Hlubší věty o počítání modulo

Příklad

Vyřešte:

$$x = 3 \text{ v } \mathbb{Z}_4 \quad x = 2 \text{ v } \mathbb{Z}_5 \quad x = 6 \text{ v } \mathbb{Z}_{21}$$

Idea řešení:

$$x = 3 \cdot \square + 2 \cdot \square + 6 \cdot \square$$

Musí být:

1. První obdélník roven 1 v $\mathbb{Z}_4$ a roven 0 v $\mathbb{Z}_5$ a v $\mathbb{Z}_{21}$.
2. Druhý obdélník roven 1 v $\mathbb{Z}_5$ a roven 0 v $\mathbb{Z}_4$ a v $\mathbb{Z}_{21}$.
3. Třetí obdélník roven 1 v $\mathbb{Z}_{21}$ a roven 0 v $\mathbb{Z}_4$ a v $\mathbb{Z}_5$.

Příklad (pokrač.)

Nulovost obdélníků:

$$x = 3 \cdot \boxed{5 \cdot 21 \cdot ?} + 2 \cdot \boxed{4 \cdot 21 \cdot ?} + 6 \cdot \boxed{4 \cdot 5 \cdot ?}$$

Jedničkovost obdélníků:

$$x = 3 \cdot \boxed{5 \cdot 21 \cdot 1} + 2 \cdot \boxed{4 \cdot 21 \cdot 4} + 6 \cdot \boxed{4 \cdot 5 \cdot 20}$$

protože:

1. $(5 \cdot 21)^{-1} = 1^{-1} = 1$ v $\mathbb{Z}_4$. ($\gcd(4,5) = 1$ a $\gcd(4,21) = 1$)
2. $(4 \cdot 21)^{-1} = 4^{-1} = 4$ v $\mathbb{Z}_5$. ($\gcd(5,4) = 1$ a $\gcd(5,21) = 1$)
3. $(4 \cdot 5)^{-1} = 20^{-1} = 20$ v $\mathbb{Z}_{21}$. ($\gcd(21,4) = 1$ a $\gcd(21,5) = 1$)

Příklad (pokrač.)

Celkově:

$$x = 3 \cdot 5 \cdot 21 \cdot 1 + 2 \cdot 4 \cdot 21 \cdot 4 + 6 \cdot 4 \cdot 5 \cdot 20 = 3\,387 = 27 \quad \text{v } \mathbb{Z}_{420}$$

protože[a] $\operatorname{lcm}(4, 5, 21) = 4 \cdot 5 \cdot 21 = 420$.

Funguje to:

$$27 = 3 \text{ v } \mathbb{Z}_4 \quad 27 = 2 \text{ v } \mathbb{Z}_5 \quad 27 = 6 \text{ v } \mathbb{Z}_{21}$$

[a] $\operatorname{lcm}(a, \ldots, b)$ značí nejmenší společný násobek celých čísel $a, \ldots, b$, anglicky least common multiple.

Čínská věta o zbytcích (Sun Zi: 3. stol. n. l.)

Ať $m_1, m_2, \ldots, m_r$ jsou navzájem nesoudělná přirozená čísla, $m_i \geq 2$ pro $i = 1, \ldots, r$. Potom každá soustava rovnic

$$\begin{aligned} x &= a_1 \quad \text{v } \mathbb{Z}_{m_1} \\ x &= a_2 \quad \text{v } \mathbb{Z}_{m_2} \\ &\vdots \\ x &= a_r \quad \text{v } \mathbb{Z}_{m_r} \end{aligned}$$

má řešení a toto řešení je určeno jednoznačně v $\mathbb{Z}_M$, kde $M = m_1 \cdot m_2 \cdot \cdots \cdot m_r$.

Zobecnění čínské věty

Ať m_1 a m_2 jsou libovolná přirozená čísla, $m_i \geq 2$ pro $i = 1, 2$. Označme $d = \gcd(m_1, m_2)$. Pak jsou následující dvě podmínky ekvivalentní:

1. Soustava

$$x = a_1 \quad \text{v } \mathbb{Z}_{m_1} \qquad x = a_2 \quad \text{v } \mathbb{Z}_{m_2}$$

   má řešení.

2. Platí $d \mid (a_2 - a_1)$.

Jestliže platí $d \mid (a_2 - a_1)$, je řešení určeno jednoznačně v $\mathbb{Z}_M$, kde $M = \operatorname{lcm}(m_1, m_2)$.

Máme tedy rekursivní algoritmus pro řešení jakékoli soustavy!

Příklad

Čísla $m_1 = 5$, $m_2 = 7$, $m_3 = 11$, $m_4 = 13$ jsou navzájem nesoudělná, $M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 5\,005$.
Čínská věta o zbytcích: pro čísla $0 \leq Z < 5\,005$ je korespondence:

$$Z \leftrightarrow ([Z]_5, [Z]_7, [Z]_{11}, [Z]_{13})$$

bijekce a respektuje sčítání a násobení (po složkách).

Příklad (pokrač.)

Vynásobte 28 a 47. Protože výsledek Z je $< 5\,005$, postupujeme takto:

1. $28 \mapsto ([28]_5, [28]_7, [28]_{11}, [28]_{13}) = (3, 0, 6, 2)$.
2. $47 \mapsto ([47]_5, [47]_7, [47]_{11}, [47]_{13}) = (2, 5, 3, 8)$.
3. Po složkách vynásobíme: $(1, 0, 7, 3)$.
4. Dekódujeme čínskou větou o zbytcích: $(1, 0, 7, 3) \mapsto 1\,316$.

Rychlost algoritmu, zobecnění (rychlé násobení matic, apod.) viz např.

- V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge Univ. Press, 2005

Malá Fermatova věta (Pierre de Fermat: 1601–1665)

Ať p je prvočíslo. Jestliže $\gcd(a, p) = 1$, pak platí

$$a^{p-1} = 1 \quad \text{v } \mathbb{Z}_p$$

Důkaz.

Zobrazení $x \mapsto x \cdot a$ je bijekce na invertibilních prvcích $\mathbb{Z}_p$.
To jsou prvky $\{1, 2, \ldots, p-1\}$.
Proto

$$\{1a, 2a, \ldots, (p-1)a\} = \{1, \ldots, (p-1)\} \text{ v } \mathbb{Z}_p$$

Proto $a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ v $\mathbb{Z}_p$.
Tedy $a^{p-1} = 1$ v $\mathbb{Z}_p$. ■

Definice

Eulerova funkce φ: pro kladné přirozené číslo m je $\varphi(m)$ počet všech čísel x z množiny $\{1, \ldots, m\}$, pro která platí $\gcd(x, m) = 1$.

Poznámka

$\varphi(m)$ je počet invertibilních prvků v $\mathbb{Z}_m$.

Vlastnosti Eulerovy funkce

1. $\varphi(1) = 1$.
2. Pro prvočíslo p je $\varphi(p) = p - 1$.
3. Pro prvočíslo p je $\varphi(p^n) = p^n - p^{n-1}$.
4. Pro nesoudělná a, b je $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Příklad

$1960 = 2^3 \cdot 5 \cdot 7^2$. Proto $\varphi(1960) = \varphi(2^3) \cdot \varphi(5) \cdot \varphi(7^2) = (2^3 - 2^2) \cdot (5 - 1) \cdot (7^2 - 7) = 4 \cdot 4 \cdot 42 = 672$.

Eulerova věta (Leonard Euler: 1707–1783)

Jestliže $\gcd(a, m) = 1$, pak platí

$$a^{\varphi(m)} = 1 \quad \text{v } \mathbb{Z}_m$$

Důkaz.

Zobrazení $x \mapsto x \cdot a$ je bijekce na invertibilních prvcích $\mathbb{Z}_m$.
To jsou prvky $\{b_1, b_2, \ldots, b_{\varphi(m)}\}$.
Proto

$$\{b_1 a, b_2 a, \ldots, b_{\varphi(m)} a\} = \{b_1, \ldots, b_{\varphi(m)}\} \text{ v } \mathbb{Z}_m$$

Proto $a^{\varphi(m)} \cdot b_1 \cdot b_2 \cdot \cdots \cdot b_{\varphi_m} = b_1 \cdot b_2 \cdot \cdots \cdot b_{\varphi(m)}$ v $\mathbb{Z}_m$.
Tedy $a^{\varphi(m)} = 1$ v $\mathbb{Z}_m$. ■

Příklad

Spočítejte $13^{12\,098}$ v $\mathbb{Z}_{1960}$.

Postup:

1. Spočítáme: $1960 = 2^3 \cdot 5 \cdot 7^2$, takže $\gcd(1960, 13) = 1$.
2. Spočítáme: $\varphi(1960) = 672$, takže $13^{672} = 1$ v $\mathbb{Z}_{1960}$.
3. Spočítáme: $12\,098 = 672 \cdot 18 + 2$.
4. Takže:

$$13^{12\,098} = 13^{672 \cdot 18 + 2} = (13^{672})^{18} \cdot 13^2 = 1 \cdot 13^2 = 13^2 = 169$$

v $\mathbb{Z}_{1960}$.

Eulerova věta drasticky snižuje exponent velkých mocnin.
Jak ale spočítat např. 13^{654} v $\mathbb{Z}_{1960}$?

Příklad (Budeme potřebovat příště)

Spočítejte $x = 11^{16\,601}$ v $\mathbb{Z}_{36\,181}$, když víme, že $36\,181 = 97 \cdot 373$ (rozklad na prvočísla).
Eulerova věta dává:

$$x = 11^{16\,601} = 11^{96\cdot 172+89} = 11^{89} \quad \text{v } \mathbb{Z}_{97}$$
$$x = 11^{16\,601} = 11^{372\cdot 44+233} = 11^{233} \quad \text{v } \mathbb{Z}_{373}$$

Použijeme čínskou větu o zbytcích a získáme x v $\mathbb{Z}_{36\,181}$.
Výpočet 11^{89} v $\mathbb{Z}_{97}$?
Výpočet 11^{233} v $\mathbb{Z}_{373}$?

Příklad (pokrač.)

Binární rozvoj exponentu 89 je $(89)_2 = (1, 0, 1, 1, 0, 0, 1)$.

Algoritmus opakovaných čtverců v $\mathbb{Z}_{97}$:

X	$11 = 11 \cdot 1$
S	$11^2 = 121 = 24$
S	$11^4 = 24^2 = 576 = 91$
X	$11^5 = 11 \cdot 91 = 1\,001 = 31$
S	$11^{10} = 31^2 = 961 = 88$
X	$11^{11} = 11 \cdot 88 = 968 = 95$
S	$11^{22} = 95^2 = 9\,025 = 4$
S	$11^{44} = 4^2 = 16$
S	$11^{88} = 16^2 = 256 = 62$
X	$11^{89} = 11 \cdot 62 = 682 = 3$

$11^{89} = 3$ v $\mathbb{Z}_{97}$.

Příklad (pokrač.)

Binární rozvoj exponentu 233 je $(233)_2 = (1, 1, 1, 0, 1, 0, 0, 1)$.

Algoritmus opakovaných čtverců v $\mathbb{Z}_{373}$:

X	$11 = 11 \cdot 1$
S	$11^2 = 121$
X	$11^3 = 11 \cdot 121 = 1\,331 = 212$
S	$11^6 = 212^2 = 44\,944 = 184$
X	$11^7 = 11 \cdot 184 = 2\,024 = 159$
S	$11^{14} = 159^2 = 25\,281 = 290$
S	$11^{28} = 290^2 = 84\,100 = 175$
X	$11^{29} = 11 \cdot 175 = 1\,925 = 60$
S	$11^{58} = 60^2 = 3\,600 = 243$
S	$11^{116} = 243^2 = 59\,049 = 115$
S	$11^{232} = 115^2 = 13\,225 = 170$
X	$11^{233} = 11 \cdot 170 = 1\,870 = 5$

$11^{233} = 5$ v $\mathbb{Z}_{373}$.

Příklad (pokrač.)

Čínská věta o zbytcích pro

$$x = 3 = 11^{89} \text{ v } \mathbb{Z}_{97} \qquad x = 5 = 11^{233} \text{ v } \mathbb{Z}_{373}$$

Řešení:

$$x = 11^{16\,601} = 3 \cdot \boxed{373 \cdot 84} + 5 \cdot \boxed{97 \cdot 50} = 118\,246 = 9\,703 \text{ v } \mathbb{Z}_{36\,181}$$

Shrnutí — výpočet a^b v $\mathbb{Z}_m$

1. Zredukujte (pokud to jde) a v $\mathbb{Z}_m$. Označte jej jako x. Platí tedy $0 \leq x < m$. Dále počítejte x^b v $\mathbb{Z}_m$.
2. Zredukujte (pokud to jde) exponent b pomocí Eulerovy věty. K tomu je nutné, aby platilo $\gcd(x, m) = 1$.
3. Počítejte x^b v $\mathbb{Z}_m$ algoritmem opakovaných čtverců.
4. Pokud navíc známe prvočíselný rozklad čísla m, může být vhodné použít čínskou větu o zbytcích.