**Poznámka.** *Pro připomenutí, $a \equiv b \ (mod\ c)$ znamená, že $a, b$ dávají stejný zbytek po dělení číslem $c$. Můžeme tomu rozumět i tak, že $c$ dělí $a - b$, nebo $a = kc + b$, pro $k \in \mathbb{Z}$.*

*Kongruence podle téhož modulu můžeme sčítat i odečítat, také násobit. Tedy pro $a \equiv b \ (mod\ m)$ a $c \equiv d \ (mod\ m)$ platí*

- $a + c \equiv b + d \ (mod\ m)$,
- $a - c \equiv b - d \ (mod\ m)$,
- $ac \equiv bd \ (mod\ m)$.

*Obě strany kongruence můžeme umocnit na stejné číslo. Obě strany kongruence můžeme vydělit jejich společným dělitelem, pokud je to číslo nesoudělné s modulem. Pokud jsou obě strany i modul soudělné, lze vydělit všechna tři čísla.*

*Tuto teoretickou výbavu není nutno memorovat, považuji za ideální si ji zkusit na co nejvíce příkladech a u toho se poučit i o tom, co při kongruencích neplatí. Proto zde předkládám několik vyřešených příkladů (lineární kongruence a jejich soustavy) jako doplnění komentovaných slidů pana docenta Vokřínka.*

*Vidíte-li zadání s tím, že tušíte jak to spočítat, zkuste si to prosím nejprve spočítat sami a poté zkontrolovat. Způsobů řešení a cest k výsledku je spousta.*

**Příklad 1.** *Spočtěte $14x \equiv 19 \ (mod\ 23)$.*

*Řešení.* Vidíme, že $(23, 14) = 1$ a samozřejmě $1 \mid 19$, tedy kongruence má právě jedno řešení modulo 23.

1. Mohli bychom obě strany vynásobit $14^{-1} \ (mod\ 23)$. Již víme, že tato inverze existuje.

$$\begin{aligned} 23 &= 1 \cdot 14 + 9 \\ 14 &= 1 \cdot 9 + 5 \\ 9 &= 1 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \end{aligned}$$

Proto $1 = 5-4 = 5-(9-5) = 2\cdot 5-9 = 2(14-9)-9 = 2\cdot 14-3\cdot 9 = 2\cdot 14-3(23-14) = 5\cdot 14-3\cdot 23$. Máme tedy $5 \cdot 14 - 3 \cdot 23 = 1$, z toho plyne $5 \cdot 14 \equiv 1 \ (mod\ 23)$.

$$\begin{aligned} 14x &\equiv 19 \ (mod\ 23) \\ 5 \cdot 14x &\equiv 5 \cdot 19 \ (mod\ 23) \\ x &\equiv 5 \cdot (-4) \equiv -20 \equiv 3 \ (mod\ 23) \\ x &\equiv 3 \ (mod\ 23) \end{aligned}$$

2. Můžeme využít Eulerovu větu $a^{\varphi(n)} \equiv 1 \ (mod\ n)$. Víme, že $14^{22} \equiv 1 \ (mod\ 23)$.

$$\begin{aligned} 14^{21} \cdot 14x &\equiv 14^{21} \cdot 19 \ (mod\ 23) \\ x &\equiv 2^{21} \cdot 7^{21} \cdot (-4) \ (mod\ 23) \\ x &\equiv 2^6 \cdot 2^6 \cdot 2^6 \cdot 2^3 \cdot (7^2)^{10} \cdot 7 \cdot (-4) \ (mod\ 23) \\ x &\equiv (-5) \cdot (-5) \cdot (-5) \cdot 8 \cdot (3)^{10} \cdot 7 \cdot (-4) \ (mod\ 23) \\ x &\equiv 25 \cdot 20 \cdot 8 \cdot (3^3)^3 \cdot 3 \cdot 7 \ (mod\ 23) \\ x &\equiv 25 \cdot 20 \cdot 24 \cdot (4)^3 \cdot 7 \ (mod\ 23) \\ x &\equiv 25 \cdot 20 \cdot 24 \cdot (-5) \cdot 7 \ (mod\ 23) \\ x &\equiv 2 \cdot (-3) \cdot 1 \cdot (-5) \cdot 7 \ (mod\ 23) \\ x &\equiv (-6) \cdot (-5) \cdot 7 \ (mod\ 23) \\ x &\equiv 30 \cdot 7 \ (mod\ 23) \\ x &\equiv 7 \cdot 7 \ (mod\ 23) \\ x &\equiv 49 - 2 \cdot 23 \equiv 3 \ (mod\ 23) \\ x &\equiv 3 \ (mod\ 23) \end{aligned}$$

3. Dalším způsobem je upravování levé i pravé strany pomocí modulu a dělení. Je to snad nejrychlejší způsob, ale vyžaduje více zkušenosti. Občas to může být na pár řádků, jindy se tento způsob může až nechutně protáhnout a skoro nevede k výsledku. Může to ovšem posloužit aspoň ke zjednodušení příkladu. V tomto konkrétním příkladě:

$$\begin{aligned} 14x &\equiv 19 \ (mod\ 23) \\ 14x &\equiv (-4) \ (mod\ 23) \\ 7x &\equiv (-2) \ (mod\ 23) \\ 7x &\equiv (-2) + 23 = 21 \ (mod\ 23) \\ x &\equiv 3 \ (mod\ 23) \end{aligned}$$

4. Poslední uvedený způsob je upravování dvou kongruencí (známo ze slidů), takže jen stručně:

$$\begin{aligned} 23x &\equiv 0 \ (mod\ 23) \\ 14x &\equiv 19 \ (mod\ 23) \\ 9x &\equiv -19 + 23 = 4 \ (mod\ 23) \\ 5x &\equiv 15 \ (mod\ 23) \\ 4x &\equiv -11 \ (mod\ 23) \\ x &\equiv 26 \equiv 3 \ (mod\ 23) \\ 0x &\equiv -11 - 3 \cdot 4 = -23 \equiv 0 \ (mod\ 23). \end{aligned}$$

□

**Příklad 2.** *Spočtěte* $37x \equiv 17 \ (mod\ 27)$.

*Řešení.* Předveďme si pouze třetí způsob.

$$\begin{aligned} 37x &\equiv 17 \ (mod\ 27) \\ 10x &\equiv -10 \ (mod\ 27) \\ x &\equiv -1 \ (mod\ 27) \\ x &\equiv 26 \ (mod\ 27) \end{aligned}$$

□

**Příklad 3.** *Spočtěte* $13x \equiv 22 \ (mod\ 36)$.

*Řešení.* Lze to spočítat třetím způsobem? Zde už to není tak jednoduché, jako v předchozím příkladě. Zkuste proto spočítat jiným způsobem.

$$\begin{aligned} 13x &\equiv 22 \ (mod\ 36) \\ ?x &\equiv ? \ (mod\ 36) \end{aligned}$$

□

**Příklad 4.** *Spočtěte* $121x \equiv 250 \ (mod\ 160)$.

*Řešení.* Předveďme si pouze třetí způsob.

$$\begin{aligned} 121x &\equiv 250 \ (mod\ 160) \\ -39x &\equiv 90 \ (mod\ 160) \\ -13x &\equiv 30 \ (mod\ 160) \\ -13x &\equiv 30 - 160 \ (mod\ 160) \\ -13x &\equiv -130 \ (mod\ 160) \\ x &\equiv 10 \ (mod\ 160) \end{aligned}$$

□

**Příklad 5.** *Spočtěte* $325x \equiv 694 \ (mod\ 471)$.

*Řešení.* Předveďme si třetí způsob. Půjde to?

$$\begin{aligned} 325x &\equiv 694 \ (mod\ 471) \\ -146x &\equiv 694 \ (mod\ 471) \\ -73x &\equiv 347 \ (mod\ 471) \\ -73x &\equiv -124 \ (mod\ 471) \\ 73x &\equiv 124 \ (mod\ 471) \end{aligned}$$

Zde už těžko říct jak pokračovat a asi si nevšimneme, že $124 + 25 \cdot 471$ je číslo dělitelné 73. Nyní bychom tedy mohli spočítat inverzi, tedy $73^{-1} \ (mod\ 471)$, nebo upravovat jako dvě rovnice.

$$\begin{aligned} 471x &\equiv 0 \ (mod\ 471) \\ 73x &\equiv 124 \ (mod\ 471) \\ 33x &\equiv -6 \cdot 124 \ (mod\ 471) \\ 7x &\equiv 13 \cdot 124 \ (mod\ 471) \\ 5x &\equiv -58 \cdot 124 \ (mod\ 471) \\ 2x &\equiv 71 \cdot 124 \ (mod\ 471) \\ x &\equiv (-58 - 2 \cdot 71) \cdot 124 \ (mod\ 471) \\ x &\equiv -200 \cdot 124 \ (mod\ 471) \\ 0x &\equiv 471 \cdot 124 \equiv 0 \ (mod\ 471) \end{aligned}$$

Výborně, víme $x \equiv -200 \cdot 124 \ (mod\ 471)$. To ještě upravíme. $(mod\ 471)\, x \equiv -200 \cdot 124 \equiv -50 \cdot 4 \cdot 124 \equiv -50 \cdot 496 \equiv -50 \cdot 25 \equiv (-20 - 20 - 10) \cdot 25 \equiv -500 - 500 - 250 \equiv -29 - 29 - 250 + 471 \equiv 163$. Takže

$$x \equiv 163 \ (mod\ 471).$$

□

Závěrem si zkusme spočítat ještě jednu soustavu lineárních kongruencí.

**Příklad 6.** *Spočtěte*

$$\begin{aligned} 21x &\equiv 27 \ (mod\ 24) \\ 26x &\equiv 10 \ (mod\ 25) \\ 27x &\equiv 30 \ (mod\ 17) \end{aligned}$$

*Řešení.* Nejprve zjednodušujeme:

$$\begin{aligned} 21x &\equiv 3 \ (mod\ 24) \\ x &\equiv 10 \ (mod\ 25) \\ 10x &\equiv 13 \ (mod\ 17) \end{aligned}$$

Všimneme si, že v první kongruenci jsou obě strany i modul dělitelný třemi. Třetí kongruenci upravíme snadno, když přičteme modul 17 k pravé straně.

$$\begin{aligned} 7x &\equiv 1 \ (mod\ 8) \\ x &\equiv 10 \ (mod\ 25) \\ 10x &\equiv 30 \ (mod\ 17) \end{aligned}$$

Číslo 7 je jako $-1$ modulo 8, toho využijeme.

$$\begin{aligned} -x &\equiv 1 \ (mod\ 8) \\ x &\equiv 10 \ (mod\ 25) \\ x &\equiv 3 \ (mod\ 17) \end{aligned}$$

Ještě jedna úprava prvního řádku.

$$\begin{aligned} x &\equiv -1 \equiv 7 \ (mod\ 8) \\ x &\equiv 10 \ (mod\ 25) \\ x &\equiv 3 \ (mod\ 17) \end{aligned}$$

Tím jsou přípravné práce hotové. Nyní tedy vidíme, že platí (mějme $k, l, m \in \mathbb{Z}$)

$$x = 7 + 8k.$$

Dosadíme do druhé kongruence a řešíme pro $k$:

$$\begin{aligned} 7 + 8k &\equiv 10 \ (mod\ 25) \\ 8k &\equiv 3 \equiv 3 + 25 \equiv 28 \ (mod\ 25) \\ 2k &\equiv 7 \equiv 7 + 25 \equiv 32 \ (mod\ 25) \\ k &\equiv 16 \ (mod\ 25) \end{aligned}$$

Proto $k = 16 + 25l$, což dosadíme pro rovnici s $x$, tedy máme

$$x = 7 + 8k = 7 + 8(16 + 25l) = 135 + 200l.$$

Opakujeme postup s třetí kongruencí a řešíme pro $l$:

$$\begin{aligned} 135 + 200l &\equiv 3 \ (mod\ 17) \\ 135 - (7 \cdot 17) + 200l - (17 \cdot 11)l &\equiv 3 \ (mod\ 17) \\ 135 - 119 + (200 - 187)l &\equiv 3 \ (mod\ 17) \\ 16 + 13l &\equiv 3 \ (mod\ 17) \\ -1 - 4l &\equiv 3 \ (mod\ 17) \\ -4l &\equiv 4 \ (mod\ 17) \\ l &\equiv -1 \equiv 16 \ (mod\ 17) \end{aligned}$$

Proto $l = 16 + 17m$ a opět dosadíme, takže

$$x = 135 + 200l = 135 + 200(16 + 17m) = 135 + 3200 + 3400m = 3335 + 3400m.$$

Řešení lze tedy zapsat také $x \equiv 3335 \ (mod\ 3400)$. □