

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 $b = a \cdot k$. V takovém případě říkáme, že a je **dělitel** b , popřípadě **faktor** b , a že b je **násobek** a . Také říkáme, že b je **dělitelné** číslem a .

Fakt.

Pro každé $a \in \mathbb{Z}$ platí $a \mid a$, $1 \mid a$ 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**, 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. Pro libovolné $a \in \mathbb{Z}$ platí, že buď je p s a nesoudělné, nebo p dělí a .

Fakt.

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

Věta. (o dělení se zbytkem)

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

Tato čísla q a r jsou jednoznačně určena.

Definice.

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

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

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

Číslu q pak říkáme **částečný podíl**.

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 $a, b \in \mathbb{Z}$, nechť $r \in \mathbb{Z}$ splňuje $r = a - qb$ pro nějaké $q \in \mathbb{Z}$. Pak $\gcd(a, b) = \gcd(b, r)$.

(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 $a, b \in \mathbb{Z}$.

Verze 1.

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

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

Dokud platí $r_{k+1} \neq 0$, opakovat kroky:

$k := k + 1,$

volba q_k aby $r_{k-1} - q_k r_k$ optimální,

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

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

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

Pokud $r_k < 0$, změnit znaménka u $r_k, A_k, B_k.$

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

Verze 2.

procedure *gcd-Bezout* (a, b : integer)

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

while $b \neq 0$ **do**

fix q **to get** $a - q \cdot b$ **optimal**

$r := a - qb;$

$r_a := A_0 - qA_1;$

$r_b := B_0 - qB_1;$

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

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

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

If $a < 0$ **do** $a := -a, A_0 := -A_0, B_0 := -B_0;$

output: $a, A_0, B_0;$