9 Řešení kongruencí

9.1. Použijte Euklidův algoritmus pro nalezení největšího společného dělitele následujících čísel.

a) 28 a 93

Najdeme největšího společného dělitele čísel 28 a 93 užitím Euklidova algoritmu.

$$\begin{aligned} 93 &= 28 \cdot 3 + 9 \\ 28 &= 9 \cdot 3 + 1 \\ 9 &= 1 \cdot 9 + 0 \end{aligned}$$

Největší společný dělitel čísel 28 a 93 je 1. Čísla jsou nesoudělná.

Můžeme také zapsat $\mathrm{NSD}(28, 93) = 1$.

b) 175 a 91

Najděme řešení užitím Euklidova algoritmu.

$$\begin{aligned} 175 &= 91 \cdot 1 + 84 \\ 91 &= 84 \cdot 1 + 7 \\ 84 &= 7 \cdot 12 + 0 \end{aligned}$$

Největší společný dělitel čísel 175 a 91 je 7.

Můžeme také zapsat $\mathrm{NSD}(175, 91) = 7$.

9.2. Použijte Euklidův algoritmus pro nalezení Bézoutových koeficientů.

a) Napište $\mathrm{NSD}(243, 49)$ jako lineární kombinaci obou čísel.

Nejprve najdeme největšího společného dělitele čísel 243 a 49 užitím Euklidova algoritmu.

$$\begin{aligned} 243 &= 49 \cdot 4 + 47 \\ 49 &= 47 \cdot 1 + 2 \\ 47 &= 2 \cdot 23 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Zpětným dosazením z (před)poslední rovnice dostaneme

$$1 = 1 \cdot 47 - 2 \cdot 23.$$

Dosazením zbytku 2 z předchozí rovnice dostaneme

$$1 = 1 \cdot 47 - (1 \cdot 49 - 1 \cdot 47) \cdot 23 = 24 \cdot 47 - 23 \cdot 49.$$

Dosazením zbytku 47 z předchozí rovnice dostaneme

$$1 = (1 \cdot 243 - 4 \cdot 49) \cdot 24 - 23 \cdot 49 = 24 \cdot 243 - (23 + 4 \cdot 24) \cdot 49.$$

Protože $1 = 24 \cdot 243 - 119 \cdot 49$, tak hledané Bézoutovy koeficienty jsou 24 a -119.

b) Napište $\mathrm{NSD}(843, 132)$ jako lineární kombinaci obou čísel.

Řešení najdeme užitím Euklidova algoritmu.

$$\begin{aligned} 843 &= 132 \cdot 6 + 51 \\ 132 &= 51 \cdot 2 + 30 \\ 51 &= 30 \cdot 1 + 21 \\ 30 &= 21 \cdot 1 + 9 \\ 21 &= 9 \cdot 2 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

$\mathrm{NSD}(843, 133) = 3$. Zpětným dosazením z (před)poslední rovnice dostaneme

$$3 = 1 \cdot 21 - 2 \cdot 9.$$

Dosazením zbytku 9 z předchozí rovnice dostaneme

$$3 = 1 \cdot 21 - 2 \cdot (1 \cdot 30 - 1 \cdot 21) = 3 \cdot 21 - 2 \cdot 30.$$

Dále dosazením zbytku 21 z předchozí rovnice dostaneme

$$3 = 3 \cdot (1 \cdot 51 - 1 \cdot 30) - 2 \cdot 30 = 3 \cdot 51 - 5 \cdot 30.$$

Dále dosazením zbytku 30 z předchozí rovnice dostaneme

$$3 = 3 \cdot 51 - 5 \cdot (1 \cdot 132 - 2 \cdot 51) = 13 \cdot 51 - 5 \cdot 132.$$

A konečně dosazením zbytku 51 z první rovnice dostaneme

$$3 = 13 \cdot (1 \cdot 843 - 6 \cdot 132) - 5 \cdot 132 = 13 \cdot 843 - 83 \cdot 132.$$

Protože $\mathrm{NSD}(843, 132) = 3 = 13 \cdot 843 - 83 \cdot 132$, tak hledané Bézoutovy koeficienty jsou 13 a -83.

9.3. Najděte inverzi čísla a modulo m.

a) Najděte inverzi čísla 7 modulo 11.

Protože $\mathrm{NSD}(7, 11) = 1$, tak inverze existuje. Inverzi určíme pomocí Euklidova algoritmu.

$$\begin{aligned} 11 &= 1 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Z předposlední rovnice dostaneme

$$1 = 1 \cdot 4 - 1 \cdot 3.$$

Dosazením zbytku 3 z předchozí rovnice dostaneme

$$1 = 1 \cdot 4 - 1 \cdot (1 \cdot 7 - 1 \cdot 4) = 2 \cdot 4 - 1 \cdot 7.$$

Dosazením zbytku 4 z první rovnice dostaneme

$$1 = 2 \cdot (1 \cdot 11 - 1 \cdot 7) - 1 \cdot 7 = 2 \cdot 11 - 3 \cdot 7.$$

Nyní víme

$$1 = 2 \cdot 11 - 3 \cdot 7 \equiv (-3) \cdot 7 \pmod{11}$$

Inverze čísla 7 modulo 11 je číslo $-3 \equiv 8 \pmod{11}$.

Snadno ověříme, že $8 \cdot 7 = 56 \equiv 1 \pmod{11}$.

b) Najděte inverzi čísla 78 modulo 15.

Protože $\mathrm{NSD}(87, 15) = 3 > 1$, tak inverze neexistuje.

c) Najděte inverzi čísla 78 modulo 25.

Protože $\mathrm{NSD}(78, 25) = 1$, tak inverze existuje. Inverzi určíme pomocí Euklidova algoritmu.

$$\begin{aligned} 78 &= 25 \cdot 3 + 3 \\ 25 &= 3 \cdot 8 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Z předposlední rovnice dostaneme

$$1 = 1 \cdot 25 - 3 \cdot 8.$$

Dosazením zbytku 3 z první rovnice dostaneme

$$1 = 1 \cdot 25 - (1 \cdot 78 - 3 \cdot 25) \cdot 8 = 25 \cdot 25 - 8 \cdot 78.$$

Nyní víme

$$1 = 25 \cdot 25 - 8 \cdot 78 \equiv (-8) \cdot 78 \pmod{25}$$

Inverze čísla 78 modulo 25 je číslo $-8 \equiv 17 \pmod{25}$.

Snadno ověříme, že $17 \cdot 87 = 1326 \equiv 1 \pmod{25}$.

9.4. Najděte všechna řešení uvedené lineární kongruence.

a) Vyřešte lineární kongruenci $3x - 4 \equiv 7 \pmod{13}$.

Převedeme 4 na pravou stranu.

$$3x \equiv 11 \pmod{13}$$

Dále můžeme k pravé straně přičíst 13 a dostaneme

$$3x \equiv 24 \pmod{13}.$$

Díky předchozímu kroku můžeme nyní celou kongruenci krátit číslem 3 nesoudělným s modulem

$$x \equiv 8 \pmod{13}$$

a dostaneme řešení $x = 13t + 8$, kde $t \in \mathbb{Z}$.

b) $x \equiv 563 \pmod{7}$

Kongruenci nejprve zjednodušíme. Protože $563 = 7 \cdot 80 + 3$, tak obecné řešení kongruence $x \equiv 563 \equiv 3 \pmod{7}$ jsou všechna čísla, která dávají zbytek 3 po dělení 7, tedy $x = 7t + 3$, kde $t \in \mathbb{Z}$.

c) $x \equiv -174 \pmod{12}$

Kongruenci nejprve zjednodušíme. Protože $-174 = -180 + 6$, tak obecné řešení kongruence $x \equiv -174 \equiv 6 \pmod{12}$ jsou všechna čísla, která dávají zbytek 6 po dělení 12, tedy $x = 12t + 6$, kde $t \in \mathbb{Z}$.

d) $2x \equiv 7 \pmod{12}$

Při řešení kongruence bychom hledali inverzi čísla 2 modulo 12. Avšak $\mathrm{NSD}(2, 12) = 2 \neq 1$, a proto číslo 2 nemá inverzi modulo 12. Kongruence nemá řešení.

Jiné řešení:

Všimneme si, že levá strana je vždy sudé číslo, které po dělení 12 nikdy nemůže dát (lichý) zbytek 7. Navíc v kongruenci nemůžeme ani krátit. Kongruence nemá řešení.

e) $2x \equiv 6 \pmod{12}$

Číslo 2 nemá inverzi modulo 12, protože $\mathrm{NSD}(2, 12) = 2 \neq 1$. Kongruenci však můžeme nejprve zjednodušit. Krátíme obě strany i modul číslem 2. Dostaneme $x \equiv 3 \pmod{6}$. Obecné řešení dané kongruence jsou všechna čísla $x = 6t + 3$, kde $t \in \mathbb{Z}$.

f) $2x \equiv 13 \pmod{11}$

Najdeme inverzi čísla 2 modulo 9. Protože $\mathrm{NSD}(2, 11) = 1$, tak inverze existuje. Pomocí Euklidova algoritmu počítáme

$$\begin{aligned} 11 &= 5 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Z předposlední rovnice dostaneme

$$1 = 1 \cdot 11 - 5 \cdot 2.$$

Nyní víme

$$1 = 1 \cdot 11 - 5 \cdot 2 \equiv (-5) \cdot 2 \equiv 6 \cdot 2 \pmod{11}$$

Inverze čísla 2 modulo 11 je číslo 6.

Obě strany kongruence roznásobíme inverzí 6 a dostaneme

$$\begin{aligned} 6 \cdot 2x &\equiv 6 \cdot 13 \pmod{11} \\ 1x &\equiv 78 \pmod{11} \\ x &\equiv 1 \pmod{11}. \end{aligned}$$

Obecné řešení dané kongruence jsou všechna čísla $x = 11t + 1$, kde $t \in \mathbb{Z}$.

Jiné řešení:

Najdeme inverzi čísla 2 modulo 11. Všimneme si, že $6 \cdot 2 = 12 \equiv 1 \pmod{11}$, a proto číslo 6 je inverzí čísla 2 modulo 11. Obě strany kongruence roznásobíme inverzí 6 a dostaneme

$$\begin{aligned} 6 \cdot 2x &\equiv 6 \cdot 13 \pmod{11} \\ 1x &\equiv 78 \pmod{11} \\ x &\equiv 1 \pmod{11}. \end{aligned}$$

Obecné řešení dané kongruence jsou všechna čísla $x = 11t + 1$, kde $t \in \mathbb{Z}$.

Jiné řešení:

Kongruenci nejprve zjednodušíme. Odečteme modul 11 od pravé strany (kongruence se nezmění, neboť $11 \equiv 0 \pmod{11}$). Upravíme

$$\begin{aligned} 2x &\equiv 13 - 11 \pmod{11} \\ 2x &\equiv 2 \pmod{11} \\ x &\equiv 1 \pmod{11}, \end{aligned}$$

kde obě strany jsme krátili číslem 2 nesoudělným s modulem. Obecné řešení dané kongruence jsou všechna čísla $x = 11t + 1$, kde $t \in \mathbb{Z}$.

9.5. Maminka klade na pekáč makové buchty. Když má v každé řadě 4 buchty, tak jedna buchta přebývá, když má v každé řadě 5 buchet, tak 3 chybí. Víme, že maminka na oslavu obvykle připraví něco mezi dvaceti a čtyřiceti buchtami. Kolik udělala maminka buchet?

Označíme počet buchet jako b a sestavíme soustavu kongruencí, která pro počet buchet dle zadání platí. Z informace, že když jsou v každé řadě 4 buchty, tak jedna buchta přebývá dostaneme rovnici

$$b \equiv 1 \pmod{4}.$$

Z informace, že když je v každé řadě 5 buchet, tak 3 buchty chybí dostaneme rovnici

$$b \equiv -3 \pmod 5.$$

Tuto soustavu kongruencí vyřešíme. Vyjádříme řešení první kongruence $b = 4t + 1$, kde $t \in \mathbb{Z}$, a dosadíme jej do druhé kongruence. Dostaneme

$$\begin{aligned} b &\equiv -3 \pmod 5 \\ 4t + 1 &\equiv -3 \pmod 5 \\ 4t &\equiv -4 \pmod 5 \\ t &\equiv -1 \pmod 5 \\ t &\equiv 4 \pmod 5. \end{aligned}$$

Řešení druhé kongruence tedy je $t = 5u + 4$, kde $u \in \mathbb{Z}$. Řešení druhé kongruence dosadíme do řešení první kongruence a dostaneme

$$b = 4t + 1 = 4(5u + 4) + 1 = 20u + 17, \quad u \in \mathbb{Z}.$$

V zadaném intervalu $[20, 40]$ existuje jediné řešení $b = 37$.