Úvod do teorie čísel

Michal Hroch

Definice. (Dělitelnost) *Řekneme, že $m \in \mathbb{N}$ dělí $n \in \mathbb{N}$, pokud existuje $k \in \mathbb{N}$, že $n = km$. Značíme $m|n$.*

Lemma. (Vlastnosti dělitelnosti)
(1) Pro všechna $n \in \mathbb{N}$ platí $1|n$ a $n|n$.
(2) Pokud $k|m$ a $m|n$ pak $k|n$.
(3) Pokud s dělí dvě z čísel rovnosti $n = m + k$, pak dělí i třetí z těchto čísel.

Definice. (prvočíslo) *Číslo $p \in \mathbb{N}$ nazveme prvočíslo, právě když pro každá $m, n \in \mathbb{N}$ platí, že pokud $p|mn$, pak $p|m$ nebo $p|n$.*

Definice. (Největší společný dělitel)
(1) Pro trojici čísel $d, n, m \in \mathbb{N}$ řekneme, že d je společný dělitel n a m, pokud $d|n$ a zároveň $d|m$.
(2) Číslo d je největší společný dělitel m a n ($d = \mathrm{NSD}(m, n)$), pokud navíc platí, že kdykoli k je společný dělitel n a m, pak $k|d$.

Tvrzení. (o dělení se zbytkem) Pro přirozené číslo m a nezáporné celé n existují nezáporná celá čísla k a r taková, že $n = km + r$ a přitom $r < m$.

Lemma. (Eukleidův algoritmus) Mějme dvě čísla $m, n \in \mathbb{N}$ a hledejme největšího společného dělitele:
1. krok: Vydělíme n číslem m se zbytkem r_1, tedy $n = k_1 m + r_1$, kde $k_1, r_1 \in \mathbb{N} \cup \{0\}$ a $r_1 < m$. Je-li $r_1 = 0$, pak $m|n$, m=NSD(n, m) a jsme hotovi. Pokud $r_1 \neq 0$, pokračujeme dál.
2. krok: Podle lemmatu má dvojice n, m stejné společné dělitele jako dvojice m, r_1. Přejděme k číslům m a r_1. Vydělíme m číslem r_1 se zbytkem r_2, tedy $m = k_2 r_1 + r_2$, kde $k_2, r_2 \in \mathbb{N} \cup 0$ a $r_2 < r_1$. Jeli $r_2 = 0$, pak $r_1|m$, $r_1 = \mathrm{NSD}(m, r_1) = \mathrm{NSD}(n, m)$ a jsme hotovi. Pokud $r_2 \neq 0$, pokračujeme dál.

...

$i$tý krok: Vydělíme r_{i-2} číslem r_{i-1} se zbytkem r_i , tedy $r_{i-2} = k_i r_{i-1} + r_i$, kde $k_i, r_i \in N \cup 0$ a $r_i < r_{i-1}$. Je-li $r_i = 0$, pak $r_{i-1}|r_{i-2}$, $r_{i-1} = \mathrm{NSD}(r_{i-2}, r_{i-1}) = \mathrm{NSD}(r_{i-3}, r_{i-2}) = \cdots = \mathrm{NSD}(m, r_1) = \mathrm{NSD}(n, m)$ a jsme hotovi. Pokud $r_i \neq 0$ pokračujeme dál.

...

Posloupnost zbytků $r_1, r_2, r_3, \ldots$ je ostře klesající, $r_1 > r_2 > r_3, \ldots$, a proto po konečném počtu kroků dojdeme ke zbytku $r_i = 0$ a algoritmus vždy skončí nalezením

největšího společného dělitele $r_{i-1} = \mathrm{NSD}(n, m)$.

Tvrzení. (Jednoznačnost prvočíselného rozkladu) Dané číslo $n \in \mathbb{N}$ lze rozložit právě jedním způsobem na součin prvočísel a lze psát $n = p_1^{k_1} \cdots p_r^{k_r}$.

Definice. (nejmenší společný násobek)
(1) Pro trojici čísel $k, n, m, \in \mathbb{N}$ řekneme, že k je společný násobek n a m, pokud $n|k$ a zároveň $m|k$.
(2) Číslo k je nejmenší společný násobek n a m, $k = \mathrm{NSN}(n, m)$, pokud navíc platí, že kdykoli l je společný násobek n a m, pak $k|l$.

Tvrzení. Pro $n = p_1^{k_1} \cdots p_r^{k_r}$ a $m = p_1^{l_1} \cdots p_r^{l_r}$ je
(1) $\mathrm{NSD}(n, m) = p_1^{\min(k_1,l_1)} p_2^{\min(k_2,l_2)} \cdots p_r^{\min(k_r,l_r)}$,
(2) $\mathrm{NSN}(n, m) = p_1^{\max(k_1,l_1)} p_2^{\max(k_2,l_2)} \cdots p_r^{\max(k_r,l_r)}$.

Definice. (soudělnost) *Je-li $\mathrm{NSD}(n, m) = 1$, čísla n a m se nazývají nesoudělná. V opačném případě říkáme, že n a m jsou soudělná.*

Lemma. *Jsou-li n a m nesoudělná a také n a l nesoudělná, pak jsou i n a ml nesoudělná. Jsou-li n a m nesoudělná a obě dělí číslo l, pak $nm|l$.*

Definice. *Řekneme, že a je kongruentní s b modulo m, píšeme $a \equiv b \pmod{m}$, právě tehdy, když $n|a - b$.*

Věta. (Čínská věta o zbytcích) *Mějme po dvou nesoudělná čísla $n_1, \ldots, n_k \in \mathbb{N}$ a nezáporná celá čísla $r_1, \ldots, r_k \in \mathbb{N} \cup \{0\}$ taková, že $r_1 < n_1, \ldots, r_k < n_k$. Pak soustava rovnic*

$$\begin{aligned} x &\equiv r_1 \pmod{n_1} \\ x &\equiv r_2 \pmod{n_2} \\ &\vdots \\ x &\equiv r_k \pmod{n_k} \end{aligned}$$

má vždy nezáporné řešení $x \in \mathbb{N} \cup \{0\}$. Existuje jediné nezáporné řešení $x < n_1 \cdots n_k$.

Definice. (Eulerova funkce) *Zobrazení, které přirozenému číslu přiřazuje počet menších nesoudělných čísel, se nazývá Eulerova funkce a značí se φ. Tedy $\varphi : N \to N$, $\varphi(n) = |\{m \in \mathbb{N}; m \leq n \text{ a } \mathrm{NSD}(n, m) = 1\}|$.*

Tvrzení. Platí $\varphi(1) = 1$. Je-li p^k mocnina prvočísla, $k > 0$, pak $\varphi(p^k) = p^k - p^{k-1}$. Jsou-li n a m nesoudělná, pak $\varphi(nm) = \varphi(n)\varphi(m)$.

Důsledek. Je-li $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ rozklad čísla n, kde $p_1, \ldots, p_r$ jsou po dvou různá prvočísla a $k_1, \ldots, k_r > 0$, pak $\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-2}) \cdots (p_r^{k_r} - p_r^{k_r-1})$.

Tvrzení. (Malá Fermatova věta) Je-li p prvočíslo a $x \in Z$ pak $x^p \equiv x \pmod{p}$. Jsou-li navíc p, x nesoudělná, pak $x^{p-1} \equiv 1 \pmod{p}$.

Věta. (Eulerova) *Nechť a, m jsou nesoudělná přirozená čísla. Pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$