Prvočísla

Prvočíslo je velmi důležitým pojmem v aritmetice, zvláště proto, že každé celé číslo lze jednoznačně zapsat jako součin prvočísel. Existuje také hodně problémů, týkajících se prvočísel, které je jednoduché vyslovit, ale obtížné vyřešit.

Definice. Každé přirozené číslo $n \geq 2$ má aspoň dva kladné dělitele: 1 a n. Pokud kromě těchto dvou jiné kladné dělitele nemá, nazývá se *prvočíslo*. V opačném případě hovoříme o *složeném čísle*.

Pro nalezení všech prvočísel nepřevyšující dané číslo n existuje jednoduchá metoda zvaná *Eratosthenovo síto* (viz např. [**??**], kapitola 1.5).

Věta. *Přirozené číslo $p \geq 2$ je prvočíslo, právě když platí: pro všechna celá čísla a, b z $p|ab$ plyne $p|a$ nebo $p|b$.*

Věta (Základní věta aritmetiky)**.** *Každé přirozené číslo je možné vyjádřit jako součin prvočísel. Toto vyjádření je jednoznačné, nebereme-li v úvahu pařadí činitelů.*

Prázdný součin je roven číslu jedna ($1 = p_i^0, i \in \mathbb{N}$), každé prvočíslo je pak součin jednoho prvočísla. Pomocí rozkladu na součin prvočísel lze určit i údaje týkající se dělitelů daného čísla.

Věta. *1. Jsou-li $p_1, \ldots, p_k$ navzájem různá prvočísla a $n_1, \ldots, n_k \in \mathbb{N}_0$, je každý kladný dělitel čísla $a = p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$ tvaru $p_1^{m_1} \cdot \cdots \cdot p_k^{m_k}$, kde $m_1, \ldots, m_k \in \mathbb{N}_0$ a $m_1 \leq n_1$, $m_2 \leq n_2$, $\ldots$, $m_k \leq n_k$.*

Číslo a má tedy právě

$$\tau(a) = (n_1 + 1)(n_2 + 1) \cdot \cdots \cdot (n_k + 1)$$

kladných dělitelů, jejichž součet je

$$\sigma(a) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

2. Jsou-li $p_1, \ldots, p_k$ navzájem různá prvočísla a $n_1, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{N}_0$ a označíme-li $r_i = \min\{n_i, m_i\}$, $t_i = \max\{n_i, m_i\}$ pro každé $i = 1, 2, \ldots, k$, platí

$$(p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}, p_1^{m_1} \cdot \cdots \cdot p_k^{m_k}) = p_1^{r_1} \cdot \cdots \cdot p_k^{r_k},$$

$$[p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}, p_1^{m_1} \cdot \cdots \cdot p_k^{m_k}] = p_1^{t_1} \cdot \cdots \cdot p_k^{t_k}.$$

Věta. *Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.*

O rozmístění prvočísel existuje mnoho tvrzení, zde však budeme používat pouze následující tři.

Věta. *(Čebyševova)*

1. *Pro libovolné přirozené číslo $n > 5$ existují mezi čísly n a $2n$ alespoň dvě prvočísla.*

2. *Pro každé číslo $n > 3$ existuje mezi čísly n a $2n - 2$ alespoň jedno prvočíslo.*

Věta. *(Dirichletova) Jsou-li a, m nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel k tak, že $mk + a$ je prvočíslo. Jinými slovy, mezi čísly $1 \cdot m + a, 2 \cdot m + a, 3 \cdot m + a, \ldots$ existuje nekonečně mnoho prvočísel.*

Třetí tvrzení lze využít i při odhadu počtu prvočísel, nepřevyšující zadané číslo x.

Věta. *(o hustotě prvočísel) Nechť $\pi(x)$ udává počet prvočísel menších nebo rovných číslu $x \in \mathbb{R}$. Pak*

$$\pi(x) \sim \frac{x}{\ln x},$$

tj. podíl funkcí $\pi(x)$ a $x/\ln x$ se pro $x \to \infty$ limitně blíží k nule.