Algorithms for Discrete Logarithm

Outline

- [1] Discrete Logarithm Problem
- [2] Algorithms for Discrete Logarithm
  - A trivial algorithm
  - Baby-step Giant-step algorithm
  - The index calculus method

[1] Discrete Logarithm Problem

- Let G be a finite multiplicative group (G, *).

For an element $\alpha \in G$ having order n, define.

$$<\alpha> = \{\alpha^i \mid i = 0, 1, 2, \ldots, n-1\}$$

Then $<\alpha>$ is a subgroup of G, and $<\alpha>$ is cyclic of order n.

- **Discrete logarithm problem**

Given $\beta \in <\alpha>$, find the unique integer a, $0 \le a \le n-1$, s.t.

$$\alpha^a = \beta$$

We will denote this integer a by $\log_a \beta$;

it is called the discrete logarithm of β.

Discrete Logarithm Problem

- **Example 1**
  $G = Z^*_{19} = \{ 1, 2, \ldots, 18\}$
  $n=18$, generator $g = 2$

i	1	2	3	4	5	6	7	8	9
g^i	2	4	8	16	13	7	14	9	18

10	11	12	13	14	15	16	17	18
17	15	11	3	6	12	5	10	1

then $\log_2 14 = 7$
$\log_2 6 = 14$

Discrete Logarithm Problem

- **Example 2**

In $Z^*_{11} = \{ 1, 2, \ldots, 10\}$

Let G= <3> ={1, 3, 9, 5, 4}, n=5,

3 is not a generator of Z^*_{11} but a generator of G.

$\log_3 5 = 3$

Discrete Logarithm Problem

- **Example 3**
  G=$GF^*(2^3)$ with irreducible poly. $p(x) = x^3 + x + 1$
  G=$Z_p{}^*/p(x)$ = { 1, x, x^2, 1+x, 1+x^2, x+x^2, 1+x+x^2 }
  n=7, generator $g = x$

i	1	2	3	4	5	6	7
g^i	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1	1

then $\log_x(x+1) = 3$
$\log_x(x^2+x+1) = 5$
$\log_x(x^2+1) = 6$

Discrete Logarithm Problem

- **Example 4**
  Let p
  =1053546280395016975304616582933958731948871814925913489342608734258717883575185867300386287737705577937382925873762451990450430661350859682697410256268271147283034897563214300237166369174066615907176472549470083113107138189921280884003892629359

  NB: $p = 158(2^{800} + 25) + 1$ and has 807 bits.
- Find $a \in \mathrm{Z}$ such that

$$2 \equiv 3^{a} \pmod{p}$$

[2] Algorithms for Discrete Logarithm

- A trivial algorithm
- Pollard rho discrete log algorithm (Omitted)
- Pohlig-Hellman algorithm (Omitted)
- Baby-step giant-step algorithm
- The index calculus method

A trivial algorithm

- Discrete Logarithm Problem in Z_p^*

  given generator α (i.e. $<\alpha>= Z_p^*$) and β *in* Z_p^* ,
  find a in $Z_{p-1}=\{0, 1, \ldots, p-2\}$ s.t. $\beta = \alpha^a \mod p$

- A trivial algorithm
  - Compute α^i and test if $\beta = \alpha^i$
  - Time complexity O(p)

Baby-step giant-step algorithm

- Shanks' algorithm (Baby-step giant-step) (1972)
  - Compute $L_1 = \{(i, \alpha^{mi}), i = 0, 1, \ldots, m\text{-}1\}$
    $L_2 = \{(i, \beta\alpha^{-i}), i = 0, 1, \ldots, m\text{-}1\}$
  - where m = $\lceil \sqrt{p-1} \rceil$
    Sort L_1 and L_2 with respect to the 2nd coordinate.
  - Find the same 2nd coordinate from L_1 and L_2, say,
    (q, α^{mq}), $(r, \beta\alpha^{-r})$, to get $\alpha^{mq} = \beta\alpha^{-r}$.
    So $\beta = \alpha^{mq+r}$ and $a = mq+r$.
  - Time complexity $O(m \log m) = O(\sqrt{p} \log p)$
  - Space complexity $O(\sqrt{p})$

Example 1

$\log_2 15 \bmod 19 = ?$

$G = Z^*_{19} = \{ 1, 2, \ldots, 18\}$

$\alpha = 2$, $\alpha^{-1} = 10$, $n = p-1 = 18$, $m = 5$, $\alpha^m = 13$

$\beta = 15$

$L_1: (i, \alpha^{mi})$	$L_2: (i, \beta\alpha^{-i})$	
(0, 1)	(0, 15)	
(1, 13)	(1, $\underline{17}$)	$q = 2$
(2, $\underline{17}$)	(2, 18)	$r = 1$
(3, 12)	(3, 9)	$mq + r = 11$
(4, 4)	(4, 14)	

$\log_2 15 \bmod 19 = 11$

Example 2

$\log_3 525 \bmod 809 = ?$

$G = Z^*_{809} = \{1, 2, \ldots, 808\} = \langle 3 \rangle$

$\alpha = 3$, $\alpha^{-1} = 270$, $n = p-1 = 808$, $m = 29$, $\alpha^m = 99$

$\beta = 525$

L_1: (i, α^{mi})	L_2: $(i, \beta\alpha^{-i})$
(0, 1)	(0, 525)
(1, 99)	(1, 175)
(2, 93)	(2, 328)
(3, 308)	(3, 379)
(4, 559)	(4, 396)
(5, 329)	(5, 132)
(6, 211)	(6, 44)
(7, 664)	(7, 554)
(8, 207)	(8, 724)
(9, 268)	(9, 511)
(10, $\underline{644}$)	(10, 440)
(11, 654)	(11, 686)
(12, 26)	(12, 768)

L_1: (i, α^{mi}) L_2: $(i, \beta\alpha^{-i})$

(13, 147)	(13, 256)
(14, 800)	(14, 355)
(15, 727)	(15, 388)
(16, 781)	(16, 399)
(17, 464)	(17, 133)
(18, 632)	(18, 314)
(19, 275)	(19, 644)
(20, 528)	(20, 754)
(21, 496)	(21, 521)
(22, 564)	(22, 713)
(23, 15)	(23,777)
(24, 676)	(24, 259)
(25, 586)	(25, 356)
(26, 575)	(26, 658)
(27, 295)	(27, 489)
(28, 81)	(28, 163)

$q = 10$, $r = 19$, so $mq + r = 29*10+19 \bmod 808 = 309$

and $\log_3 525 \bmod 809 = 309$

The index calculus method

- The index calculus method (Suitable only for $G=Z_p{}^*$)

(1st step)

To find the discrete logarithms of the B primes in the factor base.

$$B = \{p_1, p_2, ..., p_B\}.$$

(2nd step)

To compute the discrete logarithm of a desired element a, using the knowledge of the discrete logarithms of the elements in the factor base.

- **Example**

$\log_5 9451 \bmod \underline{10006}$=?

Choose B={2, 3, 5, 7}. Of course $\log_5 5=1$.

Use lucky exponents 4063, 5136, and 9865

$5^{4063} \bmod 10007 = 42 = 2 * 3 * 7$

$5^{5136} \bmod 10007 = 54 = 2 * 3^3$

$5^{9865} \bmod 10007 = 189 = 3^3 * 7$

And we have three congruences:

$\log_5 2 + \log_5 3 + \log_5 7 = 4063 \bmod \underline{10006}$

$\log_5 2 + 3 \log_5 3 = 5136 \bmod \underline{10006}$

$3 \log_5 3 + \log_5 7 = 9865 \bmod \underline{10006}$

There happens to be a unique solution modulo 10006

$\log_5 2=6578$, $\log_5 3=6190$, and $\log_5 7=1301$

Choose random exponent s = 7736 and try to calculate

$$\beta\alpha^s = 9451*5^{7736} \bmod 10007 = 8400$$

Since $8400 = 2^4*3*5^2*7$ factors over B, we obtain

$$\log_5 9451 = (4 \log_5 2 + \log_5 3 + 2 \log_5 5 + \log_5 7 - s) \bmod 10006$$

$$= (4*6578 + 6190 + 2*1 + 1301 - 7736) \bmod 10006$$

$$= 6057 \bmod 10006$$