti brojevi i jedan od njih je oblika $4k + 1$.

Sada trebamo odabrati vrijednost β i definirati A i k. Pretpostavili smo $|\beta| \leq \frac{1}{2}a$ pa uzmimo $\beta = 20$. Imamo:

$$\beta^2 - b = 400 - 31 = 9 \cdot 41$$

Dakle, $k = 3, A = 1$ iz čega zaključujemo da neće biti potrebno ponavljati postupak. Iz (2.19) imamo

$$X^2 + 31Y^2 = Z^2$$

Uočimo očito rješenje $(1, 0, 1)$. Veza između X, Y, Z i x, y, z je dana sa

$$z = 31Y + 20Z, y = 20Y + Z, x = 3X$$

pa zaključujemo da je rješenje početne jednadžbe $(x, y, z) = (3, 1, 20)$. $\diamondsuit$

2.3 Pellova jednadžba

Diofantska jednadžba oblika

$$x^2 - dy^2 = 1, \tag{2.20}$$

gdje je d prirodni broj koji nije potpuni kvadrat naziva se *Pellova jednadžba*. Njeno poopćenje,

$$x^2 - dy^2 = N, \tag{2.21}$$

za $N \in \mathbb{Z}$, naziva se *pellovska jednadžba*.

Jednadžbe (2.20) i (2.21) pobuđuju zanimanja matematičara kroz dugi niz godina. Za konkretne vrijednosti broja d, njima su se bavili starogrčki matematičari (5. st. prije Krista), zatim indijski matematičari (7. st.), te konačno europski matematičari 17. stoljeća. Velike zasluge za rješavanje Pellove jednadžbe pripadaju Lagrangeu (18. st.), no Euler zabunom pripisuje zasluge engleskom matematičaru Johnu Pellu i naziva ju po njemu.

Pellova jednažba (2.20) uvijek ima trivijalno rješenje u skupu cijelih brojeva $(\pm 1, 0)$. Za razliku od nje, pellovska jednadžba (2.21) ne mora biti rješiva u $\mathbb{Z}$. U onom što slijedi ispitat ćemo rješivost, u prvom redu Pellove jednadžbe, u skupu prirodnih brojeva. Najprije ćemo pokazati da Pellova jednadžba ima rješenja u $\mathbb{N}$ za svaki prirodni broj d koji nije potpun kvadrat. U tu svrhu koristimo sljedeću posljedicu Dirichletovog teorema:

Teorem 2.7. *Ako je α iracionalan broj, tada postoji beskonačno mnogo parova (p, q) relativno prostih cijelih brojeva takvih da je*

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

Teorem 2.8. *Neka je d prirodan broj koji nije potpun kvadrat. Postoji beskonačno mnogo parova prirodnih brojeva (x, y) koji zadovoljavaju nejednadžbu*

$$|x^2 - dy^2| < 1 + 2\sqrt{d}. \tag{2.22}$$

Dokaz. Broj $\sqrt{d}$ je iracionalan, pa prema Teoremu 2.7 postoji beskonačno mnogo parova prirodnih brojeva (x, y) takvih da je

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

Uočimo da vrijedi

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

odnosno

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

Iz toga slijedi

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

Kako postoji beskonačno mnogo ovakvih parova (x, y), zaključujemo da (2.22) ima beskonačno mnogo cjelobrojnih rješenja. □

Korolar 2.9. *Pellova jednadžba* (2.20) *ima rješenje* (u, v) *u skupu prirodnih brojeva, za svaki prirodan broj* d *koji nije potpuni kvadrat.*

Dokaz. Prema Teoremu 2.8 postoji cijeli broj k, $|k| < 1 + 2\sqrt{d}$, takav da vrijedi

$$x^2 - dy^2 = k \tag{2.23}$$

za beskonačno mnogo parova $(x, y) \in \mathbb{Z}^2$. U skupu tih parova postoje barem dva para $(x_1, y_1), (x_2, y_2)$ za koje vrijedi

$$x_1 \equiv x_2 \pmod{|k|}, \quad y_1 \equiv y_2 \pmod{|k|}. \tag{2.24}$$

Uočimo da vrijedi

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

Parovi (x_1, y_1) i (x_2, y_2) zadovoljavaju jednadžbu (2.23) pa iz $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k$ i (2.24) dobivamo

$$x_1x_2 - y_1y_2d \equiv x_1^2 - y_1^2d \equiv 0 \pmod{|k|},$$

$$x_1y_2 - x_2y_1 \equiv x_2y_2 - x_2y_2 \equiv 0 \pmod{|k|}.$$

Neka je

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

za $u, v \in \mathbb{Z}$. Sada imamo

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

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

Množenjem ovih jednadžbi dobivamo

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

Također vrijedi

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

iz čega zaključujemo $u^2 - dv^2 = 1$. Preostaje pokazati $v \neq 0$. Pretpostavimo suprotno, tj. neka je $v = 0$. Tada je $x_1y_2 - x_2y_1 = 0$, te $u = \pm 1$, iz čega dobivamo

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

odnosno

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

Dijeljenjem dobivene jednadžbe s k dobivamo $x_1 = \pm x_2$, te $y_1 = \pm y_2$. Uočimo da možemo odabrati x_1, x_2 takve da vrijedi $|x_1| \neq |x_2|$, iz čega slijedi $v \neq 0$. Dakle, dobili smo da Pellova jednadžba uvijek ima rješenje (u, v) u skupu prirodnih brojeva. □

Rješenje $(u, v) \in \mathbb{N}^2$ od (2.20) označavat ćemo kao element kvadratnog polja $\mathbb{Q}(\sqrt{d})$:

$$u + v\sqrt{d}.$$

Zahvaljujući toj oznaci lako možemo uvesti uređaj u skupu rješenja jednadžbe (2.20). Rješenje $u + v\sqrt{d}$ je veće od rješenja $u' + v'\sqrt{d}$ ako vrijedi nejednakost $u + v\sqrt{d} > u' + v'\sqrt{d}$. Najmanje rješenje Pellove jednadžbe u skupu prirodnih brojeva naziva se *fundamentalno rješenje* a označit ćemo ga s

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

Njegova važnost je u tome što se sva rješenja Pellove jednadžbe mogu generirati iz fundamentalnog rješenja. Naime, vrijedi sljedeći teorem koji opisuje sva rješenja od (2.20).

Teorem 2.10. *Neka je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe* (2.20). *Tada su sva rješenja od* (2.20) *dana formulom*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \ n \in \mathbb{N}. \tag{2.25}$$

Dokaz. Množenjem (2.25) sa $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ dobivamo

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

iz čega zaključujemo da su (x_n, y_n) zaista rješenja Pellove jednadžbe. Pokažimo još da nema drugih rješenja. Pretpostavimo da je $u + v\sqrt{d}, u, v \in \mathbb{N}$ rješenje Pellove jednadžbe koje nije oblika $(x_n, y_n), n \in \mathbb{N}$. Tada postoji $m \in \mathbb{N}$ za koji vrijedi

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

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

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

Neka je

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

Imamo

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

iz čega zaključujemo da je $a+b\sqrt{d}$ rješenje Pellove jednadžbe. Nadalje, iz $a+b\sqrt{d} > 1$ slijedi $0 < (a + b\sqrt{d})^{-1} < 1$, pa iz toga dobivamo

$$2a = a + b\sqrt{d} + (a - b\sqrt{d}) = a + b\sqrt{d} + (a + b\sqrt{d})^{-1} > 0,$$

$$2b\sqrt{d} = a + b\sqrt{d} - (a - b\sqrt{d}) = a + b\sqrt{d} - (a + b\sqrt{d})^{-1} > 0.$$

Dakle, (a, b) je rješenje Pellove jednadžbe u prirodnim brojevima i vrijedi

$$a + b\sqrt{d} < x_1 + y_1\sqrt{d},$$

što je u kontradikciji s činjenicom da je $x_1 + y_1\sqrt{d}$ fundamentalno rješenje Pellove jednadžbe. □

Napomena 2.11. Za sva rješenja Pellove jednadžbe koja su dana formulom $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ vrijedi

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

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

Za zaključiti je da sva rješenja Pellove jednadžbe leže na otkrivanju fundamentalnog rješenja. Jedna od strategija pomoću koje ćemo se sigurno dohvatiti fundamentalnog rješenja jest ispitivanjem redom je li broj $1 + dy^2$ jednak potpunom kvadratu za $y = 1, 2, \ldots$. Za neke specijalne vrijednosti broja d, na primjer $d = k^2 - 1$, fundametalno rješenje od (2.20) je očito - $k + \sqrt{k^2 - 1}$. No, postoji i niz primjera za koje to nije tako lako. Naime, već za relativno mali d vrijednost fundamentalnog rješenja može biti jako velika. Na primjer, za $d = 61$ fundamentalno rješenje od (2.20) je (1776319049, 22615390). Srećom, fundamentalno rješenje Pellove jednadžbe može se odrediti iz razvoja u verižni razlomak broja $\sqrt{d}$. Detaljno o tome može se naći u [8].

Primjer 2.12. *Ako je $a + b\sqrt{d}$ neko rješenje pellovske jednadžbe* (2.21) *za $N = -1$, onda je $(a + b\sqrt{d})^2$ Pellove jednadžbe* (2.20)*.*

Rješenje. Želimo pokazati da je $(a + b\sqrt{d})^2$ rješenje Pellove jednadžbe, odnosno da vrijedi

$$(a^2 - db^2)^2 = 1.$$

Iz činjenice da je $a + b\sqrt{d}$ rješenje Pellovske jednadžbe slijedi

$$(a - b\sqrt{d})(a + b\sqrt{d}) = -1.$$

Kvadriranjem dobivamo

$$(a - b\sqrt{d})^2(a + b\sqrt{d})^2 = (-1)^2,$$

iz čega slijedi

$$(a^2 - db^2)^2 = 1.$$

♢

Štoviše, slično kao u dokazu Teorema 2.10 može se pokazati da vrijedi:

Teorem 2.13. *Neka je $d \in \mathbb{N}$ koji nije potpun kvadrat i takav da je jednadžba* (2.21) *rješiva za $N = -1$. Ako je $u + v\sqrt{d}$ fundamentalno rješenje od* (2.21)*, tada je*

$$x_1 + y_1\sqrt{d} = (u + v\sqrt{d})^2 = u^2 + dv^2 + 2uv\sqrt{d}$$

fundamentalno rješenje Pellove jednadžbe (2.20)*.*

Primjer 2.14. *Pokažimo da jednadžba*

$$x^2 - 34y^2 = -1 \tag{2.26}$$

nema rješenja.

Rješenje. Uočimo da je $35 + 6\sqrt{34}$ fundamentalno rješenje Pellove jednadžbe $x^2 - 34y^2 = 1$. Ako jednadžba (2.26) ima rješenja, onda prema Teoremu 2.13 za njeno fundamentalno rješenje mora vrijediti

$$35 + 6\sqrt{34} = (u + v\sqrt{34})^2 = u^2 + 34v^2 + 2uv\sqrt{34}.$$

Otuda je

$$u^2 + 34v^2 = 35,\ uv = 3,$$

što očito nema cjelobrojnih rješenja. ♢

Bibliografija

[1] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations*, Birkhäuser, 2010.

[2] K. Burazin, *Nelinearne diofantske jednadžbe*, Osječki matematički list **7** (2007), 1, 11-21.

[3] K. Conrad, *Factoring in quadratic fields*, preprint, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/quadraticgrad.pdf` (srpanj 2019.)

[4] L. Costica, *Methods of solving Diophantine equations in secondary education in Romania*, `https://pdfs.semanticscholar.org/df29/73681593ffa1e19a487f0f36ff3ade85be7e.pdf` (srpanj 2019.)

[5] H. Davenport, *The higher arithmetic: An introduction to the theory of numbers*, Cambridge University Press, 1999.

[6] A. Dujella, *Diofantske jednadžbe*, skripta, Sveučilište u Zagrebu, `https://web.math.pmf.unizg.hr/~duje/dioph/dioph.pdf` (srpanj 2019.)

[7] A. Dujella, *Uvod u teoriju brojeva*, skripta, Sveučilište u Zagrebu, `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf` (srpanj 2019.)

[8] A.Dujella, *Teorija brojeva*, rukopis

[9] A. Kopecki, *Diofant i diofantske jednadžbe*, diplomski rad, Sveučilište J.J. Strossmayera u Osijeku, 2011., `http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/KOP08.pdf` (kolovoz 2019.)

[10] T. Nagell, *Introduction to Number Theory*, John Wiley and Sons, NY, 1952.

[11] I. Petrić, *Gaussovi cijeli brojevi*, završni rad, Sveučilište J.J. Strossmayera u Osijeku, 2016., `https://zir.nsk.hr/islandora/object/mathos%3A83/datastream/PDF/view` (lipanj 2019.)

[12] I. Užar, *Gaussovi cijeli brojevi*, završni rad, Sveučilište J.J. Strossmayera u Osijeku, 2011., `http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/U%C5%BEA01.pdf` (lipanj 2019.)

Sažetak

Diofantska jednadžba je jednadžba oblika

$$f(x_1, x_2, \ldots, x_n) = 0,$$

gdje je f polinom s cjelobrojnim koeficijentima, te za koju tražimo samo cjelobrojna rješenja. U ovom diplomskom radu prikazujemo neke metode rješavanja diofantskih jednadžbi kao što su metoda faktorizacije, metoda matematičke indukcije, te parametarska metoda. Također, prezentiramo neke napredne metode koje uključuju Gaussove cijele brojeve i kvadratna polja. Jedno poglavlje posvećeno je nekim klasičnim diofantskim jednadžbama kao što su Pitagorina i Pellova jednadžba.

Summary

A *diophantine equation* is an equation of the form

$$f(x_1, x_2, \ldots, x_n) = 0,$$

where f is a polynomial with integral coefficients and such that only integer solutions are sought. In this diploma thesis, we present some methods in solving Diophantine equations such as decomposition method, parametric method, method of mathematical induction. Also, we introduce some advanced methods involving Gaussian integers and quadratic fields. One chapter is devoted to some classical Diophantine equations like Pythagorean-type equations and Pell's equation.

Životopis

Rođena sam 6. prosinca 1995. godine u Sisku. Svoje obrazovanje započela sam u Osnovnoj školi Braće Ribara u Sisku. Nakon završene osnovne škole, srednjoškolsko obrazovanje stekla sam u Gimaziji Sisak. Zatim sam 2014. godine upisala Preddiplomski sveučilišni studij Matematika, smjer nastavnički na matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Nakon stjecanja prvostupničke diplome, 2017. godine upisala sam Diplomski sveučilišni studij Matematika, smjer nastavnički na istom fakultetu.