# Algebrou proti koronaviru I

## 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 $x \cdot a + y \cdot b = \mathrm{NSD}(a, b)$

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** $a_{i-1},$ $x_{i-1},$ $y_{i-1}.$

*S pomocí rozšířeného Eukleidova algoritmu můžeme například vyřešit následující úlohy:*

1. Najděte $\mathrm{NSD}(37, 10)$ a příslušné Bézoutovy koeficienty. [$1 = 3 \cdot 37 - 11 \cdot 10$; v $\mathbb{Z}_{37}$ tedy platí $10^{-1} = -11 \equiv 26 \pmod{37}$]
2. Najděte $\mathrm{NSD}(1023, 96)$ a příslušné Bézoutovy koeficienty. [$3 = 1023 \cdot (-3) + 96 \cdot 32$]
3. Najděte $27^{-1}$ v tělese $\mathbb{Z}_{41}$. [38]

## Okruhy & obory

4. Rozhodněte, zda jsou následující množiny podokruhy tělesa $\mathbb{C}$:
   (a) $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ [ano]
   (b) $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$ [ne]
   (c) $\{a + b\zeta \mid a, b \in \mathbb{Z}\}$, kde $\zeta = e^{\frac{\pi i}{4}}$ [ne]

   Je (a) dokonce obor? [ano]
5. Dokažte, že konečný obor je těleso.
6. 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
7. 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. Určete prvokruh a charakteristiku všech těchto oborů.
8. 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? [$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$; je komutativní]
9. Dokažte, že žádné dva z okruhů $\mathbb{Q}$, $\mathbb{Q}[x]$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ nejsou izomorfní.

*A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:*

10.$^\star$ Najděte $\mathrm{NSD}(2^{92}-1, 2^{31}-1)$. [1]

11.$^\star$ Najděte dvojici v součtu co nejmenších čísel tak, aby pro ně Eukleidův algoritmus skončil nulou po $n$ krocích. [$F_n$ a $F_{n+1}$, kde $F_i$ značí $i$-té Fibonacciho číslo]

12.$^\star$ Uvažujme podokruhy

(a) $R_1 := \mathbb{Z}[i] \leq \mathbb{C}$

(b) $R_2 := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \leq M_2(\mathbb{Q})$

(c) $R_3 := \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \leq M_2(\mathbb{Q})$

Určete, které z možných dvojic okruhů jsou izomorfní. [jen $R_1$ a $R_2$]

13.$^\star$ Je-li $\mathbb{Q}[\pi]$ nejmenší podokruh tělesa $\mathbb{R}$ obsahující $\mathbb{Q} \cup \{\pi\}$, dokažte, že jsou okruhy $\mathbb{Q}[x]$ a $\mathbb{Q}[\pi]$ izomorfní. (Využít můžete faktu, že $\pi$ není kořenem žádného nenulového racionálního polynomu).