Elementarne metode za rješavanje diofantskih jednadžbi

Tokić, Vedrana

Undergraduate thesis / Završni rad

2019

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:126:096096

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science

zir.nsk.hr

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Vedrana Tokić

Elementarne metode za rješavanje diofantskih jednadžbi

Završni rad

Osijek, 2019.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Vedrana Tokić

Elementarne metode za rješavanje diofantskih jednadžbi

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2019.

Sažetak: U ovom radu proučit ćemo elementarne metode za rješavanje diofantskih jednadžbi. Prvi dio rada bazira se na linearnim diofantskim jednadžbama i Euklidovom algoritmu i njegovoj važnosti u rješavanju ovog tipa jednadžbi. Osim toga, u radu su opisane metode za rješavanje nelinearnih diofantskih jednadžbi i Pitagorina jednadžba. Sve navedene metode rješavanja demonstrirane su na primjerima.

Ključne riječi: Euklidov algoritam, Teorem o dijeljenju s ostatkom, linearane diofantske jednadžbe, nelinearne diofantske jednadžbe, Pitagorina jednadžba, Pitagorine trojke

Elementary methods for solving Diophantine equations

Abstract: In this paper we will study elementary methods for solving Diophantine equations. The first part of the paper is based on linear Diophantine equations, Euclidean algorithm and its importance in solving these types of equations. Furthermore, methods for solving nonlinear Diophantine equations and Pythagorean equation are described in the second part. Examples are used to demonstrate each method.

Key words: Euclidean algorithm, the Division theorem, linear Diophantine equations, nonlinear Diophantine equations, Pythagorean equation, Pythagorean triplets

Sadržaj

Uvod **1**

1. Linearne diofantske jednadžbe **2**

1.1. Euklidov algoritam 2

1.2. Definicija i karakterizacija rješivosti linearnih diofantskih jednadžbi 3

1.3. Homogeni sustavi linearnih diofantskih jednadžbi 7

2. Nelinearne diofantske jednadžbe **8**

2.1. Metoda faktorizacije 8

2.2. Rješavanje diofantskih jednadžbi pomoću nejednakosti 9

2.3. Metoda kvocijenta 10

2.4. Metoda zbroja 12

2.5. Metoda ostataka 12

2.6. Metoda posljednje znamenke 12

2.7. Metoda parnosti 13

2.8. Metoda karakterističnih ostataka 13

2.9. Metoda matematičke indukcije 14

2.10. Fermatova metoda beskonačnog spusta 15

3. Pitagorina jednadžba **16**

Literatura **18**

Uvod

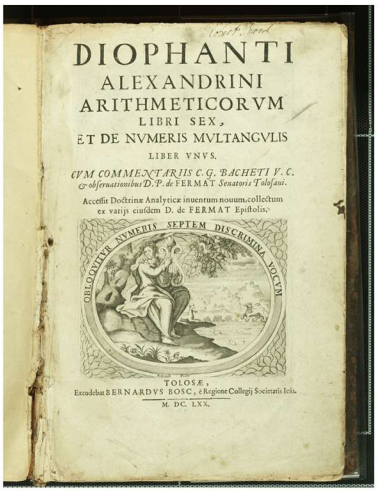


Slika 1: Diofant

Diofant, koji se smatra "ocem matematike", bio je grčki matematičar o čijem životu vrlo malo znamo. Ne mogu se točno odrediti godine njegovog djelovanja, no pretpostavlja se da je djelovao negdje između 350. i 150. g. pr. Kr., točnije većina povjesničara smatra da je Diofant živio oko 250. g. pr. Kr. što pripada Srebrnom dobu matematike. Ono što se zasigurno zna jest da je Diofant živio u Aleksandriji koja je u ono vrijeme bila središte proučavanja matematike. Najpoznatije njegovo djelo je "Aritmetika" (Slika 2), za koje se vjeruje da je originalno imalo 13 knjiga, no do danas je sačuvano samo 6. Djelo je vrlo značajno za sve grane matematike pa tako i za teoriju brojeva. Sastoji se od 150 problema koji daju aproksimacije rješenja jednadžbama do trećeg stupnja. Diofant je bio prvi koji je uveo simbole za nepoznanice u algebru, a koristio je i simbole za računske operacije.

U ovom radu napravit ćemo pregled elementarnih metoda za rješavanje diofantskih jednadžbi. Glavna pitanja na koja ćemo tražiti odgovor jesu: Je li diofantska jednadžba rješiva? Kako ju riješiti? Koja su rješenja? Ima li beskonačno mnogo ili konačno mnogo rješenja?

Rad je sistematiziran u 3 dijela, podjela na linearne i nelinarne diofantske jednadžbe te Pitagorina jednadžba. U prvom poglavlju bavimo se Euklidovim algoritmom i linearnim diofantskim jednadžbama, u drugom poglavlju nelineranim diofantskim jednadžbama i metodama koje se koriste za njihovo rješavanje, a treće poglavlje rješavanjem Pitagorine jednadžbe i Pitagorinim trojkama. Svaku od metoda za rješavanje ćemo opisati, a zatim pokazati na primjerima.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& observationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex variis eiusdem D. de FERMAT Epistolis.
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Slika 2: Aritmetika

1. Linearne diofantske jednadžbe

Za početak objasnit ćemo Euklidov algoritam za pronalaženje najvećeg zajedničkog djelitelja koji je vrlo bitan u rješavanju linearnih diofantskih jednadžbi.

1.1. Euklidov algoritam

Euklid je grčki matematičar koji je živio i djelovao oko 3.st.pr.Kr. u Aleksandriji. Njegov algoritam smatra se jednim od najstarijih, ali i najvažnijih algoritama u teoriji brojeva. Najprije navodimo teorem na kojem se bazira Euklidov algoritam, a zatim ćemo dokazati lemu koja se koristi kod Euklidovog algoritma.

Teorem 1.1 (Teorem o dijeljenju s ostatkom)**.** *Za $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ postoje jedinstveni cijeli brojevi q i r tako da je $b = aq + r$, $0 \leq r < a$.*

Lema 1.1. *Neka je a proizvoljan prirodan broj, b cijeli broj i $b = aq + r$, $0 \leq r < a$. Tada je $(a, b) = (a, r)$.*

Dokaz. Neka je $d_1 = (a, b)$ i $d_2 = (a, r)$. Kako je $b = aq + r$, možemo zaključiti da d_1 dijeli r jer $d_1|b$ i $d_1|a$, što znači da je d_1 zajednički djelitelj od a i r te da je $d_1 \leq d_2$ jer znamo da je d_2 njihov najveći zajednički djelitelj.
S druge strane, $b = aq + r$ i $d_2|a$ te $d_2|r$ što znači da d_2 dijeli b. Zaključujemo da je d_2 zajednički djelitelj od a i b što znači da je $d_2 \leq d_1$. Slijedi $d_1 = d_2$. □

Neka je b proizvoljan cijeli broj, a n proizvoljan prirodan broj. Uzastopnom primjenom Teorema o dijeljenju s ostatkom dobijamo sljedeći niz jednakosti:

$$\begin{aligned}
b &= aq_1 + r_1, \quad 0 \leq r_1 < a,\\
a &= r_1q_2 + r_2, \quad 0 \leq r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, \quad 0 \leq r_3 < r_2,\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Postupak završava kada je 0 ostatak, a znamo da postupak mora završiti u konačno mnogo koraka jer su svi $a, r_1, r_2, \ldots, r_n$ odozdo omeđeni s 0.
Primjenom Leme 1.1. zaključujemo $(a, b) = (a, r_1) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n$, što znači da je najveći zajednički djelitelj od a i b jednak posljednjem ostatku različitom od 0 u gornjem postupku kojeg nazivamo **Euklidov algoritam**.
Uočimo da iz gornjeg niza jednakosti slijedi da je svaki r_i linearna kombinacija brojeva a i b jer je r_1 linearna kombinacija brojeva a i b, r_2 je linearna kombinacija r_1 i a itd. Iz toga zaključujemo da iz Euklidovog algoritma možemo dobiti brojeve x i y sa svojstvom:

$$ax + by = (a, b).$$

Primjer 1.1. *Nađite najveći zajednički djelitelj brojeva* 555 *i* 155.

Rješenje: Provedimo Euklidov algoritam. Uočimo da vrijedi:

$$\begin{aligned} 555 &= 155 \cdot 3 + 90, \\ 155 &= 90 \cdot 1 + 65, \\ 90 &= 65 \cdot 1 + 25, \\ 65 &= 25 \cdot 2 + 15, \\ 25 &= 15 \cdot 1 + 10, \\ 15 &= 10 \cdot 1 + 5, \\ 10 &= 5 \cdot 2. \end{aligned}$$

Primijetimo da je zadnji ostatak različit od 0 jednak 5 što znači da je $(555, 155) = 5$.

1.2. Definicija i karakterizacija rješivosti linearnih diofantskih jednadžbi

Definicija 1.1. *Neka su* $a_1, ..., a_n, b \in \mathbb{Z}$, $a_1, ..., a_n \neq 0$ *i* $n \geq 1$. *Linearna diofantska jednadžba s* n *nepoznanica je jednadžba oblika*

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

Promotrimo slučaj $n = 2$.

Teorem 1.2. *Neka je* $ax + by = c$, $a, b, c \in \mathbb{Z}$, $a, b \neq 0$. *Jednadžba ima cjelobrojna rješenja ako i samo ako* $d = (a, b)$ *dijeli* c. *Ako je* (x_0, y_0) *jedno partikularno rješenje jednadžbe, onda je svako rješenje oblika*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{b}{d}t, \quad t \in \mathbb{Z}.$$

Dokaz. Ako jednadžba ima rješenja, očito $d|c$ jer $d|a$ i $d|b$. Pretpostavimo da d dijeli c i promotrimo kongruenciju:

$$ax \equiv c \pmod{b}.$$

Znamo da ova kongruencija ima rješenja (Teorem 2.6.,[5]) ako i samo ako $(a, b)|c$ što je po pretpostavci zadovoljeno. Nadalje, znamo da ako je x_0 rješenje kongruencije

$$\frac{a}{d}x \equiv \frac{c}{d} \pmod{\frac{b}{d}},$$

onda su sva međusobno nekongruentna rješenja modulo b prve kongruencije dana s (Teorem 2.1.9., [7]):

$$x_0, x_0 + \frac{b}{d}, \ldots, x_0 + (d-1) \cdot \frac{b}{d}.$$

Stoga zaključujemo da su sva rješenja linearne diofantske jednadžbe dana s:

$$x = x_0 + \frac{b}{d}t, \quad t \in \mathbb{Z}.$$

Uvrstimo li to u jednadžbu dobivamo i da je

$$y = y_0 - \frac{b}{d}t, \quad t \in \mathbb{Z}.$$

□

Analogan zaključak vrijedi za proizvoljan $n > 2$.

Teorem 1.3. *Linearna diofantska jednadžba* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, $a_i, b \in \mathbb{Z}$, $a_i \neq 0$, $i = 1, \ldots, n$ *ima rješenja ako i samo ako* $d = (a_1, a_2, \ldots, a_n)$ *dijeli* b. *U tom slučaju svako se rješenje može zapisati pomoću* $n - 1$ *cjelobrojnih parametara.*

Dokaz. Pretpostavimo da postoje $x_1, \ldots, x_n$ takvi da $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$. Kako d dijeli svaki od pribrojnika s lijeve strane jednakosti slijedi da $d|b$.
S druge strane, pretpostavimo da $d|b$. Podijelimo li cijelu jednadžbu s d, dobijemo:

$$k_1x_1 + k_2x_2 + \cdots + k_nx_n = b', \qquad k_i = \frac{a_i}{d}, \quad b' = \frac{b}{d}, \quad (k_1, \ldots, k_n) = 1. \tag{1}$$

Indukcijom po n pokazat ćemo da (1) ima rješenja i da ih možemo izraziti pomoću $n - 1$ parametara.
Za bazu indukcije uzmimo $n = 1$, to jest $k_1x_1 = b', d = k_1$. Očito je rješenje jednadžbe $x_1 = \frac{b'}{k_1}$ i rješenje nismo izrazili pomoću parametra. Pretpostavimo zatim da jednadžba (1) ima rješenja u slučaju $n-1$ varijabli i da se rješenje može zapisati pomoću $n-2$ parametra. Neka je $d_1 = (k_1, \ldots, k_{n-1})$. Kako je $(k_1, \ldots, k_n) = 1$, možemo zaključiti $(d_1, k_n) = 1$. Pogledajmo jednadžbu (1) i ostatke nakon dijeljenja s d_1:

$$k_1x_1 + k_2x_2 + \cdots + k_nx_n \equiv b' \pmod{d_1}.$$

Zbog definicije d_1 znamo da je prvi dio jednadžbe kongruentan 0 modulo d_1, stoga nam ostaje:

$$k_nx_n \equiv b' \pmod{d_1}. \tag{2}$$

Već smo zaključili da $(k_n, d_1) = 1$, što znači da ova konguencija ima jedinstveno rješenje modulo d_1. Označimo ga s c. Onda je:

$$x_n \equiv c \pmod{d_1},$$

što je ekivalentno zapisu $x_n = c + t_nd_1, t_n \in \mathbb{Z}$. Dobili smo prvi parametar. Zapišimo jednadžbu (1) u drugačijem obliku, to jest:

$$k_1x_1 + k_2x_2 + \cdots + k_{n-1}x_{n-1} = b' - k_nx_n. \tag{3}$$

Iz (2) zaključujemo da $d_1|k_nx_n - b'$, što znači da jednadžbu (3) možemo zapisati u obliku:

$$m_1x_1 + m_2x_2 + \cdots + m_{n-1}x_{n-1} = b'', \quad m_i = \frac{k_i}{d_1}, \quad b'' = \frac{b' - k_nx_n}{d_1}, \quad (m_1, \ldots, m_{n-1}) = 1. \tag{4}$$

Na jednadžbu (4) možemo primijeniti pretpostavku indukcije jer je to jednadžba s $n - 1$ nepoznanica što znači da ima rješenja i ona se mogu prikazati pomoću $n - 2$ parametara. Kad tome pridodamo parametar koji smo prethodno izračunali za jednadžbu (1), dolazimo do $n - 1$ parametara čime je dokaz potpun. □

Primjer 1.2. *Riješite sljedeću diofantsku jednadžbu:* $8x + 4y + 5z = 1$.

Rješenje: Za početak pronađemo najvećeg zajedničkog djelitelja od $8, 4, 5$ i pogledamo dijeli li on desnu stranu jednadžbe. U ovom slučaju lako vidimo $(8, 4, 5) = 1$ i $1|1$ što znači da rješenje postoji i da ga možemo zapisati pomoću 2 parametra. Prebacimo jednu nepoznanicu na desnu stranu, na primjer z:

$$8x + 4y = 1 - 5z.$$

Znamo da je $(8, 4) = 4$ i da bi ova jednadžba bila rješiva, mora vrijediti: $4|1 - 5z$ što znači da postoji neki $t \in \mathbb{Z}$ takav da je $4t = 1 - 5z$, to jest $4t + 5z = 1$. Ovo možemo riješiti Euklidovim algoritmom, no lako možemo vidjeti da je jedno rješenje ove jednadžbe $t_0 = -1, z_0 = 1$. Prema Teoremu 1.2. znamo da su onda sva rješenja te jednadžbe dana s:

$$\begin{aligned} t &= -1 + 5s, \\ z &= 1 - 4s, \end{aligned}$$

pri čemu je $s \in \mathbb{Z}$. Izrazili smo z preko parametra i uvrstimo ga u početnu jednadžbu:

$$\begin{aligned} 8x + 4y &= -4 + 20s, \\ 2x + y &= -1 + 5s. \end{aligned}$$

Pogledajmo sada jednadžbu $2x' + y' = 1$. Jedno njeno rješenje jest $x'_0 = 1, y'_0 = -1$, stoga zaključujemo da je jedno rješenje prethodne jednadžbe:

$$\begin{aligned} x_0 &= 1 \cdot (-1 + 5s), \\ y_0 &= -(-1 + 5s), \end{aligned}$$

odnosno, konačna rješenja su:

$$\begin{aligned} x &= -1 + 5s + n, \\ y &= 1 - 5s - 2n, \qquad s, n \in \mathbb{Z}. \\ z &= 1 - 4s, \end{aligned}$$

Primjer 1.3. *Riješite sljedeću diofantsku jednadžbu:* $464x - 123y = 3$.

Rješenje: U ovom primjeru je teško "pogoditi" jedno rješenje pa ćemo se poslužiti Euklidovim algoritmom i na taj način doći do rješenja.

$$\begin{aligned} 464 &= 123 \cdot 3 + 95, \\ 123 &= 95 \cdot 1 + 28, \\ 95 &= 28 \cdot 3 + 11, \\ 28 &= 11 \cdot 2 + 6, \\ 11 &= 6 \cdot 1 + 5, \\ 6 &= 5 \cdot 1 + 1, \\ 5 &= 1 \cdot 5. \end{aligned}$$

Iz gornih jednakosti izrazimo ostatke:

$$\begin{aligned} 95 &= 464 - 123 \cdot 3, \\ 28 &= 123 - 95 \cdot 1, \\ 11 &= 95 - 28 \cdot 3, \\ 6 &= 28 - 11 \cdot 2, \\ 5 &= 11 - 6 \cdot 1, \\ 1 &= 6 - 5 \cdot 1. \end{aligned}$$

Uvrstimo u posljednju jednažbu umjesto 5 izraz koji smo dobili u prethodnom koraku, zatim za 6 i tako do kraja, dobivamo:

$$\begin{aligned} 1 &= 6 - (11 - 6 \cdot 1) \cdot 1 = 6 - 11 + 6 = 6 \cdot 2 - 11 \\ &= (28 - 11 \cdot 2) \cdot 2 - 11 = 2 \cdot 28 - 5 \cdot 11 \\ &= 2 \cdot 28 - 5 \cdot (95 - 28 \cdot 3) = 17 \cdot 28 - 5 \cdot 95 \\ &= 17 \cdot (123 - 95 \cdot 1) - 5 \cdot 95 = 17 \cdot 123 - 22 \cdot 95 \\ &= 17 \cdot 123 - 22 \cdot (464 - 123 \cdot 3) = -22 \cdot 464 + 83 \cdot 123. \end{aligned}$$

Dakle, $1 = -22 \cdot 464 + 83 \cdot 123$ pa množenjem s 3 dobijemo:

$$3 = -66 \cdot 464 + 249 \cdot 123,$$

što znači da je jedno rješenje $x_0 = -66, y_0 = -249$. Sada lako dobijemo konačno rješenje koje glasi:

$$\begin{aligned} x &= -66 - 123t, \\ y &= -249 - 464t, \end{aligned}$$

pri čemu je $t \in \mathbb{Z}$.

Primjer 1.4. *Za ljuštenje ječma koristimo dva stroja. U prvi stane 400 kg ječma, a u drugi 250 kg. Koliko ćemo puta puniti svaki od njih dok ne oljuštimo 5 tona ječma?*

Rješenje: Označimo li broj punjenja prvog stroja s x, a drugog s y, dobivamo jednadžbu:

$$\begin{aligned} 400x + 250y &= 5000, \quad \text{tj.} \\ 8x + 5y &= 100. \end{aligned}$$

Lako možemo vidjeti partikularno rješenje $x_0 = 10$ i $y_0 = 4$, što znači da je opće rješenje:

$$\begin{aligned} x &= 10 + 5t, \\ y &= 4 - 8t, \end{aligned}$$

gdje je $t \in \mathbb{Z}$. Kako bi rješenje imalo smisla, očito mora biti $x, y \geq 0$, tj.

$$\begin{aligned} 10 + 5t &\geq 0, \\ 4 - 8t &\geq 0, \end{aligned}$$

iz čega možemo izvući t:

$$-\frac{5}{2} \leq t \leq \frac{1}{2}.$$

Kako t mora biti cijeli broj, jedini koji zadovoljavaju ovu nejednakost su $t \in \{-2, -1, 0\}$, što znači da imamo 3 konačna rješenja: $(0, 20), (5, 12), (10, 4)$.

1.3. Homogeni sustavi linearnih diofantskih jednadžbi

Homogena linearna diofantska jednadžba je oblika:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0, \quad a_i, \in \mathbb{Z}, \quad a_i \neq 0, \quad i = 1, \ldots, n,$$

a homogeni sustav sastoji se od dvije ili više takvih jednadžbi.
Promotrimo homogeni sustav od 2 linearne diofantske jednadžbe s 3 nepoznanice:

$$\begin{aligned} a_1x + a_2y + a_3z &= 0, \\ b_1x + b_2y + b_3z &= 0. \end{aligned}$$

Neka je barem jedan od sljedećih izraza različit od 0:

$$a_1b_2 - a_2b_1, \quad a_2b_3 - a_3b_2, \quad a_1b_3 - a_3b_1.$$

Bez smanjenja općenitosti možemo uzeti $a_1b_2 - a_2b_1 \neq 0$. Pokažimo da uz ovaj uvjet sustav zaista ima rješenja. Neka je $z \neq 0$. Zapišimo sustav u sljedećem obliku:

$$\begin{aligned} a_1\frac{x}{z} + a_2\frac{y}{z} &= -a_3, \\ b_1\frac{x}{z} + b_2\frac{y}{z} &= -b_3. \end{aligned}$$

Zbog uvjeta $a_1b_2 - a_2b_1 \neq 0$ determinanta ovog sustava različita je od 0 i sustav možemo riješiti Cramerovim pravilom ili pomoću inverzne matrice. Nakon rješavanja dobivamo sljedeće izraze:

$$\begin{aligned} x &= \frac{t}{m}\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \\ y &= \frac{t}{m}\begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}, \\ z &= \frac{t}{m}\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}, \end{aligned}$$

gdje je m najveći zajednički djelitelj brojeva $\begin{vmatrix} a_1 & a_2 \\ a_2 & a_3 \end{vmatrix}$, $\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}$, $\begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}$, a $t \in \mathbb{Z}$ i to su sva cjelobrojna rješenja sustava.

Primjer 1.5. *Riješite sustav:*

$$\begin{aligned} 3x - 5y + z &= 0, \\ x + 2y - 3z &= 0. \end{aligned}$$

Rješenje: Nakon uvrštavanja u gornje formule lako dobijemo rješenja:

$$\begin{aligned} x &= 13t, \\ y &= 10t, \qquad t \in \mathbb{Z}. \\ z &= 11t, \end{aligned}$$

Do izraza za cjelobrojna rješenja nehomogenih sustava linearnih diofantskih jednadžbi jednostavno dolazimo svodeći ih na homogene. Više o ovoj temi možete pogledati u [8].

2. Nelinearne diofantske jednadžbe

Nelinearne diofantske jednadžbe su one diofantske jednadžbe u kojima se pojavljuju nepoznanice višeg reda, odnosno pojavljuju se primjerice x^2, y^3 i slično. Ne postoji univerzalan postupak kojim bi se ove jednadžbe mogle rješavati stoga navodimo neke elementarne metode koje mogu pomoći u pronalasku rješenja ili barem eliminiranju nekih potencijalnih rješenja.

2.1. Metoda faktorizacije

Neka je diofantska jednadžba oblika $f(x_1, x_2, ..., x_n) = b$. Prema Osnovnom teoremu aritmetike znamo da b možemo faktorizirati i da je ta faktorizacija jedinstvena do na poredak faktora. Bez smanjenja općenitosti, neka je $b = b_1 \cdot b_2 \cdots b_k$. Zapišimo polinom f u obliku produkta k polinoma s cjelobrojnim koeficijentima i dobivamo sljedeći sustav:

$$\begin{aligned} f_1(x_1, x_2, ..., x_n) &= b_1, \\ f_2(x_1, x_2, ..., x_n) &= b_2, \\ &\vdots \\ f_k(x_1, x_2, ..., x_n) &= b_k. \end{aligned}$$

Rješavanjem ovih jednadžbi dobivamo rješenje početne diofantske jednadžbe.

Primjer 2.1. *Riješite jednadžbu* $xy - 2y - 6 = 0$.

Rješenje: Zapišimo jednadžbu u drugačijem obliku:

$$\begin{aligned} xy + y - 3y - 6 &= 0, \\ xy + y - 3y - 3 &= 3, \\ x(y+1) - 3(y+1) &= 3, \\ (x-3)(y+1) &= 3, \end{aligned}$$

Dolazimo do sljedećih sustava:

$x-3=3$ $y+1=1$	$x-3=1$ $y+1=3$	$x-3=-3$ $y+1=1$	$x-3=-1$ $y+1=-3$
$x=6$ $y=0$	$x=4$ $y=2$	$x=0$ $y=-2$	$x=2$ $y=-4$

To su ujedno i rješenja zadane diofantske jednadžbe.

Primjer 2.2. *([1]) Riješite jednadžbu* $(xy-7)^2 = x^2 + y^2$, *pri čemu su* x, y *cijeli brojevi.*

Rješenje: Faktorizirajmo jednadžbu:

$$\begin{aligned} (xy-7)^2 &= x^2 + y^2, \\ x^2y^2 - 14xy + 49 &= x^2 + y^2, \\ x^2y^2 - 12xy + 49 &= x^2 + 2xy + y^2, \\ (xy-6)^2 + 13 &= (x+y)^2, \\ (x+y)^2 - (xy-6)^2 &= 13, \\ (x+y+xy-6)(x+y-xy+6) &= 13. \end{aligned}$$

Znamo da je 13 prost broj pa stoga lako zaključujemo da faktori mogu biti samo $(1, 13), (13, 1)$, $(-1, -13), (-13, -1)$. Uzmimo na primjer $(1, 13)$. Tada je:

$$x + y + xy - 6 = 1,$$
$$x + y - xy + 6 = 13.$$

Zbrojimo li ove dvije jednadžbe dobivamo $x + y = 7$. Primijetimo da isto dobivamo i ako uzmemo $(13, 1)$. Možemo izraziti $x = 7 - y$ i vratiti u početnu jednadžbu. Nakon što nađemo y i izračunamo pripadne x dobivamo sljedeća rješenja: $(7, 0), (4, 3), (3, 4), (0, 7)$. Provjerimo sada slučaj s negativnim faktorima. Analogno dobijemo $x + y = -7$ i na isti način dođemo do rješenja $(7, 0), (-4, -3), (-3, -4), (0, -7)$.

Primjer 2.3. *Ako zbroju godina brata i sestre dodamo njihov umnožak, dobijemo* 76. *Tko je stariji i koliko?*

Rješenje: Označimo s x broj bratovih godina, a s y broj sestrinih godina. Sada nam problem glasi:

$$x + y + xy = 76.$$

Dodamo i oduzmemo 1 te jednadžbu zapišemo u drugačijem obliku:

$$x + y + xy + 1 = 76 + 1,$$
$$x + 1 + y(x + 1) = 77,$$
$$(x + 1)(y + 1) = 77.$$

Broj 77 možemo rastaviti na faktore 7 i 11, što znači da imamo 4 mogućnosti:

a) $x + 1 = 1$, $y + 1 = 77$: ova mogućnosti nam ne odgovara jer $x = 0$.

b) $x + 1 = 7$, $y + 1 = 11$: lako dobijemo $x = 6$ i $y = 10$, što znači da je sestra starija 4 godine.

c) $x + 1 = 11$, $y + 1 = 7$: vidimo $x = 10$ i $y = 6$, što znači da je brat stariji 4 godine.

d) Analognim računom kao u a) dobijemo $y = 0$, što nam ne odgovara.

2.2. Rješavanje diofantskih jednadžbi pomoću nejednakosti

U ovoj se metodi koriste nejednakosti kako bismo precizirali interval u kojemu se nalaze nepoznanice i na taj način reducirali broj rješenja, a onda na tom intervalu razlikujemo slučajeve.

Primjer 2.4. *Riješite jednadžbu* $3^x + 5^x = 8^x$.

Rješenje: Očito je da je $x = 1$ jedno rješenje sustava. Podijelimo cijelu jednadžbu s 8^x. Dobivamo:

$$\left(\frac{3}{8}\right)^x + \left(\frac{5}{8}\right)^x = 1.$$

Za $x < 1$:

$$\left(\frac{3}{8}\right)^x + \left(\frac{5}{8}\right)^x > \frac{3}{8} + \frac{5}{8} = 1.$$

U suprotnom, za $x > 1$:

$$\left(\frac{3}{8}\right)^x + \left(\frac{5}{8}\right)^x < \frac{3}{8} + \frac{5}{8} = 1.$$

Dakle, $x = 1$ je jedino rješenje zadane jednadžbe.

Primjer 2.5. *([1]) Pronađite rješenja jednadžbe* $3(xy + yz + zx) = 4xyz$ *u prirodnim brojevima.*

Rješenje: Zapišemo li zadanu jednadžbu u drugačijem obliku, dobijamo:

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{4}{3}.$$

Bez smanjenja općenitosti, neka je $x \leq y \leq z$. Tada iz

$$\frac{4}{3} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} \leq \frac{3}{x},$$

slijedi da je $x \leq \frac{9}{4}$, odnosno $x \in \{1, 2\}$. Ako je $x = 1$, tada iz

$$\frac{1}{3} = \frac{1}{y} + \frac{1}{z} \leq \frac{2}{y},$$

slijedi da je $y \leq 6$, odnosno $y \in \{1, 2, 3, 4, 5, 6\}$. Jednostavnim uvrštavanjem lako možemo zaključiti da nam odgovaraju jedino $y \in \{4, 6\}$ i kao rješenje dobijemo $(1, 4, 12), (1, 6, 6)$. Neka je sada $x = 2$. Onda je

$$\frac{5}{6} = \frac{1}{y} + \frac{1}{z} \leq \frac{2}{y},$$

iz čega zaključujemo $y \leq \frac{12}{5}$, tj. $y \in \{1, 2\}$. Kako je $x = 2$, a $x \leq y$, odmah možemo eliminirati $y = 1$. Uvrštavanjem u jednadžbu dolazimo do trećeg rješenja $(2, 2, 3)$.

2.3. Metoda kvocijenta

Ova metoda je vrlo slična metodi faktorizacije, samo što u ovom slučaju lijevu stranu jednadžbe nastojimo zapisati u obliku kvocijenta, odnosno razlomka, a na desnoj strani ostavimo cijeli broj. Na ovaj način brzo dolazimo do rješenja jer znamo da razlomak mora biti cijeli broj.

Primjer 2.6. *Nađite cjelobrojna rješenja jednadžbe* $x + y^2 + xy = 2$.

Rješenje: Izrazimo iz jednadžbe na primjer x. Budući da je:

$$x = \frac{2 - y^2}{y + 1} = \frac{-y^2 + 2 + y - y}{y + 1} = \frac{-y(y + 1) + y + 1 + 1}{y + 1} = -y + 1 + \frac{1}{y + 1}.$$

Kako tražimo cjelobrojan x, to znači da $y + 1$ mora dijeliti 1 pa je očito $y + 1 \in \{-1, 1\}$. Iz toga slijedi da je $y \in \{-2, 0\}$, a za oba rješenja pripadni x jednak je 2.

Primjer 2.7. *([6]) Pronađite dvoznamenkaste brojeve čiji je umnožak jednak njihovu desterostrukom zbroju.*

Rješenje: Zadatak preveden u jednadžbu glasi

$$xy = 10(x + y),$$

gdje je x prvi dvoznamenkasti broj, a y drugi. Izrazimo y pomoću x:

$$\begin{aligned} xy - 10y &= 10x, \\ y(x - 10) &= 10x, \\ y &= \frac{10x}{x - 10}, \\ y &= 10 + \frac{100}{x - 10}, \end{aligned}$$

pri čemu $\frac{100}{x-10}$ mora biti cijeli broj. Uvjet da su brojevi dvoznamenkasti je očito zadovoljen jer vidimo da su x i y sigurno veći od 10. Iz navedenog izraza lako vidimo da su traženi brojevi: 12 i 60, 14 i 35, 15 i 30, 20 i 20.

Primjer 2.8. *([6]) Nađite najmanji prirodni broj koji pri dijeljenju sa* 7 *daje ostatak* 6*, a njegov kvadrat pri dijeljenju sa* 7^2 *daje ostatak* 43*.*

Rješenje: Označimo s x traženi broj. Tada vrijedi:

$$\begin{aligned} 7k + 6 &= x, \\ 7^2m + 43 &= x^2, \end{aligned}$$

pri čemu su $k, m \in \mathbb{N}$. Možemo kvadrirati prvu jednadžbu i zatim izjednačiti prvu i drugu jednadžbu:

$$\begin{aligned} 49k^2 + 84k + 36 &= 49m + 43, \\ 7k^2 - 7m + 12k &= 1, \\ 7m &= 7k^2 + 12k - 1, \\ m &= k^2 + \frac{12k - 1}{7}. \end{aligned}$$

Da bi m bio prirodan broj, očito $\frac{12k-1}{7}$ mora biti prirodan broj, označimo ga s l. Iz ovog uvjeta dobijemo linearnu diofantsku jednadžbu

$$12k + 7l = 1,$$

kojoj je jedno partikularno rješenje $k_0 = 3, l_0 = -5$. Tada su sva rješenja oblika:

$$\begin{aligned} k &= 3 + 7t, \\ l &= -5 - 12t, \end{aligned}$$

pri čemu je $t \in \mathbb{Z}$. Kako k mora biti prirodan broj, a x najmanji, uzimamo $t = 0$, tj. $k = 3$. Uvrštavanjem u prvu jednadžbu početnog sustava, dolazimo do rješenja $x = 27$.

2.4. Metoda zbroja

Ova je metoda vrlo slična metodi faktorizacije. Razlikuju se po tome što u ovoj metodi lijevu strane jednadžbe nastojimo zapisati u obliku zbroja cijelih brojeva i onda razlikovati slučajeve.

Primjer 2.9. *Nađite cjelobrojna rješenja jednadžbe* $x^2 + y^2 + 4x - 6y - 4 = 0$.

Rješenje: Dopunimo ovu jednadžbu do potpunih kvadrata. Dobivamo:

$$\begin{aligned} x^2 + 4x + y^2 - 6y - 4 &= 0, \\ (x+2)^2 - 4 + (y-3)^2 - 9 - 4 &= 0, \\ (x+2)^2 + (y-3)^2 &= 17. \end{aligned}$$

Znamo da su jedini mogući pribrojnici 1 i 4 jer 17 možemo jedino na taj način prikazati kao sumu potpunih kvadrata. To znači da može biti samo $(x+2)^2 = 1$ i $(y-3)^2 = 4$ ili $(x+2)^2 = 4$ i $(y-3)^2 = 1$. Rješavanjem prvog slučaja dobivamo $x \in \{-1, -3\}$, a $y \in \{5, -1\}$. Slično, za drugi slučaj dobivamo $x \in \{0, -4\}$, a $y \in \{4, 2\}$.

Primjer 2.10. *Riješite u skupu cijelih brojeva jednadžbu:* $n^2 - 6n + 7 + 2m^2 = 0$.

Rješenje: Možemo n dopuniti do potpunog kvadrata:

$$\begin{aligned} n^2 - 6n + 9 + 2m^2 &= 2, \\ (n-3)^2 + 2m^2 &= 2. \end{aligned}$$

Zbroj kvadrata dva cijela broja je 2 ako su ti brojevi $0, 1, 2$. Primijetimo da ne može biti $2m^2 = 1$ i taj slučaj možemo odmah eliminirati. Neka je zatim $(n-3)^2 = 0$ i $2m^2 = 2$. U tom slučaju rješenja su: $(n, m) \in \{(3, 1), (3, -1)\}$. Na kraju vidimo da ni treći slučaj nije mogući ($(n-3)^2 = 2$), što znači da su navedena rješenja ujedno i jedina.

2.5. Metoda ostataka

Primjetimo da su metoda faktorizacije, zbroja i kvocjenta u osnovi koristile istu ideju, a to je da lijevu stranu jednadžbe transformiramo u nama odgovarajući oblik (produkt, zbroj ili kvocjent) i na taj način dolazimo do rješenja. Metoda ostataka koristi malo drugačiju ideju: podijeliti dio jednadžbe nekim cijelim brojem i promatrati ostatke pri dijeljenju te zatim te ostatke međusobno usporediti.

2.6. Metoda posljednje znamenke

Ovo je podmetoda metode ostataka. Promatramo što se događa s jednadžbom kada njen dio podijelimo s 10, odnosno promatramo ostatak pri dijeljenju s 10. Drugim riječima, promatramo zadnje znamenke dijelova jednažbe i želimo ih uskladiti.

Primjer 2.11. *Nađite cjelobrojna rješenja jednadžbe* $2x^2 + 5y = 19971849$.

Rješenje: Kvadrat cijelog broja završava znamenkama: $0, 1, 4, 5, 6$ ili 9, a kako je $2x^2$ dodatno i paran broj, on može završiti znamenkama $0, 2, 8$. S druge strane, $5y$ završava znamenkama 0 ili 5. Dakle, zbroj na lijevoj strani može završavati samo znamenkama $0, 2, 3, 5, 7, 8$ a nikako znamenkom 9 što znači da ova jednadžba nema rješenja.

2.7. Metoda parnosti

Ova metoda je podmetoda metode ostataka koja se bazira na promatranje ostataka nakon dijeljenja brojem 2. Očito je da nepoznanice mogu biti ili samo parne ili samo neparne pa prema tome i razlikujemo slučajeve.

Primjer 2.12. *Postoje li cjelobrojna rješenja jednadžbe* $x^2 + 8y = 1997$*?*

Rješenje: Pretpostavimo da je x paran. To bi značilo da je cijela lijeva strana jednadžbe parna što nije moguće, odnosno rješenje ne postoji. Uzmimo onda x neparan, to jest $x = 2k + 1$ i uvrstimo to u zadanu jednadžbu.

$$\begin{aligned}(2k+1)^2 + 8y &= 1997,\\ 4k^2 + 4k + 1 + 8y &= 1997,\\ 4(k^2 + k + 2y) &= 1996,\\ k(k+1) + 2y &= 499.\end{aligned}$$

Znamo da je produkt dva uzastopna broja uvijek paran, a znamo da je i $2y$ paran pa iz toga slijedi da je lijeva strana jednadžbe parna i da nikako ne može biti jednaka 499. Slijedi da jednadžba nema cjelobrojna rješenja.

Primjer 2.13. *Ima li jednadžba* $x! + 8y = 1025$ *rješenja u prirodnim brojevima?*

Rješenje: Znamo da je $8y$ paran što znači da $x!$ mora biti neparan da bi jednadžba bila rješiva. S druge strane, svi faktorijeli su parni osim 1! pa je onda nužno $x = 1$. Uvrstimo li to u jednadžbu, dobivamo $y = 128$, što znači da jednadžba ima rješenja u prirodnim brojevima.

2.8. Metoda karakterističnih ostataka

Ovo je podmetoda metode ostataka u kojoj gledamo što se događa s jednadžbom ako ju dijelimo s nekim cijelim brojem osim 2 ili 10 (njih smo pokrili u prethodnim metodama).

Primjer 2.14. *Riješite jednadžbu* $x^2 - 10y = 33$.

Rješenje: Podijelimo li cijelu jednadžbu s 5, dobivamo:

$$x^2 \equiv 3 \pmod 5.$$

Pogledajmo koje ostatke može dati potpun kvadrat pri dijeljenju s 5:

$x \pmod 5$	0	1	2	3	4
$x^2 \pmod 5$	0	1	4	4	1

Zaključujemo da ostatak nikako ne može biti 3 te jednadžba nema rješenja.

2.9. Metoda matematičke indukcije

Metoda matematičke indukcije koristi se u raznim granama matematike i vrlo je koristan alat za dokazivanje tvrdnji koje se odnose na prirodne brojeve, odnosno na nenegativne cijele brojeve.
Matematička indukcija (slaba forma): Neka vrijedi sljedeće:

- $P(n_0)$ istinit,
- za svaki $k \geq n_0$ vrijedi: iz $P(k)$ istinit, slijedi da je i $P(k+1)$ također istinit.

Tada je $P(n)$ istinit za svaki $n \geq n_0$.

Matematička indukcija (jaka forma): Neka vrijedi sljedeće:

- $P(n_0)$ istinit,
- za svaki $k \geq n_0$: iz $P(m)$ je istinit za sve m takve da je $n_0 \leq m \leq k$, slijedi da je i $P(k+1)$ istinit.

Tada je $P(n)$ istinit za svaki $n \geq n_0$.
Pokažimo na primjeru kako možemo iskoristiti matematičku indukciju u rješavanju diofantskih jednadžbi.

Primjer 2.15. *([1]) Pokažite da za prirodan broj n jednadžba $x^2+xy+y^2 = 7^n$ ima rješenja pri čemu su x, y cijeli brojevi.*

Rješenje: Koristimo matematičku indukciju pa prvo provjeravamo tvrdnju za bazu indukcije, odnosno za $n = 1$.

$$x_1^2 + x_1y_1 + y_1^2 = 7.$$

Možemo lako vidjeti da je jedno rješenje ove jednadžbe $x_1 = 1, y_1 = 2$, što znači da je tvrdnja zadovoljena. Pretpostavimo onda da je tvrdnja istinita za n, dakle da postoje x_n, y_n cijeli brojevi takvi da je:

$$x_n^2 + x_ny_n + y_n^2 = 7^n,$$

i pokažimo da tvrdnja vrijedi i za $n+1$.
Definirajmo $x_{n+1} = 2x_n - y_n$ i $y_{n+1} = x_n + 3y_n$. Tada vrijedi:

$$\begin{aligned}
x_{n+1}^2 + x_{n+1}y_{n+1} + y_{n+1}^2 &= 7^{n+1},\\
(2x_n - y_n)^2 + (2x_n - y_n)(x_n + 3y_n) + (x_n + 3y_n)^2 &= 7^{n+1},\\
4x_n^2 - 4x_ny_n + y_n^2 + 2x_n^2 + 6x_ny_n - x_ny_n - 3y_n^2 + x_n^2 + 6x_ny_n + 9y_n^2 &= 7^{n+1},\\
7x_n^2 + 7x_ny_n + 7y_n^2 &= 7^{n+1},\\
7(x_n^2 + x_ny_n + y_n^2) &= 7^{n+1},\\
7 \cdot 7^n &= 7^{n+1}.
\end{aligned}$$

Time je tvrdnja dokazana.

2.10. Fermatova metoda beskonačnog spusta

Ovo je ujedno i posljednja metoda koju ćemo opisati u ovom radu. "Beskonačni spust" je metoda dokaza koju je među prvima koristio poznati matematičar Fermat po kome je i dobila ime.
Neka je P svojstvo koje se odnosi na nenegativne cijele brojeve i neka je $P(n)$, pri čemu je $n \geq 1$, niz istinitih izjava: $P(n) =$"n zadovoljava svojstvo P".
Ova metoda nam pomaže dokazati da je niz izjava $P(n)$ neistinit za n dovoljno velik.
Fermatova metoda beskonačnog spusta: Neka je $k > 0$ i kad god je $P(m)$ istinit za neki $m > k$, onda mora postojati neki $j \in \mathbb{Z}$, $k < j < m$ takav da je $P(j)$ istinito. Tada $P(n)$ nije istinit za sve $n > k$.
Precizinije, to znači da ako postoji neki n za koji je $P(n)$ istinit, mogli bismo konstruirati strogo padajući niz $n > n_1 > n_2 > \ldots$ u kojem bi svi $n, n_1, n_2, \ldots$ bili veći od k, ali kako smo u skupu nenegativnih cijelih brojeva, ne postoji takav beskonačan padajući niz, odnosno "beskonačni spust".

Primjer 2.16. *([4]) Pokažite da jednadžba $x^2 + y^2 = 3z^2$ nema cjelobrojnih rješenja pri čemu je $z \neq 0$.*

Rješenje: Bez smanjenja općenitositi neka je $z > 0$. Pretpostavimo da ova jednadžba ima rješenja i označimo ga s (x, y, z) i neka je z najmanji takav. Pogledajmo ostatke jednadžbe pri dijeljenju s 3:

$$x^2 + y^2 \equiv 0 \pmod 3.$$

Znamo da potpuni kvadrati mogu biti kongruentni 0 ili 1 modulo 3 pa to onda nužno znači da su x^2 i y^2 oba kongruentni 0 modulo 3, to jest:

$$x^2 \equiv y^2 \equiv 0 \pmod 3,$$

što povlači

$$x \equiv y \equiv 0 \pmod 3.$$

Uzmimo zatim $x = 3a$ i $y = 3b$ i uvrstimo u jednadžbu. Dobivamo:

$$\begin{aligned} 9a^2 + 9b^2 &= 3z^2, \\ 3a^2 + 3b^2 &= z^2, \\ 3(a^2 + b^2) &= z^2. \end{aligned}$$

Iz ovoga zaključujemo da $3|z^2$, odnosno $3|z$. Stoga zaključujemo da $z = 3c$. Uvrštavanjem ovih jednakosti u jednadžbu, slijedi:

$$\begin{aligned} 3(a^2 + b^2) &= 9c^2, \quad \text{tj.} \\ a^2 + b^2 &= 3c^2. \end{aligned}$$

Iz ovoga možemo zaključiti da je (a, b, c) još jedno rješenje polazne jednadžbe. Međutim iz $z = 3c$ vidimo $0 < c < z$ i dolazimo do kontradikcije s pretpostavkom da je z najmanje rješenje jednadžbe.

3. Pitagorina jednadžba

Općepoznat Pitagorin poučak glasi: zbroj kvadrata duljina kateta pravokutnog troukta jednak je kvadratu duljine hipotenuze. Prevedemo li poučak u matematičke simbole i dobijamo:

$$x^2 + y^2 = z^2. \tag{5}$$

Ukoliko tražimo cjelobrojna rješenja ove jednadžbe, onda je ovo zapravo diofantska jednadžba drugog stupnja i tu jednadžbu nazivamo **Pitagorina jednadžba**.
Primijetimo da ako je (x, y, z) jedno rješenje jednadžbe (5), rješenje će također biti i (kx, ky, kz), pri čemu je $k \in \mathbb{Z}$ proizvoljan. To nam olakšava rješavanje jer ćemo se bazirati na u parovima relativno prostim brojevima. Uređenu trojku prirodnih brojeva (x, y, z) koja zadovoljava jednadžbu (5) nazivamo **Pitagorina trojka**, a ako su x, y, z relativno prosti kažemo da je (x, y, z) **primitivna Pitagorina trojka**.

Teorem 3.1. *Sve primitivne Pitagorine trojke (x, y, z) u kojima je y paran dane su formulama:*

$$\begin{aligned} x &= m^2 - n^2, \\ y &= 2mn, \\ z &= m^2 + n^2, \end{aligned}$$

pri čemu su m, n prirodni brojevi, $m > n$, $(m, n) = 1$ i m, n su različite parnosti.

Dokaz. Za početak možemo lako provjeriti da izrazi za x, y, z zadovoljavaju jednadžbu (5) tako što ih uvrstimo u jednadžbu. Iz toga možemo vidjeti da je y zaista paran. S druge strane možemo zaključiti da x ne može biti paran, odnosno da je neparan, jer ako bi x i y bili iste parnosti, z^2 bi bio kongruentan 2 modulo 4 što je u kontradikciji s tvrdnjom da je potpun kvadrat oblika $4k$ ili $4k + 1$. Stoga x je neparan. Bez smanjenja općenitosti možemo pretpostaviti m neparan, a n paran.
Provjerimo je li to zaista primitivna trojka. Neka je $(m^2 - n^2, 2mn, m^2 + n^2) = d$, pri čemu je $d \geq 2$. Kako je d djelitelj svakog, znači da d dijeli i njihov zbroj i razliku:

$$\begin{aligned} m^2 + n^2 + m^2 - n^2 &= 2m^2, \\ m^2 + n^2 - m^2 + n^2 &= 2n^2. \end{aligned}$$

Kako u pretpostavci teorema imamo $(m, n) = 1$, to bi značilo $d = 2$ i $m^2 + n^2$ parno što je u kontradickiji s pretpostavkom da su m, n različite parnosti. Zaključujemo $d = 1$, dakle trojka je zaista primitivna.
Neka je sada (x, y, z) primitivna trojka koja je rješenje jednadžbe (5) i neka je y paran, tj. $y = 2a$, $a \in \mathbb{Z}$. Tada su x, z neparni i vrijedi:

$$z + x = 2b, \tag{6}$$
$$z - x = 2c, \tag{7}$$

gdje su $b, c \in \mathbb{Z}$. Možemo pretpostaviti da je $(b, c) = 1$ jer bi inače $(x, z) \neq 1$. Sada imamo:

$$4a^2 = y^2 = z^2 - x^2 = (z - x)(z + x) = 4cb,$$

iz čega slijedi $a^2 = bc$. Iz ove jednakosti lako možemo zaključiti da $b = m^2$ i $c = n^2$ gdje su m, n nenegativni cijeli brojevi. Uvrstimo li to u izraz za y dobijemo $y = 2mn$. Zbrojimo li jednadžbe (6) i (7) dobijemo $z = b + c$, odnosno

$$z = m^2 + n^2.$$

Oduzmimo jednadžbu (7) od jednadžbe (6). Tada je $x = b - c$, odnosno

$$x = m^2 - n^2.$$

Time je teorem dokazan. □

Primjer 3.1. *Dokažite da ne postoji primitivna Pitagorina trojka u kojoj je jedan član jednak 6.*

Rješenje: Kako je 6 paran broj, može biti samo $y = 6$, odnosno $mn = 3$. Kako je 3 prost i prema pretpostavci Teorema 3.1. $m > n$, može biti samo $m = 3$ i $n = 1$. Uvrstimo li dobivene m, n u formule prethodnog teorema, dobivamo $x = 8$ i $z = 10$ što je u kontradikciji s x, y, z relativno prosti.

Primjer 3.2. *Nađite sve Pitagorine trokute kojima je jedna stranica jednaka 15.*

Rješenje: Primijetimo da u zadatku nisu u pitanju samo primitvne trojke tako da ćemo za x, y, z uzimati u obzir sljedeće formule:

$$\begin{aligned} x &= d(m^2 - n^2), \\ y &= 2dmn, \qquad d \in \mathbb{N}. \\ z &= d(m^2 + n^2), \end{aligned}$$

Kako je 15 neparan broj, može biti samo $x = 15$ ili $z = 15$. Uzmimo prvo slučaj $x = 15$. Tada je:

$$\begin{aligned} d(m^2 - n^2) &= 15, \\ d(m - n)(m + n) &= 3 \cdot 5. \end{aligned}$$

Neka je prvo $d = 1$. U tom slučaju imamo $m + n = 5$ i $m - n = 3$, to jest $m = 4$ i $n = 1$ i rezultat je primitivna trojka $(15, 8, 17)$. Zatim imamo $d = 3$, pa analognim računom dobijemo $m = 3$ i $n = 2$ te pripradnu trojku $(15, 36, 39)$. Za $d = 5$ imamo $m = 2$, $n = 1$ i Pitagorinu trojku $(15, 20, 25)$.
Neka je sada $z = 15$. Za $d = 1$ imamo $m^2 + n^2 = 15$ što nije moguće jer suma 2 kvadrata nije kongruentna 3 modulo 4 što znači da ovakva trojka ne postoji. Za $d = 3$ dobijemo trojku $(9, 12, 15)$, a za $d = 5$ trojka također ne postoji.

Literatura

[1] T. Andrescu, D. Andrica, I. Cucurezeanu, *An Intoduction to Diophantine Equations*, GIL Publishing House, Zalau, 2002.

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

[3] D. Crnjac Milić, *Pitagorini brojevi i Pitagorina jednadžba*, Osječki matematički list 9 (2009), 69-73.

[4] N. Donaldson, *Fermat's Method of Descent*, `https://www.math.uci.edu/~ndonalds/math180b/5descent.pdf`

[5] A. Dujella, *Uvod u teoriju brojeva*, Matematički odsjek, Prirodoslovno-matematički fakultet, Sveučilište u Zagrebu, 2002, skripta.

[6] M. Golac, *Nelinearne diofantske jednadžbe*, Matka 8, 1994.

[7] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku Sveučilišta J. J. Strossmayera, 2013, skripta.

[8] B. Pavković, B. Dakić, P. Mladinić, *Elementarna teorija brojeva*, Element, Zagreb, 1994.