2 Kongruence a divoká jízda po okruzích

Řešení
Verze ze dne 28. 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}.

Řešení. (a) Protože $\varphi(28) = 12$, $\varphi(12) = 4$ a dále $\mathrm{NSD}(3, 28) = 1 = \mathrm{NSD}(5, 12)$, využijeme dvakrát Eulerovu větu, díky níž

$$3^{5^7} \equiv 3^{(5^7) \bmod 12} \pmod{28}$$

a

$$5^7 \equiv 5^{7 \bmod 4} \equiv 5^3 \equiv 5 \pmod{12}.$$

Dostáváme tak, že

$$3^{5^7} \equiv 3^5 = 27 \cdot 9 \equiv (-1) \cdot 9 \equiv 19 \pmod{28}.$$

Tedy $3^{5^7} \bmod 28 = 19$.

(b) Využijeme Eulerovu větu a spočítáme kongruenci

$$1357^{246} \equiv 7^{(246) \bmod 4} \equiv 7^2 \equiv 9 \pmod{10},$$

odkud plyne, že poslední cifra 1357^{246} je 9.

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

Řešení. Postupně budeme dosazovat obecné řešení prvních $i - 1$ kongruencí do i-té kongruence.

(a) Okamžitě vidíme, že $x \equiv 2 \pmod 3$ právě když $x = 2 + 3a$ pro $a \in \mathbb{Z}$, proto dosazením za x do druhé kongruence dostaneme pomocí ekvivalentních úprav kongruencí

$$2 + 3a \equiv x \equiv 4 \pmod 7 \quad \Leftrightarrow \quad 3a \equiv 2 \pmod 7 \quad \Leftrightarrow \quad a \equiv 3 \pmod 7.$$

Nyní $a = 3 + 7b$, a proto $x = 2 + 3(3 + 7b)) = 11 + 21b$ pro libovolné $b \in \mathbb{Z}$. Dosazením vyjádření x pomocí b do třetí kongruence dostaneme

$$3 + 5b \equiv 11 + 21b \equiv x \equiv 3 \pmod 8 \quad \Leftrightarrow \quad 5b \equiv 0 \pmod 8 \quad \Leftrightarrow \quad b \equiv 0 \pmod 8,$$

proto $b = 8c$ a $x = 11 + 21 \cdot 8c = 11 + 168c$ pro libovolné $c \in \mathbb{Z}$.

(b) Kongruence nejprve převedeme na tvar

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 4, \quad x \equiv 1 \pmod 5$$

a pak stejným postupem jako v (a) spočteme obecné řešení tvaru $11 + 60m$ pro $m \in \mathbb{Z}$.

(c) Nejprve ekvivalentně upravíme první kongruenci pomocí krácení modulu a obou stran na tvar

$$5x \equiv 3 \pmod{16} \;\Leftrightarrow\; x \equiv (-3) \cdot 5x \equiv -9 \equiv 7 \pmod{16}.$$

Druhou kongruenci poté ekvivalentně převedeme na tvar $x \equiv 2 \pmod 5$ a pak obvyklým postupem spočítáme řešení $7 + 80m$ pro libovolné $m \in \mathbb{Z}$.

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

Řešení. Například soustava kongruencí $\begin{cases} x \equiv 0 \bmod 2 \\ x \equiv 1 \bmod 4 \end{cases}$ nemá řešení.

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.

Řešení. (a) Musíme ověřit kompletní axiomatiku pojmu okruh. Zde je potřeba si uvědomit, že všechna + a $\cdot$ představují symboly asociativních binárních operací, dále, že + je komutativní, že 0 (respektive $(0,0)$ nebo $(0)_{ij}$) je neutrální prvek operace + a $-$ představuje symbol unární operace určující inverzní (nebo lépe opačný) prvek vzhledem k +. Dále musíme ukázat, že 1 (respektive $(1,1)$ nebo I_2) představuje neutrální prvek operace $\cdot$ a že je + vzhledem k $\cdot$ oboustranně distributivní. Tedy například pro šestici $\mathcal{Z}^2$ ověřujeme s využitím známých vlastností operací v celých číslech pro všechna $(a,b), (c,d), (e,f) \in \mathbb{Z}^2$ (a už nikdy v životě to nechceme opakovat):

$$(a,b) + ((c,d) + (e,f)) = (a + c + e, b + d + f) = ((a,b) + (c,d)) + (e,f),$$

$$(a,b) \cdot ((c,d) \cdot (e,f)) = (a \cdot c \cdot e, b \cdot d \cdot f) = ((a,b) \cdot (c,d)) \cdot (e,f),$$

$$(a,b) + (c,d) = (a + c, b + d) = (c,d) + (a,b), \quad (a,b) + (0,0) = (a,b),$$

$$(a,b) + (-a,-b) = (-a,-b) + (a,b) = (0,0), \quad (a,b) \cdot (1,1) = (1,1) \cdot (a,b) = (a,b),$$

$$(a,b) \cdot ((c,d) + (e,f)) = (a \cdot (c + e), b \cdot (d + f)) = ((a,b) \cdot (c,d)) + ((a,b) \cdot (e,f)),$$

$$((c,d) + (e,f)) \cdot (a,b) = ((c + e) \cdot a, (d + f) \cdot b) = ((c,d) \cdot (a,b)) + ((e,f) \cdot (a,b)).$$

(b) Musíme zjistit, které z operací $\cdot$ jsou komutativní, tedy kdy $\alpha \cdot \beta = \beta \cdot \alpha$ pro všechny dvojice prvků α, β daného okruhu, což nastává právě pro $\mathcal{Z}$, $\mathcal{Z}^2$ a $\mathcal{Z}_7$. V $\mathcal{M}_2$ například

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

(c) Vybíráme z komutativních okruhů v (b) ty, pro něž $a \cdot b \neq \mathbf{0}$ (kde $\mathbf{0}$ představuje neutrální prvek operace $+$) pro všechny dvojice nenulových prvků a, b, což splňují okruhy $\mathcal{Z}$ a $\mathcal{Z}_7$. Naopak v $\mathcal{Z}^2$ vidíme, že například $(1,0) \cdot (0,1) = (0,0)$, proto nejde o obor.

(d) Nyní už vybíráme jen z oborů, protože každé těleso podle tvrzení z přednášky oborem je. Rozhodujeme otázku, zda je každý nenulový prvek daného oboru invertibilní, což platí pro $\mathcal{Z}_7$ a jde tak o těleso, a neplatí pro $\mathcal{Z}$.

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

(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 $\mathcal{C}$.

Řešení. (a) Tentokrát se na rozdíl od úlohy 2.4 neptáme po vlastnostech operací, ty už známe, neboť víme, že $\mathcal{C}$ představuje těleso. Stačí nám jen ověřit, že oba výjimečné prvky 0 a 1 leží v dané nosné množině (což zjevně platí) a pak zbývá zjistit, zda jsou naše množiny uzavřené na všechny tři operace.

Vezmeme-li dvojici prvků $a_i + b_i\sqrt{2} \in R_1$ pro $i = 1, 2$, pak snadno spočteme, že

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in R_1,$$

$$-(a_1 + b_1\sqrt{2}) = -a_1 - b_1\sqrt{2} \in R_1,$$

$$(a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \in R_1,$$

proto je $\mathcal{R}_1$ podokruhem oboru $\mathcal{C}$.

Obdobně bychom nahlédli, že množina R_2 je uzavřená na operaci $+$, ovšem hodnotu součinu $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$ nelze vyjádřit ani jako racionální lineární kombinaci čísel 1, $\sqrt{2}$, $\sqrt{3}$, protože jsou hodnoty 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ nad tělesem racionálních čísel lineárně nezávislé (důkaz viz 2.17), tedy $\sqrt{2} \cdot \sqrt{3} \notin R_2$, proto $\mathcal{R}_2$ podokruhem není.

Uzavřenost množiny R_3 na operace se dokáže úplně stejně jako v případě $\mathcal{R}_1$, proto $\mathcal{R}_3$ opět podokruhem je.

Konečně uzavřenost množiny R_3 na operace $+$ a $-$ se opět ověří obdobným argumentem jako v případě podokruhu $\mathcal{R}_1$ a snadno spočítáme součin prvků $(a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}) \cdot (a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}) =$

$$(a_1a_2 + 2b_1c_2 + 2c_1b_2) + (a_1b_2 + b_1a_2 + 2c_1c_2)\sqrt[3]{2} + (a_1c_2 + c_1a_2 + b_1b_2)\sqrt[3]{4} \in R_4,$$

čímž jsme dokázali, že je $\mathcal{R}_4$ podokruhem $\mathcal{C}$.

(b) Protože jsme zjistili, že $\mathcal{R}_2$ není podokruh, zbývá rozhodnout, zda pro dané $i = 1, 3$ a všechny nenulové prvky z $a + b\sqrt{2} \in R_i$ platí, že $(a + b\sqrt{2})^{-1} \in R_i$. Inverzní prvky ovšem v $\mathbb{C}$ umíme spočítat a víme, že se musí shodovat s případnými inverzními prvky podokruhu. Zvolíme-li například prvek 2, pak $2^{-1} \notin R_1$, proto $\mathcal{R}_1$ netvoří podtěleso. Naopak

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \cdot \sqrt{2}.$$

Protože jsou pro každou dvojici $(a, b) \in \mathbb{Q}^2 \setminus \{(0, 0)\}$ oba koeficienty $\frac{a}{a^2-2b^2}$, $\frac{b}{a^2-2b^2}$ racionální, leží inverzní prvek opět v R_3.

Zjistili jsme, že z prvních tří šestic tvoří podtěleso pouze obor $\mathcal{R}_3$.

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 a $\mathcal{Q}[i]$ je těleso,

(c) zobrazení $f(\frac{a_1+a_2i}{b_1+b_2i}) = \frac{a_1b_1+a_2b_2}{b_1^2+b_2^2} + \frac{a_2b_1-a_1b_2}{b_1^2+b_2^2}i$ je dobře definovaný izomorfismus podílového tělesa oboru $\mathcal{Z}[i]$ na těleso $\mathcal{Q}[i]$.

Řešení. (a) Stejně jako v 2.5 stačí ukázat, že jsou obě množiny $\mathbb{Z}[i]$ a $\mathbb{Q}[i]$ uzavřené na všechny tři operace, proveďme to například pro $\mathbb{Z}[i]$, v druhém případě by byl důkaz úplně stejný. V zápisu můžeme využít časté chápání operace $-$ jako binární prostřednictvím předpisu $a - b = a + (-b)$ (uvědomte si, že místo uzavřenosti na operace původní operace + a $-$ můžeme ověřovat uzavřenost na dvojici binárních operací + a $-$). Tedy pro každé $(a_1 + a_2i), (b_1 + b_2i) \in \mathbb{Z}[i]$ dostáváme

$$(a_1 + a_2i) \pm (b_1 + b_2i) = (a_1 \pm b_1) + (a_2 \pm b_2)i \in \mathbb{Z}[i]$$

$$(a_1 + a_2i) \cdot (b_1 + b_2i) = (a_1b_1 - a_2b_2) + (a_1b_2 + a_2b_1)i \in \mathbb{Z}[i]$$

(b) Protože z (a) víme, že jde o podokruhy tělesa, máme tím už dokázáno, že se jedná o obory integrity, tedy žádné axiomy oboru nebo tělesa už ověřovat nemusíme. Zbývá pouze nahlédnout, že každý inverzní prvek (v tělese komplexních čísel) k nenulovému prvku $a_1 + a_2i \in Q[i]$, kde tedy $a_1, a_2 \in \mathbb{Q}$ opět leží v $Q[i]$, což platí, neboť

$$(a_1 + a_2i)^{-1} = \frac{a_1 - a_2i}{a_1^2 + a_2^2} = \frac{a_1}{a_1^2 + a_2^2}i\frac{a_2}{a_1^2 + a_2^2}i \in Q[i].$$

(c) Nejprve si uvědomíme, že pro každé $a, b \in \mathbb{Z}[i]$ platí $f(\frac{a}{b}) = \frac{a\cdot\overline{b}}{b\cdot\overline{b}} = \frac{a\cdot\overline{b}}{|b|^2}$, dále si všimneme, že obraz f leží v $\mathbb{Q}[i]$ a poté si rozmyslíme, že je zobrazení korektně definované. Mějme dvě vyjádření $\frac{a}{b} = \frac{c}{d}$ téhož prvku podílového tělesa a všimněme si, potom

$$f(\frac{a}{b}) = \frac{a}{b}\frac{\overline{b}}{\overline{b}} = \frac{c}{d}\frac{\overline{b}}{\overline{d}} = f(\frac{c}{d}).$$

Ověřili jsme, že je definice nezávislá na výběru reprezentantů daného racionálního čísla, a tudíž korektní.

Zbývá nahlédnout, že $f(\frac{0}{1}) = 0$ a $f(\frac{1}{1}) = 1$ a podobně jako u důkazu korektnosti ověřit, že zobrazení přenáší operace, tedy že pro každý zlomek $\frac{a}{b}, \frac{c}{d}$ z podílového tělesa platí

$$f(\frac{a}{b} \pm \frac{c}{d}) = f(\frac{ad \pm bc}{bd}) = \frac{ad \pm bc}{bd} \cdot \frac{\overline{bd}}{\overline{bd}} = \frac{a}{b}\frac{\overline{b}}{\overline{b}} \pm \frac{c}{d}\frac{\overline{d}}{\overline{d}} = f(\frac{a}{b}) \pm f(\frac{c}{d}),$$

$$f(\frac{a}{b} \cdot \frac{c}{d}) = \frac{ac}{bd} \cdot \frac{\overline{bd}}{\overline{bd}} = \frac{a}{b}\frac{\overline{b}}{\overline{b}} \cdot \frac{c}{d}\frac{\overline{d}}{\overline{d}} = f(\frac{a}{b}) \cdot f(\frac{c}{d}).$$

A na závěr záplava úloh pro zábavu i poučení:

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

Řešení. (a) Postupujeme podobně jako v 2.1(a). Protože $\varphi(39) = 24$ a $\mathrm{NSD}(22, 39) = 1$, dostaneme s využitím Eulerovy věty kongruenci:

$$100^{99^{98}} \equiv 22^{(99^{98}) \bmod 24} \pmod{39}.$$

Dále počítáme

$$99^{98} \equiv 3^{98} \equiv 3 \cdot 3^{97} \pmod{24}.$$

Základ mocniny a modul jsou soudělné, proto nemůžeme využít Eulerovu větu přímo, ale protože

$$3^{97} \equiv 3^{(97)) \bmod 4} \equiv 3^1 \equiv 3 \pmod 8,$$

dostáváme s využitím vlastností kongruencí (konkrétně té, která nám umožňuje vydělit konstantou modul a obě strany kongruence)

$$99^{98} \equiv 3 \cdot 3^{97} \equiv 3 \cdot 3 \equiv 9 \pmod{3 \cdot 8}.$$

Nyní zbývá například (ne zas tak moc) hrubou silou spočítat, že $(22^3) \bmod 3 = 1$ a tudíž

$$100^{99^{98}} \equiv 22^9 \equiv (22^3)^3 \equiv 1^3 \equiv 1 \pmod{39}.$$

(b) Tentokrát Eulerovu větu kvůli soudělnosti základu modulu využít nemůžeme, ale ani ji naštěstí nepotřebujeme, místo toho si všimneme-li, že $40 \mid 100^2 \mid 100^{99^{98}}$, a proto $100^{99^{98}} \bmod 40 = 0$.

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

Řešení. Stačí si jen všimnout, že $999^2 \equiv (-1)^2 \equiv 1 \pmod{100}$, proto

$$999^{888^{777}} \equiv ((-1)^2)^{888^{777}/2} \equiv 1^{888^{777}/2} \equiv 1 \pmod{100},$$

Tudíž poslední dvě cifry druhé mocniny jsou 01.

V druhém případu nás zajímá hodnota $249^{19} \bmod 1000$. Nejprve spočítáme

$$249^2 \equiv (250-1)^2 \equiv 250 \cdot (250-2) + 1 \equiv 62 \cdot 4 \cdot 250 + 1 \equiv 1 \pmod{1000},$$

proto $249^{19} \bmod 1000 = 249$ a poslední 3 cifry mocniny jsou 249.

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

Řešení. Podle Eulerovy (respektive Malé Fermatovy) věty pro každé $i = 1, \ldots, p-1$ platí, že $i^p \equiv i \pmod p$, proto

$$1^p + 2^p + 3^p + \ldots + p^p \equiv 1 + 2 + 3 + \ldots + p - 1 + 0 \equiv \frac{p(p-1)}{2} \equiv 0 \pmod p,$$

neboť p je liché prvočíslo, $\frac{p-1}{2}$ je přirozené a tudíž p dělí číslo $\frac{p(p-1)}{2}$.

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.

Řešení. (a) Pomocí modulární aritmetiky, resp. Eulerovy věty zjistíme, že platí $23^{32} \equiv 9 \pmod{13}$, $29^{33} \equiv 1 \pmod{13}$, $36^{34} \equiv 3 \pmod{13}$ a součet je tedy modulo 13 roven 0.

(b) Dokážeme indukcí dle n. Pro $n = 1$ tvrzení zřejmě platí.

Platí-li tvrzení pro $n \geq 1$, pak $4^n \equiv 1 - 6n \pmod 9$, proto

$$4^{n+1} + 6(n+1) - 1 \equiv 4 \cdot (4^n) + 6n + 5 \equiv 4 \cdot (1 - 6n) + 6n + 5 \equiv -18n + 9 \equiv 0 \pmod 9$$

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

Řešení. Nejprve pomocí Eulerovy věty spočítáme

$$26^5 \equiv 4^5 \equiv 2^{10} \equiv 2^{(10)} \equiv 1 \pmod{11},$$

Nyní snadno vyřešíme ekvivalentní kongruenci $x \equiv 5 \pmod{11}$ a snadno určíme všechna řešení $5 + 11k$ pro libovolné $k \in \mathbb{Z}$.

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

Řešení. Z první kongruence plyne, že $x \equiv 0 \pmod{3}$, zatímco druhá říká, že $x \equiv 2 \pmod{3}$, proto je množina řešení prázdná.

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

Řešení. (a) Z prvního cvičení víme, že rovnice $x^2 \equiv 1 \pmod{p}$ má pro prvočíslo p řešení právě $\pm 1 + k \cdot p$ pro $k \in \mathbb{Z}$. Dostaneme 4 možné soustavy (kombinace) lineárních kongruencí, které vyřešíme stejným postupem jako v úloze 2.2 a dostaneme tak množinu všech řešení

$$\{1 + 21m \mid m \in \mathbb{Z}\} \cup \{8 + 21m \mid m \in \mathbb{Z}\} \cup \{13 + 21m \mid m \in \mathbb{Z}\} \cup \{20 + 21m \mid m \in \mathbb{Z}\}.$$

(b) Protože řešení kongruence $x^2 \equiv -1 \pmod{66}$ by řešilo i kongruenci $x^2 \equiv -1 \pmod{3}$, která zjevně žádné řešení nemá. Je množina všech řešení naší kongruence prázdná.

(c) Nejprve vyřešíme soustavu kongruencí $\begin{cases} x^2 \equiv -1 \pmod{5} \\ x^2 \equiv -1 \pmod{13} \end{cases}$, což lze provést hrubou silou počítáním v tělesech $\mathbb{Z}_5$ a $\mathbb{Z}_{13}$, tedy $x \equiv \pm 2 \pmod{5}$ a $x \equiv \pm 5 \pmod{13}$ a poté opětovným použitím Čínské větu o zbytcích dostaneme množinu všech řešení

$$\{8 + 65m \mid m \in \mathbb{Z}\} \cup \{-8 + 65m \mid m \in \mathbb{Z}\} \cup \{18 + 65m \mid m \in \mathbb{Z}\} \cup \{-18 + 65m \mid m \in \mathbb{Z}\}.$$

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

Řešení. Z druhé kongruence dostáváme vyjádření $x = 9 + 13a$, která když dosadíme do druhé kongruence a využijeme Eulerovu větu, dostaneme

$$3^x \equiv 3^{(9+13a) \bmod 12} \equiv 3^{(9+a) \bmod 12} \equiv 1 \pmod{13}.$$

Všimneme-li si, že $3^i \equiv 1 \pmod{13} = 1$, právě když $3 \mid i$, pak řešíme kongruenci $9 + a \equiv 0 \pmod{3}$. Tudíž $a = 3k$ a obecné řešení je tvaru $9 + 39k$ pro $k \in \mathbb{Z}$.

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

Řešení. Pro $x \equiv 0 \pmod{7}$ zřejmě rovnice žádné řešení nemá a pokud $x \not\equiv 0 \pmod{7}$ platí podle Eulerovy věty, že $x^6 \equiv 1 \pmod{7}$. Tudíž se kongruence redukuje na $x(1 + y) \equiv 0 \pmod{7}$, což je díky tomu, že 7 je prvočíslo ekvivalentní podmínce $x \equiv 0 \pmod{7}$ nebo $y \equiv 6 \pmod{7}$, a proto máme řešení právě pro $x \not\equiv 0$, $y \equiv 6 \pmod{7}$.

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

Řešení. Převeďme na $x^2+8x+15=(x+3)(x+5)\equiv 0 \pmod{77}$, pomocí Čínské věty o zbytcích vyřešíme modulo 7, resp. 11 čtyři možné případy a zvedneme zpět modulo 77 a dostaneme řešení $30, 39, 72, 74$.

Úloha 2.17.* Dokažte, že je čtveřice prvků $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ lineárně nezávislá ve vektorovém prostoru komplexních čísel nad tělesem racionálních čísel.

Řešení. Tvrzení dokážeme sporem. Existuje-li nějaká netriviální racionální lineární kombinace čísel $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, jejímž výsledkem je nula, pak existuje netriviální celočíselná lineární kombinace (rovnost vynásobíme společným jmenovatelem všech zlomků), jejíž čtveřice koeficientů nemá žádného netriviálního společného dělitele (celou rovnost vydělíme největším společným dělitelem všech koeficientů). Napíšeme si ji ve tvaru

$$a+b\sqrt{2}=c\sqrt{3}+d\sqrt{6}=\sqrt{3}(c+d\sqrt{2}),$$

pro $a,b,c,d\in Z$ a $\mathrm{NSD}(a,b,c,d)=1$. Umocníme-li rovnost na druhou, dostaneme:

$$a^2+2b^2+2ab\sqrt{2}=3(c^2+2d^2+2cd\sqrt{2}).$$

Protože je $\sqrt{2}$ iracionální, je dvojice 1 a $\sqrt{2}$ lineárně nezávislá nad $\mathbb{Q}$ a předchozí rovnost nám tak srovnáním koeficientů lineárních kombinací této posloupnosti dá dvojici rovností:

$$a^2+2b^2=3(c^2+2d^2),\quad 2ab=6cd.$$

Z první rovnosti plyne, že $3 \mid (a^2+2b^2)$ a z druhé $3 \mid ab$, a proto $3 \mid a$ nebo $3 \mid b$. Pokud $3 \mid a$ a $3 \mid (a^2+2b^2)$, platí, že $3 \mid 2b^2=(a^2+2b^2)-a^2$, tedy $3 \mid b$. Podobně, pokud 3 dělí b i a^2+2b^2 dostáváme $3 \mid a$, což znamená, že 3 dělí obě čísla a i b. Tudíž $9 \mid a^2+2b^2=3(c^2+2d^2)$ a $9 \mid ab=3cd$, a tudíž $3 \mid (c^2+2d^2)$ a $3 \mid cd$. Nyní opakovaným argumentem jako pro a,b dostáváme, že 3 dělí rovněž obě hodnoty c i d. Našli jsme společný dělitel 3 čtveřice a,b,c,d, což je spor s jejich nesoudělností.

Úloha 2.18.* Ověřte, že $\mathcal{R}_4$ z 2.5 tvoří podtěleso tělesa $\mathcal{C}$.

Řešení. Postupujeme jako v 2.5 a hledaný inverzní prvek vyjádříme jako řešení nehomogenní soustavy lineárních rovnic s koeficienty v $\mathbb{Q}$, o níž si lineárně algebraickými prostředky uvědomíme, že má řešení.

Úloha 2.19. 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 $(\mathbb{C},+,-,\cdot,0,1)$.

Řešení. Snadno si rozmyslíme, že $\sqrt[3]{2}\cdot\sqrt[3]{2}=\sqrt[3]{4}\notin S_1$ a že $e^{\pi i/4}\cdot e^{\pi i/4}=e^{\pi i/2}=i\notin S_2$, tedy množiny nejsou uzavřené na násobení a nemůže se tak jednat o nosné množiny podokruhů.

Úloha 2.20.* Jestliže alespoň dvouprvkovou množinu X označíme $P(X)=\{Y:Y\subseteq X\}$ 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 $-A=A$, rozhodněte, zda šestice $(P(X),\triangle,-,\cap,\emptyset,X)$ tvoří komutativní okruh nebo obor.

Řešení. Po ověření axiomů zjistíme, že se jedná o komutativní okruh. Pokud zvolíme jednoprvkovou množinu $A=\{a\}$ a položíme $B=X\setminus A$, pak $A\cap B=\emptyset$, ačkoli $A\neq\emptyset\neq B$, proto nejde o obor.