Vlastnosti celých čísel

Pracujeme s množinou

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

všech přirozených čísel a s množinou

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

všech celých čísel. Řekneme, že číslo $a \in \mathbb{Z}$ **dělí** číslo $b \in \mathbb{Z}$, jestliže existuje číslo $z \in \mathbb{Z}$ takové, že $b = a{\cdot}z$. Pak rovněž říkáme, že číslo a je **dělitel** čísla b, a píšeme $a \,|\, b$. Z této definice pro číslo 0 plyne, že $a \,|\, 0$ pro každé $a \in \mathbb{Z}$ a že $0 \,|\, b$ když a jen když $b = 0$. Základní vlastností je věta o dělení celých čísel se zbytkem:

Věta. Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Pak existují $q, r \in \mathbb{Z}$ splňující

$$a = b{\cdot}q + r, \quad 0 \leq r < b.$$

Přitom čísla q, r jsou určena jednoznačně.

Poznámka. Číslo q se potom nazývá **podíl** a číslo r **zbytek** po dělení čísla a číslem b.

Důkaz. Dokážeme existenci čísel q, r. Uvažme množinu

$$M = \{x \in \mathbb{Z} \,|\; b{\cdot}x \leq a\}.$$

Pak $M \neq \emptyset$, poněvadž $0 \in M$ pokud $a \geq 0$ a $a \in M$ pokud $a < 0$. Dále množina M je zřejmě shora omezená, takže obsahuje největší prvek, který označíme q. Dále položíme $r = a - b{\cdot}q$. Pak ovšem $a = b{\cdot}q + r$ a ukážeme, že platí také $0 \leq r < b$. Nerovnost $0 \leq r$ plyne z toho, že $b{\cdot}q \leq a$. Dále z definice čísla q plyne, že $b{\cdot}(q + 1) > a$, takže $b > a - b{\cdot}q$, čili $b > r$.

Dokážeme jednoznačnost čísel q, r. Nechť $q, q', r, r' \in \mathbb{Z}$ jsou čísla splňující $a = b{\cdot}q + r$, $0 \leq r < b$, $a = b{\cdot}q' + r'$, $0 \leq r' < b$.

Předpokládejme napříkld, že $r \leq r'$. Pak odečtením uvedených rovností dostáváme $0 = b{\cdot}(q - q') + r - r'$, čili $r' - r = b{\cdot}(q - q')$, kde ovšem $0 \leq r' - r < b$. Odtud plyne, že nutně $q - q' = 0$, a tedy také $r' - r = 0$. Takže $q = q'$ a $r = r'$, čímž je ověřena jednoznačnost q, r.

Číslo $c \in \mathbb{Z}$ se nazývá **společný dělitel** čísel $a, b \in \mathbb{Z}$, jestliže $c \,|\, a$ a také $c \,|\, b$. Číslo $d \in \mathbb{Z}$, které je společným dělitelem čísel a, b a které je přitom největším číslem s touto vlastností, se nazývá **největší společný dělitel** čísel a, b. Je-li $a \neq 0$ nebo $b \neq 0$, pak tento největší společný dělitel d čísel a, b existuje, přitom $d \in \mathbb{N}$, a značí se (a, b). Je-li $a = b = 0$, pak největší společný dělitel čísel a, b podle dané definice neexistuje.

Je známa metoda pro nalezení největšího společného dělitele (a, b) dvou čísel $a, b \in \mathbb{N}$, nazývaná **Euklidův algoritmus**. Provádí se postupně následující dělění se zbytkem podle předchozí věty. To znamená, že se hledají čísla $q_0, q_1, \ldots, q_n, q_{n+1} \in \mathbb{N} \cup \{0\}$ a $r_0, r_1, \ldots, r_n \in \mathbb{N}$ taková, že platí:

$$
\begin{aligned}
a &= b{\cdot}q_0 + r_0, \quad 0 \leq r_0 < b, \\
b &= r_0{\cdot}q_1 + r_1, \quad 0 \leq r_1 < r_0, \\
r_0 &= r_1{\cdot}q_2 + r_2, \quad 0 \leq r_2 < r_1, \\
r_1 &= r_2{\cdot}q_3 + r_3, \quad 0 \leq r_3 < r_2, \\
&\ldots \\
r_{n-2} &= r_{n-1}{\cdot}q_n + r_n, \quad 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n{\cdot}q_{n+1}.
\end{aligned}
$$

Poslední dělení je tedy vlastně tvaru $r_{n-1} = r_n{\cdot}q_{n+1} + r_{n+1}$, kde ale $r_{n+1} = 0$. Poněvadž $b > r_0 > r_1 > r_2 > \ldots$, musí tato posloupnost dělení opravdu skončit tímto způsobem, což znamená, že buďto již $r_0 = 0$ pokud $b \,|\, a$, anebo skutečně existuje $n \in \mathbb{N} \cup \{0\}$ takové, že $r_{n+1} = 0$. Jestliže ovšem $r_0 = 0$, položme $n = -1$ a označme ještě $r_{-1} = b$. Pak máme následující fakt:

Věta. Nechť $a, b \in \mathbb{N}$. Pak při označení z předchozího textu platí $(a, b) = r_n$.

Důkaz. Postupujeme-li v předchozím schematu zdola nahoru, postupně krok za krokem odtud plyne $r_n | r_{n-1}$, $r_n | r_{n-2}, \ldots$, $r_n | r_2$, $r_n | r_1$, $r_n | r_0$, $r_n \,|\, b$, $r_n \,|\, a$, takže r_n je společným dělitelem čísel a, b. Nechť naopak $c \in \mathbb{Z}$ je společným dělitelem čísel a, b. Postupujeme-li v předchozím schematu naopak shora dolů, pak z toho, že $c \,|\, a$, $c \,|\, b$, podobným způsobem postupně dostáváme $c | r_0$, $c | r_1$, $c | r_2$, $\ldots$, $c | r_{n-2}$, $c | r_{n-1}$, $c | r_n$. Takže $r_n = c{\cdot}z$ pro jisté $z \in \mathbb{Z}$. Poněvadž $r_n > 0$, plyne odtud $r_n \geq c$. To znamená, že r_n je největším společným dělitelem čísel a, b.

Důsledkem této věty je následující **Bezoutova rovnost**:

Věta. Pro libovolná $a, b \in \mathbb{Z}$ taková, že $a \neq 0$ nebo $b \neq 0$, existují $u, v \in \mathbb{Z}$ taková, že $(a, b) = a{\cdot}u + b{\cdot}v$.

Důkaz. Je-li $a = 0$ pak $b \neq 0$, $(a, b) = |b|$ a tvrzení je zřejmé. Je-li $b = 0$ pak podobně $a \neq 0$, $(a, b) = |a|$ a tvrzení je rovněž zřejmé. Poněvadž dále platí $(a, b) = (|a|, |b|)$, stačí tvrzení dokázat už jen pro $a, b \in \mathbb{N}$. Je-li zde $b \,|\, a$, pak ovšem $(a, b) = b$ a tvrzení je opět zřejmé. Předpokládejme tedy dále navíc, že $b \not| \, a$, a přepišme všechny rovnosti v předchozím schematu Euklidova algoritmu vyjma poslední následovně:

$$
\begin{aligned}
r_0 &= a - b{\cdot}q_0, \\
r_1 &= b - r_0{\cdot}q_1, \\
r_2 &= r_0 - r_1{\cdot}q_2, \\
r_3 &= r_1 - r_2{\cdot}q_3, \\
&\ldots \\
r_n &= r_{n-2} - r_{n-1}{\cdot}q_n.
\end{aligned}
$$

Poněvadž $b \not| \, a$, máme zde přinejmenším první uvedenou rovnost. Označme ještě $r_{-1} = b$ a $r_{-2} = a$. Zpětnou indukcí pro každé

$i = n-1, n-2, \ldots, 1, 0, -1$ ukážeme, že existují $u_i, v_i \in \mathbb{Z}$ taková, že $r_n = r_{i-1}{\cdot}u_i + r_i{\cdot}v_i$. Pro $i = n-1$ to ihned plyne z poslední z výše uvedených rovností. Nechť nyní $i \in \{n-2, \ldots, 1, 0, -1\}$. Pak rovnost pro r_{i+1} v předchozím systému má tvar $r_{i+1} = r_{i-1} - r_i{\cdot}q_{i+1}$. Podle indukčního předpokladu pro $i+1$ máme $r_n = r_i{\cdot}u_{i+1} + r_{i+1}{\cdot}v_{i+1}$ pro jistá $u_{i+1}, v_{i+1} \in \mathbb{Z}$. Dosazením z předchozí rovnosti odtud dostáváme $r_n = r_i{\cdot}u_{i+1} + (r_{i-1} - r_i{\cdot}q_{i+1}){\cdot}v_{i+1} = r_{i-1}{\cdot}v_{i+1} + r_i{\cdot}(u_{i+1} - q_{i+1}{\cdot}v_{i+1})$. Tím je proveden indukční krok a důkaz indukcí je hotov. Pro $i = -1$ odtud plyne dokazované tvrzení, poněvadž $r_{-2} = a$, $r_{-1} = b$ a $r_n = (a, b)$.

Důsledek. Nechť $a, b \in \mathbb{Z}$, $a \neq 0$ nebo $b \neq 0$. Pak číslo $d \in \mathbb{N}$ je největším společným dělitelem čísel a, b, právě když $d \mid a$, $d \mid b$ a je splněna podmínka, že pro každé číslo $e \in \mathbb{N}$ s vlastností, že $e \mid a$, $e \mid b$, platí $e \mid d$.

Poznámka. Uvedené požadavky lze chápat jako alternativní definici pojmu největšího společného dělitele čísel a, b, která pro $a \neq 0$ nebo $b \neq 0$ splývá s definicí předchozí. Navíc tyto podmínky se nezmění, zaměníme-li v nich množinu $\mathbb{N}$ množinou $\mathbb{N} \cup \{0\}$. V tom případě ale obdržíme definici, která určuje největšího společného dělitele i pro $a = b = 0$, a to takovým způsobem, že $(0, 0) = 0$.

Důkaz. Nechť $d \in \mathbb{N}$ je největší společný dělitel čísel a, b a nechť $e \in \mathbb{N}$ je nějakým společným dělitelem čísel a, b. Pak podle předchozí věty existují $u, v \in \mathbb{Z}$ taková že $d = a{\cdot}u + b{\cdot}v$. Dále $e \mid a$, $e \mid b$, takže existují $x, y \in \mathbb{Z}$ taková, že $a = e{\cdot}x$, $b = e{\cdot}y$. Odtud vyplývá, že $d = e{\cdot}x{\cdot}u + e{\cdot}y{\cdot}v$, což ukazuje, že $e \mid d$.

Nechť naopak $d \in \mathbb{N}$ je společný dělitel čísel a, b takový, že pro každý společný dělitel $e \in \mathbb{N}$ těchto čísel platí $e \mid d$. Pak rovněž pro každý společný dělitel $f \in \mathbb{Z}$ těchto čísel platí $f \mid d$, čili existuje $g \in \mathbb{Z}$ takové, že $d = f{\cdot}g$. Odtud ovšem plyne, že $f \leq d$, což ukazuje, že d je největším společným dělitelem čísel a, b.

Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **nesoudělná**, jestliže $(a, b) = 1$.

Důsledek. Jestliže pro čísla $a, b, c \in \mathbb{Z}$ platí $a \mid b{\cdot}c$ a současně $(a, b) = 1$, pak odtud plyne $a \mid c$.

Důkaz. Jestliže $(a, b) = 1$, pak podle předchozí věty existují $u, v \in \mathbb{Z}$ taková, že $1 = a{\cdot}u + b{\cdot}v$. Odtud vynásobením číslem c dostáváme $c = a{\cdot}c{\cdot}u + b{\cdot}c{\cdot}v$. Jestliže tedy $a \mid b{\cdot}c$, plyne odtud, že $a \mid c$.

Přirozené číslo $p \geq 2$ se nazývá **prvočíslo**, jestliže přirozenými čísly, která jsou jeho děliteli, jsou pouze čísla 1 a p.

Věta. Pro každé přirozené číslo $a \geq 2$ platí, že buďto a je prvočíslo, anebo a je možno rozložit na součin prvočísel, přičemž tento rozklad je jediný až na pořadí činitelů.

Důkaz. Fakt, že každé přirozené číslo $a \geq 2$ buď je prvočíslem nebo ho lze rozložit na součin prvočísel, dokážeme indukcí vzhledem k velikosti čísla a. Číslo $a = 2$ je prvočíslo. Nechť tedy $a > 2$. Je-li a prvočíslo, není co dokazovat. Není-li a prvočíslo, pak má přirozeného dělitele b takového, že $1 < b < a$. Tedy lze psát $a = b{\cdot}c$ pro jisté přirozené číslo c takové, že $1 < c < a$. Podle indukčního předpokladu pak pro každé z čísel b, c platí, že jde buď o prvočíslo nebo o číslo, které lze rozložit na součin prvočísel. Pak ovšem také číslo $a = b{\cdot}c$ lze rozložit na součin prvočísel.

Dokážeme jednoznačnost tohoto rozkladu. Předpokládejme, že $a = p_1{\cdot} \ldots {\cdot}p_n = q_1{\cdot} \ldots {\cdot}q_k$, kde $p_1, \ldots, p_n, q_1, \ldots, q_k$ jsou prvočísla. Dokážeme, že v rovnosti $p_1{\cdot} \ldots {\cdot}p_n = q_1{\cdot} \ldots {\cdot}q_k$ stojí na obou stranách stejní činitelé, případně v odlišném pořadí. Postupujeme indukcí vzhledem k počtu n činitelů v prvním součinu. Je-li $n = 1$, je tam jedno prvočíslo, což znamená, že také $q_1{\cdot} \ldots {\cdot}q_k$ je prvočíslo, takže $k = 1$ a $p_1 = q_1$. Nechť tedy $n > 1$. Pak z uvedené rovnosti plyne, že $p_1 | q_1{\cdot} \ldots {\cdot}q_k$. Vícenásobným použitím předchozího důsledku odtud odvodíme, že $p_1|q_i$ platí alespoň pro jeden index $i \in \{1, \ldots, k\}$. Skutečně, pokud $p_1|q_1$, jsme hotovi. Pokud ovšem $k > 1$ a $p_1 \not| q_1$, pak $(p_1, q_1) = 1$, neboť p_1 je prvočíslo. Pak ale z předchozího důsledku plyne, že $p_1|q_2 \cdot \ldots \cdot q_k$. Nyní pokud $p_1|q_2$, jsme opět hotovi. Pokud ale $k > 2$ a $p_1 \not| q_2$, pak $(p_1, q_2) = 1$ a opět z předchozího důsledku plyne, že $p_1|q_3 \cdot \ldots \cdot q_k$. Postupujeme-li takto dále, pak buďto jednou narazíme na $i \in \{1, \ldots, k-1\}$ takové, že $p_1|q_i$, anebo v posledním kroku zjistíme, že $p_1|q_k$. Existuje tedy $i \in \{1, \ldots, k\}$ takové, že $p_1|q_i$. Poněvadž q_i je prvočíslo, znamená to, že $p_1 = q_i$. Vydělíme-li nyní shora vedenou rovnost tímto prvočíslem, dostaneme rovnost $p_2 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_{i-1} \cdot q_{i+1} \cdot \ldots \cdot q_k$. Nyní podle indukčního předpokladu oba tyto součiny obsahují stejné činitele, možná v nestejném pořadí. To potvrzuje dokazovanou jednoznačnost.

Důsledek. Existuje nekonečně mnoho prvočísel.

Důkaz. Připusťme, že existuje pouze konečně mnoho prvočísel $p_1, p_2, \ldots, p_n$. Uvažme číslo $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Podle předchozí věty číslo a je možno rozložit na součin prvočísel. Odtud zejména plyne, že existuje prvočíslo q takové, že $q \mid a$. Ovšem pro každé $i = 1, 2, \ldots, n$ máme $p_i \not| a$, neboť v opačném případě bychom měli $p_i \mid 1$, což není možné. To znamená, že q je prvočíslo takové, že $q \neq p_i$ pro všechna $i = 1, 2, \ldots, n$, což dává spor.