Teorija brojeva

Filip Najman

9. predavanje

24.5.2021.

Zadatak

Je li funkcija $\lambda(n) = (-1)^{\omega}(n)$*, gdje je* $\omega(n) =$ *broj prostih djelitelja od n multiplikativna?*

Zadatak

Je li funkcija $F(n) = \varphi(n^2)$*, multiplikativna?*

Diofantske aproksimacije

Za dani realni broj α s $\{\alpha\}$ ćemo označavati razlomljeni dio od α, tj. $\{\alpha\} = \alpha - \lfloor\alpha\rfloor$, a sa $\|\alpha\|$ označavat ćemo udaljenost od α do najbližeg cijelog broja, tj. $\|\alpha\| = \min(\{\alpha\}, 1 - \{\alpha\})$.

Očito je $0 \leq \{\alpha\} < 1$ i $0 \leq \|\alpha\| \leq \frac{1}{2}$.

Na primjer, $\{3.7\} = 0.7$ i $\|3.7\| = 0.3$.

Teorem (Dirichlet)

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: Pretpostavimo najprije da je Q prirodan broj. Promotrimo sljedećih $Q+1$ brojeva:

$$0, 1, \{\alpha\}, \{2\alpha\}, \ldots, \{(Q-1)\alpha\}.$$

Svi ovi brojevi leže na segmentu $[0,1]$. Podijelimo segment $[0,1]$ na Q disjunktnih podintervala duljine $\frac{1}{Q}$:

$$[0, \frac{1}{Q}\rangle,\ [\frac{1}{Q}, \frac{2}{Q}\rangle,\ [\frac{2}{Q}, \frac{3}{Q}\rangle,\ \ldots,\ [\frac{Q-1}{Q}, 1].$$

Prema Dirichletovom principu, barem jedan podinterval sadrži dva (ili više) od gornjih $Q+1$ brojeva.

Uočimo da broj $\{r\alpha\}$ ima oblik $r\alpha - s$, $r, s \in \mathbb{Z}$, a brojevi 0 i 1 se također mogu zapisati u tom obliku (uz $r = 0$).

Dakle, postoje cijeli brojevi r_1, r_2, s_1, s_2 takvi da je $0 \le r_i < Q$, $i = 1, 2$, $r_1 \ne r_2$ i da vrijedi

$$\left|(r_1\alpha - s_1) - (r_2\alpha - s_2)\right| \le \frac{1}{Q}.$$

Možemo pretpostaviti da je $r_1 > r_2$. Stavimo: $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \le q < Q$ (jer su i r_1 i r_2 manji od q) i $|\alpha q - p| \le \frac{1}{Q}$, čime je tvrdnja teorema dokazana u slučaju $Q \in \mathbb{N}$.

Pretpostavimo sada da Q nije prirodan broj. Neka je $Q' = \lfloor Q \rfloor + 1 > Q$. Prema prije dokazanom, postoje cijeli brojevi p, q takvi da je $1 \le q < Q'$ i $|\alpha q - p| \le \frac{1}{Q'} < \frac{1}{Q}$.

Također zbog $1 \le q < Q'$ slijedi $1 \le q \le \lfloor Q \rfloor$, odnosno $1 \le q < Q$. $\square$

Korolar

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

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

Dokaz: Tvrdnja Dirichletovog Teorema očito vrijedi i ukoliko zahtjevamo da su p i q relativno prosti. Naime ako je $(p, q) = d$ i $p = dp_1$, $q = dq_1$, tada je

$$|dq_1\alpha - dp_1| \leq \frac{1}{Q}, \text{ pa je } |q_1\alpha - p_1| \leq \frac{1}{dQ} \leq \frac{1}{Q}.$$

Dakle, za $Q > 1$ postoje relativno prosti cijeli brojevi p, q takvi da je $|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} < \frac{1}{q^2}$. Budući da je α iracionalan, slijedi da $\alpha q - p \neq 0$ tj. $|\alpha - \frac{p}{q}| > 0$ za sve $\frac{p}{q} \in \mathbb{Q}$.

Pretpostavimo da postoji samo konačno mnogo racionalnih brojeva $\frac{p}{q}$ koji zadovoljavaju (1).

Neka su to brojevi $\frac{p_j}{q_j}$, $j = 1, \ldots, n$.

Izaberimo prirodan broj m tako da je $\frac{1}{m} < |\alpha q_j - p_j|$ za sve $j = 1, \ldots, n$.

Primijenimo sada Teorem 3 uz $Q = m$, pa dobivamo racionalan broj $\frac{p}{q}$ s $q < m$ za koji vrijedi $|\alpha q - p| \leq \frac{1}{m} < \frac{1}{q}$, pa vrijedi i $|\alpha - \frac{p_j}{q_j}| \leq \frac{1}{mq} < \frac{1}{q^2}$.

Također, $\frac{p}{q}$ je različit od $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, što je kontradikcija. $\square$

Napomena

Tvrdnja prethodnog Korolara ne vrijedi ukoliko je α racionalan.

Zaista, neka je $\alpha = \frac{u}{v}$. Ako je $\frac{p}{q} \neq \alpha$, onda

$$\frac{1}{q^2} > |\alpha - \frac{p}{q}| = |\frac{u}{v} - \frac{p}{q}| = |\frac{uq - vp}{vq}| \geq \frac{1}{vq},$$

povlači da je $q < v$. To znači da (1) može biti zadovoljeno samo za konačno parova p, q relativno prostih cijelih brojeva.

Neka je α proizvoljan realan broj. Stavimo: $a_0 = \lfloor \alpha \rfloor$.

Ako je $a_0 \neq \alpha$, onda zapišimo α u obliku $\alpha = a_0 + \frac{1}{\alpha_1}$, tako da je $\alpha_1 > 1$, i stavimo $a_1 = \lfloor \alpha_1 \rfloor$.

Ako je $a_1 \neq \alpha_1$, onda α_1 zapišimo u obliku $\alpha_1 = a_1 + \frac{1}{\alpha_2}$, tako da je $\alpha_2 > 1$, i stavimo $a_2 = \lfloor \alpha_2 \rfloor$.

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

Jasno je da ako je $a_n = \alpha_n$ za neki n, onda je α racionalan broj.

Naime, tada je

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots + \cfrac{1}{a_n}}}}, \qquad (2)$$

Ovo ćemo kraće zapisivati u obliku $\alpha = [a_0, a_1, \ldots, a_n]$.

Zadatak Dokažite da je $a_n \geq 1$ za sve $n \in \mathbb{N}$. Mora li biti $a_0 \geq 1$?

Pretpostavimo sada da je $a_n \neq \alpha_n$ za sve n.

Definirajmo racionalne brojeve $\frac{p_n}{q_n}$ sa

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

Zadatak Odredite sve p_n/q_n za $\alpha = 17/7$.

Teorem

Brojevi p_n, q_n zadovoljavaju rekurzije

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

Dokaz: Za $n = 2$ tvrdnja se provjerava direktno. Pretpostavimo da je $n > 2$ i da tvrdnja vrijedi za $n - 1$. Definirajmo brojeve p'_j, q'_j sa $\frac{p'_j}{q'_j} = [a_1, a_2, \ldots, a_{j+1}]$. Tada je

$$p'_{n-1} = a_n p'_{n-2} + p'_{n-3}, \quad q'_{n-1} = a_n q'_{n-2} + q'_{n-3}.$$

po pretpostavci indukcije. No,

$$\frac{p_j}{q_j} = a_0 + \frac{1}{[a_1, \ldots, a_j]} = a_0 + \frac{q'_{j-1}}{p'_{j-1}} = \frac{a_0 p'_{j-1} + q'_{j-1}}{p'_{j-1}}.$$

Stoga je $p_j = a_0 p'_{j-1} + q'_{j-1}$, $q_j = p'_{j-1}$.

Prema tome,

$$\begin{aligned} p_n &= a_0(a_n p'_{n-2} + p'_{n-3}) + (a_n q'_{n-2} + q'_{n-3}) \\ &= a_n(a_0 p'_{n-2} + q'_{n-2}) + (a_0 p'_{n-3} + q'_{n-3}) = a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n p'_{n-2} + p'_{n-3} = a_n q_{n-1} + q_{n-2}. \end{aligned}$$

$\square$

Dogovorno uzimamo da je $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$. Lako se provjerava da uz ovaj dogovor Teorem 6 vrijedi za sve $n \geq 0$.

Zadatak Dokažite da je q_n rastući niz i da je $q_n \geq n$ za sve $n \geq 0$.

Teorem

Za sve $n \geq -1$ vrijedi: $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$.

Dokaz: Teorem dokazujemo indukcijom. Za $n = -1$ imamo: $q_{-1}p_{-2} - p_{-1}q_{-2} = 0 \cdot 0 - 1 \cdot 1 = (-1)^{-1}$.

Pretpostavimo da tvrdnja vrijedi za $n-1$. Tada je

$$\begin{aligned} q_n p_{n-1} - p_n q_{n-1} &= (a_n q_{n-1} + q_{n-2})p_{n-1} - (a_n p_{n-1} + p_{n-2})q_{n-1} \\ &= -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = -(-1)^{n-1} = (-1)^n. \end{aligned}$$

$\square$

Korolar

Brojevi p_n i q_n su relativno prosti.

Dokaz: Slijedi jer se 1 može pokazati kao linearna kombinacija od p_n i q_n.

Teorem

1) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots,$

2) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots,$

3) Ako je n paran, a m neparan, onda je $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.

Dokaz: Iz prethodnih Teorema je

$$\begin{aligned}\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} &= \frac{p_{n-2}(a_n q_{n-1} + q_{n-2}) - (a_n p_{n-1} + p_{n-2}) q_{n-2}}{q_n q_{n-2}} \\ &= \frac{a_n (p_{n-2} q_{n-1} - p_{n-1} q_{n-2}) + p_{n-2} q_{n-2} - p_{n-2} q_{n-2}}{q_n q_{n-2}} \\ &= \frac{(-1)^{n-1} a_n}{q_n q_{n-2}}. \qquad (3)\end{aligned}$$

Primijenimo li (3) za n paran, dobivamo $\frac{p_{n-2}}{q_{n-2}} < \frac{p_n}{q_n}$, a za n neparan dobivamo $\frac{p_{n-2}}{q_{n-2}} > \frac{p_n}{q_n}$.

Preostaje dokazati tvrdnju 3). Neka je $n < m$. To možemo pretpostaviti jer je ako je ova tvrdnja zadovoljena onda je zadovoljena i za sve $m \leq n$, pošto $\frac{p_m}{q_m}$ rastu s m, a $\frac{p_n}{q_n}$ padaju s n.

Budući da je $\frac{p_n}{q_n} \leq \frac{p_{m-1}}{q_{m-1}}$, dovoljno je dokazati da je $\frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$.

Zadnja nejednakost je točna jer je, po prethodnom Teoremu, $q_m p_{m-1} - p_m q_{m-1} = (-1)^m = -1 < 0$. $\square$

Teorem

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

Dokaz: Budući da $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_1}{q_1}$, slijedi da $\lim\limits_{\substack{n \to \infty \\ n \text{ paran}}} \frac{p_n}{q_n}$ postoji.

Iz istog razloga postoji i $\lim\limits_{\substack{n \to \infty \\ n \text{ neparan}}} \frac{p_n}{q_n}$.

Ali ova dva limesa su jednaka jer je $\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n-1}q_n}$ i zbog $q_n \geq n$ je $\lim_{n\to\infty} \frac{(-1)^n}{q_{n-1}q_n} = 0$.

Neka je $\vartheta = \lim_{n\to\infty} \frac{p_n}{q_n}$.

Iz definicije brojeva $\alpha_1, \alpha_2, \ldots$ slijedi da je $\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}]$, gdje je $0 < \frac{1}{\alpha_{n+1}} \leq \frac{1}{a_{n+1}}$.

Vidimo da α leži između brojeva $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$. Prema prethodnom Teoremu znači da je $\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$ za n paran i $\frac{p_{n+1}}{q_{n+1}} < \alpha < \frac{p_n}{q_n}$ za n neparan. Dakle, $\alpha = \vartheta$. $\square$

Zadatak

Izračunajte prve četiri konvergente $\frac{p_0}{q_0}$, $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$, $\frac{p_3}{q_3}$ *u razvoju broja* $e = 2.7182818284\cdots$ *u jednostavni verižni razlomak.*

Sada možemo zaključiti da ako je α racionalan, onda je $a_n = \alpha_n$ za neki n.

Zaista, u protivnom bi, zbog toga što α leži između $\frac{p_n}{q_n}$ i $\frac{p_{n+1}}{q_{n+1}}$, imali

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_{n+1}q_n} < \frac{1}{q_n^2} \tag{4}$$

za svaki n.

To bi značilo da postoji beskonačno mnogo racionalnih brojeva $\frac{p}{q}$ takvih da je $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$, što je u suprotnosti s Napomenom.

Definicija

Ako je a_0 cijeli broj, $a_1, \dots, a_n$ prirodni brojevi, te ako je $\alpha = [a_0, a_1, \dots, a_n]$, onda ovaj izraz zovemo razvoj broja α u konačni jednostavni verižni (neprekidni) razlomak; $\frac{p_i}{q_i} = [a_0, \dots, a_i]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent od α, a $\alpha_i = [a_i, a_{i+1}, \dots, a_n]$ je i-ti potpuni kvocijent od α.

Ako je α iracionalan broj, onda uvodimo oznaku $\lim\limits_{n\to\infty}[a_0, a_1, \dots, a_n] = [a_0, a_1, a_2, \dots]$. Ako je $\alpha = [a_0, a_1, a_2, \dots]$, onda ovaj izraz zovemo razvoj od α u (beskonačni) jednostavni verižni razlomak; $\frac{p_i}{q_i} = [a_0, \dots, a_i]$ je i-ta konvergenta od α, a_i je i-ti parcijalni kvocijent, a $\alpha_i = [a_i, a_{i+1}, \dots]$ je i-ti potpuni kvocijent od α.

Neka je α iracionalan broj. Prema formuli (4) svaka konvergenta od α zadovoljava nejednakost $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

Teorem

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

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

Dokaz: Brojevi $\alpha - \frac{p_n}{q_n}$, $\alpha - \frac{p_{n-1}}{q_{n-1}}$ imaju suprotni predznak, pa je

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

(jer je $2ab < a^2 + b^2$ za $a \neq b$, mi uzmemo $a = \frac{1}{q_n}$, $b = \frac{1}{q_{n-1}}$).
Prema tome, vrijedi

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{ili} \quad \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}.$$

$\square$

Teorem (Borel)

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

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

Dokaz: Stavimo $\alpha = [a_0, a_1, \dots]$, $\alpha_i = [a_i, a_{i+1}, \dots]$ i $\beta_i = \frac{q_{i-2}}{q_{i-1}}$ za $i \geq 1$.

Imamo $\alpha = [a_0, a_1, \dots, a_n, \alpha_{n+1}]$, pa je

$$q_n\alpha - p_n = q_n \cdot \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - p_n = \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}}. \qquad (5)$$

Stoga je

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}. \qquad (6)$$

Da bi dovršili dokaz, moramo pokazati da ne postoji prirodan broj n takav da za $i = n-1, n, n+1$ vrijedi

$$\alpha_i + \beta_i \leq \sqrt{5}. \qquad (7)$$

Pretpostavimo da je (7) ispunjeno za $i = n-1, n$. Tada iz

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n},$$

$$\frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = \frac{a_{n-1}q_{n-2} + q_{n-3}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1}$$

slijedi

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}.$$

Stoga je

$$1 = \alpha_n \cdot \frac{1}{\alpha_n} = \left(\sqrt{5} - \frac{1}{\beta_n}\right)\alpha_n \leq \left(\sqrt{5} - \beta_n\right)\left(\sqrt{5} - \frac{1}{\beta_n}\right),$$

$$\Longrightarrow 5 - \sqrt{5}\beta_n - \frac{\sqrt{5}}{\beta_n} + 1 \geq 1.$$

Množenjem s $-\beta_n/\sqrt{5}$ dobivamo $\beta_n^2 - \sqrt{5}\beta_n + 1 \leq 0$. Odavde slijedi da je $\beta_n \in \left[\frac{\sqrt{5}-1}{2}, \frac{\sqrt{5}+1}{2}\right]$, dakle budući da je β_n racionalan, $\beta_n > \frac{\sqrt{5}-1}{2}$.

Ako bi (7) također bilo ispunjeno za $i = n, n+1$, onda bi korištenjem istih argumenata dobili $\beta_{n+1} > \frac{\sqrt{5}-1}{2}$, pa iz

$$q_n = a_n q_{n-1} + q_{n-2} \quad \text{slijedi} \quad a_n = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}},$$

$$1 \leq a_n = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}} = \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} = 1,$$

što je kontradikcija. $\square$