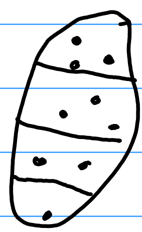
Kongruence

- zbytkové třídy
- počítání s kongruencemi
- malá Fermatova věta, Eulerova věta
- lineární kongruence
- soustavy lin. kongruencí, čínská zbytková věta

Zbytkové třídy



$\mathbb{Z} \longrightarrow \mathbb{Z}_n$ $\quad$ n - modul

$x \sim y \iff$
- stejný zbytek po dělení n
- $n \mid x-y$
- $x = y + an$

$x \equiv y \pmod{n}$

$2^5 = (3-1)^5 =$ zb. po dělení 3

$$= 3^5 - \binom{5}{1} 3^4 + \binom{5}{2} 3^3 - \binom{5}{3} 3^2 + \binom{5}{4} \cdot 3 - 1 \Rightarrow -1$$

$$2^5 = (3-1)^5 \equiv (-1)^5 = -1 \pmod{3}$$

Počítání

- $$\frac{\begin{array}{ll} a \equiv b & \pmod{n} \\ c \equiv d & \pmod{n} \end{array}}{a + c \equiv b + d \pmod{n}}$$

- $a \equiv b \pmod{n}$
  $ca \equiv cb \pmod{n}$
  $ac \equiv bd \pmod{n}$

- $a/(a,b) \equiv b/(a,b) \pmod{n}$, pokud $((a,b), n) = 1$
- $a \equiv b \pmod{n_1, \dots, n_k}$
  $a \equiv b \pmod{[n_1, \dots, n_k]}$

Př. 1) zb. po dělení 5^{20} číslem 26

$$5^{20} = 25^{10} = (26-1)^{10} \equiv (-1)^{10} = \underline{\underline{1}} \quad (\mathrm{mod}\ 26)$$

2) dokažte, že $37^{n+2} + 16^{n+1} + 23^{n}$ je dělitelné 7, $n \in \mathbb{N}$

$$37^{n+2} + 16^{n+1} + 23^{n} \equiv 2^{n+2} + 2^{n+1} + 2^{n} \quad (\mathrm{mod}\ 7)$$
$$= 2^{n}(4+2+1) \equiv 0$$

Malá Fermatova věta

V. Nechť p je prvočíslo, $a \in \mathbb{Z}$, $p \nmid a$. Pak platí
$$a^{p-1} \equiv 1 \quad (\mathrm{mod}\ p)$$

D. Indukcí k a:

I. $a = 1$ $\quad 1^{p-1} = 1$

II. předp., že platí $a^{p-1} \equiv 1 \ (\mathrm{mod}\ p)$, dokazujeme $(a+1)^{p-1} \equiv 1 \ (\mathrm{mod}\ p)$

$$(a+1)^{p} = a^{p} + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a + 1$$

p prvočíslo $\Rightarrow$ $\underbrace{p \mid \binom{p}{k}}$ $= \frac{p!}{k!(p-k)!}$ $\quad k \in \{1, \dots, p-1\}$

$$\equiv a^{p} + 1 \equiv a + 1 \quad (\mathrm{mod}\ p)$$
$$(a+1)^{p-1} \equiv 1 \quad (\mathrm{mod}\ p)$$

Př. $21^{480} = \underbrace{21}^{460+20} \equiv \quad (\mathrm{mod}\ 47)$

$47 = 46 + 1$

$$\equiv 1 \cdot 21^{20} = 441^{10} \equiv$$
$$(-29)^{10} \equiv 18^{10} = 324^{5} \equiv (-146)^{5} \equiv$$
$$\equiv (-99)^{5} \equiv (-5)^{5} = 25^{2} \cdot (-5) = 625 \cdot (-5) \equiv$$
$$\equiv -5 \cdot 155 = -5 \cdot 14 = -70 \equiv \underline{\underline{24}}$$

Eulerova věta

V. $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a,n) = 1$ — Eulerova funkce

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

$\varphi(n)$ ... počet nesoudělných čísel mezi 1 až $n-1$ s n

Př. $\varphi(12) = |\{1,5,7,11\}| = 4$

vlastnosti φ:
- $\varphi(a,b) = \varphi(a)\cdot\varphi(b)$ pro $(a,b)=1$
- $\varphi(p) = p-1$
- $\varphi(p^k) = (p-1)p^{k-1}$

$$\varphi(12) = \varphi(3)\cdot\varphi(\underbrace{4}_{2^2}) = (3-1)\cdot(2-1)\cdot 2^1 = 4$$

jiný vzorec: $\varphi(n) = p_1^{\alpha_1-1}\cdot \ldots \cdot p_k^{\alpha_k-1}\cdot(p_1-1)\cdot\ldots\cdot(p_k-1)$

$$= n\cdot\left(1-\frac{1}{p_1}\right)\cdot \ldots \cdot\left(1-\frac{1}{p_k}\right)$$

$n = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$

Př. $\varphi(72) = \varphi(2^3\cdot 3^2) = 2^2\cdot 3^1\cdot(2-1)\cdot(3-1) =$
$= 24$

$$= 72\cdot\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right) =$$
$$= 72\cdot\frac{1}{\cancel{2}}\cdot\frac{\cancel{2}}{3} = 24$$

x řád prvku: $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $(a,n)=1$

$a^x \equiv 1 \pmod{n}$, x nejmenší takové

Př. zjistěte řád 2 modulo 7.

$2^1 = 2 \not\equiv 1 \pmod 7$
$2^2 = 4 \not\equiv 1$ -"-
$2^3 = 8 \equiv 1 \pmod 7 \Rightarrow 3$ řád

primitivní kořen – řád je $\varphi(n)$

Lineární kongruence

$ax \equiv b \pmod n$

V. ↑ má řešení $\Leftrightarrow (a,n) \mid b$
Pak je řešení právě (a,n).

Př. (1) $2x \equiv 1 \pmod 3$ $\quad (2,3) = 1 \quad 1 \mid 1$
1 řešení $\quad 2 \cdot 2 \equiv 1 \quad 2 \cdot (-1) \equiv 1$

(2) $10x \equiv 5 \pmod{15}$ $\quad (10,15) = 5 \quad 5 \mid 5$
5 řešení

$10 \cdot 2 = 20 \equiv 5$ $\quad 10 \cdot 5 = 50 \equiv 5$
$10 \cdot 8 = 80 \equiv 5$ $\quad 10 \cdot 11 \equiv 10 \cdot (-4) = -40 \equiv 5$
$10 \cdot 14 \equiv 10 \cdot (-1) = -10 \equiv 5$

Př $39x \equiv 41 \pmod{47}$
1) Euler – obecný přístup
2) $39x + 47y = 41$
3) úpravy

$\pmod{47}$ $39x \equiv 41$ $\quad$ mělo by být jediné řešení
$-8x \equiv -6$ $\quad 2x \equiv 25 \equiv -22$
$4x \equiv 3 \equiv 50$ $\quad x \equiv -11 \equiv 36$
$39 \cdot (-11) = -429 \equiv 41$

Soustavy lineárních kongruencí

(čínská zbytková věta)

V. Soustava

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv c_k \pmod{m_k}$$

je řešitelná a to jednoznačně (modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_k$), pokud $m_1, \ldots, m_k$ jsou po dvou nesoudělné.

Př.

$$x \equiv 1 \pmod{10}$$
$$x \equiv 5 \pmod{18}$$
$$x \equiv -4 \pmod{25}$$

$x = 10k + 1$

$10k + 1 \equiv 5 \pmod{18}$

$10k \equiv 4 \pmod{18}$

$5k \equiv 2 \pmod{9}$

$k \equiv 4 \pmod{9}$

$k = 9l + 4$

$x = 90l + 41$

$\underline{x \equiv 221} \pmod{450}$