

Teorie čísel

Milan Radojčić

SSPŠaG – KBB

29. září 2026



Hlavní body

Úvod

Prvočísla

Kongruence

Algoritmus *Square and Multiply*

Eulerova věta



Hlavní body

Úvod

Prvočísla

Kongruence

Algoritmus *Square and Multiply*

Eulerova věta



Úvod

- ▶ Teorie čísel se zabývá vlastnostmi (hlavně celých) čísel.
- ▶ Jedná se o jednu z nejstarších matematických disciplín vedle algebry, aritmetiky a geometrie.
- ▶ Poznatky jsou v současné době používány v asymetrické kryptografii (RSA, pseudonáhodné generátory).



Hlavní body

Úvod

Prvočísla

Kongruence

Algoritmus *Square and Multiply*

Eulerova věta



Dělitelnost

Definice

Mějme $a, b \in \mathbb{Z}$, platí, že a **dělí** b , značíme $a \mid b$, právě tehdy, když:
 $(\exists k \in \mathbb{Z})(a \cdot k = b)$.

Definice

Číslo $c \in \mathbb{N}_0$ je **největším společným dělitelem** čísel $a, b \in \mathbb{Z}$, značíme $c = \gcd(a, b)$, pokud je jejich společný dělitel a zároveň je celočíselným násobkem každého jiného jejich společného dělitele.

Definice

Čísla $a, b \in \mathbb{Z}$ nazýváme **nesoudělná** právě tehdy, když $\gcd(a, b) = 1$.



Definice prvočísla

Definice

Přirozené číslo $n \geq 2$ nazýváme **prvočíslem** právě tehdy, když má jen dva dělitele: 1 a sebe sama.

Definice

Přirozené číslo $n \geq 2$ nazýváme **složeným číslem** právě tehdy, když není prvočíslem (má jiného dělitele než 1 a sebe sama).

Z těchto definic je patrné, že číslo 1 nepatří ani do čísel složených ani do prvočísel a tvoří samotnou skupinu.



Základní věta aritmetiky

Věta

Každé $c \in \mathbb{N}$, $c \geq 2$ lze vyjádřit ve tvaru:

$$c = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_n^{m_n} = \prod_{i=1}^n p_i^{m_i}$$

kde $p_1, \dots, p_n$ jsou prvočísla a $m_1, \dots, m_n$ jsou celá čísla. Tento zápis také nazýváme **prvočíselným rozkladem**.

Příklad

$$36 = 2 \cdot 18 = 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$$



Základní věta aritmetiky

- ▶ Problém faktorizace je předpokládán za velice obtížný.
- ▶ Není znám obecný algoritmus co by dokázal faktorizovat „rychle.“¹
 - Předpokládá se, že takový algoritmus *neexistuje*.
- ▶ Na tomto je založena bezpečnost RSA.

¹V polynomiálním čase vůči počtu cifer.



Hlavní body

Úvod

Prvočísla

Kongruence

Algoritmus *Square and Multiply*

Eulerova věta



Kongruence modulo n

Definice

Mějme $a, b, n \in \mathbb{N}$ a $n \geq 2$. Říkáme, že a je **kongruentní** s b modulo n , značíme

$$a \equiv b \pmod{n}$$

právě tehdy, když $n \mid (a - b)$.

Příklad

$$11 \equiv 7 \equiv 3 \pmod{4}$$



Věta

Následující tvrzení jsou ekvivalentní:

- ▶ $a \equiv b \pmod{n}$
- ▶ $a \bmod n = b \bmod n$
- ▶ $(\exists l \in \mathbb{N})(b = a + l \cdot n)$



Úpravy v kongruencích modulo n

- ▶ Můžeme nejprve zmodulovat čísla a pak s nimi dále počítat (u sčítání, odčítání, násobení a dělení).
- ▶ Můžeme obě strany rovnic vynásobit stejným číslem. Také můžeme od nich stejné čísla odečítat nebo přičítat.
- ▶ **Nemůžeme** modulovat čísla v exponentech. Tzn. provádět úpravy typu: $4^7 \not\equiv 4^2 \pmod{5}$
- ▶ **Nemůžeme** *jednoduše* dělit obě strany rovnice číslem. Např.: $4x \equiv 12 \pmod{20}$ a $x \equiv 3 \pmod{20}$ nejsou stejné rovnice. První rovnice platí pro $x = 8$, ale druhá ne.



Krácení rovnic v kongruencích modulo n

Věta

Mějme $a, b, c, n \in \mathbb{N}$ a $n \geq 2$, pak platí:

$$ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{\gcd(c,n)}}$$

Příklad

$$4x \equiv 8 \pmod{18} \div 4$$

$$4x \equiv 8 \pmod{18} \div 4, \gcd(18, 4) = 2$$

$$x \equiv 2 \pmod{9}$$



Zjednodušte tak, aby se na levé straně nacházelo jen x

$$8 + 5x \equiv 18 \pmod{15}$$

$$18 + 12x \equiv 78 \pmod{9}$$

$$9 + 12x \equiv 225 \pmod{30}$$

$$2 + 8x \equiv 39 \pmod{29}$$

$$9 + 5x \equiv 49 \pmod{17}$$

$$6 + 12x \equiv 42 \pmod{15}$$

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

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

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

$$x \equiv 1 \pmod{29}$$

$$x \equiv 8 \pmod{17}$$

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



Hlavní body

Úvod

Prvočísla

Kongruence

Algoritmus *Square and Multiply*

Eulerova věta



Algoritmus *Square and Multiply*

- ▶ Jako příklad si vezměme např. a^8 .
 - Naivně na to potřebujeme 7 násobení.
 - Jde to lépe?
- ▶ Mocninu si můžeme rozložit jako $((a^2)^2)^2$.
 - To jsou jen **3 násobení**!
- ▶ Na tomto je založen algoritmus *Square and Multiply*.
 - Někdy se používá český výraz *binární umocňování*.



Ukázka *Square and Multiply*

Ukažme si *Square and Multiply* na příkladě. Zkusíme vypočítat $2^{15} \bmod 5$.

Jako první si rozdělíme 2^{15} na $2^1 \cdot 2^2 \cdot 2^4 \cdot 2^8$.

A nyní už jen vypočítáme jednotlivé mocniny:

$$2^1 \equiv 2 \pmod{5}, \quad 2^2 \equiv (2^1)^2 \equiv 2^2 \equiv 4 \pmod{5}$$

$$2^4 \equiv (2^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{5}$$

$$2^8 \equiv (2^4)^2 \equiv 1^2 \equiv 1 \pmod{5}$$

$$2^{15} \equiv 2 \cdot 4 \cdot 1 \cdot 1$$



Popis *Square and Multiply*

1. Rozdělíme naši mocninu na součin tak, aby v exponentech byly jen mocniny dvojek.
2. Postupně vypočítáme od nejmenšího exponentu všechny mocniny v našem součinu tak, že využijeme výsledek z té předchozí.
3. Vypočítáme naši mocninu ze součinu mocnin.



Square and Multiply pseudokód

Vstup: a, e, m

Výstup: $v \equiv a^e \pmod{m}$

$v \leftarrow 1$

$temp \leftarrow a$

for $i \leftarrow 0, \dots, n-1$ **do**

if $e_i = 1$ **then** $\triangleright$ zápisem e_i myslíme bit na i -té pozici čísla e

$v \leftarrow v \cdot temp \pmod{m}$

end if

$temp \leftarrow temp^2 \pmod{m}$

end for



Příklady

Zjednodušte následující výrazy

$$2^{16} \pmod{8}$$

$$3^{31} \pmod{10}$$

$$6^{64} \pmod{7}$$

$$7^7 \pmod{8}$$



Hlavní body

Úvod

Prvočísla

Kongruence

Algoritmus *Square and Multiply*

Eulerova věta



Definice

Eulerova funkce (značíme $\varphi(n)$) je počet všech $k \in \mathbb{N}$ takových, že $1 \leq k \leq n$ a $\gcd(k, n) = 1$.

Slovně: **Eulerova funkce** nám udává počet čísel menší než n , která jsou s ním **nesoudělná**.



Vlastnosti Eulerovy funkce

Pro výpočet se nám budou často hodit následující vlastnosti Eulerovy funkce.

- ▶ $\varphi(p) = p - 1$, kde p je prvočíslo (plyne přímo z definice prvočísla)
- ▶ $\varphi(p^a) = (p - 1) \cdot p^{a-1}$, pro prvočíslo p a kladné celé a
- ▶ Pro nesoudělná x, y platí: $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$



Z těchto vlastností a ze základní věty aritmetiky (prvočíselný rozklad) nám plyne následující věta.

Věta

Pro $c \in \mathbb{N}$ platí, že pokud: $c = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_n^{m_n}$, tak platí:

$$\varphi(c) = (p_1 - 1) \cdot p_1^{m_1-1} \cdot (p_2 - 1) \cdot p_2^{m_2-1} \cdot \dots \cdot (p_n - 1) \cdot p_n^{m_n-1}$$



Eulerova věta

Věta

Pro každé $n \in \mathbb{N}$ a každé $a \in \mathbb{N}$ takové, že $\gcd(n, a) = 1$, platí:

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

- Pro prvočíselné n se dá odvodit vztah

$$a^{n-1} \equiv 1 \pmod{n}.$$

- Tomuto vztahu se říká *malá Fermatova věta*.



Příklady

Zjednodušte následující výrazy

$$3^5 \pmod{8}$$

$$8^6 \pmod{9}$$

$$3^5 \pmod{9}$$

$$7^{17} \pmod{15}$$

