

# 1 Opakování teorie čísel

## 1.1 Základní pojmy

Buďte  $a, b \in \mathbb{Z}$ .

- $n \in \mathbb{N}_0$  je *společný dělitel* čísel  $a, b$ , jestliže  $n|a \wedge n|b$ .
- $\gcd(a, b)$  je *největší společný dělitel* (greatest common divisor).
- $a, b$  jsou *nesoudělné*, jestliže  $\gcd(a, b) = 1$ .
- $n \in \mathbb{N}_0$  je *společný násobek* čísel  $a, b$ , jestliže  $a|n \wedge b|n$ .
- $\text{lcm}(a, b)$  je *nejmenší společný násobek* (least common multiple).

## 1.2 Vztah gcd a lcm

$$\gcd(a, b) \cdot \text{lcm}(a, b) = |a| \cdot |b|$$

## 1.3 Kongruence modulo $m$

$$\begin{aligned} a &\equiv b \pmod{m} \\ a \bmod m &= b \bmod m \\ |a|_m &= |b|_m \\ |a - b|_m &= 0 \\ a &= b + k \cdot m, \quad k \in \mathbb{Z} \\ m &| (a - b), \text{ tzn. } m \text{ dělí rozdíl } a - b \end{aligned}$$

## 1.4 Operace v modulu

Kongruence modulo  $m$  zachovává operace  $+, -, \cdot$ . Pro libovolné  $c \in \mathbb{Z}$  a  $k \in \mathbb{N}$  platí:

$$\begin{aligned} a + c &\equiv b + c \pmod{m} \\ a - c &\equiv b - c \pmod{m} \\ a \cdot c &\equiv b \cdot c \pmod{m} \\ a^k &\equiv b^k \pmod{m} \end{aligned}$$

Označíme-li  $d = \gcd(c, m)$ , pak lze i krátit:

$$a \cdot c \equiv b \cdot c \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{d}}$$

## 1.5 Multiplikativní inverze

V  $\mathbb{Z}_m$  existuje multiplikativní inverze k  $a$  právě tehdy, když  $\gcd(a, m) = 1$ , a lze najít pomocí EEA, případně Malou Fermatovou nebo Eulerovou větou.

## 1.6 Extended Euclidean algorithm

$r_i$	$\alpha_i$	$\beta_i$	$q_i$
$a$	1	0	—
$b$	0	1	$q_2 = \lfloor \frac{a}{b} \rfloor$
$r_3 = a - q_2 \cdot b$	$1 - q_2 \cdot 0$	$0 - q_2 \cdot 1$	$q_3$
...	...	...	...
$r_k = \gcd(a, b)$	$\alpha$	$\beta$	$q_k$
$r_{k+1} = 0$	—	—	—

## 1.7 Square and Multiply

$$|6^{23}|_{13} = |6^{101112}|_{13} = ?$$

$$\begin{aligned} |6^{12}|_{13} &= |6|_{13} = 6 \\ |6^{102}|_{13} &= |6^2|_{13} = 10 \\ |6^{1002}|_{13} &= |10^2|_{13} = 9 \\ |6^{1012}|_{13} &= |9 \cdot 6|_{13} = 2 \\ |6^{10102}|_{13} &= |2^2|_{13} = 4 \\ |6^{10112}|_{13} &= |4 \cdot 6|_{13} = 11 \\ |6^{101102}|_{13} &= |11^2|_{13} = 4 \\ |6^{101112}|_{13} &= |4 \cdot 6|_{13} = 11 \end{aligned}$$

## 1.8 Eulerova věta

Pokud jsou  $m \geq 2$  a  $a \in \mathbb{N}$  nesoudělná, pak platí kongruence:

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

## 1.9 Hodnoty Eulerovy funkce

Číslo  $p$  je prvočíslem, právě když  $\varphi(p) = p - 1$ , a platí:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Jedná se o speciální případ rozkladu složeného čísla  $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$ :

$$\varphi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Pokud jsou  $m \in \mathbb{N}$  a  $a \in \mathbb{Z}_m$  nesoudělné, pak  $a^{\varphi(m)-1}$  je multiplikativní inverzí čísla  $a \bmod m$ .

## 1.10 Malá Fermatova věta

Jedná se o speciální případ Eulerovy věty. Pokud jsou prvočíslo  $p$  a  $a \in \mathbb{N}$  nesoudělné ( $p \nmid a$ ), potom platí kongruence:

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ \text{a pro } a \in \mathbb{Z}_p \setminus \{0\}: \quad a^{p-2} &\equiv a^{-1} \pmod{p} \end{aligned}$$