

Teorija brojeva

Filip Najman

9. predavanje

25.5.2023.

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:

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

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

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \left[\frac{2}{Q}, \frac{3}{Q}\right), \dots, \left[\frac{Q-1}{Q}, 1\right).$$

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 $0 \leq r_i < Q$, $i = 1, 2$, $r_1 \neq r_2$ i da vrijedi

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

Možemo pretpostaviti da je $r_1 > r_2$. Stavimo: $q = r_1 - r_2$, $p = s_1 - s_2$. Tada je $1 \leq q < Q$ (jer su i r_1 i r_2 manji od Q) i $|\alpha q - p| \leq \frac{1}{Q}$, 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 $1 \leq q < Q'$ i $|\alpha q - p| \leq \frac{1}{Q'} < \frac{1}{Q}$.

Također zbog $1 \leq q < Q'$ slijedi $1 \leq q \leq \lfloor Q \rfloor$, odnosno $1 \leq q < Q$. □

Korolar

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

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

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 $\frac{p_j}{q_j}$, $j = 1, \dots, n$.

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

Primijenimo sada Dirichletov teorem 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 $|\alpha - \frac{p}{q}| \leq \frac{1}{mq} < \frac{1}{q^2}$.

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

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

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

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

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

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

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

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

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

Teorem

Brojevi p_n, q_n zadovoljavaju rekurzije

$$p_n = a_n p_{n-1} + p_{n-2}, \quad p_0 = a_0, \quad p_1 = a_0 a_1 + 1;$$

$$q_n = a_n q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_1 = a_1.$$

Dokaz: Za $n = 2$ tvrdnja se provjerava direktno. Pretpostavimo da je $n > 2$ i da tvrdnja vrijedi za sve nizove do $(n - 1)$ -tog člana.

Definirajmo brojeve p'_j, q'_j sa $\frac{p'_j}{q'_j} = [a_1, a_2, \dots, a_{j+1}]$. 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,

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

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

Prema tome,

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



Dogovorno uzimamo da je $p_{-2} = 0$, $p_{-1} = 1$, $q_{-2} = 1$, $q_{-1} = 0$.
Lako se provjerava da uz ovaj dogovor Teorem 4 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

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



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

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

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

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

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

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 prvo $n < m$.

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

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

Neka je sada $n > m$. Tada je $\frac{p_{n-1}}{q_{n-1}} \leq \frac{p_m}{q_m}$, pa je dovoljno dokazati da je $\frac{p_n}{q_n} < \frac{p_{n-1}}{q_{n-1}}$ da bi dobili $\frac{p_n}{q_n} < \frac{p_m}{q_m}$.

Zadnja nejednakost je točna jer je, po prethodnom Teoremu, $q_n p_{n-1} - p_n q_{n-1} = -1 \cdot (-1)^n = -1 < 0$, pa slijedi da je $\frac{p_n}{q_n} < \frac{p_{n-1}}{q_{n-1}}$.



Teorem

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

Dokaz: Budući da $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \frac{p_1}{q_1}$, slijedi da $\lim_{\substack{n \rightarrow \infty \\ n \text{ paran}}} \frac{p_n}{q_n}$ postoji.

Iz istog razloga postoji i $\lim_{\substack{n \rightarrow \infty \\ n \text{ neparan}}} \frac{p_n}{q_n}$.

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 $\lim_{n \rightarrow \infty} \frac{(-1)^n}{q_{n-1}q_n} = 0$.

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

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

Iz ovoga i iz definicije konvergenata 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, $\alpha = \vartheta$. □

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 $e = 2.7182818284 \dots$ u jednostavni verižni razlomak.

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

$\lim_{n \rightarrow \infty} [a_0, a_1, \dots, a_n] = [a_0, a_1, a_2, \dots]$. 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 .