Dělitelnost

- Nechť $a, b \in \mathbb{Z}$. Řekneme, že a **dělí** b, jestliže existuje $q \in \mathbb{Z}$ takové, že $b = a \cdot q$. Značíme $a|b$.

- Nechť $a, b, m \in \mathbb{Z}$, $d \in \mathbb{N}$. Řekneme, že m je **společný dělitel** čísel a a b, jestliže $m|a \wedge m|b$. Řekneme, že d je **největší společný dělitel** a a b, jestliže je d společným dělitelem a a b a zároveň, je-li m libovolným společným dělitelem čísel a, b, pak $m|d$. Značíme $D(a, b) = d$.

- **Zbytkový tvar čísla:** $a, b, q, r \in \mathbb{Z}$
$$a = b \cdot q + r,$$
$0 \leq r < |b|$.

- **Bezoutova rovnost:** $a, b \in \mathbb{Z} \;\Rightarrow\; \exists\, x, y \in \mathbb{Z};$
$$D(a, b) = a \cdot x + b \cdot y$$

- **Nesoudělná** čísla $a, b \in \mathbb{Z}$ jsou taková čísla, pro která platí $D(a, b) = 1$.

- **Prvočíslo** je takové číslo, které je dělitelné pouze číslem 1 a sebou samým.

- Každé přirozené číslo lze rozložit na součin pročísel a to jednoznačně až na pořadí činitelů. Zápis $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde $p_1, p_2, \ldots, p_k$ jsou navzájem různá prvočísla, $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}_0$ se nazývá **kanonický rozklad** čísla n.

- $\varphi : \mathbb{N} \to \mathbb{N}$ je tzv. **Eulerova funkce**; $\forall n \in \mathbb{N}$; $\varphi(n)$ udává počet přirozených čísel menších nebo rovných n, která jsou s n nesoudělná. Klademe $\varphi(1) = 1$.

  1. Jsou-li m, n nesoudělná přirozená čísla, pak $\varphi(mn) = \varphi(m)\varphi(n)$, tj. Eulerova funkce je multiplikativní.
  2. Je-li p prvočíslo, pak
  $$\varphi(p) = p - 1.$$
  3. Je-li p prvočíslo a k kladné celé číslo, pak
  $$\varphi(p^k) = p^{k-1}(p-1).$$
  4. Je-li $n > 1$ přirozené číslo a $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ jeho kanonický rozklad, pak
  $$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1),$$
  resp.
  $$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

- **Euklidův algoritmus** pro hledání největšího společného dělitele čísel a, b:
$$\begin{array}{llllll}
 & & a = bq_1 + r_1 & & \Rightarrow & r_1 = 0 \;\Rightarrow\; b|a, \text{ a tedy } D(a,b) = b \\
r_1 \neq 0 & \Rightarrow & b = r_1 q_2 + r_2 & \Rightarrow & r_2 = 0, & \text{pak } D(a,b) = r_1 \\
r_2 \neq 0 & \Rightarrow & r_1 = r_2 q_3 + r_3 & & & \\
 & & \vdots & & & \\
 & & r_{n-2} = r_{n-1} q_n + r_n & & & \\
 & & r_{n-1} = r_n q_{n+1} + 0, & & & \text{pak } D(a,b) = r_n.
\end{array}$$

1. Euklidovým algoritmem určete největší společný dělitel čísel 1128 a 291. Určete koeficienty x, y

v Bezoutově nerovnosti.

Kongruence

$a, b \in \mathbb{Z}, m \in \mathbb{N}$, pak řekneme, že a je kongruentní s b modulo m, píšeme $a \equiv b \pmod{m}$, jestliže a i b dávají po dělení m stejný zbytek.

$$a \equiv b \pmod{m} \;\Leftrightarrow\; a = b + m \cdot q,\; q \in \mathbb{Z} \;\Leftrightarrow m|(a-b)$$

Relace kongruence je na množině $\mathbb{Z}$ reflexivní, symetrická a tranzitivní (je to relace ekvivalence).
Dále platí:

$$\begin{array}{c} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array} \;\Rightarrow\; \begin{array}{c} a + c \equiv b + d \pmod{m} \\ a - c \equiv b - d \pmod{m} \\ a \cdot c \equiv b \cdot d \pmod{m} \end{array}$$

$$\begin{array}{rclr} & a^n \equiv b^n \pmod{m} & a + km \equiv b \pmod{m} & \\ & ka \equiv kb \pmod{km} & a \equiv b + ml \pmod{m} & \\ & ka \equiv kb \pmod{m} & a + km \equiv b + ml \pmod{m} & \\ ak \equiv bk \pmod{m} \;\wedge\; D(k,m) = 1 & \Rightarrow & a \equiv b \pmod{m} & k, l \in \mathbb{Z} \end{array}$$

Eulerova věta: Nechť $a, m \in \mathbb{Z}, m \geq 1;\; D(a,m) = 1$. Pak

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

2. Určete zbytek po dělení čísla $2^{50} + 3^{50} + 4^{50}$ číslem 17.
3. Určete zbytek po dělení čísla $\left(4^{4^4} + 5^{5^5}\right)$ číslem 17.
4. Je číslo $2^{60} + 7^{30}$ dělitelné číslem 13?
5. Určete poslední cifru v dekadickém zápisu čísla 7^{7^7}.
6. Určete poslední cifru v dekadickém zápisu čísla $17^{13^{11^9}}$.
7. Určete všechna řešení lineární kongruence

$$4x \equiv 1 \pmod{15}$$

Zbytkové třídy

Značí se $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$, kde $[k]_n$ značí množinu čísel, které po dělení číslem n dávají zbytek k.

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n \cdot [b]_n = [a \cdot b]_n$$

$(\mathbb{Z}_n, +)$ je abelovská grupa, $(\mathbb{Z}_n, \cdot)$ je komutativní pologrupa s neutrálním prvkem $[1]_n$. Je-li n prvočíslo, pak $(\mathbb{Z}_n^*, \cdot)$ je abelovská grupa. Pokud n není prvočíslo, pak $(\mathbb{Z}_n^\times, \cdot)$, kde $\mathbb{Z}_n^\times$ je množina invertibilních prvků, je abelovská grupa.

8. Určete $[17]_{181}^{-1}$.

Permutace

- bijektivní zobrazení $\mathbb{A}$ na $\mathbb{A}$, kde $\mathbb{A}$ uvažujeme neprázdnou konečnou podmnožinu $\mathbb{N}$.
- $n \in \mathbb{N}$; množina všech permutací tvoří grupu, která je pro $n \geq 3$ nekomutativní; má $n!$ prvků.
- Libovolnou permutaci můžeme rozložit na součin **nezávislých cyklů**.
- Cyklus délky 2 = **transpozice**.
- Každou permutaci můžeme rozložit na součin transpozic. Pokud je počet transpozic lichý, pak mluvíme o **liché permutaci**, pokud je sudý, pak o **sudé perumutaci**.
- **Inverze** – dvojice prvků a, b tak, že

$$a < b \ \wedge \ \pi(a) > \pi(b)$$

- **Parita = znaménko permutace** $\operatorname{sgn}(\pi) = (-1)^n$; n udává počet inverzí. Pro dvě permutace platí

$$\operatorname{sgn}(\pi \circ \pi') = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}\pi').$$

  Je-li permutace π součinem nezávislých cyklů $\pi = \pi_1 \circ \pi_2 \circ \cdots \circ \pi_n$, delka cyklu $\pi_i = k_i + 1$:

$$\operatorname{sgn}(\pi) = \prod_{i=1}^{m} (-1)^{k_i} = (-1)^{\sum_{i=1}^{m} k_i}$$

9. Jsou dány permutace s a t:

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 2 & 8 & 5 & 6 & 7 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 2 & 3 & 7 & 1 & 8 & 6 \end{pmatrix}$$

   (a) Rozložte s a t na součin nezávislých cyklů.
   (b) Spočtěte součiny $s \circ t$ a $t \circ s$.
   (c) Určete inverzní prvky s^{-1}, t^{-1}.
   (d) Spočtěte permutaci $(s^{120} \circ t^{-3})^{17}$.
   (e) Permuteace s, t rozložte na součin transpozic a určete jejich paritu.

Symeetrie logotypů (obrazců)

$\mathbf{T_a}$ – translace o vektror a;
$\mathbf{R}_\varphi$ – otočení o úhel φ;
$\mathbf{Z_l}$ – zrcadlení vůči přímce l procházející počátkem.

Symetrie tvoří grupu.

Dihedrálni grupy řádu $2k$ – grupy symetrií s k různými rotacemi a k zrcadleními. U pravidelných k-úhelníků $\mathbf{D_{2k}}$.

10. Popište grupu symetrií čtverce.