MB141 – 12. přednáška
Aplikace teorie čísel

Martin Čadek
s využitím přednášek pro předmět MB104

Jarní semestr 2021

Osnova 12. přednášky

- Výpočetní aspekty teorie čísel
- Kryptografie s věřejným klíčem

Základní úlohy výpočetní teorie čísel

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
2. zbytek mocniny celého čísla a na přirozené číslo n po dělení daným m.
3. inverzi celého čísla a modulo $m \in \mathbb{N}$,
4. největší společný dělitel dvou celých čísel (a případně koeficienty do Bezoutovy rovnosti),
5. rozhodnout o daném čísle, je-li prvočíslo nebo složené,
6. v případě složenosti rozložit dané číslo na součin prvočísel.

Základní aritmetické operace

Základní aritmetické operace se i na velkých číslech obvykle provádějí obdobně jako jsme se to učili na základní a střední škole, kdy umíme sčítat v *lineárním* čase, násobit a dělit se zbytkem v *kvadratickém* čase. Pro násobení, které je základem mnoha dalších operací, existují asymptoticky rychlejší algoritmy (typu *rozděl a panuj*) - např. první takový Karatsubův (1960) časové náročnosti $\Theta(n^{\log_2 3})$ nebo algoritmus Schönhage-Strassenův (1971) časové náročnosti $\Theta(n \log n \log\log n)$. Číslo n zde udává celkový počet cifer vstupujících do výpočtu. Pěkný přehled najdete např. na

`http://en.wikipedia.org/wiki/Computational_complexity_of_mathematical_operations`

Největší společný dělitel a modulární inverze

Jak už jsme ukazovali dříve, výpočet výpočet inverze modulo m, tj. řešení kongruence $a \cdot x \equiv 1 \pmod{m}$ s neznámou x lze snadno (díky Bezoutově větě) převést na výpočet největšího společného dělitele čísel a a m a na hledání koeficientů k, l do Bezoutovy rovnosti $k \cdot a + l \cdot m = 1$ (nalezené k je pak onou hledanou inverzí a modulo m).

Podrobná analýza ukazuje, že tento algoritmus je kvadratické časové složitosti.

$$a x + m y = 1$$
$$a x \equiv 1 \mod m$$

Modulární umocňování

V kryptografii s veřejným klíčem budeme budeme potřebovat umocňování modulo m. To se také využívá při ověřování, zda je dané číslo prvočíslo nebo číslo složené. Jedním z efektivních algoritmů je tzv. modulární umocňování zprava doleva:

$((2^2)^2)^2$ $\qquad$ $2^{64} \bmod 341$

```
function modular_pow(base, exponent, modul)
    result := 1
    while exponent > 0
      if (exponent mod 2 == 1):
        result := (result * base) mod modul
      exponent := exponent >> 1
      base = (base * base) mod modul
    return result
```

Symbol $>>$ ve třetím řádku zdola znamená, že od exponentu zapsaného v dvojkové soustavě odebereme poslední cifru 1.

Idea algoritmu

Algoritmus modulárního umocňování je založen na myšlence, že např. při počítání $2^{64} \pmod{1000}$

- není třeba nejprve počítat 2^{64} a poté jej vydělit se zbytkem číslem 1000, ale lépe je postupně násobit „dvojky“ a kdykoliv je výsledek větší než 1000, provést redukci modulo 1000,
- ale zejména, že není třeba provádět takové množství násobení (v tomto případě 63 naivních násobení je možné nahradit pouze šesti umocněními na druhou, neboť

$$2^{64} = (((((2^2)^2)^2)^2)^2)^2.$$

Ukázka průběhu algoritmu

Vypočtěme $2^{560} \pmod{561}$. Protože $560 = (1000110000)_2$, dostaneme uvedeným algoritmem

$560 = 2 \cdot 280$

exponent	base	result	exp's last digit
560	2	1	0
280	4	1	0
140	16	1	0
70	256	1	0
35	460	1	1
17	103	460	1
8	511	256	0
4	256	256	0
2	460	256	0
1	103	256	1
0	~~511~~ ?	1	0

$2^{560} \cdot 1$

$16^{140} \cdot 1$

$[(256)^2]^{35} \cdot 1$

$(103^2)^8 \cdot 460 \cdot 460$

$4^{280} \cdot 1$

$(16^2)^{70} \cdot 1$

$[(460)^2]^{17} \cdot 460 \cdot 1$

$(511^2)^4 \cdot 256$

$((256)^2)^2 \cdot 256$

$460^2 \cdot 256$

$103 \cdot 256 \equiv 1$

A tedy $2^{560} \equiv 1 \pmod{561}$.

$35 = 2 \cdot 17 + 1$ $\quad 17 = 2 \cdot 8 + 1$

Efektivita modulárního umocňování

V průběhu algoritmu se pro každou binární číslici exponentu provede umocnění základu na druhou modulo m (což je operace proveditelná v nejhůře kvadratickém čase), a pro každou „jedničku“ v binárním zápisu navíc provede jedno násobení. Celkově jsme tedy schopni provést modulární umocňování nejhůře v **kubickém** čase.

n^3

Další úlohy výpočetní teorie čísel jsou testování prvočíselnosti a rozklad složených čísel na prvočísla. Tato témata jsou na samostatnou přednášku, nebudeme se jimi zde zabývat. Více lze najít v učebnici Drsná matematika v odstavcích 10.38-47.

~ 6 10

Kryptografie s veřejným klíčem

Dva hlavní úkoly pro „public-key cryptography“ jsou zajistit

- šifrování, kdy zprávu zašifrovanou veřejným klíčem není schopen rozšifrovat nikdo kromě držitele soukromého klíče,
- podepisování, kdy integrita zprávy podepsané soukromým klíčem odesílatele může být ověřena kýmkoliv s přístupem k veřejnému klíči odesílatele.

Nejčastěji používané systémy:

1
- RSA (šifrování) a odvozený systém pro podepisování zpráv
- Digital signature algorithm (DSA) a varianta založená na eliptických křivkách (ECDSA)

2
- Rabinův kryptosystém (a podepisování)

3
- Diffie-Hellmanův protokol na výměnu klíčů (DH)
- ElGamal kryptosystém (a podepisování)

- Kryptografie eliptických křivek (ECC)

RSA

Rivest, Shamir, Adleman (1977); *Cocks*(1973) (n, e)

- Jsou dva typy klíčů – veřejný a soukromý. p, q $\varphi(n)$
- Generování klíčů: zvolí se dvě velká prvočísla p, q, vypočte se $\boxed{n = pq}$, $\varphi(n) = (p-1)(q-1)$. Přitom pouze n je veřejné, $\varphi(n)$ nelze snadno spočítat. $(a, n) = 1$ $a^{\varphi(n)} \equiv 1 \bmod n$
- Veřejný klíč je číslo e s vlastností $(e, \varphi(n)) = 1$
- Soukromý klíč je číslo d s vlastností $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Ze znalosti $\varphi(n)$ ho spočítáme např. pomocí Eukleidova algoritmu.
- Zpráva je číslo $M \pmod{n}$. Zašifrujeme ji jako $C \equiv M^e \pmod{n}$. M^e
- Dešifrování šifry C spočívá ve výpočtu: $C^d \pmod{n}$.
- Na základě Eulerovy věty totiž $\pmod{n}$ dostaneme $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k\varphi(n)+1} \equiv \underbrace{\left(M^{\varphi(n)}\right)^k \cdot M}_{\equiv 1^k \cdot M} \equiv M$.

Příklad na RSA

veřejný klíč $n = 33$
$e = 7$

$(e, n) = (7, 33)$

$33 = 3 \cdot 11$
$p \cdot q$

$\varphi(n) = (3-1) \cdot (11-1)$
$= 2 \cdot 10 = 20$

Najdeme soukromý klíč d

$e \cdot d \equiv 1 \mod 20$
$7 \cdot d \equiv 1 \mod 20$
$d \equiv 3$

Dostaneme zprávu $C = 29$.
Máme najít původní zprávu M.

$$C = M^e \mod 33$$

$$C^d \equiv 29^3 \equiv (-4)^3 \equiv -64 \equiv -66+2 \equiv 2 \mod 33$$

$M \in \{1, \quad , n-1\}$

Rabinův kryptosystém

Dalším veřejným kryptosystémem je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi:

- Každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A.
- Generování klíčů: A zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.
- $V_A = n$, $S_A = (p, q)$ - dvojice prvočísel, nikoliv jejich největší společný dělitel, který je 1.
- Zašifrování numerického *kódu* zprávy M: $C \equiv M^2 \pmod n$.
- Dešifrování šifry C: vypočtou se (čtyři) odmocniny z C modulo n a snadno se otestuje, která z nich byla původní zprávou.

$x^2 \equiv C \mod n$

Výpočet druhé odmocniny

$x^2 \equiv 1 \mod 7$

$1,\ 6 \equiv (-1)$

$(-1)^2 = 1^2$

Výpočet druhé odmocniny z C modulo $n = pq$, kde $p \equiv q \equiv 3 \pmod 4$ probíhá takto:

- vypočti $r = C^{(p+1)/4} \pmod p$ a $s = C^{(q+1)/4} \pmod q$
- vypočti a, b tak, že $ap + bq = 1$ $\boxed{\pm aps \pm bqr}$
- polož $x = (aps + bqr) \pmod n$, $y = (aps - bqr) \pmod n$
- druhými odmocninami z C modulo n jsou $\pm x, \pm y$.

$x^2 \equiv C \mod (pq)$

Zdůvodnění: Z Čínské zbytkové věty vyplývá, že $z^2 \equiv C \pmod{pq}$, právě když současně platí $z^2 \equiv C \pmod p$ a $z^2 \equiv C \pmod{\cancel{p}\, q}$. Lze ukázat, že pro každé liché prvočíslo platí, že kvadratická kongruece $z^2 \equiv C \pmod p$ má řešení právě když $C^{\frac{p-1}{2}} \equiv 1 \pmod p$. Tedy při počítání $\pmod p$ dostaváme $x^2 \equiv y^2 \equiv (bq)^2 r^2 \equiv 1^2 \cdot C^{\frac{p+1}{2}} \equiv C^{\frac{p-1}{2}} \cdot C \equiv 1 \cdot C \equiv C \pmod p$. Analogický výpočet lze provést $\pmod q$.

$$Z^2 \equiv C \mod p \qquad \Big| \ {}^{\frac{p-1}{2}}$$

$$\left(Z^2\right)^{\frac{p-1}{2}} \equiv C^{\frac{p-1}{2}}$$

$$\parallel$$

$$Z^{p-1} \equiv C^{\frac{p-1}{2}}$$

$$\equiv$$

$$1 \equiv C^{\frac{p-1}{2}} \qquad\qquad C \equiv M^2$$

mod p

$$(\pm a p s \pm b q r)^2 \equiv (\pm b q r)^2 \equiv (b q r)^2$$

$$\equiv \underbrace{(bq)^2}_{\equiv 1} r^2 \equiv r^2 \equiv \left(C^{\frac{p+1}{4}}\right)^2 \equiv$$

$$\equiv C^{\frac{p+1}{2}} \equiv C^{\frac{p-1}{2}+1} \equiv \underline{C^{\frac{p-1}{2}}} \cdot C \equiv 1 \cdot C \equiv C$$

mod p.

Příklad

Příklad

V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23, q = 31$, veřejným klíčem je pak $n = pq = 713$. Zašifrujte zprávu $M = 327$ pro Alici a ukažte, jak bude Alice tuto zprávu dešifrovat.

$C \equiv 327^2 \equiv 692$. Při dešifrování spočítáme $C^6 \equiv (2)^6 \equiv 18 \pmod{23}$ a $C^8 \equiv 10^8 \equiv 14 \pmod{31}$. Dále $-4 \cdot 23 + 3 \cdot 31 = 1$. Proto máme 4 kandidáty na zprávu, a to $\pm 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18 \pmod{713}$. To jsou čísla ± 38 a $\pm 327 \pmod{731}$.

$p = 23 \qquad q = 31 \qquad \equiv 3 \bmod 4 \qquad n = p \cdot q = 713$

$\underline{327^2 \bmod 713}$ $\qquad 327^2 \equiv 692 \bmod 713$

$C = 327^2 \bmod 23 \qquad C \equiv$ nico $\bmod \underline{23}$

$\boxed{\bmod 23} \qquad C \equiv$ nico $\bmod \underline{31}$

$r = C^{\frac{p+1}{4}} = (692)^6 \equiv 2^6 \equiv 2^4 \cdot 2^2 \equiv 16 \cdot 4 \equiv$

$64 = 46 + 18 \qquad \equiv (-7) \cdot 4 = -28 \equiv -5 \equiv 18$

$r \equiv 18 \qquad 3 \cdot 31 = 93$

mod 31

$C^8 = (692)^8 \equiv 10^8 \equiv (100)^4 \equiv$

$\equiv 7^4 \equiv 49 \cdot 49 \equiv$

$\equiv 18 \cdot 18 \equiv 18 \cdot 3 \cdot 6 \equiv$

$\equiv 54 \cdot 6 \equiv (-8) \cdot 6 \equiv -48 \equiv +14$

mod 31

$$a\,23 + b\,31 = 1$$

23	31	$a23+b31$
1	0	23
0	1	31
-1	1	8
$-3-1$	3	1
-4	3	1

$a = (-4) =$

$b = 3$

$$\pm\, a p s \pm b q r$$

$$\pm\, 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18$$

výsledek výše

Princip digitálního podpisu

Podepisování

1. Vygeneruje se otisk (hash) H_M zprávy pevně stanovené délky (např. 160 nebo 256 bitů).
2. Podpis zprávy $S_A(H_M)$ je vytvořen (pomocí dešifrování) z tohoto hashe s nutností znalosti soukromého klíče S_A podepisujícího.
3. Zpráva M (případně zašifrovaná veřejným klíčem příjemce) je spolu s podpisem odeslána.

Ověření podpisu

1. K přijaté zprávě M se (po jejím případném dešifrování) vygeneruje otisk H'_M
2. S pomocí veřejného klíče V_A (deklarovaného) odesílatele zprávy se rekonstruuje původní otisk zprávy $V_A(S_A(H_M)) = H_M$.
3. Oba otisky se porovnají $H_M = H'_M$?.

Výměna klíčů podle Diffie-Hellmana

Alice $p, g, a, g^b \longrightarrow g^{ab} = (g^b)^a$ | Bob $p, g, b, g^a \longrightarrow g^{ab} = (g^a)^b$

Diffie, Hellman (1976), *Williamson* (1974)
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na prvočísle p a primitivním kořenu g modulo p (veřejné). (Zopakujme, že g je primitivní kořen modulo prvočíslo p, jestliže $g^n \equiv 1 \pmod p$ pouze pro násobky $p - 1$.)
- Alice vybere náhodné číslo a a pošle Bobovi $g^a \pmod p$
- Bob vybere náhodné b a pošle Alici $g^b \pmod p$
- Společným klíčem pro komunikaci je $g^{ab} \pmod p$.

p prvočíslo $\qquad$ g prim. kořen mod p

$g^{p-1} \equiv 1$ mod p $\qquad$ $g^n \equiv 1$ mod p pouze pro násobky $p-1$

Kryptosystém ElGamal

$C_2 \cdot I = M \cdot g^{ab} \cdot I \equiv M \mod p$

Z protokolu Diffie–Hellman na výměnu klíčů je odvozen šifrovací algoritmus ElGamal:

- Alice zvolí prvočíslo p spolu s primitivním kořenem g.
- Alice zvolí **tajný klíč** a, spočítá $h = \underline{g^a} \pmod p$ a zveřejní **veřejný klíč** (p, g, h). $= g^a$
- Šifrování zprávy M: Bob zvolí náhodné b a vypočte $\underline{C_1} = g^b \pmod p$ a $\underline{C_2} = \underline{M} \cdot \underbrace{h^b}_{= g^{ab}} \pmod p$ a pošle Alici (C_1, C_2).
- Dešifrování zprávy provede Alice tak, že spočítá inverzi I k $C_1^a = (g^b)^a = g^{ab} \pmod p$ a vynásobí $C_2 \cdot I \equiv M \cdot g^{ab} \cdot I \equiv M \pmod p$.

Příklad najdete ve cvičení. Analogicky jako pro RSA lze odvodit podepisování.

$C_1^a = g^{ab}$

$(\underbrace{g^b}_{=C_1}, \underbrace{M \cdot g^{ab}}_{=C_2})$

$g^{ab} \cdot I \equiv 1 \mod p$

Příklad na El Gamal

Alice

$p = 41 \quad g = 11$

Bob

$p = 41 \quad g = 11$

g je skutečně primitivní ~~ko~~ ≡ -
ukáže

$$g^{40} \equiv 1 \mod 41$$

$40 = 5 \cdot 2^3$

$$\underline{g^{2^3}} \equiv g^8 \equiv 11^8 \equiv (11 \cdot 11)^4 \equiv$$

$$g^{20} \quad \equiv (121)^4 \equiv (-2)^4 \equiv 16 \mod 41$$

$$g^{20} \equiv 11^{20} = (121)^{10} \equiv (-2)^{10} = (-2)^5 (-2)^5 =$$

$\equiv 32 \cdot 32 \equiv (-9)^2 \equiv 81 \equiv -1 \mod 41$

Alice Bob

$p = 41,\ g = 11$

$a = 10$ soukromý

$g^a = 11^{10} \equiv 9 \mod 41$

Bob Alici pošle zprávu

$(C_1, C_2) = (22, 6)$

$g^b \quad M \cdot g^{ab}$

Dešifrování

I inverze k $\quad 22^{10} = g^{ab}$

mod 41

$$(22)^{10} = 22^2 \cdot (22^2)^2 \cdot (22^2)^2$$

$23 \equiv -18$ mod 41

$$= (-8)\ (-8)^2\ (-8)^2$$

$$= (-8)\ 64 \cdot 64 \equiv (-8) \cdot 23 \cdot 23$$

$$\equiv -9 \mod 41$$

$(-9)^{(-1)}$ mod 41

$9^2 = 81 \equiv -1 \mod 41$

$$(-9) \cdot 9 \equiv -81 \equiv 1 \mod 41$$

$$I = 9$$

$$M \equiv C_2 \cdot I \equiv 6 \cdot 9 \equiv 13 \mod \underline{41}$$