Algebra — cvičení 1, řešení

2. (c) Pro každé $x \in \mathbb{Z}$ platí $6x \equiv 2 \pmod 8$ dle **1(a)** právě tehdy, když $3x \equiv 1 \pmod 4$. To je dále, užitím **1(b)**, ekvivalentní s $x \equiv 3 \pmod 4$. Závěr: Kongruenci řeší právě celá čísla tvaru $4k + 3$, kde $k \in \mathbb{Z}$.

Tady bych snad upozornil jen na to, že neplatí $3x \equiv 1 \pmod 4 \iff 6x \equiv 2 \pmod 4$, tj. vynásobení dvěma v $\mathbb{Z}_4$ není ekvivalentní úprava, jelikož 2 nemá v $\mathbb{Z}_4$ inverní prvek vzhledem k násobení (což dokazuje, že $\mathbb{Z}_4$ není těleso). Stačí dosadit $x = 1$.

2. (d) Platí $x^2 \equiv 36 \pmod{45} \iff x^2 - 36 \equiv 0 \pmod{45} \iff 5 \cdot 3^2 = 45 \mid x^2 - 36 = (x - 6)(x + 6)$. Jelikož $3 \mid (x - 6) \iff 3 \mid (x + 6) \iff 3 \mid x$ a $9 \mid (x - 6)(x + 6)$, musí být všechna řešení x zadané kongruence tvaru $3y$ pro nějaké $y \in \mathbb{Z}$. Užitím **1(a)** máme $(3y)^2 \equiv 36 \pmod{45} \iff y^2 \equiv 4 \pmod 5$, což je dále ekvivalentní $5 \mid (y-2)(y+2)$. Dostáváme $y = 5k \pm 2$, kde $k \in \mathbb{Z}$, což — po vynásobení třemi — nakonec vede k obecnému tvaru řešení $x = 15k \pm 6$, kde $k \in \mathbb{Z}$ může být libovolné.

Nejčastější chybou při výpočtu, která nutně nevede ke špatnému výsledku, zde byla asi úprava $x^2 \equiv 36 \pmod{45} \iff \frac{x^2}{9} \equiv 4 \pmod 5$. Tady je veskrze formální problém vyvěrající z faktu, že pravá strana ekvivalence není pro případ $3 \nmid x$ definována. Chápu, že chcete udělat úpravu „vydělit vše devíti“. To ale lze jen pokud skutečně vše vydělit devíti můžete, pak se jedná o ekvivalentní úpravu **1(a)**.

3. Chceme ukázat, že $n^2 \equiv 1 \pmod 8$ pro lichá $n \in \mathbb{Z}$. Jedna možnost je uvědomit si, že $n^2 \equiv k^2 \pmod 8$, kde $k \in \{1, 3, 5, 7\}$, a dále, že $1 = 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod 8$. Druhou alternativou je napsat si $n = 2m + 1$, kde $m \in \mathbb{Z}$, a rozepsat $n^2 = 4m^2 + 4m + 1 = 4m(m+1)+1 \equiv 1 \pmod 8$, což plyne ihned z $8 \mid 4m(m+1)$; zde používáme, že $m(m+1)$ je sudé.

6. Běh rozšířeným Eukleidovým algoritmem je následující:

n	a_n	x_n	y_n	q_n
0	1023	1	0	–
1	96	0	1	10
2	63	1	−10	1
3	33	−1	11	1
4	30	2	−21	1
5	3	−3	32	30
6	0	–	–	–

Závěr: $\mathrm{NSD}(1023, 96) = 3 = (-3) \cdot 1023 + 32 \cdot 96$.

7. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$. Samozřejmě, že když si všimneme, že v $\mathbb{Z}_{41}$ máme $27 = -14$ a $(-14) \cdot (-3) = 42 = 1$, dostaneme ihned kýžené $27^{-1} = -3 = 38$. Jinak musíme spustit rozšířený Eukleidův algoritmus na 41 a 27. Jeho běh je níže (všimněte si, že x_n nepotřebujeme).

n	a_n	y_n	q_n
0	41	0	–
1	27	1	1
2	14	−1	1
3	13	2	1
4	1	−3	13

Dostáváme $\mathrm{NSD}(41, 27) = 1 =$ „nezajímavé celé číslo“ $\cdot\, 41 + (-3) \cdot 27$.

9. (a) Jen připomínám, že minulý týden jsme ukázali, že se o podokruh nejedná. Sporem jsme ověřili, že $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ do zadané množiny nenáleží. Po vyjádření $\sqrt[3]{4} = a + b\sqrt[3]{2}$, kde $a, b \in \mathbb{Z}$, jsme nejprve obě strany vynásobili $\sqrt[3]{2}$, posléze jsme dosadili za $\sqrt[3]{4}$; využitím toho, že $\sqrt[3]{2}$ je iracionální, jsme porovnáním koeficientů obdrželi $a + b^2 = 0$ a následně $2 = -b^3$, což byl hledaný spor.

9. (b) Tvoří podokruh. Jelikož $\mathbb{C}$ má komutativní a asociativní obě binární operace (a platí tam i distributivita), potřebujeme ověřit jednak, že zadaná množina obsahuje 0 a 1, což je zřejmé, a dále, že je uzavřená na binární operace $+, \cdot$ a na unární operaci $-$.

Uzavřenost na $-$ a $+$ je ihned patrná. Pro násobení uvažujme obecné prvky $a + b\sqrt{2}$ a $c + d\sqrt{2}$, kde $a, b, c, d \in \mathbb{Z}$. Dostaneme $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, což je opět prvek zadané množiny.

9. (c) Netvoří podokruh, neboť není uzavřená na násobení. K tomu stačí ukázat, že $\zeta^2 = e^{\frac{\pi i}{2}} = i$ není prvkem zadané množiny. To je celkem zřejmé, ale asi by neměl být problém přijít s nějakým přesvědčivým argumentem jako třeba, že všechna komplexní čísla tvaru $a + b\zeta$, kde $a, b \in \mathbb{Z}$, mají imaginární složku rovnu $\frac{b\sqrt{2}}{2}$, což je iracionální číslo, a tedy není nikdy rovno jedné.

10. Jedná se o podokruh tvořený množinou

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} ;\, a, b \in \mathbb{Z} \right\}.$$

Jelikož podokruh musí mít jednotku (a nulu) a musí být uzavřen na sčítání a opačné prvky (tj. odčítání), musí být v hledaném okruhu jak všechny matice tvaru

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \text{ tak i matice tvaru } \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix},$$

kde a, b jsou libovolná celá čísla. Hledaná množina tedy jistě nemůže být menší. Zbývá ukázat, že S je uzavřená na násobení. Počítáme:

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad + bc \\ 0 & ac \end{pmatrix} \in S.$$

Ukázali jsme uzavřenost na násobení. Zároveň snadno ověříme, že když oba činitele prohodíme, výsledek se nijak nezmění. Podokruh S okruhu $\mathrm{M}_2(\mathbb{Z})$ je tedy komutativní.

12. Máme vyšetřit, pro která celá čísla x platí $17 \mid x^2 + 10x + 6$, tj. pro která $x \in \mathbb{Z}$ platí v $\mathbb{Z}_{17}$, že $x^2 + 10x + 6 = 0$. Můžeme si ihned všimnout, že $x = 1$ je řešením. Druhým je pak $x = 6$, tj. v $\mathbb{Z}_{17}$ platí $x^2 + 10x + 6 = (x - 1)(x - 6)$. Hledáme proto $x \in \mathbb{Z}$ taková, že $17 \mid (x - 1)(x - 6)$. Vzhledem k tomu, že 17 je prvočíslo (a tedy 17 dělí součin právě tehdy, když dělí jeden z činitelů), jedná se právě o x tvaru $17k + 1$ a $17k + 6$, kde $k \in \mathbb{Z}$.

14. Klíčem k řešení je vyhledat si méně známé detaily ohledně přestupných let. Konkrétně jde o to, že rok dělitelný 100 je přestupný tehdy a jen tehdy, když je dělitelný rovněž 400. Počítáme-li správně, zjistíme, že 1. ledna 2101 bude sobota, 1. ledna 2201 bude čtvrtek, 1. ledna 2301 bude úterý, 1. ledna 2401 pak opět pondělí (jelikož 23. století, kam se počítá i rok 2400, bude o jeden den delší), dále 1. ledna 2501 zase sobota atd.

15. Lze řešit matematickou indukcí. Další možností je psát $4^n = (3+1)^n = \sum_{k=0}^{n} \binom{n}{k} 3^k = 1 + 3n + \sum_{k=2}^{n} \binom{n}{k} 3^k$, což je po přičtení $6n$ a odečtení jedné zřejmě dělitelné 9.