Modulární aritmetika

prof. RNDr. Miroslav Vlček, DrSc.

vlcek@fd.cvut.cz

1. listopadu 2007

Modulární aritmetika

1. Dělitelnost čísel a kongruence

2. Modulární operace sčítání, odčítání a násobení

3. Modulární dělení

4. Fermatova věta

Dělitelnost čísel a kongruence

- Říkáme, že dvě přirozená čísla a a b jsou kongruentní modulí n, jestliže při dělení a číslem n obdržíme zbytek b nebo, že jejich rozdíl $a - b$ je násobkem čísla n. Píšeme

$$a \equiv b \,(\mathrm{mod}\, n) \iff a - b = k \times n \quad (1)$$

- Příklady kongruence

$$\begin{aligned}
17 &\equiv 5 \,(\mathrm{mod}\, 12) &&\iff 17 - 5 = 1 \times 12 \\
35 &\equiv 11 \,(\mathrm{mod}\, 12) &&\iff 35 - 11 = 2 \times 12 \\
168 &\equiv 0 \,(\mathrm{mod}\, 12) &&\iff 168 - 0 = 14 \times 12 \\
169 &\equiv 1 \,(\mathrm{mod}\, 12) &&\iff 169 - 1 = 14 \times 12 \\
2\,k + 1 &\equiv 1 \,(\mathrm{mod}\, 2) &&\iff 2\,k + 1 - 1 = k \times 2
\end{aligned}$$

- Je zřejmé, že pro přirozené číslo a dělitelné číslem n beze zbytku platí

$$a \equiv 0 \,(\mathrm{mod}\, n) \iff a = k \times n$$

Modulární operace

- Kongruence je symetrická a transitivní

$$a \equiv b \,(\mathrm{mod}\, n) \quad \longleftrightarrow \quad b \equiv a \,(\mathrm{mod}\, n)$$
$$a \equiv b \equiv c \,(\mathrm{mod}\, n) \quad \longleftrightarrow \quad a \equiv c \,(\mathrm{mod}\, n)$$

- Sčítání

$$a \equiv b \,(\mathrm{mod}\, n) \,\&\, c \equiv d \,(\mathrm{mod}\, n) \quad \rightarrow \quad a + c \equiv b + d \,(\mathrm{mod}\, n)$$

- Odčítání

$$a \equiv b \,(\mathrm{mod}\, n) \,\&\, c \equiv d \,(\mathrm{mod}\, n) \quad \rightarrow \quad a - c \equiv b - d \,(\mathrm{mod}\, n)$$

- Násobení, pro a, b, c, d celá čísla

$$a \equiv b \,(\mathrm{mod}\, n) \,\&\, c \equiv d \,(\mathrm{mod}\, n) \quad \rightarrow \quad a \times c \equiv b \times d \,(\mathrm{mod}\, n)$$

- Mocnina, opakované násobení, pro a, b, m celá čísla

$$a \equiv b \,(\mathrm{mod}\, n) \,\&\, a \equiv b \,(\mathrm{mod}\, n) \quad \rightarrow \quad a^m \equiv b^m \,(\mathrm{mod}\, n)$$

- Příklad 1- Protože platí

$$2^2 \equiv 1 \,(\mathrm{mod}\, 3)$$
$$2^2 \equiv 1 \times 2^2 \equiv 1 \,(\mathrm{mod}\, 3) \Rightarrow 2^4 \equiv 1 \,(\mathrm{mod}\, 3)$$
$$\vdots$$
$$\Rightarrow 2^{2m} \equiv 1 \,(\mathrm{mod}\, 3) \Rightarrow 2^{2m} - 1 \equiv 0 \,(\mathrm{mod}\, 3)$$

  je každé Mersenneovo číslo $2^n - 1$ dělitelné 3, jestliže $n = 2\,m$ je sudé.

- Příklad - Určete zda číslo 11^{207} je dělitelné třemi. Protože platí

$$11^{207}(\mathrm{mod}\, 3) \equiv 11^{128+64+8+4+2+1}(\mathrm{mod}\, 3) \equiv$$
$$\equiv [11^{128} \times 11^{64} \times 11^8 \times 11^4 \times 11^2 \times 11](\mathrm{mod}\, 3) \equiv$$
$$\equiv [1 \times 1 \times 1 \times 1 \times 1 \times 2](\mathrm{mod}\, 3) \equiv 2(\mathrm{mod}\, 3)$$

- Z kongruence $11^{207} \equiv 2(\mathrm{mod}\, 3)$ již plyne, že

11^{207} není dělitelné třemi,

$11^{207} - 2$ je dělitelné třemi.

Modulární operace - dělení

- Pokud

$$a \times d \equiv b \times d \,(\mathrm{mod}\, n)$$

obecně neplatí, že

$$a \equiv b \,(\mathrm{mod}\, n).$$

- Například z kongruence

$$10 \equiv 6 \,(\mathrm{mod}\, 4) \longrightarrow 5 \times 2 \equiv 3 \times 2 \,(\mathrm{mod}\, 4)$$

neplyne $5 \equiv 3 \,(\mathrm{mod}\, 4)$

- Modulární dělení, lze provést pro d, n nesoudělná čísla (relative prime),

$$a \times d \equiv b \times d \,(\mathrm{mod}\, n) \iff a \equiv b \,(\mathrm{mod}\, n)$$

- Například z kongruence

  $170 \equiv 35 \,(\mathrm{mod}\, 3) \longrightarrow 5 \times 34 \equiv 5 \times 7 \,(\mathrm{mod}\, 3)$

  plyne $34 \equiv 7 \,(\mathrm{mod}\, 3)$, protože $3, 5$ jsou nesoudělná čísla.

- Modulární dělení, lze provést pro $d \neq 0$ celé

  $a \times d \equiv b \times d \,(\mathrm{mod}\, n \times d) \iff a \equiv b \,(\mathrm{mod}\, n)$

- Například z kongruence

  $10 \equiv 6 \,(\mathrm{mod}\, 4) \longrightarrow 5 \times 2 \equiv 3 \times 2 \,(\mathrm{mod}\, 2 \times 2)$

  plyne $5 \equiv 3 \,(\mathrm{mod}\, 2)$

Malá Fermatova věta

Z roku 1640, anglický název Fermat´s Little Theorem

- Jestliže p je prvočíslo, které není dělitelem a, pak
$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

- Alternativní tvar
$$a^{p} \equiv a (\mathrm{mod}\, p).$$

- V témže roce 1640 Fermat napsal Mersenneovi, že přepokládá, že čísla $F_n = 2^{2^n} + 1$ jsou prvočísla.

- Ukážeme si, jak použít malou Fermatovu větu k důkazu, že čísla $F_3 = 2^{2^3} + 1 = 257$ resp. $F_4 = 2^{2^4} + 1 = 65537$ jsou prvočísla.

Zvolme $a = 3$ a předpokládejme, že

$$p = 257 = 2^{2^3} + 1$$

je prvočíslo. Potom podle malé Fermatovy věty musí platit

$$3^{2^{2^3}} \equiv 1 (\mathrm{mod}\, 2^{2^3} + 1),$$

resp.

$$3^{2^8} \equiv 1 (\mathrm{mod}\, 2^8 + 1).$$

Platí postupně

$$\begin{aligned}
3^2 &\equiv 9 (\mathrm{mod}\, 257) \\
3^{2^2} &\equiv 81 (\mathrm{mod}\, 257) \\
3^{2^3} &\equiv 136 (\mathrm{mod}\, 257) && 6561 = 25 \times 257 + 136 \\
3^{2^4} &\equiv 249 (\mathrm{mod}\, 257) && 18496 = 71 \times 257 + 249 \\
3^{2^5} &\equiv 64 (\mathrm{mod}\, 257) && 62001 = 211 \times 257 + 64 \\
3^{2^6} &\equiv 241 (\mathrm{mod}\, 257) && 4096 = 151 \times 257 + 241 \\
3^{2^7} &\equiv 256 (\mathrm{mod}\, 257) && 58081 = 225 \times 257 + 256 \\
3^{2^8} &\equiv 1 (\mathrm{mod}\, 257) && 65536 = 255 \times 257 + 1
\end{aligned}$$

Poslední kongruence potvrzuje, že 257 je prvočíslo.