

## Uvod u teoriju brojeva, vježbe

Asistentica: Sanda Bujačić, Odjel za matematiku, Sveučilište u Rijeci

# Diofantiske jednadžbe

## Pellove i pellovske jednadžbe

Diofantika jednadžba je algebarska (polinomna) jednadžba s dvjema ili više nepoznanica, s cjelobrojnim koeficijentima, kojoj se traže cjelobrojna ili racionalna rješenja. Primjer takve jednadžbe je  $x^2 - 7y^2 = 1$ .

### Teorem 1.

Neka su  $a, b, c \in \mathbb{Z}$ ,  $d = (a, b)$ . Ako  $d \nmid c$ , tada jednadžba

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

nema cjelobrojnih rješenja. Ako  $d|c$ , onda jednadžba (1) ima beskonačno mnogo cjelobrojnih rješenja. Ako je  $(x_1, y_1)$  jedno rješenje, onda su sva druga rješenja dana s

$$x = x_1 + \frac{b}{d}t,$$

$$y = y_1 - \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

### Teorem 2.

Neka su  $a_1, a_2, \dots, a_n \in \mathbb{Z} \setminus \{0\}$ . Tada linearna diofantinska jednadžba

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \quad (2)$$

ima rješenja ako i samo ako  $(a_1, a_2, \dots, a_n)|c$ . Ako ta jednadžba ima barem jedno rješenje, onda ih ima beskonačno mnogo.

### Definicija 1.

Uređenu trojku prirodnih brojeva  $(x, y, z)$  zovemo **Pitagorina trojka** ako su  $x, y$  katete, a  $z$  hipotenuza nekog pravokutnog trokuta, odnosno ako vrijedi

$$x^2 + y^2 = z^2. \quad (3)$$

Ako su  $x, y, z$  relativno prosti, onda kažemo da je  $(x, y, z)$  **primitivna Pitagorina trojka**, a takav trokut zovemo **primitivni Pitagorin trokut**.

### Napomena

U svakoj primitivnoj Pitagorinoj trojci točno je jedan od brojeva  $x, y$  neparan. Za  $x, y$  parne ne bi se radilo o primitivnoj Pitagorinoj trojci ( $(x, y) = 2$ ), a za  $x, y$  neparne, iz  $x^2 + y^2 \equiv 2 \pmod{4}$

i  $z^2 \equiv 0 \pmod{4}$  uslijedila bi kontradikcija.

### Teorem 3.

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

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

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

### Napomena

Sve Pitagorine trojke dane su identitetom

$$(d(m^2 - n^2))^2 + (2dmn)^2 = (d(m^2 + n^2))^2, \quad d = (x, z).$$

**Zadatak 1.** Naći sve Pitagorine trojke u kojima je jedna stranica a) 39 b) 1999.

**Zadatak 2.** Naći sve Pitagorine trojke u kojima je jedna stranica a) 34 b) 2001.

### Teorem 4.

Jednadžba

$$x^4 + y^4 = z^4$$

nema rješenja u prirodnim brojevima. Ne postoji pravokutni trokut kojemu su duljine kateta kvadrati prirodnih brojeva.<sup>1</sup>

**Zadatak 3.** Naći sva rješenja diofantske jednadžbe  $x^2 + 5y^2 = z^2$  uz uvjet  $(x, y, z) = 1$ .

### Definicija 2.

Diofantska jednadžba

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

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

$$x^2 - dy^2 = N, \quad N \in \mathbb{Z} \setminus \{0\}$$

zove se **pellovska jednadžba**.

### Teorem 5.

Pellova jednadžba  $x^2 - dy^2 = 1$  ima barem jedno netrivijalno rješenje.

### Definicija 3.

Najmanje rješenje  $(x, y)$  u prirodnim brojevima Pellove jednadžbe zovemo **fundamentalno rješenje** i označavamo ga s  $(x_1, y_1)$  ili  $x_1 + y_1\sqrt{d}$ .

---

<sup>1</sup>Specijalan slučaj Velikog Fermatovog teorema.

**Teorem 6.**

Pellova jednadžba  $x^2 - dy^2 = 1$  ima beskonačno mnogo rješenja. Ako je  $(x_1, y_1)$  njeno fundamentalno rješenje, onda su sva njena rješenja u prirodnim brojevima dana s

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{N}. \quad (4)$$

Odnosno,

$$\begin{aligned} x_n &= x_1^n + \binom{n}{2} dx_1^{n-2} y_1^2 + \binom{n}{4} d^2 x_1^{n-4} y_1^4 + \dots \\ y_n &= nx_1^{n-1} y_1 + \binom{n}{3} dx_1^{n-3} y_1^3 + \binom{n}{5} d^2 x_1^{n-5} y_1^5 + \dots \end{aligned}$$

**Napomena**

Iz (4) se lako dobiju rekurzije za nizove  $(x_n)_{n \in \mathbb{N}}$ ,  $(y_n)_{n \in \mathbb{N}}$ . Naime, vrijedi

$$x_n = 2x_1 x_{n-1} - x_{n-2}, \quad y_n = 2x_1 y_{n-1} - y_{n-2}$$

za  $n \geq 2$ , gdje je  $(x_1, y_1)$  fundamentalno rješenje od  $x^2 - dy^2 = 1$ , a  $(x_0, y_0) = (1, 0)$  njeno trivijalno rješenje.

Za razliku od Pellove jednadžbe  $x^2 - dy^2 = 1$ , Pellova jednadžba

$$x^2 - dy^2 = -1 \quad (5)$$

ne mora imati rješenja. Nužan uvjet da ova jednadžba ima rješenje jest da  $d$  nema prostih djelitelja oblika  $p = 4k + 3$ . Naime,  $-1$  mora biti kvadratni ostatak modulo  $d$ . No, taj uvjet nije i dovoljan. Jedan od kriterija je duljina perioda u razvoju broja  $\sqrt{d}$  u verižni razlomak.

**Teorem 7.**

Pretpostavimo da jednadžba  $x^2 - dy^2 = -1$  ima rješenje i neka je  $x_1 + y_1\sqrt{d}$  njeno fundamentalno rješenje. Tada je  $(x_1 + y_1\sqrt{d})^2$  fundamentalno rješenje jednadžbe  $x^2 - dy^2 = 1$ . Nadalje, ako definiramo  $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ , tada su  $x_{2n} + y_{2n}\sqrt{d}$  sva rješenja jednadžbe  $x^2 - dy^2 = 1$ , a  $x_{2n+1} + y_{2n+1}\sqrt{d}$  sva rješenja jednadžbe  $x^2 - dy^2 = -1$ .

**Primjer**

Jednadžba

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

nema rješenja.

Promotrimo jednadžbu  $x^2 - dy^2 = 4$ , gdje je  $d \in \mathbb{N}$ ,  $d$  nije potpun kvadrat. Odmah je jasno da ova jednadžba uvijek ima rješenja u prirodnim brojevima. Naime, ako je  $(x, y)$  rješenje od  $x^2 - dy^2 = 1$ , tada je  $(2x, 2y)$  rješenje jednadžbe  $x^2 - dy^2 = 4$ . No, postoje i neka rješenja, za neke vrijednosti  $d$ , koja se ne dobivaju na ovaj način.

### Teorem 8.

Sva rješenja jednadžbe  $x^2 - dy^2 = 4$  dana su s

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

gdje je  $(x_1, y_1)$  fundamentalno rješenje te jednadžbe.

### Propozicija

Ako jednadžba  $x^2 - dy^2 = 4$  ima rješenja u neparnim brojevima i ako je  $(x_1, y_1)$  njeno fundamentalno rješenje, onda je

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

fundamentalno rješenje od  $x^2 - dy^2 = 1$ .

### Primjer

Fundamentalno rješenje od  $x^2 - 5y^2 = 4$  je  $3 + \sqrt{5}$ , a koje je fundamentalno rješenje od  $x^2 - 5y^2 = 1$ ?

Jednadžba  $x^2 - dy^2 = -4$  ne mora imati rješenja. Ako jednadžba  $x^2 - dy^2 = -1$  ima rješenje, onda rješenja ima i spomenuta jednadžba u parnim brojevima. No, jednadžba  $x^2 - dy^2 = -4$  može imati rješenja i u neparnim brojevima (za  $d = 5$  je fundamentalno rješenje  $(1, 1)$ ).

### Teorem 9.

Pretpostavimo da  $x^2 - dy^2 = -4$  ima rješenja i neka je  $(x_1, y_1)$  njeno fundamentalno rješenje. Tada su sva rješenja te jednadžbe dana s

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

Fundamentalno rješenje jednadžbe  $x^2 - dy^2 = 4$  dano je s

$$\frac{x_2 + y_2 \sqrt{d}}{2} = \left( \frac{x_1 + y_1 \sqrt{d}}{2} \right)^2.$$

Kako naći fundamentalno rješenje jednadžbe koja je Pellova ili pellovska?

### Definicija 4.

1. **Konačni verižni razlomak** je izraz oblika:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}},$$

gdje su  $a_0 \in \mathbb{R}$  i  $a_i > 0$  za  $1 \leq i \leq n$ . Za ovaj izraz ćemo koristiti oznaku  $[a_0; a_1, \dots, a_n]$ .

2. Verižni razlomak se zove **jednostavan** ako vrijedi  $a_0, \dots, a_n \in \mathbb{Z}$ .
3. Verižni razlomak  $c_k = [a_0; a_1, \dots, a_k]$ , za  $0 \leq k \leq n$ , se zove **k-ta konvergenta** od  $[a_0; a_1, \dots, a_n]$ .

Očito je svaki jednostavan konačan verižni razlomak racionalan broj, a vrijedi i obrat, svaki racionalan broj možemo zapisati kao jednostavan konačan verižni razlomak koristeći Euklidov algoritam. Za svaki (konačan) verižni razlomak  $[a_0; a_1, \dots, a_n]$  definiramo brojeve  $p_0, p_1, \dots, p_n$  i  $q_0, q_1, \dots, q_n$  s:

$$\begin{aligned} p_0 &= a_0, & p_1 &= a_0a_1 + 1, & p_k &= a_k p_{k-1} + p_{k-2}, \\ q_0 &= 1, & q_1 &= a_1, & q_k &= a_k q_{k-1} + q_{k-2}, \end{aligned}$$

za  $k = 2, \dots, n$ .

**Primjer 1.** Razvijmo broj  $\frac{41}{47}$  u jednostavni verižni razlomak.

*Rješenje:*

$$\begin{aligned} 47 &= 41 \cdot 1 + 6 \\ 41 &= 6 \cdot 6 + 5 \\ 6 &= 5 \cdot 1 + 1 \\ 5 &= 1 \cdot 5 \end{aligned}$$

Slijedi da je  $\frac{47}{41} = [1; 6, 1, 5]$  pa je  $\frac{41}{47} = [0; 1, 6, 1, 5]$ .

**Zadatak 4.** Razviti brojeve  $\frac{3}{17}$  i  $\frac{101}{11}$  u verižni razlomak.

**Definicija 5.**

Neka je  $(a_n)_{n \geq 0}$  niz cijelih brojeva takav da je  $a_n > 0$  za  $n \geq 1$ . **Beskonačni verižni razlomak** definiramo kao limes konačnog verižnog razlomka

$$[a_0; a_1, \dots, a_k] = \lim_{n \rightarrow \infty} c_n. \quad (6)$$

Lako se vidi da je beskonačan verižni razlomak reprezentant iracionalnog broja, a i s druge strane svaki se iracionalni broj može razviti u beskonačan verižni razlomak.

**Definicija 6.**

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

**Definicija 7.**

Za beskonačni verižni razlomak  $[a_0; a_1, a_2, \dots]$  kažemo da je periodski ako postoji cijeli brojevi  $k \geq 0, m \geq 1$  takvi da je  $a_{m+n} = a_n$  za sve  $n \geq k$ . U tom slučaju verižni razlomak pišemo u obliku

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

gdje "crla" iznad brojeva  $a_k, \dots, a_{k+m-1}$  znači da se taj blok brojeva ponavlja.

Kvadratnoj iracionalnosti  $\sqrt{d}$  je razvoj u verižni razlomak periodičan. Točnije,  $\sqrt{d}$  ima razvoj oblika

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \dots, a_{l-1}, 2a_0}],$$

gdje je  $a_0 = \lfloor \sqrt{d} \rfloor$  te vrijedi  $a_1 = a_{l-1}, a_2 = a_{l-2}, \dots$

Verižni razlomak se može izračunati pomoću sljedećeg algoritma:

$$a_0 = \lfloor \sqrt{d} \rfloor, \quad s_0 = 0, \quad t_0 = 1,$$

$$s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, \quad a_i = \left\lfloor \frac{\sqrt{d} + s_i}{t_i} \right\rfloor \quad \text{za } i \geq 0.$$

**Primjer 2.** Razvijmo broj  $\sqrt{15}$  u jednostavni verižni razlomak.

Rješenje:

$$s_0 = 0, \quad t_0 = 1, \quad a_0 = 3,$$

$$s_1 = a_0 t_0 - s_0 = 3, \quad t_1 = \frac{15 - s_1^2}{t_0} = 6, \quad a_1 = \left\lfloor \frac{s_1 + \lfloor \sqrt{d} \rfloor}{t_1} \right\rfloor = \left\lfloor \frac{3 + \lfloor \sqrt{15} \rfloor}{6} \right\rfloor = 1,$$

$$s_2 = 3, \quad t_2 = 1, \quad a_2 = \left\lfloor \frac{3 + \lfloor \sqrt{15} \rfloor}{1} \right\rfloor = 6,$$

$$s_3 = 3, \quad t_3 = 6.$$

Dakle,  $(s_1, t_1) = (s_3, t_3)$ , pa je  $\sqrt{15} = [3, \overline{1, 6}]$ .

### Teorem 10.

Neka je  $l$  duljina perioda u razvoju u verižni razlomak broja  $\sqrt{d}$ . Ako je  $l$  paran, onda jednadžba  $x^2 - dy^2 = -1$  nema rješenja, a sva rješenja od  $x^2 - dy^2 = 1$  dana su s  $(x, y) = (p_{nl-1}, q_{nl-1})$ ,  $n \in \mathbb{N}$ . Specijalno, fundamentalno rješenje dano je s  $(p_{l-1}, q_{l-1})$ . Ako je  $l$  neparan, onda su sva rješenja jednadžbe  $x^2 - dy^2 = -1$  dana s  $(x, y) = (p_{(2n-1)l-1}, q_{(2n-1)l-1})$ ,  $n \in \mathbb{N}$ , a sva rješenja jednadžbe  $x^2 - dy^2 = 1$  dana su s  $(x, y) = (p_{2nl-1}, q_{2nl-1})$ ,  $n \in \mathbb{N}$ . Specijalno, fundamentalno rješenje od  $x^2 - dy^2 = 1$  dano je s  $(p_{2l-1}, q_{2l-1})$ .

**Zadatak 5.** Nadite fundamentalno rješenje jednadžbe  $x^2 - 103y^2 = 1$ . Možete li po tim rješenjima zaključiti koje bi bilo fundamentalno rješenje jednadžbe  $x^2 - 103y^2 = 4$ ?

**Zadatak 6.** Naći fundamentalno rješenje jednadžbe  $x^2 - 71y^2 = 1$ .

**Zadatak 7.** Naći sva rješenja jednadžbi  $x^2 - 21y^2 = \pm 1$  za koja je  $1 < x < 7000$ .

### Definicija 8.

Neka je  $d \in \mathbb{N}$ ,  $d$  nije potpun kvadrat. Tad jednadžbu

$$x^2 - dy^2 = N, \quad N \in \mathbb{Z} \setminus \{0\}$$

zovemo **Pellovska jednadžba**.

Očito je da takva jednadžba ne mora biti rješiva, ali ako je  $(x + y\sqrt{d})$  njen rješenje, a  $u + v\sqrt{d}$  rješenje jednadžbe  $x^2 - dy^2 = 1$ , onda je

$$(x + y\sqrt{d})(u + v\sqrt{d})$$

također rješenje polazne pellovske jednadžbe. Za to rješenje kažemo da je *asocirano* s rješenjem  $x + y\sqrt{d}$ . Skup svih međusobno asociranih rješenja tvori jednu klasu rješenja pellovske jednadžbe. Rješenja su asocirana ako i samo ako vrijedi:

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

Ako se klasa rješenja  $K$  sastoji od rješenja  $x_i + y_i\sqrt{d}$ ,  $i = 1, 2, \dots$ , onda i rješenja  $x_i - y_i\sqrt{d}$ ,  $i = 1, 2, \dots$  tvore također klasu rješenja koju označavamo s  $\bar{K}$  i kažemo da je ta klasa *konjugirana* klasi  $K$ .

Neka je  $N > 0$ .

### Teorem 11.

Neka je  $u + v\sqrt{d}$  fundamentalno rješenje jednadžbe  $x^2 - dy^2 = 1$ . Tada za fundamentalno rješenje  $x^* + y^*\sqrt{d}$  jednadžbe  $x^2 - dy^2 = N$  vrijedi

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+1)}}\sqrt{N},$$

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

Neka je  $N < 0$ .

### Teorem 12.

Neka je  $u + v\sqrt{d}$  fundamentalno rješenje jednadžbe  $x^2 - dy^2 = 1$ . Tada za fundamentalno rješenje  $x^* + y^*\sqrt{d}$  jednadžbe  $x^2 - dy^2 = N$  vrijedi

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

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

### Propozicija 1.

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

**Zadatak 8.** Naći fundamentalno rješenje jednadžbe

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

**Zadatak 9.** Naći sva rješenja jednadžbe

$$x^2 - 6y^2 = -29.$$

**Zadatak 10.** Pokazati da jednadžba

$$x^2 - 82y^2 = 23$$

nema rješenja.

**Zadatak 11.** Dokazati da je u svakom Pitagorinom trokutu duljina barem jedne katete djeljiva s 4.