

Poglavlje 6

Diofantske aproksimacije

Teorem: Neka je $\alpha \in \mathbb{R}$. Definiramo

$$\frac{p_n}{q_n} := [a_0, a_1, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}},$$

pri čemu je $a_0 = [\alpha], \dots$. Tada je $\lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \alpha$ pa kažemo da je $\alpha = [a_0, a_1, a_2, \dots]$ razvoj broja α u jednostavni verižni razlomak.

Teorem (Euler, Lagrange): Razvoj u jednostavni verižni razlomak realnog broja α je periodičan od nekog člana nadalje ako i samo ako je α kvadratna iracionalnost, tj. $\alpha = \frac{a+\sqrt{b}}{c}$ za neke $a, b, c \in \mathbb{Z}, b > 0, c \neq 0$.

Algoritam za razvoj kvadratne iracionalnosti u jednostavni verižni razlomak. Neka je $\alpha = \alpha_0 = \frac{s_0 + \sqrt{d}}{t_0}$. Definirajmo niz

$$\alpha_i = \frac{s_i + \sqrt{d}}{t_i} \implies a_i = [\alpha_i], s_{i+1} = a_i t_i - s_i, t_{i+1} = \frac{d - s_{i+1}^2}{t_i}.$$

Postoje prirodni brojevi $j < k$ takvi da je $s_j = s_k, t_j = t_k$. Tada je

$$\alpha = [a_0, \dots, a_{j-1}, \overline{a_j, \dots, a_{k-1}}].$$

Zadatak 6.1. Razvijte brojeve $\frac{21}{52}$ i $\frac{1+\sqrt{13}}{5}$ u jednostavni verižni razlomak.

Rješenje.

$$\begin{aligned} \frac{21}{52} &= 0 + \frac{1}{\frac{52}{21}}, \\ \frac{52}{21} &= 2 + \frac{1}{\frac{21}{10}}, \\ \frac{21}{10} &= 2 + \frac{1}{\frac{10}{1}}, \\ \frac{10}{1} &= 10. \end{aligned}$$

Stoga je $\frac{21}{52} = [0, 2, 2, 10]$. Promotrimo sada broj $\frac{1+\sqrt{13}}{5}$. Primjenjujemo algoritam za razvoj u verižni razlomak:

$$\begin{aligned} s_0 &= 1, t_0 = 5, \alpha_0 = \frac{1 + \sqrt{13}}{5}, a_0 = 0 \\ \implies s_1 &= -1, t_1 = \frac{12}{5}, \alpha_1 = \frac{-5 + 5\sqrt{13}}{12}, a_1 = 1 \\ \implies s_2 &= \frac{17}{5}, t_2 = \frac{3}{5}, \alpha_2 = \frac{5\sqrt{13} + 17}{3}, a_2 = 11 \\ \implies s_3 &= \frac{16}{5}, t_3 = \frac{23}{5}, \alpha_3 = \frac{5\sqrt{13} + 16}{23}, a_3 = 1 \\ \implies s_4 &= \frac{7}{5}, t_4 = \frac{12}{5}, \alpha_4 = \frac{5\sqrt{13} + 7}{12}, a_4 = 2 \\ \implies s_5 &= \frac{17}{5}, t_5 = \frac{3}{5}. \end{aligned}$$

Dobili smo ponavljanje para (s_i, t_i) pa je $\left[\frac{1+\sqrt{13}}{5} \right] = [0, 1, \overline{11, 1, 2}]$.

Zadatak 6.2. Odredite realni broj čiji je razvoj u jednostavni verižni razlomak jednak $[3, \overline{1, 2, 1}]$.

Rješenje. Neka je $x = [3, \overline{1, 2, 1}]$ i neka je $x = 3 + \frac{1}{y}$. Tada je

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

Dobili smo kvadratnu jednadžbu $3y^2 - 2y - 3 = 0$ čija su rješenja $y = \frac{2 \pm \sqrt{2^2 + 4 \cdot 3 \cdot 3}}{2 \cdot 3} = \frac{1 \pm \sqrt{10}}{3}$. Zbog uvjeta $y \geq 1$ koji se javlja pri razvoju u verižni razlomak mora biti $y = \frac{1 + \sqrt{10}}{3}$. Dakle,

$$x = 3 + \frac{1}{y} = 3 + \frac{3}{1 + \sqrt{10}} = 3 + \frac{\sqrt{10} - 1}{3} = \frac{8 + \sqrt{10}}{3}.$$

Zadatak 6.3. Neka je $n \in \mathbb{N}$. Dokažite da je $1 + \frac{n}{1 + \frac{n}{1 + \frac{n}{\ddots}}} = \sqrt{n + \sqrt{n + \sqrt{n + \sqrt{n + \dots}}}}$.

Rješenje. Neka je $x_1 = 1 + \frac{n}{1 + \frac{n}{1 + \frac{n}{\ddots}}}$ i $x_2 = \sqrt{n + \sqrt{n + \sqrt{n + \sqrt{n + \dots}}}}$. Tada je

$$x_1 = 1 + \frac{n}{x_1} \implies x_1^2 - x_1 - n = 0 \text{ te } x_2^2 = n + x_2.$$

Oba broja su korijeni iste kvadratne jednadžbe i pozitivni su. Stoga je $x_1 = x_2$.

Zadatak 6.4 (Egipatski razlomci). Neka je $q \in \mathbb{Q}$ takav da je $0 < q < 1$. Dokažite da postoje $n_1 < \dots < n_k \in \mathbb{N}$ takvi da je $q = \frac{1}{n_1} + \dots + \frac{1}{n_k}$.

Rješenje. Neka je $q = \frac{a}{b}$ za prirodne brojeve $a < b$ i neka je $n_1 \in \mathbb{N}$ takav da je $\frac{1}{n_1} \leq \frac{a}{b} < \frac{1}{n_1-1}$. Tada je

$$\frac{a}{b} - \frac{1}{n_1} = \frac{an_1 - b}{bn_1}.$$

Primijetimo da iz uvjeta $\frac{1}{n_1} \leq \frac{a}{b} < \frac{1}{n_1-1}$ slijedi $0 \leq an_1 - b < a$. Stoga novi razlomak ima manji brojnik od starog.

Dakle, ovaj proces će završiti nakon konačno mnogo koraka i dobit ćemo jedna-
kost

$$\frac{a}{b} = \frac{1}{n_1} + \dots + \frac{1}{n_k}.$$

Još moramo dokazati da je $n_1 < \dots < n_k$. Međutim, iz $\frac{a}{b} < \frac{1}{n_1-1} \leq \frac{2}{n_1} = \frac{1}{n_1} + \frac{1}{n_1}$ slijedi da je $n_1 < n_2$ (i analogno se dobije da je $n_i < n_{i+1}$ za sve $i \geq 1$).

Napomena: Prikazani algoritam je pohlepni algoritam jer u svakom koraku uzima najmanji mogući broj n_i . Zanimljiv je i problem prikaza racionalnog broja q preko egipatskih razlomaka s neparnim nazivnicima. Nije teško zaključiti da q mora imati neparan nazivnik, a 1954. dokazano je da svaki racionalan broj $0 < \frac{a}{b} < 1, 2 \nmid b$ ima prikaz $\frac{a}{b} = \frac{1}{n_1} + \dots + \frac{1}{n_k}$, $n_i \in \mathbb{N}, 2 \nmid n_i$. Međutim, otvoren je problem može li se traženi prikaz uvijek dobiti pohlepnim algoritmom nakon konačno mnogo koraka.

Zadatak 6.5. (Eulerova formula za verižne razlomke) Neka su $a_0, a_1, \dots, a_n \in \mathbb{R}$. Dokažite da je

$$\frac{a_0}{1 - \frac{a_1}{1+a_1 - \frac{a_2}{1+a_2 - \frac{a_3}{\ddots - \frac{a_n}{1+a_n}}}}} = a_0 + a_0a_1 + a_0a_1a_2 + \dots + a_0a_1 \dots a_n.$$

Rješenje. Indukcijom ćemo dokazati da za proizvoljne $a_1, \dots, a_n \in \mathbb{R}$ vrijedi

$$\frac{a_1}{1 + a_1 - \frac{a_2}{1+a_2 - \frac{a_3}{\ddots - \frac{a_n}{1+a_n}}}} = \frac{a_1 + a_1a_2 + a_1a_2a_3 + \dots + a_1 \dots a_n}{1 + a_1 + a_1a_2 + a_1a_2a_3 + \dots + a_1 \dots a_n}.$$

Baza $n = 1$ vrijedi trivijalno jer je $\frac{a_1}{1+a_1} = \frac{a_1}{1+a_1}$. Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N}$. Tada imamo

$$\begin{aligned} \frac{a_1}{1 + a_1 - \frac{a_2}{1+a_2 - \frac{a_3}{\ddots - \frac{a_{n+1}}{1+a_{n+1}}}}} &= \frac{a_1}{1 + a_1 - \frac{a_2 + a_2a_3 + \dots + a_2 \dots a_{n+1}}{1 + a_2 + a_2a_3 + \dots + a_2 \dots a_{n+1}}} \\ &= \frac{a_1(1 + a_2 + a_2a_3 + \dots + a_2 \dots a_{n+1})}{1 + a_1 + a_1a_2 + a_1a_2a_3 + \dots + a_1 \dots a_{n+1}} = \frac{a_1 + a_1a_2 + \dots + a_1 \dots a_{n+1}}{1 + a_1 + a_1a_2 + \dots + a_1 \dots a_{n+1}}. \end{aligned}$$

Time je dokazan korak indukcije. Sada je

$$\frac{a_0}{1 - \frac{a_1}{1+a_1 - \frac{a_2}{1+a_2 - \frac{a_3}{\ddots - \frac{a_n}{1+a_n}}}}} = \frac{a_0}{1 - \frac{a_1 + a_1a_2 + \dots + a_1 \dots a_n}{1 + a_1 + a_1a_2 + \dots + a_1 \dots a_n}} = a_0 + a_0a_1 + a_0a_1a_2 + \dots + a_0a_1 \dots a_n.$$

Napomena: Ako u formulu ubacimo brojeve $a_0 = 1, a_1 = x, a_2 = \frac{x}{2}, a_3 = \frac{x}{3}, \dots$, dobit ćemo razvoj u verižni razlomak broja $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!} = a_0 + a_0 a_1 + \dots$

$$e^x = \frac{1}{1 - \frac{x}{1 + x - \frac{\frac{x}{2}}{1 + \frac{x}{2} - \frac{\frac{x}{3}}{1 + \frac{x}{3} - \dots}}}}.$$

Zadatak 6.6. (*) Neka su $a_1, \dots, a_k \in \mathbb{N}$ i neka je $x = [\overline{a_1, \dots, a_n}], y = [\overline{a_n, \dots, a_1}]$. Dokažite da je $xy = -1$.

Rješenje. Vrijedi

$$\begin{aligned} x = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\dots + \frac{1}{a_n + \frac{1}{x}}}}} &\implies \frac{1}{-a_1 + x} = a_2 + \frac{1}{a_3 + \frac{1}{\dots + \frac{1}{a_n + \frac{1}{x}}}} \\ &\implies \frac{1}{-a_2 + \frac{1}{-a_1 + x}} = a_3 + \frac{1}{\dots + \frac{1}{a_n + \frac{1}{x}}} \\ &\dots \\ &\implies -a_n + \frac{1}{-a_{n-1} + \frac{1}{\dots + \frac{1}{-a_2 + \frac{1}{-a_1 + x}}}} = \frac{1}{x} \\ &\implies a_n + \frac{1}{a_{n-1} + \frac{1}{\dots + \frac{1}{a_2 + \frac{1}{a_1 + \frac{1}{x}}}}} = \frac{-1}{x}. \end{aligned}$$

Iz ovoga vidimo da je $\frac{-1}{x} = [\overline{a_n, a_{n-1}, \dots, a_2, a_1}] = y$.

Poglavlje 7

Diofantske jednačbe

Pitagorine trojke

Teorem: Sve Pitagorine trojke (x, y, z) dane su formulom

$$x = d(m^2 - n^2), y = 2dmn, z = d(m^2 + n^2),$$

pri čemu su $d, m, n \in \mathbb{N}$ takvi da je $m > n$ i m, n su različite parnosti.

Teorem: Jednačba $x^4 + y^4 = z^4$ nema rješenja u prirodnim brojevima.

Ovaj rezultat je jedan od koraka u dokazu Velikog Fermatovog teorema jer je njegova trivijalna posljedica da jednačba $x^4 + y^4 = z^4$ nema rješenja u \mathbb{N} .

Veliki Fermatov teorem (Wiles, 1994.): Neka je $n \geq 3$ prirodan broj. Tada jednačba $x^n + y^n = z^n$ nema rješenja u prirodnim brojevima.

Zadatak 7.1. Odredite sve Pitagorine trokute čija je jedna stranica jednaka

(a) 38.

(b) 55.

Rješenje. Sve Pitagorine trojke parametrizirane su formulama

$$a = d(m^2 - n^2), b = 2dmn, c = d(m^2 + n^2),$$

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

(a) Imamo 3 slučaja.

- $a = d(m^2 - n^2) = 38$: Kako $2 \nmid m^2 - n^2$, mora biti $2 \mid d$.
 - $d = 2, m^2 - n^2 = 19 \implies (m, n) = (10, 9) \implies (a, b, c) = (38, 360, 362)$.
 - $d = 38, m^2 - n^2 = 1 \implies$ nema rješenja.
- $b = 2dmn = 38$: $dmn = 19$, ovdje nema rješenja jer m, n moraju biti različite parnosti.

- $c = d(m^2 + n^2) = 38$: Izraz $m^2 + n^2$ ne može biti djeljiv s 19 (jer je $19 = 4k + 3$) pa je (zbog $m, n \geq 1$) jedina mogućnost $d = 19, m^2 + n^2 = 2$. Međutim, m, n su različite parnosti pa ni ovdje nema rješenja.

Dakle, jedina trojka je $(38, 360, 362)$.

(b) Imamo 3 slučaja.

- $a = d(m^2 - n^2) = 55$: Imamo nekoliko mogućnosti.
 - $d = 1, m^2 - n^2 = 55 \implies (m, n) = (28, 27), (8, 3) \implies (a, b, c) = (55, 1512, 1513), (55, 48, 73)$.
 - $d = 5, m^2 - n^2 = 11 \implies (m, n) = (6, 5) \implies (a, b, c) = (55, 300, 305)$.
 - $d = 11, m^2 - n^2 = 5 \implies (m, n) = (3, 2) \implies (a, b, c) = (55, 132, 143)$.
 - $d = 55, m^2 - n^2 = 1 \implies$ nema rješenja.
- $a = 2dmn = 55$: Nema rješenja jer $2 \nmid 55$.
- $c = d(m^2 + n^2) = 55$: Izraz $m^2 + n^2$ ne može biti djeljiv s 11 pa je (zbog $m, n \geq 1$) jedina mogućnost $d = 11, m^2 + n^2 = 5 \implies (m, n) = (2, 1) \implies (a, b, c) = (33, 44, 55)$.

Dakle, sve trojke su $(55, 1512, 1513), (48, 55, 73), (55, 300, 305), (55, 132, 143), (33, 44, 55)$.

Zadatak 7.2. Odredite sve Pitagorine trojke čiji su elementi uzastopni članovi

(a) aritmetičkog niza.

(b) geometrijskog niza.

Rješenje. (a) Uzmimo Pitagorinu trojku (a, b, c) i neka je BSO $a < b < c$. Tada je

$$a^2 + b^2 = c^2, a + c = 2b \implies a^2 + b^2 = (2b - a)^2 \implies 3b^2 = 4ab \implies \frac{b}{a} = \frac{4}{3}.$$

Stoga su jedine takve trojke oblika $(3n, 4n, 5n)$.

(b) Uzmimo Pitagorinu trojku (a, b, c) i neka je BSO $a < b < c$. Tada je

$$a^2 + b^2 = c^2, ac = b^2 \implies a^2 + ac = c^2 \implies (2a + c)^2 = 5c^2.$$

Ovo je nemoguće jer jednačba $x^2 = 5y^2$ nema rješenje u \mathbb{N} . Stoga ne postoji takva trojka.

Zadatak 7.3. Dokažite da za svaki $n \in \mathbb{N}$ postoji Pitagorina trojka koja sadrži n .

Rješenje. Znamo da je $n^2 \equiv 0, 1 \pmod{4}$. Za svaki neparni broj imamo identitet $2k+1 = (k+1)^2 - k^2$, a za svaki broj djeljiv s 4 imamo identitet $4k = (k+1)^2 - (k-1)^2$. Zato se n^2 može prikazati kao razlika 2 kvadrata.

Zadatak 7.4. Dokažite da ne postoji Pitagorina trojka (a, b, c) za koju vrijedi $b^2 = a + 2$.

Rješenje. Za takvu trojku vrijedilo bi $a^2 + a + 2 = a^2 + b^2 = c^2$, odnosno

$$4a^2 + 4a + 8 = (2a + 1)^2 + 7 = 4c^2.$$

Jedina dva kvadrata koja se razlikuju za 7 su 9, 16 pa mora vrijediti $a = 1, c = 2$. Međutim, sada $a + 2 = 3$ nije potpun kvadrat i dobili smo kontradikciju.

Zadatak 7.5. Dokažite da je u svakom pravokutnom trokutu s cjelobrojnim stranicama radijus upisane kružnice također cjelobrojan.

Rješenje. Neka su duljine kateta a, b , duljina hipotenuze c i radijus upisane kružnice r . Tada za površinu trokuta vrijedi

$$P = \frac{ab}{2} = \frac{r(a + b + c)}{2}.$$

Neka je BSO $a = d(m^2 - n^2), b = 2dmn, c = d(m^2 + n^2)$. Tada je

$$r = \frac{ab}{a + b + c} = \frac{2d^2mn(m^2 - n^2)}{d(2m^2 + 2mn)} = dn(m - n) \in \mathbb{N}.$$

Zadatak 7.6. Odredite sva rješenja jednadžbe $x^2 + 2y^2 = z^2$ u skupu prirodnih brojeva.

Rješenje. Za početak možemo pretpostaviti da su x, y, z u parovima relativno prosti jer ih inače možemo podijeliti s njihovim najvećim zajedničkim djeliteljem. Ako $2 \mid x$, tada $2 \mid z$ pa i $2 \mid y$ što je kontradikcija s $(x, y, z) = 1$. Dakle, $2 \nmid x, z$. Zapišimo jednadžbu u obliku

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

Zbog $(x - z, x + z) = 2$ imamo 2 slučaja.

- $x + z = 4a^2, z - x = 2b^2$, pri čemu je $(a, b) = 1$ i $2 \nmid b$. Tada je

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

- $x + z = 2b^2, z - x = 4a^2$, pri čemu je $(a, b) = 1$ i $2 \nmid b$. Tada je

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

Dakle, sva rješenja su parametrizirana s

$$x = \pm(b^2 - 2a^2), y = 2ab, z = b^2 + 2a^2 : (a, b) = 1, 2 \nmid b.$$

Zadatak 7.7. Odredite sve primitivne Pitagorine trojke čije sve 3 stranice leže u intervalu $[2000, 3000]$.

Rješenje. Neka je (a, b, c) takva trojka. Tada postoje relativno prosti prirodni brojevi $m, n \in \mathbb{N}$ različite parnosti takvi da je $a = m^2 - n^2$, $b = 2mn$, $c = m^2 + n^2$. Vrijedi $m \geq n$, a redom možemo dobiti i sljedeća ograničenja na m, n :

$$\begin{aligned} c^2 = a^2 + b^2 &\geq 2000^2 + 2000^2 \implies c = m^2 + n^2 \geq 2829, \\ c = m^2 + n^2 &\geq 2829, \quad a = m^2 - n^2 \geq 2000 \implies 2m^2 \geq 4829 \implies m \geq 50, \\ c = m^2 + n^2 &\leq 3000 \implies n^2 \leq 3000 - 50^2 \implies n \leq 22, \\ c = m^2 + n^2 &\leq 3000 \implies m^2 \leq 3000 \implies m \leq 54, \\ b = 2mn &\geq 2000 \implies n \geq \frac{1000}{54} \implies n \geq 19. \end{aligned}$$

Dobili smo $m \in \{50, 51, 52, 53, 54\}$, $n \in \{19, 20, 21, 22\}$. Sada ćemo provjeriti svaku od tih mogućnosti, a zbog uvjeta različite parnosti brojeva m, n možemo smanjiti broj slučajeva.

- $n = 19$: zbog uvjeta $2mn \geq 2000$ mora biti $m \geq 53$. U slučaju $m = 54$ nema rješenja.
- $n = 20$: U slučajevima $m = 51$, $m = 53$ nema rješenja.
- $n = 21$: U slučaju $m = 50$ dobivamo rješenje $(a, b, c) = (2059, 2100, 2941)$. Za $m = 52$ nema rješenja, a slučaj $m = 54$ možemo eliminirati zbog uvjeta $(m, n) = 1$.
- $n = 22$: U slučajevima $m = 51$, $m = 53$ nema rješenja.

Dakle, jedina trojka je $(a, b, c) = (2059, 2100, 2941)$.

Zadatak 7.8. Ako su $(A, B, C), (a, b, c)$ primitivne Pitagorine trojke takve da je $A < B < C, a < b < c$. Dokažite da je $Aa + Bb + Cc = x^2$ ili $Aa + Bb + Cc = 2y^2$.

Rješenje. Brojevi A, B te a, b su različite parnosti. Pretpostavimo BSO da $2 \nmid A, 2 \mid B$, drugi slučaj se tretira analogno. Tada postoje $M, N \in \mathbb{N}$ takvi da je $A = M^2 - N^2, B = 2MN, C = M^2 + N^2$. Sada imamo 2 slučaja.

1. $2 \nmid a, 2 \mid b$: tada postoje $m, n \in \mathbb{N}$ takvi da je $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$ pa imamo

$$Aa + Bb + Cc = (M^2 - N^2)(m^2 - n^2) + 4MNmn + (M^2 + N^2)(m^2 + n^2) = 2(Mm + Nn)^2.$$

2. $2 \mid a, 2 \nmid b$: tada postoje $m, n \in \mathbb{N}$ takvi da je $a = 2mn, b = m^2 - n^2, c = m^2 + n^2$ pa imamo

$$Aa + Bb + Cc = (M^2 - N^2) \cdot 2mn + (m^2 - n^2) \cdot 2MN + (M^2 + N^2)(m^2 + n^2)$$

Želimo ovaj izraz prikazati kao potpun kvadrat. Kako to mora vrijediti za sve $M, N, m, n \in \mathbb{N}$, bilo bi logično da je ovaj algebarski izraz kvadrat nekog drugog algebarskog izraza.

U izrazu se pojavljuju kvadrati monoma Mm, Mn, Nm, Nn pa pokušajmo s izrazom $(\pm Mm + \pm Mn \pm Nm \pm Nn)^2$. Pri namještanju predznaka \pm gledamo predznake u izrazu

$$(M^2 - N^2) \cdot mn + (m^2 - n^2) \cdot MN = Mm \cdot Mn - Nm \cdot Nn + Mm \cdot Nm - Mn \cdot Nn.$$

Nakon malo igranja s predznacima možemo pokazati da je naš algebarski izraz jednak $(Mm + Mn + Nm - Nn)^2$.

Zadatak 7.9. Dokažite da umnožak k uzastopnih prirodnih brojeva ne može biti potpun kvadrat za

(a) $k = 2$.

(b) $k = 3$.

(c) $k = 4$.

Rješenje. (a) Pretpostavimo da je $n(n+1) = x^2$. Kako je $(n, n+1) = 1$, brojevi $n, n+1$ moraju biti potpuni kvadrati. Međutim, razlika dva kvadrata prirodnih brojeva ne može biti 1.

(b) Pretpostavimo da je $n(n+1)(n+2) = x^2$. Kako je $(n, n+1) = (n+1, n+2) = 1$, broj $n+1$ mora biti potpun kvadrat, tj. $n+1 = a^2$. Sada imamo

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

Međutim, razlika dva kvadrata prirodnih brojeva ne može biti 1.

(c) Pretpostavimo da je $n(n+1)(n+2)(n+3) = x^2$. Primijetimo da je

$$x^2 = n(n+3)(n+1)(n+2) = (n^2 + 3n)(n^2 + 3n + 2) = (n^2 + 3n + 1)^2 - 1.$$

Međutim, razlika dva kvadrata prirodnih brojeva ne može biti 1.

Napomena: Erdős i Selfridge su 1974. dokazali teorem koji kaže da za $k \geq 2$ produkt k uzastopnih prirodnih brojeva nikad ne može biti potencija prirodnog broja, tj. jednadžba

$$n(n+1) \dots (n+k-1) = a^b, \quad k \geq 2, b \geq 2$$

nema rješenja u \mathbb{N} .

Zadatak 7.10. (*) Postoje li $a, b, c, d \in \mathbb{N}$ takvi da je $a^2 + b^2 = c^2, b^2 + c^2 = d^2$?

Rješenje. Mora vrijediti $c^4 - b^4 = (c^2 - b^2)(b^2 + c^2) = a^2 d^2 = (ad)^2$. Dokažimo da jednadžba $x^4 + y^2 = z^4$ nema rješenja u \mathbb{N} .

Pretpostavimo suprotno, neka je (x, y, z) minimalno rješenje (preciznije, s minimalnim z). Tada x, y, z moraju biti u parovima relativno prosti jer je inače $(\frac{x}{d}, \frac{y}{d^2}, \frac{z}{d})$ manje rješenje.

Ako $2 \nmid x$, tada postoje $m, n \in \mathbb{N}$ takvi da je $x^2 = m^2 - n^2, y = 2mn, z^2 = m^2 + n^2$ pa je $(xz)^2 = m^4 - n^4$. Tada je (n, xz, m) manje rješenje (jer $m < z$) što je kontradikcija.

Dakle, $2 \mid x$ pa postoje $m, n \in \mathbb{N}$ takvi da je $x^2 = 2mn, y = m^2 - n^2, z^2 = m^2 + n^2$. Mora vrijediti $(m, n) = 1$ jer inače x, y, z ne bi bili relativno prosti. Zato je (m, n, z) primitivna Pitagorina trojka pa postoje relativno prosti $p, q \in \mathbb{N}$ takvi da je BSO $m = p^2 - q^2, n = 2pq, z = p^2 + q^2$. Sada je

$$x^2 = 2mn = 4pq(p^2 - q^2).$$

Kako je $(p, q) = 1$, brojevi $p, q, p^2 - q^2$ su potpuni kvadrati pa je $p = p'^2, q = q'^2$ i $r^2 = p^2 - q^2 = p'^4 - q'^4$. Trojka (q', r, p') je također rješenje i manja je jer $p' \leq p'^2 = p \leq p^2 < p^2 + q^2 = z$ pa smo dobili kontradikciju i u ovom slučaju.

Zadatak 7.11. (*) Odredite sve proste brojeve p oblika $n^4 + 4$ za neki $n \in \mathbb{N}$.

Rješenje. Vrijedi

$$p = n^4 + 4 = (n^2 - 2n + 2)(n^2 + 2n + 2).$$

Stoga jedan od brojeva $n^2 \pm 2n + 2$ mora biti jednak 1. Nije teško vidjeti da onda mora biti $n = 1$ i $p = 5$.

Napomena: Općenito vrijedi sljedeća jednakost, poznata pod nazivom Sophie-Germain identitet:

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

Pellova jednadžba

Teorem: Ako $d \in \mathbb{N}$ nije potpun kvadrat, tada razvoj u jednostavni verižni razlomak broja \sqrt{d} ima oblik

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

pri čemu je $a_0 = \lfloor \sqrt{d} \rfloor$ te $a_1 = a_{r-1}, a_2 = a_{r-2}, \dots$

Teorem: Ako $d \in \mathbb{N}$ nije potpun kvadrat, sva rješenja jednadžbe $x^2 - dy^2 = \pm 1$ su oblika $(x, y) = (p_n, q_n)$, pri čemu su $\frac{p_n}{q_n}$ konvergente u razvoju broja \sqrt{d} u jednostavni verižni razlomak.

Preciznije, ako je r duljina perioda razvoja, tada vrijedi sljedeće.

- Ako $2 \mid r$, tada jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja jednadžbe $x^2 - dy^2 = 1$ su $(x, y) = (p_{nr-1}, q_{nr-1}), n \in \mathbb{N}$.
- Ako $2 \nmid r$, tada su sva rješenja jednadžbe $x^2 - dy^2 = -1$ dana s $(x, y) = (p_{nr-1}, q_{nr-1}), 2 \nmid n$, a sva rješenja jednadžbe $x^2 - dy^2 = 1$ su dana s $(x, y) = (p_{nr-1}, q_{nr-1}), 2 \mid n$.

Teorem: Neka je (x_1, y_1) najmanje rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ u prirodnim brojevima. Tada su sva rješenja ove jednadžbe u prirodnim brojevima parovi $(x_n, y_n), n \in \mathbb{N}$, pri čemu je

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

Ako definiramo $(x_0, y_0) = (1, 0)$ (trivijalno rješenje Pellove jednadžbe), tada vrijedi i rekursivna formula

$$x_{n+2} = 2x_1x_{n+1} - x_n, \quad y_{n+2} = 2x_1y_{n+1} - y_n, \quad n \geq 0.$$

Zadatak 7.12. Odredite imaju li jednadžbe

(a) $x^2 - 41y^2 = \pm 1$

(b) $x^2 - 23y^2 = \pm 1$

rješenja u prirodnim brojevima. Ako imaju, nađite neko njihovo rješenje.

Rješenje. (a) Razvoj u jednostavni verižni razlomak broja $\sqrt{41}$ je $[6, \overline{2, 2, 12}]$. Period je neparan pa pellovska jednadžba ima rješenje. Minimalno rješenje pellovske jednadžbe je

$$\frac{p_2}{q_2} = 6 + \frac{1}{2 + \frac{1}{2}} = \frac{32}{5}.$$

Dakle, $(x, y) = (32, 5)$. Minimalno rješenje Pellove jednadžbe možemo dobiti kvadriranjem ovog rješenja:

$$(32 + 5\sqrt{41})^2 = 2049 + 320\sqrt{41}.$$

Naravno, mogli smo računati i $\frac{p_5}{q_5}$, ali ovo je brži način. Dakle, minimalno rješenje Pellove jednadžbe je $(x, y) = (2049, 320)$.

(b) Razvoj u jednostavni verižni razlomak broja $\sqrt{23}$ je $[4, \overline{1, 3, 1, 8}]$. Period je paran pa pellovska jednadžba nema rješenja (mogli smo to zaključiti i zbog $(\frac{-1}{23}) = -1$). Minimalno rješenje Pellove jednadžbe je

$$\frac{p_3}{q_3} = 4 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1}}} = \frac{24}{5}.$$

Dakle, minimalno rješenje je $(x, y) = (24, 5)$.

Zadatak 7.13. Dokažite da postoji beskonačno mnogo Pitagorinih trojki čije su katete uzastopni prirodni brojevi.

Rješenje. Jednadžba $m^2 - n^2 = 2mn + 1$ ima beskonačno mnogo rješenja jer je ekvivalentna Pellovoj jednadžbi $(m-n)^2 - 2n^2 = 1$. Sada možemo uzeti beskonačno mnogo trojki $(m^2 - n^2, 2mn, m^2 + n^2)$.

Zadatak 7.14. Dokažite da postoji beskonačno mnogo trokutastih brojeva koji su potpuni kvadrati.

Rješenje. Trokutasti brojevi su oni prirodni brojevi koji se mogu prikazati kao zbroj prvih n prirodnih brojeva. Stoga zadatak postaje traženje rješenja jednadžbe $\frac{n(n+1)}{2} = x^2$. Ona je ekvivalentna jednadžbi $(2n+1)^2 = 8x^2 + 1$. Postoji beskonačno mnogo rješenja Pellove jednadžbe $a^2 - 8b^2 = 1$ i za sva vrijedi $2 \nmid a$.

Zadatak 7.15. Dokažite da pellovska jednadžba $x^2 - 82y^2 = 17$ nema rješenja u prirodnim brojevima.

Rješenje. Ako je (x, y) rješenje, tada je $x^2 \equiv 17 \pmod{41}$. Međutim,

$$\left(\frac{17}{41}\right) = \left(\frac{41}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -1$$

pa to nije moguće.

Zadatak 7.16. Dokažite da postoji beskonačno mnogo prirodnih brojeva $k < m$ za koje vrijedi $k + (k + 1) + \dots + m = km$.

Rješenje. Rješavamo jednađbu

$$\frac{m(m+1)}{2} - \frac{k(k-1)}{2} = km \iff m^2 - (2k-1)m - (k^2 - k) = 0.$$

Ako definiramo $a = 2k - 1$, tada je $k^2 - k = \frac{a^2 - 1}{4}$ i sva pozitivna rješenja ove kvadratne jednađbe su $m = \frac{a + \sqrt{2a^2 - 1}}{2}$.

Pellovska jednađba $2a^2 - 1 = b^2$ ima beskonačno mnogo rješenja (najmanje je $(a, b) = (1, 1)$) i gledajući mod 4 se lako vidi da mora biti $2 \nmid a$. Zaključujemo da postoji beskonačno mnogo vrijednosti a za koje je $m \in \mathbb{N}$.

Zadatak 7.17. Dokažite da postoji beskonačno mnogo $n \in \mathbb{N}$ takvi da za neki $1 < k < n$ vrijedi $\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}$.

Rješenje. Dana jednakost je ekvivalentna s

$$\begin{aligned} \frac{n!}{(k-1)!(n-k+1)!} &= \frac{2n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\ \iff \frac{1}{(n-k+1)(n-k)} &= \frac{2}{k(n-k)} + \frac{1}{(k+1)k} \\ &\iff k(k+1) = 2(n-k+1)(k+1) + (n-k-1)(n-k) \\ &\iff n^2 + 3n + 2 = 2k^2 + 2k \\ &\iff (2n+3)^2 + 1 = 2(2k+1)^2. \end{aligned}$$

Pellovska jednađba $a^2 - 2b^2 = -1$ ima beskonačno mnogo rješenja i sva su dana formulom $a + b\sqrt{2} = (1 + \sqrt{2})^{2t+1}$. Također, gledajući mod 4 nije teško dobiti da a, b moraju biti neparni. Stoga sva rješenja Pellovske jednađbe daju rješenja početne jednađbe pa postoji beskonačno mnogo traženih $n, k \in \mathbb{N}$.

Zadatak 7.18. Ako su $3n + 1$ i $4n + 1$ potpuni kvadrati za neki $n \in \mathbb{N}$, dokažite da $56 \mid n$.

Rješenje. Neka je $3n + 1 = a^2, 4n + 1 = b^2$. Tada je b neparan pa $2 \mid n$. Zato je i a neparan pa mora vrijediti $8 \mid n$. Trebamo još dokazati da $7 \mid n$.

Vrijedi $4a^2 - 3b^2 = 1$. Stoga je

$$2a + \sqrt{3}b = (2 + \sqrt{3})^t$$

za neki $t \in \mathbb{N}$. Raspisivanjem ove jednakosti i gledajući parnost nije teško pokazati da je $t = 2s + 1$ pa je

$$2a + \sqrt{3}b = (2 + \sqrt{3})(7 + 4\sqrt{3})^s \equiv (2 + \sqrt{3})(4\sqrt{3})^s \pmod{7}.$$

Kako je $(4\sqrt{3})^2 = 48 \equiv -1 \pmod{7}$, to znači da je

$$2a + \sqrt{3}b \equiv \pm(2 + \sqrt{3}), \pm(2 + \sqrt{3})4\sqrt{3} \pmod{7}.$$

$$\implies (a, b) \equiv (1, 1), (-1, -1), (-1, 1), (1, -1) \pmod{7}.$$

U svakom od tih slučajeva je $n = b^2 - a^2 = (a + b)(b - a) \equiv 0 \pmod{7}$.

Zadatak 7.19. Odredite sve proste brojeve p za koje je $7p^2 + 1$ potpun kvadrat.

Rješenje. Minimalno rješenje Pellove jednadžbe $x^2 - 7y^2 = 1$ je $(x, y) = (8, 3)$. Stoga su sva rješenja oblika

$$x_n + y_n\sqrt{7} = (8 + 3\sqrt{7})^n.$$

Iz ovoga se raspisivanjem lako vidi da $3 \mid y_n$ pa je jedina mogućnost $p = 3$ što je ujedno i rješenje zadatka.

Zadatak 7.20. Neka je $k \geq 3$ neparan prirodni broj. Odredite fundamentalno rješenje Pellove jednadžbe $x^2 - (k^2 + 4)y^2 = 1$.

Rješenje. Odredimo razvoj broja $\sqrt{k^2 + 4}$ u jednostavni verižni razlomak. Prisjetimo se formula $s_{i+1} = a_i s_i - t_i$, $t_{i+1} = \frac{d - s_{i+1}^2}{t_i}$. Vrijedi

$$\begin{aligned} s_0 &= 0, t_0 = 1, \alpha_0 = \sqrt{k^2 + 4}, a_0 = k \\ \implies s_1 &= k, t_1 = 4, \alpha_1 = \frac{\sqrt{k^2 + 4} + k}{4}, a_1 = \frac{k - 1}{2} \\ \implies s_2 &= k - 2, t_2 = k, \alpha_2 = \frac{\sqrt{k^2 + 4} + k - 2}{k}, a_2 = 1 \\ \implies s_3 &= 2, t_3 = k, \alpha_3 = \frac{\sqrt{k^2 + 4} + 2}{k}, a_3 = 1 \\ \implies s_4 &= k - 2, t_4 = 4, \alpha_4 = \frac{\sqrt{k^2 + 4} + k - 2}{4}, a_4 = \frac{k - 1}{2} \\ \implies s_5 &= k, t_5 = 1, \alpha_5 = \sqrt{k^2 + 4} + k, a_5 = 2k \\ \implies s_6 &= k, t_6 = 4. \end{aligned}$$

Pri računanju brojeva a_i, s_i, t_i koristili smo da je $k < \sqrt{k^2 + 4} < k + 1$.

Dobili smo ponavljanje parova (s_i, t_i) pa je razvoj u verižni razlomak broja $\sqrt{k^2 + 4}$ jednak $[k, \frac{k-1}{2}, 1, 1, \frac{k-1}{2}, 2k]$. Period je neparan pa pellovska jednadžba ima fundamentalno rješenje

$$\frac{x_4}{y_4} = \left[k, \frac{k-1}{2}, 1, 1, \frac{k-1}{2} \right] = \frac{k^3 + 3k}{k^2 + 1} = \frac{\frac{k^3+3k}{2}}{\frac{k^2+1}{2}}.$$

Moramo paziti da je $(x_4, y_4) = 1$, a vrijedi da je $(k^3 + 3k, k^2 + 1) = (2k, k^2 + 1) = (2, k^2 + 1) = 2$. Stoga je $x_4 = \frac{k^3+3k}{2}, y_4 = \frac{k^2+1}{2}$. Sada je fundamentalno rješenje Pellove jednadžbe jednako

$$x_9 + y_9\sqrt{k^2 + 4} = (x_4 + y_4\sqrt{k^2 + 4})^2 = \frac{k^6 + 6k^4 + 9k^2 + 2}{2} + \frac{k^5 + 4k^3 + 3k}{2}\sqrt{k^2 + 4}.$$

Zadatak 7.21. (*) Odredite sva cjelobrojna rješenja jednadžbe $x^2 = 2y^4 + 1$.

Rješenje. Vrijedi $x^2 - 1 = (x - 1)(x + 1) = 2y^4$. Lako se vidi da $2 \mid x$ pa je $(x - 1, x + 1) = 2$. Sada imamo 2 slučaja.

- $x - 1 = 2a^4, x + 1 = 16b^4$: mora vrijediti $2 \nmid a$ i $8b^4 - a^4 = 1$. Ova jednadžba nema rješenja mod 4.
- $x - 1 = 16b^4, x + 1 = 2a^4$: mora vrijediti $2 \nmid a$ i $a^4 - 8b^4 = 1$. Iz toga se dobije $(a^2 - 1)(a^2 + 1) = 8b^4$. Kako je $(a^2 - 1, a^2 + 1) = 2$, jedan od brojeva $a^2 \pm 1$ je potpun kvadrat. To je moguće samo za $a = 0$. Stoga je $(x, y) = (\pm 1, 0)$ jedino rješenje jednadžbe.

Zadatak 7.22. (*) Ako je $m = 2 + 2\sqrt{28n^2 + 1} \in \mathbb{N}$ za neki $n \in \mathbb{N}$, dokažite da je m potpun kvadrat.

Rješenje. Par $(\frac{m}{2} - 1, n)$ je rješenje Pellove jednadžbe $x^2 - 28y^2 = 1$. Pronađimo njezino minimalno rješenje.

Minimalno rješenje Pellove jednadžbe $x^2 - 7y^2 = 1$ je $(x, y) = (8, 3)$, ali $2 \nmid 3$ pa ono ne daje rješenje jednadžbe $x^2 - 28y^2 = 1$. Međutim,

$$(8 + 3\sqrt{7})^2 = 127 + 48\sqrt{7} = 127 + 24\sqrt{28}$$

pa je $(127, 24)$ minimalno rješenje. Dakle,

$$\left(\frac{m}{2} - 1\right) + n\sqrt{28} = (127 + 24\sqrt{28})^t \implies m = (127 + 24\sqrt{28})^t + (127 - 24\sqrt{28})^t + 2 \implies$$

$$m = (8 + 3\sqrt{7})^{2t} + (8 - 3\sqrt{7})^{2t} + 2 = ((8 + 3\sqrt{7})^t + (8 - 3\sqrt{7})^t)^2.$$

Čitatelju za vježbu ostavljamo dokaz da je $(8 + 3\sqrt{7})^t + (8 - 3\sqrt{7})^t \in \mathbb{Z}$.

Zadatak 7.23. (*) Dokažite da postoji beskonačno mnogo $n \in \mathbb{N}$ za koje vrijedi $n^2 + 1 \mid n!$.

Rješenje. Pellovska jednadžba $n^2 + 1 = 5a^2$ ima beskonačno mnogo rješenja (minimalno je $(n, a) = (2, 1)$). Za sva rješenja te jednadžbe vrijedi $n^2 = 5a^2 - 1 \geq 4a^2 \implies n \geq 2a$. Ako je (n, a) rješenje jednadžbe takvo da je $a \geq 6$, tada je $5 < a < 2a \leq n$ pa

$$n^2 + 1 = 5a^2 \mid 5 \cdot a \cdot 2a \mid (2a)! \mid n!.$$

Zadatak 7.24. (*) Odredite sve $n \in \mathbb{N}$ za koje je $3^n - 2$ potpun kvadrat.

Rješenje. Lako se provjeri da je $3^1 - 2 = 1^2, 3^3 - 2 = 5^2$. Neka je sada $n \geq 4$. Rješavamo jednadžbu $3^n - 2 = x^2$. Ako $2 \mid n$, tada bi razlika dva kvadrata morala biti 2 što je nemoguće. Dakle, $2 \nmid n$.

Sada tražimo rješenja pellovske jednadžbe $x^2 - 3y^2 = -2$ uz uvjet da je y potencija od 3. Pellovska jednadžba općenito može imati više minimalnih rješenja, ali postoje ograde za njihove vrijednosti i može se pokazati da ova jednadžba ima jedinstveno minimalno rješenje $(x, y) = (1, 1)$.

Minimalno rješenje pripadne Pellove jednadžbe je $(2, 1)$ pa su sva rješenja naše pellovske jednadžbe jednaka

$$x + y\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^t.$$

Pogledajmo za koje t vrijedi $9 \mid y$. Vrijedi $(2 + \sqrt{3})^3 = 26 + 15\sqrt{3} \equiv -1 \pmod{3}$. Zato je

$$x + y\sqrt{3} \equiv \pm(1 + \sqrt{3}), \pm(1 + \sqrt{3})(2 + \sqrt{3}), \pm(1 + \sqrt{3})(2 + \sqrt{3})^2 \pmod{3}.$$

To znači da mora vrijediti $t = 3k + 1$ da bi bilo $3 \mid y$. Sad ćemo opet koristiti istu ideju. Vrijedi $(2 + \sqrt{3})^9 = (26 + 15\sqrt{3})^3 \equiv -1 \pmod{9}$ i $(1 + \sqrt{3})(2 + \sqrt{3}) = 5 + 3\sqrt{3}$. Zato je

$$x + y\sqrt{3} \equiv \pm(5 + 3\sqrt{3}), \pm(5 + 3\sqrt{3})(26 + 15\sqrt{3}), \pm(5 + 3\sqrt{3})(26 + 15\sqrt{3})^2 \pmod{9}.$$

Provjerom se utvrdi da mora vrijediti $t = 9l + 4$ da bi bilo $9 \mid y$. Međutim, vrijedi $(1 + \sqrt{3})(2 + \sqrt{3})^4 = 265 + 153\sqrt{3}$ pa je y ovdje djeljiv sa 153. Dokažimo da je y djeljiv sa 17 za sve $t = 9l + 4$. Imamo

$$(2 + \sqrt{3})^9 = 70226 + 40545\sqrt{3} \equiv -1 \pmod{17} \implies$$

$$\implies (1 + \sqrt{3})(2 + \sqrt{3})^{9l+4} \equiv (265 + 153\sqrt{3})(-1)^t \equiv 10 \cdot (-1)^t \pmod{7}.$$

To znači da $17 \mid y$ za sve $t = 9l + 4$. Zaključak je da za rješenja jednadžbe $x^2 - 3y^2 = -2$ vrijedi $9 \mid y \implies 17 \mid y$ pa su jedina rješenja $n = 1, 3$.

Napomena 1: Nakon ovog zadatka možemo se zapitati i npr. za koje sve brojeve $n \in \mathbb{N}$ je $3^n - 1$ potpun kvadrat. Ovo je poseban slučaj poznate Catalanove slutnje koju je dokazao Mihăilescu 2002. godine.

Catalanova slutnja (Mihăilescu, 2002.): Neka su a, b, c, d prirodni brojevi takvi da je $b, d \geq 2$ i $a^b - c^d = 1$. Tada je $a = 3, b = 2, c = 2, d = 3$.

Napomena 2: Pellovska jednadžba $x^2 - dy^2 = -1$, ako ima cjelobrojnih rješenja, ima točno jedno minimalno rješenje koje je drugi korijen minimalnog rješenja Pellove jednadžbe $x^2 - dy^2 = 1$. Općenita pellovska jednadžba $x^2 - dy^2 = a$, gdje $a \in \mathbb{Z}$ nije potpun kvadrat, može imati više fundamentalnih rješenja. Preciznije, vrijedi sljedeći teorem.

Teorem: Neka je (x_0, y_0) minimalno rješenje Pellove jednadžbe $x^2 - dy^2 = 1$ i neka je $z_0 = x_0 + y_0\sqrt{d}$. Ako pellovska jednadžba $x^2 - dy^2 = a$ ima rješenje u \mathbb{N} , tada postoji rješenje $(x, y) \in \mathbb{N}^2$ takvo da je

$$|x| \leq \frac{z_0 + 1}{2\sqrt{z_0}} \sqrt{|a|}.$$

Takva rješenja se zovu fundamentalna rješenja. Sva ostala rješenja pellovske jednadžbe (x_1, y_1) mogu se prikazati u obliku

$$x_1 + y_1\sqrt{d} = (x + y\sqrt{d})(x_0 + y_0\sqrt{d})^n$$

za neko fundamentalno rješenje (x, y) i neki $n \in \mathbb{N}_0$.

Napomena 3: Kao što smo vidjeli, Pellova i pellovska jednadžba $x^2 - dy^2 = \pm 1$ su usko povezane s realnim kvadratnim poljem

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

Na polju $\mathbb{Q}(\sqrt{d})$ može se definirati norma

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

Norma N je multiplikativna i sva rješenja Pellove/pellovske jednadžbe su norme ± 1 (takve brojeve zovemo jedinice u $\mathbb{Q}(\sqrt{d})$). Jedinice čine grupu i može se pokazati da je ta grupa izomorfna grupi $\{\pm 1\} \times \mathbb{Z}$. Drugim riječima, sve su jedinice oblika $\pm \epsilon^n$ za neki $n \in \mathbb{Z}$, pri čemu je ϵ minimalno rješenje Pellove jednadžbe

$$\begin{cases} x^2 - dy^2 = \pm 1 & : \text{ ako } d \not\equiv 1 \pmod{4}, \\ x^2 - dy^2 = \pm 4 & : \text{ ako } d \equiv 1 \pmod{4}. \end{cases}$$

Usporedbe radi, lako se vidi da imaginarna kvadratna polja $\mathbb{Q}(\sqrt{-d})$, $d > 0$ imaju samo konačno mnogo jedinica.

Kvadratna polja su općenito vrlo zanimljivi objekti u teoriji brojeva. Npr. važan problem je određivanje broja klasa $h(d)$ kvadratnog polja $\mathbb{Q}(\sqrt{d})$ (ista oznaka kao broj reduciranih formi s diskriminantom d - ta dva pojma su usko povezana). Za $d < 0$ je poznat konačan skup svih diskriminanti d takvih da je $h(d) = 1$, dok je za $d > 0$ taj problem još uvijek otvoren.

Bibliografija

- [1] D. A. Cox: *Primes of the form $x^2 + ny^2$* , Wiley, New York (2013.)
- [2] A. Dujella: *Teorija brojeva*, Školska knjiga, Zagreb (2019.)
- [3] E. Howe: *A new proof of Erdős's theorem on monotone multiplicative functions*, <https://services.artofproblemsolving.com/download.php?id=YXR0YWNobWVudHMvMy91LzAzODljZWU3ZjI4M2VjMGUyZDc0OTFlZWZiODc5Njk1NDljM2MxLnBkZg==&rn=RXJkb3MgVGh1b3J1bS5wZGY=>
- [4] M. Jukić Bokun, I. Soldo: *Zbirka zadataka iz teorije brojeva*, Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike, Osijek (2023,)
- [5] K. Ireland, M. I. Rosen: *A Classical Introduction to Modern Number Theory*, Springer Science & Business Media (1990.)
- [6] D. A. Marcus: *Number Fields. Second edition*, Springer (2018.)
- [7] M. B. Nathanson: *Additive Number Theory: The Classical Bases*, Graduate Texts in Mathematics. Vol. 164. Springer-Verlag. (1996.)
- [8] M. C. Relyea: *On Finite Fields and Higher Reciprocity*, <https://arxiv.org/abs/2407.03559>
- [9] Art of Problem Solving, *AoPS Online*, <https://artofproblemsolving.com/>
- [10] IMOmath, *The IMO Compendium and Mathematics Resources*, <https://imomath.com/>
- [11] Matematička natjecanja, *Materijali za pripremu*, <https://natjecanja.math.hr/priprema-za-natjecanja/materijali-za-pripremu/>
- [12] Školjka, *Web arhiva zadataka iz matematike*, <https://skoljka.org/>