

# Diofantske jednadžbe

---

Ivšić, Violeta

Undergraduate thesis / Završni rad

2016

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://um.nsk.hr/um:nbn:hr:126:462808>

Rights / Prava: [In copyright](#) / [Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2024-11-07**



**mathos**

Repository / Repozitorij:

[Repository of School of Applied Mathematics and Informatics](#)



**Sveučilište J. J. Strossmayera u Osijeku**  
**Odjel za matematiku**

**Violeta Ivšić**

**DIOFANTSKE JEDNADŽBE**

Završni rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku  
Odjel za matematiku

Violeta Ivšić

**DIOFANTSKE JEDNADŽBE**

Završni rad

*mentor:* izv. prof. dr. sc. Ivan Matić

Osijek, 2016.

**Sažetak.** Kroz ovaj rad upoznat ćemo neke klasične diofantske jednačbe. Primjenom osnovnih definicija i teorema, kroz primjere objašnjeno je njihovo djelovanje.

**Ključne riječi:** diofantske jednačbe, Pitagorine trojke, Fermatova metoda.

**Summary.** This work will explain some of the classical Diophantine equations. With definitions and theorems, finding the solution will be demonstrated with examples.

**Keywords:** Diophantine equations, Fermat's Method, Pythagorean Triple.

# Sadržaj

<b>1. Uvod</b>	<b>1</b>
<b>2. Klasične diofantske jednađbe</b>	<b>2</b>
2.1. Linearne diofantske jednađbe . . . . .	2
2.2. Pitagorine trojke . . . . .	4
<b>3. Metode za rješavanje diofantskih jednađbi</b>	<b>5</b>
3.1. Metode faktorizacije . . . . .	5
3.2. Metode nejednakosti . . . . .	8
3.3. Metoda matematičke indukcije . . . . .	10
3.4. Fermatova metoda . . . . .	12
<b>4. Zaključak</b>	<b>14</b>

## 1. Uvod

Diofant najpoznatiji je po svojoj knjizi Aritmetika, radu na rješavanju algebarskih jednadžbi i teoriji brojeva. Ipak, njegov nam je život u suštini ostao nepoznat, te je doba u kojem je živio predmet debata.

Diofant je naučavao u gradu Aleksandriji u razdoblju od 250. pr. Kr. do 350. pr. Kr., poznato kao "Srebrno doba". U tom razdoblju matematičari su otkrivali brojne ideje koje su oblikovale današnju matematiku.

Najviše informacija o Diofantovom životu nalazimo u kolekciji zagonetki koju je napisao Metrodor, grčki gramatičar i matematičar oko 500. godine.

Njegovo najpoznatije djelo Aritmetika je kolekcija 150 matematičkih problema u kojoj on na vješt način prikazuje rješavanje jednadžbi prvog i drugog stupnja, uz rješavanje temeljnih problema iz teorije brojeva. Danas znamo za 160 problema koje je Diofant napisao, no vjerujemo da je Aritmetika sadržavala više poglavlja od poznatih 6. Nagadamo da je u izvornom obliku sadržavala 13 poglavlja, od kojih se 7 smatra izgubljenim. Postoji mogućnost da su nestala u velikom požaru koji se dogodio nedugo nakon što je Diofant završio sa svojim radom.

## 2. Klasične diofantske jednačbe

### 2.1. Linearne diofantske jednačbe

Jednačbu oblika

$$ax + by = c \quad (1)$$

gdje su  $a$ ,  $b$  i  $c$  cijeli brojevi zovemo linearna diofantska jednačba. Linearna diofantska jednačba (1) ima rješenje ako  $d$  dijeli  $c$ , gdje je  $d = (a, b)$ . Ako  $d$  dijeli  $c$ , onda rješenje možemo naći u obliku

$$d = ua + vb, \\ x_0 = \frac{uc}{d} \text{ i } y_0 = \frac{vc}{d}$$

te su sva rješenja dana sa

$$x = x_0 + \frac{b}{d}t \text{ i } y = y_0 + \frac{a}{d}t,$$

za  $t \in \mathbb{Z}$ .

Linearnom diofantskom jednačbom sa  $n$  nepoznanica nazivamo jednačbu oblika:

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b \quad (2)$$

gdje su  $x_1, \dots, x_n$  nepoznanice, a  $a_1, \dots, a_n, b$  cjelobrojni koeficijenti.

**Teorem 2.1** *Neka su  $a_1, \dots, a_n$  cijeli brojevi različiti od nule. Tada linearna diofantska jednačba:*

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

*ima rješenja ako i samo ako  $(a_1, \dots, a_n)$  dijeli  $b$ . Ako jednačba ima barem jedno rješenje, onda ih ima beskonačno mnogo.*

*Dokaz: Neka je  $d = (a_1, \dots, a_n)$ . Ako  $d$  dijeli  $b$  onda jednačba (2) nema rješenja. Ako  $d$  dijeli  $b$ , dobivamo ekvivalentnu jednačbu:*

$$a'_1x_1 + \dots + a'_nx_n = b'$$

*gdje je  $a'_i = a_i/d$  za  $i = 1, \dots, n$  i  $b' = b/d$ . Imamo  $(a'_1, \dots, a'_n) = d$ . Dokazat ćemo matematičkom indukcijom. Za  $n \geq 2$  tvrdnja vrijedi, pa pretpostavimo da vrijedi za jednačbe sa  $n - 1$  varijabli. Želimo pokazati da vrijedi za jednačbe sa  $n$  varijabli. Stavimo  $d_{n-1} = (a_1, \dots, a_{n-1})$  onda sva rješenja  $(x_1, \dots, x_n)$  jednačbe (2) zadovoljavaju kongruenciju:*

$$a_1x_1 + a_2x_2 + \dots + a_nx_n \equiv b \pmod{d_{n-1}}$$

*to je jednako*

$$a_nx_n \equiv b \pmod{d_{n-1}}. \quad (3)$$

Pomnožimo obje strane jednadžbe (3) sa  $a^{\varphi(d_{n-1})-1}$ , gdje je  $\varphi$  Eulerova funkcija za koju je  $a^{\varphi(d_{n-1})} \equiv 1 \pmod{d_{n-1}}$ , dobivamo

$$x_n \equiv c \pmod{d_{n-1}},$$

gdje je  $c = a^{\varphi(d_{n-1})-1}b$ , slijedi da je  $x_n = c + d_{n-1}t_{n-1}$ ,  $t_{n-1} \in \mathbb{Z}$ . Jednadžbu (2) smo zapisali kao jednadžbu od  $n - 1$  varijabli

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b - a_nc - a_{n-1}d_{n-1}t_{n-1}.$$

Još ostaje pokazati da  $d_{n-1}$  dijeli  $(b - a_nc - a_{n-1}d_{n-1}t_{n-1})$ , što je jednako  $a_nc \equiv b \pmod{d_{n-1}}$ . Zadnja jednadžba je točna zbog izbora  $c$ , ako je podjelimo sa  $d_{n-1}$  dobijemo

$$a'_1x_1 + \dots + a'_{n-1}x_{n-1} = b' \quad (4)$$

gdje je  $a'_i = \frac{a_i}{d_{n-1}}$  za  $i = 1, \dots, n-1$  i  $b' = \frac{(b - a_nc)}{d_{n-1} - a_{n-1}t_{n-1}}$ . Kako je  $(a'_1, \dots, a'_{n-1}) = d$  jednadžba (4) ima rješenje za svaki  $t_{n-1} \in \mathbb{Z}$ . To rješenje vrijedi za jednadžbe sa  $n - 2$  varijable. Ako dodamo  $x_n = c + d_{n-1}t_{n-1}$  dobijemo rješenje jednadžbe (2).

**Korolar 2.1** Neka su  $a_1, a_2$  cijeli brojevi. Ako je  $(x_1^{(0)}, x_2^{(0)})$  jedno rješenje jednadžbe

$$a_1x_1 + \dots + a_2x_2 = b$$

ostala rješenja su dana s

$$\begin{aligned} x_1 &= x_1^{(0)} + a_2t \\ x_2 &= x_2^{(0)} - a_1t \end{aligned} \quad (5)$$

za  $t \in \mathbb{Z}$ .

**Primjer 2.1** Riješite jednadžbu:

$$3x + 4y + 5z = 6.$$

Radi (5) imamo  $3x + 4y \equiv 1 \pmod{5}$ , stoga je

$$3x + 4y = 1 + 5s, \quad s \in \mathbb{Z}.$$

Rješenja ove jednadžbe su  $x = -1 + 3s$ ,  $y = 1 - s$ . Koristeći (5) dobivamo  $x = 1 - 3s + 4t$ ,  $y = 1 - s - 3t$ ,  $t \in \mathbb{Z}$ . Kada to vratimo u polaznu jednadžbu dobivamo  $z = 1 - s$ . Konačno rješenje jednadžbe je dano s

$$(x, y, z) = (-1 + 3s + 4t, 1 - s - 3t, 1 - s), \quad s, t \in \mathbb{Z}.$$



## 2.2. Pitagorine trojke

**Definicija 2.1** Uređenu trojku prirodnih brojeva  $(x, y, z)$  zovemo Pitagorina trojka ako su  $x, y$  katete, a  $z$  hipotenuza nekog pravilnog trokuta, tj. 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.

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

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \quad (6)$$

gdje je  $m > n$  i  $m, n$  su relativno prosti prirodni brojevi različite parnosti.

**Primjer 2.2** Riješite jednadžbu:

$$x^{-2} + y^{-2} = z^{-2}.$$

Jednadžba je ekvivalentna sa

$$x^2 + y^2 = \left(\frac{xy}{z}\right)^2$$

To znači da  $z$  dijeli  $xy$  i  $x^2 + y^2$  je potpun kvadrat. Tada je  $x^2 + y^2 = t^2$  za neki pozitivan cijeli broj i jednadžba prelazi u

$$t = \frac{xy}{z}.$$

Neka je  $d = (x, y, t)$ . Onda je  $x = ad$ ,  $y = bd$ ,  $t = cd$ , gdje su  $a, b, c \in \mathbb{Z}_+$ ,  $(a, b, c) = 1$ . Tada se jednadžba  $t = \frac{xy}{z}$  reducira na

$$z = \frac{abd}{c}.$$

Iz izbora od  $t$ , slijedi da je

$$a^2 + b^2 = c^2,$$

gdje su  $a, b, c$  relativno prosti parni brojevi. Koristeći polaznu jednadžbu zaključujemo da  $c$  dijeli  $d$ ,  $d = kc$ ,  $k \in \mathbb{Z}_+$ . Dobijamo

$$x = ad = kac, \quad y = bd = kbc, \quad t = ad = kc^2, \quad z = kab.$$

Koristeći jednadžbu  $a^2 + b^2 = c^2$  i formulu (6) imamo  $a = m^2 - n^2$ ,  $b = 2mn$ ,  $c = m^2 + n^2$ .

Rješenja jednadžbe su dana sa

$$x = k(m^4 - n^4), \quad y = 2kmn(m^2 + n^2), \quad z = 2kmn(m^2 - n^2)$$

gdje su  $k, m, n \in \mathbb{Z}_+$  i  $m > n$ .

### 3. Metode za rješavanje diofantskih jednačbi

#### 3.1. Metode faktorizacije

Ova metoda se sastoji u zapisivanju jednačbe  $f(x_1, x_2, \dots, x_n) = 0$  u obliku:

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

gdje su  $f_1, f_2, \dots, f_k \in \mathbb{Z}[x_1, x_2, \dots, x_n]$  i  $a \in \mathbb{Z}$ . S obzirom na glavnu jednačbu dobijemo sustav konačno mnogo jednačbi .

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

Rješavanjem ovog sustava jednačbi dobijemo rješenje za  $f(x_1, x_2, \dots, x_n) = 0$ .

**Primjer 3.1** *Nadite sva rješenja jednačbe:*

$$(x^2 + 1)(y^2 + 1) + 2(x - y)(1 - xy) = 4(1 + xy).$$

*Zapišemo jednačbu u obliku:*

$$x^2y^2 - 2xy + 1 + x^2 + y^2 - 2xy + 2(x - y)(1 - xy) = 4$$

*ili*

$$(xy - 1)^2 + (x - y)^2 - (x - y)(xy - 1) = 4.$$

*To je jednako:*

$$[xy - 1 - (x - y)]^2 = 4$$

*ili*

$$(x + 1)(y - 1) = \pm 2.$$

*Ako je  $(x + 1)(y - 1) = 2$ , dobivamo sustav jednačbi:*

$$\begin{array}{cccc} x + 1 = 2 & x + 1 = -2 & x + 1 = 1 & x + 1 = -1 \\ y - 1 = 1 & y - 1 = -1 & y - 1 = 2 & y - 1 = -2 \end{array}$$

*dobivamo rješenja  $(1, 2)$ ,  $(-3, 0)$ ,  $(0, 3)$ ,  $(-2, -1)$ .*

*Ako je  $(x + 1)(y - 1) = -2$ , dobivamo sustav jednačbi:*

$$\begin{array}{cccc} x + 1 = 2 & x + 1 = -2 & x + 1 = 1 & x + 1 = -1 \\ y - 1 = -1 & y - 1 = 1 & y - 1 = -2 & y - 1 = 2 \end{array}$$

*dobivamo rješenja  $(1, 0)$ ,  $(-3, 2)$ ,  $(0, -1)$ ,  $(-2, 3)$ .*

**Primjer 3.2** Nađite sva cjelobrojna rješenja jednadžbe:

$$3xy + 2y = 7.$$

Jednadžbu zapišemo u obliku

$$y(3x + 2) = 7,$$

pa imamo sljedeće mogućnosti

$$\begin{array}{cccc} y = 1 & y = -1 & y = 7 & y = -7 \\ 3x + 2 = 7 & 3x + 2 = -7 & 3x + 2 = 1 & 3x + 2 = -1 \\ \\ x = 5/3 & x = -3 & x = -1/3 & x = -1 \\ y = 1 & y = -1 & y = 7 & y = -7 \end{array}$$

Imamo dva rješenja:  $(-1, -7)$ ,  $(-3, -1)$ .

**Primjer 3.3** Pokažimo da jednadžba

$$(x - y)^3 + (y - z)^3 + (z - x)^3 = 35$$

nema cjelobrojnih rješenja.

Lijevu stranu jednadžbe rastavimo u produkt

$$\begin{aligned} & (x - y)^3 + (y - z)^3 + (z - x)^3 \\ &= (x - y + y - z)[(x - y)^2 - (x - y)(y - z) + (y - z)^2] - (x - z)^3 \\ &= (x - z)[(x - y)^2 - (x - y)(y - z) + (y - z)^2 - (z - x)^2] \\ &= (x - z)[(x - y)(x - 2y + z) + (y - 2z + x)(y - x)] \\ &= (x - z)(x - y)(3z - 3y) = 3(x - z)(x - y)(z - y). \end{aligned}$$

Slijedi da je lijeva strana jednadžbe djeljiva s 3. Kako 35 nije djeljiv s 3, ta jednadžba nema cjelobrojnih rješenja.

**Primjer 3.4** Nađite sva rješenja jednadžbe:

$$x^2(y - 1) + y^2(x - 1) = 1.$$

Uvodimo supstituciju  $x = u + 1$ ,  $y = v + 1$  i uvrstimo u jednadžbu

$$(u + 1)^2v + (v + 1)^2u = 1.$$

Što je jednako

$$uv(u + v) + 4uv + (u + v) = 1.$$

Jednadžbu možemo zapisati u obliku

$$uv(u + v + 4) + (u + v + 4) = 5$$

ili

$$(u + v + 4)(uv + 1) = 5.$$

Jedan od faktora mora biti 5 ili  $-5$ , a drugi 1 ili  $-1$ . To znači da suma  $u + v$  ili umnožak  $uv$  mora zadovoljavati jedan od četiri sustava jednadžbi.

$$\begin{array}{cccc} u + v = 1 & u + v = -9 & u + v = -3 & u + v = -5 \\ uv = 0 & uv = -2 & uv = 4 & uv = -6 \end{array}$$

Prvi i zadnji sustav jednadžbi imaju rješenja u skupu cijelih brojeva. To su  $(0, 1)$ ,  $(1, 0)$ ,  $(-6, 1)$ ,  $(1, -6)$ . Kada ova rješenja vratimo u supstituciju dobivamo  $(1, 2)$ ,  $(-5, 2)$ ,  $(2, 1)$ ,  $(2, -5)$ .

### 3.2. Metode nejednakosti

Ova metoda se koristi kako bi smanjili skup mogućih rješenja dane jednadžbe, a zatim se na tom smanjenom skupu razlikuju slučajevi.

**Primjer 3.5** *Nadi sva rješenja jednadžbe:*

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

*Primjetimo da je svaki zapis u obliku  $(k, -k)$ ,  $k \in \mathbb{Z}$  rješenje.*

*Ako je  $x + y \neq 0$ , jednadžba poprima oblik*

$$x^2 - xy + y^2 = x + y,$$

*što je jednako*

$$(x + y)^2 + (x - 1)^2 + (y - 1)^2 = 2.$$

*Ako je  $(x - 1)^2 \leq 1$  i  $(y - 1)^2 \leq 1$  suženje, znači da su varijable  $x$ ,  $y$  sužene na interval  $[0, 2]$ . Dobivamo rješenja  $(0, 1)$ ,  $(1, 0)$ ,  $(1, 2)$ ,  $(2, 1)$ ,  $(2, 2)$ .*

**Primjer 3.6** *Riješi jednadžbu:*

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}.$$

*Možemo pretpostaviti da je  $2 \leq x \leq y \leq z$ . To nam daje jednadžbu  $\frac{3}{x} \geq \frac{3}{5}$ ,  $x \in \{2, 3, 4, 5\}$ . Ako je  $x = 2$ , onda je  $\frac{1}{y} + \frac{1}{z} = \frac{1}{10}$ ,  $y \in \{11, 12, \dots, 20\}$ . Slijedi da je  $z = 10 + \frac{100}{y - 10}$  i  $(y - 10)$  dijeli 100, što nam daje rješenja  $(2, 11, 110)$ ,  $(2, 12, 60)$ ,  $(2, 14, 35)$ ,  $(2, 15, 30)$ ,  $(2, 20, 20)$ .*

*Ako je  $x = 3$ , onda je  $\frac{1}{y} + \frac{1}{z} = \frac{1}{15}$ ,  $y \in \{3, 4, 5, 6, 7\}$ , što nam daje rješenja  $(3, 4, 60)$ ,  $(3, 5, 15)$ ,  $(3, 6, 10)$ .*

*Ako je  $x = 4$ , onda je  $\frac{1}{y} + \frac{1}{z} = \frac{7}{20}$ ,  $y \in \{4, 5\}$ , što nam daje rješenje  $(4, 4, 10)$ .*

*Ako je  $x = 5$ , onda je  $\frac{1}{y} + \frac{1}{z} = \frac{2}{5}$  i  $y = z = 5$ , što nam daje rješenje  $(5, 5, 5)$ .*

**Primjer 3.7** *U skupu prirodnih brojeva riješite jednadžbu:*

$$a! + b! = c!$$

Očito mora biti  $a < b$  i  $b < c$ . Bez smanjenja općenitosti neka je i  $a \leq b$ . Jednostavnom transformacijom iz jednadžbe dobivamo

$$a! \left( 1 + \frac{b!}{a!} - \frac{c!}{a!} \right) = 0,$$

a kako je  $a! > 0$  to je nužno

$$1 + \frac{b!}{a!} - \frac{c!}{a!} = 0,$$

odnosno

$$1 = \frac{c!}{a!} - \frac{b!}{a!} = \frac{b!}{a!} \left( \frac{c!}{b!} - 1 \right).$$

Za  $a < b$  bilo bi  $\frac{b!}{a!} > 1$  pa stoga jednakost ne bi mogla vrijediti, odakle sljedi stoga nužno  $a = b$  odakle slijedi

$$\frac{c!}{b!} = 2.$$

Zbog  $c > b \geq 1$  gornja jednadžba ima rješenje za  $c > 2$ , te joj je  $c = 2$ ,  $b = 1$  jedno rješenje. Nadalje, tada je i  $a = 1$  te smo dobili jedinstveno rješenje polazne jednadžbe.

**Primjer 3.8** U skupu prirodnih brojeva riješite jednadžbu

$$a + b + c = abc.$$

Neka je  $a \leq b \leq c$ . Tada je

$$abc = a + b + c \leq 3c,$$

odnosno  $ab \leq 3$ , pa razlikujemo tri slučaja:

I.  $a = 1, b = 1;$

II.  $a = 1, b = 2;$

III.  $a = 1, b = 3.$

Uvrstimo te vrijednosti u polaznu jednadžbu, II. daje  $c = 3$ . Dakle, rješenje je  $(1, 2, 3)$ .

### 3.3. Metoda matematičke indukcije

Metoda matematičke indukcije (slaba forma):

Pretpostavimo:

- Tvrdnja  $P(n_0)$  je istinita;
- Za svaki  $k \geq n_0$ , tvrdnja  $P(k)$  je istinita, što povlači istinitost tvrdnje  $P(k+1)$ .

Onda je tvrdnja  $P(n)$  istinita za svaki  $n \geq n_0$ .

Metoda matematičke indukcije (s korakom  $s$ ). Neka je  $s$  pozitivan cijeli broj.

Pretpostavimo:

- Tvrdnja  $P(n_0), P(n_0+1), \dots, P(n_0+s-1)$  su istinite;
- Za svaki  $k \geq n_0$ , tvrdnja  $P(k)$  je istinita, što povlači istinitost tvrdnje  $P(k+s)$ .

Onda je tvrdnja  $P(n)$  istinita za svaki  $n \geq n_0$ .

Metoda matematičke indukcije (jaka forma):

Pretpostavimo:

- Tvrdnja  $P(n_0)$  je istinita;
- Za svaki  $k \geq n_0$ , tvrdnja  $P(m)$  je istinita za svaki  $m$ , takav da je  $n_0 \leq m \leq k$ , što povlači istinitost tvrdnje  $P(k+1)$ .

Onda je tvrdnja  $P(n)$  istinita za svaki  $n \geq n_0$ .

**Primjer 3.9** *Dokažite da za svaki  $n \geq 3$ , postoje neparni prirodni brojevi  $x_n, y_n$  za koje je*

$$7x_n^2 + y_n^2 = 2^n.$$

*Dokazat ćemo da postoje neparni prirodni brojevi  $x_n, y_n$  koji zadovoljavaju jednadžbu  $7x_n^2 + y_n^2 = 2^n$ ,  $n \geq 3$ . Za  $n = 3$ , imamo  $x_3 = y_3 = 1$ . Pretpostavimo da za  $n \geq 3$ , brojevi  $x_n, y_n$  zadovoljavaju jednadžbu  $7x_n^2 + y_n^2 = 2^n$ . Dokažimo da postoji par  $(x_{n+1}, y_{n+1})$  neparnih prirodnih brojeva koji zadovoljavaju  $7x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$ . Odnosno,  $7\left(\frac{x_n \pm y_n}{2}\right)^2 + \left(\frac{7x_n \mp y_n}{2}\right)^2 = 2(7x_n^2 + y_n^2) = 2^{n+1}$ . Preciznije jedan od brojeva  $\frac{x_n + y_n}{2}$  i  $\frac{|x_n - y_n|}{2}$  je neparan. Ako je  $\frac{x_n + y_n}{2}$  neparan, onda je  $\frac{7x_n - y_n}{2} = 3x_n + \frac{x_n - y_n}{2}$ , isto neparan, kao suma neparnog i parnog broja. Stoga u ovom slučaju možemo odabrati  $x_{n+1} = \frac{x_n + y_n}{2}$  i  $y_{n+1} = \frac{7x_n - y_n}{2}$ . Ako je  $\frac{x_n - y_n}{2}$  neparan, onda je  $\frac{7x_n + y_n}{2} = 3x_n + \frac{x_n + y_n}{2}$ , tako da biramo  $x_{n+1} = \frac{|x_n - y_n|}{2}$  i  $y_{n+1} = \frac{7x_n + y_n}{2}$ .*

**Primjer 3.10** *Dokažite da jednačba*

$$x^2 + y^2 + z^2 = 59^n$$

*ima rješenje u skupu prirodnih brojeva.*

*Koristimo metodu matematičke indukcije sa korakom  $s = 2$  i  $n_0 = 1$ . Primjetimo da za  $(x_1, y_1, z_1) = (1, 3, 7)$  i  $(x_2, y_2, z_2) = (14, 39, 42)$  imamo*

$$x_1^2 + y_1^2 + z_1^2 = 59$$

*i*

$$x_2^2 + y_2^2 + z_2^2 = 59^2.$$

*Definiramo  $(x_n, y_n, z_n)$ ,  $n \geq 3$ , sa  $x_{n+2} = 59x_n$ ,  $y_{n+2} = 59y_n$ ,  $z_{n+2} = 59z_n$ , za svaki  $n \geq 1$ . Onda je,*

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^2(x_k^2 + y_k^2 + z_k^2),$$

*stoga*

$$x_k^2 + y_k^2 + z_k^2 = 59^k,$$

*odakle slijedi*

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 59^{k+2}.$$



### 3.4. Fermatova metoda

Fermatovu metodu koristimo za dokazivanje da je tvrdnja  $P(n)$  lažna za dovoljno veliki prirodni broj  $n$ . Neka je  $k$  pozitivan cijeli broj. Pretpostavimo:

- Tvrdnja  $P(k)$  je lažna.
- Ako je tvrdnja  $P(m)$  istinita za neki  $m > k$ , onda postoji manji broj  $j$ ,  $m > j \geq k$ , za koji je tvrdnja  $P(j)$  istinita.

Onda je tvrdnja  $P(n)$  lažna za  $n \geq k$ . Ova dva slučaja koristimo u rješavanju diofant-skih jednadžbi:

1. Ne postoji niz nenegativnih cijeli brojeva  $n_1 > n_2 > \dots$ . U nekim slučajevima dobro je zamjeniti 1. ovim ekvivalentnim oblikom: Ako je  $n_0$  najmanji pozitivan broj za koji je tvrdnja  $P(n)$  istinita, onda je tvrdnja  $P(n)$  lažna za svaki  $n < n_0$ .
2. Ako niz nenegativnih brojeva  $(n_i)_{i \geq n}$  zadovoljava nejednakost  $n_1 \geq n_2 \geq \dots$ , onda postoji  $i_0$  tako da je  $n_{i_0} = n_{i_0+1} = \dots$

**Primjer 3.11** *Riješite u nenegativnim cijelim brojevima jednadžbu*

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

*Primjetimo da je  $(0, 0, 0)$  rješenje. Dokažimo da ne postoji nijedno drugo rješenje. Pretpostavimo da je  $(x_1, y_1, z_1)$  netrivialno rješenje. Ako su  $\sqrt[3]{2}$ ,  $\sqrt[3]{4}$  iracionalni, nije teško uočiti da je  $x_1 > 0$ ,  $y_1 > 0$ ,  $z_1 > 0$ . Iz  $x_1^3 + 2y_1^3 = 4z_1^3$  slijedi da 2 dijeli  $x_1$ , te je  $x_1 = 2x_2$ ,  $x_2 \in \mathbb{Z}_+$ . Onda je  $x_2^3 + 2y_1^3 = 4z_1^3$ , te je  $y_1 = 2y_2$ ,  $y_2 \in \mathbb{Z}_+$ . Slično,  $z_1 = 2z_2$ ,  $z_2 \in \mathbb{Z}_+$ . Nastavljamo ovaj proces, konstruiramo niz pozitivnih cijelih brojeva  $(x_n, y_n, z_n)_{n \geq 1}$ , za koje je  $x_1 > x_2 > x_3 > \dots$ . Dobivamo kontradikciju s 1.*

**Primjer 3.12** *Riješite u nenegativnim cijelim brojevima jednadžbu*

$$2^x - 1 = xy.$$

*Primjetimo da su  $(0, k)$ ,  $k \in \mathbb{Z}_+$  i  $(1, 1)$  rješenja. Dokazati ćemo da ne postoje druga rješenja. Neka je  $p_1$  djeljitelj od  $x$  i  $q$  najmanji pozitivan cijeli broj takav da  $p_1$  dijeli  $2^q - 1$ . Mali Fermatov teorem nam kaže da  $p_1$  dijeli  $2^{p_1-1} - 1$ , za  $q \leq p_1 - 1 < p_1$ .*

Dokažimo da  $q$  dijeli  $x$ . Pretpostavimo da ne dijeli, onda je  $x = k \cdot q + r$ , za  $0 < r < q$  i vrijedi:

$$\begin{aligned} 2^x - 1 &= 2^{kq} 2^r - 1 \\ &= (2^q)^k 2^r - 1 \\ &= (2^q - 1 + 1)^k 2^r - 1 \\ &= 2^r - 1 \pmod{p_1} \end{aligned} \tag{1}$$

Iz toga slijedi da  $p_1$  dijeli  $2^r - 1$ , što daje kontradikciju s odabirom od  $q$ . Tada  $q$  dijeli  $x$  i  $1 < q < p_1$ . Sada, neka je  $p_2$  djeljitelj od  $q$ . Jasno je da je  $p_2$  djeljitelj od  $x$  i  $p_2 < p_1$ . Nastavljajući ovaj proces, konstruiramo beskonačno padajuću niz djeljitelja od  $x$ :  $p_1 > p_2 > \dots$ , što je u kontradikciji s 1.

## 4. Zaključak

Mnogi matematički problemi svode se na rješavanje diofantskih jednažbi. Upoznali smo se sa nekim od načina njihovog rješavanja. Ostalo je još nekih kao što su parametarska metoda, mješovite diofanske jednažbe, kvadratne itd. Ostali primjeri kao i ovi koje smo koristili mogu se naći u knjizi [1].

## Literatura

- [1] T. Andreescu, D. Andrica: An introduction to Diophante Equations, GIL 2002.
- [2] K. Burazin, Nelinearne diofantske jednadzbe, Osječki matematički list 7(1), 11-21, 2007.
- [3] A. Dujella: Uvod u teoriju brojeva, PMF - Matematički odsjek, Zagreb, 2015.