Dobré aproximace

Pomocí teorie dobrých aproximací popsané v textu se poměrně snadno odvodí následující věta o algoritmu hledání dobrých aproximací reálného čísla:

Věta. *Nechť $\theta \in \mathbb{R}$. Generujme rekurentně celá čísla p_n, q_n, a_n; nejprve položme*

$$\begin{aligned} p_0 &= 1, & q_0 &= 0, \\ p_1 &= [\theta], & q_1 &= 1. \end{aligned}$$

Pak pro libovolné přirozené n pokračujme takto: jestliže $q_n\theta = p_n$, generování končí, jinak položíme

$$a_n = \left[\frac{|q_{n-1}\theta - p_{n-1}|}{|q_n\theta - p_n|} \right]$$

a dále

$$\begin{aligned} p_{n+1} &= a_n p_n + p_{n-1}, \\ q_{n+1} &= a_n q_n + q_{n-1}. \end{aligned}$$

Pak všechny dobré aproximace čísla θ jsou právě čísla $\frac{p_n}{q_n}$ pro $n \geq 1$, je-li $a_1 > 1$, resp. pro $n \geq 2$, je-li $a_1 = 1$. Navíc platí

$$\begin{aligned} (-1)^n(q_n\theta - p_n) &\leq 0, \\ q_{n+1}p_n - q_n p_{n+1} &= (-1)^n. \end{aligned}$$

Pomocí konstrukce dobrých aproximací nyní dokážeme nepatrně slabší variantu užívaného případu Lehmannovy věty pro $r = [\sqrt[3]{N}]$.

Věta. *Nechť N je liché, $N = pq$, kde $p \leq q$ jsou prvočísla. Pak existují celá čísla x, y, k tak, že*

(1) $x^2 - y^2 = 4kN, \quad 1 \leq k \leq [\sqrt[3]{N}];$

(2) $2|k \implies x \equiv 1 \pmod 2; \qquad 2 \nmid k \implies x \equiv k + N \pmod 4;$

(3) $0 \leq x^2 - 4kN < \frac{N}{[\sqrt[3]{N}]}.$

Důkaz. Je-li $p = q$, věta platí pro $x = 2p$, $y = 0$, $k = 1$, neboť

$$N = p^2 \equiv 1 \pmod 4,$$

a tedy $k + N \equiv 2 \equiv 2p \pmod 4$. Nechť dále $p < q$. Sestrojme posloupnost dobrých aproximací $\frac{p_n}{q_n}$ čísla $\theta = \frac{q}{p}$ a zvolme n tak, aby $p_n q_n \le \sqrt[3]{N} < p_{n+1}q_{n+1}$. To lze, protože algoritmus výpočtu dobrých aproximací se zastaví až pro $p_n = q$, $q_n = p$, kdy je přesně dosaženo θ. Protože $\theta > 1$, jsou čísla p_n, p_{n+1}, q_n, q_{n+1} kladná. Položme

$$k = p_n q_n, \qquad x = pp_n + qq_n, \qquad y = pp_n - qq_n.$$

Zřejmě $x^2 - y^2 = 4pp_nqq_n = 4kN$, odkud plyne (1). Jestliže $2|k$, pak je právě jedno z čísel p_n a q_n sudé (vždyť jsou nesoudělná), a protože p a q jsou lichá, je x liché. Je-li naopak k liché, jsou p_n a q_n lichá, odkud

$$q_n p x = q_n p^2 p_n + q q_n^2 p \equiv q_n p_n + qp = k + N \pmod 4$$

a ze sudosti x plyne $q_n p x \equiv x \pmod 4$, celkem tedy (2). Z teorie dobrých aproximací

$$\left|\frac{p_n}{q_n} - \frac{q}{p}\right| < \frac{1}{q_n q_{n+1}},$$

odkud

$$|y| = |pp_n - qq_n| = \left|\frac{p_n}{q_n} - \frac{q}{p}\right| \cdot pq_n < \frac{p}{q_{n+1}}.$$

Dále

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{q}{p}\right| < \frac{1}{q_{n+1}^2},$$

odkud

$$\left|\frac{p_{n+1}}{q} - \frac{q_{n+1}}{p}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{q}{p}\right| \cdot \frac{q_{n+1}}{q} < \frac{1}{qq_{n+1}},$$

jinými slovy

$$\frac{p_{n+1}}{q} - \frac{1}{qq_{n+1}} < \frac{q_{n+1}}{p} < \frac{p_{n+1}}{q} + \frac{1}{qq_{n+1}}.$$

Vynásobením levé nerovnosti číslem $\frac{q_{n+1}}{p}$ dostaneme

$$\frac{q_{n+1}^2}{p^2} > \frac{p_{n+1}q_{n+1}}{pq} - \frac{1}{pq} = \frac{p_{n+1}q_{n+1} - 1}{N}.$$

Ovšem $p_{n+1}q_{n+1} > \sqrt[3]{N} \ge [\sqrt[3]{N}]$, tedy $p_{n+1}q_{n+1} - 1 \ge [\sqrt[3]{N}]$. Dohromady

$$x^2 - 4kN = y^2 < \frac{p^2}{q_{n+1}^2} < \frac{N}{p_{n+1}q_{n+1} - 1} \le \frac{N}{[\sqrt[3]{N}]}$$

a platí i (3).

Poznámka. Odhadneme-li $x + 2\sqrt{kN} \geq 4\sqrt{kN}$ pomocí (3) ve výrazu

$$x - 2\sqrt{kN} = \frac{x^2 - 4kN}{x + 2\sqrt{kN}} < \frac{N}{[\sqrt[3]{N}]} \cdot \frac{1}{4\sqrt{kN}} = \frac{1}{4[\sqrt[3]{N}]} \cdot \sqrt{\frac{N}{k}},$$

dostáváme nepatrně slabší odhad, než je odhad uvedený v Lehmannově větě v textu:

$$x - 2\sqrt{kN} \leq \frac{1}{4([\sqrt[3]{N}] + 1)} \cdot \sqrt{\frac{N}{k}},$$

avšak i námi získaný odhad postačí k odvození udané časové náročnosti Lehmannova algoritmu.