Příklad na lineární kongruenci

Vyřešte lineární kongruenci $15x \equiv 9 \pmod{51}$.

Příklad na lineární kongruenci

Vyřešte lineární kongruenci $15x \equiv 9(\mod 51)$.
Nejprve zjistíme, zda zadaná kongruence má řešení.

Příklad na lineární kongruenci

Vyřešte lineární kongruenci $15x \equiv 9(\mod 51)$.
Nejprve zjistíme, zda zadaná kongruence má řešení.

$$\gcd(15, 51) = 3$$

Příklad na lineární kongruenci

Vyřešte lineární kongruenci $15x \equiv 9(\mod 51)$.
Nejprve zjistíme, zda zadaná kongruence má řešení.

$$\gcd(15, 51) = 3$$

a číslo 3 je dělitelem čísla 9.

Příklad na lineární kongruenci

Vyřešte lineární kongruenci $15x \equiv 9(\mod 51)$.
Nejprve zjistíme, zda zadaná kongruence má řešení.

$$\gcd(15, 51) = 3$$

a číslo 3 je dělitelem čísla 9. Proto zadaná kongruence má řešení a budou tři různá (kdyby 3 nedělila číslo 9, pak by řešení neexistovalo).

Příklad na lineární kongruenci

Řešíme lineární kongruenci $15x \equiv 9 \pmod{51}$.

Příklad na lineární kongruenci

Řešíme lineární kongruenci $15x \equiv 9(\mod 51)$. Zjistili jsme, že číslo 3 dělí čísla 15, 9 i 51.

Příklad na lineární kongruenci

Řešíme lineární kongruenci $15x \equiv 9(\mod 51)$. Zjistili jsme, že číslo 3 dělí čísla 15, 9 i 51. V zadané kongruenci všechna čísla podělíme číslem 3.

Příklad na lineární kongruenci

Řešíme lineární kongruenci $15x \equiv 9(\mod 51)$. Zjistili jsme, že číslo 3 dělí čísla 15, 9 i 51. V zadané kongruenci všechna čísla podělíme číslem 3. Obdržíme tak kongruenci

$$5x \equiv 3(\mod 17)$$

Příklad na lineární kongruenci

Řešíme lineární kongruenci $15x \equiv 9(\mod 51)$. Zjistili jsme, že číslo 3 dělí čísla 15, 9 i 51. V zadané kongruenci všechna čísla podělíme číslem 3. Obdržíme tak kongruenci

$$5x \equiv 3(\mod 17)$$

Tato kongruence má jediné řešení - označme jej x_0 - neboť $\gcd(5, 17) = 1$.

Příklad na lineární kongruenci

Řešíme lineární kongruenci $15x \equiv 9(\mod 51)$. Zjistili jsme, že číslo 3 dělí čísla 15, 9 i 51. V zadané kongruenci všechna čísla podělíme číslem 3. Obdržíme tak kongruenci

$$5x \equiv 3(\mod 17)$$

Tato kongruence má jediné řešení - označme jej x_0 - neboť $\gcd(5, 17) = 1$.
Nalezneme jej.

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3(\mod 17)$.

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3(\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3(\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$17 = 3 \cdot 5 + 2$$

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3(\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3(\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3 (\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{array}{rcl} 17 & = & 3 \cdot 5 + 2 \\ 5 & = & 2 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \end{array} \quad \Rightarrow \quad 1 \quad = \quad 5 - 2 \cdot 2$$

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3(\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{array}{rcl@{\quad\Rightarrow\quad}rcl} 17 & = & 3 \cdot 5 + 2 & 1 & = & 5 - 2 \cdot (17 - 3 \cdot 5) \\ 5 & = & 2 \cdot 2 + 1 & 1 & = & 5 - 2 \cdot 2 \\ 2 & = & 2 \cdot 1 + 0 & & & \end{array}$$

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3 (\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{array}{rcl} 17 & = & 3 \cdot 5 + 2 \\ 5 & = & 2 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} 1 & = & 5 - 2 \cdot (17 - 3 \cdot 5) \\ 1 & = & 5 - 2 \cdot 2 \end{array}$$

Z posledně zjištěné rovnosti určíme, že

$$1 = 7 \cdot 5 - 2 \cdot 17.$$

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3 (\mod 17)$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{array}{rcl} 17 & = & 3 \cdot 5 + 2 \\ 5 & = & 2 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} 1 & = & 5 - 2 \cdot (17 - 3 \cdot 5) \\ 1 & = & 5 - 2 \cdot 2 \end{array}$$

Z posledně zjištěné rovnosti určíme, že

$$1 = 7 \cdot 5 - 2 \cdot 17.$$

Odtud $3 = 21 \cdot 5 - 6 \cdot 17$.

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3 \pmod{17}$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{array}{rcl} 17 & = & 3 \cdot 5 + 2 \\ 5 & = & 2 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} 1 & = & 5 - 2 \cdot (17 - 3 \cdot 5) \\ 1 & = & 5 - 2 \cdot 2 \end{array}$$

Z posledně zjištěné rovnosti určíme, že

$$1 = 7 \cdot 5 - 2 \cdot 17.$$

Odtud $3 = 21 \cdot 5 - 6 \cdot 17$. Proto $3 \equiv 21 \cdot 5 \pmod{17}$ a vidíme,

Příklad na lineární kongruenci

Hledáme řešení x_0 kongruence $5x \equiv 3 \pmod{17}$. Vyjádříme číslo $1 = \gcd(5, 17)$ jako lineární kombinaci čísel 5 a 17. A to zpětným vyjádřením z Euklidova algoritmu pro nalezení $\gcd(5, 17)$:

$$\begin{array}{rcl} 17 & = & 3 \cdot 5 + 2 \\ 5 & = & 2 \cdot 2 + 1 \\ 2 & = & 2 \cdot 1 + 0 \end{array} \quad \Rightarrow \quad \begin{array}{rcl} 1 & = & 5 - 2 \cdot (17 - 3 \cdot 5) \\ 1 & = & 5 - 2 \cdot 2 \end{array}$$

Z posledně zjištěné rovnosti určíme, že

$$1 = 7 \cdot 5 - 2 \cdot 17.$$

Odtud $3 = 21 \cdot 5 - 6 \cdot 17$. Proto $3 \equiv 21 \cdot 5 \pmod{17}$ a vidíme, že $\overline{x_0}_{17} = \overline{21}_{17} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3 \pmod{17}$.

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3(\mod 17)$.

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3(\mod 17)$. Řešeními zadané kongruence $15x \equiv 9(\mod 51)$ jsou proto zbytkové třídy:

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3(\mod 17)$. Řešeními zadané kongruence $15x \equiv 9(\mod 51)$ jsou proto zbytkové třídy:

$$\overline{x} =$$

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3 \pmod{17}$.
Řešeními zadané kongruence $15x \equiv 9 \pmod{51}$ jsou proto zbytkové třídy:

$$\nearrow \quad = \quad \overline{4 + 0 \cdot 17}_{51} \quad = \quad \overline{\mathbf{4}}_{51}$$

$$\overline{x} =$$

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3 \pmod{17}$. Řešeními zadané kongruence $15x \equiv 9 \pmod{51}$ jsou proto zbytkové třídy:

$$\nearrow \;=\; \overline{4 + 0 \cdot 17}_{51} \;=\; \overline{\mathbf{4}}_{51}$$

$$\overline{x} = \quad \rightarrow \;=\; \overline{4 + 1 \cdot 17}_{51} \;=\; \overline{\mathbf{21}}_{51}$$

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3 \pmod{17}$.
Řešeními zadané kongruence $15x \equiv 9 \pmod{51}$ jsou proto zbytkové třídy:

$$\begin{array}{rccccc} & \nearrow & = & \overline{4 + 0 \cdot 17}_{51} & = & \overline{\mathbf{4}}_{51} \\ \overline{x} = & \rightarrow & = & \overline{4 + 1 \cdot 17}_{51} & = & \overline{\mathbf{21}}_{51} \\ & \searrow & = & \overline{4 + 2 \cdot 17}_{51} & = & \overline{\mathbf{38}}_{51} \end{array}$$

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3(\mod 17)$. Řešeními zadané kongruence $15x \equiv 9(\mod 51)$ jsou proto zbytkové třídy:

$$\begin{array}{rcccc} & \nearrow & = & \overline{4 + 0 \cdot 17}_{51} & = & \overline{\mathbf{4}}_{51} \\ \overline{x} = & \rightarrow & = & \overline{4 + 1 \cdot 17}_{51} & = & \overline{\mathbf{21}}_{51} \\ & \searrow & = & \overline{4 + 2 \cdot 17}_{51} & = & \overline{\mathbf{38}}_{51} \end{array}$$

$\overline{4 + 3 \cdot 17}_{51} = \overline{55}_{51}$ je zase zbytková třída $\overline{4}_{51}$, proto dále nepokračujeme -

Příklad na lineární kongruenci

Zjistili jsme, že $\overline{x_0} = \overline{4}_{17}$ je řešením kongruence $5x \equiv 3(\mod 17)$. Řešeními zadané kongruence $15x \equiv 9(\mod 51)$ jsou proto zbytkové třídy:

$$\begin{array}{rccccc} & \nearrow & = & \overline{4 + 0 \cdot 17}_{51} & = & \overline{4}_{51} \\ \overline{x} = & \rightarrow & = & \overline{4 + 1 \cdot 17}_{51} & = & \overline{21}_{51} \\ & \searrow & = & \overline{4 + 2 \cdot 17}_{51} & = & \overline{38}_{51} \end{array}$$

$\overline{4 + 3 \cdot 17}_{51} = \overline{55}_{51}$ je zase zbytková třída $\overline{4}_{51}$, proto dále nepokračujeme - nalezli jsme již všechna řešení zadané kongruence