**Věta (Čínská zbytková):** Nechť $m_1, \dots, m_n \in \mathbb{N}$ jsou navzájem nesoudělná čísla ($\gcd(m_i, m_j) = 1$ pro $i \neq j$). a $b_1, b_2, \dots, b_n \in \mathbb{Z}$. Potom existuje právě jedna zbytková třída modulo $m_1 \cdot \dots \cdot m_n$, která je řešením soustavy kongruencí:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned} \qquad (*)$$

**Důkaz:** 1.) existence: Označme $M = m_1 \cdot \dots \cdot m_n$. Potom $\forall i = 1, \dots, n: \gcd(m_i, \frac{M}{m_i}) = 1$ a tak $\forall i = 1, \dots, n \; \exists y_i \in \mathbb{Z}: \frac{M}{m_i} y_i \equiv b_i \pmod{m_i}$
(lin. kongruence $\frac{M}{m_i} x \equiv b_i \pmod{m_i}$ řešení jistě má)

Označme $x_0 = y_1 \frac{M}{m_1} + y_2 \frac{M}{m_2} + \dots + y_n \frac{M}{m_n}$

$\Rightarrow \forall i = 1, \dots, n: x_0 \equiv b_i \pmod{m_i}$

(neboť pro $j \neq i$: $m_i \mid \frac{M}{m_j}$, tzn. $\frac{M}{m_j} \equiv 0 \pmod{m_i}$ a $y_i \frac{M}{m_i} \equiv b_i \pmod{m_i}$)

$\Rightarrow x_0$ ~~je řešením~~ vyhovuje všem kongruencím $(*)$

2.) jednoznačnost: Předpokládejme, že také $x_1$ splňuje $(*)$ $\Rightarrow$

$\forall i = 1, \dots, n: x_0 \equiv b_i \pmod{m_i} \wedge x_1 \equiv b_i \pmod{m_i}$

$\Rightarrow \forall i = 1, \dots, n: x_0 \equiv x_1 \pmod{m_i}$

$\forall i = 1, \dots, n: (x_0 - x_1) = k_i \cdot m_i \quad \Rightarrow \forall i = 1, \dots, n: m_i \mid (x_0 - x_1) \Rightarrow$

$M \mid (x_0 - x_1)$ (díky tomu, že $m_i$ jsou navz. nesoud.)

$x_0 - x_1 = k \cdot M$

$x_0 \equiv x_1 \pmod{M}$

$\Rightarrow$ Všechna $x$ splňující $(*)$ patří do $\overline{x_0}_M$ $\square$

Př. V koši jsou vajíčka. Vyndáváme-li je po dvou, zbyde v koši jedno. Vyndáváme-li po pěti, zbyde jedno. Vyndáváme-li po třech nezbyde žádné. Kolik může být v koši vajíček, jestliže se do něj vejde maximálně 100 vajíček?

Řešení: Označíme-li počet vajíček v koši $x$, řešíme soustavu kongruencí:

$$x \equiv 1 \pmod 2$$
$$x \equiv 1 \pmod 5$$
$$x \equiv 0 \pmod 3$$

1.) $\frac{2\cdot5\cdot3}{2} y_1 \equiv 1 \pmod 2$

$15 y_1 \equiv 1 \pmod 2$

$y_1 \equiv 1 \pmod 2$

2.) $\frac{2\cdot5\cdot3}{5} y_2 \equiv 1 \pmod 5$

$6 y_2 \equiv 1 \pmod 5$

$y_2 \equiv 1 \pmod 5$

3.) $\frac{2\cdot5\cdot3}{3} y_3 \equiv 0 \pmod 3$

$10 y_3 \equiv 0 \pmod 3$

$y_3 \equiv 0 \pmod 3$

$$x \equiv \frac{2\cdot5\cdot3}{2}\cdot 1 + \frac{2\cdot5\cdot3}{5}\cdot 1 + \frac{2\cdot5\cdot3}{3}\cdot 0 \pmod{2\cdot5\cdot3}$$

$$x \equiv 15\cdot 1 + 6\cdot 1 + 10\cdot 0 \pmod{30}$$

$$x \equiv 21 \pmod{30}$$

$\Rightarrow x \in \{21, 51, 81\}$

V koši může být 21, 51, nebo 81 vajíček.

**Důsledek:** Nechť $m_1, \dots, m_n \in \mathbb{N}$ jsou navzájem nesoudělná, $a_1, \dots, a_n \in \mathbb{Z}$, $b_1, \dots, b_n \in \mathbb{Z}$, $\forall i \in \{1, \dots, n\}: \gcd(a_i, m_i) = 1$.

Potom systém lineárních kongruencí

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned} \qquad (**)$$

má právě jedno řešení modulo $m_1 \cdot \dots \cdot m_n$

**Důkaz:** $\forall i = 1, \dots, n$: $a_i x \equiv b_i \pmod{m_i}$ má právě jedno řešení mod $m_i$ – označme jej $\overline{x_{0i}}_{m_i}$

$\Rightarrow$ Soustava $(**)$ je ekvivalentní soustavě

$$\begin{aligned} x &\equiv x_{01} \pmod{m_1} \\ &\vdots \\ x &\equiv x_{0n} \pmod{m_n} \end{aligned} \qquad (***)$$

Soustava $(***)$ má podle Čínské zbytkové věty jediné řešení modulo $m_1 \cdot \dots \cdot m_n$.

□

**Věta:** Nechť $b_1, b_2 \in \mathbb{Z}$ ; $m_1, m_2 \in \mathbb{N}$ ; $d = \gcd(m_1, m_2)$.
Potom platí:

1.) $\exists x \in \mathbb{Z} : (x \equiv b_1 \pmod{m_1} \wedge x \equiv b_2 \pmod{m_2}) \Leftrightarrow$

$\Leftrightarrow \quad d \mid b_2 - b_1$

2.) Jestliže $d \mid b_2 - b_1$, pak existuje právě $d$ různých zbytkových tříd modulo $m_1 m_2$ takových, že jejich prvky $x$ vyhovují kongruencím: $x \equiv b_1 \pmod{m_1} \wedge x \equiv b_2 \pmod{m_2}$

Důkaz:

ad 1) $\boxed{\Rightarrow}$ Předpokládejme, že $\exists x \in \mathbb{Z} : (x \equiv b_1 \pmod{m_1} \wedge x \equiv b_2 \pmod{m_2})$.

$x \equiv b_1 \pmod{m_1} \Rightarrow \exists k_1 \in \mathbb{Z} : \quad x = k_1 m_1 + b_1 \qquad (1)$

$x \equiv b_2 \pmod{m_2} \Rightarrow \exists k_2 \in \mathbb{Z} : \quad x = k_2 m_2 + b_2$

$\Rightarrow b_2 - b_1 = k_1 m_1 - k_2 m_2 = \underset{\in \mathbb{Z}}{k} \cdot d$ neboť $d \mid m_1 \wedge d \mid m_2 \Rightarrow d \mid b_2 - b_1$

$\Leftarrow$ Předpokládejme, že $d \mid b_2 - b_1$

$d = \gcd(m_1, m_2) \Rightarrow \exists\, c_1, c_2 \in \mathbb{Z} : \quad m_1 c_1 - m_2 c_2 = d$

Všimněme si, že $\gcd\left(d, \frac{m_1 m_2}{d}\right) = d$. Navíc, podle předpokladu $d \mid b_2 - b_1$. Proto existuje řešení kongruence:

$$d\,x \equiv b_2 - b_1 \pmod{\frac{m_1 m_2}{d}}$$

označme jej $x_0$. A tak:

$$(m_1 c_1 - m_2 c_2)\, x_0 \equiv b_2 - b_1 \pmod{\frac{m_1 m_2}{d}}$$

$$\underbrace{m_1 c_1 x_0 + b_1}_{x} \equiv m_2 c_2 x_0 + b_2 \pmod{\frac{m_1 m_2}{d}} \qquad (4)$$

Označme $x = m_1 c_1 x_0 + b_1 \qquad (5)$

a) Okamžitě z (5) plyne, že $\boxed{x \equiv b_1 \pmod{m_1}}$

b) Z (4) plyne, že $\exists\, r \in \mathbb{Z}$:

$$x = r \cdot \frac{m_1 m_2}{d} + m_2 c_2 x_0 + b_2$$

$$x = m_2 \underbrace{\left(r \frac{m_1}{d} + c_2 x_0\right)}_{\in \mathbb{Z}} + b_2$$

$$\boxed{x \equiv b_2 \pmod{m_2}}$$

ad 2) V předcházející části důkazu jsme zjistili, že

$$x = m_1 c_1 x_0 + b_1 \equiv m_2 c_2 x_0 + b_2 \pmod{\frac{m_1 m_2}{d}}$$

a $x$ vyhovuje kongruencím:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \end{aligned} \qquad (6)$$

Dokážeme, že také každý jiný prvek $x^*$ zbytkové třídy $\overline{x}_{\frac{m_1 m_2}{d}}$ splňuje kongruence (6) $\Rightarrow$

uvažujme $x^* = x + k\frac{m_1 m_2}{d} \in \overline{x}_{\frac{m_1 m_2}{d}}$.

α) $x^* = m_1 c_1 x_0 + b_1 + k\frac{m_1 m_2}{d} = m_1 \underbrace{\left(c_1 x_0 + k\frac{m_2}{d}\right)}_{\in \mathbb{Z}} + b_1 \Rightarrow \boxed{x^* \equiv b_1 \pmod{m_1}}$

β) Víme, že $x \equiv b_2 \pmod{m_2} \Rightarrow \exists s \in \mathbb{Z}$:

$$x^* = \underbrace{s m_2 + b_2}_{x} + k\frac{m_1 m_2}{d} = m_2 \underbrace{\left(s + k\frac{m_1}{d}\right)}_{\in \mathbb{Z}} + b_2 \Rightarrow \boxed{x^* \equiv b_2 \pmod{m_2}}$$

---

Vidíme, že všechny prvky zbytkové třídy $\underbrace{m_1 c_1 x_0 + b_1}_{x}\ \frac{m_1 m_2}{d}$ vyhovují kongruencím (6). Dokážeme, že kongruencím (6) vyhovují pouze prvky této zbytkové třídy a žádné jiné

– stačí ukázat, že libovolná dvě $x_1$ a $x_2 \in \mathbb{Z}$ splňující (6) jsou kongruentní modulo $\frac{m_1 m_2}{d}$.

Předpokládejme prodo, že:

$$\underline{x_1 \equiv b_1 \pmod{m_1}} \quad \wedge \quad \underline{x_1 \equiv b_2 \pmod{m_2}}$$
$$\underline{x_2 \equiv b_1 \pmod{m_1}} \qquad \underline{x_2 \equiv b_2 \pmod{m_2}}$$
$$\Downarrow \qquad\qquad \Downarrow$$
$$x_1 \equiv x_2 \pmod{m_1} \quad \wedge \quad x_1 \equiv x_2 \pmod{m_2}$$
$$\Downarrow \qquad\qquad \Downarrow$$

$\exists k_1 \in \mathbb{Z}$: $\qquad\qquad$ $\exists k_2 \in \mathbb{Z}$:

$$\boxed{x_1 - x_2 = k_1 m_1 \quad \wedge \quad x_1 - x_2 = k_2 m_2} \qquad (7)$$

$$\Downarrow$$

$$k_1 m_1 = k_2 m_2 \quad / \; d = \gcd(m_1, m_2) \Rightarrow \; m_1 = d\, m_1^* \in \mathbb{Z}, \; m_2 = d\, m_2^* \in \mathbb{Z}$$

$$k_1 m_1^* = k_2 m_2^* \quad / \; \gcd(m_1^*, m_2^*) = 1 \Rightarrow m_2^* \mid k_1 \Rightarrow$$

$$k_1 = t \cdot m_2^* \in \mathbb{Z}$$

dosadíme do (7) $\Rightarrow$

$$\Rightarrow x_1 - x_2 = t\, m_2^* m_1 = t \frac{m_1 m_2}{d} \Rightarrow x_1 \equiv x_2 \pmod{\frac{m_1 m_2}{d}}$$

$\Rightarrow$ $X$ vyhovuje kongruenci (6) $\Leftrightarrow$ $X \in \overline{m_1 c_1 x_0 + b_1}_{\frac{m_1 m_2}{d}}$

Navíc platí

$$\overline{X}_{\frac{m_1 m_2}{d}} = \overline{X}_{m_1 m_2} \cup \overline{X + 1 \cdot \frac{m_1 m_2}{d}}_{m_1 m_2} \cup \overline{X + 2\frac{m_1 m_2}{d}}_{m_1 m_2} \cup \dots \cup \overline{X + (d-1)\frac{m_1 m_2}{d}}_{m_1 m_2}$$

$\Rightarrow \exists d$ různých zbytkových tříd, jejichž prvky vyhovují kongruenci (6).

□

Př. Vyřešte soustavu lineárních kongruencí:

$$X \equiv \underset{b_1}{15} \pmod{\underset{m_1}{21}}$$
$$X \equiv \underset{b_2}{12} \pmod{\underset{m_2}{36}}$$

Nejprve určíme $d = \gcd(21, 36)$:

$$36 = 1 \cdot 21 + 15$$
$$21 = 1 \cdot 15 + 6$$
$$15 = 2 \cdot 6 + \textcircled{3}$$
$$6 = 2 \cdot 3 + 0$$

$3 \mid (\underbrace{15-12}_{b_1 - b_2})$ $\Rightarrow$ Řešení existuje $\Rightarrow$ určíme $d$ jako lin. kombinaci 21 a 36

$$3 = 15 - 2 \cdot 6 = 15 - 2(21-15) = -2 \cdot 21 + 3 \cdot 15 = -2 \cdot 21 + 3(36-21) \Rightarrow$$

$$d = \underbrace{-5}_{c_1} \cdot \underbrace{21}_{m_1} + \underbrace{3}_{-c_2} \cdot \underbrace{36}_{m_2} =$$

Vyřešíme lineární kongruenci $dx \equiv b_2 - b_1 \pmod{\frac{m_1 m_2}{d}}$:

$$3X \equiv 12 - 15 \pmod{\frac{21 \cdot 36}{3}}$$
$$3X \equiv -3 \pmod{21 \cdot 12}$$
$$X \equiv -1 \pmod{252} \Rightarrow X_0 = -1$$

Řešením je potom $\overline{m_1 c_1 x_0 + b_1}_{\frac{m_1 m_2}{d}}$:

$$X \in \overline{-5 \cdot 21 \cdot (-1) + 15}_{252} = \underline{\underline{\overline{120}_{252}}} = \overline{120}_{756} \cup \overline{372}_{756} \cup \overline{624}_{756}$$

Tzn. vyhovují $X = 120 + k252$, $k \in \mathbb{Z}$.

Zk.:
$$120 + k \cdot 252 = 5 \cdot 21 + 15 + k \cdot 21 \cdot 12 \equiv 15 \pmod{21}$$
$$120 + k \cdot 252 = 3 \cdot 36 + 12 + k \cdot 7 \cdot 36 \equiv 12 \pmod{36}$$