6. Diofantske aproksimacije

Motivacija: Vjerojatnosni algoritam za aproksimaciju (Suhorov algoritam)

Neka je $N = p \cdot q$, $p \neq q$ prosti brojevi. Problem je naći p i q.

1. Odaberimo slučajan prirodan broj $a < N$.
2. Izračunamo (a, N) (Euklidov alg.)
3. Ako $(a, N) \neq 1$ gotovi smo.
4. Inače, promatramo red r od a modulo N,
   tj. minimalan $r \in \mathbb{N}$ t.d. $a^r \equiv 1 \ (N)$.
   (kvantni potprogram).
5. Ako je r neparan, idi na korak 1.
6. Ako je $a^{r/2} \equiv -1 \ (N)$ idi na korak 1.
7. Inače $(a^{\frac{r}{2}} + 1, N)$ i $(a^{\frac{r}{2}} - 1, N)$ $\rightsquigarrow$ dobit ćemo faktor od N

$$(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) = a^r - 1 \equiv 0 \ (N)$$

4. korak (kvantni potprogram za traženje reda r)

⋮

$Q = 2^9$ → neka konstanta.

U jednom koraku algoritma "izmjerim" y

takav da je $\frac{y \cdot r}{Q}$ "blizu" nekom (nepoznatom) prirodnom broju c:

$\frac{yr}{Q} \sim c$; tj. razlomci $\frac{y}{Q}$ i $\frac{c}{r}$ su "blizu" jedan drugom.

$\frac{y}{Q}$ — poznato; $\frac{c}{r}$ — nepozn.

Q: Kako na osnovu ove informacije odrediti r ?
(odrediti kandidate za r)

A: Koristeći razvoj u verižni razlomak broja $\frac{y}{Q}$ dobit ćemo kandidate za r.

↑

Diofantske aproksimacije.

Oznake: $\alpha \in \mathbb{R}$; $\lfloor \alpha \rfloor$, $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$, $\|\alpha\|$ = udaljenost broja α do najbližeg cijelog broja

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

Ako je $\alpha = \frac{p}{q}$, onda je $\|r\alpha\| = |r\alpha - c|$ "blizu" nuli.

Pokazat ćemo za općenite α: ako je $\|r\alpha\| < \frac{1}{2r}$ onda je

r nazivnik neke konvergente verižnog razlomka od α

(tj. elemet. jednog rekurzivno definiranog niza).

Teorem 6.1. (Dirichletov teorem) Neka su α i Q realni brojevi i $Q > 1$.

Tada postoje cijeli brojevi p i q t.d. $1 \leq q < Q$

i $\|\alpha q\| = |\alpha q - p| \leq \frac{1}{Q}$.

$\{\|\alpha q\|\}_{q=1,\dots,\lfloor Q \rfloor}$

$\vdots$

$\alpha \cdot q$

Dokaz: Pretp. $Q \in \mathbb{N}$ (slučaj $Q \notin \mathbb{N}$ za D.Z.)

Promotrimo sljedećih $Q+1$ brojeva:

$0, 1, \{\alpha\}, \{2\alpha\}, \dots, \{(Q-1)\alpha\}$. Svi ovi brojevi leže u $[0,1]$. Podijelimo $[0,1]$ na Q dijelova: $[0, \frac{1}{Q}>, [\frac{1}{Q}, \frac{2}{Q}>, \dots, [\frac{Q-1}{Q}, 1]$. Prema Dirichletovom principu postoji barem jedan podinterval koji sadrži barem 2 od gornjih $Q+1$ brojeva. Neka su to brojevi $\{r_1\alpha\}$ i $\{r_2\alpha\}$ (pretp. $r_1 > r_2$). Tada postoji $s_1, s_2 \in \mathbb{Z}$ t.d.

$\{r_1\alpha\} = r_1\alpha - s_1$ i $\{r_2\alpha\} = r_2\alpha - s_2$. Tada je

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

Dakle, za $q = r_1 - r_2$ i $p = s_1 - s_2$ tvrdnja slijedi.

∎

Korolar 6.2. Ako je α iracionalan broj onda postoji
iz mnoge parova p, q, $(p,q)=1$ t.d. je
$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Dokaz: Prema Teoremu 6.1, za $Q>1$ postoji rel. prosti cijeli brojevi
p, q t.d. $\quad (*) \quad \left|\alpha - \frac{p}{q}\right| < \frac{1}{Qq} < \frac{1}{q^2}$ (ako p i q ni Teorem 6.1.
nisu relativno prosti, onda ih skratimo).
Budući da je α iracionalan, to je $\alpha q - p \neq 0$. Pretp. da postoji
konačno mnogo rac. brojeva $\frac{p}{q}$ koji zadovoljavaju $(*)$. Neka su to
brojevi $\frac{p_i}{q_i}$ za $i=1,\dots,n$. Odaberemo $m \in \mathbb{N}$ t.d.
$$\frac{1}{m} < |\alpha q_j - p_j| \quad \forall j.$$ Primijenimo Teorem 6.1.
na $Q=m$ pa dobivamo $\frac{p}{q} \in Q$ koji zadovoljava $(*)$.

i za koji vrijedi

$$0 < |\alpha q - p| \leq \frac{1}{m} \Rightarrow \frac{p}{q} \neq \frac{p_i}{q_i} \quad \forall i = 1 \dots n \quad \Rightarrow\Leftarrow .$$