

# Modulární aritmetika, Malá Fermatova věta.

Matematické algoritmy (11MAG)

Jan Příkryl

Ústav aplikované matematiky  
ČVUT v Praze, Fakulta dopravní

3. přednáška 11MAG  
pondělí 14. října 2013

verze: 2013-10-22 14:28



# Obsah přednášky

- 1 Dělitelnost
- 2 Modulární aritmetika
- 3 Malá Fermatova věta
- 4 Příklady
- 5 Závěr



# 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  $a \mid b$ .

V případě, že  $a \nmid b$ , dělíme se zbytkem: platí

$$b = q \cdot a + r,$$

kde  $q \in \mathbb{Z}$  a  $r \in \mathbb{N}$  je zbytek po dělení.



# Dělitelnost

## Příklady

### Příklad

Pro čísla 7 a 8 platí  $8 = 1 \cdot 7 + 1$ , tedy  $7 \nmid 8$ . Zbytek po dělení je 1.

Pro čísla 7 a 71 platí  $8 = 10 \cdot 7 + 1$ , tedy  $7 \nmid 71$ . Zbytek po dělení je opět 1.

### Příklad (Dělitelnost záporných čísel)

Pro čísla 7 a 8 platí  $8 = 1 \cdot 7 + 1$ , tedy  $7 \nmid 8$ . Zbytek po dělení je 1.

Pro čísla 7 a -8 platí  $-8 = -2 \cdot 7 + 6$ , tedy  $7 \nmid -8$ . Zbytek po dělení je ovšem **6!**



# Dělitelnost

## Největší společný dělitel

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

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 nějaké  $c \neq d$  takové, že  $c \mid a$  a zároveň  $c \mid b$ , pak také  $c \mid d$ .

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



# Operace modulo

Elegantní vyjádření pro zbytek po dělení

Připomeňme, že pro  $a, b, q \in \mathbb{Z}$  a  $r \in \mathbb{N}$  platí

$$b = q \cdot a + r.$$

## Definice

Zbytek po dělení dvou čísel označíme **modulo**, zapisujeme  $b \bmod a$ . Platí

$$b = q \cdot a + r \Leftrightarrow r = b \bmod a.$$

## Příklad

Je  $23 \bmod 4 = 3$ , neboť  $23 = 5 \cdot 4 + 3$ .



# Bézoutova rovnost

## Zajímavé pozorování

Pozorujeme-li mezivýsledky jednotlivých kroků Eulerova algoritmu, nahlédneme, že jde vždy o lineární kombinace čísel  $a$  a  $b$  s celočíselnými koeficienty. To vede k následujícímu pozorování.

### Definice (Bézoutova rovnost)

Nejvyšší společný dělitel celých čísel  $a$  a  $b$  lze vyjádřit jako

$$a \cdot x + b \cdot y = \gcd(a, b),$$

kde  $x, y \in \mathbb{Z}$ .

Hodnoty  $x$  a  $y$  lze spočítat **rozšířeným Eukleidovým algoritmem**.



# Rozšířený Eukleidův algoritmus

**Require:**  $a, b \in \mathbb{Z}$

**Ensure:**  $\gcd(a, b), x, y$

$a_x \leftarrow 1; a_y \leftarrow 0;$

$b_x \leftarrow 0; b_y \leftarrow 1;$

**repeat**

$m \leftarrow b \operatorname{div} a$

$b \leftarrow b - m \cdot a$

$b_x \leftarrow b_x - m \cdot a_x$

$b_y \leftarrow b_y - m \cdot a_y$

$a \iff b; a_x \iff b_x; a_y \iff b_y;$

**until**  $a = 0$

**return**  $b, b_x, b_y$





# Obsah přednášky

① Dělitelnost

② Modulární aritmetika

Kongruence

Vlastnosti čísel v modulární aritmetice

③ Malá Fermatova věta

④ Příklady

⑤ Závěr



# Modulární aritmetika

O čem to vlastně všechno je

**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 (Aritmetika osmibitových čísel)

$250+10$  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

## Definice

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

### Definice

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

## Příklad

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

$$-41 \equiv 43 \pmod{42} \Leftrightarrow -41 = 43 + 42 \cdot (-2),$$

$$-41 \equiv 320328919 \pmod{42} \Leftrightarrow -41 = 320328919 + 42 \cdot (-7626880),$$

$$320328919 \equiv 43 \pmod{42} \Leftrightarrow 320328919 = 43 + 42 \cdot 7626878.$$

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



# Kongruence

## 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.



# Vlastnosti modulární aritmetiky

## Uzavření

Modulární aritmetika je uzavřená vůči operacím sčítání a násobení:

$$[a]_n + [b]_n = [a + b]_n,$$

$$[a]_n - [b]_n = [a - b]_n,$$

$$[a]_n \cdot [b]_n = [a \cdot b]_n.$$

### Příklad

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

Podobně zkuste v aritmetice modulo 7 ověřit  $[2]_7 \cdot [6]_7 = [5]_7$ .



# Vlastnosti modulární aritmetiky

## Komutativita a asociativita

Sčítání a násobení v modulární aritmetice je komutativní a asociativní:

$$[a]_n + [b]_n = [b]_n + [a]_n,$$

$$[a]_n \cdot [b]_n = [b]_n \cdot [a]_n,$$

$$([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n),$$

$$([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n).$$





# Vlastnosti modulární aritmetiky

## Komutativita

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

$$[0]_n + [a]_n = [a]_n,$$

$$[a]_n + [-a]_n = [0]_n,$$

$$[1]_n \cdot [a]_n = [a]_n.$$

### Příklad (Dva příklady)

V modulární aritmetice modulo 7 je  $28 \in [0]_n$  a  $15 \in [1]_n$ . Pro jejich součet platí  $(28 + 15) \bmod 7 = 43 \bmod 7 = 1$ .

V modulární aritmetice modulo 3 je  $10 \in [1]_n$  a  $8 \in [2]_n$ . Pro jejich součin platí  $(10 \cdot 8) \bmod 3 = 80 \bmod 3 = 2$ .

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



# Vlastnosti modulární aritmetiky

## Modulární krácení

Pokud

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

obecně neplatí, že také

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

Jsou dvě varianty

- 1 Pro  $\gcd(d, n) = 1$  je opravdu  $a \equiv b \pmod{n}$ .
- 2 Pro  $\gcd(d, n) = k, k > 1$  je  $d = k \cdot x$  a  $n = k \cdot y$  a kongruence se postupně změní na

$$akx \equiv b kx \pmod{ky}$$

$$ax \equiv bx \pmod{y}$$

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



# Vlastnosti modulární aritmetiky

## Příklady na modulární krácení

**Příklad (Modulární krácení pro  $d$  a  $n$  nesoudělná)**

Pro  $170 \equiv 35 \pmod{3} \rightarrow 5 \cdot 34 \equiv 5 \cdot 7 \pmod{3}$  je  
 $34 \equiv 7 \pmod{3}$ , protože 3 a 5 jsou nesoudělná čísla.

**Příklad (Modulární krácení pro obecné  $d \neq 0$ )**

Z kongruence  $10 \equiv 6 \pmod{4} \rightarrow 5 \cdot 2 \equiv 3 \cdot 2 \pmod{2 \cdot 2}$  plyne  
 $5 \equiv 3 \pmod{2}$ .

Co vyjde pro  $10 \equiv 6 \pmod{3}$  ?



# Multiplikativní inverze

## Definice

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

$$a \cdot x \equiv 1 \pmod{n}. \quad (1)$$

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



# Obsah přednášky

- 1 Dělitelnost
- 2 Modulární aritmetika
- 3 Malá Fermatova věta**
- 4 Příklady
- 5 Závěr



# Definice

Pierre de Fermat, 1640

## Definice

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

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{resp.} \quad a^p \equiv a \pmod{p}$$

Malá Fermatova věta je základním stavebním kamenem šifry RSA. Je také nutnou podmínkou pro prvočísla a základním kamenem **Fermatova testu prvočíselnosti**.

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

### Příklad (Výpočet inverze)

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

### Příklad (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  $a = 5$ .



# Obsah přednášky

## 1 Dělitelnost

## 2 Modulární aritmetika

## 3 Malá Fermatova věta

## 4 Příklady

Opice a kokosy

Kontrolní součty

Čísla bankovních účtů

Rodné číslo

Pseudonáhodná čísla

Aritmetika velkých čísel





# 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 dělí 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

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

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, ...).



# 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 (Výpočet 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

$$0 \cdot 10 + 5 \cdot 9 + 5 \cdot 8 + 2 \cdot 7 + 1 \cdot 6 + 3 \cdot 5 + 1 \cdot 4 + 0 \cdot 3 + 5 \cdot 2 + 9 \cdot 1 = 143 \bmod 11 = 9. \text{ Uvedené ISBN je opravdu platné.}$$

Což takhle 80-85609-70-3?



# Čísla bankovních účtů

Jak odhalit jednoduché překlepy

Číslo bankovního účtu v ČR má tvar 123456-1234567890/1234, kde první a druhá část čísla účtu jsou chráněny proti překlepům opět algoritmem váženého ciferného součtu mod 11.

## Příklad (Kontrola čísla účtu)

Mějme číslo účtu 000019-2000145399/0800. Kontrolní součet první části je

$0 \cdot 10 + 0 \cdot 5 + 0 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 9 \cdot 1 = 11 \bmod 11 = 0$ . Kontrolní součet druhé části je

$2 \cdot 6 + 0 \cdot 3 + 0 \cdot 7 + 0 \cdot 9 + 1 \cdot 10 + 4 \cdot 5 + 5 \cdot 8 + 3 \cdot 4 + 9 \cdot 2 + 9 \cdot 1 = 121 \bmod 11 = 0$ .



# 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 (Výpočet kontrolní cifry)

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



# Generátory pseudonáhodných čísel

Matematické přiblížení k  $U(0, 1)$

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

## Příklad (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  $2^{109951162776}$  ... 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

- 1 Dělitelnost
- 2 Modulární aritmetika
- 3 Malá Fermatova věta
- 4 Příklady
- 5 Závěr**



# V příštím díle se můžete těšit na

Čínskou větu o zbytcích

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

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

