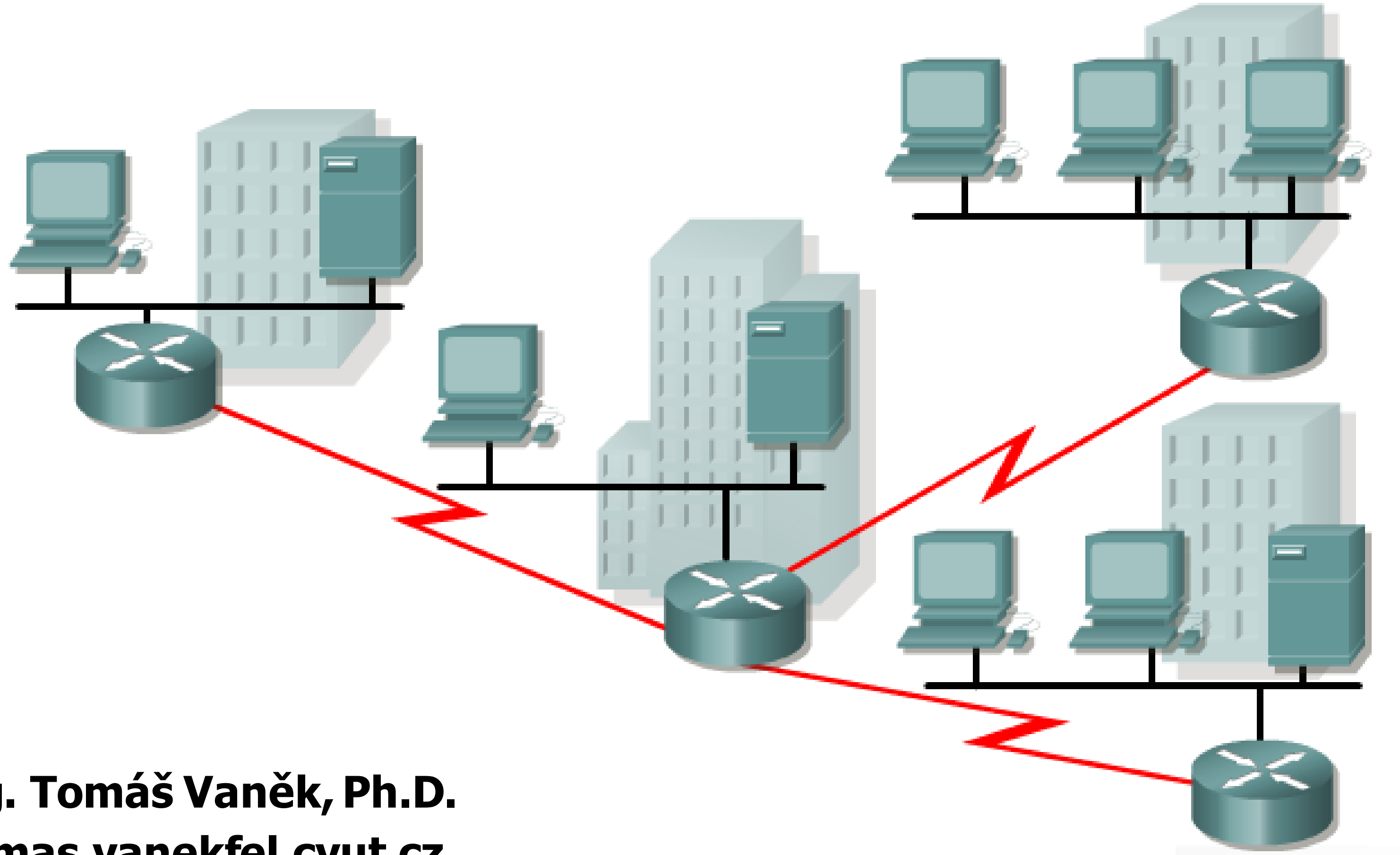
B2M32IBE - 2.cvičení



Ing. Tomáš Vaněk, Ph.D.
tomas.vanekfel.cvut.cz

Zakladatelé teorie čísel a algebry

Leonhard Euler (1707-1783)

http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Euler.html

Carl Friedrich Gauss (1777-1855)

http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html

GCD

GCD – (Greatest Common Divisor) – Největší společný dělitel

- značíme gcd(a,b)
- čísla *a* a *b* jsou nesoudělná (relativní prvočísla), pokud gcd(a,b)=1
- Speciální případy:
  - gcd (0, 0) = 0
  - gcd (a, 1) = 1
  - gcd (a, a) = |a|
- spočte se nejsnáze pomocí Euklidova algoritmu

Euklidův algoritmus

Algoritmus spočívá v opakovaném dělení dělitele zbytkem dokud zbytek není nula. Největší společný dělitel Je poslední nenulový zbytek v tomto algoritmu.
Výpočetní složitost Euklidova algoritmu je $O(\log^3 a)$

VSTUP: dvě nezáporná čísla *a* a *b*, taková, že a≥b,
VÝSTUP: největší společný dělitel čísel *a* a *b*

$$a = n*b+r$$

Pokud b≠0, provádíme následující operace:

1. Nahrazovat r←a mod b, a ← b ,b ← r
2. Získávat *a*

Výpočet GCD

Příklad: Výpočet GCD pomocí Euklidova algoritmu

$$\gcd(4864, 3458)$$

$$4864 = 1 \cdot 3458 + 1406$$

$$3458 = 2 \cdot 1406 + 646$$

$$1406 = 2 \cdot 646 + 114$$

$$646 = 5 \cdot 114 + 76$$

$$114 = 1 \cdot 76 + 38$$

$$76 = 2 \cdot 38 + 0$$

- v okamžiku, kdy r=0 výpočet končí
- gcd(4864,3548)=38

LCM

LCM – (Least Common Multiplier)

- nejmenší společný násobek čísel a,b
- značíme lcm(a,b)

$$lcm(a,b) = \frac{a \cdot b}{\mathrm{gcd}(a,b)}$$

Příklad: $\mathrm{lcm}(10,8) = \frac{10 \cdot 8}{\mathrm{gcd}(10,8)} = \frac{80}{2} = 40$

Identický a inverzní prvek

- Identický prvek

Nechť je dán prvek *a*, operace o. Identický prvek *X* je takový, pro který platí rovnice:

$$a \circ X = a$$

Příklad 1 – operace sčítání $a + 0 = a$

Příklad 2 – operace násobení $a \cdot 1 = a$

- Inverzní prvek

Nechť je dán prvek *a*, operace o. Inverzní prvek *Y* je takový, pro který platí rovnice:

$$a \circ Y = X$$

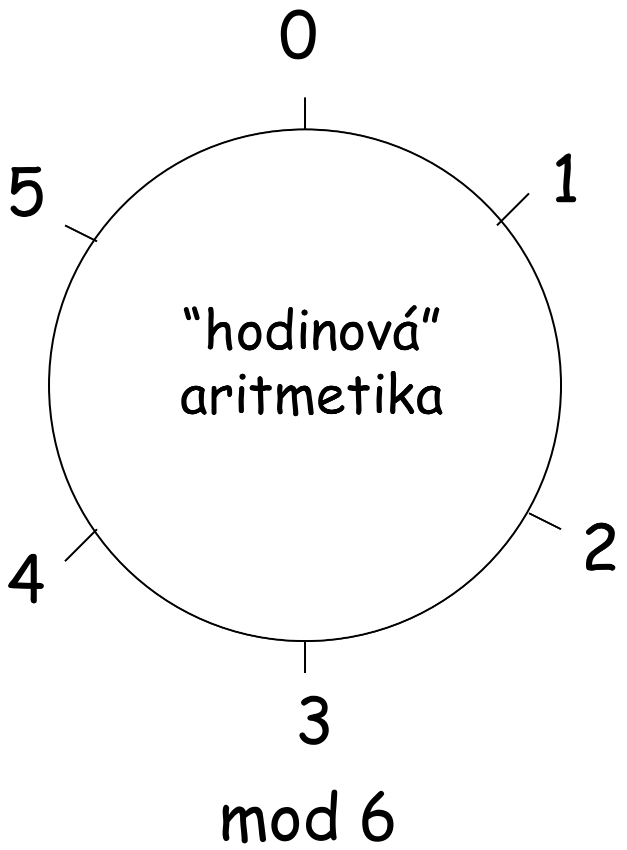
Příklad 1 – operace sčítání $a + (-a) = 0$

Příklad 2 – operace násobení $a \cdot (a^{-1}) = 1$

Modulární Aritmetika

- Pro čísla x a n, je x mod n zbytek po dělení x ÷ n

- Příklady
  - 7 mod 6 = 1
  - 33 mod 5 = 3
  - 33 mod 6 = 3
  - 51 mod 17 = 0
  - 17 mod 6 = 5



Modulární redukce

Pokud výsledek jakékoliv aritmetické operace v modulární aritmetice mod *n* leží mimo interval <0;n-1>, je třeba provést modulární redukci.

Modulární redukce spočívá v opakovaném odčítání (přičítání) hodnoty *n* k výsledku, tak dlouho dokud hodnota výsledku neleží v intervalu <0;n-1>.

Kongruence

– zavedl ho Gauss (18. století)

– značí se symbolem „≡“

– čísla $a,b \in Z$ jsou kongruentní (značíme $a \equiv b \pmod n$), pokud n beze zbytku dělí $(a-b)$

– Základní vlastnosti:

- reflexivnost – $a \equiv a \pmod n$
- symetričnost – pokud $a \equiv b \pmod n$, pak $b \equiv a \pmod n$
- tranzitivnost – pokud $a \equiv b \pmod n$ a pak $b \equiv c \pmod n$, pak $a \equiv c \pmod n$
- $((a \bmod n) + (b \bmod n)) \bmod n = (a + b) \bmod n$
- $((a \bmod n)(b \bmod n)) \bmod n = ab \bmod n$

Kongruence

Příklad:

48 ≡ 9 mod 13, protože 39 = 3·13 + 9 mod 13

48 ≡ 6 mod 14, protože 48 = 3·14 + 6 mod 14

15 ≡ 7 mod 8, protože 15 = 1 · 8 + 7 mod 8

Reziduum

- **zbytek po modulární redukci**
- **číslo v intervalu <0,*n-1*>**

Příklad:

52 mod 11 ≡ 8 mod 11

15 mod 9 ≡ 6 mod 15

-10 mod 6 ≡ 2 mod 6

Multiplikativní inverze

- Aditivní inverze čísla x mod n, zapsaná jako $-x$, je číslo které musíme přičíst k x abychom dostali výsledek 0 mod n

Příklad: 2 mod 6 ≡ 4 takže 2 + 4 ≡ 0 mod 6
2 je aditivní inverzí ke 4 (a naopak)

- Multiplikativní inverze čísla x mod n, zapsaná jako x^{-1}, je číslo, kterým musím vynásobit x abych dostal výsledek 1 mod n

Příklad: 3^{-1} mod 7 = 5 protože $3 \cdot 5 \equiv 1$ mod 7

- multiplikativní inverze a^{-1} mod b existuje pouze tehdy když a and b jsou nesoudělná

Příklad: neexistuje multiplikativní inverze 6^{-1} mod 10

- multiplikativní inverze a^{-1} mod b se snadno vypočítá (pokud existuje) pomocí malé Fermatovy věty

Multiplikativní inverze

Malá Fermatova věta

Je-li p prvočíslo a gcd(a,p)=1, pak $a^{p-1} \equiv 1 \pmod{p}$

Je-li p prvočíslo pak $a^{p} \equiv a \pmod{p}$

Je-li p prvočíslo a gcd(a,p)=1, pak $a^{p-2} \equiv a^{-1} \pmod{p}$

Příklad:

1) Určete multiplikativní inverzi 18 mod 31

$18^{29} \bmod 31 \equiv 19 \bmod 31$ $\quad$ $18 * 19 \bmod 31 \equiv 1 \bmod 31$

2) Spočtěte mocninu 4^{961} mod 479:

$4^{961} \equiv (4^{478})^2 * 4^5 \equiv 256 \bmod 479$, protože $4^{478} \equiv 1 \pmod{479}$

Základní operace v modulární aritmetice

Sčítání

- $3 + 5 \equiv 2 \bmod 6$
- $2 + 4 \equiv 0 \bmod 6$
- $3 + 3 \equiv 0 \bmod 6$
- $(7 + 12) \bmod 6 \equiv 19 \bmod 6 \equiv 1 \bmod 6$
- $(7 + 12) \bmod 6 \equiv (1 + 0) \bmod 6 \equiv 1 \bmod 6$

Odčítání

- je definováno jako sčítání pomocí aditivní inverze mod n

$$a - b \bmod n = a + (-b) \bmod n$$

Příklad:

- $8 - 5 \equiv 8+(-5) \equiv 3 \bmod 9$
- $5 - 8 \equiv 5+(-8) = -3 \equiv 6 \bmod 9$

Základní operace v mod *n*

Násobení

- výsledkem násobení může být nula i když žádný z činitelů není roven nule
- odvozeno z opakovaného sčítání

Příklad:

- $2 \cdot 4 \equiv 2 \pmod 6$
- $5 \cdot 5 \equiv 1 \pmod 6$
- $3 \cdot 4 \equiv 0 \pmod 6$
- $(7 \cdot 4) \bmod 6 \equiv 28 \bmod 6 \equiv 4 \bmod 6$
- $(7 \cdot 4) \bmod 6 \equiv (1 \cdot 4) \bmod 6 \equiv 4 \bmod 6$

Dělení

- je definováno jako násobení pomocí multiplikativní inverzí mod *n*

Příklad:

$$3 : 5 \bmod 7$$
$$\equiv$$
$$3 \cdot 5^{-1} \bmod 7$$
$$\equiv$$
$$3 \cdot 3 \bmod 7$$
$$\equiv$$
$$9 \bmod 7$$
$$\equiv$$
$$2 \bmod 7$$

Podíl dvou celých čísel v modulární aritmetice mod *n* je vždy celé číslo (v případě, že lze dělení provést)

Základní operace v mod *n*

Umocňování

- lze realizovat pomocí opakovaného násobení se složitostí O(n) (tzn. $n^5 = n \cdot n \cdot n \cdot n \cdot n$)
- efektivnější metoda je algoritmus „square and multiply“
- rekurzivní výpočet mocniny x^n pro celé kladné číslo *n*

$$Mocnina(x,n) = \begin{cases} x & pro\ n = 1 \\ Mocnina(x^2, \frac{n}{2}) & pro\ n\ sudé \\ x \cdot Mocnina(x^2, \frac{n-1}{2}) & pro\ n\ liché \end{cases}$$

- pro mocninu n vyžaduje pouze $O(\log_2 n)$ násobení

http://en.wikipedia.org/wiki/Square-and-multiply_algorithm

Čínská věta o zbytcích (CTR)

Jsou-li čísla $n_1, n_2, \dots, n_k$ párově nesoudělná, pak systém simultálních kongruencí

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

má jediné řešení modulo $n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

Řeší se tzv. Gaussovým algoritmem:

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

$$N_i = \frac{n}{n_i} \qquad M_i = N_i^{-1} \bmod n_i$$

Čínská věta o zbytcích (CTR)

Příklad: Pomocí CTR určete, pro jaké *n* platí, že číslo *x*

$$x \equiv 3 \bmod 4$$
$$x \equiv 5 \bmod 9$$
$$x \equiv 2 \bmod 5$$

$n=180$

$N_4 = 45 \quad M_4 = 45^{-1} \bmod 4 \equiv 1$

$N_9 = 20 \quad M_9 = 20^{-1} \bmod 9 \equiv 5$

$N_5 = 36 \quad M_5 = 36^{-1} \bmod 5 \equiv 1$

$x = 3 \cdot 45 \cdot 1 + 5 \cdot 20 \cdot 5 + 2 \cdot 36 = 135 + 500 + 72 = 707 \bmod 180 = 167$

Důkaz: $167 \bmod 4 = 3 \bmod 4$
$167 \bmod 9 = 5 \bmod 9$
$167 \bmod 5 = 2 \bmod 5$

Eulerova φ-funkce

- φ(n) udává počet čísel menších než *n* pro která platí, že gcd(x,n)=1 tzn. která jsou nesoudělná (relativní prvočísla)
- Hodnota Eulerovy fí funkce se vypočte podle vzorce:

$$\varphi(n) = n \cdot (1 - \frac{1}{n_1}) \cdot (1 - \frac{1}{n_2}) \cdot \ldots \cdot (1 - \frac{1}{n_i})$$

$$n = n_1^x \cdot n_2^y \cdot n_3^z \cdot \ldots$$

- Příklady
  - φ(4) = 2
  - φ(5) = 4
  - φ(12) = 4
- Finta č.1: pokud *n* je prvočíslo, pak $\varphi(n) = n - 1$
- Finta č.2: pokud *n* je součin dvou prvočísel *p* a *q*, pak

$$\varphi(pq) = (\mathrm{p}-1)(\mathrm{q}-1)$$

Eulerova φ-funkce

Nechť p je prvočíslo. Pak $\varphi(p^a) = p \cdot a - p \cdot a^{-1}$

Spočtěte:

$\varphi(31) = 30$

$\varphi(141) = 92$

$\varphi(238) = 96$

Zobecněný Eluerův teorém

- Nechť gcd(a,n)=1, pak $a^{\rho(n)} \bmod n = 1$

Kvadratické kořeny (rezidua)

Čísla *a* , která vyhovují rovnici $x^2 \equiv a \bmod n$ $x \in \langle 1;n-1 \rangle$ jsou kvadratické kořeny (rezidua) mod *n*.

$Q_i = \{a_1, a_2 \ldots\}$ …množina kvadratických reziduí

$\tilde{Q}_i = Q_i^{'}$ …množina kvadratických non-reziduí

Počet kvadratických reziduí mod *n* = počet kvadratických non-reziduí mod *n* = $\varphi(n)/2$

Příklad:
Určete počet kvadratických reziduí mod 13
Odpověď: 6

Určete počet kvadratických non-reziduí mod 35
Odpověď: 12

Kvadratické kořeny (rezidua)

Příklad: Určete kvadratická rezidua mod 7

$x^2 \equiv a \bmod n \qquad x \in \langle 1;6 \rangle$

$1^2 \equiv 1 \bmod 7$

$2^2 \equiv 4 \bmod 7$

$3^2 \equiv 2 \bmod 7$

$4^2 \equiv 2 \bmod 7$

$5^2 \equiv 4 \bmod 7$

$6^2 \equiv 1 \bmod 7$

$Q_i=\{1,2,4\}$ …kvadratická rezidua

$Q_i'=\{3,5,6\}$ …kvadratická non-rezidua

Řád čísla

Nejmenší číslo s , která vyhovují rovnici $a^s \equiv 1 \bmod n$, kde $s \in \langle 1;n-1 \rangle$ označujeme jako řád čísla $a \bmod n$. Značí se ord(a)

Příklad: Určete řád čísla 5 mod 7 … ord(5)=?

Odpověď: $5^S \equiv 1 \bmod 7$ pro s=6 platí, že $5^6 \equiv 1 \bmod 7$ a tedy ord(5)=6

Grupa

Definice: Grupa je množina prvků spolu s nějakou binární operací (definovanou na prvcích grupy), která splňuje následující podmínky:

1. množina je vzhledem k operaci uzavřená, tj. výsledkem binární operace, do které vstupují libovolné dva prvky grupy je opět nějaký prvek grupy
2. operace je asociativní, tj. A+ (B+C)= (A+B)+C
3. v množině existuje jednotkový prvek
4. v množině existuje ke každému prvku inverzní prvek

Nepovinná podmínka:

Pokud je operace v grupě komutativní, tj. A+B=B+A jedná se se o komutativní grupu (Ábelevská grupa, Ábelova grupa).

Grupa

Příklad:

Množina celých čísel {1,2,3,4,5,6} spolu s operací * tvoří multiplikativní grupu Z_7*

Operace v grupě probíhají stejně jako v mod. aritmetice

Generátor

- prvek řádu $\varphi(n)$
- pokud má grupa generátor – cyklická grupa
- pokud *n* je prvočíslo, pak má grupa minimálně jeden generátor

Grupa

Příklad: Určete nejmenší generátor v grupě Z_7*

1) Nebude to číslo 1, protože jakákoliv mocnina 1 je opět 1
2) Nebude to číslo 2, protože řád čísla 2 v grupě Z_7* je $2^S \equiv 1 \mod 7$ platí pro s=3 a není tedy splněna podmínka, že generátor má řád $\varphi(n)$
3) Bude to číslo 3, protože kongruence $3^S \equiv 1 \mod 7$ má řešení pro s=6. $3^6 \equiv 729 \equiv 1 \mod 7$

   Ověření:

$3^1 \equiv 3 \mod 7 \equiv 3$
$3^2 \equiv 9 \mod 7 \equiv 2$
$3^3 \equiv 27 \mod 7 \equiv 6$
$3^4 \equiv 81 \mod 7 \equiv 4$
$3^5 \equiv 243 \mod 7 \equiv 5$
$3^6 \equiv 729 \mod 7 \equiv 1$

Číslo 3 je nejmenší generátor v grupě Z_7*

Pole

Definice: Pole je množina *F* s operacemi násobení a sčítání, které vyhovují pravidlům asociativity a komutativity na obou operacích, distributivnímu zákonu, existenci prvku 0 pro sčítání a prvku 1 pro násobení, existence inverzního prvku pro sčítání a existence inverzního prvku pro násobení pro vše kromě 0.

V anglicky psané literatuře se často označuje jako Galoisovo těľeso a značí se GF (p)

Pole

- Prvočíselná – F_p
- Binární – F_2^m
  - Prvky jsou polynomy stupně nižšího než *n*
  - Pole F_2^m má 2^m prvků
  - stejně jako čísla mají i polynomy residua po dělení (nedělí se číslem ale opět polynomem)

Násobení s polynomy v $F_2{}^m$

- násobení se skládá z
  - vlastního vynásobení polynomu polynomem
  - modulární rekudkce vynásobeného polynomu **nerozložitelným polynom** stupně *n*
- nerozložitelný polynom f(x) je takový, který na oboru reálných čísel nemá jiné dělitele než 1 a sám sebe
- má stejnou roli jako „mod p" v normální modulární aritmetice
- modulární redukce polynomu p(x) se v tomto případě znamená nalezení nějakého polynomu r(x) takového, že $p(x)=q(x)f(x)+r(x)$

- Aritmetika v polích $F_2{}^m$ je výrazně rychlejší než klasická modulární aritmetika s čísly (zvláště pokud je vhodně zvolen nerozložitelný polynom f(x))

Násobení s polynomy v F_2^m

Příklad:

Mějme pole F_2^3 a nerozložitelný polynom $f(x)=x^3+x+1$

Toto pole obsahuje 8 prvků: $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$

Prvky je možné zapsat také jako vektory (000),(001),(010), (011),(100),(101),(110),(111)

Vynásobte polynomy $a(x)=x^2$ a $b(x)=x+1$

1) $x^2 * (x+1) = x^3+x^2$
2) Modulární redukce nerozložitelným polynomem x^3+x+1

$x^3+x^2 : x^3+x+1 = 1$

x^3+x+1 (koeficienty polynomů jsou v mod 2 neboli pouze 0,1)

---

x^2+x+1 ..zbytek po dělení (a výsledek celého násobení)