4.1. Lineární kongruence o jedné neznámé.

VĚTA 21. *Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Označme $d = (a, m)$. Pak kongruence*

$$ax \equiv b \pmod{m}$$

(o jedné neznámé x) má řešení právě tehdy, když $d \mid b$.

V případě, kdy $d \mid b$, má tato kongruence právě d řešení (modulo m).

DŮKAZ. Dokážeme nejprve, že uvedená podmínka je nutná. Je-li celé číslo c řešením této kongruence, pak nutně $m \mid a \cdot c - b$. Pokud přitom $d = (a, m)$, pak protože $d \mid m$ i $d \mid a \cdot c - b$ a $d \mid a \cdot c - (a \cdot c - b) = b$.

Obráceně dokážeme, že pokud $d \mid b$, pak má daná kongruence právě d řešení modulo m. Označme $a_1, b_1 \in \mathbb{Z}$ a $m_1 \in \mathbb{N}$ tak, že $a = d \cdot a_1$, $b = d \cdot b_1$ a $m = d \cdot m_1$. Řešená kongruence je tedy ekvivalentní s kongruencí

$$a_1 \cdot x \equiv b_1 \pmod{m_1},$$

kde $(a_1, m_1) = 1$. Tuto kongruenci můžeme vynásobit číslem $a_1^{\varphi(m_1)-1}$ a díky Eulerově větě obdržíme

$$x \equiv b_1 \cdot a_1^{\varphi(m_1)-1} \pmod{m_1}.$$

Tato kongruence má jediné řešení modulo m_1 a tedy $d = m/m_1$ řešení modulo m. □

Následující příklad ukáže, že postup uvedený v důkazu věty obvykle není tím nejefektivnějším – s výhodou lze použít jak Bezoutovu větu, tak ekvivalentní úpravy řešené kongruence.

PŘÍKLAD. Řešte $39x \equiv 41 \pmod{47}$

ŘEŠENÍ. (1) Nejprve využijeme Eulerovu větu.

Protože $(39, 47) = 1$, platí

$$39^{\varphi(47)} = 39^{46} \equiv 1 \pmod{47},$$

tj.

$$\underbrace{39^{45} \cdot 39}_{39^{46} \equiv 1} x \equiv 39^{45} \cdot 41 \pmod{47},$$

z čehož už dostáváme

$$x \equiv 39^{45} \cdot 41 \pmod{47}.$$

Úplné řešení vyžaduje ještě vypočtení zbytku po dělení čísla $39^{45} \cdot 41$ číslem 47, ale to již jistě laskavý čtenář zvládne sám a zjistí výsledek $x \equiv 36 \pmod{47}$

(2) Další možností je využít Bezoutovu větu.
Euklidovým algoritmem pro vypočtení $(39, 47)$ dostáváme

$$\begin{aligned} 47 &= 1 \cdot 39 + 8 \\ 39 &= 4 \cdot 8 + 7 \\ 8 &= 1 \cdot 7 + 1 \end{aligned}$$

Z čehož zpětným odvozením dostáváme

$$\begin{aligned} 1 = 8 - 7 = 8 - (39 - 4 \cdot 8) = 5 \cdot 8 - 39 = \\ = 5 \cdot (47 - 39) - 39 = 5 \cdot 47 - 6 \cdot 39. \end{aligned}$$

Uvážíme-li tuto rovnost modulo 47, dostaneme

$$\begin{aligned} 1 &\equiv -6 \cdot 39 \pmod{47} \quad / \cdot 41 \\ 41 &\equiv \underbrace{41 \cdot (-6)}\cdot 39 \pmod{47} \quad / \cdot 41 \\ x &\equiv 41 \cdot (-6) \pmod{47} \\ x &\equiv -246 \pmod{47} \\ x &\equiv 36 \pmod{47} \end{aligned}$$

(3) Obvykle nejrychlejším, ale nejhůře algoritmizovatelným způsobem řešení je metoda takových úprav kongruence, které zachovávají množinu řešení.

$$\begin{aligned} 39x &\equiv 41 \pmod{47} \\ -8x &\equiv -6 \pmod{47} \\ 4x &\equiv 3 \pmod{47} \\ 4x &\equiv -44 \pmod{47} \\ x &\equiv -11 \pmod{47} \\ x &\equiv 36 \pmod{47} \end{aligned}$$

□

Pomocí věty o řešitelnosti lineárních kongruencí lze dokázat mj. významnou Wilsonovu větu udávající nutnou (i postačující) podmínku prvočíselnosti. Takové podmínky jsou velmi významné ve výpočetní teorii čísel, kdy je třeba efektivně poznat, je-li dané velké číslo prvočíslem. Bohužel dosud není známo, jak rychle vypočítat modulární faktoriál velkého čísla, proto není v praxi Wilsonova věta k tomuto účelu používána.

Věta 22 (Wilsonova). *Přirozené číslo $n > 1$ je prvočíslo, právě když*

$$(n-1)! \equiv -1 \pmod{n} \tag{18}$$

Důkaz. Dokážeme nejprve, že pro libovolné složené číslo $n > 4$ platí $n \mid (n-1)!$, tj. $(n-1)! \equiv 0 \pmod{n}$. Nechť $1 < d < n$ je netriviální dělitel n. Je-li $d \neq n/d$, pak protože $1 < d, n/d \leq n-1$,

je $n = d \cdot n/d \mid (n-1)!$. Pokud $d = n/d$, tj. $n = d^2$, pak protože je $n > 4$, je i $d > 2$ a $n \mid (d \cdot 2d) \mid (n-1)!$. Pro $n = 4$ snadno dostáváme $(4-1)! \equiv 2 \not\equiv -1 \pmod 4$.

Nechť je nyní p prvočíslo. Čísla z množiny $\{2, 3, \ldots, p-2\}$ seskupíme do dvojic vzájemně inverzních čísel modulo p, resp. dvojic čísel, jejichž součin dává zbytek 1 po dělení p. Pro dané číslo a z této množiny existuje podle předchozí věty jediné řešení kongruence $a \cdot x \equiv 1 \pmod p$. Protože $a \neq 0, 1, p-1$, je zřejmé, že rovněž pro řešení c této kongruence platí $c \not\equiv 0, 1, -1 \pmod p$. Číslo a nemůže být ve dvojici samo se sebou; kdyby totiž $a \cdot a \equiv 1 \pmod p$, pak nutně $a \equiv \pm 1 \pmod p$. Součin všech čísel uvedené množiny je tedy tvořen součinem $(p-3)/2$ dvojic (jejichž součin je vždy kongruentní s 1 modulo p). Proto je

$$(p-1)! \equiv 1^{(p-3)/2} \cdot (p-1) \equiv -1 \pmod p.$$

□

4.2. Soustavy lineárních kongruencí o jedné neznámé. Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle Věty 21 rozhodnout o řešitelnosti každé z nich. V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$. Dostaneme tak soustavu kongruencí

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned} \tag{19}$$

Zkoumejme nejprve případ $k = 2$, který – jak uvidíme později – má stěžejní význam pro řešení soustavy (19) s $k > 2$.

Věta 23. *Nechť c_1, c_2 jsou celá čísla, m_1, m_2 přirozená. Označme $d = (m_1, m_2)$. Soustava dvou kongruencí*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \tag{20}$$

v případě $c_1 \not\equiv c_2 \pmod d$ nemá řešení. Jestliže naopak $c_1 \equiv c_2 \pmod d$, pak existuje celé číslo c tak, že $x \in \mathbb{Z}$ splňuje soustavu (19), právě když vyhovuje kongruenci

$$x \equiv c \pmod{[m_1, m_2]}.$$

Důkaz. Má-li soustava (20) nějaké řešení $x \in \mathbb{Z}$, platí nutně $x \equiv c_1 \pmod d$, $x \equiv c_2 \pmod d$, a tedy i $c_1 \equiv c_2 \pmod d$. Odtud plyne, že v případě $c_1 \not\equiv c_2 \pmod d$ soustava (20) nemůže mít řešení.

Předpokládejme dále $c_1 \equiv c_2 \pmod d$. První kongruenci soustavy (20) vyhovují všechna celá čísla x tvaru $x = c_1 + tm_1$, kde $t \in \mathbb{Z}$ je

libovolné. Toto x bude vyhovovat i druhé kongruenci soustavy (20), právě když bude platit $c_1 + tm_1 \equiv c_2 \pmod{m_2}$, tj.

$$tm_1 \equiv c_2 - c_1 \pmod{m_2}.$$

Podle Věty 21 má tato kongruence (vzhledem k t) řešení, neboť $d = (m_1, m_2)$ dělí $c_2 - c_1$, a $t \in \mathbb{Z}$ splňuje tuto kongruenci právě když

$$t \equiv \frac{c_2 - c_1}{d} \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})-1} \left(\mathrm{mod}\ \frac{m_2}{d}\right),$$

tj. právě když

$$t = \frac{c_2 - c_1}{d} \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})-1} + r \cdot \frac{m_2}{d},$$

kde $r \in \mathbb{Z}$ je libovolné. Dosazením

$$x = c_1 + tm_1 = c_1 + (c_2 - c_1) \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})} + r\frac{m_1 m_2}{d} = c + r \cdot [m_1, m_2],$$

kde $c = c_1 + (c_2 - c_1) \cdot (m_1/d)^{\varphi(m_2/d)}$, neboť $m_1 m_2 = d \cdot [m_1, m_2]$. Našli jsme tedy takové $c \in \mathbb{Z}$, že libovolné $x \in \mathbb{Z}$ splňuje soustavu (20), právě když

$$x \equiv c \pmod{[m_1, m_2]},$$

což jsme chtěli dokázat. □

Všimněme si, že důkaz této věty je konstruktivní, tj. udává vzorec, jak číslo c najít. Věta 23 nám tedy dává metodu, jak pomocí jediné kongruence zachytit podmínku, že x vyhovuje soustavě (20). Podstatné je, že tato nová kongruence je téhož tvaru jako obě původní. Můžeme proto tuto metodu aplikovat i na soustavu (19) – nejprve z první a druhé kongruence vytvoříme kongruenci jedinou, které vyhovují právě ta x, která vyhovovala původním dvěma kongruencím, pak z nově vzniklé a z třetí kongruence vytvoříme další atd. Při každém kroku se nám počet kongruencí soustavy sníží o 1, po $k-1$ krocích tedy dostaneme kongruenci jedinou, která nám bude popisovat všechna řešení soustavy (19). Poznamenejme ještě, že číslo c z Věty 23 není nutné určovat pomocí uvedeného vzorce. Můžeme vzít libovolné $t \in \mathbb{Z}$ vyhovující kongruenci

$$t \cdot \frac{m_1}{d} \equiv \frac{c_2 - c_1}{d} \left(\mathrm{mod}\ \frac{m_2}{d}\right)$$

a položit $c = c_1 + tm_1$.

Důsledek (Čínská zbytková věta). *Nechť $m_1, , \ldots, m_k \in \mathbb{N}$ jsou po dvou nesoudělná, $a_1, \ldots, a_k \in \mathbb{Z}$. Pak platí: soustava*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{21}$$

má jediné řešení modulo $m_1 \cdot m_2 \cdots m_k$.

PŘÍKLAD. Řešte systém kongruencí

$$\begin{aligned} x &\equiv -3 \pmod{49} \\ x &\equiv \ \ 2 \pmod{11}. \end{aligned}$$

ŘEŠENÍ. První kongruenci splňují právě všechna celá čísla x tvaru $x = -3 + 49t$, kde $t \in \mathbb{Z}$. Dosazením do druhé kongruence dostáváme

$$-3 + 49t \equiv 2 \pmod{11},$$

odkud

$$5t \equiv 5 \pmod{11},$$

tedy, vzhledem k $(5, 11) = 1$, po vydělení pěti

$$t \equiv 1 \pmod{11},$$

neboli $t = 1+11s$ pro libovolné $s \in \mathbb{Z}$. Proto $x = -3+49(1+11s) = 46+539s$, kde $s \in \mathbb{Z}$, což můžeme také zapsat jako $x \equiv 46 \pmod{539}$. □

PŘÍKLAD. Řešte systém kongruencí

$$\begin{aligned} x &\equiv \ \ 1 \pmod{10} \\ x &\equiv \ \ 5 \pmod{18} \\ x &\equiv -4 \pmod{25}. \end{aligned}$$

ŘEŠENÍ. Z první kongruence dostáváme $x = 1 + 10t$ pro $t \in \mathbb{Z}$. Dosazením do druhé kongruence získáme

$$1 + 10t \equiv 5 \pmod{18},$$

tedy $10t \equiv 4 \pmod{18}$. Protože $(10, 18) = 2$ dělí číslo 4, má tato kongruence podle věty 4.2 řešení $t \equiv 2 \cdot 5^5 \pmod{9}$, přičemž $2 \cdot 5^5 = 10 \cdot 25^2 \equiv 1 \cdot (-2)^2 = 4 \pmod{9}$, a tedy $t = 4+9s$, kde $s \in \mathbb{Z}$. Dosazením $x = 1 + 10(4 + 9s) = 41 + 90s$. Z třetí kongruence pak vychází

$$41 + 90s \equiv -4 \pmod{25},$$

tedy $90s \equiv -45 \pmod{25}$. Vydělením pěti (včetně modulu, neboť $5 \mid 25$)

$$18s \equiv -9 \pmod{5},$$

odkud $-2s \equiv 1 \pmod{5}$, tedy $2s \equiv 4 \pmod{5}$, $s \equiv 2 \pmod{5}$, a proto $s = 2 + 5r$, kde $r \in \mathbb{Z}$. Dosazením $x = 41 + 90(2 + 5r) = 221 + 450r$, tedy $x \equiv 221 \pmod{450}$. □

PŘÍKLAD. Řešte systém kongruencí

$$\begin{aligned} x &\equiv 18 \pmod{25} \\ x &\equiv 21 \pmod{45} \\ x &\equiv 25 \pmod{73}. \end{aligned}$$

Řešení. Z první kongruence $x = 18 + 25t$, kde $t \in \mathbb{Z}$. Dosazením do druhé kongruence

$$18 + 25t \equiv 21 \pmod{45},$$

tedy

$$25t \equiv 3 \pmod{45}.$$

Tato kongruence však podle Věty 21 nemá řešení, neboť $(25, 45) = 5$ nedělí číslo 3. Proto nemá řešení ani celý systém. Tento výsledek bychom také dostali přímo z Věty 23, neboť $18 \not\equiv 21 \pmod{(25, 45)}$. □

Příklad. Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Řešení. Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a tedy podle Věty 23 má kongruence řešení. Protože $\varphi(3564) = 2 \cdot (3^3 \cdot 2) \cdot 10 = 1080$, je řešení tvaru $x \equiv 915 \cdot 23\,941^{1079} \pmod{3564}$. Úprava čísla stojícího na pravé straně by však vyžádala značné úsilí. Proto budeme kongruenci řešit poněkud jinak. Podle Věty 13 (6) je $x \in \mathbb{Z}$ řešením dané kongruence právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11} \end{aligned} \tag{22}$$

Vyřešíme nyní každou z kongruencí soustavy (22) zvlášť. První z nich je splněna, právě když

$$x \equiv 3 \pmod{4},$$

druhá, právě když

$$46x \equiv 24 \pmod{81},$$

odkud vynásobením dvěma $92x \equiv 48 \pmod{81}$, tj. $11x \equiv -33 \pmod{81}$ a po vydělení jedenácti

$$x \equiv -3 \pmod{81}.$$

Třetí kongruence je splněna, právě když

$$5x \equiv 2 \pmod{11},$$

odkud vynásobením číslem -2 dostaneme $-10x \equiv -4 \pmod{11}$, tedy

$$x \equiv -4 \pmod{11}.$$

Libovolné $x \in \mathbb{Z}$ je tedy řešením soustavy (22), právě když je řešením soustavy

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv -3 \pmod{81} \\ x &\equiv -4 \pmod{11} \end{aligned} \tag{23}$$

Z druhé kongruence dostáváme, že $x = -3 + 81t$, kde $t \in \mathbb{Z}$. Dosazením do třetí kongruence soustavy (23) dostaneme

$$-3 + 81t \equiv -4 \pmod{11},$$

tedy $81t \equiv -1 \pmod{11}$, tj. $4t \equiv 32 \pmod{11}$, odkud $t \equiv 8 \pmod{11}$, a proto $t = -3 + 11s$, kde $s \in \mathbb{Z}$. Dosazením $x = -3 + 81(-3 + 11s) = -3 - 3 \cdot 81 + 11 \cdot 81s$ do první kongruence soustavy (23) dostaneme

$$-3 - 3 \cdot 81 + 11 \cdot 81s \equiv 3 \pmod{4},$$

tedy

$$1 + 1 \cdot 1 + (-1) \cdot 1s \equiv 3 \pmod{4},$$

tj. $-s \equiv 1 \pmod{4}$ a proto $s = -1 + 4r$, kde $r \in \mathbb{Z}$. Je tedy

$$x = -3 - 3 \cdot 81 + 11 \cdot 81(-1 + 4r) = -3 - 14 \cdot 81 + 4 \cdot 11 \cdot 81r = -1137 + 3564r,$$

neboli $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence. □

4.3. Kongruence vyšších stupňů. Vraťme se k obecnějšímu případu, kdy na obou stranách kongruence stojí mnohočleny téže proměnné x s celočíselnými koeficienty. Snadno můžeme tuto kongruenci odečtením upravit na tvar

$$F(x) \equiv 0 \pmod{m}, \tag{24}$$

kde $F(x)$ je mnohočlen s celočíselnými koeficienty a $m \in \mathbb{N}$. Věta 20 nám poskytuje sice pracnou, ale univerzální metodu řešení této kongruence. Při řešení kongruence (24) totiž stačí zjistit, pro která celá čísla a, $0 \leq a < m$, platí $F(a) \equiv 0 \pmod{m}$. Nevýhodou této metody je její pracnost, která se zvyšuje se zvětšující se hodnotou m. Je-li m složené, $m = p_1^{n_1} \dots p_k^{n_k}$, kde $p_1, \dots, p_k$ jsou různá prvočísla, a je-li navíc $k > 1$, můžeme nahradit kongruenci (24) soustavou kongruencí

$$\begin{aligned} F(x) &\equiv 0 \pmod{p_1^{n_1}} \\ &\vdots \\ F(x) &\equiv 0 \pmod{p_k^{n_k}}, \end{aligned} \tag{25}$$

která má stejnou množinu řešení, a řešit každou kongruenci této soustavy zvlášť. Tím získáme obecně několik soustav kongruencí (19), které už umíme řešit. Výhoda této metody spočívá v tom, že moduly kongruencí soustavy (25) jsou menší než modul původní kongruence (24).

Příklad. Řešte kongruenci $x^5 + 1 \equiv 0 \pmod{11}$.