1. cvičení - Eukleidův algoritmus

PŘ: Najděte $\gcd(260, 84)$ a nakombinujte ho celočíselně pro $a = 260$ a $b = 84$.

Eukleid:
$260 = 3 \cdot 84 + 8$
$84 = 10 \cdot 8 + 4$
$8 = 2 \cdot 4 + 0$

$8 = a - 3b$
$4 = b - 10 \cdot 8 = -10a + 31b$

$\gcd(260, 84) = 4 = -10 \cdot 260 + 31 \cdot 84$

PŘ: Řešte v $\mathbb{Z}$ $12x + 45y = 6$.

Rozšíř. Eukleid

$45 = 3 \cdot 12 + 9$ ... $45 = a$
$12 = 1 \cdot 9 + 3$ ... $12 = b$
$9 = 3 \cdot 3 + 0$ ... $9 = a - 3b$

$3 = -a + 4b$
$0 = 4a - 15b$

$\gcd(12, 45) = 3 \mid 6$
→ exist. řeš. v $\mathbb{Z}$ tvaru $(x, y) = (x_p, y_p) + k(x_0, y_0)$, $k \in \mathbb{Z}$
part. řeš. nesoudělné řeš. hom. rov.

$6 = 2 \cdot 3 = \underbrace{-2}_{y_p} \cdot 45 + \underbrace{8}_{x_p} \cdot 12$

$0 = \underbrace{4}_{y_0} \cdot 45 \underbrace{-15}_{x_0} \cdot 12$

$(x, y) = (8, -2) + k(-15, 4)$

PŘ: Řešte v $\mathbb{Z}_{45}$ $12x = 6$.

Převedeme na Diofantickou rovnici $12x + 45y = 6$ v $\mathbb{Z}$,
řešení je výše, nás zajímá $x = 8 + (-15)k \in \{8, 23, 38, \cancel{53 = 8}\}$
$k=0$ $k=-1$ $k=-2$ $k=-3$
Celkem $3 = \gcd(12, 45)$ různá řešení.

PŘ: Řešte v $\mathbb{Z}_{204}$ $150x = 12$.

Tedy v $\mathbb{Z}$ $150x + 204y = 12$

Rozšířený Eukleid

$204 = 1 \cdot 150 + 54$ ... $204 = a$
$150 = 2 \cdot 54 + 42$ ... $150 = b$
$54 = 1 \cdot 42 + 12$ ... $54 = a - b$
$42 = 3 \cdot 12 + 6$ ... $42 = -2a + 3b$
$12 = 2 \cdot 6 + 0$ ... $12 = 3a - 4b$

$6 = -11a + 15b \quad / \cdot 2$
$0 = 25a - 34b \quad / \cdot k \in \mathbb{Z}$

$\gcd(204, 150) = 6 \mid 12$
→ exist. řeš. v $\mathbb{Z}$

$12 = \underbrace{(-22 + 25k)}_{y} \cdot 204 + \underbrace{(30 - 34k)}_{x} \cdot 150$

V $\mathbb{Z}_{204}$ $x = 30 - 34k \in \{30, 64, 98, 132, 166, 200\}$.

PF: Najdi 3^{-1} a 7^{-1} v $\mathbb{Z}_{54}$

$\gcd(3,54) = 3 \quad \rightarrow 3^{-1}$ neexist. v $\mathbb{Z}_{54}$

$\gcd(7,54) = 1 \quad \rightarrow 7^{-1}$ exist. v $\mathbb{Z}_{54}$

Rozšíř. Euklid, řešíme $7x = 1$ v $\mathbb{Z}_{54}$

$7x + 54y = 1$ v $\mathbb{Z}$

$54 = 7 \cdot 7 + 5 \quad \begin{matrix} 54 = n \\ 7 = a \end{matrix}$

$7 = 1 \cdot 5 + 2 \quad \begin{matrix} -1\times \\ -2\times \end{matrix}$ $\begin{matrix} 5 = n - 7a \\ 2 = -n + 8a \end{matrix}$

$5 = 2 \cdot 2 + 1 \quad 1 = 3n - 23a$

$x = 7^{-1} = -23 = 31$ v $\mathbb{Z}_{54}$

PF: Řeště $6x = 3$ v $\mathbb{Z}_9$

v $\mathbb{Z}$ $6x + 9y = 3$

$(x_p, y_p) = (-1, 1)$ uhodnu

$(x_0, y_0) = (3, -2)$ zkrátím hom. rov. $6x + 9y = 0 \quad /:3$

$2x + 3y = 0$

v $\mathbb{Z}_9 \quad x = -1 + k \cdot 3 \in \{2, 5, 8\}$