Uvod u teoriju brojeva

6. Diofantske aproksimacije

7. Diofantske jednadžbe

Borka Jadrijević

6.1 Diofantske aproksimacije

Diofantska jednadžba - algebarska (polinomijalna) jednadžba s dvjema ili više nepoznanica s cjelobrojnim koeficijentima, kojoj se traže cjelobrojna ili racionalna rješenja.

Diofantske aproksimacije - ispituju koliko se dobro iracionalni brojevi mogu aproksimirati racionalnima.

Diofantska analiza - proučavanje diofantskih jednadžbi. Tu se isprepliću se dva različita ali usko povezana područja: diofantske aproksimacije i diofantske jednadžbe.

Primjer

Promatrajmo (diofantsku) jednadžbu

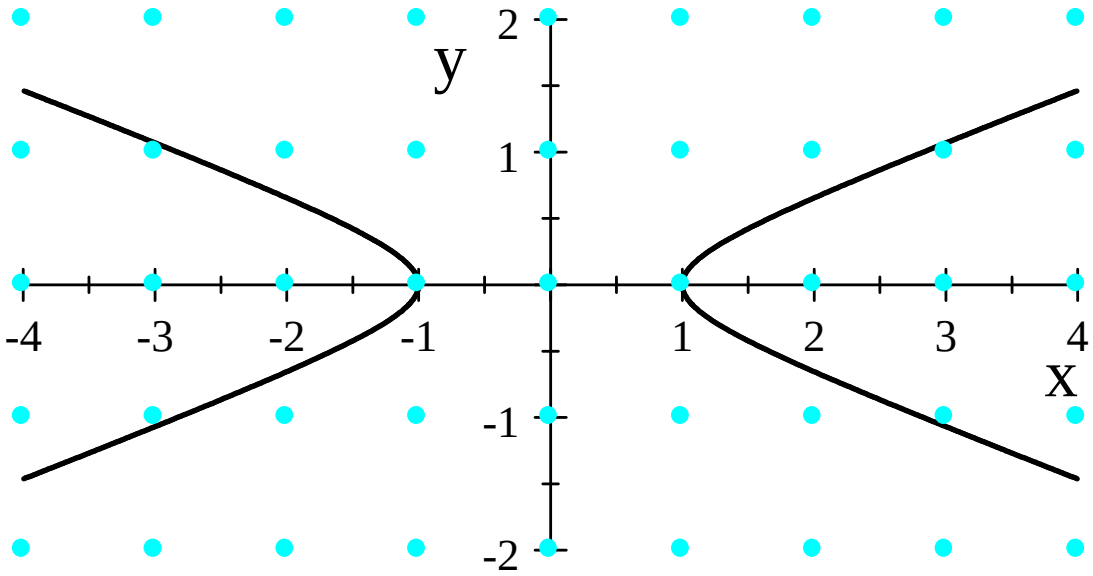
$$x^2 - 7y^2 = 1, \tag{1}$$

Želimo joj naći rješenja u cijelim brojevima. Očito, $(x, y) = (\pm 1, 0)$ *su (trivijalana) rješenja.*

Pitanja:

- Postoji li i neko netrivijlano cjelobrojno rješenje?
- Postoji li beskonačno cjelobrojnih rješenja?
- Postoji li algoritam za nalaženje svih cjelobrojnih rješenja?

Sljedeći graf (hiperbola) opisuje sva realna rješenja od (1):



Cjelobrojna rješenja dobivamo presjekom ovog grafa s cjelobrojnom rešetkom.

Uočimo da je $(x, y) = (8, 3)$ cjelobrojno rješenje od

$$x^2 - 7y^2 = 1. \tag{1}$$

Dakle, postoji i netrivijlano rješenje od (1):

$$8^2 - 7 \cdot 3^2 = \left(8 - 3\sqrt{7}\right)\left(8 + 3\sqrt{7}\right) = 1,$$

pa je

$$\frac{8}{3} - \sqrt{7} = \frac{1}{3\left(8 + 3\sqrt{7}\right)} = 0.020915\ldots\ .$$

Vidimo, da je racionalan broj $\frac{8}{3}$ jako blizu iracionalnom broju $\sqrt{7}$, tj. da cjelobrojno rješenje jednadžbe (1) inducira jako dobru aproksimaciju iracionalnog broja $\sqrt{7}$ pridruženog toj jednadžbi.

Neka je α dani realan broj. Oznake:

- $\lfloor \alpha \rfloor$ - najveći cijeli broj manji ili jednak α ;
- $\{\alpha\}$ - razlomljeni dio od α , tj.

$$\{\alpha\} = \alpha - \lfloor \alpha \rfloor ;$$

- $\|\alpha\|$ - udaljenost od α do najbližeg cijelog broja , tj.

$$\|\alpha\| = \min \{\{\alpha\}, 1 - \{\alpha\}\}.$$

Očito vrijedi:

$$0 \leq \{\alpha\} < 1, \quad 0 \leq \|\alpha\| \leq \frac{1}{2}.$$

Teorem (6.1)(Dirichletov)

Neka su α i Q realni brojevi i $Q > 1$. Tada postoje cijeli brojevi p, q takvi da je $1 \leq q < Q$ i $\|\alpha q\| = |\alpha q - p| \leq \frac{1}{Q}$.

Dokaz:

Korolar (6.1)

Ako je α iracionalan broj, onda postoji beskonačno mnogo parova p, q relativno prostih cijelih brojeva takvih da je

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

Dokaz:

Napomena (6.1)

Tvrdnja Korolara 6.1 ne vrijedi ukoliko je α racionalan.

Neka je α proizvoljan realan broj. Označimo

$$a_0 = \lfloor \alpha \rfloor .$$

Ako je $a_0 \neq \alpha$ zapišimo

$$\alpha = a_0 + \frac{1}{\alpha_1},$$

gdje je $\alpha_1 > 1$. Označimo

$$a_1 = \lfloor \alpha_1 \rfloor$$

Ako je $a_1 \neq \alpha_1$ zapišimo

$$\alpha_1 = a_1 + \frac{1}{\alpha_2},$$

gdje je $\alpha_2 > 1$. Označimo

$$a_2 = \lfloor \alpha_2 \rfloor$$

Ovaj proces možemo nastaviti u nedogled ukoliko nije $a_n = \alpha_n$ za neki n.

Ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj i vrijedi

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}},$$

što kraće zapisujemo $\alpha = [a_0, a_1, ..., a_n]$.
Ako je $a_n \neq \alpha_n$ za sve n, definirajmo racionalne brojeve $\frac{p_n}{q_n}$ sa

$$\frac{p_n}{q_n} = [a_0, a_1, ..., a_n].$$

Teorem (6.2)

Brojevi p_n i q_n zadovoljavaju rekurzivne relacije

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \quad p_0 = a_0, \quad p_1 = a_0 a_1 + 1; \\ q_n &= a_n q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_1 = a_1. \end{aligned}$$

Dokaz:

Napomena (6.2)

Uz dogovor $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$, *Teorem 6.2 vrijedi za sve* $n \geq 0$.

Teorem (6.3)

Za sve $n \geq -1$ *vrijedi:*

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n .$$

Dokaz:

Teorem (6.4)

1. $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots,$
2. $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots,$
3. *Ako je* n *paran, a* m *neparan, onda je* $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.

Dokaz:

Napomena (6.3)

Neka svojstva:

1. $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$ *i* $\alpha_n = a_n + \frac{1}{\alpha_{n+1}} \Longrightarrow \alpha_n > a_n$;
2. $\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$, $n \geq 1$;
3. $\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1} q_n + q_{n-1}) q_n} \Longrightarrow$
   - **a)** $\alpha > \frac{p_n}{q_n}$, *n paran;*
   - **b)** $\alpha < \frac{p_n}{q_n}$, *n neparan;*

   $\Longrightarrow$ *α leži između dva susjedna.*
4. $q_n = a_n q_{n-1} + q_{n-2}$, $q_0 = 1$, $q_1 = a_1 \Longrightarrow q_n \geq n$ *(q_n rastući);*
5. *1., 3. i 4.* $\Longrightarrow \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{n+1} q_n} \leq \frac{1}{n(n+1)}$;
6. $a_{n+1} = \lfloor \alpha_{n+1} \rfloor > \alpha_{n+1} - 1 \Longrightarrow \alpha_{n+1} < a_{n+1} + 1$;

Napomena (6.3 - nastavak)

7. *3. i 6.* $\Longrightarrow$

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{(\alpha_n q_n + q_{n-1})q_n} \overset{(6)}{>} \frac{1}{((a_{n+1}+1)q_n + q_{n-1})q_n} = \frac{1}{(q_n + q_{n+1})q_n};$$

8. $\left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{(a_{n+1}q_{n+1} + q_n)q_{n+1}} \leq \frac{1}{(q_n + q_{n+1})q_{n+1}} \underset{(q_n)\ rast.}{\overset{4)}{<}} \frac{1}{(q_n + q_{n+1})q_n};$

9. *7. i 8.* $\Longrightarrow \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\alpha - \frac{p_n}{q_n}\right| \Longrightarrow$ *svaki sljedeći bolje aproks.* α;

10. *Ako je* α *racionalan, onda je* $a_n = \alpha_n$ *za neki* n, *inače*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^2} \tag{3}$$

$\Longrightarrow$ *postoji beskonačno brojeva koji zadovoljavaju* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$, *što je u suprotnosti s Napomenom 6.1.*

Teorem (6.5)

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha.$$

Dokaz:

Definicija (6.1)

Ako je a_0 cijeli broj, $a_1, \ldots, a_n$ prirodni brojevi, te ako je

$$\alpha = [a_0, a_1, \ldots, a_n],$$

onda ovaj izraz nazivamo razvoj broja α u konačni jednostavni verižni (neprekidni) razlomak. Ako je α iracionalan, onda uvodimo oznaku

$$\lim_{n\to\infty} [a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_n, \ldots].$$

Ako je

$$\alpha = [a_0, a_1, \ldots, a_n, \ldots],$$

onda ovaj izraz nazivamo razvoj broja α u beskonačni jednostavni verižni (neprekidni) razlomak.

Definicija (6.1 - nastavak)

Racionalan broj

$$\frac{p_i}{q_i} = [a_0, a_1, ..., a_i]$$

nazivamo $i-$*ta konvergenta od* α .

Cijeli broj a_i *nazivamo* $i-$*ti parcijalni kvocijent.*

Realan broj

$$\alpha_i = [a_i, a_{i+1}, ...]$$

nazivamo $i-$*ti potpuni kvocijent od* α.

Primjer (6.1)

Ako je $\frac{b}{c}$ *racionalan broj,* $\gcd(b,c)=1$, $b>c>0$ *i (iz Euklidovog algoritma)*

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c \\ c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\vdots \\ r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1} \\ r_{j-1} &= r_j q_{j+1}. \end{aligned}$$

Tada je $\gcd(b,c) = r_j$ *i*

$$\frac{b}{c} = [q_1, q_2, ..., q_{j+1}] = [q_1, q_2, ..., q_j, q_{j+1} - 1, 1].$$

Napomena

Može se pokazati da je razvoj broja α u beskonačni jednostavni verižni (neprekidni) razlomak je jedinstven.

Zadatak (6.1)

Prikažite kao jednostavni verižni (neprekidni) razlomak:

- $\frac{21}{25} = [0, 1, 5, 4]$;
- $\frac{25}{21} = [1, 5, 4]$;
- $\frac{F_{n+1}}{F_n} = \left[\underbrace{1, 1, ..., 1}_{n}\right] = \left[\underbrace{1, 1, ..., 1, 2}_{n-1}\right]$, F_n – *n-ti Fibonaccijev broj.*

Zadatak (6.2)

Nađite prve četiri konvergente jednostavnog verižniog razlomaka

- $e = [1, 2, 1, 1, 4, 1, ..., 1, 2k, 1, ..]$
- $\sqrt{7} = [2, 1, 1, 1, 4, ...]$.

Napomena

Neka je α iracionalan broj, iz formule 3. slijedi da svaka konvergenta od α zadovoljava nejednakost

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

Teorem (6.6)

Neka su $\frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_n}{q_n}$ dvije uzastopne konvergente od α. Tada barem jedna od njih zadovoljava nejednakost

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

Korolar (6.2)

Za svaki α iracionalan broj postoji beskonačno racionalnih brojeva $\frac{p}{q}$ takvih da je

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

Teorem (6.7) (Legendere)

Neka su p i q cijeli brojevi takvi da je $q \geq 1$ i

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

tada je $\frac{p}{q}$ neka konvergenta od α.

Teorem (6.8) (Borel)

Neka su $\frac{p_{n-2}}{q_{n-2}}, \frac{p_{n-1}}{q_{n-1}}$ i $\frac{p_n}{q_n}$ tri uzastopne konvergente od α. Tada barem jedna od njih zadovoljava nejednakost

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Teorem (6.9)(Hurwitz)

Za svaki α iracionalan broj postoji beskonačno racionalnih brojeva $\frac{p}{q}$ takvih da je

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Konstanta $\sqrt{5}$ je najbolja moguća, tj. tvrdnja ne vrijedi ako se $\sqrt{5}$ zamijeni s bilo kojom drugom konstantom $A > \sqrt{5}$.

Aproksimacija iracionalnih brojeva racionalnima

Aproksimacija je bolja što je udaljenost iracionalnog broja od racionalnog manja u usporedbi s veličinom nazivnika racionalnog broja.

Pitanje: Ako je α **realan broj** za koje pozitivane realane brojeve μ nejednadžba

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\mu}} \qquad (2)$$

ima (najviše) konačno mnogo rješenja u cijelim brojevima p i $q > 0$?

Definirajmo

$$\mu(\alpha) = \inf_{\mu \in S} \mu,$$

gdje je $S \neq \emptyset$ skup svih pozitivnih realanih brojeva μ za koje nejednadžba (2) ima (najviše) konačno mnogo rješenja. Ako je $S = \emptyset$, definiramo $\mu(\alpha) = \infty$.

Rezultati:

Teorem (Dirichlet)

Ako je α **iracionalan broj**, *onda postoji beskonačno mnogo parova p, q relativno prostih cijelih brojeva takvih da je*

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

Problem pronalaženja racionalnih brojeva $\frac{p}{q}$ s ovim svojstvom vodi do Fareyevih nizova i verižnih (neprekidnih) razlomaka.

Napomena

Tvrdnja ne vrijedi ukoliko je α **racionalan**.

Uočimo:

$$\alpha \textbf{ iracionalan} \quad \overset{Dir.}{\Longrightarrow} \quad 2 \leq \mu(\alpha)$$

Teorem (Liouville)

Neka je α **realan algebarski broj** *stupnja* $n \geq 2$. *Tada postoji konstanta* $c(\alpha) > 0$ *tako da vrijedi*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}$$

za sve racionalne brojeve $\frac{p}{q}$, *gdje je* $q > 0$.

Korolar

Neka je α **realan algebarski broj** *stupnja* $n \geq 2$, *tada nejednadžba*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{n+\varepsilon}}$$

gdje je $\varepsilon > 0$, *ima konačno mnogo rješenja.*

Uočimo:

$$\alpha \textbf{ realan algebarski stupnja } n \geq 2 \implies \mu(\alpha) \overset{Liouv.}{\leq} n$$

Pitanje: Je li n najbolji mogući rezultat, tj. je li $\mu(\alpha) = n$?

Odgovor: Ne!

Rezultat su poboljšavali **Thue** $\left(\mu(\alpha) \leq \frac{n}{2} + 1\right)$, **Siegel** $\left(\mu(\alpha) \leq 2\sqrt{n}\right)$, **Gelfond** $\left(\mu(\alpha) \leq \sqrt{2n}\right)$ ....

Konačan odgovor:

Teorem (Roth)

[a] *Za* **realan algebarski broj** α *nejednadžba*

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

gdje je $\varepsilon > 0$, *ima konačno mnogo rješenja.*

[a] Njemački matematičar Klaus Roth je za ovaj rezultat dobio Fieldsovu medalju 1958.

Ovo je, po Dirichletovom teoremu, najbolji mogući rezultat za α realan algebarski stupnja $n \geq 2$:

$$2 \overset{Dir.}{\leq} \mu(\alpha) \overset{Roth}{\leq} 2 \implies \mu(\alpha) = 2$$

Zaključak:

- $\mu(\alpha) = 1$, ako je α racionalan; (Dirichlet)
- $\mu(\alpha) = 2$, ako je α realan algebarski stupnja $n \geq 2$; (Roth)
- $2 \leq \mu(\alpha) \leq \infty$, ako je α transcendentan.

Broj $\mu(\alpha)$ se naziva iracionalna mjera ili Liouville - Rothova konstanta.

Primjer:

- Za transcendentan broj α kažemo da je Liouvilleov broj ako je $\mu(\alpha) = \infty$. Npr. Liouvilleov broj je

$$\sum_{j=1}^{\infty} 10^{-j!} = 0.11000100000000000000001000...;$$

- $\mu(\pi) < 8.0161 \implies \pi$ nije Liouvilleov broj;
- $\mu(e) = 2$.

Za rješavanje mnogih Diofantskih jednadžbi važna je aproksimacija algebarskih brojeva racionalnima.

- **Problem:** Rothov (Thueov, Siegelov, ... , osim Liouvilleovog) rezultat je "neefektivan", tj. ne daje način (algoritam) za nalaženje svih rješenja nejednadžbe

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

- "Efektivne" rezultate daje nam Bakerova teorija linearnih formi u logaritmima algebarskih brojeva, pomoću koje su rješeni mnogi problemi vezani za Diofantske jednadžbe.

Definicija (6.2)

Za beskonačan verižni razlomak

$$[a_0, a_1, a_2, \ldots]$$

kažemo da je periodski ako postoje cijeli brojevi $k \geq 0$, $m \geq 1$ takvi da je $a_{n+m} = a_n$ za sve $n \geq k$. U tom slučaju verižni razlomak pišemo u obliku

$$\left[a_0,\ a_1, \ldots,\ a_{k-1},\ \overline{a_k,\ a_{k+1}, \ldots, a_{k+m-1}}\right],$$

gdje "crta" iznad brojeva a_k, $a_{k+1}, \ldots, a_{k+m-1}$ znači da se taj blok brojeva ponavlja u nedogled.

Primjer

- $\beta = \left[\overline{2, 8}\right] \Longrightarrow \beta = \left[2, 8, \overline{2, 8}\right] = [2, 8, \beta] \Longrightarrow$

  $\beta = 2 + \frac{1}{8+\frac{1}{\beta}} \overset{\lfloor\beta\rfloor=2}{\Longrightarrow} \beta = \frac{2+\sqrt{5}}{2}$;

- $\alpha = \left[3, 1, \overline{2, 8}\right] \Longrightarrow \alpha = 3 + \frac{1}{1+\frac{1}{\beta}} \Longrightarrow \alpha = \frac{36+2\sqrt{5}}{11}$.

Definicija (6.3)

Za iracionalan broj α kažemo da je kvadratna iracionalnost ako je α korijen kvadratne jednadžbe s racionalnim koeficijentima.

Teorem (6.10)(Euler, Lagrange)

Razvoj u jednostavni verižni razlomak realnog broja α je periodski ako i samo ako je α kvadratna iracionalnost.

Dokaz:

Iz dokaza slijedi *algoritam* za nalaženje jednostavnog verižnog (neprekidnog) razlomka od

$$\alpha = \frac{a + \sqrt{d}}{b}.$$

Množeći brojnik i nazivnik s $\pm b$, ako je nužno, možemo pretpostaviti da $b|(d - a^2)$.

Neka je

$$\alpha = \frac{a+\sqrt{d}}{b},\ s_0 = a,\ t_0 = b,\ t_0 \,\big|\, \left(d - s_0^2\right),$$

$$a_n = \left\lfloor \frac{s_n + \sqrt{d}}{t_n} \right\rfloor, \quad s_{n+1} = a_n t_n - s_n,$$

$$t_{n+1} = \frac{d - s_{n+1}^2}{t_n} \quad \text{za} \quad n \geq 0.$$

Ako je

$$(s_j, t_j) = (s_k, t_k) \quad \text{za} \quad j < k,$$

onda je

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

Zadatak (6.4)

Nađite jednostavni verižni (neprekidni) razlomak od:

- $\sqrt{6} = \left[2, \overline{2, 4}\right]$;
- $\sqrt{d^2 - d} = \left[d - 1, \overline{2, 2d - 2}\right]$, $d \in \mathbb{N}$, $d \geq 2$;
- $\sqrt{\frac{5}{3}} = \left[1, \overline{3, 2}\right]$;
- $\sqrt{\frac{2c+1}{2c}} = \left[1, \overline{4c, 2}\right]$, $c \in \mathbb{N}$;
- $\frac{2+\sqrt{5}}{3} = \left[\overline{1, 2, 2, 1, 12}\right]$.

Teorem (6.11)

Kvadratna iracionalnost α ima čisto periodski razvoj u jednostavni verižni razlomak ako i samo ako je $\alpha > 1$, te $-1 < \alpha' < 0$, gdje je α' konjugat od α (u tom slučaju kažemo da je α reducirana kvadratna iracionalnost).

Teorem (6.12)

Neka je d prirodan broj koji nije potpun kvadrat, onda jednostavan verižni razlomak od $\sqrt{d}$ ima oblik

$$\sqrt{d} = \left[a_0; \overline{a_1, a_2 \ldots, a_{r-1}, 2a_0}\right],$$

gdje je $a_0 = \left\lfloor \sqrt{d} \right\rfloor$, a niz $a_1, a_2 \ldots, a_{r-1}$ je centralno simetričan, tj. vrijedi

$$a_i = a_{r-i} \quad za\ i = 1, \ldots, r-1.$$

Ovdje $r = r(d)$ označava duljinu najkraćeg perioda u razvoju od $\sqrt{d}$. Nadalje, uz oznake od prije, imamo $\alpha_0 = \sqrt{d}$, $t_0 = 1$, $s_0 = 0$. Tada vrijedi: $t_i = 1$ ako i samo ako $r \mid i$. Nadalje, $t_i \neq -1$ za svaki i.

Napomena

Neka $r = r(d)$ označava duljinu najkraćeg perioda u razvoju od $\sqrt{d}$, tada vrijedi sljedeće:

- *ako je $s_n = s_{n+1}$ onda je $r = 2n$;*
- *ako je $t_n = t_{n+1}$ onda je $r = 2n+1$.*

Zadatak (6.5)

Nađite jednostavni verižni (neprekidni) razlomak od:

- $\sqrt{15} = \left[3, \overline{1, 6}\right]$;
- $\sqrt{29} = \left[5, \overline{2, 1, 1, 2, 10}\right]$. $(t_2 = t_3 = 5 \Longrightarrow r = 5)$

Teorem (6.13)

Neka je d prirodan broj koji nije potpun kvadrat, onda za sve $n \geq -1$ vrijedi

$$p_n^2 - dq_n^2 = (-1)^{n+1} t_{n+1}.$$

Dokaz:

7. Diofantske jednadžbe

Diofantska jednadžba

$$x^2 - dy^2 = 1, \tag{4}$$

gdje je $d \in \mathbb{N}$, $d \neq \square$, naziva se **Pellova jednadžba.**

Diofantska jednadžba oblika

$$x^2 - dy^2 = N, \tag{5}$$

gdje je $d \in \mathbb{N}$, $d \neq \square$ i $N \in \mathbb{Z}$, $N \neq 0$, naziva se **pellovska jednadžba.**

Napomena

- $d \in \mathbb{Z}$ *i* $d < 0 \Longrightarrow (4)$ *i* (5) *imaju konačno rješenja;*
- $d = \square = a^2 \Longrightarrow x^2 - a^2y^2 = (x - ay)(x + ay) = N \Longrightarrow$ *konačno rješenja;*
- *Pellova jednadžba ima beskonačno rješenja, a pellovska, ako ih ima, ima ih beskonačno.*

Teorem (7.1)

Neka je $d \in \mathbb{N}$, $d \neq \square$, *te neka su* $\frac{p_n}{q_n}$ *konvergente u razvoju od* $\sqrt{d}$. *Neka je* $N \in \mathbb{Z}$, $|N| < \sqrt{d}$. *Tada za svako rješenje u prirodnim brojevima* $x = u$, $y = v$ *jednadžbe*

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

takvo da je $\gcd(u, v) = 1$ *vrijedi* $u = p_n$, $v = q_n$ *za neki* $n \in \mathbb{N}$.

Dokaz:

Iz Teorema 6.12, 6.13, 6.14 slijedi:

Teorem (7.2)

Sva rješenja u prirodnim brojevima jednadžbi

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

nalaze se među $x = p_n$, $y = q_n$, *gdje su* $\frac{p_n}{q_n}$ *konvergente u razvoju od* $\sqrt{d}$. *Neka je* r *duljina perioda u razvoju od* $\sqrt{d}$.

Teorem (7.2 - nastavak)

Ako je r paran, onda jednadžba $x^2 - dy^2 = -1$ nema rješenja, a sva rješenja od $x^2 - dy^2 = 1$ su dana sa $x = p_{kr-1}$, $y = q_{kr-1}$, $k \in \mathbb{N}$. Ako je r neparan, onda su sva rješenja od $x^2 - dy^2 = -1$ dana sa $x = p_{kr-1}$, $y = q_{kr-1}$, $k \in \mathbb{N}$, k neparan, a sva rješenja od $x^2 - dy^2 = 1$ dana sa $x = p_{kr-1}$, $y = q_{kr-1}$, $k \in \mathbb{N}$, k paran.

Dokaz:

Teorem (7.3)

Ako je (x_1, y_1) je najmanje rješenje[a] u prirodnim brojevima jednadžbe $x^2 - dy^2 = 1$ (fundamentalno rješenje), onda su sva rješenja ove jednadžbe u prirodnim brojevima dana sa (x_n, y_n) za $n \in \mathbb{N}$, gdje su x_n i y_n prirodni brojevi definirani sa

$$x_n + \sqrt{d}y_n = \left(x_1 + \sqrt{d}y_1\right)^n, \tag{6}$$

[a] (x_1, y_1) je najmanje rješenje ako za svako drugo rješenje (s, t) vrijedi $x_1 + \sqrt{d}y_1 < s + \sqrt{d}t$.

Teorem (7.3 - nastavak)

tj.

$$x_n = x_1^n + \sum_{j=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n}{2j} x_1^{n-2j} y_1^{2j} d^j,$$

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

Dokaz:

Teorem (7.4)

Neka je (x_n, y_n) *niz svih rješenja od* $x^2 - dy^2 = 1$ *u prirodnim brojevima zapisan u rastućem redosljedu. Definirajmo* $(x_0, y_0) = (1, 0)$, *tada vrijede rekurzivne relacije*

$$x_{n+2} = 2x_1 x_{n+1} - x_n, \quad n \geq 0,$$

$$y_{n+2} = 2x_1 y_{n+1} - y_n \quad n \geq 0.$$

Dokaz: Korištenjem (6).

Primjer (7.1)

Nađite najmanja rješenja u prirodnim brojevima od:

$$x^2 - 29y^2 = 1 \quad i \quad x^2 - 29y^2 = -1$$

Rješenje:

$$\sqrt{29} = \left[5, \overline{2, 1, 1, 2, 10}\right] \Longrightarrow r = 5 \text{ (neparan)} \Longrightarrow$$

- $x^2 - 29y^2 = -1 \overset{T.\ 7.2}{\Longrightarrow}$ *sva pozitivna rješenja su dana sa*

$$x = p_{5k-1}, y = q_{5k-1}, \quad k \in \mathbb{N}, \quad k \text{ neparan}$$

$\Longrightarrow$ *najmanje za* $k = 1$ $(n = 4) \overset{rek.}{\Longrightarrow}$

$$(x_1, y_1) = (p_4, q_4) = (70, 13);$$

Primjer (7.1 -nastavak)

$x^2 - 29y^2 = 1 \overset{T.\ 7.2}{\Longrightarrow}$ *sva pozitivna rješenja su dana sa*

$$x = p_{5k-1}, y = q_{5k-1}, k \in \mathbb{N}, \quad k \text{ paran}$$

$\Longrightarrow$ *najmanje za* $k = 2$ $(n = 9) \overset{rek.}{\Longrightarrow}$

$$(x_1, y_1) = (p_9, q_9) = (9801, 1820);$$

Traženje konvergenti, tj. minimalnih rješenja u prirodnim brojevima:

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \qquad p_0 = a_0, \qquad p_1 = a_0 a_1 + 1; \\ q_n &= a_n q_{n-1} + q_{n-2}, \qquad q_0 = 1, \qquad q_1 = a_1. \end{aligned}$$

n	0	1	2	3	4	5	6	7	8	9
a_n	5	2	1	1	2	10	5	2	1	1
p_n	5	11	16	27	**70**	727	1524	2251	3775	**9801**
q_n	1	2	3	5	**13**	135	283	418	701	**1820**

Primjer (7.1 - nastavak)

Kako je $(x_1, y_1) = (p_9, q_9) = (9801, 1820)$ *najmanje rješenje od* $x^2 - 29y^2 = 1$ *sva pozitivna rješenja su dana sa*

$$\begin{aligned} x_{n+2} &= 2x_1 x_{n+1} - x_n, \quad n \geq 0, \\ y_{n+2} &= 2x_1 y_{n+1} - y_n \quad n \geq 0, \end{aligned}$$

gdje je $(x_0, y_0) = (1, 0)$ *i* $(x_1, y_1) = (9801, 1820)$. *Npr. imamo:*

$$\begin{aligned} x_2 &= 2x_1 x_1 - x_0 = 2 \cdot (9801)^2 - 1 = 192\,119\,201 \\ y_2 &= 2x_1 y_1 - y_0 = 2 \cdot 9801 \cdot 1820 - 0 = 35\,675\,640. \end{aligned}$$

Uočimo: $(x_2, y_2) = (p_{19}, q_{19})$.

Još neke diofantske jednadžbe

Teorem (7.5)

Neka su $a, b, c \in \mathbb{Z}$ cijeli brojevi i neka je $\gcd(a, b) = d$. Tada (linearna) diofantska jednadžba

$$ax + by = c \tag{7}$$

ima rješenje onda i samo onda ako $d \mid c$. Ako $d \mid c$, onda jednadžba (7) ima beskonačno cjelobrojnih rješenja. Ako je (x_1, y_1) jedno rješenje, onda su sva rješenja dana sa $x = x_1 + \frac{b}{d}t$, $y = y_1 - \frac{a}{d}t$, $t \in \mathbb{Z}$.

Dokaz:

Teorem (7.6)

Neka su $a_1, a_2, ..., a_n \in \mathbb{Z}$ cijeli brojevi i neka je $\gcd(a_1, a_2, ..., a_n) = d$. Tada (linearna) diofantska jednadžba

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c \tag{8}$$

ima rješenje onda i samo onda ako $d \mid c$. Ako jednadžba (8) ima cjelobrojnih rješenja, onda ih ima beskonačno.

Dokaz: Indukcijom.

Definicija (7.1)

Uređenu trojku prirodnih brojeva (x, y, z) nazivamo Pitagorina trojka ako vrijedi

$$x^2 + y^2 = z^2, \tag{9}$$

tj. ako su x, y katete, a z hipotenuza pravokutnog trokuta. Ako su x, y, z relativno prosti, onda kažemo da je (x, y, z) primitivna Pitagorina trojka (a pripadni trokut primitivni Pitagorin trokut).

Napomena

U primitivnoj Pitagorinoj trojci točno jedan od brojeva x, y je neparan:

- *oba parna $\Longrightarrow$ z paran $\Longrightarrow$ nije primitivna;*
- *oba neparna $\Longrightarrow x^2 + y^2 \equiv 2 \pmod 4 \Longrightarrow z^2 \equiv 2 \pmod 4$ $(\Longrightarrow\Longleftarrow)$;*

Teorem (7.7)

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

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

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

Dokaz:

Iz prethodnog teorema slijedi da su sve Pitagorine trojke dane identitetom

$$\left[d\left(m^2 - n^2\right)\right]^2 + (2dmn)^2 = \left[d\left(m^2 + n^2\right)\right]^2. \tag{10}$$

Primjer (7.2)

Nađite sve Pitagorine trokute u kojima je jedna stranica jednaka

a) 39, **b)** 199, **c)** 34, **b)** 2001.