ZDM – BI-SPOL-33

Modulární aritmetika, základy teorie čísel, Malá Fermatova věta, diofantické rovnice, lineární kongruence, Čínská věta o zbytcích.

Obsah

1 Modulární aritmetika

Z_m (nebo též $Zmodm$) je množina celých čísel modulo nějaké dané přirozené číslo m. Nejčastěji se setkáme se zápisem $Zm = \{0, 1, 2..., m-1\}$.

Nechť $a, b, c, d, m \in Z$, $m \geq 2$. Pak pokud platí současně $a \equiv b \bmod m$ a $c \equiv d \bmod m$, potom platí:

$$a + c \equiv b + d \bmod m$$

$$a - c \equiv b - d \bmod m$$

$$a \cdot c \equiv b \cdot d \bmod m$$

Nechť $a, b \in Z$. Řekneme, že a dělí b, značíme $a|b$, jestliže existuje $k \in Z$ takové, že $b = k \cdot a$.

Vlastnosti

- uzavřenost $a \bigoplus b \in Z_m$, $a \bigodot b \in Z_m$
- komutativita $a \bigoplus b = b \bigoplus a$, $a \bigodot b = b \bigodot a$
- asociativita $a \bigoplus (b \bigoplus c) = (a \bigoplus b) \bigoplus c$, $a \bigodot (b \bigodot c) = (a \bigodot b) \bigodot c$
- neutrální prvek $a \bigoplus 0 = |a|_m$, $a \cdot 1 = |a|_m$
- inv. prvek $a \bigoplus \bar{a} = 0$
- distributivita $a \bigodot (b \bigoplus c) = a \bigodot b \bigoplus a \bigodot c$

2 GCD & LCM

Číslo $d \in N^+$ je společný dělitel čísel a, b, jestliže $d|a$ a $d|b$. Největší z nich je poté $\gcd(a, b)$.

Číslo $n \in N^+$ je společný násobek čísel a, b, jestliže $a|n$ a $b|n$. Nejmenší z nich je poté $\text{lcm}(a, b)$.

(Vlastnosti gcd a lcm). Nechť a, $b \in Z$. Potom platí:

- Jestliže je n společný násobek a, b, pak $\text{lcm}(a, b)$ dělí n.
- Jestliže $a|n$ a $b|n$, pak $\text{lcm}(a, b)|n$.
- $\gcd(a, b) = \gcd(|a|, |b|)$ a $\text{lcm}(a, b) = \text{lcm}(|a|, |b|)$.
- Označme $d = \gcd(a, b)$. Potom $\gcd(ad, bd) = 1$.
- $\gcd(a + cb, b) = \gcd(a, b)$ pro libovolné $c \in Z$.
- Jestliže $a|bc$, pro nějaké $c \in Z$ a čísla a, b jsou nesoudělná (tj. $\gcd(a, b) = 1$), potom $a|c$.
- $|a| \cdot |b| = \gcd(a, b) \cdot \text{lcm}(a, b)$

  $$\gcd(a, b) = d = \alpha \cdot a + \beta \cdot b,$$

  kde α, β jsou celočíselné koeficienty této lineární kombinace.

3 Teorie čísel

3.1 Vlastnosti prvočísel

Funkce $(n) : N^+ \to N$ určuje počet prvočísel, která jsou menší než n.

Poměr (n) k výrazu $n/\log(n)$ se s rostoucím n přibližuje hodnotě 1.

Eulerova funkce Φ Eulerova funkce $\Phi(n) : N^+ \to N^+$ udává počet kladných celých čísel menších nebo rovných n, která jsou nesoudělná s n.

Nechť $m \in N^+$ a $a \in Z$ je číslo nesoudělné s m. Potom platí $a^{\Phi(m)} \equiv 1 \pmod{m}$.

Přirozené číslo p je prvočíslem, právě když platí $\Phi(p) = p - 1$.

Nechť p je prvočíslo a $a \in N$. Potom $\Phi(p^a) = p^a - p^{a-1}$.

Nechť $m, n \in N$ a $\gcd(m, n) = 1$. Potom $\Phi(mn) = \Phi(m)\Phi(n)$.

n	$\pi(n)$	$n/\log(n)$	$\pi(n)/\frac{n}{\log(n)}$
10^3	168	144,8	1,160
10^4	1229	1085,7	1,132
10^5	9592	8685,9	1,104
10^6	78498	72382,4	1,085
10^7	664579	620420,7	1,071
10^8	5761455	5428681,0	1,061
10^9	50847534	48254942,4	1,054
10^{10}	455052512	434294481,9	1,048
10^{11}	4118054813	3948131663,7	1,043
10^{12}	37607912018	36191206825,3	1,039

3.2 Eukleidův algoritmus

Nechť a, b jsou celá čísla, pro která platí $a \geq b > 0$. Nechť $\{r_n\}_{n=0}^{k+1}$ je klesající posloupnost zbytků definovaná rekurentním vztahem $r_{n+2} = r_n \bmod r_{n+1}$ s počátečními podmínkami $r_0 = a$, $r_1 = b$. kde $r_{k+1} = 0$ pro $(k > 0)$ je její první nulový člen. Potom její poslední nenulový člen (tj. poslední nenulový zbytek) je největším společným dělitelem a a b, tedy $\gcd(a, b) = r_k$.

4 Malá Fermatova věta

Nechť p je prvočíslo a $a \in N^+$ takové přirozené číslo, které není násobkem p. Potom platí $a^{p-1} \equiv 1 \pmod{p}$.

Nechť $a, b, c \in Z$ a $m \in N^+$ a nechť platí $ac \equiv bc \pmod{m}$. Potom platí $a \equiv b \pmod{m/d}$, kde d je největší společný dělitel čílsel m a c.

5 Diofantické rovnice

Jako lineární diofantickou rovnici označujeme libovolnou rovnici typu $ax + by = c$ s neznámými x, y, kde $a, b, c \in Z$, pro jejíž řešení má rovněž platit $x, y \in Z$.

Lineární diofantická rovnice $ax + by = c$ má alespoň jedno řešení právě tehdy, když c je násobkem $\gcd(a, b)$.

Nechť a, b jsou nenulová celá čísla a dvojice (x_0, y_0) je řešením rovnice $ax + by = c$. Potom množina všech celočíselných řešení této rovnice je $\{(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k) : k \in Z\}$, kde $d = \gcd(a, b)$.

6 Lineární kongruence

(skvělá ukázka na: `http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/linearni_kongruence.pdf`)
Pro daná celá čísla a, b a $m > 1$ hledáme celé x takové, že platí $ax \equiv b \pmod{m}$.

Lineární kongruence má řešení právě tehdy, když $\gcd(a, m)|b$. Všechna řešení jsou tvaru

$$x = x_0 + k\frac{m}{\gcd(a, m)},$$

kde k je libovolné celé číslo a pro x_0 existuje y_0 takové, že dvojice (x_0, y_0) je řešením rovnice $ax + my = b$.

Jestliže $\gcd(a, m)|b$, potom kongruence $ax \equiv b \pmod{m}$ má konečně mnoho řešení modulo m. Tato řešení jsou dána výrazem

$$|x_0 + k\frac{m}{\gcd(a, m)}|_m$$

pro $k = 1, 2, 3, ..., \gcd(a, m)$, kde pro x_0 existuje nějaké y_0 tak, že dvojice (x_0, y_0) je řešením $ax + my = b$.

7 Čínská věta

Budeme řešit systém lineárních kongruencí:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$. \quad . \quad .$$
$$x \equiv a_N \pmod{m_N}$$

kde čísla m_i jsou po dvou nesoudělná, tedy $\gcd(m_i, m_j) = 1$ pro všechna i, j, kde $i \neq j$.

Řešení tohoto systému existuje a všechna řešení jsou kongruentní modulo M (tedy v Z_M je řešení určeno jednoznačně), kde

$$M = \prod_{i=1}^{N} m_i.$$

Definujme $M_i = \frac{M}{m_i}$.

Jelikož $\gcd(m_i, M_i) = 1$, pak existují řešení X_i lineárních kongruencí $M_i X_i \equiv 1 \pmod{mi}$ pro všechna $i \in \{1, ..., N\}$, navíc platí pro všechna $j \neq i$ $M_i X_i \equiv 0 \pmod{m_j}$.

Z čehož plyne:

$$x \equiv a_1 X_1 M_1 + ... + a_N X_N M_N \pmod{M}$$

Příklad 1:

$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$

- - -

$$M = 2 \cdot 3 \cdot 5 = 30$$
$$M_1 = 15, \ M_2 = 10, \ M_3 = 6$$

$$M_1 X_1 = 15 X_1 \equiv 1 \pmod{2}$$
$$X_1 = 1$$

$$M_2 X_2 = 10 X_2 \equiv 1 \pmod{3}$$
$$X_2 = 1$$

$$M_3 X_3 = 6 X_3 \equiv 1 \pmod{5}$$
$$X_3 = 1$$

- - -

$$x = 1 \cdot 1 \cdot 15 + 2 \cdot 1 \cdot 10 + 3 \cdot 1 \cdot 6 = 53 \equiv 23 \pmod{30}$$

8 Zobecněná Čínská věta

Systém lineárních kongruencí má řešení právě tehdy, když $\gcd(m_i, m_j)$ dělí $a_i - a_j$ pro všechna $i, j : 1 \leq i < j \leq N$. Pokud řešení existuje, je určeno jednoznačně modulo $\text{lcm}(m_1, m_2, ..., m_N)$.

Příklad 2:

$$x \equiv 5 \pmod 6$$
$$x \equiv 3 \pmod{10}$$
$$x \equiv 8 \pmod{15}$$

- - -

$$x = 5 + 6t$$

$$5 + 6t \equiv 3 \pmod{10}$$
$$6t \equiv 8 \pmod{10}$$
$$t \equiv 8 \cdot 6^{-1} \pmod{10}$$
$$t \equiv 3 \pmod{10}$$
$$t = 3 + 10u$$

$$x = 5 + 6t = 5 + 6(3 + 10u) = 23 + 60u$$

$$23 + 60u \equiv 8 \pmod{15}$$
$$0 \cdot u \equiv 0 \pmod{15}$$
$$u \in N$$

- - -

$$x = 5 + 6t = 23 + 60u$$
$$\operatorname{lcm}(6, 10, 15) = 30$$

$$x \equiv 23 \pmod{30}$$