Př.: Vyřešte soustavu lineárních kongruencí

a) $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 7$
$x \equiv 1 \pmod 4$

Vyřešíme kongruence:

1.) $\frac{3\cdot 7\cdot 4}{3} y_1 \equiv 2 \pmod 3$

$28 y_1 \equiv 2 \pmod 3$

$y_1 \equiv 2 \pmod 3$

$y_1 = 2$

2.) $\frac{3\cdot 7\cdot 4}{7} \cdot y_2 \equiv 3 \pmod 7$

$12 y_2 \equiv 3 \pmod 7$

$5 y_2 \equiv 3 \pmod 7$

$\gcd(5;7) = 1$:

$7 = 1\cdot 5 + 2$
$5 = 2\cdot 2 + 1$
$2 = 2\cdot 1 + 0$

$1 = 5 - 2\cdot 2 = 5 - 2(7-5) =$
$1 = 3\cdot 5 - 2\cdot 7 \quad / \cdot 3$
$3 = 9\cdot 5 - 6\cdot 7 \quad / \pmod 7$
$3 \equiv 5\cdot 9 \pmod 7$
$\equiv 2 \pmod 7$

$y_2 = 2$

3.) $\frac{3\cdot 7\cdot 4}{4} \cdot y_3 \equiv 1 \pmod 4$

$21 y_3 \equiv 1 \pmod 4$

$y_3 \equiv 1 \pmod 4$

$y_3 = 1$

$\Rightarrow x \equiv \frac{3\cdot 7\cdot 4}{3}\cdot 2 + \frac{3\cdot 7\cdot 4}{7}\cdot 2 + \frac{3\cdot 7\cdot 4}{4}\cdot 1 \pmod{3\cdot 7\cdot 4}$

$x \equiv 28\cdot 2 + 12\cdot 2 + 21\cdot 1 \pmod{84}$

$x \equiv 56 + 24 + 21 \pmod{84}$

$x \equiv 101 \pmod{84}$

$x \equiv 17 \pmod{84}$

b) $X \equiv -1 \pmod 7$

$X \equiv 8 \pmod{13}$

$X \equiv 5 \pmod{18}$

Vyřešíme kongruence:

1.) $\frac{7\cdot 13\cdot 18}{7} y_1 \equiv -1 \pmod 7$

$13\cdot 18 \cdot y_1 \equiv -1 \pmod 7$

$6\cdot 4 = 24$

$3 y_1 \equiv -1 \pmod 7$

$-y_1 \equiv 2 \pmod 7$

2.) $\frac{7\cdot 13\cdot 18}{13} y_2 \equiv 8 \pmod{13}$

$7\cdot 18\, y_2 \equiv 8 \pmod{13}$

$7\cdot 5 = 35$

$-4 y_2 \equiv 8 \pmod{13}$

$-y_2 \equiv -2 \pmod{13}$

3.) $\frac{7\cdot 13\cdot 18}{18} y_3 \equiv 5 \pmod{18}$

$7\cdot 13\, y_3 \equiv 5 \pmod{18}$

$7\cdot(-5) = -35$

$1\cdot y_3 \equiv 5 \pmod{18}$

$-y_3 \equiv 5 \pmod{18}$

$\Rightarrow X \equiv \frac{7\cdot 13\cdot 18}{7}\cdot 2 + \frac{7\cdot 13\cdot 18}{13}(-2) + \frac{7\cdot 13\cdot 18}{18}\cdot 5 \pmod{7\cdot 13\cdot 18}$

$X \equiv 13\cdot 18\cdot 2 - 7\cdot 18\cdot 2 + 7\cdot 13\cdot 5 \pmod{1638}$

$X \equiv 6\cdot 18\cdot 2 + 91 \pmod{1638}$

$X \equiv 180 + 36 + 91\cdot 5 \pmod{1638}$

$X \equiv 180 + 36 + 455 \pmod{1638}$

$X \equiv 671 \pmod{1638}$

Tzn. vyhovují všechna $x \in \mathbb{Z}$ ve tvaru $X = 671 + k\,1630$, kde $k \in \mathbb{Z}$.

Zkouška: $671 + k\cdot 1630 \overset{7\cdot 13\cdot 18}{\equiv} 671 \overset{-630}{\pmod 7} \equiv 41 \pmod 7 \equiv -1 \pmod 7$

$671 + k\cdot 7\cdot 13\cdot 18 \equiv 671 \overset{-520}{\pmod{13}} \equiv 151 \overset{-130-13}{\pmod{13}} \equiv 8 \pmod{13}$

$671 + k\cdot 7\cdot 13\cdot 18 \equiv 671 \overset{-720}{\pmod{18}} \equiv -49 \overset{+54}{\pmod{18}} \equiv 5 \pmod{18}$

Př. Vyřešte soustavu lineárních kongruencí

$$\begin{aligned} 3x &\equiv 5 \pmod 7 \\ 4x &\equiv 2 \pmod 6 \\ 9x &\equiv 8 \pmod{11} \end{aligned} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad \begin{aligned} 3x &\equiv 5 \pmod 7 \\ 2x &\equiv 1 \pmod 3 \\ 9x &\equiv 8 \pmod{11} \end{aligned}$$

a) $3x \equiv 5 \pmod 7$

$7 = 2\cdot 3 + 1 \Rightarrow 7 - 2\cdot 3 = 1 \quad /\cdot 5$

$3 = 3\cdot 1 + 0$

$7\cdot 5 - 10\cdot 3 = 5 \quad /\pmod 7$

$-10\cdot 3 \equiv 5 \pmod 7$

$x \equiv -10 \equiv 4 \pmod 7$

b) $2x \equiv 1 \pmod 3$

$3 = 1\cdot 2 + 1$

$3 - 2 = 1 \quad /\cdot$

$3 + (-1)\cdot 2 = 1 \quad /\pmod 3$

$(-1)\cdot 2 \equiv 1 \pmod 3$

$x \equiv -1 \equiv 2 \pmod 3$

c) $9x \equiv 8 \pmod{11}$

$11 = 1\cdot 9 + 2$

$9 = 4\cdot 2 + 1$

$1 = 9 - 4\cdot 2 \cdot$

$1 = 9 - 4(11 - 9)$

$1 = 5\cdot 9 - 4\cdot 11 \quad /\cdot 8$

$8 = 40\cdot 9 - 32\cdot 11 \pmod{11}$

$8 \equiv 40\cdot 9 \pmod{11}$

$x \equiv 40 \equiv 7 \pmod{11}$

$$\Leftrightarrow \quad \begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 7 \pmod{11} \end{aligned}$$

1.) $\frac{7\cdot 3\cdot 11}{7} y_1 \equiv 4 \pmod 7$

$33 y_1 \equiv 4 \pmod 7$

$5 y_1 \equiv 4 \pmod 7$

$\vdots$

$y_1 \equiv 5 \pmod 7$

2.) $\frac{7\cdot 3\cdot 11}{3} y_2 \equiv 2 \pmod 3$

$77 y_2 \equiv 2 \pmod 3$

$2 y_2 \equiv 2 \pmod 3$

$y_2 \equiv 1 \pmod 3$

3.) $\frac{7\cdot 3\cdot 11}{11} y_3 \equiv 7 \pmod{11}$

$21 y_3 \equiv 7 \pmod{11}$

$10 y_3 \equiv 7 \pmod{11}$

$\vdots$

$y_3 \equiv 4 \pmod{11}$

$$\Rightarrow \quad x \equiv \frac{7\cdot 3\cdot 11}{7}\cdot 5 + \frac{7\cdot 3\cdot 11}{3}\cdot 1 + \frac{7\cdot 3\cdot 11}{11}\cdot 4 \pmod{7\cdot 3\cdot 11}$$

$$x \equiv 326 \equiv 95 \pmod{231}$$

Příklad: Vyřešte soustavu lineárních kongruencí:

$$X \equiv 31 \pmod{42} \quad (b_1, m_1)$$
$$X \equiv 25 \pmod{39} \quad (b_2, m_2)$$

Nejprve určíme $\gcd(42, 39)$:

$$\begin{cases} 42 = 1 \cdot 39 + 3 \\ 39 = 13 \cdot 3 + 0 \end{cases} \Rightarrow d = 3 \mid (25-31) \Rightarrow$$ soustava má 3 řešení modulo 42.39

$25-31 = -6$

Vyjádříme $d = \gcd(42, 39)$ ve tvaru $d = 42c_1 - 39c_2$:

$$d = 42 \cdot 1 - 39 \cdot 1$$
$$\Downarrow$$
$$\boxed{c_1 = 1}$$

Nalezneme nějaké řešení $x_0 \in \mathbb{Z}$ kongruence:

$$3x \equiv 25-31 \pmod{\frac{42 \cdot 39}{3}} \quad (d \mid b_2 - b_1)$$
$$3x \equiv -6 \pmod{\frac{42 \cdot 39}{3}} \quad \mid \text{tam řešení, nebot } 3 \mid -6$$
$$\Updownarrow$$
$$x \equiv -2 \pmod{\frac{42 \cdot 39}{3 \cdot 3}}$$
$$\Downarrow$$

Řešením je například $x_0 = -2$

Označme $X = m_1 c_1 x_0 + b_1 = 42 \cdot 1 \cdot (-2) + 31 = -84 + 31 = -53.$

$\Rightarrow X$ vyhovuje zadanými kongruencím $\Leftrightarrow X \in \overline{-53}_{\frac{42 \cdot 39}{3}} = \overline{-53}_{546}$

$$\Leftrightarrow X \in \overline{-53}_{\underbrace{42 \cdot 39}_{1638}} \cup \overline{-53+546}_{1638} \cup \overline{-53+2 \cdot 546}_{1638} = \overline{-53}_{1638} \cup \overline{493}_{1638} \cup \overline{1039}_{1638}$$

Př. Vyřešte soustavu lineárních kongruencí:

$$13X \equiv 8 \pmod{27}$$
$$11X \equiv 1 \pmod{30}$$

Nejprve vyřešíme každou kongruenci zvlášť:

a) $13X \equiv 8 \pmod{27}$

$27 = 2 \cdot 13 + \textcircled{1} = \gcd(13,27)$ } $\Rightarrow$ $27 - 2 \cdot 13 = 1 \ / \cdot 8$

$13 = 13 \cdot 1 + 0$

$8 \cdot 27 \textcircled{-16} 13 \equiv 8 \pmod{27} \Rightarrow X \equiv -16 \equiv 11 \pmod{27}$

b) $11X \equiv 1 \pmod{30}$

$30 = 2 \cdot 11 + 8$

$11 = 1 \cdot 8 + 3$

$8 = 2 \cdot 3 + 2$

$3 = 1 \cdot 2 + \textcircled{1} = \gcd(30,11)$ } $\Rightarrow$

$1 = 3 - 2 = 3 - (8 - 2 \cdot 3)$

$= -1 \cdot 8 + 3 \cdot 3 = -1 \cdot 8 + 3(11 - 8) =$

$= 3 \cdot 11 - 4 \cdot 8 = 3 \cdot 11 - 4(30 - 2 \cdot 11)$

$= -4 \cdot 30 + \textcircled{11} \, 11 \equiv 1 \pmod{30} \Rightarrow X \equiv 11 \pmod{30}$

$\Rightarrow$ Zadaná soustava je ekvivalentní se soustavou:

$$X \equiv \underset{\text{“}b_1}{11} \pmod{\underset{\text{“}m_1}{27}}$$
$$X \equiv \underset{\text{“}b_2}{11} \pmod{\underset{\text{“}m_2}{30}}$$

Určíme $d = \gcd(m_1, m_2)$:

$30 = 1 \cdot 27 + \textcircled{3}$ $\quad 3 \mid (11 - 11) \Rightarrow$ řeš. existuje $\Rightarrow$ $3 = \underset{\text{“}c_1}{-1} \cdot \underset{\text{“}m_1}{27} + \underset{\text{“}c_2}{1} \cdot \underset{\text{“}m_2}{30}$

$27 = 9 \cdot 3 + 0$

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

$$3x \equiv 0 \pmod{\frac{27 \cdot 30}{3}}$$
$$x \equiv 0 \pmod{270} \Rightarrow x_0 = 0$$

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

$$X \in \overline{-1 \cdot 27 \cdot 0 + 11}_{270} = \overline{11}_{270} = \overline{11}_{810} \cup \overline{281}_{810} \cup \overline{551}_{810}$$

Tzn. vyhovují $X = 11 + k \cdot 270$, kde $k \in \mathbb{Z}$.

Zk: $13X = 13 \cdot 11 + k \cdot 13 \cdot 27 \cdot 10 \equiv 13 \cdot 11 \pmod{27} \equiv \underbrace{143}_{5 \cdot 27 + 8} \pmod{27} \equiv 8 \pmod{27}$

$11X = 11 \cdot 11 + k \cdot 11 \cdot 30 \cdot 9 \equiv 11 \cdot 11 \pmod{30} \equiv 121 \pmod{30} \equiv 1 \pmod{30}$

Příklad: Vyřeš soustavu lineárních kongruencí:

$$\begin{aligned} X &\equiv 14 \pmod{18} \\ X &\equiv 6 \pmod{14} \\ X &\equiv 1 \pmod{25} \\ X &\equiv 3 \pmod{11} \end{aligned} \qquad (1)$$

Čísla 18 a 14 jsou soudělná proto vyřešíme nejprve soustavu

$$\begin{aligned} X &\equiv 14 \pmod{18} \\ X &\equiv 6 \pmod{14} \end{aligned} \qquad (2)$$

($b_1 = 14$, $m_1 = 18$; $b_2 = 6$, $m_2 = 14$)

$18 = 1 \cdot 14 + 4$
$14 = 3 \cdot 4 + 2$
$4 = 2 \cdot 2 + 0$

$\Rightarrow = \gcd(18, 14) \mid 6 - 14$ $\Rightarrow$ soustava má dvě řešení modulo $18 \cdot 14$, ale jedno modulo $\frac{18 \cdot 14}{2}$ - to použijeme

Vyjádříme $d = 2 = 14 - 3 \cdot 4 = 14 - 3(18 - 14) = 4 \cdot 14 \underbrace{-3}_{c_1} \cdot 18$ $\Rightarrow \boxed{c_1 = -3}$

Nalezneme nějaké řešení kongruence: $\underbrace{2}_{d} X \equiv \underbrace{6 - 14}_{b_2 - b_1} \pmod{\frac{18 \cdot 14}{2}}$

$$\Uparrow$$

$$X \equiv \underbrace{\frac{6 - 14}{2}}_{x_0} \pmod{\frac{18 \cdot 14}{2}}$$

$$\Rightarrow X = m_1 c_1 x_0 + b_1 = 18 \cdot (-3) \frac{6 - 14}{2} + 14 = 18 \cdot 12 + 14 = 216 + 14 = \underline{230}$$

$$\Rightarrow \quad \begin{aligned} X &\equiv 14 \pmod{18} \\ X &\equiv 6 \pmod{14} \end{aligned} \Leftrightarrow X \equiv 230 \pmod{\underbrace{\frac{18 \cdot 14}{2}}_{126}} \Leftrightarrow X \equiv -22 \pmod{126} \Rightarrow$$

$\Rightarrow$ Zadaná soustava (1) je ekvivalentní se soustavou:

$$\begin{aligned} X &\equiv -22 \pmod{126} \quad (9\cdot 14) \\ X &\equiv 1 \pmod{25} \\ X &\equiv 3 \pmod{11} \end{aligned} \qquad (3)$$

Čísla 126, 25 a 11 jsou navzájem nesoudělná. Můžeme proto použít čínskou zbytkovou větu. Řešíme proto kongruence:

a) $25\cdot 11\, y_1 \equiv -22 \pmod{126} \Leftrightarrow 23 y_1 \equiv -22 \pmod{126}$ $\quad (25\cdot 11 = 275)$

$126 = 5\cdot 23 + 11$
$23 = 2\cdot 11 + 1 \quad = \gcd(23, 126) \Rightarrow$

$1 = 23 - 2\cdot 11 = 23 - 2(126 - 5\cdot 23) =$
$= 11\cdot 23 - 2\cdot 126$

$-22 = (-22)\cdot 11 \cdot 23 + (-22)(-2)\cdot 126$
$-22 \equiv (-22\cdot 11)\cdot 23 \pmod{126}$
$-22 \equiv (-242)\cdot 23 \pmod{126}$ $\quad (+2\cdot 126 = 252)$
$-22 \equiv 10 \cdot 23 \pmod{126}$

$10 = y_1$

b) $126\cdot 11\, y_2 \equiv 1 \pmod{25} \Leftrightarrow 11 y_2 \equiv 1 \pmod{25}$ $\quad (126 \equiv 1)$

$25 = 2\cdot 11 + 3$
$11 = 3\cdot 3 + 2$
$3 = 1\cdot 2 + 1 = \gcd(11, 25) \Rightarrow$

$1 = 3 - 2 = 3 - (11 - 3\cdot 3) = 4\cdot 3 - 11 =$
$= 4(25 - 2\cdot 11) - 11 = 4\cdot 25 - 9\cdot 11$

$1 \equiv 4\cdot 25 - 9\cdot 11 \pmod{25}$
$1 \equiv -9 \cdot 11 \pmod{25}$

$-9 = y_2$

c) $126 \cdot 25\, y_3 \equiv 3 \pmod{11} \iff 4 y_3 \equiv 3 \pmod{11}$

$126 = 5 \cdot 25$, $5 \cdot 3 = 4$

$11 = 2 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1 = \gcd(9, 11) \Rightarrow$

$1 = 4 - 3 = 4 - (11 - 2 \cdot 4) =$

$= -11 + 3 \cdot 4$

$3 = (-3) \cdot 11 + 9 \cdot 4$

$3 \equiv 9 \cdot 4 \pmod{11}$

$9 = y_3$

$\Rightarrow$ X je řešením (3), a tedy i (1) $\iff$

$$X \equiv 25 \cdot 11 \cdot 10 + 126 \cdot 11 (-9) + 126 \cdot 25 \cdot 9 \pmod{126 \cdot 25 \cdot 11}$$

$$X \equiv 18626 \pmod{34\,650}$$