Připomeňme, že gcd(a,b) je možné vyjádřit jako lineární kombinaci čísel a a b.

Př: $a = 48 \quad b = 63$

$$63 = 1 \cdot 48 + 15$$
$$48 = 3 \cdot 15 + 3 = \gcd(63,48)$$
$$15 = 5 \cdot 3 + 0$$

$$\Rightarrow 3 = 48 - 3 \cdot 15 = 48 - 3(63-48) = \underline{\underline{4 \cdot 48 - 3 \cdot 63}}$$

Lineární kongruence

Problém: Jsou dána čísla $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Cílem je nalezení všech $x \in \mathbb{Z}$, které splňují:

$$ax \equiv b \pmod{m}$$

Příklad: Nalezněte všechna $x \in \mathbb{Z}$ splňující:

$$2x \equiv 1 \pmod{5}$$

Všimněme si, že $x = 3$ této lineární kongruenci vyhovuje a také každý jiný prvek zbytkové třídy $\overline{3}_m$.

Věta: Nechť $a, b, x \in \mathbb{Z}$ a platí $ax \equiv b \pmod{m}$.
Potom $\forall y \in \overline{x}_m : \quad ay \equiv b \pmod{m}$.

Důkaz: $\forall y \in \overline{x}_m : \quad y \equiv x \pmod{m} \Rightarrow$

$\Rightarrow ay \equiv ax \pmod{m} \quad | \; ax \equiv b \pmod{m} \Rightarrow$

$\Rightarrow ay \equiv b \pmod{m}$

Def (Řešení lin. kongruence): Nechť $a, b, x_0 \in \mathbb{Z}$, $m \in \mathbb{N}$. Jestliže $ax_0 \equiv b \pmod{m}$, pak zbytkovou třídu $\overline{x_0}_m$ nazveme řešením lineární kongruence $ax \equiv b \pmod{m}$.

Příklad: $6x \equiv 2 \pmod{4}$

Z čísel $0, 1, 2, 3$ (zástupci všech možných zbytkových tříd modulo 4) vyhovují zadané kongruenci pouze $x = 1$ a $x = 3$. Zadaná lineární kongruence má proto dvě různá řešení $\overline{1}_4$ a $\overline{3}_4$.

(Ale pozor! Dosadíme-li za x libovolný prvek z těchto zbytkových tříd, bude kongruence $6x \equiv 2 \pmod{4}$ splněna. Existuje tedy nekonečně mnoho čísel $x \in \mathbb{Z}$, které splňují $6x \equiv 2 \pmod{4}$ – všechny ale mají tvar $x = 4k+1$, nebo $x = 4k+3$, kde $k \in \mathbb{Z}$.

Věta: Nechť $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Jestliže $\gcd(a, m) = 1$, pak řešení lineární kongruence $ax \equiv b \pmod{m}$ existuje a je jediné.

Důkaz:

1.) Existence: $\gcd(a, m) = 1 \quad \Rightarrow \quad \exists x_0, y_0 \in \mathbb{Z}$:

$$a x_0 + m y_0 = 1 \quad / \cdot b$$

$$a(b x_0) + m(y_0 b) = b$$

$$a \underbrace{(b x_0)}_{\ddot{x} \in \mathbb{Z}} - b = \underbrace{(y_0 b)}_{k \in \mathbb{Z}} m \quad \Rightarrow \quad a(b x_0) \equiv b \pmod{m}$$

$\Rightarrow \overline{x}_m = \overline{b x_0}_m$ je řešením lin. kong. $ax \equiv b \pmod{m}$.

2.) Jednoznačnost: Předpokládejme, že $a x_1 \equiv b \pmod{m}$ a také $a x_2 \equiv b \pmod{m}$. $\Rightarrow$

$$a x_1 \equiv a x_2 \pmod{m} \quad \text{(z tranzitivity } \equiv)$$

a protože $\gcd(a, m) = 1$, můžeme v kongruenci krátit $\Rightarrow$

$$x_1 \equiv x_2 \pmod{m}$$

Znamená to, že všechna x vyhovující kongruenci $ax \equiv b \pmod{m}$ patří do stejné zbytkové třídy modulo m $\Rightarrow$ existuje jediné řešení kongruence $ax \equiv b \pmod{m}$.

$\square$

Příklad: Nalezněte všechna řešení lineární kongruence.

a) $13x \equiv 21 \pmod{72}$

$$\left.\begin{aligned} 72 &= 5\cdot 13 + 7 \\ 13 &= 1\cdot 7 + 6 \\ 7 &= 1\cdot 6 + 1 = \gcd(72,13) \end{aligned}\right\} \Rightarrow \left.\begin{aligned} 1 &= 7 - 6 = 7 - (13-7) = \\ &= 2\cdot 7 - 13 = 2(72 - 5\cdot 13) - 13 = \\ &= 2\cdot 72 - 11\cdot 13 \end{aligned}\right\} \Rightarrow$$

$\Rightarrow \exists!$ řešení

$$\Rightarrow \quad 1 = 2\cdot 72 - 11\cdot 13 \quad / \cdot 21$$

$$21 = 42\cdot \underbrace{72}_{\equiv\, 0 \pmod{72}} - 231\cdot 13 \quad / \pmod{72}$$

$$21 \equiv -231\cdot 13 \pmod{72} \qquad / \, 3\cdot 72 = 216$$

$$21 \equiv -15\cdot 13 \pmod{72}$$

$$21 \equiv 57\cdot 13 \pmod{72}$$

$$\Rightarrow \quad \underline{\underline{x \in \overline{57}_{72}}}$$

Lema: Nechť $m, d, m_0 \in \mathbb{N}$, $m = d\,m_0$. Potom

$$\overline{x}_{m_0} = \overline{x}_m \cup \overline{x+m_0}_m \cup \overline{x+2m_0}_m \cup \dots \cup \overline{x+(d-1)m_0}_m$$

Důkaz: $u \in \overline{x}_{m_0 = \frac{m}{d}} \iff u = x + k\cdot m_0$, kde $k \in \mathbb{Z}$

ale k může patřit do různých zbytkových tříd modulo d $\Rightarrow$

$$u = x + k m_0 = \begin{cases} x + (k_0 d + 0) m_0 = x + \overbrace{k_0 d m_0}^{m} \in \overline{x}_m \\ x + (k_0 d + 1) m_0 = x + k_0 d m_0 + m_0 \in \overline{x+m_0}_m \\ x + (k_0 d + 2) m_0 = x + k_0 d m_0 + 2m_0 \in \overline{x+2m_0}_m \\ \vdots \\ x + (k_0 d + (d-1)) m_0 = x + k_0 d m_0 + (d-1) m_0 \in \overline{x+(d-1)m_0}_m \end{cases}$$

$$\Rightarrow \overline{x}_{\frac{m}{d}} \subseteq \overline{x}_m \cup \overline{x+m_0}_m \cup \overline{x+2m_0}_m \cup \dots \cup \overline{x+(d-1)m_0}_m$$

Opačná inkluze je zřejmá.

Příklad:

$$\overline{3}_5 = \overline{3}_{\underset{5\cdot 4}{20}} \cup \overline{8}_{20} \cup \overline{13}_{20} \cup \overline{18}_{20}$$

$$3_5 = \overline{3}_{\underset{5\cdot 5}{25}} \cup \overline{8}_{25} \cup \overline{13}_{25} \cup \overline{18}_{25} \cup \overline{23}_{25}$$

Věta: Nechť $\gcd(a,m) = d$. Potom lineární kongruence

$$ax \equiv b \pmod{m}$$

má řešení $\iff d \mid b$. V případě, že $d \mid b$ má právě d různých řešení.

Důkaz: $\boxed{\Rightarrow}$ Předpokládejme, že $ax \equiv b \pmod{m}$ má řešení $x = x_0 \in \mathbb{Z}$
Označme $a = da_0$, $m = dm_0$ ($d \mid a \wedge d \mid m$, neboť $d = \gcd(a,m)$).

$$ax_0 \equiv b \pmod{m}$$

$$ax_0 - b = k \cdot m$$

$$da_0x_0 - b = k \cdot dm_0$$

$$d(a_0x_0 - km_0) = b \qquad \Rightarrow \quad d \mid b$$

$\boxed{\Leftarrow}$ Předpokládejme, že $d \mid b$
$\Rightarrow b = db_0$, $a = da_0$, $m = dm_0$, kde $b_0, a_0, m_0 \in \mathbb{Z}$ $\Rightarrow$

$$ax \equiv b \pmod{m}$$

$$\Updownarrow$$

$$ax - b = k \cdot m$$

$$\Updownarrow$$

$$da_0x - db_0 = k \cdot dm_0 \qquad /:d \qquad \text{víme, že } d \neq 0 \text{, neboť } m \in \mathbb{N}.$$

$$\Updownarrow$$

$$a_0x - b_0 = k \cdot m_0$$

$$\Updownarrow$$

$$a_0x \equiv b_0 \pmod{m_0}$$

To znamená, že $x_0 \in \mathbb{Z}$ vyhovuje $ax \equiv b \pmod{m}$ právě tehdy, když vyhovuje kongruenci $a_0x \equiv b_0 \pmod{m_0}$.

Kongruence $a_0 x \equiv b_0 \pmod{m_0}$ má jediné řešení , neboť

$\gcd(a_0, m_0) = \gcd\left(\frac{a}{d}, \frac{m}{d}\right) = \gcd\left(\frac{a}{\gcd(a,m)}, \frac{m}{\gcd(a,m)}\right) = 1$. To jest $\exists x_0 \in \mathbb{Z}$:

x je řešením $a_0 x \equiv b_0 \pmod{m_0}$ $\Leftrightarrow$ $x \equiv x_0 \pmod{m_0}$ $\Leftrightarrow$

$$\Leftrightarrow \quad x \in \overline{x_0}_{m_0} = \bigcup_{i=0}^{d-1} \overline{x_0 + i m_0}_m$$

Tzn. všechna $x \in \mathbb{Z}$ vyhovující $ax \equiv b \pmod m$ jsou stejná jako x vyhovující kongruenci $a_0 x \equiv b_0 \pmod m$ jsou to celá čísla patřící do jediné zbytkové třídy modulo m_0. Mohou ale (v případě $d>1$) patřit do více zbytkových tříd modulo $m = d \cdot m_0$

Navíc $\overline{x_0 + i m_0}_m$, $i \in \{0, \dots, d-1\}$ jsou navzájem disjunktní, neboť:

pro $i, j \in \{0, \dots, d-1\}$: $x_0 + i m_0 \equiv x_0 + j m_0 \pmod m$

$$i m_0 \equiv j m_0 \pmod m$$

$$(i-j) m_0 \equiv 0 \pmod m \quad \Leftrightarrow \quad (i-j) m_0 = k \cdot d \cdot m_0 \Rightarrow$$

$$\Rightarrow (i-j) = k \cdot d \Rightarrow$$

$$\Rightarrow i \equiv j \pmod d \Rightarrow i = j$$

$\square$

Příklad: Nalezněte všechna řešení lineární kongruence.

a) $21x \equiv 24 \pmod{77}$

$\gcd(21, 77) = 7 \nmid 24 \Rightarrow$ nemá řešení

$\boxed{\text{Př.: Vyřešte lineární kongruenci } 26x \equiv 14 \pmod{48}}$

1.) $\gcd(26,48) = ?$

$$48 = 1\cdot 26 + 22$$
$$26 = 1\cdot 22 + 4$$
$$22 = 5\cdot 4 + 2$$
$$4 = 2\cdot 2 + 0$$

2.) $\Rightarrow$ $\gcd(26,48) = 2 \mid 14$ $\Rightarrow$ lineární kongruence $26x \equiv 14 \pmod{48}$ má 2 různá řešení

3.) $26x \equiv 14 \pmod{48} \Leftrightarrow 13x \equiv 7 \pmod{24}$ má jediné řešení mod 24 neboť $\gcd(13,24) = 1$

$$24 = 1\cdot 13 + 11 \quad \Rightarrow \quad 11 = 24 - 13$$
$$13 = 1\cdot 11 + 2 \quad \Rightarrow \quad 2 = 13 - 11$$
$$11 = 5\cdot 2 + 1$$
$$2 = 2\cdot 1 + 0$$

$$\Rightarrow \quad 1 = 11 - 5\cdot 2$$
$$1 = 11 - 5(13-11)$$
$$1 = 24-13-5(13-(24-13))$$
$$1 = 24 - 13 - 5\cdot 13 + 5(24-13)$$
$$1 = 6\cdot 24 - 11\cdot 13$$

$$\Rightarrow \quad 7 = 42\cdot 24 - 77\cdot 13$$

$$7 + 77\cdot 13 = 42\cdot 24 \quad \Rightarrow \quad \underset{-5}{\underbrace{-77}}\cdot 13 \equiv 7 \pmod{24}$$

$$\Rightarrow \underline{x_0 \equiv -5 + k\cdot 24}$$

$\Rightarrow$ Řešením $26x \equiv 14 \pmod{48}$ jsou zbytkové třídy: $\underline{\underline{\overline{-5}_{48} \text{ a } \overline{19}_{48}}}$.