Př. Určete $\gcd(a,b)$ a vyjádřete $\gcd(a,b)$ jako lineární kombinaci čísel a a b.

1.) $a = 328 \quad b = 421$

$421 = 1 \cdot 328 + 93$
$328 = 3 \cdot 93 + 49$
$93 = 1 \cdot 49 + 44$
$49 = 1 \cdot 44 + 5$
$44 = 8 \cdot 5 + 4$
$5 = 1 \cdot 4 + \textcircled{1} = \gcd(328, 421)$
$4 = 4 \cdot 1 + 0$

$\Rightarrow$

$1 = 5 - 1 \cdot 4 =$
$= 5 - 1 \cdot (44 - 8 \cdot 5) = -1 \cdot 44 + 9 \cdot 5 =$
$= -1 \cdot 44 + 9 \cdot (49 - 1 \cdot 44) = 9 \cdot 49 - 10 \cdot 44 =$
$= 9 \cdot 49 - 10 (93 - 1 \cdot 49) = 19 \cdot 49 - 10 \cdot 93 =$
$= -10 \cdot 93 + 19 (328 - 3 \cdot 93) = 19 \cdot 328 - 67 \cdot 93$
$= 19 \cdot 328 - 67 (421 - 328) = \underline{-67 \cdot 421 + 86 \cdot 328}$

2.) $a = 385 \quad b = 273$

$385 = 1 \cdot 273 + 112$
$273 = 2 \cdot 112 + 49$
$112 = 2 \cdot 49 + 14$
$49 = 3 \cdot 14 + \textcircled{7} = \gcd(385, 273)$
$14 = 2 \cdot 7 + 0$

$\Rightarrow$

$7 = 49 - 3 \cdot 14 = 49 - 3 (112 - 2 \cdot 49) =$
$= -3 \cdot 112 + 7 \cdot 49 = -3 \cdot 112 + 7 (273 - 2 \cdot 112) =$
$= 7 \cdot 273 - 17 \cdot 112 = 7 \cdot 273 - 17 (385 - 273) =$
$= \underline{-17 \cdot 385 + 24 \cdot 273}$

3.) $a = 520 \quad b = 221$

$520 = 2 \cdot 221 + 78$
$221 = 2 \cdot 78 + 65$
$78 = 1 \cdot 65 + \textcircled{13} = \gcd(520, 221)$

$\Rightarrow$

$13 = 78 - 65 = 78 - (221 - 2 \cdot 78) =$
$= -1 \cdot 221 + 3 \cdot 78 = -1 \cdot 221 + 3 (520 - 2 \cdot 221) =$
$= \underline{3 \cdot 520 - 7 \cdot 221}$

4.) $a = 1321 \quad b = 600$

$1321 = 2 \cdot 600 + 121$
$600 = 4 \cdot 121 + 116$
$121 = 1 \cdot 116 + 5$
$116 = 23 \cdot 5 + \textcircled{1} = \gcd(1321, 600)$

$\Rightarrow$

$1 = 116 - 23 \cdot 5 = 116 - 23 (121 - 116) =$
$= -23 \cdot 121 + 24 \cdot 116 = -23 \cdot 121 + 24 (600 - 4 \cdot 121) =$
$= 24 \cdot 600 - 119 \cdot 121 = 24 \cdot 600 - 119 (1321 - 2 \cdot 600) =$
$= \underline{-119 \cdot 1321 + 262 \cdot 600}$

Př: Vyřešte lineární kongruenci $ax \equiv b \pmod m$

a) $3x \equiv 5 \pmod{18}$

$\gcd(3,18) = 3$ ale $3 \nmid 5$ $\Rightarrow$ nemá řešení

b) $5x \equiv 6 \pmod 8$

1.) Určíme $\gcd(5,8)$ pomocí eukl. algoritmu:

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$ $\Rightarrow$ kongruence má jedno řešení

$2 = 2 \cdot 1 + 0$

2.) Zpětně vyjádříme $\gcd(5,8) = 1$ z rovnic eukl. algoritmu:

$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = (8 - 1 \cdot 5) - 1 \cdot (5 - (8-5)) =$

$= 8 - 5 - 5 + 8 - 5 = 2 \cdot 8 - 3 \cdot 5$

$2 \cdot 8 - 3 \cdot 5 = 1$

3.) Obdrženou rovnici vynásobíme číslem $b = 6$

$12 \cdot 8 - 18 \cdot 5 = 6$ / kon. $\pmod 8$

$12 \cdot 8 - 18 \cdot 5 \equiv 6 \pmod 8$

$0 \quad 6$

$5 \cdot 6 \equiv 6 \pmod 8$ $\Rightarrow$ $x \equiv 6 \pmod 8$

x

b) $12X \equiv 31 \pmod{35}$

1.) $\gcd(12, 35)$:

$35 = 2 \cdot 12 + 11$

$12 = 1 \cdot 11 + 1 \Rightarrow$ kongruence má 1 řešení

$11 = 11 \cdot 1 + 0$

2.) Vyjádříme číslo $1 = \gcd(12, 35)$:

$1 = 12 - 11 = 12 - (35 - 2 \cdot 12) = 3 \cdot 12 - 35 \Rightarrow$

$3 \cdot 12 - 35 = 1$

3.) Vynásobíme číslem $b = 31$:

$93 \cdot 12 - 31 \cdot 35 = 31 \quad / \pmod{35}$

$12 \cdot 93 - 31 \cdot 35 \equiv 31 \pmod{35}$

$93 \equiv 23$

$12 \cdot 23 \equiv 31 \pmod{35} \Rightarrow \underline{X \equiv 23 \pmod{35}}$

Zk: $12 \cdot 23 = 276 \equiv 66 \equiv 31 \pmod{35}$ ✓

c) $12x \equiv 9 \pmod{15}$

1.) Určíme $\gcd(12,15)$: $15 = 1 \cdot 12 + 3 \Rightarrow$ kongruence má 3 řešení!
$12 = 4 \cdot 3 + 0$

a platí $12x \equiv 9 \pmod{15} \Leftrightarrow 4x \equiv 3 \pmod{5}$

2.) Vyřešíme kongruenci $4x \equiv 3 \pmod{5}$

I.) $\gcd(4,5)$: $5 = 1 \cdot 4 + 1 = \gcd(4,5) \Rightarrow$ jednořešení!
$4 = 4 \cdot 1 + 0$

II.) Vyjádříme 1: $1 = 5 - 4 \Rightarrow 1 \cdot 5 - 1 \cdot 4 = 1$

III.) Vynásobíme číslem 3: $3 \cdot 5 - 3 \cdot 4 = 3 \quad / \pmod 5$

$3 \cdot \underset{\equiv 0}{5} - \underset{\equiv 2}{3} \cdot 4 \equiv 3 \pmod 5$

$4 \cdot 2 \equiv 3 \pmod 5 \Rightarrow x = \overline{2}_5 \Rightarrow$

$x = 2, 7, 12, 17 \ldots$

$\Rightarrow x \equiv \begin{cases} 2 \pmod{15} \\ 7 \pmod{15} \\ 12 \pmod{15} \end{cases}$

Zk: $12 \cdot 2 = 24 \equiv 9 \pmod{15}$ ✓
$12 \cdot 7 = 84 \equiv 24 \equiv 9 \pmod{15}$ ✓
$12 \cdot 12 = 144 \equiv 24 \equiv 9 \pmod{15}$ ✓

d) $18x \equiv 25 \pmod{49}$

$49 = 2 \cdot 18 + 13$

$18 = 1 \cdot 13 + 5$

$13 = 2 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1 = \gcd(18, 49)$

$\Rightarrow$ ∃! řešení

$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 =$

$= 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5 =$

$= 2 \cdot 13 - 5(18 - 13) = 7 \cdot 13 - 5 \cdot 18 =$

$= 7 \cdot (49 - 2 \cdot 18) - 5 \cdot 18 = 7 \cdot 49 - 19 \cdot 18$ $\Rightarrow$

$1 = 7 \cdot 49 - 19 \cdot 18 \quad / \cdot 25$

$25 = 25 \cdot 7 \cdot 49 - 475 \cdot 18 \pmod{49}$

$475 \equiv 15 \pmod{49}$

$49 \equiv 0 \pmod{49}$

$25 \equiv 15 \cdot 18 \pmod{49}$

$15 = x$

$\underline{x \in \overline{15}_{49}}$

e) $42x \equiv 24 \pmod{72}$

$\gcd(72, 42) = 6 \Rightarrow$ řešíme $7x \equiv 4 \pmod{12} \Rightarrow \gcd(12, 7) = 1 = 3 \cdot 12 - 5 \cdot 7$

$4 = 12 \cdot 12 - 20 \cdot 7$

$4 \equiv -20 \cdot 7 \pmod{12}$

$4 \equiv 4 \cdot 7 \pmod{12}$

$\Rightarrow x \in \overline{4}_{12} = \underline{\overline{4}_{72} \cup \overline{16}_{72} \cup \overline{28}_{72} \cup \overline{40}_{72} \cup \overline{52}_{72} \cup \overline{64}_{72}}$

Př. Na množině $G = \{\bar{1}_5, \bar{2}_5, \bar{3}_5, \bar{4}_5\}$ zavedeme násobení předpisem:

$$\forall \bar{a}_5, \bar{b}_5 \in G: \quad \bar{a}_5 \cdot \bar{b}_5 = \overline{a \cdot b}_5$$ (tj. násobení modulo 5)

a) Nalezněte prvek inverzní k prvku $\bar{2}_5$

- to jest zbytkovou třídu $\bar{x}_5$ splňující $\bar{2}_5 \cdot \bar{x}_5 = \bar{1}_5$

Hledáme proto $x \in \mathbb{Z}$ splňující $2 \cdot x \equiv 1 \pmod 5$

$\gcd(2,5) = 1 \Rightarrow$ řešení této kongruence je jediné, a to

$$\underline{\bar{x}_5 = \bar{3}_5}$$

Značíme $\bar{2}_5^{-1} = \bar{3}_5$.

b) Dokažte, že $\forall \bar{a}_5 \in G \quad \exists! \, \bar{a}_5^{-1} \in G$

$\bar{a}_5^{-1} = \bar{x}_5 \iff (a)\ x \equiv 1 \pmod{(5)}$

$\gcd(a, 5) = 1$, neboť 5 je prvočíslo $(\forall a \in \{1,2,3,4\}) \Rightarrow$

$\forall \bar{a}_5 \in G \quad \exists!$ řešení kongruence $ax \equiv 1 \pmod 5$

c) Určete tabulku násobení na G.

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\Rightarrow$

$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$

Pro jednoduchost zápisu místo $\bar{a}_5$ píšeme jen a.

Př. Na množině $G = \{\bar{1}_{18}, \bar{2}_{18}, \dots, \overline{17}_{18}\}$ zavedeme násobení:

$$\forall \bar{a}_{18}, \bar{b}_{18} \in G: \quad \bar{a}_{18} \cdot \bar{b}_{18} = \overline{a.b}_{18}$$

Nalezněte všechny prvky z G, které nemají inverzní prvek.

Víme, že $\bar{x}_{18} = \bar{a}^{-1}_{18} \iff x \cdot a \equiv 1 \pmod{18}$

Tato kongruence má řešení $\iff \gcd(a, 18) \mid 1 \iff$

$\iff \gcd(a, 18) = 1$

$\Rightarrow$ Inverzi mají právě ty zbytkové třídy $\bar{a}_{18}$, kde $\gcd(a, 18) = 1$.

$\Rightarrow$ Inverzi nemají zbytkové třídy:

$$\bar{2}_{18}, \bar{3}_{18}, \bar{4}_{18}, \bar{6}_{18}, \bar{8}_{18}, \bar{9}_{18}, \bar{10}_{18}, \bar{12}_{18}, \bar{14}_{18}, \bar{15}_{18}, \bar{16}_{18}$$

Př: Nechť $(G, \cdot)$ je grupa, kde $G = \mathbb{Z}_{43} - \{\bar{0}\}$ ... zbytkové třídy modulo 43 bez $\bar{0}$ a $\cdot$ je násobení modulo 43.

Určete inverzní prvek vzhledem k prvku $\overline{28}$.

Řešení: Hledáme $\bar{X} = \overline{28}^{-1}$. To jest, zbytkovou třídu $\bar{X}$ splňující:

$$\bar{X} \cdot \overline{28} = \bar{1}$$

To můžeme zapsat pomocí kongruence takto:

$$X \cdot 28 \equiv 1 \pmod{43} \quad (*)$$

Najít $\bar{x}$ je proto ekvivalentní vyřešení kongruence $(*)$

1.) $\gcd(28, 43)$:

$$43 = 1 \cdot 28 + 15$$
$$28 = 1 \cdot 15 + 13$$
$$15 = 1 \cdot 13 + 2$$
$$13 = 6 \cdot 2 + \textcircled{1} \Rightarrow \text{kongruence má řešení}$$
$$2 = 2 \cdot 1 + 0$$

$$1 = 13 - 6 \cdot \textcircled{2} = \textcircled{13} - 6 \cdot (15 - \textcircled{13}) = (28 - \textcircled{15}) - 6(\textcircled{15} - (28 - \textcircled{15})) =$$

$$= (28 - (43 - 28)) - 6((43 - 28) - (28 - (43 - 28))) =$$

$$= 28 - 43 + 28 - 6 \cdot 43 + 6 \cdot 28 + 6 \cdot 28 - 6 \cdot 43 + 6 \cdot 28 =$$

$$1 = 20 \cdot 28 - 13 \cdot 43 \quad / \pmod{43}$$

$$1 \equiv \boxed{20} \cdot 28 \pmod{43}$$

$$\Downarrow$$

$$\bar{X} = \overline{20}$$

Zk: $20 \cdot 28 = 560 \equiv 130 = 1 \pmod{43}$