Čínská zbytková věta

Anša Lauschmannová

Motivační příklad

Máme několik předmětů, jejich počet není znám. Když je postupně rozdělujeme do trojic, zbydou dva; při dělení do pětic zbydou tři; při dělení do sedmic zbydou opět dva. Jaký počet předmětů máme? (Sun Tsu Suan Ching, 4. století)

Historka s morálním ponaučením

Stará žena šla na trh. Do jejího košíku s vejci kopl kůň a vejce se rozbila. Majitel koně ženě nabídl, že zaplatí škodu, a ptal se, kolik měla v košíku vajec. Ale žena je stará a nepamatuje si to. Ví jen, že když je z košíku vyndavala po dvou, zbylo na dně jedno vajíčko. Totéž se stalo, když je vyndavala po třech, po čtyřech, po pěti a po šesti, ale když je vyndavala po sedmi, nezbylo na dně žádné. Jaký nejmenší počet vajec mohl být v košíku? (Brahmagupta: Brahma Sútra Siddhanta, 7. století)

Značení.

- $(n1, n2)$ – největší společný dělitel čísel $n1$ a $n2$
- $\mathrm{nsn}(n1, n2)$ – nejmenší společný násobek čísel $n1$ a $n2$

Lemma. *Soustava dvou kongruencí*

$$x \equiv r_1 \pmod{n_1},$$
$$x \equiv r_2 \pmod{n_2}$$

je řešitelná, pouze pokud $r_1 \equiv r_2 \pmod{(n_1, n_2)}$. *Existuje jediné nezáporné řešení menší než* $\mathrm{nsn}(n_1, n_2)$.

Věta. (Čínská věta o zbytcích) *Mějme po dvou nesoudělná čísla* $n_1, \ldots, n_k \in \mathbb{N}$ *a nezáporná celá čísla* $r_1, \ldots, r_k \in \mathbb{N} \cup \{0\}$ *taková, že* $r_1 < n_1, \ldots, r_k < n_k$. *Pak soustava rovnic*

$$x \equiv r_1 \pmod{n_1},$$
$$\vdots$$
$$x \equiv r_k \pmod{n_k}$$

má vždy nezáporné řešení $x \in \mathbb{N} \cup \{0\}$. *Existuje jediné nezáporné řešení* x *menší než* $n_1 \cdot n_2 \cdots n_k$.

Důsledek. Soustava kongruencí $x \equiv r_i \pmod{n_i}$, $i = 1, \ldots, k$, je řešitelná právě tehdy, když pro každé i, j $(1 \leq i < j \leq k)$ platí $a_i \equiv a_j \pmod{(ni, nj)}$. Je-li tato pod-

mínka splněna, existuje celé číslo y takové, že soustava je ekvivalentní s kongruencí $x \equiv y \pmod{\mathrm{nsn}(n_1, \ldots, n_k)}$.

Příklad. Zjistěte, jestli existuje 21 po sobě jdoucích přirozených čísel, z nichž každé je dělitelné jedním nebo více prvočísly z intervalu $\langle 2, 13 \rangle$.

Definice. *Nechť M je množina. Řekneme, že funkce f je binární operace na M, jestliže $M \neq \emptyset$ a f je zobrazeni z $M \times M$ do M. Pro $a, b \in M$ obvykle $f(a, b)$ zapisujeme jako $a \cdot b$, ab (multiplikativní zápis) nebo $a + b$ (aditivní zápis). Množina M se nazývá uzavřená vzhledem k operaci f, jestliže pro každé $a, b \in M$ platí $afb \in M$. Řekneme, že binární operace $\cdot$ je asociativní, pokud $\forall a, b, c \in M$ $((a \cdot b) \cdot c) = (a \cdot (b \cdot c))$. Řekneme, že binární operace $\cdot$ je komutativní, pokud $\forall a, b \in M$ $a \cdot b = b \cdot a$. Prvek e množiny M nazveme neutrální prvek, pokud $\forall a \in M$ $a \cdot e = e \cdot a = a$. Řekneme, že b je inverzní prvek k prvku a a píšeme $b = a^{-1}$, pokud $b \cdot a = a \cdot b = e$. Pokud používáme aditivní zápis, mluvíme obvykle o opačném prvku a píšeme $-a$.*

Definice. *Struktura $(M, +, \cdot, 0, 1)$ se nazývá komutativní okruh, pokud jsou splněny následující podmínky:*
1) $M \neq \emptyset$ a $+$ a $\cdot$ jsou binární operace, vzhledem ke kterým je M uzavřená.
2) Obě operace $+$ a $\cdot$ jsou asociativní a komutativní.
3) 0 je prvek neutrální vůči $+$, 1 je prvek neutrální vůči $\cdot$, $0 \neq 1$.
4) Vzhledem k $+$ existuje ke každému prvku prvek opačný.
5) Platí distributivita, tj. $\forall a, b, c \in M$ $a \cdot (b + c) = a \cdot b + a \cdot c$.

Definice. *Řekneme, že okruh je obor integrity, pokud $\forall a, b$ $(ab = 0) \rightarrow (a = 0$ nebo $b = 0)$. Řekneme, že a dělí b, a píšeme $a|b$, pokud $\exists x : ax = b$. Obor integrity nazveme bezoutovský, pokud $\forall a, b$ $\exists x, y$ $(ax + by|a)$ & $(ax + by|b)$.*

Příklad. Bezoutovské obory integrity jsou např
1) $(\mathbb{Z}, +, \cdot, 0, 1)$,
2) $(\mathbb{Z}_p, +_p, \cdot_p, 0, 1)$, kde p je prvočíslo a $+_p$, $\cdot_p$ značí sčítání a násobení modulo p,
3) $(Q[x], +, \cdot, 0, 1)$, kde $Q[x]$ je množina všech polynomů s racionálními koeficienty, $+$ a $\cdot$ značí běžné sčítání a násobení polynomů, 0 značí funkci $p(x) = 0$ a 1 značí funkci $p(x) = 1$.

Věta. (Lagrangeova interpolační metoda) *Ke každým dvěma k-ticím čísel $b_1, \ldots, b_k, r_1, \ldots, r_k$ existuje polynom $p(x)$ stupně $k-1$ takový, že $\forall i$ $p(b_i) = r_i$. Označíme-li $P_i(x) = (x - b_1)(x - b_2) \cdots (x - b_{i-1})(x - b_{i+1}) \cdots (x - b_k)$, pak $p(x) = \sum_{i=1}^{k} \frac{P_i(x)}{P_i(b_i)} r_i$.*

Na přednášce si ukážeme, že toto řešení je jednoduchým důsledkem zobecnění čínské zbytkové věty pro bezoutovské obory integrity.