Věta (Čínská zbytková): Nechť $m_1, \dots, m_n \in \mathbb{N}$ jsou navzájem nesoudělná čísla (tzn. $\gcd(m_i, m_j) = 1$ pro $i \neq j$) a $b_1, \dots, b_n \in \mathbb{Z}$.

Potom existuje právě jedna zbytková třída $\overline{x_0}_M$, $M = m_1 \dots m_n$, která je řešením soustavy kongruencí:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned} \qquad (1)$$

Tzn. $x \in \mathbb{Z}$ vyhovuje kongruencím (1) právě když $x \in \overline{x_0}_M$.

Důkaz: Zvolme:

$$x_0 = y_1 \underbrace{\frac{m_1 \cdots m_n}{m_1}}_{\equiv 0 \pmod{m_i} \text{ pro } i \neq 1} + y_2 \underbrace{\frac{m_1 \cdots m_n}{m_2}}_{\equiv 0 \pmod{m_i} \text{ pro } i \neq 2} + \dots + y_n \underbrace{\frac{m_1 \cdots m_n}{m_n}}_{\equiv 0 \pmod{m_i} \text{ pro } i \neq n}$$

a čísla y_i tak, že $\forall i \in \{1, \dots, n\}$:

$$y_i \frac{m_1 \cdots m_n}{m_1} \equiv b_i \pmod{m_i} \qquad (2)$$

(Takové řešení y_i kongruence (2) jistě existuje, neboť $\gcd\left(\frac{m_1 \cdots m_n}{m_i}, m_i\right) = 1$)

$$\Rightarrow x_0 = \sum_{i=1}^{n} y_i \frac{m_1 \cdots m_n}{m_i} \equiv b_i \pmod{m_i} \Rightarrow x_0 \text{ vyhovuje (1).}$$

Navíc $\forall x \in \overline{x_0}_M$: $x = x_0 + k \cdot M = x_0 + k_i \underbrace{m_i}_{\in \mathbb{Z}} \equiv x_0 \pmod{m_i} \equiv b_i \pmod{m_i} \Rightarrow x$ také vyhovuje (1).

(Dále ukážeme, že (1) vyhovují jen prvky z $\overline{x_0}_M$ - předpokl. že x_1 vyhovuje (1) také $\Rightarrow$)

$$\Rightarrow \forall i \in \{1, \dots, n\}: \left(x_0 \equiv b_i \pmod{m_i} \wedge x_1 \equiv b_i \pmod{m_i}\right)$$

$$\Rightarrow \forall i \in \{1, \dots, n\}: x_0 \equiv x_1 \pmod{m_i} \Rightarrow \exists k_i \in \mathbb{Z}: (x_0 - x_1) = k_i m_i$$

$$\Rightarrow x_0 - x_1 = k_1 m_1 = k_2 m_2 \quad / \gcd(m_1, m_2) = 1 \Rightarrow m_2 \mid k_1 \Rightarrow \exists k_1^{(1)}: k_1 = k_1^{(1)} m_2 \Rightarrow$$

$$x_0 - x_1 = k_1^{(1)} m_2 m_1 = k_3 m_3 \quad / \gcd(m_1 m_2, m_3) = 1 \Rightarrow m_3 \mid k_1^{(1)} \Rightarrow \exists k_1^{(2)}: k_1^{(1)} = k_1^{(2)} m_3 \Rightarrow$$

$$x_0 - x_1 = k_1^{(2)} m_3 m_2 m_1 = k_4 m_4$$

$$\vdots$$

$$x_0 - x_1 = \underbrace{k_1^{(n-1)}}_{\in \mathbb{Z}} m_n \dots m_1 = k_1^{(n-1)} \cdot M \Rightarrow x_0 \equiv x_1 \pmod{M}$$

$$\Rightarrow x_1 \in \overline{x_0}_M$$

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 $b_1, b_2 \in \mathbb{Z}$; $m_1, m_2 \in \mathbb{N}$; $d = c_1 m_1 - c_2 m_2 = \gcd(m_1, m_2)$, $c_1, c_2 \in \mathbb{Z}$. Potom platí:

1.) Existuje $x \in \mathbb{Z}$ vyhovující kongruencím:

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

právě tehdy, když $d \mid b_2 - b_1$.

2.) Jestliže $d \mid b_2 - b_1$, pak $x \in \mathbb{Z}$ vyhovuje kongruencím $(*)$ právě když:

$$x \equiv m_1 c_1 \frac{b_2 - b_1}{d} + b_1 \pmod{\frac{m_1 m_2}{d}}.$$

Tzn. právě když $x \in \overline{m_1 c_1 \frac{b_2 - b_1}{d} + b_1}_{\frac{m_1 m_2}{d}}$.

Důkaz: ad 1.) $\boxed{\Rightarrow}$ Předpokládejme, že $\exists x \in \mathbb{Z}$ vyhovující $(*)$

Potom: $x - b_1 = k_1 \cdot m_1$, kde $k_1 \in \mathbb{Z}$

$x - b_2 = k_2 \cdot m_2$, kde $k_2 \in \mathbb{Z}$

$$\Rightarrow b_2 - b_1 = k_1 m_1 - k_2 m_2 = k_1 \underbrace{d m_1'}_{m_1} - k_2 \underbrace{d m_2'}_{m_2} = d \cdot k \qquad k \in \mathbb{Z}$$

$$\Rightarrow d \mid b_2 - b_1$$

(⇐) Předpokládejme, že $d \mid b_2 - b_1$.

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

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

$$d x \equiv b_2 - b_1 \pmod{\frac{m_1 m_2}{d}} \qquad (1)$$

Je zřejmé, že $x_0 = \frac{b_2 - b_1}{d}$ ($\in \mathbb{Z}$ díky předpokladu) jistě vyhovuje (1).

a tak:

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

$$\underbrace{c_1 m_1 x_0 + b_1}_{x} \equiv c_2 m_2 x_0 + b_2 \pmod{\frac{m_1 m_2}{d}} \qquad (2)$$

Označme $x = c_1 m_1 x_0 + b_1$ (3)

a) Okamžitě z (3) plyne, že $x \equiv b_1 \pmod{m_1}$.

b) Z (2) plyne, že $\exists\, r \in \mathbb{Z}$ ($r \in \mathbb{Z}$):

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

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:

$$X \equiv 15 \pmod{21}$$
$$X \equiv 12 \pmod{36}$$

Označme: $m_1 = 21$, $m_2 = 36$, $b_1 = 15$, $b_2 = 12$; $c_1 = ?$ $d = ?$ $\Rightarrow$

Určíme $d = \gcd(m_1, m_2) = c_1 m_1 - c_2 m_2$

$$\left(\begin{array}{cc|cc} 21 & 1 & 1 & 0 \\ 36 & 0 & 0 & 1 \end{array}\right) \overset{-r_1}{\sim} \left(\begin{array}{cc|cc} 21 & 1 & 1 & 0 \\ 15 & -1 & -1 & 1 \end{array}\right) \overset{-r_2}{\sim} \left(\begin{array}{cc|cc} 6 & 2 & -1 & \\ 15 & -1 & 1 & \end{array}\right) \overset{-2r_1}{\sim} \left(\begin{array}{cc|cc} 6 & 2 & -1 & \\ 3 & -5 & 3 & \end{array}\right) \overset{-2r_2}{\sim} \left(\begin{array}{cc|cc} 0 & 12 & -7 & \\ \textcircled{3} & -5 & 3 & \end{array}\right)$$

(③ = d)

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

$$\Rightarrow X \equiv \underbrace{-5 \cdot 21 \cdot \frac{12-15}{3} + 15}_{c_1 m_1 \frac{b_2 - b_1}{d} + b_1} \pmod{\frac{21 \cdot 36}{3}}$$

$$X \equiv -5 \cdot 21 \cdot (-1) + 15 \pmod{252}$$

$$X \equiv 120 \pmod{252} \quad \text{Tzn.} \quad X \in \overline{120}_{252}$$

Zk:

$$X = 120 + k \cdot 252 = \begin{cases} 120 + k \cdot 12 \cdot 21 \equiv 120 \pmod{21} \equiv 120 - 5 \cdot 21 \equiv 15 \\ 120 + k \cdot 7 \cdot 36 \equiv 120 \pmod{36} \equiv 120 - 3 \cdot 36 \equiv 12 \end{cases}$$