Modulární aritmetika, Malá Fermatova věta,

Matematické algoritmy (11MA)

Jan Přikryl, Miroslav Vlček

3. přednáška 11MA
čtvrtek 14. října 2010

verze: 2010-11-29 13:27

1 Úvod

Modulární aritmetika je aritmetikou na množině celých čísel $\mathbb{Z}$ v níž se čísla opakují po dosažení určité hodnoty n, již nazýváme **modul**.

Na rozdíl od běžných celočíselných operací se zde po každé operaci provede ještě *celočíselné dělení* modulem n a výsledkem operace je *zbytek* po tomto dělení.

Příklad

V modulární aritmetice modulo 7 mají operace $2 \cdot 4$ a $70 + 1$ shodné reprezentace, protože $8 \bmod 7 = 1$ a zároveň $71 \bmod 7 = 1$.

Celočíselná aritmetika v počítačích je modulární.

Příklad pro osmibitová čísla

250+10 je v osmibitové aritmetice rovno 4 (tedy $260 \bmod 2^8$). 12-16 je v osmibitové aritmetice rovno 252 (což je $-4 \bmod 2^8$).

Praktické aplikace modulární aritmetiky:

- **přenos zpráv** – ochrana zpráv proti chybám, komprese, zajištění integrity, utajování,
- **výpočetní technika** – hašovací funkce, pseudonáhodná čísla, dvojková komplementární reprezentace celých čísel, aritmetika s VELKÝMI celými čísly.

2 Dělitelnost a kongruence

2.1 Dělitelnost

Připomenutí

Na množině celých čísel $\mathbb{Z}$ mějme definována dvě čísla: a, b. Říkáme, že a **dělí** b, pokud existuje libovolné $c \in \mathbb{Z}$ takové, že $b = ac$.

Pro zkrácený zápis toho vztahu používáme symbol $a|b$.

Pro **společný dělitel** c čísel a a b platí, že $c|a$ a zároveň $c|b$.

Největší společný dělitel

Číslo d označujeme jako **největšího společného dělitele** čísel a a b a zapisujeme $d = \gcd(a, b)$, pokud platí, že

- číslo d je společný dělitel a a b, a
- pokud existuje $c \neq d$ takové, že $c|a$ a zároveň $c|b$, pak také $c|d$.

Číslo $\gcd(a, b)$ je tedy největším kladným celým číslem jež dělí jak a, tak i b, s výjimkou $\gcd(0, 0) = 0$.

2.2 Kongruence

Uvažujme libovolný modul n takový, že $n \in \mathbb{N}$ a zvolme si dvě celá čísla $a, b \in \mathbb{Z}$.

Pokud v modulární aritmetice platí, že $a \bmod n$ a $b \bmod n$ jsou si rovny (mají stejný zbytek po dělení n), říkáme, že že *a je kongruentní s b modulo n* a zapisujeme

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

Příklad

Je tedy $8 \equiv 71 \,(\mathrm{mod}\, 7)$, 8 je kongruentní s 71 modulo 7.

Pozor na záporná čísla: $-1 \equiv 6 \,(\mathrm{mod}\, 7)$.

Označme si m onen zbytek po dělení $a \bmod n$ a $b \bmod n$. Bude potom platit, že

$$a = i \cdot n + m$$
$$b = j \cdot n + m$$

pro nějaká $i, j \in \mathbb{Z}$. V příkladu, uvedeném výše, je

$$8 = 1 \cdot 7 + 1$$
$$71 = 10 \cdot 7 + 1$$
$$-6 = -1 \cdot 7 + 1.$$

Příklad

Mějme abecedu velkých písmen české abecedy, $\{\mathsf{A}, \mathsf{Á}, \mathsf{B}, \ldots, \mathsf{Z}, \mathsf{Ž}\}$, reprezentovanou numerickými hodnotami $\{0, 1, \ldots, 41\}$. Nad touto abecedou provádíme všechny matematické operace modulárně, s modulem 42.

V takové modulární aritmetice jsou si rovny například reprezentace celých čísel -41, 43 a 320328919, protože zbytek po dělení 42 je vždy 1:

$$-41 \equiv 43 \,(\mathrm{mod}\ \ 42) \Leftrightarrow -41 = 43 + 42 \cdot (-2),$$
$$-41 \equiv 320328919 \,(\mathrm{mod}\ \ 42) \Leftrightarrow -41 = 320328919 + 42 \cdot (-7626880),$$
$$320328919 \equiv 43 \,(\mathrm{mod}\ \ 42) \Leftrightarrow 320328919 = 43 + 42 \cdot 7626878.$$

Znak A může tedy reprezentovat libovolné z čísel -41, 43 a 320328919.

Třída kongruence

Množinu všech celých čísel, která jsou kongruentní s nějakým m modulo n je zvykem nazývat **třída kongruence** a zapisovat ji $\overline{m}$, bez uvedení modulu kongruence nebo $[m]_n$.

Příklad

Například číslo 3 v modulu 5 může zastupovat i všechna čísla s ním kongruentní $(\dots, -7, -2, 3, 8, 13, \dots)$. V textech bude tato třída kongruence označována jako $[3]_5$ nebo jako $\overline{3}$.

Vlastnosti kongruence modulo n umožňují počítat pouze se zbytky po dělení tímto modulem a výsledek pak zobecnit na všechna čísla.

3 Vlastnosti čísel v modulární aritmetice

Modulární aritmetika je uzavřená vůči operacím sčítání a násobení:

$$\begin{aligned}[a]_n + [b]_n &= [a+b]_n,\\ [a]_n - [b]_n &= [a-b]_n,\\ [a]_n \cdot [b]_n &= [a \cdot b]_n,\end{aligned}$$

Příklad

V aritmetice modulo 7 by mělo platit $[2]_7 + [6]_7 = [1]_7$. Pro $9 \in \overline{2}$ a $-1 \in \overline{6}$ je výsledek $9 - 1 = 8 \in \overline{1}$.

Dokázat to můžeme jednoduše prostým sečtením reprezentací čísel:

$$\begin{aligned}a + b &= i \cdot n + m + j \cdot n + m =\\ &= (i+j) \cdot n + 2m\end{aligned}$$

a protože $2m = k \cdot n + o$ bude celkový součet $(i + j + k) \cdot n + o$

Podobně zkuste v aritmetice modulo 7 ověřit $\overline{2} \cdot \overline{6} = \overline{5}$.

Sčítání a násobení v modulární aritmetice je komutativní a asociativní:

$$\begin{aligned}\overline{a} + \overline{b} &= \overline{b} + \overline{a},\\ \overline{a} \cdot \overline{b} &= \overline{b} \cdot \overline{a},\\ \left(\overline{a} + \overline{b}\right) + \overline{c} &= \overline{a} + \left(\overline{b} + \overline{c}\right),\\ \left(\overline{a} \cdot \overline{b}\right) \cdot \overline{c} &= \overline{a} \cdot \left(\overline{b} \cdot \overline{c}\right).\end{aligned}$$

Pro sčítání a násobení v modulární aritmetice existuje identita, pro sčítání i inverze:

$$\begin{aligned}\overline{0} + \overline{a} &= \overline{a},\\ \overline{a} + \overline{-a} &= \overline{0},\\ \overline{1} \cdot \overline{a} &= \overline{a}.\end{aligned}$$

Příklady

V modulární aritmetice modulo 7 je $28 \in \overline{0}$ a $15 \in \overline{1}$. Pro jejich součet platí $(28+15) \bmod 7 = 43 \bmod 7 = 1$.[0.2ex] V modulární aritmetice modulo 3 je $10 \in \overline{1}$ a $8 \in \overline{2}$. Pro jejich součin platí $(10 \cdot 8) \bmod 3 = 80 \bmod 3 = 2$.

Jak dopadne součet 57 a -73 v aritmetice modulo 8?

Modulární dělení (redukce)

Pokud

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

obecně neplatí, že také

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

Jsou dvě varianty

1. Pro d a n nesoudělná je opravdu $a \cdot d \equiv b \cdot d \,(\mathrm{mod}\, n)$.
2. Pro $d \neq 0$ je $a \cdot d \equiv b \cdot d \,(\mathrm{mod}\, n \cdot d)$.

Příklad

Čísla 15 a 50 patří do stejné třídy kongruence modulo 7. Chceme-li zapsanou kongruenci redukovat na nižší hodnoty členů té samé třídy kongurence, dostáváme

$$\begin{aligned} 15 &\equiv 50 \,(\mathrm{mod}\, 7) \\ 3 \cdot 5 &\equiv 10 \cdot 5 \,(\mathrm{mod}\, 7) \\ 3 &\equiv 10 \,(\mathrm{mod}\, 7) \end{aligned}$$

protože $d = 5$, $n = 7$ a jde o nesoudělná čísla. Oproti tomu

$$\begin{aligned} 15 &\equiv 35 \,(\mathrm{mod}\, 10) \\ 3 \cdot 5 &\equiv 7 \cdot 5 \,(\mathrm{mod}\, 10) \\ 3 &\not\equiv 7 \,(\mathrm{mod}\, 10) \end{aligned}$$

nevychází, protože $d = 5$, $n = 10 = 2 \cdot 5$ jsou čísla soudělná. Správně bude

$$\begin{aligned} 15 &\equiv 35 \,(\mathrm{mod}\, 10) \\ 3 \cdot 5 &\equiv 7 \cdot 5 \,(\mathrm{mod}\, 2 \cdot 5) \\ 3 &\equiv 7 \,(\mathrm{mod}\, 2). \end{aligned}$$

Modulární dělení pro d a n nesoudělná

Pro $170 \equiv 35 \,(\mathrm{mod}\, 3) \longrightarrow 5 \cdot 34 \equiv 5 \cdot 7 \,(\mathrm{mod}\, 3)$ je $34 \equiv 7 \,(\mathrm{mod}\, 3)$, protože 3 a 5 jsou nesoudělná čísla.

Modulární dělení pro obecné $d \neq 0$

Z kongruence $10 \equiv 6 \,(\mathrm{mod}\, 4) \longrightarrow 5 \cdot 2 \equiv 3 \cdot 2 \,(\mathrm{mod}\, 2 \cdot 2)$ plyne $5 \equiv 3 \,(\mathrm{mod}\, 2)$.

Co vyjde pro $10 \equiv 6 \,(\mathrm{mod}\, 3)$?

Stále nám ovšem chybí aparát, s jehož pomocí bychom mohli hledat řešení x kongruencí typu

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

4 Malá Fermatova věta

Pro $a \in \mathbb{Z}$ a prvočíslo $p \in \mathbb{N}$ takové, že $p \nmid a$ platí

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

a v alternativním tvaru

$$a^{p} \equiv a \,(\mathrm{mod}\, p)$$

Ve skutečnosti je $a^{\phi(p)} \equiv 1 (\mathrm{mod}\, p)$, kde $\phi(p)$ je takzvaná **Eulerova funkce**.

Malá Fermatova věta je základním stavebním kamenem algoritmu generování šifrovacího klíče asymetrické šifry RSA. Je také nutnou podmínkou pro prvočísla.

Osvěžte si, co je to nutná a postačující podmínka pro dvě tvrzení.

Pro $a \in \mathbb{Z}$ a $n \in \mathbb{N}$ je celé číslo x **multiplikativní inverzí**, pokud splňuje podmínku

$$a \cdot x \equiv 1 \,(\mathrm{mod}\ n). \tag{1}$$

Pro **nejmenší multiplikativní inverzi** platí, že x je nejmenší možnou kladnou multiplikativní inverzí k a a označujeme ji a^{-1}.

Z Malé Fermatovy věty přitom plyne, že

$$a^{-1} \equiv a^{p-2} \,(\mathrm{mod}\ p). \tag{2}$$

pro $a \in \mathbb{Z}$ a prvočíselná $p \in \mathbb{N}$ taková, že $p \nmid a$.

Výpočet inverze

Chceme spočítat a^{-1} pro $n = 11$ a $a = -3$. Volíme postupně $x = 1, 2, \ldots$, první kladné číslo x splňující vztah (1) je $x = 7$: $-3 \cdot 7 \equiv 1 \,(\mathrm{mod}\ 11)$.

Výpočet inverze pomocí Malé Fermatovy věty

Použitím Malé Fermatovy věty (2) máme $a^{-1} \equiv (-3)^{11-2} \,(\mathrm{mod}\ 11)$, tedy $a^{-1} \equiv -19683 \,(\mathrm{mod}\ 11)$ což je to samé, jako $a^{-1} \equiv 7 \,(\mathrm{mod}\ 11)$ protože jde o stejnou třídu kongruence.

Zkuste si to nyní sami pro $n = 7$ a $a = 5$.

4.1 Opice a kokosy

Na pustém ostrově ztroskotají tři námořníci. Jediná potrava, kterou během dne našli, je hromada kokosových ořechů.

V noci se první námořník probudí, spravedlivě rozdělí hromadu na tři díly, přičemž jeden kokos zbyde – ten dostane opice. Svou třetinu námořník ukryje, zbytek navrší zpátky a jde zase spát. Postupně hromadu stejným způsobem „třetina pro mne, jeden kokos opici, zbytek vrátit“ zmenší jeho oba druhové.

Ráno si hromadu rozdělí na třetiny, opět zbyde jeden kokos, ten dostane opice.

Kolik musí být v původní hromadě kokosů, aby to fungovalo?

První námořník začíná s hromadou obsahující $n \equiv 1 \,(\mathrm{mod}\, 3)$ kokosových ořechů.

Druhý námořník dělil hromadu s

$$m_1 = \frac{2(n-1)}{3} \equiv 1 \,(\mathrm{mod}\, 3)$$

ořechy, třetí námořník přerozděloval

$$m_2 = \frac{2(m_1-1)}{3} \equiv 1 \,(\mathrm{mod}\, 3)$$

ořechů a ve zbylé hromadě jich muselo zůstat

$$m_3 = \frac{2(m_2-1)}{3} \equiv 1 \,(\mathrm{mod}\, 3).$$

Hodnotu m_3 spočteme jako

$$m_3 = \frac{2}{3}m_2 - \frac{2}{3} = \cdots = \frac{8}{27}n - \frac{38}{27} = k \cdot 3 + 1$$

což po vynásobení pravé části 27 upravíme na

$$8n - 38 = k \cdot 81 + 27,$$
$$8n - 38 \equiv 27 \,(\mathrm{mod}\, 81),$$

a v modulární aritmetice řešíme pro n kongruenci

$$8n - 38 \equiv 27 \,(\mathrm{mod}\, 81) \Leftrightarrow 8n \equiv 65 \,(\mathrm{mod}\, 81).$$

Dělit osmi nemůžeme, můžeme ale násobit multiplikativní inverzí osmičky (pro jejíž výpočet nelze použít Fermatovu větu – proč?):

$$n \equiv 8^{-1} \cdot 65 \equiv 71 \cdot 65 \equiv 79 \,(\mathrm{mod}\, 81).$$

Nejmenší počet kokosů v hromadě je tedy 79 (ale může být i 160, 241, ...).

Poznámka k výpočtu 8^{-1}:
Protože 8 a 81 jsou nesoudělná čísla, můžeme $x \equiv 8^{-1} \,(\mathrm{mod}\, 81)$ spočítat rozšířeným Euklidovým algoritmem takto:

$$\begin{aligned} 0 \cdot 8 + 1 \cdot 81 &= 81 \\ 1 \cdot 8 + 0 \cdot 81 &= 8 \ldots 81 = \boxed{10} \cdot 8 + 1 \\ -10 \cdot 8 + 1 \cdot 81 &= 1 \end{aligned}$$

a protože $-10 \equiv 71 \,(\mathrm{mod}\, 81)$, je $8 \cdot 71 \equiv 1 \,(\mathrm{mod}\, 81)$. Vzhledem k tomu, že $-80 = (-1) \cdot 80 + 1$, možná to někoho napadlo už rovnou.

Poznámka k výpočtu $71 \cdot 65 \,(\mathrm{mod}\, 81)$:
Stačí, abyste si spočetli (na kalkulačce nebo ručně) $4615/81 = 56{,}9573\ldots$ a z toho $4615 - 56 \cdot 81 = 4615 - 4536 = 79$.

5 Příklady

5.1 Kontrolní součty

ISBN Neboli *International Standard Book Number*

Má ho každá kniha, identifikuje zemi či region původu, nakladatele a vydání. Existuje ve verzi ISBN-10 a ISBN-13. Na poslední pozici každého ISBN je *kontrolní cifra*.

Příklad výpočtu kontrolní cifry ISBN-10

Mějme ISBN 0-552-13105-9. Kontrolní cifra ISBN-10 se počítá v modulu 11, pro případ zbytku 10 se použije znak X. Kontrolní součet je $0{\cdot}10{+}5{\cdot}9{+}5{\cdot}8{+}2{\cdot}7{+}1{\cdot}6{+}3{\cdot}5{+}1{\cdot}4{+}0{\cdot}3{+}5{\cdot}2{+}9{\cdot}1 = 143 \bmod 11 = 9$. Uvedené ISBN je opravdu platné.

Což takhle 80-85609-70-3?

ISBN-13 je varianta ISBN unifikovaná s EAN-13 (čárový kód), používá trošku jiné váhy a kontrolní číslici počítá mod 10.

Rodné číslo Varianta po roce 1954

Jednoznačný identifikátor občanů ČR a SR obsahující údaj o datumu narození, pohlaví a do roku 2004 i lokalitě porodnice.

Příklad výpočtu kontrolní cifry

Muž narozen 22. února 1959, rozlišující trojčíslí 177 (Zlín?). Poslední cifra rodného čísla zajišťuje dělitelnost celého čísla jedenácti, musí mít proto hodnotu $590222177 \bmod 11 = 6$. Odpovídající rodné číslo má tvar 590222/1776.

O kohopak asi jde?

Pokud uvažujete, jak je možné zajistit dělitelost jedenácti přidáním zbytku po dělení k původnímu číslu, uvědomte si, že pro původní rodné číslo k bez kontrolní cifry platí $k = 11i + m$, kde m je kontrolní číslice. Rozšířené rodné číslo má tvar $10k + m = 10 \cdot (11i + m) + m = 11 \cdot 10i + 10m + m = 11 \cdot (10i + 1)$ a je tedy opravdu dělitelné jedenácti beze zbytku.

Pokud by při operaci modulo vyšel zbytek deset, psala se u RČ místo kontrolní číslice nula a kontrolní součet neplatil. V dnešní době se ale taková čísla nepřidělují.

5.2 Pseudonáhodná čísla

Generátory pseudonáhodných čísel Matematické přiblížení k $U(0, 1)$

Jednou z možností je **lineární kongruentní generátor** *(LCG, Linear Congruence Generator).*

Jak funguje LCG

Uživatel zvolí x_0 (pevné nebo třeba odvozené od aktuálního času). Potom $x_{k+1} = (a \cdot x_k + b) \bmod m$, kde a, b a m jsou zvolené parametry určující kvality generátoru. Jedna z možných voleb je třeba $a = 1664525$, $b = 1013904223$ a $m = 2^{32}$.

LCG jsou *velmi citlivé na volby parametrů.* Pokud dodržíme jisté předpoklady, generátor pracuje s periodou m, ale i to je v mnoha případech statistických výpočtů (například u vícerozměrné Monte Carlo integrace) žalostně málo.

5.3 Aritmetika velkých čísel

Aritmetika velkých čísel Co s čísly, která počítač nedokáže reprezentovat?

Registry v dnešních procesorech jsou většinou 32 nebo 64 bitové:

- největší binární číslo, s nímž počítač dokáže *pohodlně* pracovat, je tedy 2^{32} respektive 2^{64},
- největší binární číslo, jež můžeme reprezentovat v 1GB operační paměti, je $2^{1099511627776}$ ... jak rychle s ním ale budeme schopni počítat?

Jak se ale algoritmy typu RSA efektivně vypořádávají se sčítáním či násobením celých čísel v aritmetice velkých modulů (třeba 340282366920938463463374607431768211507)? Jak provádět operace s třídami čísel, která se do paměti počítače prostě nevejdou?