Kongruence

Def. (Kongruence na $\mathbb{Z}$): Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Čísla a a b jsou kongruentní modulo m právě tehdy, když $\exists k \in \mathbb{Z}$:

$$a - b = k \cdot m.$$

značíme : $a \equiv b \pmod{m}$

Poznámka: $a \equiv b \pmod{m} \Leftrightarrow$ a i b dávají při dělení číslem m stejný zbytek.

Příklad : $a = 31$, $b = 15$ $\Rightarrow$

$$\left.\begin{aligned} a &= 31 = 7 \cdot \underbrace{4}_{=m} + 3 \\ b &= 15 = 3 \cdot 4 + 3 \end{aligned}\right\} \Rightarrow a - b = (7 \cdot 4 + 3) - (3 \cdot 4 + 3) = 4 \cdot \underbrace{4}_{=m} \Rightarrow$$

$$\Rightarrow \underline{31 \equiv 15 \pmod{4}}$$

ale

$$\left.\begin{aligned} a &= 31 = 6 \cdot 5 + 1 \\ b &= 15 = 3 \cdot 5 + 0 \end{aligned}\right\} \Rightarrow a - b = 3 \cdot 5 + 1 \neq k \cdot 5 \Rightarrow$$

$$\Rightarrow \underline{31 \not\equiv 15 \pmod{5}}$$

Věta: Pro každé $a, b, c \in \mathbb{Z}$ a pro každé $m \in \mathbb{N}$ platí:

1.) $a \equiv a \pmod m$

2.) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

3.) $(a \equiv b \pmod m \wedge b \equiv c \pmod m) \Rightarrow a \equiv c \pmod m$.

Tzn. relace kongruence je reflexivní, symetrická a tranzitivní. Takovou relaci nazýváme ekvivalencí.

Důkaz: ad 1.) $\forall a \in \mathbb{Z}\ \forall m \in \mathbb{N}$:

$$a - a = 0 = \underset{\in \mathbb{Z}}{0} \cdot m \Rightarrow a \equiv a \pmod m.$$

ad 2.) $\forall a, b \in \mathbb{Z}\ \forall m \in \mathbb{N}$:

$$a \equiv b \pmod m \Rightarrow \exists k \in \mathbb{Z}: a - b = k \cdot m \Rightarrow b - a = \underset{\in \mathbb{Z}}{-k} \cdot m \Rightarrow b \equiv a \pmod m.$$

ad 3.) $\forall a, b, c \in \mathbb{Z}\ \forall m \in \mathbb{N}$:

$$\left.\begin{array}{l} a \equiv b \pmod m \Rightarrow \exists k_1 \in \mathbb{Z}: a - b = k_1 \cdot m \\ b \equiv c \pmod m \Rightarrow \exists k_2 \in \mathbb{Z}: b - c = k_2 \cdot m \end{array}\right\} \Rightarrow a - c = \underset{\in \mathbb{Z}}{(k_1 + k_2)} m \Rightarrow a \equiv c \pmod m$$

□

Věta: Nechť $a_1 \equiv b_1 \pmod m$ a $a_2 \equiv b_2 \pmod m$. Potom:

1.) $a_1 + a_2 \equiv b_1 + b_2 \pmod m$

2.) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m$

3.) $a_1 - a_2 \equiv b_1 - b_2 \pmod m$

Důkaz:

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod m \Rightarrow \exists k_1 \in \mathbb{Z}: \quad a_1 - b_1 = k_1 m \\ a_2 \equiv b_2 \pmod m \Rightarrow \exists k_2 \in \mathbb{Z}: \quad a_2 - b_2 = k_2 m \end{array}\right\} \Rightarrow$$

ad 1.) Rovnice sečteme $\Rightarrow$

$$(a_1 + a_2) - b_1 - b_2 = k_1 m + k_2 m$$

$$(a_1 + a_2) - (b_1 + b_2) = \underbrace{(k_1 + k_2)}_{\in \mathbb{Z}} m$$

$$(a_1 + a_2) \equiv (b_1 + b_2) \pmod m$$

ad 2.) Vyjádříme a_1, a_2 a vynásobíme $\Rightarrow$

$$a_1 \cdot a_2 = (b_1 + k_1 m)(b_2 + k_2 m) = b_1 b_2 + m(\underbrace{b_1 k_2 + k_1 b_2 + k_1 k_2 m}_{"k \in \mathbb{Z}"})$$

$$a_1 \cdot a_2 - b_1 b_2 = k \cdot m$$

$$a_1 a_2 \equiv b_1 b_2 \pmod m$$

ad 3.) Rovnice odečteme $\Rightarrow$

$$a_1 - a_2 - b_1 + b_2 = k_1 m - k_2 m$$

$$(a_1 - a_2) - (b_1 - b_2) = \underbrace{(k_1 - k_2)}_{\in \mathbb{Z}} m$$

$$a_1 - a_2 \equiv b_1 - b_2 \pmod m$$

□

Věta: Nechť $c \in \mathbb{Z}$. Potom platí:

$$a \equiv b \pmod{m} \Rightarrow ac \equiv bc \pmod{m}$$

Důkaz: $\forall c \in \mathbb{Z}$ platí:

$$a \equiv b \pmod{m} \Rightarrow \exists k \in \mathbb{Z}: a - b = k \cdot m \Rightarrow$$
$$c(a-b) = c\,k\,m$$
$$ca - cb = (ck) \cdot m$$
$$ca \equiv cb \pmod{m} \quad (ck \in \mathbb{Z})$$

□

Věta: Nechť $c \in \mathbb{Z}$. Potom platí:

$$[ac \equiv bc \pmod{m} \wedge \gcd(c, m) = 1] \Rightarrow a \equiv b \pmod{m}$$

Důkaz: $\forall c \in \mathbb{Z}$ platí:

$$ac \equiv bc \pmod{m} \Rightarrow \exists k \in \mathbb{Z}: ac - bc = k \cdot m$$
$$c(a-b) = k \cdot m$$
$$m \mid c(a-b)$$

a protože $\gcd(c, m) = 1 \Rightarrow$

$$m \mid (a-b)$$
$$\exists k^* \in \mathbb{Z}: a - b = k^* \cdot m \Rightarrow a \equiv b \pmod{m}$$

□

Poznámka: Předpoklad $\gcd(c, m) = 1$ je důležitý! Viz například

$28 \equiv 16 \pmod{6}$ (28 i 16 dává zbytek 4 při dělení číslem 6)

$\Downarrow$

$7 \cdot 4 \equiv 4 \cdot 4 \pmod{6}$

ale: $7 \not\equiv 4 \pmod{6}$

Def. (Zbytková třída): Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$. Potom zbytkovou třídou modulo m nazveme množinu

$$\bar{a}_m = \{ z \in \mathbb{Z} \mid z \equiv a \pmod m \}$$

Tzn $\bar{a}_m$ je množina všech celých čísel kongruentních s číslem a.

Příklad: $\bar{2}_5 = \{ z \in \mathbb{Z} \mid z \equiv 2 \pmod 5 \}$

$$z \equiv 2 \pmod 5 \iff \exists k \in \mathbb{Z} : \; z - 2 = k \cdot 5 \iff$$
$$\exists k \in \mathbb{Z} : \; z = k \cdot 5 + 2$$

$$\Downarrow$$

$$\bar{2}_5 = \{ k \cdot 5 + 2 \mid k \in \mathbb{Z} \} = \{ \ldots, -13, -8, -3, 2, 7, 12, 17, \ldots \}$$

Lema: Nechť $a \equiv b \pmod m$. Potom $\bar{a}_m = \bar{b}_m$.

Důkaz: I.) $\forall z \in \bar{a}_m$: $z \equiv a \pmod m$ a podle předpokladu $a \equiv b \pmod m$.
Z tranzitivity relace kongruence plyne $z \equiv b \pmod m \Rightarrow$
$\Rightarrow z \in \bar{b}_m \Rightarrow \bar{a}_m \subseteq \bar{b}_m$

II.) $\forall z \in \bar{b}_m$: ... analogicky dojdeme k tomu, že $\bar{b}_m \subseteq \bar{a}_m$.

Př.: $\bar{2}_5 = \bar{7}_5 = \bar{12}_5 = \ldots \Rightarrow$ „nezáleží na výběru reprezentanta"

Důsledek: $\forall m \in \mathbb{N}\ \forall z \in \mathbb{Z}\ \exists\, a \in \{0,1,\dots,m-1\} : \quad z \in \bar{a}_m$

Tzn. každé celé číslo patří do některé ze zbytkových tříd

$\bar{0}_m, \bar{1}_m, \dots, \overline{m-1}_m$

Důkaz: $\forall m \in \mathbb{N}\ \forall z \in \mathbb{Z}\ \exists\, a \in \{0,1,\dots,m-1\}\ \exists q \in \mathbb{Z}:$

$$z = q \cdot m + a$$

a ↑ zbytek po dělení čísla z číslem m

$$\Rightarrow z \equiv a \pmod m \Rightarrow z \in \bar{a}_m$$

□

Př.: Každé celé číslo patří do některé ze zbytkových tříd

$\bar{0}_4, \bar{1}_4, \bar{2}_4, \bar{3}_4 \Rightarrow \bar{0}_4 \cup \bar{1}_4 \cup \bar{2}_4 \cup \bar{3}_4 = \mathbb{Z}$

Věta: Pro každé $m \in \mathbb{N}$ platí:

1.) $\bigcup_{a=0}^{m-1} \bar{a}_m = \mathbb{Z}$

2.) $\forall a, b \in \{0, 1, \dots, m-1\}: \quad a \neq b \Rightarrow \bar{a}_m \cap \bar{b}_m = \emptyset$

Tzn. zbytkové třídy tvoří rozklad množiny celých čísel na navzájem disjunktní množiny

Důkaz: ad 1.) Dříve jsme dokázali, že každé celé číslo patří do některé ze zbytkových tříd $\bar{0}_m, \bar{1}_m, \dots, \overline{m-1}_m \Rightarrow \mathbb{Z} \subseteq \bigcup_{a=0}^{m-1} \bar{a}_m \subseteq \mathbb{Z}$

ad 2.) Předpokládejme, že $\bar{a}_m \cap \bar{b}_m \neq \emptyset$ a $a, b \in \{0, 1, \dots, m-1\} \Rightarrow$

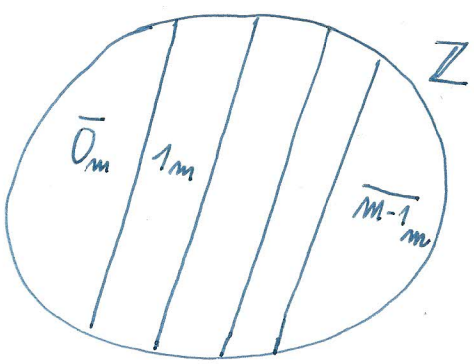
$\Rightarrow \exists z \in \bar{a}_m \cap \bar{b}_m \Rightarrow [z \equiv a \pmod m \wedge z \equiv b \pmod m] \Rightarrow$

$\Rightarrow a \equiv b \pmod m \Rightarrow \exists k \in \mathbb{Z}: a - b = k \cdot m \Rightarrow$

$0 \leq a \leq m-1$
$-(m-1) \leq -b \leq 0$
$\Rightarrow -(m-1) \leq a - b \leq m-1$

$\Downarrow$

$k = 0 \Rightarrow a = b$



□