Základní pojmy

Než se podíváme na některé nové vlastnosti čísel, je potřeba si zopakovat některé jejich základní vlastnosti.

Definice. Řekneme, že celé číslo a *dělí* celé číslo b (neboli číslo b je *dělitelné* číslem a, též b je *násobek* a), právě když existuje celé číslo c tak, že platí $a \cdot c = b$. Píšeme pak $a|b$.

Často se stane, že pro daná čísla x a y neplatí, že y dělí x; v tom případě píšeme $y \nmid x$. I pro tato čísla lze ale určit takzvaný kvocient a zbytek:

Věta 0.1 (Věta o dělení celých čísel se zbytkem)**.** *Pro libovolně zvolená čísla $a \in \mathbb{Z}$, $m \in \mathbb{N}$ existují jednoznačně určená čísla $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m-1\}$ tak, že $a = qm + r$.*

Každé celé číslo má tedy množinu dělitelů; z definice plyne, že vždy obsahuje alespoň číslo 1. Pro dvě a více různých celých čísel říkáme, že průnik množin jejich dělitelů je množina jejich společných dělitelů. Ta je určitě neprázdná, protože vždy obsahuje alespoň číslo 1.

Definice. Každé celé číslo, dělící současně celá čísla $a_1, a_2, \ldots, a_n$ se nazývá jejich společným dělitelem. Je-li alespoň jedno z čísel $a_1, a_2, \ldots, a_n$ různé od nuly, je počet těchto dělitelů konečný a tedy je jeden z nich největší. Ten se nazývá největším společným dělitelem čísel $a_1, a_2, \ldots, a_n$ a značí se $(a_1, a_2, \ldots, a_n)$.
Každé celé číslo, které je násobkem všech čísel $a_1, a_2, \ldots, a_n$, se nazývá jejich společným násobkem. Nejmenší kladný společný násobek celých nenulových čísel $a_1, a_2, \ldots, a_n$ se nazývá jejich nejmenším společným násobkem a značí se $[a_1, a_2, \ldots, a_n]$.

K nalezení největšího společného dělitele dvou celých čísel slouží *Euklidův algoritmus*. Jelikož se lze snadno přesvědčit, že $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$, je vhodný i k nalezení společného dělitele více čísel.

Věta 0.2 (Euklidův algoritmus)**.** *Nechť a_1, a_2 jsou přirozená čísla. Pro každé $n \geq 3$, pro které $a_{n-1} \neq 0$, označme a_n zbytek po dělení čísla a_{n-2} číslem a_{n-1}. Pak po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = (a_1, a_2)$.*

Věta 0.3. *(Bezoutova) Pro libovolná celá čísla a_1, a_2 existuje jejich největší společný dělitel (a_1, a_2), přitom existují celá čísla k_1, k_2 tak, že $(a_1, a_2) = k_1 a_1 + k_2 a_2$.*

Předchozí věta platí i pro více než dvě čísla, zabývat se tím však nebudeme.
Důležitý význam má však pojem *nesoudělných* čísel.

Definice. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *nesoudělná*, jestliže platí $(a_1, a_2, \ldots, a_n) = 1$. Čísla $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ se nazývají *po dvou nesoudělná*, jestliže pro každé i, j takové, že $1 \leq i < j \leq n$, platí $(a_i, a_j) = 1$.