Řešení kongruencí o jedné neznámé

Řešené příklady

Příklad. Určete počet řešení a kongruenci vyřešte:
$12x \equiv 3 \pmod{45}$

Řešení. $d = (12, 45) = 3 \wedge 3|3$. Kongruence tedy je řešitelná, a má právě 3 řešení.

$$\begin{aligned} 12x &\equiv 3 \pmod{45} \\ 4x &\equiv 1 \pmod{15} \\ 4x &\equiv 16 \pmod{15} \\ x &\equiv 4 \pmod{15} \end{aligned}$$

$x \in \{45t + 4, 45t + 19, 45t + 34, t \in \mathbb{Z}\}$. □

Příklad. Řešte soustavu lineárních kongruencí:

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 5 \pmod{6} \end{aligned}$$

Řešení. $x = 6t + 5, t \in \mathbb{Z}$

$$\begin{aligned} 6t + 5 &\equiv 4 \pmod{5} \\ t &\equiv 4 \pmod{5} \end{aligned}$$

$t = 5s + 4, s \in \mathbb{Z} \Rightarrow x = 30s + 29$
$x \equiv 29 \pmod{30}$ □

Příklad. Řešte soustavu kongruencí:

$$\begin{aligned} 5x + 7y &\equiv 3 \pmod{17} \\ 2x + 3y &\equiv -2 \pmod{17} \end{aligned}$$

Řešení. Vzhledem k tomu, že obě kongruence jsou vztaženy ke stejnému modulu, lze je například sčítat. Pokud by kongruence byly vztaženy k různým modulům, bylo by nutné je před aplikací následujícího postupu upravit tak, aby ke stejnému modulu vztaženy byly.

Nejdříve upravíme druhou kongruenci:

$$\begin{aligned} 2x + 3y &\equiv -2 \pmod{17} \\ 2x + 20y &\equiv -2 \pmod{17} \\ x + 10y &\equiv -1 \pmod{17} \end{aligned}$$

Tuto upravenou kongruenci přičteme k první kongruenci, čímž se zbavíme jedné z proměnných.

$$\begin{aligned} 6x + 17y &\equiv 2 \pmod{17} \\ 3x &\equiv 1 \pmod{17} \\ 3x &\equiv 18 \pmod{17} \\ x &\equiv 6 \pmod{17} \end{aligned}$$

Podobně jako u soustav lineárních rovnic o dvou neznámých, i zde dosadíme nyní již známou proměnnou x do jedné ze zadaných kongruencí:

$$\begin{aligned} 2 \cdot 6 \quad +3y &\equiv -2 \pmod{17} \\ 12 \quad +3y &\equiv -2 \pmod{17} \\ 3y &\equiv -14 \pmod{17} \\ 3y &\equiv 3 \pmod{17} \\ y &\equiv 1 \pmod{17} \end{aligned}$$

□

Příklad. Určete primitivní kořeny modulo 23.

Řešení. $\varphi(23) = 22 = 2 \cdot 11$

$$\begin{aligned} g = 2: \quad & 2^2 \equiv 4 \pmod{23} \\ & 2^{11} \equiv (2^5)^2 \cdot 2 \equiv 9^2 \cdot 2 \equiv 9 \cdot 18 \equiv 9 \cdot (-5) \equiv 1 \\ g = 3: \quad & 3^2 \equiv 9 \pmod{23} \\ & 3^{11} \equiv (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv 4^2 \cdot 36 \equiv 4 \cdot 2 \cdot 2 \cdot 13 \equiv 8 \cdot 26 \equiv 1 \pmod{23} \\ g = 4: \quad & \text{řád } 4 = 2^2 \text{ vždy dělí řád } 2 \\ g = 5: \quad & 5^2 \equiv 25 \equiv 2 \pmod{23} \\ & 5^{11} = (5^2)^5 \cdot 5 \equiv 2^5 \cdot 5 \equiv 9 \cdot 5 \equiv 45 \equiv -1 \pmod{23} \end{aligned}$$

Číslo 5 je tedy nejmenším kladným primitivním kořenem modulo 23. Další primitivní kořeny získáme umocněním čísla 5 na čísla nesoudělná s $\varphi(23) = 22$. Obecně totiž, je-li g řádu $\varphi(m)$, je g^n řádu $\frac{\varphi(m)}{(n,\varphi(m))} = \frac{\varphi(m)}{1} = \varphi(m)$ a je tedy rovněž primitivním kořenem, kterých je obecně nekonečně mnoho.
Primitivních kořenů je v redukované soustavě zbytků modulo 23 právě $\varphi(\varphi(23)) = 10$.

$5^3 \equiv 10 \pmod{23}$
$5^5 \equiv 20 \pmod{23}$
$5^7 \equiv 17 \pmod{23}$
$5^9 \equiv 11 \pmod{23}$
$5^{13} \equiv 21 \pmod{23}$
$5^{15} \equiv 19 \pmod{23}$
$5^{17} \equiv 15 \pmod{23}$
$5^{19} \equiv 7 \pmod{23}$
$5^{21} \equiv 14 \pmod{23}$
Primitivními kořeny modulo 23 jsou čísla 5, 7, 10, 11, 14, 15, 17, 19, 20, 21. □

Příklad. Určete $\left(\frac{3}{11}\right)$.

Řešení. $\left(\frac{3}{11}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{11-1}{2}} \cdot \left(\frac{11}{3}\right) = (-1)\left(\frac{2}{3}\right) = (-1)(-1) = 1$ □

Příklad. Nalezněte všechna x splňující kongruenci $x^2 \equiv 7 \pmod{43}$.

Řešení. Nejdříve pomocí Legenrova symbolu rozhodneme, zda je kongruence řešitelná:
$\left(\frac{7}{43}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{43-1}{2}} \cdot \left(\frac{43}{7}\right) = (-1)\left(\frac{1}{7}\right) = (-1)\cdot 1 = -1$
Kongruence tedy není řešitelná; žádné x, které by ji spňovalo, neexistuje. □

Příklad. Vyčíslete Jacobiho symbol $\left(\frac{38}{165}\right)$, a rozhodněte, zda je řešitelná kongruence $x^2 \equiv 38 \pmod{165}$.

Řešení. $\left(\frac{38}{165}\right) = \left(\frac{2}{165}\right)\left(\frac{19}{165}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{11}\right)\left(\frac{19}{3}\right)\left(\frac{19}{5}\right)\left(\frac{19}{11}\right) = (-1)^{\frac{3^2-1}{8}} \cdot (-1)^{\frac{5^2-1}{8}} \cdot (-1)^{\frac{11^2-1}{8}} \cdot \left(\frac{1}{3}\right) \cdot \left(\frac{-1}{5}\right) \cdot \left(\frac{2}{11}\right)^3 = 1$
Kongruenci $x^2 \equiv 38 \pmod{165}$ lze zapsat jako soustavu kongruencí:

$$\begin{aligned} x^2 &\equiv 38 \pmod{3} \\ x^2 &\equiv 38 \pmod{5} \\ x^2 &\equiv 38 \pmod{11}, \end{aligned}$$

což je ekvivalentní soustavě

$$\begin{aligned} x^2 &\equiv -1 \pmod{3} \\ x^2 &\equiv 3 \pmod{5} \\ x^2 &\equiv 5 \pmod{11}. \end{aligned}$$

Z těchto tří kongruencí je řešitelná pouze poslední jmenovaná, celá soustava tak řešení nemá, a nemá ho ani původní kongruence podle složeného modulu. □