Diszkrét matematika I.
középszint

11. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Gyors hatványozás

Legyenek m, a, n pozitív egészek, $m > 1$. Szeretnénk kiszámolni $a^n \bmod m$ maradékot hatékonyan.

Ábrázoljuk n-et 2-es számrendszerben:

$$n = \sum_{i=0}^{k} \varepsilon_i 2^i = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_1 \varepsilon_0)_{(2)}, \text{ ahol } \varepsilon_0,\ \varepsilon_1, \dots,\ \varepsilon_k \in \{0, 1\}.$$

Legyen n_j $(0 \le j \le k)$ az első $j+1$ jegy által meghatározott szám: $n_j = \lfloor n/2^{k-j} \rfloor = (\varepsilon_k \varepsilon_{k-1} \dots \varepsilon_{k-j})_{(2)}$

Ekkor meghatározzuk minden j-re az $x_j \equiv a^{n_j} \pmod m$ maradékot:

$n_0 = \varepsilon_k = 1$, $x_0 = a$.

$n_j = 2 \cdot n_{j-1} + \varepsilon_{k-j} \Rightarrow$

$$x_j = a^{\varepsilon_{k-j}} x_{j-1}^2 \bmod m = \begin{cases} x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_{k-j} = 0 \\ a x_{j-1}^2 \bmod m, & \text{ha } \varepsilon_{k-j} = 1 \end{cases} \Rightarrow$$

$x_k = a^n \bmod m$.

Az algoritmus helyessége az alábbi formulából következik (Biz.: HF):

$$a^n = a^{\sum_{i=0}^{k} \varepsilon_i 2^i} = \prod_{i=0}^{k} \left(a^{2^i}\right)^{\varepsilon_i}$$

Gyors hatványozás

Példa

Mi lesz $3^{111} \bmod 10$? (Euler-Fermat $\Rightarrow$ 7)

$111_{(10)} = 1101111_{(2)}$ itt $k = 6$, $a = 3$, $m = 10$.

j	n_j	$x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$	$x_j \bmod 10$
0	1	–	3
1	11	$x_1 = 3 \cdot 3^2$	7
2	110	$x_2 = 7^2$	9
3	1101	$x_3 = 3 \cdot 9^2$	3
4	11011	$x_4 = 3 \cdot 3^2$	7
5	110111	$x_5 = 3 \cdot 7^2$	7
6	1101111	$x_6 = 3 \cdot 7^2$	7

Gyors hatványozás

Példa

Oldjuk meg a $23x \equiv 4 \pmod{211}$ kongruenciát!
Euler-Fermat $\Rightarrow$ $x \equiv 4 \cdot 23^{209} \equiv \ldots \pmod{211}$.

Mi lesz 23^{209} mod 211?
$209_{(10)} = 11010001_{(2)}$ itt $k = 7$, $a = 23$.

j	n_j	$x_j = a^{\varepsilon_{k-j}} \cdot x_{j-1}^2$	x_j mod 211
0	1	–	23
1	11	$x_1 = 23 \cdot 23^2$	140
2	110	$x_2 = 140^2$	188
3	1101	$x_3 = 23 \cdot 188^2$	140
4	11010	$x_4 = 140^2$	188
5	110100	$x_5 = 188^2$	107
6	1101000	$x_6 = 107^2$	55
7	11010001	$x_6 = 23 \cdot 55^2$	156

$x \equiv 4 \cdot 23^{209} \equiv 4 \cdot 156 \equiv 202 \pmod{211}$.

Generátor

Tétel (NB)

Legyen p prímszám. Ekkor $\mathbb{Z}_p^*$-ban van generátor (primitív gyök): van olyan $1 < g < p$ egész, mely hatványaiként előáll minden redukált maradékosztály: $\{\overline{g^0} = \overline{1}, \overline{g}, \overline{g^2}, \ldots, \overline{g^{p-2}}\} = \mathbb{Z}_p^*$, azaz $\{1 = g^0, g \bmod p, g^2 \bmod p, \ldots, g^{p-2} \bmod p\} = \{1, 2, \ldots, p-1\}$.

Példa

3 generátor modulo 7:

$$
\begin{aligned}
3^0 &= 1 = 1 \equiv 1 = 1 \equiv 1 \pmod 7\\
3^1 &= 3 = 3^0 \cdot 3 \equiv 1 \cdot 3 = 3 \equiv 3 \pmod 7\\
3^2 &= 9 = 3^1 \cdot 3 \equiv 3 \cdot 3 = 9 \equiv 2 \pmod 7\\
3^3 &= 27 = 3^2 \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 6 \pmod 7\\
3^4 &= 81 = 3^3 \cdot 3 \equiv 6 \cdot 3 = 18 \equiv 4 \pmod 7\\
3^5 &= 243 = 3^4 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 5 \pmod 7
\end{aligned}
$$

Generátor

Példa

2 generátor modulo 11:

n	0	1	2	3	4	5	6	7	8	9
2^n mod 11	1	2	4	8	5	10	9	7	3	6

2 nem generátor modulo 7:

n	0	1	2	3	4	5
2^n mod 7	1	2	4	1	2	4

Diszkrét logaritmus

Definíció

Legyen p prímszám, g generátor modulo p. Ekkor az $a \in \mathbb{Z}$ $(p \nmid a)$ g alapú diszkrét logaritmusa (indexe):

$$\log_g a = n : \quad a \equiv g^n \pmod p, \quad 0 \le n < p.$$

Példa

3 generátor modulo 7:

n	0	1	2	3	4	5
3^n	1	3	2	6	4	5

$\longrightarrow$

3^n	1	3	2	6	4	5
n	0	1	2	3	4	5

azaz

a	1	3	2	6	4	5
$\log_3 a$	0	1	2	3	4	5

$\longrightarrow$

a	1	2	3	4	5	6
$\log_3 a$	0	2	1	4	5	3

Diszkrét logaritmus

Példa

2 generátor modulo 11:

n	0	1	2	3	4	5	6	7	8	9
$2^n \bmod 11$	1	2	4	8	5	10	9	7	3	6

Logaritmus-táblázat:

a	1	2	3	4	5	6	7	8	9	10
$\log_2 a$	0	1	8	2	4	9	7	3	6	5

Tétel (HF)

Legyen p prímszám, g generátor modulo p, $1 \leq a, b < p$, $n \in \mathbb{Z}$. Ekkor

$$\log_g(a \cdot b) \equiv \log_g a + \log_g b \pmod{p-1}$$
$$\log_g(a^n) \equiv n \cdot \log_g a \pmod{p-1}$$

Alkalmazások

Számelmélet alkalmazási területei:

- Kriptográfia
  - üzenetek titkosítása;
  - digitális aláírás;
  - azonosítás, ...
- Kódelmélet
- ...

Caesar kód

Julius Caesar katonáival a következő módon kommunikált:

Feleltessük meg az (angol) ábécé betűit a $\{0, 1, \ldots, 25\}$ halmaznak:

$$\begin{array}{l} \mathtt{a} \mapsto 0 \\ \mathtt{b} \mapsto 1 \\ \mathtt{c} \mapsto 2 \\ \vdots \\ \mathtt{z} \mapsto 25 \end{array}$$

Titkos kulcs: $s \in \{0, 1, \ldots, 25\}$.

Titkosítás: adott $a \in \{0, 1, \ldots, 25\}$ esetén a titkosítása $a \mapsto a + s \bmod 26$. Üzenet titkosítása betűnként.

Kititkosítás: adott $b \in \{0, 1, \ldots, 25\}$ esetén b kititkosítása $b \mapsto b - s \bmod 26$. Üzenet kititkosítása betűnként.

Példa

`hello` titkosítása az $s = 13$ kulccsal:

`hello` $\rightarrow 7\ 4\ 11\ 11\ 14 \xrightarrow{\text{titkosítás}} 20\ 17\ 24\ 24\ 1 \rightarrow$ `uryyb`

`uryyb` kititkosítása az $s = 13$ kulccsal:

`uryyb` $\rightarrow 20\ 17\ 24\ 24\ 1 \xrightarrow{\text{kititkosítás}} 7\ 4\ 11\ 11\ 14 \rightarrow$ `hello`

Caesar kód

Ha $s = 13$ kulcsot választjuk: Rot13.
Titkosítás és kititkosítás ugyanazzal a kulccsal: $-13 \equiv 13 \pmod{26}$.

A titkosítás nem biztonságos: betűgyakoriság vizsgálattal törhető (al-Kindi i.sz. 9 sz.)

Ha a különböző pozíciókban különböző kulcsokat választhatunk (véletlenszerűen) $\Rightarrow$ bizonyítottan biztonságos

Gyakorlatban: One Time Pad – OTP

Üzenetek: bináris formában: m=100100101
Kulcs: bináris sorozat: s=010110110
Titkosítás: bitenkénti XOR (mod2 összeadás):

$$\begin{array}{r} \texttt{m}=100100101 \\ \text{XOR } \texttt{s}=010110110 \\ \hline \texttt{c}=110010011 \end{array}$$

Kritikus pont: az s titkos kulcs átadása.

RSA

Ron **Rivest**, Adi **Shamir** és Leonard **Adleman** 1977-ben a következő eljárást javasolták:

Kulcsgenerálás: Legyen p, q két (nagy, 1024 bites) prím, $n = p \cdot q$.
Legyen $e \in \{1, \ldots, \varphi(n)\}$ olyan, hogy $(e, \varphi(n)) = 1$.
Legyen d az $ex \equiv 1 \pmod{\varphi(n)}$ kongruencia megoldása.
Kulcsok: - nyilvános kulcs (n, e),
- titkos kulcs d.

Titkosítás: Adott $0 \leq m < n$ üzenet titkosítása:
$c = m^e \bmod n$.

Kititkosítás Adott $0 \leq c < n$ titkosított üzenet kititkosítása:
$m = c^d \bmod n$.

Algoritmus helyessége:

$$c^d = (m^e)^d = m^{e \cdot d} = m^{k \cdot \varphi(n)+1} \overset{\text{E-F}}{\equiv} m \pmod{n}$$

RSA

Valóságban az m üzenet egy titkos kulcs további titkosításhoz.

Az eljárás biztonsága azon múlik, hogy nem tudjuk hatékonyan faktorizálni az $n = p \cdot q$ szorzatot.

Feladat

Találjuk meg a következő szám osztóit.
RSA-100 =
5226050279225333605356183781326374297180681149613806886
57908494580122963258952897654000350692006139

RSA-2048=

2519590847565789349402718324004839857142928212620403202777713783604366202070759555 6
2640185258807844069182906412495150821892985591491761845028084891200728449926873928 0
7287776735971418347270261896375014971824691165077613379859095700097330459748808428 4
0179742910064245869181719511874612151517265463228221686998754918242243363725908514 1
8654620435767984233871847744479207399342365848238242811981638150106748104516603773 0
6056201619676256133844143603833904414952634432190114657544454178424020924616515723 3
5077870774981712577246796292638635637328991215483143816789988504044536402352738195 1
378636564391212010397122822120720357

RSA

RSA-2048 faktorizálása:

Próbaosztás (Eratoszthenész szitája): n szám esetén $\sim \sqrt{n}$ osztást kell végezni:

RSA-2048 $n \sim 2^{2048}$, $\sqrt{n} \sim 2^{1024}$ próbaosztás.

Ha 1 másodperc alatt $\sim 10^9 \approx 2^{30}$ osztás $\Rightarrow$ $2^{1024}/2^{30} = 2^{994}$ másodperc kell a faktorizáláshoz.

2^{994} másodperc $\approx 2^{969}$ év.

Ugyanezt 2 db géppel: 2^{968} év.

Ugyanezt a legjobb (ismert) algoritmussal: $2500000000000000000000000000000$ év $(= 2,5 \cdot 10^{30})$

Univerzum életkora: $1,38 \cdot 10^{10}$ év.

RSA

Példa

Kulcsgenerálás:

Legyen $p = 61$, $q = 53$ és $n = 61 \cdot 53 = 3233$, $\varphi(3233) = 3120$.

Legyen $e = 17$. Bővített euklidészi algoritmussal: $d = 2753$.

Nyilvános kulcs: $(n = 3233, e = 17)$;

Titkos kulcs: $d = 2753$.

Titkosítás: Legyen $m = 65$.

$c = 2790 \equiv 65^{17} \pmod{3233}$

Kititkosítás: Ha $c = 2790$:

$2790^{2753} \equiv 65 \pmod{3233}$

Digitális aláírást is lehet generálni: e és d felcserélésével:

(Ekkor külön n', e', d' kell a titkosításhoz!)

Aláírás Legyen $s = m^d \bmod n$, ekkor az aláírt üzenet: (m, s).

Ellenőrzés $m \stackrel{?}{\equiv} s^e \pmod{n}$.

Diffie-Hellman kulcscsere protokoll

Az első nyilvános kulcsú kriptográfiai rendszert Whitfield **Diffie** és Martin **Hellman** 1976-ban publikálta.

Alice	nem megbízható csatorna	Bob
választ $a \in_R \{0, 1, \ldots, p-2\}$		választ $b \in_R \{0, 1, \ldots, p-2\}$
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
kiszámolja $\left(g^b\right)^a$		kiszámolja $\left(g^a\right)^b$
	közös titkos kulcs: g^{ab}	

Diffie-Hellman kulcscsere protokoll

Nyilvános paraméterek: p (nagy) prím, g generátor $\bmod p$.
Kulcsok: Alice titkos kulcsa a: $1 \leq a < p-1$, nyilvános kulcsa $g^a \bmod p$,
Bob titkos kulcsa b: $1 \leq a < p-1$, nyilvános kulcsa $g^b \bmod p$.
Közös kulcs: $g^{ab} \bmod p$.

A protokoll biztonsága azon múlik, hogy a diszkrét logaritmus kiszámítás nehéz.

Ha $p \sim 2^{2048}$ (2048 bites), diszkrét logaritmus számolása $\sim 10^{30}$ év.

Példa

Nyilvános paraméterek: Legyen $p = 11$, $g = 2$.

Kulcsok: Alice titkos kulcsa $a = 4$, nyilvános kulcsa $2^4 \bmod p = 5$.

Bob titkos kulcsa $b = 8$, nyilvános kulcsa $2^8 \bmod p = 3$.

Közös kulcs: $\left(g^b\right)^a = 3^4 \bmod p = 4$, $\quad \left(g^a\right)^b = 5^8 \bmod = 4$.