

DMA Přednáška – Dělitelnost

Definice.

Nechť $a, b \in \mathbb{Z}$. Řekneme, že a **dělí** b , značeno $a \mid b$, jestliže existuje $k \in \mathbb{Z}$ takové, že $b = k \cdot a$.
V takovém případě říkáme, že a je **faktor** b a že b je **násobek** a . Také říkáme, že b je **dělitelné** a .

Fakt.

Pro každé $a \in \mathbb{Z}$ platí $1 \mid a$, $a \mid a$ a $a \mid 0$.

Věta.

Nechť $a, b, c \in \mathbb{Z}$.

- (i) Jestliže $a \mid b$ a $b \mid c$, pak $a \mid c$.
- (ii) $a \mid b$ právě tehdy, když $|a| \mid |b|$.
- (iii) Jestliže $a \mid b$ a $b \neq 0$, tak $|a| \leq |b|$.

Věta.

Nechť $a, b \in \mathbb{N}$. Jestliže $a \mid b$ a $b \mid a$, pak $a = b$.

Definice.

Nechť $a \in \mathbb{N}$, $a \geq 2$.

Řekneme, že je to **prvočíslo (prime)**, jestliže jediná přirozená čísla, která a dělí, jsou 1 a a .
Řekneme, že a je **složené číslo**, jestliže to není prvočíslo.

Definice.

Nechť $a, b \in \mathbb{Z}$.

Číslo $d \in \mathbb{N}$ je **společný dělitel** čísel a, b , jestliže $d \mid a$ a $d \mid b$.

Číslo $d \in \mathbb{N}$ je **společný násobek** čísel a, b , jestliže $a \mid d$ a $b \mid d$.

Definice.

Nechť $a, b \in \mathbb{Z}$.

Definujeme jejich **největší společný dělitel**, značeno $\gcd(a, b)$, jako největší prvek množiny jejich společných dělitelů, pokud je alespoň jedno z a, b nenulové. Jinak definujeme $\gcd(0, 0) = 0$.

Definujeme jejich **nejmenší společný násobek**, značeno $\text{lcm}(a, b)$, jako nejmenší prvek množiny jejich společných násobků, pokud jsou a, b obě nenulové. Jinak definujeme $\text{lcm}(a, 0) = \text{lcm}(0, b) = 0$.

Definice.

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

Fakt.

Nechť p je prvočíslo. Pak pro libovolné $a \in \mathbb{Z}$ platí, že buď je s p nesoudělné, nebo p dělí a .

Fakt.

Nechť $a \in \mathbb{N}$. Pak $\gcd(a, 0) = a$, $\text{lcm}(a, 0) = 0$ a $\gcd(a, a) = \text{lcm}(a, a) = a$.

Fakt.

Nechť $a, b \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(|a|, |b|)$ a $\text{lcm}(a, b) = \text{lcm}(|a|, |b|)$.

Věta.

Nechť $a, b \in \mathbb{Z}$. Pak $\text{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$.

Definice.

Nechť $a, d \in \mathbb{Z}$, $d \neq 0$.

Zbytek při dělení čísla a číslem d říkáme číslu $r \in \mathbb{N}_0$ takovému, že $a = qd + r$ a $0 \leq r < |d|$.

Značíme jej $r = a \bmod d$, čteno a **modulo** b .

Číslu q říkáme **částečný podíl**.

Věta. (o dělení se zbytkem)

Nechť $a, d \in \mathbb{Z}$, $d \neq 0$. Pak existují $q \in \mathbb{Z}$ a $r \in \mathbb{N}_0$ takové, že $a = qd + r$ a $0 \leq r < |d|$.

Tato čísla q a r jsou jednoznačně určena.

Fakt.

Nechť $a, b \in \mathbb{Z}$, $a \neq 0$. Pak $a \mid b$ právě tehdy, když $b \bmod |a| = 0$, tedy zbytek po dělení b číslem $|a|$ je 0.

Lemma.

Nechť $a > b \in \mathbb{N}$, nechť $q, r \in \mathbb{N}_0$ splňují $a = qb + r$. Pak platí následující:

- (i) $d \in \mathbb{N}$ je společný dělitel a, b právě tehdy, když je to společný dělitel b, r .
- (ii) $\gcd(a, b) = \gcd(b, r)$.

Euklidův algoritmus pro nalezení $\gcd(a, b)$ pro $a > b \in \mathbb{N}$.

Verze 1.

Iniciace: $r_0 := a, r_1 := b, k := 0$.

Krok: $k := k + 1, r_{k+1} = r_{k-1} \bmod r_k$

Opakovat dokud nenastane $r_{k+1} = 0$.

Pak $\gcd(a, b) = r_k$.

nebo

Verze 2.

procedure $\gcd(a, b: \text{integer})$

repeat

$r := a \bmod b;$

$a := b; b := r;$

until $b = 0;$

output: $a;$

Věta. (Bezoutova věta/rovnost)

Nechť $a, b \in \mathbb{Z}$. Pak existují $A, B \in \mathbb{Z}$ takové, že $\gcd(a, b) = Aa + Bb$.

Rozšířený Euklidův algoritmus pro nalezení $\gcd(a, b) = Aa + Bb$ pro $a > b \in \mathbb{N}$.

Verze 1.

Inicializace: $r_0 := a, r_1 := b, k := 0,$

$A_0 := 1, A_1 := 0, B_0 := 0, B_1 := 1.$

Krok: $k := k + 1, q_k := \left\lfloor \frac{r_{k-1}}{r_k} \right\rfloor,$

$r_{k+1} := r_{k-1} - q_k r_k,$

$A_{k+1} := A_{k-1} - q_k A_k,$

$B_{k+1} := B_{k-1} - q_k B_k.$

Opakovat dokud nenastane $r_{k+1} = 0$.

Pak $\gcd(a, b) = r_k = A_k a + B_k b$.

nebo

Verze 2.

procedure $\gcd\text{-Bezout}(a, b: \text{integer})$

$A_0 := 1; A_1 := 0; B_0 := 0; B_1 := 1;$

repeat

$q_k := \left\lfloor \frac{a}{b} \right\rfloor;$

$r := a - q_k b;$

$a := b; b := r;$

$r_a := A_0 - q_k A_1;$

$r_b := B_0 - q_k B_1;$

$a := b; b := r;$

$A_0 := A_1; A_1 := r_a;$

$B_0 := B_1; B_1 := r_b;$

until $b = 0;$

output: $a, A_0, B_0;$

Lemma. (Euklidovo lemma)

Nechť $a, b, d \in \mathbb{Z}$.

Jestliže $d \mid (ab)$ a $\gcd(d, a) = 1$, pak $d \mid b$.

Prvočísla v první stovce:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Lemma.

Nechť $a_1, \dots, a_m \in \mathbb{N}$ a p je prvočíslo.

Jestliže $p \mid (a_1 a_2 \cdots a_m)$, pak existuje i takové, že $p \mid a_i$.

Lemma.

Pro každé $a \in \mathbb{N}$, $a \geq 2$ existuje prvočíslo, které jej dělí.

Věta. (Fundamentální věta aritmetiky, prvočíselný rozklad)

Nechť $n \in \mathbb{N}$. Pak existují prvočísla p_1, p_2, \dots, p_m a exponenty

$k_1, k_2, \dots, k_m \in \mathbb{N}_0$ takové, že

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} = \prod_{i=1}^m p_i^{k_i}.$$

Jestliže přidáme podmínky $p_1 < p_2 < \dots < p_m$ a $k_i > 0$, tak je tato dekompozice jednoznačně určena.