Učební text k přednášce TEORETICKÁ ARITMETIKA
Michal Marvan
Slezská univerzita v Opavě

Čínská věta o zbytcích

Čínská věta o zbytcích pojednává o řešení soustav kongruencí tvaru

$$\begin{aligned} x &\equiv_1 r_1, \\ &\vdots \\ x &\equiv_n r_n, \end{aligned}$$

kde $\equiv_i$ jsou kongruence na nějakém okruhu R, r_i jsou zadané prvky okruhu R a x je neznámá.

Připomeňme, že kongruenci na okruhu se rozumí relace ekvivalence $\equiv$ taková, že kdykoliv $x \equiv x'$ a $y \equiv y'$, pak také $x + y \equiv x' + y'$, $xy \equiv x'y'$ a $-x \equiv -x'$. Jak známo, existuje vzájemně jednoznačný vztah mezi kongruencemi na okruhu R a jeho ideály. Kongruenci $\equiv$ při něm odpovídá ideál $I_{\equiv} = \{r \in R \mid r \equiv 0\}$. A naopak, ideálu I odpovídá kongruence $\equiv_I$ taková, že $x \equiv_I y$ právě tehdy, když $x - y \in I$. Pro třídy kongruence $\equiv_I$ existuje přiléhavé označení $x + I$; platí totiž

$$[x]_{\equiv_I} = \{y \in R \mid y \equiv_I x\} = \{y \in R \mid y - x \in I\} = \{x + z \in R \mid z \in I\} =: x + I.$$

Součtem ideálů I, J okruhu R rozumíme ideál

$$I + J = \{\, i + j \mid i \in I, j \in J\}$$

(ověřte, že se jedná o ideál).

Tvrzení (Abstraktní čínská věta o zbytcích). *Buďte $I_1, \dots, I_n$ ideály v okruhu R takové, že*

$$I_i + I_j = R \quad \text{pro každé } i \neq j.$$

Pak (a) *ke každé n-tici prvků $r_1, \dots, r_n \in R$ existuje prvek $r \in R$ takový, že*

$$r \equiv_{I_1} r_1, \quad \dots, \quad r \equiv_{I_n} r_n.$$

(b) *Takový prvek r je určen jednoznačně modulo $I_1 \cap \dots \cap I_n$.*
(c) *Předpisem*

$$(r_1 + I_1, \dots, r_n + I_n) \longmapsto r + I_1 \cap \dots \cap I_n$$

je zadán izomorfismus

$$(R/I_1) \times \dots \times (R/I_n) \cong R/(I_1 \cap \dots \cap I_n).$$

Důkaz. Podle předpokladu pro každé $i \neq j$ existuje dvojice $a_{ij} \in I_i$, $b_{ij} \in I_j$ taková, že $a_{ij} + b_{ij} = 1$. Položme

$$b_i := \prod_{i \neq j} b_{ij} \in \bigcap_{i \neq j} I_j.$$

Pak

$$b_i \equiv_{I_j} 0 \qquad \text{pro } i \neq j,$$

zatímco pro $i = j$ dostáváme

$$b_i \equiv_{I_i} 1.$$

Vskutku,

$$b_i = \prod_{i \neq j} (1 - a_{ij}) \equiv_{I_i} \prod_{i \neq j} 1 = 1,$$

kde jsme použili vztah $a_{ij} \equiv_i 0$.

Položíme-li $r := r_1 b_1 + \cdots + r_n b_n$, máme $r \equiv_{I_i} 0r_1 + \cdots + 0r_{i-1} + 1r_i + 0r_{i+1} + \cdots + 0r_n = r_i$, což dokazuje tvrzení (a).

Zaveďme dále zobrazení $h : R \longrightarrow (R/I_1) \times \cdots \times (R/I_n)$ předpisem $r \longmapsto (r + I_1, \ldots r + I_n)$. Zobrazení h je zřejmě homomorfismus okruhů; podle již dokázaného tvrzení (a) je surjektivní. Jeho jádro je $\operatorname{Ker} h = \{r \in R \mid h(r) = 0\} = \{r \in R \mid r \in I_1, \ldots, r \in I_n\} = I_1 \cap \cdots \cap I_n$. Odtud

$$(R/I_1) \times \cdots \times (R/I_n) = \operatorname{Im} h \cong R/\operatorname{Ker} h = R/(I_1 \cap \cdots \cap I_n),$$

čímž je dokázáno tvrzení (c). Tvrzení (b) plyne z tvrzení (c).

Aplikací abstraktní čínské věty o zbytcích na okruh $\mathbf{Z}$ celých čísel dostáváme konkrétní čínskou větu o zbytcích. Připomeňme, že $\mathbf{Z}$ je okruh hlavních ideálů a $m\mathbf{Z}$, $m \in \mathbf{N}$, jsou veškeré jeho ideály. Jim odpovídající kongruence značíme $\equiv_m$, načež $a \equiv_m b$ platí právě tehdy, když $a - b$ je násobek čísla m. Odpovídající faktorový pokruh se značí $\mathbf{Z}_m = \mathbf{Z}/m\mathbf{Z}$.

Tvrzení (Konkrétní čínská věta o zbytcích). *Buďte $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla. Pak* (a) *ke každé n-tici celých čísel $r_1, \ldots, r_n \in \mathbf{Z}$ existuje číslo $r \in \mathbf{Z}$ takové, že*

$$r \equiv_{m_1} r_1, \quad \cdots, \quad r \equiv_{m_n} r_n.$$

(b) *Takové číslo r je určeno jednoznačně modulo $m_1 \cdots m_n$.*

(c) *Předpisem*

$$(r_1 + m_1\mathbf{Z}, \ldots, r_n + m_n\mathbf{Z}) \longmapsto r + m_1 \cdots m_n\mathbf{Z}$$

je zadán izomorfismus

$$\mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_n} \cong \mathbf{Z}_{m_1 \cdots m_n}.$$

Důkaz. Tvrzení získáme jako důsledek abstraktní čínské věty o zbytcích volbou $R = \mathbf{Z}$, $I_i = m_i\mathbf{Z}$, načež $R/I_i = \mathbf{Z}/m_i\mathbf{Z} = \mathbf{Z}_{m_i}$. Ověřme platnost podmínky $m_i\mathbf{Z} + m_j\mathbf{Z} = \mathbf{Z}$ pro $i \neq j$. Podle předpokladu jsou čísla m_i, m_j nesoudělná, načež existují čísla u, v taková, že $1 = m_i u + m_j v$. Pro libovolné $a \in \mathbf{Z}$ pak vskutku máme $a = m_i ua + m_j va$, kde $m_i ua \in m_i\mathbf{Z}$ a $m_j va \in m_j\mathbf{Z}$.

Dále z abstraktní čínské věty o zbytcích plyne izomorfismus

$$\mathbf{Z}_{m_1} \times \cdots \times \mathbf{Z}_{m_n} \cong \mathbf{Z}/(m_1\mathbf{Z} \cap \cdots \cap m_n\mathbf{Z}).$$

Zbývá jen ověřit rovnost $m_1\mathbf{Z} \cap \cdots \cap m_n\mathbf{Z} = m_1 \cdots m_n\mathbf{Z}$. Dokažme inkluzi "$\subseteq$". Nechť $z \in m_1\mathbf{Z} \cap \cdots \cap m_n\mathbf{Z}$, tj. nechť z je společným násobkem čísel $m_1, \ldots, m_n$. Z předpokladu nesoudělnosti plyne, že žádná dvě čísla m_i, m_j nemají polečného prvočinitele. Jejich nejmenší společný násobek je proto roven jejich součinu $m_1 \cdots m_n$, tj. z je násobkem $m_1 \cdots m_n$, což se mělo dokázat. Inkluze "$\supseteq$" je zřejmá.

Konkrétní čínská věta o zbytcích vlastně říká, že za předpokladů o nesoudělnosti modulů m_i je množina všech celočíselných řešení soustavy kongruencí

$$x \equiv_{m_1} r_1, \quad \cdots, \quad x \equiv_{m_n} r_n.$$

s neznámou x totožná s množinou všech celočíselných řešení jediné kongruence

$$x \equiv_{m_1 \cdots m_n} r$$

pro vhodné r.

Obecně můžeme řešit soustavu n kongruencí například tak, že postupně redukujeme podsoustavy složené z prvních k kongruencí, $k = 2, \ldots, n$, na jedinou kongruenci.

Příklad. Řešte systém kongruencí

$$x \equiv_6 2, \quad x \equiv_5 1, \quad x \equiv_7 4.$$

Řešení: Platí $D(6,5) \parallel 1$, $D(6,7) \parallel 1$, $D(5,7) \parallel 1$, a proto podle konkrétní čínské věty o zbytcích celočíselné řešení x existuje a je jediné modulo $6 \cdot 5 \cdot 7 = 210$.

V prvním kroku řešme podsoustavu složenou z prvních dvou kongruencí. Můžeme je zapsat ve tvaru $6p + 2 = x = 5q + 1$ s neznámými $p, q \in \mathbf{Z}$, tedy

$$6p - 5q = -1.$$

Máme však $D(6,-5) \parallel 1$, načež existují celočíselná řešení rovnice $6u - 5v = 1$, např. $u = 6, v = 7$ (nalézt je můžeme s pomocí rozšířeného Eukleidova algoritmu). Odtud $p = -1 \cdot 6 = 6$, $q = -1 \cdot 7 = -7$, což vede na řešení $x = 6p + 2 = 6 \cdot (-6) + 2 = -34$, které je podle čínské věty o zbytcích jednoznačně určeno modulo $6 \cdot 5 = 30$. Tudíž, obecné řešení první podsoustavy je $x \equiv_{30} -34$, čili $x \equiv_{30} -4$.

V druhém kroku řešme soustavu vzniklou z obecného řešení předchozí podsoustavy a z další kongruence soustavy, tedy

$$x \equiv_{30} -4, \quad x \equiv_7 4.$$

Podobně jako v prvním kroku hledáme celočíselná řešení rovnice $30p - 4 = 7q + 4$, tj.

$$30p - 7q = 8.$$

Opět $D(30,7) \parallel 1$, načež má rovnice $30u - 7v = 1$ celočíselná řešení, např. $u = 4$, $v = 17$, a odtud $p = 8 \cdot 4 = 32$, $q = 8 \cdot 17 = 136$. Dostáváme tedy $x = 30p - 4 = 30 \cdot 32 - 4 = 956$ modulo $30 \cdot 7 = 210$, čili $x \equiv_{210} 956 \equiv_{210} 116$, což je již konečný výsledek. Odpověď tedy zní: obecné řešení soustavy je $x \equiv_{210} 116$.