Algebrou proti koronaviru I

(cvičení cihlovou barvou jsme udělali na cvičení, a tak je můžete vynechat)

Dělitelnost & počítání modulo

Připomeňme si, že je-li $n \in \mathbb{N}$, pak pro celá čísla a, b definujeme $a \equiv b \pmod n$ právě tehdy, když $n \mid (a-b)$. 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 $a, b, c, m \in \mathbb{Z}$, $c, m \neq 0$ platí:

   (a) $a \equiv b \pmod m \Leftrightarrow ac \equiv bc \pmod{mc}$ [rozepíše se definice (viz výše) a upraví, pro implikaci „$\Rightarrow$“ např. $a \equiv b \pmod m \Rightarrow m \mid (a-b) \Rightarrow t \cdot m = (a-b)$ pro nějaké $t \in \mathbb{Z}$ $\Rightarrow ctm = c \cdot (a-b) = (ca - cb)$, tj. $cm \mid (ca - cb)$]

   (b) jsou-li c a m nesoudělná, pak $a \equiv b \pmod m \Leftrightarrow ac \equiv bc \pmod m$

2. Ukažte, že $n^2 \equiv 1 \pmod 8$ pro každé liché $n \in \mathbb{N}$.

3. Vyřešte v celých číslech následující rovnice:

   (a) $x \equiv 2 \pmod 8$ $[x = 2 + 8k; k \in \mathbb{Z}]$

   (b) $3x \equiv 2 \pmod 5$ $[x = 4 + 5k; k \in \mathbb{Z}]$

   (c) $6x \equiv 2 \pmod 8$ $[x = 3 + 4k; k \in \mathbb{Z}]$

   (d) $x^2 \equiv 36 \pmod{45}$ $[\{6, 9\} + 15k, k \in \mathbb{Z}]$

4. Buď p prvočíslo. Najděte všechna řešení rovnice $x^2 \equiv 1 \pmod p$ a ukažte, že jsou opravdu všechna. *(Na cvičení jsme si k tomu zmínili charakterizaci prvočísel, která často ulehčí život: p je prvočíslo $\Leftrightarrow (p \mid a \cdot b \Rightarrow p \mid a \vee p \mid b)$.)* $[\pm 1 + p \cdot k, k \in \mathbb{Z}]$

Eukleidův algoritmus & Bézoutovy koeficienty

Připomeňme si rozšířený Eukleidův algoritmus:

- **vstup**: $a, b \in \mathbb{N}, a \geq b$
- **výstup**: NSD(a, b) a $x, y \in \mathbb{Z}$ taková, že $x \cdot a + y \cdot b = \text{NSD}(a, b)$ (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 NSD $(37, 10)$ a příslušné Bézoutovy koeficienty. $[1 = 3 \cdot 37 - 11 \cdot 10$; v $\mathbb{Z}_{37}$ tedy platí $10^{-1} = -11 \equiv 26 \pmod{37}]$

6. Najděte NSD $(1023, 96)$ a příslušné Bézoutovy koeficienty. $[3 = 1023 \cdot (-3) + 96 \cdot 32]$

7. Najděte 27^{-1} v tělese $\mathbb{Z}_{41}$. $[38]$

Okruhy & obory

8. Ověřte, že polynomy s reálnými koeficienty $\mathbb{R}[x]$ chápané jako reálné funkce 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. [Ze jsou $\mathbb{Q}[x]$, resp. $\mathbb{Z}[x]$ okruhy/obory, se ověří stejně jako pro $\mathbb{R}[x]$ (viz cvičení). Podobory jsou to proto, že příslušné operace jsou restrikcemi operací z $\mathbb{R}[x]$ a 0, resp. 1 lze považovat jak za polynomy s reálnými, tak i s racionálními, resp. celočíselnými koeficienty.]

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

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

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

   (c) $\{a + b\zeta \mid a, b \in \mathbb{Z}\}$, kde $\zeta = e^{\frac{\pi i}{4}}$ [ne: problém je s násobením, $(a + b\zeta) \cdot (c + d\zeta) = (ac) + (ad + bc)\zeta + bd \cdot e^{\frac{\pi i}{2}}$]

Následují otázky ulehčí pohled do skript:

10. 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

11. Určete prvookruh (*definice na str. 6 dole v rámci příkladu*) a charakteristiku oborů z příkladu 8 (*definice na str. 5*). [pro oba platí: prvookruh je $\mathbb{Z}$, charakteristika je tudíž 0]

12. 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? [$\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z}\}$; je komutativní]

Ať to jde od ruky a za týden na viděnou,
P.

P.S. Pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

13.⋆ Pomocí modulární aritmetiky odvoďte kritérium dělitelnosti pro

   (a) 9

   (b) 11

   [Číslo c uvažujme v jeho dekadickém zápise jako $c = \sum_{i=0}^{n} a_i 10^i$, pro $a_i \in \{0 \dots 9\}$ a uvažme 10^i modulo 9, resp. 11.]

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

15.⋆ Vyřešte v celých číslech $x^2 + 10x + 6 \equiv 0 \pmod{17}$. [např. lze převést na čtverec a využít cvičení 4; $\{1, 6\} + 17k; k \in \mathbb{Z}$]

16.⋆ Ukažte, že je-li obor integrity konečný, pak už jde o těleso. [Tvrzení 1.5 ze skript]

17.⋆ Rozmyslete si, že žádné dva z okruhů $\mathbb{Q}$, $\mathbb{Q}[x]$, $\mathbb{Q}[\sqrt{2}]$ nejsou izomorfní.