Bohuslav Sivák

Elementárny dôkaz Richterovej vety

In: Petr Benda (editor); Jozef Moravčík (editor); Jan Vyšín (editor); František Zítek (editor): [dokumenty-07] 20 let matematické olympiády v ČSSR. 1951-1971. (Slovak). Praha: Ústřední výbor matematické olympiády, 1971. pp. 45–50.

Persistent URL: http://dml.cz/dmlcz/405319

Bohuš Sivák, Zvolen

ELEMENTÁRNY DÔKAZ RICHERTOVEJ VETY

Medzi najznámejšie hypotézy o prvočíslach patrí Goldbachova hypotéza, podľa ktorej sa každé nepárne číslo $a \geqq 7$ dá písať ako súčet troch prvočísel. Pre nepárne čísla

$$a > 3^{3^{16}}$$

ju dokázal I.M. Vinogradov. O inom vyjadrení hovorí Richertova veta: Každé prirodzené číslo väčšie ako 6 je súčtom navzájom rôznych prvočísel.

Ukážme si elementárny dokaz Richertovej vety. Zaveďme takéto označenia:

N ... množina všetkých prirodzených čísel

P ... množina všetkých prvočísel

P(x) ... množina všetkých prvočísel neprevyšujúcich x ($x > 0$ reálne)

$\pi(x)$ ... počet prvkov množiny P(x)

Z elementárnej teórie čísel je známe, že každé prirodzené číslo $a > 1$ sa dá práve jedným sposobom vyjadriť v tvare

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\cdots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \ldots < p_k$ sú prvočísla a $\alpha_1, \alpha_2, \ldots, \alpha_k$ sú prirodzené čísla. Takýto rozklad sa nazýva kanonickým rozkladom čísla a.

Veta 1

Nech $p \in P$, $n \in N$. Prvočíslo p má v kanonickom rozklade čísla n! exponent

$$\sum_{k=1}^{\infty} \left[\frac{n}{p^k} \right] .$$

(Ak p nedelí a, považujeme za exponent 0.)

Veta 2

Ak x je kladné reálne číslo, je $\prod_{p \in P(x)} p < 4^x$.

Dôkazy týchto viet sú jednoduché, prenechávame ich čitateľovi. Ak s je reálne číslo, platí

$$-1 = 2s - 1 = 2s < [2s] - 2[s] < 2s - 2(s - 1) = 2.$$

teda $[2s] - 2[s]$ sa rovná 0 alebo 1.

Veta 3

Ak rozklad

$$\binom{2n}{n} = \prod_{p \in P(2n)} p^{\alpha_p}$$

je kanonický, $p^{\alpha_p} \leqq 2n.$

Dôkaz: Podľa vety 1

$$\alpha_p = \sum_{k=1}^{\infty} \left\{ \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right\}$$

Položme $m_p = \log_p (2n)$, potom $p^{m_p} \leqq 2n < p^{m_p + 1}$.

Vo vzťahu pre α_p sa každý sčítanec rovná 0 alebo 1, lebo má tvar $[2s] - 2[s]$; pretože pre $k > m_p$ sú všetky sčítance rovné 0, platí $\alpha_p \leqq m_p$,

z čoho

$$p^{\alpha_p} \leqq p^{m_p} \leqq 2n ,$$

čo sme mali dokázať.

O čísle $\binom{2n}{n}$ sa dá dokázať, že $\binom{2n}{n} > \frac{2^{2n}}{2n}$. (1)

Dôkaz sporom. Nech n je prirodzené číslo väčšie ako 1 a medzi n a $2n$ neexistuje prvočíslo. Potom

$$\binom{2n}{n} = \prod_{p \in P(n)} p^{\alpha_p} ,$$

$$\text{kde } \alpha_p = \sum_{k=1}^{\infty} \left\{ \left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right\} .$$

Položme

$$T_1 = \prod_{p \in P(\sqrt{2n})} p^{\alpha_p}, \quad T_2 = \prod_{\substack{p \in P(\frac{2}{3} n) \\ p > \sqrt{2n}}} p^{\alpha_p}, \quad T_3 = \prod_{\substack{p \in P(n) \\ p > \frac{2}{3} n}} p^{\alpha_p},$$

potom

$$\binom{2n}{n} = T_1 \cdot T_2 \cdot T_3 .$$

Podľa vety 3

$$T_1 \leqq (2n)^{\pi(\sqrt{2n})} .$$

Skúmajme T_3:

Nech $\frac{2}{3} n < p \leqq n$, kde $n \geqq 5$. Potom $p^2 > \frac{4}{9} n^2 > 2n$, preto vo vzťahu pre α_p sú všetky sčítance okrem prvého rovné 0.

Preto

$$\alpha_p = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2.1 = 0,$$

takže $T_3 = 1$.

Ak $\sqrt{2n} < p \leqq \frac{2}{3} n$, je $p^2 > 2n$, preto vo vzťahu pre α_p zostane tiež iba prvý sčítanec:

$$\alpha_p = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = \left[2s\right] - 2\left[s\right] \leqq 1,$$

$$T_2 = \prod_{\substack{p \in P(\frac{2n}{3}) \\ p > \sqrt{2n}}} p^{\alpha_p} \leqq \prod_{\substack{p \in P(\frac{2}{3}n) \\ p > \sqrt{2n}}} p \leqq \prod_{p \in P(\frac{2}{3}n)} p$$

a podľa vety 2

$$T_2 \leqq 2^{\frac{4}{3}n} \quad . \qquad (3)$$

Dosadíme (2), (3) a $T_3 = 1$ do 1:

$$\frac{2^{2n}}{2n} < (2n)^{\pi(\sqrt{2n})} \cdot 2^{\frac{4}{3}n} \quad ,$$

$$2^{2n} < (2n)^{\pi(\sqrt{2n}) + 1} \cdot 2^{\frac{4}{3}n} \leqq 2n^{\sqrt{2n}} \cdot 2^{\frac{4}{3}n} \; .$$

Označme $t = 0{,}5 . \log_2 2n$, potom

$2n = 2^{2t}$, $\sqrt{2n} = 2^t$, po dosadení

$$2^{2^{2t}} < (2^{2t})^{2^t} \cdot 2^{\frac{2}{3} \cdot 2^{2t}} \quad ,$$

$$2^{\frac{1}{3} \cdot 2^{2t}} < (2^{2t})^{2^t} \quad ,$$

$$2^{2t} < 6t . 2^t \quad ,$$

$$2^t < 6t .$$

Indukciou sa dá dokazať, že pre všetky prirodzené čísla väčšie ako 5

$$2^k > 6(k + 1).$$

Preto, ak $t \geqq 6$,

$$2^t \geqq 2^{[t]} > 6\,([t] + 1) > 6t,$$

preto $t < 6$,

$$2n = 2^{2t} < 2^{12} \quad ,$$

$$n < 2048.$$

Stačí teda dokázať vetu pre $n < 2048$. Vezmime túto konečnú postupnosť

$h_1 = 2$, $h_2 = 3$, $h_3 = 5$, $h_4 = 7$, $h_5 = 13$, $h_6 = 23$, $h_7 = 43$, $h_8 = 83$,

$h_9 = 163$, $h_{10} = 317$, $h_{11} = 631$, $h_{12} = 1259$, $h_{13} = 2503$.

Všetky jej členy sú prvočísla a $h_{i+1} < 2h_i$. Ak $n < 2048$, padne n do niektorého intervalu (h_i, h_{i+1}), teda

$$h_i \leqq n < h_{i+1} < 2h_i \leqq 2n ,$$

h_{i+1} je prvočíslo z intervalu $(n, 2n)$. Veta je dokázaná.

Veta 5

Každé prirodzené číslo väčšie ako 6 je súčtom navzájom rôznych prvočísel.

Dôkaz: Nech $\{p_j\}$ je rastúca postupnosť všetkých prvočísel, definujme postupnosť $\{s_j\}$ rekurentne:

$$s_o = 13, \quad s_r = s_{r-1} + p_{r+5} .$$

Potom $s_o = p_6$. Ak $s_{r-1} \geqq p_{r+5}$,

$$s_r = s_{r-1} + p_{r+5} \geqq 2p_{r+5}$$

a podla vety 4 $s_r \geqq p_{r+6}$. Indukciou sme dokázali, že

$$s_{r-1} \geqq p_{r+5} . \tag{4}$$

Ak $v > 6$, je $v > p_{v+6} > s_v$. Stačí teda dokázať nasledujúcu vetu:

Pre každé prirodzené číslo r je každé z čísel

$$7, 8, \ldots, 6 + s_{r-1}$$

súčtom navzájom rôznych prvočísel neprevyšujúcich p_{r+4}.

Pre $r = 1$ overíme platnosť vety experimentálne. Nech veta platí pre nejaké prirodzené číslo r. Uvažujme o číslach

$$7,\ 8,\ \dots,\ 6 + s_r\ .$$

Podľa indukčného predpokladu je každé z čísel

$$7,\ 8,\ \dots,\ 6 + s_{r-1}$$

súčtom navzájom rôznych prvočísel. Vezmime prirodzené číslo n, pre ktoré platí

$$6 + s_{r-1} < n \leqq 6 + s_r\ ,\ \text{potom}$$

$$n > 6 + s_{r-1} \geqq 6 + p_{r+5}$$

podľa (4), zároveň

$$n - p_{r+5} \leqq 6 + s_r - p_{r+5} = 6 + s_{r-1}\ ,$$

podľa indukčného předpokladu je $n - p_{r+5}$ súčtom navzájom rôznych prvočísel neprevyšujúcich p_{r+4}, teda ani p_{r+5}, z čoho veta.