Příklady na modulární aritmetiku
Čínská věta o zbytcích

Matematické algoritmy (K611MA)

Jan Přikryl, Miroslav Vlček

Ústav aplikované matematiky
Fakulta dopravní ČVUT

5. přednáška K611MA
čtvrtek 8. listopadu 2007

Obsah přednášky

O čem to vlastně všechno je
Krátká motivační vložka

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 čísla 8 a 71 shodné reprezentace, protože $8 \bmod 7 = 1$ a zároveň $71 \bmod 7 = 1$.

K čemu to vlastně všechno je

Krátká motivační vložka

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.

Kongruence
Připomenutí

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 a b jsou kongruentní modulo n a zapisujeme

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

Příklad

Je tedy $8 \equiv 71 \pmod{7}$, 8 je kongruentní s 71 modulo 7.

Pozor na záporná čísla: $-1 \equiv 7 \pmod{8}$.

Kongruence
Příklady

Mějme abecedu velkých písmen české abecedy, $\{\mathrm{A}, \acute{\mathrm{A}}, \mathrm{B}, \ldots, \mathrm{Z}, \check{\mathrm{Z}}\}$, reprezentovanou numerickými hodnotami $\{1, 2, \ldots, 42\}$. 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:

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

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

Kongruence
Příklady

Množinu všech celých čísel, která jsou kongruentní s nějakým m modulo n je zvykem nazývat **zbytková třída** a zapisovat ji $\overline{m}$, bez uvedení modulu kongruence (v anglosaské literatuře), resp. $[m]_n$ v české literatuře.

Příklad

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

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

Obsah přednášky

Definice

Pierre de Fermat, 1640

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.

Multiplikativní inverze

Definice

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

$$a \cdot x \equiv 1 \pmod{n}. \tag{1}$$

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

$$a^{-1} \equiv a^{p-2} \pmod{p}. \tag{2}$$

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

Multiplikativní inverze
Příklad

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 $x = 7$: $-3 \cdot 7 \equiv 1 \pmod{11}$.

Výpočet inverze pomocí Malé Fermatovy věty

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

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

Tři námořníci, opice a kokosy

Problém

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?

Tři námořníci, opice a kokosy

Řešení (1)

První námořník začíná s hromadou obsahující $n \equiv 1 \pmod 3$ kokosových ořechů.

Druhý námořník dělil hromadu s

$$m_1 = \frac{2(n-1)}{3} \equiv 1 \pmod 3$$

ořechy, třetí námořník přerozděloval

$$m_2 = \frac{2(m_1-1)}{3} \equiv 1 \pmod 3$$

ořechů a ve zbylé hromadě jich muselo zůstat

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

Tři námořníci, opice a kokosy

Řešení (2)

Hodnotu m_3 spočteme jako

$$m_3 = \frac{2}{3}m_2 - \frac{2}{3} = \cdots = \frac{8}{27}n - \frac{38}{27} \equiv 1 \pmod 3$$

a rovnici v modulární aritmetice řešíme pro n

$$8n - 38 \equiv 27 \pmod{81} \Rightarrow 8n \equiv 65 \pmod{81}.$$

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

$$n \equiv 8^{-1} \cdot 65 \equiv 71 \cdot 65 \equiv 79 \pmod{81}.$$

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

Obsah přednášky

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?

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. Je beze zbytku dělitelné jedenácti.

Příklad výpočtu kontrolní cifry

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

O kohopak asi jde?

Poznámka: Rozlišující trojčíslí, pro něž by vyšel zbytek po dělení roven 10, se dnes nepoužívají.

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.

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?

Obsah přednášky

Čínská věta o zbytcích
(Chinese Reminder Theorem, CRT)

Více vzájemně ekvivalentních tvrzení z algebry a teorie čísel.
Nejstarší zmínka z Číny ve 3. století našeho letopočtu.

Motivace: Jak najít x takové, že

$$\begin{aligned} x &\equiv 2 \,(\mathrm{mod}\, 3), \\ x &\equiv 3 \,(\mathrm{mod}\, 5), \\ x &\equiv 2 \,(\mathrm{mod}\, 7)? \end{aligned}$$

Čínská věta o zbytcích

Postup řešení (1/2)

Zbytkové třídy jsou $[2]_3$, $[3]_5$ a $[2]_7$.

V prvním kroku hledáme nulové a jednotkové zbytkové třídy pro kombinace původních modulů. V našem případě platí

$$\begin{aligned} 70 &\equiv 0 \,(\mathrm{mod}\, 5 \cdot 7) \quad \wedge \quad 70 \equiv 1 \,(\mathrm{mod}\, 3), \\ 21 &\equiv 0 \,(\mathrm{mod}\, 3 \cdot 7) \quad \wedge \quad 21 \equiv 1 \,(\mathrm{mod}\, 5), \\ 15 &\equiv 0 \,(\mathrm{mod}\, 3 \cdot 5) \quad \wedge \quad 15 \equiv 1 \,(\mathrm{mod}\, 7). \end{aligned}$$

Čínská věta o zbytcích

Postup řešení (2/2)

Řešením dané soustavy kongruencí je v takovém případě číslo

$$\hat{x} = 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233.$$

Minimální hodnota x je dána třídou kongruence modulo $3 \cdot 5 \cdot 7 = 105$, tedy

$$x = 233 \bmod 105 = 23.$$

Čínská věta o zbytcích

Vlastní tvrzení

Nechť $n_1, n_2, \ldots, m_k$ jsou navzájem nesoudělná přirozená čísla, $n_i \geq 2$ pro všechna $i = 1, \ldots, k$. Potom řešení soustavy rovnic

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

existuje a je určeno jednoznačně v modulo $n = n_1 \cdot n_2 \cdot \ldots \cdot m_k$.

Jak si Sun Tzu ušetří práci

Lehký náznak důkazu

Díky nesoudělnosti existuje ve třídě operací modulo n_i ke každému $N_i = n/n_i$ jeho multiplikativní inverze M_i, tedy

$$M_i \cdot N_i \equiv 1 \pmod{n_i}$$

a platí

$$x = \sum_{i=1}^{k} a_i M_i N_i.$$

Ve výše uvedeném případě se zbytkovými třídami $[2]_3$, $[3]_5$ a $[2]_7$ je

$$x = 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 233.$$

Praktický význam věty

Výpočty modulo velké M lze převést na výpočty modulo menší součinitelé čísla M – zrychlení výpočtu.

Lze generalizovat pro soudělná čísla.

Význam hlavně v šifrovacích systémech.

Problém nůše s vejci

Ilustrace použití CRT

V nůši je n vajec. Pokud z ní odebíráme vejce po dvou, třech a pěti najednou, v nůši nakonec zůstane 1, 2, respektive 4 vejce. Pokud odebíráme vejce po sedmi kusech, v nůši nakonec nezůstane vejce žádné.

Jaká je nejmenší hodnota n pro niž může uvedená situace nastat?

Problém nůše s vejci

Ilustrace použití CRT

Zbytkové třídy jsou $[1]_2$, $[2]_3$, $[4]_5$ a $[0]_7$.

V příštím díle uvidíte

Jak se *Čínskou větu o zbytcích* počítají v modulární aritmetice zbytky po dělení velkých čísel.

A podíváme se, jak se tento postup využívá v asymetrické šifře RSA.