2 Kongruence a divoká jízda po okruzích

Zadání
Verze ze dne 27. února 2024

Cíle cvičení: Ke zdárnému počítání kongruencí si osvojíme využití Eulerovy věty a naučíme se řešit soustavy lineárních kongruencí, což odpovídá nalezení vzoru v Čínské větě o zbytcích. Poté už se vrhneme na abstraktní algebru. Rozmyslíme si, jak bezpečně poznat, co je okruhem, oborem, tělesem či jakoukoli jinou algebraickou strukturou, což je často nepříjemná a zdlouhavá procedura. Naopak, jakmile se nás někdo zeptá na podstrukturu, pochopíme, že je to důvod k velké radosti, neboť jde obvykle o mnohem snazší úkol.

Úlohy, které bychom určitě měli umět řešit:

Úloha 2.1. Spočítejte (a) $3^{5^7} \bmod 28$, (b) poslední cifru čísla 1357^{246}.

Úloha 2.2. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 7$, $x \equiv 3 \pmod 8$.

(b) $2x + 1 \equiv 2 \pmod 3$, $3x + 2 \equiv 3 \pmod 4$, $4x + 3 \equiv 2 \pmod 5$.

(c) $10x \equiv 6 \pmod{32}$, $3x \equiv 1 \pmod 5$

Úloha 2.3. Najděte příklad, na kterém bude vidět nezbytnost předpokladu nesoudělnosti čísel m_i v Čínské větě o zbytcích ve skriptech.

Úloha 2.4. Uvážíme čtyři šestice:
$\mathcal{Z} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ celá čísla s obvyklými operacemi a vybranými prvky,
$\mathcal{Z}_7 = (\mathbb{Z}_7, +, -, \cdot, 0, 1)$ celá čísla modulo 7 s obvyklými operacemi a prvky,
$\mathcal{Z}^2 = (\mathbb{Z}^2, +, -, \cdot, (0, 0), (1, 1))$ dvojice s operacemi a prvky definovanými po složkách na $\mathbb{Z}$
$\mathcal{M}_2 = (\mathbb{Z}_7^{2\times 2}, +, -, \cdot, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$ matice 2×2 nad $\mathbb{Z}_7$ s obvyklými operacemi a prvky .

(a) Načrtněte důkaz, že všechny šestice tvoří okruh (tj. přesně uveďte, co všechno je třeba ověřit),

(b) rozhodněte, které ze šestic tvoří komutativní okruh,

(c) rozhodněte, které ze šestic tvoří obor,

(d) rozhodněte, které ze šestic tvoří těleso.

Úloha 2.5. Rozhodněte pro podmnožiny tělesa komplexních čísel $\mathcal{C} = (\mathbb{C}, +, -, \cdot, 0, 1)$:
$\mathcal{R}_1 = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, $\mathcal{R}_2 = \{a + b\sqrt{2} + c\sqrt{3} : a, b, c \in \mathbb{Z}\}$,
$\mathcal{R}_3 = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, $\mathcal{R}_4 = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b \in \mathbb{Q}\}$.

(a) které ze šestic $\mathcal{R}_i = (R_i, +, -, \cdot, 0, 1)$, $i = 1, \ldots, 4$, tvoří podokruhy okruhu $\mathcal{C}$,

(b) které z šestic $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{R}_3$ tvoří podtělesa tělesa $\mathcal{C}$.

Úloha 2.6. Je-li $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Z}\}$ a $\mathbb{Q}[i] = \{a + bi \in \mathbb{C} : a, b \in \mathbb{Q}\}$, ověřte, že

(a) $\mathcal{Z}[i] = (\mathbb{Z}[i], +, -, \cdot, 0, 1)$ a $\mathcal{Q}[i] = (\mathbb{Q}[i], +, -, \cdot, 0, 1)$ jsou podokruhy tělesa komplexních čísel,

(b) $\mathcal{Z}[i]$ je obor integrity a $\mathcal{Q}[i]$ je těleso,

(c) zobrazení $f(\frac{a_1+a_2 i}{b_1+b_2 i}) = \frac{a_1 b_1 + a_2 b_2}{b_1^2+b_2^2} + \frac{a_2 b_1 - a_1 b_2}{b_1^2+b_2^2} i$ je dobře definovaný izomorfismus podílového tělesa oboru $\mathcal{Z}[i]$ na těleso $\mathcal{Q}[i]$.

A na závěr záplava úloh pro zábavu i poučení:

Úloha 2.7. Spočítejte (a) $100^{99^{98}} \bmod 39$, (b) $100^{99^{98}} \bmod 40$.

Úloha 2.8. Určete poslední dvě cifry čísla $999^{888^{777}}$ a poslední tři cifry čísla 249^{19}.

Úloha 2.9. Dokažte, že pro každé prvočíslo $p \neq 2$ platí $p \mid 1^p + 2^p + 3^p + \ldots + p^p$.

Úloha 2.10. Dokažte, že

(a) 13 dělí $23^{32} + 29^{33} + 36^{34}$,

(b) $9 \mid 4^n + 6n - 1$ pro každé n přirozené.

Úloha 2.11. Najděte všechna $x \in \mathbb{Z}$ splňující $26^5 x \equiv 16 \pmod{11}$.

Úloha 2.12. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} 13x \equiv 15 \pmod{27} \\ 2x \equiv 1 \pmod{3}. \end{cases}$

Úloha 2.13. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $x^2 \equiv 1 \pmod{3}$, $x^2 \equiv 1 \pmod{7}$.

(b) $x^2 \equiv -1 \pmod{66}$.

(c) $x^2 \equiv -1 \pmod{65}$.

Úloha 2.14. Najděte všechna $x \in \mathbb{Z}$, pro která platí $\begin{cases} 3^x \equiv 1 \pmod{13} \\ 3x \equiv 1 \pmod{13}. \end{cases}$

Úloha 2.15. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod{7}$.

Úloha 2.16. Najděte všechna $x \in \{0, 1, \ldots, 76\}$ splňující $x^2 + 8x \equiv 62 \pmod{77}$.

Úloha 2.17.* Ověřte, že $\mathcal{R}_4$ z 2.5 tvoří podtěleso tělesa $\mathcal{C}$.

Úloha 2.18. Rozhodněte, zda množiny $S_1 = \{a + b\sqrt[3]{2} :\ a, b \in \mathbb{Z}\}$ a $S_2\{a + b\zeta :\ a, b \in \mathbb{Z}\}$, kde $\zeta = e^{\pi i/4}$, tvoří nosné množiny podokruhů tělesa komplexních čísel $(\mathbb{C}, +, -, \cdot, 0, 1)$.

Úloha 2.19.* Jestliže alespoň dvouprvkovou množinu X označíme $P(X) = \{Y : Y \subseteq X\}$ $\triangle, -, \cap, \emptyset, X)$ a pro každé $A, B \in P(X)$ je $A \triangle B = (A \cup B) \setminus (A \cap B)$ (tedy $\triangle$ je operace symetrické diference) a $-A = A$, rozhdoněte, zda šestice $(P(X), \triangle, -, \cap, \emptyset, X)$ tvoří komutativní okruh nebo obor.