Řešení kongruencí o jedné neznámé

Podobně jako řešení rovnic vede k výpočtu neznámé, řešení kongruencí vede k určení hodnot, kterých neznámá může nabývat. Navíc se u kongruencí pohybujeme pouze v oboru celých čísel.

Definice. Nechť $m \in \mathbb{N}$, $f(x), g(x) \in \mathbb{Z}[x]$. Zápis

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

nazýváme *kongruencí o jedné neznámé* x a rozumíme jím úkol nalézt *množinu řešení*, tj. množinu všech takových čísel $c \in \mathbb{Z}$, pro která $f(c) \equiv g(c) \pmod{m}$.

Dvě kongruence o jedné neznámé nazveme *ekvivalentní*, mají-li stejnou množinu řešení. Kongruence (**??**) je ekvivalentní s kongruencí $\underbrace{f(x) - g(x)}_{\in \mathbb{Z}[x]} \equiv 0 \pmod{m}$.

Co je to počet řešení kongruence uvádí následující definice.

Definice. *Počtem řešení* kongruence o jedné neznámé modulo m rozumíme počet zbytkových tříd modulo m obsahujících řešení této kongruence.

Pro určení hodnot kongruence o jedné neznámé může sloužit následující věta.

Věta. *Nechť $m \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$. Pro libovolná $a, b \in \mathbb{Z}$ platí*

$$a \equiv b \pmod{m} \implies f(a) \equiv f(b) \pmod{m}.$$

Podle výše uvedené věty je řešením kongruence vždy buď celá zbytková třída, nebo žádný její prvek. Její využití tedy spočívá v postupném zkoušení zástupců všech zbytkových tříd, a zjišťování, zda je kongruence splněná. Pro vyšší moduly je však tento postup velmi pracný.

Lineární kongruence a soustavy lineárních kongruencí

Nejdříve zjistíme, kdy má lineární kongruence o jedné neznámé řešení, a pokud ano, kolik řešení má. To pak využijeme i u soustav lineárních kongruencí.

Věta. *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).

Pomocí předchozí věty lze dokázat Wilsonovu větu, která udává nutnou a postačující podmínku prvočíselnosti.

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

$$(n-1)! \equiv -1 \pmod{n} \tag{2}$$

Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme rozhodnout o řešitelnosti každé z kongruencí. Pokud alespoň jedna z nich není řešitelná, pak ani soustava nemá řešení. V opačném případě lze každou z kongruencí upravit na tvar $x \equiv c_i \pmod{m_i}$.

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

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \tag{3}$$

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 danou soustavu, právě když vyhovuje kongruenci

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

Podobným způsobem lze určit i řešení soustavy o více než dvou kongruencích.

Věta (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*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{4}$$

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

Kongruence vyšších stupňů

V obecnějším případě mohou na obou stranách kongruence stát polymony téže proměnné x s celočíselnými koeficienty. Tuto kongruenci můžeme snadno převést na tvar $F(x) \equiv 0 \pmod{m}$, kde $F(x) \in \mathbb{Z}[x]$, $m \in \mathbb{N}$. Tuto kongruenci pak můžeme řešit podle věty **??**.

Nevýhodou výše uvedené metody je její pracnost, zvyšuje-li se hodnota modulu. Je-li m složené, $m = p_1^{n_1} \dots p_k^{n_k}$, kde $p_i, i \in \{1, 2, \dots, k\}$ jsou různá prvočísla, můžeme kongruenci $F(x) \equiv 0 \pmod{m}$ nahradit soustavou kongruencí

$$\begin{aligned} F(x) &\equiv 0 \pmod{p_1^{n_1}} \\ &\vdots \\ F(x) &\equiv 0 \pmod{p_k^{n_k}}, \end{aligned} \tag{5}$$

kterou umíme řešit např. pomocí Čínské zbytkové věty; v případě vyšších mocnin prvočísel můžeme k řešení využít následující větu:

Věta (Henselovo lemma)**.** *Nechť p je prvočíslo, $f(x) \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ je takové, že $p \mid f(a), p \nmid f'(a)$. Pak platí: pro každé $n \in \mathbb{N}$ má soustava*

$$\begin{aligned} x &\equiv a \pmod{p} \\ f(x) &\equiv 0 \pmod{p^n} \end{aligned} \tag{6}$$

právě jedno řešení modulo p^n.

Věta. *Buď p prvočíslo, $f(x) \in \mathbb{Z}[x]$. Má-li kongruence $f(x) \equiv 0 \pmod{p}$ více než $\mathrm{st}(f)$ řešení, pak jsou všechny koeficienty polynomu f násobkem p.*

Binomické kongruence a primitivní kořeny

Definice. Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Číslo a nazveme *n-tým mocninným zbytkem modulo m*, pokud je kongruence

$$x^n \equiv a \pmod{m}$$

řešitelná. V opačném případě nazveme *a n-tým mocninným nezbytkem modulo m.*

Pro $n = 2, 3, 4$ používáme termíny kvadratický, kubický a bikvadratický zbytek, resp. nezbytek modulo m.

Binomické kongruence je často vhodné řešit pomocí *primitivních kořenů.*

Definice. Nechť $m \in \mathbb{N}$. Celé číslo $a \in \mathbb{Z}$, $(a, m) = 1$ nazveme *primitivním kořenem* modulo m, pokud je jeho řád modulo m roven $\varphi(m)$.

Lemma 1. *Je-li g primitivní kořen modulo m, pak pro každé číslo $a \in \mathbb{Z}$, $(a, m) = 1$ existuje jediné $x_a \in \mathbb{Z}$, $0 \le x_a < \varphi(m)$ s vlastností $g^{x_a} \equiv a \pmod{m}$.*

Pomocí primitivních kořenů a Eulerovy funkce můžeme rozhodnout, zda je daná binomická kongruence řešitelná, a kolik má řešení.

Věta. *Buď $m \in \mathbb{N}$ takové, že modulo m existují primitivní kořeny. Dále nechť $a \in \mathbb{Z}$, $(a, m) = 1$. Pak kongruence*

$$x^n \equiv a \pmod{m}$$

je řešitelná (tj. a je n-tý mocninný zbytek modulo m), právě když

$$a^{\varphi(m)/d} \equiv 1 \pmod{m},$$

kde $d = (n, \varphi(m))$.
Přitom, je-li tato kongruence řešitelná, má právě d řešení.

Je potřeba vědět, pro jaké moduly primitivní kořeny existují.

Věta. *Buď $m \in \mathbb{N}$, $m > 1$. Primitivní kořeny modulo m existují právě tehdy, když m splňuje některou z následujících podmínek:*

- *$m = 2$ nebo $m = 4$,*
- *m je mocnina lichého prvočísla*
- *m je dvojnásobek mocniny lichého prvočísla.*

Nyní tedy víme, pro jaké moduly primitivní kořeny existují. Obecně je ale nalezení primitivního kořene pro daný modul výpočetně náročná operace. Následující věta udává ekvivalentní podmínku pro to, aby zkoumané číslo bylo primitivním kořenem.

Věta. *Buď m takové, že modulo m existují primitivní kořeny. Zapišme $\varphi(m) = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$. Pak pro libovolné $g \in \mathbb{Z}$, $(g, m) = 1$ platí, že g je primitivní kořen modulo m, právě když*

$$g^{\frac{\varphi(m)}{q_1}} \not\equiv 1 \pmod{m}, \ldots, g^{\frac{\varphi(m)}{q_k}} \not\equiv 1 \pmod{m}.$$

Kvadratické kongruence, Legendrův a Jacobiho symbol

Důvodem pro zavedení Lagendrova symbolu byla snaha najít jednodušší způsob ověření řešitelnosti kvadratické kongruence $x^2 \equiv a \pmod{p}$, resp. $x^2 + bx + c \equiv 0 \pmod{p}$, než jaký byl uveden v předchozí části (věta **??**).

Definice. Nechť je p liché prvočíslo. *Legendreův symbol* definujeme předpisem

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a,\ a \text{ je kvadratický zbytek modulo } p, \\ 0 & p \mid a, \\ -1 & p \nmid a,\ a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Jakým způsobem pracovat s Legendrovým symbolem uvádí následující věta:

Lemma 2. *Nechť p je liché prvočíslo, $a, b \in \mathbb{Z}$ libovolná. Pak platí:*

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Vztah mezi Legendrovým symbolem a kvadratickými kongruencemi dokládá i následující věta.

Věta. *1. V libovolné redukované soustavě zbytků modulo p je stejný počet kvadratických zbytků a nezbytků.*

2. Součin dvou kvadratických zbytků je zbytek, součin dvou nezbytků je zbytek, součin zbytku a nezbytku je nezbytek.

3. $(-1/p) = (-1)^{\frac{p-1}{2}}$, tj. kongruence $x^2 \equiv -1 \pmod{p}$ je řešitelná právě tehdy, když $p \equiv 1 \pmod{4}$.

Protože kongruence $x^2 \equiv 1 \pmod{p}$ je řešitelná pro libovolné liché prvočíslo p, je Legendrův symbol $\left(\frac{1}{p}\right) = 1$. Pro výpočet Legendrova symbolu je důležitá následující věta:

Věta (Zákon kvadratické reciprocity)**.** *Nechť p, q jsou různá lichá prvočísla. Pak*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Podmínku 2 předchozí věty lze ekvivalentně zapsat také takto:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{je-li } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{je-li } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Ne vždy se ale v kvadratických kongruencích na pozici modulu vyskytuje prvočíslo, bylo by ale vhodné mít k dispozici podobný nástroj k rozhodnutí o řešitelnosti, resp. neřešitelnosti, takové kongruence. Takovéto rozšíření Legendrova symbolu se nazývá *Jacobiho symbol*.

Definice. Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $2 \nmid b$. Nechť $b = p_1 p_2 \cdots p_k$ je rozklad b na (lichá) prvočísla (výjimečně neseskupujeme stejná prvočísla do mocniny, ale vypisujeme každé zvlášť, např. $135 = 3 \cdot 3 \cdot 3 \cdot 5$). Symbol

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

se nazývá *Jacobiho symbol*.

Vlastnosti Jacobiho symbolu jsou velmi podobné vlastnostem Legendrova symbolu. Nelze ale z jeho hodnoty zjistit, zda je daná kvadratická kongruence řešitelná, je však možné dokázat, že řešitelná není. Vlastnosti Jacobiho symbolu uvádí následující věty.

Věta. *Nechť a, a_1, $a_2 \in \mathbb{Z}$, b, b_1, $b_2 \in \mathbb{N}$, $2 \nmid b_1 b_2$, $2 \nmid b$. Pak platí:*

1. $a_1 \equiv a_2 \pmod{b} \implies \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$
2. $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right)$
3. $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right)$

Věta. *Nechť $a, b \in \mathbb{N}$ jsou lichá nesoudělná čísla. Pak platí:*

1. $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$
2. $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$
3. $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$