Teorie čísel 1. přednáška

Dělitelnost na množině celých čísel

Motivace: Dělí brojka sedmičku? Dělí brojka šestku?

Def (a dělí b) Nechť $a, b \in \mathbb{Z}$. Říkáme, že číslo a dělí číslo b (a je dělitelem čísla b, b je dělitelné číslem a) právě tehdy, když

$$\exists k \in \mathbb{Z} : \quad b = k \cdot a$$

Značíme $a|b$.

Př 1.) $6 = 2 \cdot 3 \Rightarrow 3|6$

2.) $7 = \frac{7}{2} \cdot 3 \Rightarrow 3 \nmid 7$ ($\frac{7}{2} \notin \mathbb{Z}$)

Základní vlastnosti dělitelnosti:

1.) $\forall a \in \mathbb{Z}: \; a|a$

Důkaz: $a = \underbrace{1}_{\in\mathbb{Z}} \cdot a \Rightarrow a|a$ □

2.) $\forall a, b, c \in \mathbb{Z}: (a|b \wedge b|c) \Rightarrow a|c$

Důkaz: $\left.\begin{array}{l} a|b \Rightarrow \exists k_1 \in \mathbb{Z}: b = k_1 a \\ b|c \Rightarrow \exists k_2 \in \mathbb{Z}: c = k_2 b \end{array}\right\} \Rightarrow c = \underbrace{k_2 k_1}_{=k \in \mathbb{Z}} a \Rightarrow a|c$ □

3.) $\forall d, a, x \in \mathbb{Z}: \; d|x \Rightarrow d|ax$

Důkaz: $d|x \Rightarrow x = k_1 d \Rightarrow ax = \underbrace{k_1 a}_{=k} d = \underbrace{k}_{\in\mathbb{Z}} \cdot d \Rightarrow d|ax$ □

4.) $\forall d, x, y \in \mathbb{Z}: (d|x \wedge d|y) \Rightarrow d|(x+y)$

Důkaz: $\left.\begin{array}{l} d|x \Rightarrow x = k_1 d \\ d|y \Rightarrow y = k_2 d \end{array}\right\} \Rightarrow x+y = k_1 d + k_2 d = \underbrace{(k_1+k_2)}_{=k} \cdot d = \underbrace{k}_{\in\mathbb{Z}} \cdot d \Rightarrow d|x+y$ □

5.) $\forall d, a, b, x, y \in \mathbb{Z}: (d|x \wedge d|y) \Rightarrow d|ax+by$

Důkaz: $\left.\begin{array}{l} d|x \Rightarrow d|ax \; (\text{bod 3.}) \\ d|y \Rightarrow d|by \; (\text{bod 3.}) \end{array}\right\} \Rightarrow d|ax+by \; (\text{bod 4.})$ □

6.) $\forall a,b \in \mathbb{Z}-\{0\}$: $a|b \Rightarrow |a| \leq |b|$

Důkaz: $a|b \Rightarrow \exists k \in \mathbb{Z}: b = k \cdot a$ ($k \neq 0$, protože $b \in \mathbb{Z}-\{0\}$) $\Rightarrow$

$\Rightarrow |b| = |k| \cdot |a|$ (protože $k \neq 0 \Rightarrow |k| \geq 1$) $\Rightarrow$

$\Rightarrow \underbrace{|b| = |k|\,|a| \geq 1 \cdot |a| = |a|}_{|k| \geq |a|}$

7.) $\forall a,b \in \mathbb{Z}$: $(a|b \wedge b|a) \Leftrightarrow |a| = |b|$

Důkaz: I. Nejprve dokážeme hravzení $\forall a,b \in \mathbb{Z}-\{0\}$

$\boxed{a|b \wedge b|a} \Rightarrow \left.\begin{array}{l} a|b \Rightarrow |a| \leq |b| \\ b|a \Rightarrow |b| \leq |a| \end{array}\right\} \Rightarrow \boxed{|a| = |b|}$

$\boxed{|a| = |b|} \Rightarrow a = \begin{cases} b \\ -b \end{cases}$ tzn.: $a = 1 \cdot b$ nebo $a = -1 \cdot b$ $\Rightarrow b|a$

a naopak: tzn.: $b = 1 \cdot a$ nebo $b = -1 \cdot a$ $\Rightarrow a|b$ $\Big\} \boxed{b|a \wedge a|b}$

II. Uvažujme případ, kdy $a = 0 \vee b = 0$

$\boxed{a|b \wedge b|a} \Rightarrow \begin{array}{l} b = k_1 \cdot a \\ a = k_2 \cdot b \end{array} \Rightarrow (b = 0 \text{ nebo } a = 0) \xrightarrow{b = k_1} \Rightarrow a = b = 0 \Rightarrow \boxed{|a| = |b|} = 0$

$a = 0 \Downarrow \qquad b = 0 \Downarrow$

$\boxed{|a| = |b|} \Rightarrow |a| = |b| = 0 \Rightarrow (a = 0 \wedge b = 0) \Rightarrow \boxed{a|b \wedge b|a}$

Největší společný dělitel

Def. (gcd(a,b)): Největším společným dělitelem čísel $a, b \in \mathbb{Z}$ nazveme číslo $d \in \mathbb{Z}$ splňující:

1.) $d \geq 0$

2.) $d \mid a \wedge d \mid b$ (d je společným dělitelem čísel a a b)

3.) $d^* \mid a \wedge d^* \mid b \Rightarrow d^* \mid d$

Značíme $d = \gcd(a, b)$

Př. Nalezněte největšího společného dělitele čísel a a b.

1.) $a = 12, \; b = 18$

dělitelé a : $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

dělitelé b : $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

společní dělitelé : $\pm 1, \pm 2, \pm 3, \pm 6$

Všichni společní dělitelé dělí čísla $\pm 6 \Rightarrow \underline{d = 6 \geq 0}$

2.) $a = 0, \; b = z \in \mathbb{Z}$

dělitelé a : Všechna celá čísla
dělitelé $b \in D(b)$
$\Rightarrow d \in \mathbb{Z} \cap D(b) = D(b)$

Všichni společní dělitelé dělí čísl $\pm b \Rightarrow \underline{\gcd(0, b) = |b|}$

3.) $a = 0, \; b = 0$

a i b jsou dělitelná všemi celými čísly. ale pouze $d = 0$ je dělitelné všemi ostatními děliteli a $0 \geq 0 \Rightarrow \underline{d = 0}$

(Nebo to plyne ze 2.)

Věta: Nechť $a, b \in \mathbb{Z}$; $a > 0$. Potom existují čísla $q, r \in \mathbb{Z}$ takové, že:

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

čísla q a r jsou pro daná a, b určena jednoznačně.

Důkaz: Označme $S = \{ b - xa \mid x \in \mathbb{Z} \wedge b - xa \geq 0 \}$

Množina S má jistě nejmenší prvek $\min S = r \geq 0$.

$\Rightarrow \quad \exists\, q \in \mathbb{Z} : \quad b - qa = r$

Dokážeme, že $r < a$. (sporem)

Předpokládejme, že $r \geq a$. Potom

$$r > r - a \geq 0 \qquad / r = b - qa$$

$$r > b - qa - a \geq 0$$

$$r > \underbrace{b - \underbrace{(q+1)}_{\in \mathbb{Z}} a}_{\in S} \geq 0 \qquad \Rightarrow \text{Spor s minimalitou } r!$$

Dokážeme jednoznačnost. Předpokládejme, že

$$b = q_1 a + r_1 = q_2 a + r_2 \quad , \text{kde} \quad 0 \leq r_1, r_2 < a, \quad q_1, q_2 \in \mathbb{Z}$$

$$a(q_1 - q_2) = r_2 - r_1 \qquad (*)$$

$$a \mid r_2 - r_1 \Rightarrow r_2 - r_1 \text{ je násobkem } a$$

ale $\left.\begin{array}{l} 0 \leq r_2 < a \\ -a < -r_1 \leq 0 \end{array}\right\} \Rightarrow -a < r_2 - r_1 < a \Rightarrow$ jediný násobek a, který leží mezi $-a$ a a je 0

$\Rightarrow r_2 - r_1 = 0$ a $(*)$ a $(a > 0)$ pak plyne $q_1 - q_2 = 0$.

□

Věta: Nechť $a, b \in \mathbb{N}$. $M(a,b) = \{ax+by \mid x,y \in \mathbb{Z}\} \cap \mathbb{N}$. Potom:

$$\min M(a,b) = \gcd(a,b)$$

Důkaz: $\min M(a,b)$ jistě existuje, neboť $M(a,b) \subseteq \mathbb{N}$. Označme $d = \min M(a,b)$. Potom platí:

1.) $d \geq 0$ Neboť $d \in M(a,b) \subseteq \mathbb{N}$.

2.) Pro libovolný prvek $ax+by \in M(a,b)$ existují $q \in \mathbb{Z}$ a $0 \leq r < d$:

$ax+by = qd + r$ | $d = ax_0 + by_0$ ($x_0, y_0 \in \mathbb{Z}$), protože $d \in M(a,b)$

$ax+by = qx_0a + qy_0b + r$

$r = (x-qx_0)a + (y-qy_0)b \Rightarrow r \in M(a,b) \Rightarrow$ spor! s minimalitou d

nebo:

$r = 0$

$\Rightarrow r = 0 \Rightarrow$

$ax+by = q \cdot d + 0$ pro libovolné $ax+by \in M(a,b)$

$\Rightarrow$ zvolme $y=0, x=1 \Rightarrow a = q \cdot d \Rightarrow d \mid a$

zvolme $x=0, y=1 \Rightarrow b = q \cdot d \Rightarrow d \mid b$

3.) Předpokládejme, že $d^* \mid a \wedge d^* \mid b \Rightarrow$

$$d = ax_0 + by_0 = k_1 d^* x_0 + k_2 d^* y_0 = d^*(k_1x_0 + k_2y_0)$$

$\Rightarrow d^* \mid d$

$\Rightarrow$ Z 1.), 2) a 3.) plyne, že $d = \gcd(a,b)$.

Důsledek: Nechť $a, b \in \mathbb{N}$. Potom $\gcd(a,b)$ existuje

Lema 1: Nechť $a, b \in \mathbb{Z}$. Potom $a|b \Leftrightarrow a|-b$

Důkaz: $a|b \Rightarrow \exists k \in \mathbb{Z} : b = k \cdot a \Rightarrow -b = -k \cdot a \Rightarrow a|-b$

$a|-b \Rightarrow a|b$ (plyne z předchozího)

Lema 2: Nechť $a, b \in \mathbb{N}$. Potom $\gcd(-a, b) = \gcd(a, b)$.

Důkaz: $\gcd(a,b)$ existuje. Označme jej d. $\Rightarrow$

1.) $d \geq 0$
2.) $d|a \wedge d|b$
3.) $d^*|a \wedge d^*|b \Rightarrow d^*|d$

$\Rightarrow$

1.) $d \geq 0$
2.) $d|-a \wedge d|b$ (Lema 1)
3.) $(d^*|-a \wedge d^*|b) \Rightarrow (d^*|a \wedge d^*|b) \Rightarrow d^*|d$

$\Rightarrow d = \gcd(-a, b)$

Lema 3: Nechť $a, b \in \mathbb{N}$. Potom $\gcd(a, -b) = \gcd(a, b)$

Důkaz: $\gcd(a,b) \overset{\text{2. def.}}{=} \gcd(b,a) \overset{\text{Lema 2}}{=} \gcd(-b,a) \overset{\text{2 def.}}{=} \gcd(a,-b)$.

Lema 4: Nechť $a, b \in \mathbb{N}$. Potom $\gcd(-a, -b) = \gcd(a, b)$

Důkaz: $\gcd(a,b) \overset{\text{Lema 2}}{=} \gcd(-a,b) \overset{\text{Lema 3.}}{=} \gcd(-a,-b)$

Lema 5. Nechť $a, b \in \mathbb{Z}$. Potom $\gcd(a,b) = \gcd(|a|, |b|)$.

a) $a = 0 \Rightarrow \gcd(a,b) = \gcd(0,b) = |b| = \gcd(\overset{|a|}{0}, |b|)$

(Plyne přímo z definice - viz dříve - příklad)

b) $b = 0 \Rightarrow \gcd(a,b) = \gcd(a,0) = |a| = \gcd(|a|, \overset{|b|}{0})$

c) $a, b \in \mathbb{Z} - \{0\} \Rightarrow \gcd(|a|, |b|)$ existuje a z Lema 2 - Lema 3 :

$$\gcd(a,b) = \gcd(\pm|a|, \pm|b|) = \gcd(|a|, |b|)$$

□

Věta (O existenci a jednoznačnosti $\gcd(a,b)$):

Nechť $a, b \in \mathbb{Z}$. Potom $\gcd(a,b)$ existuje a je určen jednoznačně.

Důkaz: Existence $\gcd(a,b)$ plyne z Lemma 5. Dokážeme jednoznačnost. Předpokládejme, že $d_1 = \gcd(a,b) \wedge d_2 = \gcd(a,b)$.

$$d_1 = \gcd(a,b) \Rightarrow (d_1 \mid a \wedge d_1 \mid b) \Rightarrow d_1 \mid d_2$$

protože $d_2 = \gcd(a,b)$

$$d_2 = \gcd(a,b) \Rightarrow (d_2 \mid a \wedge d_2 \mid b) \Rightarrow d_2 \mid d_1$$

protože $d_1 = \gcd(a,b)$

$$\Rightarrow (d_1 \mid d_2 \wedge d_2 \mid d_1) \Rightarrow (|d_1| = |d_2|) \Rightarrow d_1 = d_2$$

protože $d_1 \geq 0 \wedge d_2 \geq 0$

□