Teória čísel

Matej Balog

TEÓRIA ČÍSEL je oblasť matematiky zaoberajúca sa vlastnosťami prirodzených čísel. Množinu prirodzených čísel označujeme N.

Relácia „a **DELÍ** b“ vyjadruje existenciu čísla c takého, že $b = ca$. $(a, b, c \in N)$
Vtedy b je násobok a, b je deliteľné a, a je deliteľ b. Zapisujeme $a|b$.
Pre ľubovoľné $a, b, c, k \in N$ a ľubovoľné $m, n \in Z$ platí:

- $1|a \wedge a|a$
- $a|b \wedge b|a \Rightarrow a = b$
- $a|b \wedge b|c \Rightarrow a|c$
- $a|b \Rightarrow a|kb$
- $a|b \wedge a|c \Rightarrow a|mb \pm nc$
- $ab|c \Rightarrow a|c \wedge b|c$

Na základe počtu deliteľov rozdeľujeme prirodzené čísla do troch skupín:

a) číslo 1
b) **PRVOČÍSLA** majú práve dvoch deliteľov (jednotku a samého seba)
c) **ZLOŽENÉ** čísla majú viac ako dvoch deliteľov

ZÁKLADNÁ VETA ARITMETIKY: Každé prirodzené číslo $n \geq 2$ možno práve jedným spôsobom rozložiť na prvočinitele, t. j. zapísať v tvare $n = {p_1}^{a_1}{p_2}^{a_2} \cdots {p_k}^{a_k}$.

ROZKLAD ČÍSLA NA PRVOČINITELE umožňuje vyčítať mnohé jeho vlastnosti:

- Všetky delitele čísla $n = {p_1}^{a_1}{p_2}^{a_2} \cdots {p_k}^{a_k}$ sú tvaru $m = {p_1}^{b_1}{p_2}^{b_2} \cdots {p_k}^{b_k}$, pričom pre všetky $1 \leq i \leq k$ platí $0 \leq b_i \leq a_i$.
- Číslo $n = {p_1}^{a_1}{p_2}^{a_2} \cdots {p_k}^{a_k}$ má $(a_1 + 1)(a_2 + 2) \cdots (a_k + 1)$ rôznych deliteľov.
- Číslo $n = {p_1}^{a_1}{p_2}^{a_2} \cdots {p_k}^{a_k}$ je e-tou mocninou prirodzeného čísla práve vtedy, keď pre všetky $1 \leq i \leq k$ platí $e|a_i$.

DELITEĽNOSŤ. Najmenší netriviálny (všetky okrem 1 a n) deliteľ čísla n je nanajvýš $\sqrt{n}$. Pre niektoré delitele d existujú jednoduché **KRITÉRIÁ DELITEĽNOSTI**:

- $2|n \Leftrightarrow$ posledná cifra n je párna
- $3|n \Leftrightarrow$ ciferný súčet čísla n je deliteľný 3
- $4|n \Leftrightarrow$ posledné dvojčíslie n je deliteľné 4
- $5|n \Leftrightarrow$ posledná cifra n je 0 alebo 5
- $6|n \Leftrightarrow$ n je deliteľné 2 a 3 zároveň
- $7|n \Leftrightarrow 7|(a + 5b)$, kde $n = 10a + b$
- $8|n \Leftrightarrow$ posledné trojčíslie n je deliteľné 8
- $9|n \Leftrightarrow$ ciferný súčet čísla n je deliteľný 9
- $10|n \Leftrightarrow$ posledná cifra n je 0
- $11|n \Leftrightarrow$ rozdiel súčtu cifier na párnych a nepárnych miestach je deliteľný 11
- $2^k|n \Leftrightarrow$ posledné k-číslie n je deliteľné 2^k

NAJVÄČŠÍ SPOLOČNÝ DELITEĽ čísel a a b je najväčšie d také, že $d|a$ a $d|b$. Píšeme $\mathrm{NSD}(a, b) = d$. Ak $\mathrm{NSD}(a, b) = 1$, tak čísla a a b nazývame vzájomne **NESÚDELITEĽNÉ**.

EUKLIDOV ALGORITMUS je efektívny postup na výpočet NSD(a, b) založený na platnosti vzťahu

$$\text{NSD}(a, b) = \text{NSD}(a, a - b)$$

pre $b > a$ (bez ujmy na všeobecnosti). Postup opakujeme, pokým $a = b$, čo je najväčší spoločný deliteľ pôvodnej dvojice čísel.

NAJMENŠÍ SPOLOČNÝ NÁSOBOK čísel a a b je najmenšie n také, že $a|n$ a $b|n$. Píšeme $nsn(a, b) = n$.

Pre každé $a, b \in N$ existuje NSD(a, b) aj nsn(a, b) a navyše platí:

- NSD$(a, b) \times$ nsn$(a, b) = ab$
- $1 \leq \text{NSD}(a, b) \leq \min(a, b) \leq \max(a, b) \leq \text{nsn}(a, b) \leq ab$

Dôkazy

Prvočísel je nekonečne veľa.

> Sporom: Nech množina prvočísel P je konečná: $P = \{p_1, p_2, \dots, p_k\}$. Číslo $p_1 p_2 \dots p_k + 1$ (súčin všetkých prvočísel zväčšený o jedna) však nie je deliteľné žiadnym z prvočísel a teda samo musí byť prvočíslom.

$2^k|n \;\Leftrightarrow$ posledné k-číslie n je deliteľné 2^k

> Číslo n vieme jednoznačne zapísať v tvare $n = 10^k a + b$ tak, že b je posledné k-číslie n. Potom $n = 2^k(5^k a) + b$ a teda $n \equiv b \pmod{2^k}$.