Algebra — cvičení 1

(příklady cihlovou barvou jsme dělali on-line, na doma jsou ty ostatní)

Dělitelnost & počítání modulo

Připomeňme si, že je-li $n \in \mathbb{N}$, pak pro celá čísla a, b definujeme $a \equiv b \pmod{n}$ vztahem $n \mid (a-b)$, který čteme „n dělí $a-b$“ a je definován jako $(\exists c \in \mathbb{Z})\, cn = a-b$. Rychle se zjistí, že pro $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$ platí $a \square c \equiv b \square d \pmod{m}$, kde $\square$ je některá z operací $+, -, \cdot$.

1. Dokažte, že pro $a, b \in \mathbb{Z}$ a $c, m \in \mathbb{N}$ platí:
   (a) $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{mc}$;
   (b) jsou-li c a m nesoudělná, pak $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{m}$.
2. Vyřešte v celých číslech následující kongruence:
   (a) $x \equiv 2 \pmod{8}$;
   (b) $3x \equiv 2 \pmod{5}$;
   (c) $6x \equiv 2 \pmod{8}$;
   (d) $x^2 \equiv 36 \pmod{45}$.
3. Ukažte, že $n^2 \equiv 1 \pmod{8}$ pro každé liché $n \in \mathbb{N}$.
4. Buď p prvočíslo. Najděte všechna řešení kongruence $x^2 \equiv 1 \pmod{p}$ a ukažte, že jsou opravdu všechna.

Eukleidův algoritmus & Bézoutovy koeficienty

Připomeňme si rozšířený Eukleidův algoritmus:

- **vstup**: $a, b \in \mathbb{N}, a \geq b$
- **výstup**: $\mathrm{NSD}(a,b)$ a $x, y \in \mathbb{Z}$ taková, že $x \cdot a + y \cdot b = \mathrm{NSD}(a,b)$ (x, y říkáme *Bézoutovy koeficienty čísel a a b*)

krok 1. $i := 1$; $(a_0, a_1) := (a, b)$; $(x_0, x_1) := (1, 0)$; $(y_0, y_1) := (0, 1)$;

krok 2. **while** $(a_i > 0)$ **do**
$\{a_{i+1} := (a_{i-1}) \bmod a_i$; $q_i := (a_{i-1}) \operatorname{div} a_i$; $x_{i+1} := x_{i-1} - x_i \cdot q_i$; $y_{i+1} := y_{i-1} - y_i \cdot q_i$; $i := i+1\}$

krok 3. **return** a_{i-1}, x_{i-1}, y_{i-1}.

5. Najděte $\mathrm{NSD}\,(37, 10)$ a příslušné Bézoutovy koeficienty.
6. Najděte $\mathrm{NSD}\,(1023, 96)$ a příslušné Bézoutovy koeficienty.
7. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$.

Okruhy & obory

8. Ověřte, že polynomy s reálnými koeficienty $\mathbb{R}[x]$ tvoří s obvyklými operacemi $+, -, \cdot$ a konstantami 0 a 1 obor a polynomy s racionálními koeficienty $\mathbb{Q}[x]$, resp. s celočíselnými koeficienty $\mathbb{Z}[x]$ jsou jeho podobory.

9. Rozhodněte, zda tvoří následující množiny podokruhy tělesa $\mathbb{C}$:

   (a) $\{a + b\sqrt[3]{2};\ a, b \in \mathbb{Z}\}$;

   (b) $\{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$;

   (c) $\{a + b\zeta;\ a, b \in \mathbb{Z}\}$, kde $\zeta = e^{\frac{\pi i}{4}}$.

10. Popište nejmenší podokruh (s jednotkou!) maticového okruhu $M_2(\mathbb{Z})$, který obsahuje prvek $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Tvoří tento podokruh komutativní okruh?

11. Ukažte, že pro $n \in \mathbb{N}$ jsou následující podmínky ekvivalentní:

    (a) $\mathbb{Z}_n$ je těleso;

    (b) $\mathbb{Z}_n$ je obor;

    (c) n je prvočíslo.

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

12.⋆ Vyřešte v celých číslech $x^2 + 10x + 6 \equiv 0 \pmod{17}$.

13.⋆ Pomocí modulární aritmetiky odvoďte kritérium dělitelnosti pro

   (a) 9

   (b) 11

14.⋆ Ukažte, že století (pokud se nezmění kalendář) nikdy nebudou začínat středou, pátkem ani nedělí. (1. ledna 2001 bylo pondělí.)

15.⋆ Dokažte, že $9 \mid 4^n + 6n - 1$ pro všechna $n \in \mathbb{N}$.