# LINEÁRNÍ ROVNICE $ax = b$ v $\mathbb{Z}_n$

→ o jedné neznámé

(PŘ) $2x = 2$ v $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

dosazením: $2 \cdot 0 = 0 \rightarrow \neq 2$

$2 \cdot 1 = 2 \rightarrow x_1 = 1$

$2 \cdot 2 = 4 = 0 \rightarrow \neq 2$

$2 \cdot 3 = 6 = 2 \rightarrow x_2 = 3$

⇒ může být i více řešení

Chci řešit rovnici $a \cdot x = b$ v $\mathbb{Z}_n$

↓

$ax + ny = b$ v $\mathbb{Z}_n$

neboť $[a] \odot [x] = [b]$

$[ax] = [b]$ v $\mathbb{Z}_n$

$ax \equiv b \pmod n$

↓

Diofantická rovnice

↓

řeší se o násobek $n$

existuje řešení

iff $\gcd(a, n) \mid b$

pak v $\mathbb{Z}$ $x = x_p + kx_0$ kde $x_0$ z $ax + ny = 0 \;/ : \gcd(a, n)$

↑

rozšířený Euklid → $x_0 = \frac{n}{\gcd(a, n)}$

Přejdeme se do $\mathbb{Z}_n$ $x = x_p + k \cdot \frac{n}{\gcd(a, n)}$

vyjde $GCD(a, n)$ různých řešení pro

$k = 0, 1, \ldots, GCD - 1$

$[k = GCD \quad x = x_p + GCD \frac{n}{GCD} = x_p]$

(PŘ) $54x = 18 \pmod{150}$

$\hookrightarrow 54x + 150y = 18$ v $\mathbb{Z}$

viz minulá hodina řešení

$x = -33 + 25k, \quad k \in \mathbb{Z}$

$y =$

v $\mathbb{Z}_{150}$ $x \in \{ \underbrace{-33 = 117}_{k=0}, \underbrace{-33+25 = -8 = 142}_{k=1},$

$\underbrace{-33+50 = 17}_{k=2}, \underbrace{42}_{k=3}, \underbrace{67}_{k=4},$

$\underbrace{82}_{k=5}, \underbrace{117}_{k=6} \}$

→ již dám je

→ je 6 řešení (viz minule $6 = GCD(54, 150)$)

Inverzní prvek k. a v $\mathbb{Z}_n$ (vůči násobení)
je takové $b \in \mathbb{Z}_n$, že $a \cdot b = 1$ v $\mathbb{Z}_n$

Lze dokázat, že pokud existuje, tak je jediný.
Značíme $A^{-1}$ nebo $a^{-1}$.

Poznámka: v $\mathbb{Z}$ má inverzní prvek ~~k = ±1~~

$x \cdot x = 1$

$x = \frac{1}{x} \in \mathbb{Z} \rightarrow x = \pm 1$

jenom $+1, -1$

~~v $\mathbb{Z}_n$ pouze pro~~

v $\mathbb{Z}_n$ může mít inverz více prvků

v $\mathbb{Z}_5$ $\quad 2 \cdot 3 = 1 \longrightarrow 2^{-1} = 3$

Hledání $a^{-1}$ v $\mathbb{Z}_n$ - 1. metoda + a základní

= řešení rovnice $a \cdot x = 1$ v $\mathbb{Z}_n$

použiju rozšířený Euklid

(stačí najít jakékoliv řešení $\longrightarrow a^{-1}$ je jediný)

Věta: existuje řešení iff $GCD(a,n) \mid 1$

iff $a$ nesoudělné s $n$

v $\mathbb{Z}_n$ mají inverz právě všechna $a$ nesoudělná s $n$

(PŘ) $19^{-1}, 20^{-1}$ v $\mathbb{Z}_{26}$

$20^{-1}$ neexistuje $\leftarrow$ 20 soudělné s 26

$19^{-1} = x \longrightarrow 19x = 1$ v $\mathbb{Z}_{26}$

$19x + 26y = 1$ v $\mathbb{Z}$

Euklid

$26 = 19 + 7$ (n = 19, a = 7)

$19 = 2 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$7 = n - a$

$5 = a - 2(n-a) = -2n + 3a$

$2 = 7 \cdot 5 = (n-a) - (-2n + 3a)$

$= 3n - 4a$

$1 = 5 - 2 \cdot 2 = (-2n + 3a) - 2(3n - 4a)$

$= -8n + 11a$

$= 8 \cdot 26 + \underbrace{11}_{x} \cdot 19$

$\longrightarrow 19^{-1} = 11$ v $\mathbb{Z}_{26}$