## Kongruenční rovnice

Každou rovnici ve tvaru

$$f(x) \equiv 0 \pmod{m} \tag{1}$$

s neznámou $x \in \mathbb{Z}$, kde $m \in \mathbb{N}$, $m > 1$, $f(x) = a_n x^n + \ldots + a_1 x + a_0$ je polynom ze $\mathbb{Z}[x]$ a $a_n \not\equiv 0 \pmod{m}$, nazýváme *kongruenční rovnice stupně $n$ s neznámou $x$*.

**Poznámka.** Je-li $x \in \mathbb{Z}$ řešením rovnice $f(x) \equiv 0 \pmod{m}$ a $x \equiv y \pmod{m}$, pak vzhledem k vlastnostem kongruencí je $y$ také řešením této rovnice. Proto *řešením* uvažované rovnice rozumíme celou třídu $\overline{x} \in \mathbb{Z}_m$. Rovnici (1) je tedy možno chápat jakožto algebraickou rovnici nad $\mathbb{Z}_m$ ve tvaru

$$f(\overline{x}) = \overline{a}_n \overline{x}^n + \ldots + \overline{a}_1 \overline{x} + \overline{a}_0 = \overline{0} \tag{2}$$

pro $\overline{a}_n \neq \overline{0}$. Nebudeme tedy rozlišovat mezi tvary rovnice (1) a (2) a budeme používat vždy ten tvar, který se nám v dané situaci bude lépe hodit.

Odtud také okamžitě plyne, že rovnice (1) *nemůže* mít více než $m$ řešení (počet prvků $\mathbb{Z}_m$ je totiž právě $m$).

**Příklad.** Řešte kongruenční rovnice

a) $2x^3 + 3x - 5 \equiv 0 \pmod{7}$,

b) $x^2 + x - 2 \equiv 0 \pmod{5}$.

**Poznámka.** Při úpravách kongruenčních rovnic je třeba dát pozor na skutečnost, že při násobení obou stran rovnice číslem soudělným s modulem $m$ nemusíme dostat ekvivalentní rovnice, např. $x^3 - x + 1 \equiv 0 \pmod 3$ a $3x^3 - 3x + 3 \equiv 0 \pmod 3$ nejsou ekvivalentní, neboť první nemá žádné řešení a druhá je identická.

## Kongruenční rovnice 1. stupně

Obecný tvar kongruenčních rovnic 1. stupně je

$$ax \equiv b \pmod m,$$

kde $a \not\equiv 0 \pmod m$. Ve tvaru (2) má lineární rovnice tvar

$$\overline{a} \cdot \overline{x} = \overline{b} \tag{3}$$

v $\mathbb{Z}_m$ pro $\overline{a} \neq \overline{0}$.

1. Předpokládejme nejprve, že $(a, m) = 1$.

V tom případě víme, že prvek $\overline{a}$ je invertibilní v $\mathbb{Z}_m$. Vynásobíme-li obě strany rovnice prvkem $\overline{a}^{-1}$, dostaneme $\overline{x} = \overline{b}\overline{a}^{-1}$, tedy rovnice (3) má *jediné řešení.*

**Příklad.** Řešme rovnici $5x \equiv 7 \pmod 8$.

2. Nechť nyní $(a, m) = d > 1$. Mohou nastat dvě možnosti:

a) $d \nmid b$ – v tomto případě rovnice *nemá* řešení, neboť obě strany rovnice musí mít s modulem stejné společné dělitele.

**Příklad.** Rovnice $6x \equiv 7 \pmod{15}$ není řešitelná, neboť $3 = (6, 15) \nmid 7$.

b) $d|b$ – v tomto případě $d|ax$, $d|b$, $d|m$, platí tedy

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \quad \text{kde } \left(\frac{a}{d}, \frac{m}{d}\right) = 1.$$

Je-li $x_1$ řešení redukované rovnice, máme právě d řešení

$$\overline{x}_t \in \left\{ \overline{x}_1 + \overline{\left(\frac{m}{d}\right)}\overline{t};\ t \in \{0, \ldots, d-1\} \right\}.$$

**Příklad.** Řešme rovnici $15x \equiv 35 \pmod{55}$.

Někdy bývá výhodné rovnici upravit tak, abychom na pravé straně rovnice dostali násobek čísla a. V tom případě je možno buď celou kongruenční rovnici (i s modulem) nebo pouze obě strany kongruence krátit číslem a.

Musíme ovšem dávat pozor na to, zda dostáváme rovnici ekvivalentní s původní či ne.

Příklad. Řešme kongruenční rovnici $5x \equiv 7 \pmod{8}$.

Příklad. Řešme kongruenční rovnici $7x \equiv 6 \pmod{15}$.

## Řešení kongruenčních rovnic 1. stupně pomocí Eulerovy věty

**Věta 4.1 (Euler)** *Nechť* NSD($c$, $m$) = 1. *Pak platí* $c^{\phi(m)} = 1 \pmod m$.

V řeči zbytkových tříd lze Eulerovu větu přepsat do tvaru $a^{\varphi(m)} = 1$ v $Z_m$. Lze ji také interpretovat tak, že k prvku a existuje v okruhu $Z_m$ prvek inverzní, přičemž $a^{-1} = a^{\varphi(m)-1}$.

odkud pro ax ≡ b máme

$$x \equiv a^{\varphi(m)-1}b \pmod m.$$

Příklad. Řešme rovnici $3x \equiv 7 \pmod{11}$.

Příklad. Řešme rovnici $17x \equiv 25 \pmod{28}$.

*Úloha: Vytvořte algoritmus, jenž vyřeší lineární kongruenční rovnici. Uveďte algoritmus a naprogramujte.*

## Důkaz Eulerovy věty

Vezměmě jen takové prvky Rm, které jsou nesoudělné s m.

*Důkaz.* Označme (viz 4.19) prvky redukovaného systému zbytkových tříd modulo $m$ následovně

$$R_m = \{\overline{r_1}, \overline{r_2}, \ldots, \overline{r_{\varphi(m)}}\},$$

kde $1 \leqq r_i \leqq m$ pro všechna $i \in \{1, 2, \ldots, \varphi(m)\}$.

Podle předpokladu věty je číslo $a$ nesoudělné s $m$ a také všechna čísla $r_i$, $i \in \{1, 2, \ldots, \varphi(m)\}$ jsou nesoudělná s $m$. Proto, podle Lemmatu 4.20, je číslo $ar_i$ nesoudělné s $m$. A tak můžeme říci, že $\overline{ar_i}$ je některá ze zbytkových tříd z $R_m$. Nevíme v tuto chvíli která, ale to nevadí, označme ji $\overline{z_i}$, kde $1 \leqq z_i \leqq m$ pro všechna $i \in \{1, 2, \ldots, \varphi(m)\}$.

Dostáváme tak soustavu kongruencí

$$\begin{aligned} ar_1 &\equiv z_1 (\mathrm{mod}\, m), \\ ar_2 &\equiv z_2 (\mathrm{mod}\, m), \\ &\vdots \\ ar_{\varphi(m)} &\equiv z_{\varphi(m)} (\mathrm{mod}\, m). \end{aligned} \tag{4.53}$$

Jejich vynásobením obdržíme

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv z_1 z_2 \cdots z_{\varphi(m)} (\mathrm{mod}\, m). \tag{4.54}$$

Čísla $z_1, z_2, \ldots, z_{\varphi(m)}$ na pravých stranách kongruencí (4.53) jsou navzájem různá, neboť ze vztahu

$$z_i \equiv z_j (\mathrm{mod}\, m)$$

okamžitě plyne

$$ar_i \equiv ar_j (\mathrm{mod}\, m)$$

a odtud[1]

$$r_i \equiv r_j (\mathrm{mod}\, m).$$

Pro $r_i \neq r_j$ proto dostáváme $z_i \neq z_j$. Je tedy zřejmé, že každé z čísel $z_i$ je rovno některému z čísel $r_i$, kde $i \in \{1, 2, \ldots, \varphi(m)\}$. Proto

$$r_1 r_2 \cdots r_{\varphi(m)} = z_1 z_2 \cdots z_{\varphi(m)} \tag{4.55}$$

Dosaďíme z (4.55) do (4.54) a obdržíme tak

$$r_1 r_2 \cdots r_{\varphi(m)} a^{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} (\mathrm{mod}\, m). \tag{4.56}$$

[1] $\gcd(a, m) = 1$, v dané kongruenci proto můžeme krátit číslem $a$.

Číslo $r_1 r_2 \cdots r_{\varphi(m)}$ je jistě s číslem $m$ nesoudělné, neboť všechna čísla $r_1$, $r_2$, $\ldots$, $r_{\varphi(m)}$ jsou s $m$ nesoudělné. Můžeme proto v kongruenci (4.56) krátit číslem $r_1 r_2 \cdots r_{\varphi(m)}$. Odtud

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

□

**Lemma 4.20.** *Nechť* $a, b \in \mathbb{Z}$. *Jestliže* $\gcd(a, m) = \gcd(b, m) = 1$, *potom* $\gcd(ab, m) = 1$.

## Lineární diofantické rovnice

Uvažujme nejprve následující jednoduchou úlohu z praxe. Máme dvě nádoby o objemech 5 l a 7 l a třetí nádobu dostatečně velkého objemu. Ptáme se, zda je možno pouze pomocí prvních dvou nádob do třetí nádoby nalít 8 l vody. Jedno z možných řešení může vypadat tak, že nejprve nalejeme do třetí nádoby 4 nádoby o objemu 7 l a pak odebereme ze třetí nádoby 4 nádoby 5 litrové. Kdybychom měli ale první dvě nádoby o objemech 12 l a 20 l a chtěli do třetí nádoby pomocí nich dostat 38 l vody, nikdy se nám to nepovede.

Úlohy uvedeného typu vedou k řešení rovnic ve tvaru

$$ax + by = c, \tag{1}$$

přičemž $a, b, c \in \mathbb{Z}$ jsou daná čísla a hledáme všechny uspořádané dvojice $(x, y) \in \in \mathbb{Z}^2$ vyhovující rovnosti (1). Rovnice (1) nazýváme *neurčité rovnice 1. stupně o dvou neznámých* nebo také *lineární diofantické rovnice o dvou neznámých.*

Z rovnice (1) okamžitě dostaneme kongruenční rovnici 1. stupně

$$ax \equiv c \pmod{b}. \tag{2}$$

Využijeme nyní toho, co už víme o řešení rovnic (2). Jestliže $d = (a, b) \nmid c$, pak rovnice (2) (a tedy ani rovnice (1)) není řešitelná. V opačném případě lze celou rovnici (1) vydělit číslem $b$ a zabývat se pouze případem, kdy $(a, b) = 1$.

Jak už víme, rovnice (2) má v tom případě jediné řešení

$$x \equiv x_1 \pmod{b}, \quad \text{tj. } x = x_1 + bt,\ t \in \mathbb{Z}.$$

Dosadíme-li nyní za $x$ do rovnice (1), dostaneme pro $y$ vyjádření

$$y = \frac{c - ax_1}{b} - at = y_1 - at, \quad t \in \mathbb{Z}.$$

Zřejmě $y_1 = \frac{c-ax_1}{b} \in \mathbb{Z}$, neboť $b|c - ax_1$ ($x_1$ je totiž řešením rovnice (2)), a tedy obecné řešení rovnice (1) je ve tvaru

$$\begin{aligned} x &= x_1 + bt \\ y &= y_1 - at,\ t \in \mathbb{Z}. \end{aligned}$$

**Příklad.** Řešme rovnici $53x + 17y = 25$.

## Lineární diofantické rovnice s n neznámými

Obecně lze uvažovat rovnice typu

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{3}$$

kde $a_1, \ldots, a_n, b$ jsou daná celá čísla, řešením jsou všechny $n$-tice $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ vyhovující vztahu (3). Rovnice (3) nazýváme *neurčité rovnice 1. stupně s n neznámými* nebo *lineární diofantické rovnice o n neznámých*. Pro řešitelnost rovnic (3) lze dokázat následující větu.

**Věta 3.1.** *Rovnice* (3) *je řešitelná právě když* $d = (a_1, \ldots, a_n) | b$, *přičemž řešení závisí na* $n - 1$ *nezávislých celočíselných parametrech.*

Příklad. Najděte všechny mřížové body nadroviny $9x - 15y + 4z = 6$ v $E_3$.

## Soustavy kongruenčních rovnic 1. stupně

Einsteinova úloha: *Uvažujeme schodiště mající následující vlastnosti: budeme-li přecházet po dvou schodech najednou, zůstane nám na konci jeden schod, půjdeme- li po třech schodech, zůstanou nám nakonec dva schody, půjdeme-li po čtyřech, zůstanou tři schody, po pěti zůstanou čtyři schody, po šesti pět schodů a teprve překročili bychom-li najednou sedm schodů, došli bychom na konec schodiště. Kolik schodů má schodiště?*

Snadno je vidět, že Einsteinova úloha je ekvivalentní nalezení všech přiroze- ných čísel vyhovujících následující soustavě kongruenčních rovnic 1. stupně:

$$x \equiv 1 \pmod 2,\ x \equiv 2 \pmod 3,\qquad x \equiv 3 \pmod 4,$$

$$x \equiv 4 \pmod 5,\ x \equiv 5 \pmod 6,\ x \equiv 0 \pmod 7.$$

Uvažujme systém kongruenčních rovnic 1. stupně s neznámou $x \in Z$

$$A_1 x \equiv B_1 \pmod{m_1},\ \ldots,\ A_k x \equiv B_k \pmod{m_k}. \qquad (1)$$

Z předešlých úvah je zřejmé, že pokud je soustava (1) řešitelná, je řešitelná každá z rovnic

soustavy, a má tedy smysl zabývat se pouze soustavami ve tvaru

$$x \equiv b_1 \pmod{m_1},\ \ldots,\ x \equiv b_k \pmod{m_k}. \qquad (2)$$

Soustavu (1) nazýváme *soustava lineárních kongruenčních rovnic 1. stupně*.

V případě řešitelnosti soustavy (2) lze řešení vždy hledat ve tvaru

$$x \equiv x_1 \pmod{[m_1, \ldots, m_k]}.$$

Zde $[m_1, \ldots, m_k]$ označuje nejmenší společný násobek.

Příklad. Řešme soustavu

$$x \equiv 5 \pmod{18}$$
$$x \equiv 8 \pmod{21}.$$

Příklad. Řešme Einsteinovu úlohu.

## Čínská věta o zbytcích

Zabývejme se nyní soustavami (2), v nichž jsou moduly po dvou nesoudělné, tj. platí $(m_i, m_j) = 1$ pro $i \neq j$.V tomto případě zřejmě platí

$$[m_1, \ldots, m_k] = m_1 \cdot \ldots \cdot m_k = M$$

a z předchozích úvah vyplývá, že řešení soustavy (2) lze hledat ve tvaru

$$x \equiv x_0 \pmod{M}.$$

Položme $M_i = \frac{M}{m_i}$ pro $i = 1, \ldots, k$. Vzhledem ke vzájemné nesoudělnosti modulů platí $(m_i, M_i) = 1$ (ověřte!). To ovšem znamená, že existují prvky $M_i^*$ tak, že

$$M_i \cdot M_i^* = 1 \pmod{m_i}$$

(prvky $M_i$ jsou totiž invertibilní v $\mathbb{Z}_m$). Položme

$$x_0 = M_1 M_1^* b_1 + \ldots + M_k M_k^* b_k.$$

Pak $x_0 \equiv M_1 M_1^* b_1 \equiv b_1 \pmod{m_1}$, neboť $M_k \equiv 0 \pmod{m_j}$ pro $j \neq k$. Podobně $x_0 \equiv b_j \pmod{m_j}$ pro každé $j = 1, \ldots, k$, tedy

Příklad. Řešme soustavu

$$x \equiv 20 \pmod{21}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 5 \pmod{8}.$$

Na závěr ještě uveďme, že soustavy typu (2) vyjadřují zadání staré čínské úlohy: *najít číslo, které po vydělení číslem $m_1$ dává zbytek $b_1$, atd., až po vydělení číslem $m_k$ dá zbytek $b_k$.* Řešitelnost soustavy (2) lze shrnout do následující věty:

Věta 3.2. (čínská věta o zbytcích)
*Buďte $m_1, \ldots, m_k$ po dvou nesoudělná přirozená čísla a $b_1, \ldots, b_k$ libovolná k-tice celých čísel. Pak je soustava lineárních kongruenčních rovnic (2) řešitelná a její řešení lze najít v modulu $m = m_1 \cdot \ldots \cdot m_k$.*

*Úloha: Napište algoritmus výpočtu řešení čínské věty. Naprogramujte.Prezentujte.*

## Kvadratické kongruenční rovnice

Zabývejme se nyní řešením kongruenčních rovnic 2. stupně. Jejich obecný tvar je

$$Ax^2 + Bx + C \equiv 0 \pmod{M}, \tag{1}$$

kde $A, B, C \in \mathbb{Z}$ jsou daná čísla, $A \not\equiv 0 \pmod{M}$ a neznámá $x \in \mathbb{Z}$.

Ukažme, že každou rovnici tvaru (1) je možno převést na tvar

$$x^2 \equiv a \pmod{m} \tag{2}$$

pro nějaké $a \in \mathbb{Z}$. Rovnici (1) nejprve vynásobíme číslem $4A$:

$$4A^2x^2 + 4ABx + 4AC \equiv 0 \pmod{4AM}, \tag{3}$$

která je ekvivalentní s rovnicí (1) (proč?). Z rovnice (3) plyne

$$(2Ax + B)^2 \equiv B^2 - 4AC \pmod{4AM}.$$

Substitucemi $y = 2Ax + B, D = B^2 - 4AC$ dostaneme

$$y^2 \equiv D \pmod{4AM}, \tag{4}$$

která je už rovnicí tvaru (2). Je třeba si uvědomit, že řešitelnost rovnice (4) ještě neznamená řešitelnost původní rovnice (1). Je-li totiž $y_1$ řešením rovnice (4), $y \equiv y_1 \pmod{4AM}$, pak po dosazení za $y$ dostaneme rovnici $2Ax \equiv y_1 - B \pmod{4AM}$, která v případě $2A \nmid (y_1 - B)$, není řešitelná. Dále je třeba mít na paměti fakt, že řešení rovnice (4) jsou v modulu $2M$, kdežto řešení rovnice (1) hledáme v modulu $M$. Počet řešení rovnice (4) se tedy přechodem k původnímu modulu může zmenšit.

**Příklad.** Řešme rovnice:

a) $4x^2 - 11x - 3 \equiv 0 \pmod{13}$

## Kvadratická kongruenční rovnice v lichém prvočíselném modulu

$$x^2 \equiv a \pmod{p}, \qquad (2, p) = 1, \qquad (a, p) = 1.$$

Je-li rovnice řešitelná pro $a \neq 0 \pmod{m}$, nazýváme číslo $a$ *kvadratický zbytek* modulo $m$; v opačném případě se nazývá *kvadratický nezbytek* modulo $m$.

Počet kvadratických zbytků modulo p je právě ½(p-1) a jsou to právě všechny prvky posloupnosti $1^2, 2^2, \ldots, (\frac{1}{2}(p-1))^2$. Ostatní prvky nepatřící do této posloupnosti jsou kvadratické nezbytky.

Toto platí proto, že $Z_p = \{+-1, +-2, \ldots, +-1/2(p-1)\}$

Příklad. Kvadratických zbytků $\pmod{17}$ je právě $\frac{1}{2}(17-1) = 8$ a jsou to čísla
$1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16$, $5^2 = 25 \equiv 8$, $6^2 = 36 \equiv 2$, $7^2 = 49 \equiv 15$,
$8^2 = 64 \equiv 13$. Kvadratické nezbytky jsou potom čísla 3, 5, 6, 7, 10, 11, 12, 14.

**Věta 3.3. (Eulerovo kritérium)** *Buď $a \in \mathbb{Z}$, $(a, p) = 1$. Pak*

*i) $a$ je kvadratický zbytek modulo $p$, právě když*

$$a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p},$$

*ii) $a$ je kvadratický nezbytek modulo $p$, právě když*

$$a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}.$$

Příklad. Určete, zda je řešitelná rovnice $x^2 \equiv 7 \pmod{19}$

**Lemma 7.20** *Je-li $p$ prvočíslo tvaru $4k-1$ a $d$ kvadratický zbytek modulo $p$, řešení kongruenční rovnice tvaru*

$$y^2 = d \pmod p \tag{7.31}$$

*je dáno předpisem*

$$y = d^k \pmod p. \tag{7.32}$$

**Důkaz.** Z Eulerova kritéria máme, že

$$1 = d^{\frac{p-1}{2}} \bmod p.$$

Protože $k = \frac{1}{4}(p+1)$, máme

$$d^{\frac{1}{4}(p+1)} d^{\frac{1}{4}(p+1)} = d^{\frac{1}{2}(p+1)} = d^{\frac{1}{2}(p-1)} d = d \bmod p.$$

Příklad. Vyřešte rovnici $x^2 \equiv 7 \pmod{19}$

**Lemma 7.16** *Řešení rovnice*

$$x^2 + B \cdot x = C \pmod{p \cdot q} \tag{7.27}$$

*lze obdržet jako kombinaci řešení $u, v$ rovnic*

$$x^2 + B \cdot x = C \pmod{p} \tag{7.28}$$

$$x^2 + B \cdot x = C \pmod{q} \tag{7.29}$$

*a přirozených čísel $a, b$ splňujících*

$$a = 1 \pmod{p}, \quad a = 0 \pmod{q}, \quad b = 0 \pmod{p}, \quad b = 1 \pmod{q}, \tag{7.30}$$

*a pak*

$$x = a \cdot u + b \cdot v$$

*splňuje 7.27.*