

DMA Přednáška – Rovnice nad \mathbb{Z} **Definice.**

Pojmem **lineární diofantická rovnice** o dvou neznámých 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 $x_p, y_p \in \mathbb{Z}$ je nějaké její **partikulární řešení**.

Dvojice $x_0, y_0 \in \mathbb{Z}$ je řešením této rovnice právě tehdy, když

existuje dvojice $x_h, y_h \in \mathbb{Z}$ taková, že $x_0 = x_p + x_h$, $y_0 = y_p + y_h$ a x_h, y_h řeší přidruženou homogenní rovnici.

Věta.

Uvažujme netriviální rovnici $ax + by = 0$ pro $a, b \in \mathbb{Z}$. Její obecné řešení je dáno vzorcem

$$x = \frac{b}{\gcd(a, b)}k, \quad y = -\frac{a}{\gcd(a, b)}k, \quad k \in \mathbb{Z}.$$

Algoritmus pro nalezení všech celočíselných řešení netriviální rovnice $ax + by = c$.

0. Jestliže na první pohled vidíme $d > 1$, které dělí a i b , ale nedělí c , tak rovnice nemá řešení.

Jinak například pomocí rozšířeného Euklidova algoritmu najdeme $\gcd(a, b) = Aa + Bb$.

1. Jestliže c není násobkem $\gcd(a, b)$, pak řešení rovnice neexistuje.

Jestliže c je násobkem $\gcd(a, b)$, tak:

a) Získanou rovnost $aA + bB = \gcd(a, b)$ vynásobíme číslem $\tilde{c} = \frac{c}{\gcd(a, b)} \in \mathbb{Z}$ tak, aby se zachovaly koeficienty a, b , a dostaneme $a(A\tilde{c}) + b(B\tilde{c}) = c$. To ukazuje partikulární řešení $x_p = A\tilde{c}$, $y_p = B\tilde{c}$.

b) Přidruženou homogenní rovnici $ax + by = 0$ zkrátíme číslem $\gcd(a, b)$ na tvar $\tilde{a}x + \tilde{b}y = 0$ neboli $\tilde{a}x = -\tilde{b}y$, což dává řešení $x_h = \tilde{b}k$, $y_h = -\tilde{a}k$, popřípadě $x_h = -\tilde{b}k$, $y_h = \tilde{a}k$ pro $k \in \mathbb{Z}$.

c) Sečtením partikulárního a obecného homogenního řešení získáme obecné řešení $x = x_p + \tilde{b}k$, $y = y_p - \tilde{a}k$, $k \in \mathbb{Z}$, popřípadě verzi s mínusem u x_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_0 .

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 $ax \equiv 0 \pmod{n}$.

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 $y_0 \in \mathbb{Z}$ dvojice x_0, y_0 řeší 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 kongruence $ax \equiv b \pmod{n}$ neexistuje.

(ii) Jestliže $\gcd(a, n)$ dělí b , tak kongruence $ax \equiv b \pmod{n}$ má nějaké řešení $x_p \in \mathbb{Z}$. Označme $n' = \frac{n}{\gcd(a, n)}$.

Pak obecné řešení lineární kongruence $ax \equiv b \pmod{n}$ je

$$x = x_p + kn', \quad k \in \mathbb{Z}.$$

• 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) Jestliže $\gcd(a, n)$ dělí b , pak má rovnice $\gcd(a, n)$ řešení.

Nechť $x_p \in \mathbb{Z}$ řeší kongruenci $ax \equiv b \pmod{n}$, označme $\tilde{n} = \frac{n}{\gcd(a, n)}$.

Nechť $x_0 = x_p \pmod{\tilde{n}}$. Pak množina všech řešení rovnice $ax = b$ v \mathbb{Z}_n je

$$\{x_0 + i\tilde{n}; i = 0, 1, \dots, \gcd(a, n) - 1\}.$$

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 kongruencí

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

Jestliže jsou všechna čísla n_i po dvou nesoudělná, pak má tato soustava řešení $x_p \in \mathbb{Z}$. Obecné řešení je $x = x_p + kn$, $k \in \mathbb{Z}$, 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. Označíme $n = n_1 n_2 \cdots n_m$ a $N_i = \frac{n}{n_i}$ pro všechna i .

2. Pro každé i najdeme inverzní číslo x_i k N_i vzhledem k násobení modulo n_i .

3. Nechť $x_p = \sum_{i=1}^m b_i x_i N_i$. Obecné řešení soustavy je $x = x_p + kn$, $k \in \mathbb{Z}$.