# DMA Přednáška – Rovnice nad $\mathbb{Z}$

**Definice.**
Pojmem **lineární diofantická rovnice** označujeme libovolnou rovnici typu $ax + by = c$ s neznámými $x, y$, kde $a, b, c \in \mathbb{Z}$ a vyžadujeme také řešení $x, y \in \mathbb{Z}$.

**Věta.**
Nechť $a, b, c \in \mathbb{Z}$. Lineární diofantická rovnice $ax+by = c$ má alespoň jedno řešení právě tehdy, když $c$ je násobkem $\gcd(a, b)$.

**Definice.**
Je-li dána lineární diofantická rovnice $ax + by = c$, pak definujeme její **přidruženou homogenní rovnici** jako $ax + by = 0$.

**Věta.**
Nechť $a, b, c \in \mathbb{Z}$. Uvažujme lineární diofantickou rovnici $ax + by = c$.
Nechť $(x_p, y_p) \in \mathbb{Z}^2$ je nějaké její **partikulární** řešení.
Dvojice $(x_0, y_0) \in \mathbb{Z}^2$ je řešení této rovnice právě tehdy, když
existuje $(x_h, y_h) \in \mathbb{Z}^2$ takové, že $(x_0, y_0) = (x_p, y_p) + (x_h, y_h)$ a $(x_h, y_h)$ řeší přidruženou homogenní rovnici.

**Věta.**
Uvažujme rovnici $ax + by = 0$ pro $a, b \in \mathbb{Z}$. Množina všech jejích celočíselných řešení je

$$\Big\{\Big(k\frac{b}{\gcd(a,b)}, -k\frac{a}{\gcd(a,b)}\Big) : k \in \mathbb{Z}\Big\}.$$

**Algoritmus** pro nalezení všech celočíselných řešení rovnice $ax + by = c$.
**0.** Například pomocí rozšířeného Euklidova algoritmu najděte $\gcd(a,b) = Aa + Bb$.
**1.** Jestliže $c$ není násobkem $\gcd(a,b)$, pak řešení rovnice neexistuje.
**2.** Případ $\gcd(a,b)$ dělí $c$:
a) Získanou rovnost $aA + bB = \gcd(a,b)$ vynásobte číslem $c' = \frac{c}{\gcd(a,b)} \in \mathbb{Z}$ tak, aby se zachovaly koeficienty $a, b$, a dostanete $a(Ac') + b(Bc') = c$, tudíž i jedno partikulární řešení $x_p = Ac'$, $y_p = Bc'$ neboli vektor $(Ac', Bc')$.
b) Přidruženou homogenní rovnici $ax + by = 0$ zkraťte číslem $\gcd(a,b)$ na tvar $a'x + b'y = 0$, což dává řešení $x_h = b'k$, $y_h = -a'k$ neboli dvojice $(b'k, -a'k)$ pro $k \in \mathbb{Z}$, popřípadě $x_h = -b'k$, $y_h = a'k$ neboli dvojice $(-b'k, a'k)$.
c) Sečtením partikulárního a obecného homogenního řešení získáte množinu všech celočíselných řešení

$$\{(x_p + kb', y_p - ka') : k \in \mathbb{Z}\} \text{ neboli } x = x_p + kb',\ y = x_p - ka' \text{ pro } k \in \mathbb{Z},$$

popřípadě verzi s mínusem u $y_h$.

**Definice.**
Termínem **lineární kongruence** označujeme rovnice typu $ax \equiv b \pmod{n}$, kde $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ a hledáme celočíselná řešení $x$.

**Fakt.**
Nechť $n \in \mathbb{N}$. Uvažujme $a, b \in \mathbb{Z}$. Číslo $x_0 \in \mathbb{Z}$ řeší lineární kongruenci $ax \equiv b \pmod{n}$ právě tehdy, když pro nějaké $y_0 \in \mathbb{Z}$ řeší vektor $(x_0, y_0)$ diofantickou rovnici $ax + ny = b$.

**Věta.**
Nechť $n \in \mathbb{N}$, uvažujme $a, b \in \mathbb{Z}$.
(i) Jestliže $b$ není násobkem $\gcd(a, n)$, tak řešení rovnice $ax \equiv b \pmod{n}$ neexistuje.
(ii) Jestliže $\gcd(a, n)$ dělí $b$, tak rovnice $ax \equiv b \pmod{n}$ má nějaké řešení $x_p \in \mathbb{Z}$. Označme $n' = \frac{n}{\gcd(a,n)}$. Množina všech řešení lineární kongruence $ax \equiv b \pmod{n}$ je

$$\{x_p + kn' : k \in \mathbb{Z}\}.$$

**Věta.**
Nechť $n \in \mathbb{N}$, uvažujme kongruenci $ax \equiv b \pmod{n}$ pro nějaká $a, b \in \mathbb{Z}$. Nechť $x_p$ je nějaké její partikulární řešení. Definujme čísla $x_i = x_p + \frac{n}{\gcd(a,n)} i$ pro $i = 0, 1, \ldots, \gcd(a, b) - 1$. Množina všech řešení dané kongruence je sjednocením množin $\{x_i + kn : k \in \mathbb{Z}\}$ pro $i = 0, 1, \ldots, \gcd(a, b) - 1$, tyto množiny jsou navzájem disjunktní.

**Věta.**
Nechť $n \in \mathbb{N}$. Uvažujme kongruenci $ax \equiv b \pmod{n}$ pro nějaká $a, b \in \mathbb{Z}$, nechť $x_p$ je nějaké její řešení.
Číslo $x_0 \in \mathbb{Z}$ je řešením kongruence $ax \equiv b \pmod{n}$ právě tehdy, když existuje $x_h \in \mathbb{Z}$, které splňuje $x_0 = x_p + x_h$ a je řešením přidružené homogenní rovnice $ax \equiv 0 \pmod{n}$.

• Množinu všech řešení rovnice $a \odot x = b$ v $\mathbb{Z}_n$ získáme tak, že v množině všech řešení kongruence $ax \equiv b \pmod{n}$ nahradíme všechna čísla jejich zbytky po dělení $n$ neboli jejich kongruentními zástupci z množiny $\mathbb{Z}_n$.

**Věta.**
Nechť $n \in \mathbb{N}$, uvažujme rovnici $ax = b$ v $\mathbb{Z}_n$ pro nějaká $a, b \in \mathbb{Z}_n$.
(i) Jestliže $\gcd(a, n)$ nedělí $b$, pak řešení neexistuje.
(ii) Předpokládejme, že $\gcd(a, n)$ dělí $b$. Nechť $x_p \in \mathbb{Z}$ řeší kongruenci $ax \equiv \pmod{n}$, označme $n' = \frac{n}{\gcd(a,n)}$.
Nechť $x_0 = \min\{x_p + kn' : k \in \mathbb{Z} \text{ a } x_p + kn' \geq 0\}$. Pak množina všech řešení rovnice $ax = b$ v $\mathbb{Z}_n$ je

$$\{x_0 + in' : i = 0, 1, \dots, \gcd(a, n) - 1\}.$$

Jde o $\gcd(a, n)$ různých čísel.

Soustavy lineárních kongruencí:
Jsou dány moduly $n_1, \dots, n_m \in \mathbb{N}$ a pravé strany $b_1, \dots, b_m \in \mathbb{Z}$. Hledáme celá čísla $x$ taková, že

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

**Věta.**
Uvažujme moduly $n_1, n_2, \dots, n_m \in \mathbb{N}$ a čísla $b_1, b_2, \dots, b_m \in \mathbb{Z}$.
Nechť $x_p$ je nějaké řešení soustavy kongruencí

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Číslo $x_0$ je také řešením této soustavy právě tehdy, pokud existuje číslo $x_h$ takové, že $x_0 = x_p + x_h$ a $x_h$ je řešením přidružené homogenní soustavy kongruencí

$$\begin{aligned} x &\equiv 0 \pmod{n_1} \\ x &\equiv 0 \pmod{n_2} \\ &\vdots \\ x &\equiv 0 \pmod{n_m}. \end{aligned}$$

**Věta.** (Čínská věta o zbytcích)
Nechť $n_1, n_2, \dots, n_m \in \mathbb{N}$, $b_1, b_2, \dots, b_m \in \mathbb{Z}$. Uvažujme soustavu rovnic

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_m \pmod{n_m}. \end{aligned}$$

Jestliže jsou všechna čísla $n_i$ po dvou nesoudělná, pak má tato soustava řešení $x_0 \in \mathbb{Z}$. Množina všech řešení je $\{x_0 + kn : k \in \mathbb{Z}\}$, kde $n = n_1 n_2 \cdots n_m$.

**Algoritmus** pro řešení soustavy kongruencí $x \equiv b_1 \pmod{n_1}, x \equiv b_2 \pmod{n_2}, \dots, x \equiv b_m \pmod{n_m}$ pro případ, že jsou všechna čísla $n_i$ po dvou nesoudělná.

**1.** Označte $n = n_1 n_2 \cdots n_m$ a $N_i = \frac{n}{n_i}$ pro všechna $i$.

**2.** Pro každé $i$ najděte inverzní číslo k $N_i$ vzhledem k násobení modulo $n_i$.

**3.** Nechť $x_p = \sum\limits_{i=1}^{m} b_i N_i x_i$. Množina všech řešení soustavy je $\{x_p + kn : k \in \mathbb{Z}\}$.