§ 5 Discrete Logarithms

Discrete Logarithm Problem

Question :

Let p be prime and let α and β be integers such that $1 \le \alpha, \beta \le p-1$.

Find an integer x such that $\beta \equiv \alpha^x \pmod p$ —— (*).

(*) has a solution $m \in \mathbb{Z}$ $\Leftrightarrow$ $\beta \equiv \alpha^m \pmod p$

$\Leftrightarrow$ $[\beta] \in \langle[\alpha]\rangle$, where $[\alpha], [\beta] \in (\mathbb{Z}/p\mathbb{Z})^\times$

Therefore, if $[\alpha]$ is a primitive root (i.e. $G = \langle[\alpha]\rangle$), then (*) must be solvable.

Example 5.1

In $(\mathbb{Z}/5\mathbb{Z})^\times$, $[2]$ is an primitive root while $[4]$ is not (see example 3.11)

$\beta \equiv 2^x \pmod 5$ has a solution for any $1 \le \beta \le 4$, but

$\beta \equiv 4^x \pmod 5$ has a solution only when $\beta = 1$ or 4.

Definition 5.1

$L_\alpha(\beta)$ is defined to be the least nonnegative integer x such that $\beta \equiv \alpha^x \pmod p$.

Back to example 5.1,

we have $2^3 \equiv 2^{3+4k} \equiv 3 \pmod 5$, where $k \in \mathbb{Z}$, order of $2 = 4$ so $L_2(3) = 3$.

Similarly $L_4(1) = 0$ and $L_4(4) = 1$ but $L_4(2)$ and $L_4(3)$ are undefined.

Proposition 5.1

$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{p-1}$

proof :

It follows from the fact that

if $m_1, m_2 \in \mathbb{Z}$ such that $\alpha^{m_1} \equiv \alpha^{m_2} \pmod p$, then $m_1 \equiv m_2 \pmod{p-1}$.

Proposition 5.2

Let p be a prime. Then $(\mathbb{Z}/p\mathbb{Z})^\times$ has a primitive root.

As a result, $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $\varphi(p) = p-1$

$((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ is isomorphic to $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ which has $\varphi(p-1)$ generators.

Question: Even we know the existence of a primitive root of $(\mathbb{Z}/p\mathbb{Z})^\times$, how to find one?

Take any $1 \le \alpha \le p-1$, if $[\alpha]^d = [1]$ where d is the order of $[\alpha]$, then $d \mid p-1$.

Therefore, if $[\alpha]^d \ne [1]$ for every $d \mid p-1$ with $1 \le d < p-1$, then $[\alpha]$ is a primitive root.

However, the following proposition helps to reduce the number of factors to be tested.

Proposition 5.3

Let p be a prime and $1 \le \alpha \le p-1$.

Suppose that $p-1$ can be factorized as $\prod_{i=1}^{m} p_i^{d_i}$, where p_i are primes.

Let $N_i = \frac{p-1}{p_i}$ for $i = 1, 2, \cdots, m$.

$\alpha^d \equiv 1 \pmod p$ for some $d \mid p-1$ with $1 \le d < p-1$ if and only if

$\alpha^{N_i} \equiv 1 \pmod p$ for some $i = 1, 2, \cdots, m$

(To show $[\alpha]$ is a primitive root, we only need to show $\alpha^{N_i} \not\equiv 1 \pmod p$ for all $i = 1, 2, \cdots, m$)

Example 5.2

Consider the prime $p = 601$.

$p-1 = 600 = 2^3 \cdot 3 \cdot 5^2$ $(p_1 = 2, p_2 = 3, p_3 = 5;\ N_1 = 300, N_2 = 200, N_3 = 120)$

Direct computation: $7^{300} \equiv 600$, $7^{200} \equiv 576$, $7^{120} \equiv 423 \pmod{601}$

$\therefore [7]$ is a primitive root.

Computing Discrete Logs

We are going to introduce some algorithms to compute discrete logs.

However, none of them run in polynomial time.

The Polhig-Hellman Algortthm

Solve $\beta \equiv \alpha^x \pmod p$, where α is a primitive root.

Example 5.3

Find an integer x such that $0 \le x \le 135$ and $3^x \equiv 23 \pmod{137}$

(Remark : 136 cannot be a solution as $3^{136} \equiv 1 \pmod{137}$ by Euler's theorem)

$137 - 1 = 136 = 2^3 \times 17$

Idea : Suppose we know $x \equiv a \pmod 8$ and $x \equiv b \pmod{17}$,

then x can be found by using Chinese remainder theorem.

Express x as $x_0 + 2x_1 + 4x_2 + \cdots$, where $0 \le x_i \le 1$.

$$3^x \equiv 3^{x_0+2x_1+4x_2+\cdots} \equiv 23 \pmod{137}$$

$$(3^{x_0+2x_1+4x_2+\cdots})^{68} \equiv 23^{68} \pmod{137}$$

$$(3^{68})^{x_0} \cdot (3^{136})^{(x_1+2x_2+\cdots)} \equiv 23^{68} \pmod{137}$$

$$(-1)^{x_0} \equiv -1 \pmod{137}$$ (Euler's theorem $\Rightarrow 3^{136} \equiv 1 \pmod{137}$)

$\therefore x_0 = 1$ (i.e. $L_3(23) \equiv 1 \pmod 2$)

$$3^{1+2x_1+4x_2+\cdots} \equiv 23 \pmod{137}$$

$$3^{2x_1+4x_2+\cdots} \equiv 3^{-1}\ 23 \equiv 99 \pmod{137}$$ $3^{-1} \equiv 46 \pmod{137}$

$$(3^{2x_1+4x_2+\cdots})^{34} \equiv 99^{34} \pmod{137}$$

$$(3^{68})^{x_1} \cdot (3^{136})^{(x_2+2x_3+\cdots)} \equiv 99^{34} \pmod{137}$$

$$(-1)^{x_1} \equiv 1 \pmod{137}$$

$\therefore x_1 = 0$ (i.e. $L_3(23) \equiv 0 \pmod 4$)

$$3^{2\cdot 0+4x_2+\cdots} \equiv 99 \pmod{137}$$

$$(3^{4x_2+\cdots})^{17} \equiv 99^{17} \pmod{137}$$

$$(3^{68})^{x_2} \cdot (3^{136})^{(x_3+2x_4+\cdots)} \equiv 99^{17} \pmod{137}$$

$$(-1)^{x_2} \equiv -1 \pmod{137}$$

$\therefore x_2 = 1$ (i.e. $L_3(23) \equiv 1 \pmod 8$)

$\therefore x \equiv x_0 + 2x_1 + 4x_2 + \cdots \equiv 1 + 2 \cdot 0 + 4 \cdot 1 + \cdots \equiv 5 \pmod 8$

(Remark: we do not have to know $x_3, x_4, \ldots$!)

Express x as $x_0 + 17x_1 + \cdots$, where $0 \le x_i \le 16$.

$$3^x = 3^{x_0+17x_1} \equiv 23 \pmod{137}$$
$$\left(3^{x_0+17x_1+\cdots}\right)^8 \equiv 23^8 \pmod{137}$$
$$(3^8)^{x_0} \cdot (3^{136})^{(x_1+17x_2+\cdots)} \equiv 23^8 \pmod{137}$$
$$122^{x_0} \equiv 34 \pmod{137}$$

n	0	1	2	3	4	5	$\boxed{6}$	7	8	9	10	11	12	13	14	15	16
122^n mod 137	1	122	88	50	72	16	$\boxed{34}$	38	115	56	119	133	60	59	74	123	73

(i.e. $L_3(23) \equiv 6 \pmod{17}$)

Remark: It can be done since 17 is a small prime.

$x \equiv 5 \pmod 8$

$x \equiv 6 \pmod{17}$

By Chinese remainder theorem, $x = 125$.

Baby Step, Giant Step

Solve $\beta \equiv \alpha^x \pmod p$.

(If $\beta = 1$, $x = p-1$ is a solution. Therefore, assume $\beta \ne 1$, then $p-1$ is not a solution.)

Let $N \in \mathbb{Z}^+$ such that $N^2 \ge p-1$ and construct two lists:

1. $\alpha^j \pmod p$ for $0 \le j < N$ (Baby steps)
2. $\beta\alpha^{-kN} \pmod p$ for $0 \le k < N$ (Giant steps)

Look for a match, say $\alpha^{j_0} \equiv \beta\alpha^{-k_0N} \pmod p$.

then $\alpha^{j_0+k_0N} \equiv \beta \pmod p$ i.e. $x = j_0 + k_0N$ is a solution

Question: Why does it always have a match of the two lists?

For a solution $1 \le x \le p-1 < N^2$, there exists $0 \le j, k < N$ such that $x = j + kN$.

Example 5.4

Find an integer x such that $0 \le x \le 29$ and $3^x \equiv 24 \pmod{31}$

Take $N=6$ and so $N^2 = 36 \ge 30 = p-1$.

j	0	1	2	3	4	5
$3^j \pmod{31}$	1	3	9	27	19	26

By extended Euclidean algorithm $3\times 21 + 31 \times(-2) = 1$, i.e. $3\times 21 \equiv 1 \pmod{31}$

and so $3^{-1} \equiv 21 \pmod{31}$

k	0	1	2	3	4	5
$24\cdot 3^{-6k} \pmod{31}$	24	17	3	6	12	24

$3^1 \equiv 3 \equiv 24\cdot 3^{-12} \pmod{31}$

$\therefore\ 3^{13} \equiv 24 \pmod{31}$

Index Calculus

Solve $\beta \equiv \alpha^x \pmod{p}$, where α is a primitive root.

Example 5.5

Find an integer x such that $0 \le x \le 601$ and $7^x \equiv 23 \pmod{137}$

Precomputation Step:

Choose $B \in \mathbb{Z}^+$ (say $B=12$) and

let $p_1, \cdots, p_m$ be primes less than B (in this case, 2, 3, 5, 7, 11)

Compute $\alpha^k \pmod{p}$ for $k = 1, 2, 3, \cdots$ and so on

If $\alpha^k \equiv \prod_{i=1}^{m} p_i^{a_i} \pmod{p}$, then $k \equiv \sum_{i=1}^{m} a_i L_\alpha(p_i) \pmod{p-1}$

Idea: $L_\alpha(p_i)$ for $i=1,2,\cdots,m$ are unknowns,

try to find m linear equations to solve them.

$7^1 \equiv 7 \pmod{601} \Rightarrow L_7(7) \equiv 1 \pmod{600}$

$7^2 \equiv 49 \equiv 7^2 \pmod{601}$ (gives you nothing new!)

$\vdots$

$7^4 \equiv 598 \equiv 2\times 13\times 23 \pmod{601}$ (Discard, since $13, 23 > B = 12$)

$\vdots$

$7^8 \equiv 9 \equiv 3^2 \pmod{601} \Rightarrow 8 \equiv 2L_7(3) \pmod{600}$

(Note $\gcd(2,600) = 2 \neq 1$, so we cannot simply say $4 \equiv L_7(3) \pmod{600}$.

Actually, $8 \equiv 2x \pmod{600}$ has two solutions $x \equiv 4$ or $304 \pmod{600}$.

Try both: $7^4 \equiv 598 \not\equiv 3$, $7^{304} \equiv 3 \pmod{600}$, so $L_7(3) \equiv 304 \pmod{600}$.)

$\vdots$

$7^9 \equiv 63 \equiv 3^2\times 7 \pmod{601}$ (gives you nothing new!)

$\vdots$

$7^{14} \equiv 480 \equiv 2^5\times 3\times 5 \pmod{601} \Rightarrow 14 \equiv 5L_7(2) + L_7(3) + L_7(5) \pmod{600}$

$\vdots$

$7^{18} \equiv 363 \equiv 3\times 11^2 \pmod{601} \Rightarrow 18 \equiv L_7(3) + 2L_7(11) \pmod{600}$

(so $18 \equiv 304 + 2L_7(11) \pmod{600}$

Ex: $L_7(11) \equiv 157 \pmod{600}$)

$\vdots$

$7^{24} \equiv 128 \equiv 2^7 \pmod{601} \Rightarrow 24 \equiv 7L_7(2) \pmod{600}$

(Note $\gcd(7,600) = 1$ and $7^{-1} \equiv 343 \pmod{600}$

$\therefore L_7(2) \equiv 7^{-1}\times 24 \equiv 343\times 24 \pmod{600}$

$L_7(2) \equiv 432 \pmod{600}$)

By $14 \equiv 5L_7(2) + L_7(3) + L_7(5) \pmod{600}$

$\equiv 5\cdot 432 + 304 + L_7(5) \pmod{600}$

$\therefore L_7(5) \equiv 550 \pmod{600}$

Computation of Discrete Logs

Compute $\beta\cdot\alpha^k \pmod p$ for $k = 1, 2, 3, \cdots$ and so on

If $\beta\cdot\alpha^k \equiv \prod_{i=1}^{m} p_i^{b_i} \pmod p$, then $L_\alpha(\beta) \equiv -k + \sum_{i=1}^{m} b_i L_\alpha(p_i) \pmod{p-1}$

$23 \times 7^1 \equiv 23 \times 7 \pmod{601}$ (Discard, since $23 > B = 12$)

$23 \times 7^2 \equiv 526 \equiv 2 \times 263 \pmod{601}$ (Discard again)

$\vdots$

$23 \times 7^6 \equiv 225 \equiv 3^2 \times 5^2 \pmod{601}$

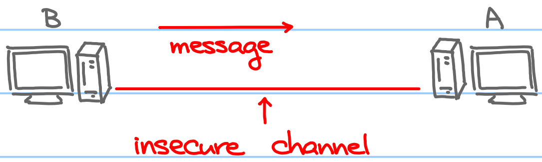
$\therefore L_7(23) \equiv -6 + 2L_7(3) + 2L_7(5) \equiv 502 \pmod{600}$

Remark: Once the precomputation is done, it can be reused.

Exercise 5.1

Compute $L_7(123)$. Ans: 483

The ElGamal Cryptosystem



Algorithm:

1) A chooses a large prime and a primitive root α.

2) A chooses a secret integer d and compute $\beta \equiv \alpha^d \pmod p$

3) A sends (p, α, β) to B.

4) Suppose that the message is an integer m such that $0 \le m < p$.
   B chooses a random integer k and computes $r \equiv \alpha^k \pmod p$ and $t \equiv \beta^k m \pmod p$,
   then B sends (r, t) back to A.

5) A decrypts by computing
$$\begin{aligned} tr^{-d} &\equiv (\beta^k m)\cdot(\alpha^k)^{-d} && \pmod p \\ &\equiv ((\alpha^d)^k m)\cdot \alpha^{-kd} && \pmod p \\ &\equiv m && \pmod p \end{aligned}$$

If a person E gets p, α, β, r, s, in order to obtain m:

1) Solve d from $\beta \equiv \alpha^d \pmod p$;

2) Solve k from $r \equiv \alpha^k \pmod p$, then $m \equiv t(\beta^k)^{-1} \pmod p$

However, both involve discrete logarithm problems (Assume to be difficult).

Computing Discrete Logs Mod 4

Let p be an odd prime. Then, we either have $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$

For the case $p \equiv 1 \pmod 4$, $p-1$ is divisible by 4.

The Pohlig-Hellman algorithm provides a way to find $L_\alpha(\beta)$ modulo 4.

For the case $p \equiv 3 \pmod 4$, $p-1$ is only divisible by 2 but not 4.

Trouble with using the Pohlig-Hellman algorithm:

Suppose that $\beta \equiv \alpha^x \pmod p$ and $x = x_0 + 2x_1 + 4x_2 + \cdots$, where $0 \le x_i \le 1$.

x_0 can be determined (see example 5.3)

$$\beta \cdot \alpha^{-x_0} \equiv \alpha^{2x_1 + 4(x_2 + 2x_3 + \cdots)} \pmod{p-1}$$

We cannot raise both sides to the power $\frac{p-1}{4}$!

Also, there is one more reason why we believe that computing $L_\alpha(\beta)$ mod 4 is hard for primes $p \equiv 3 \pmod 4$

Lemma 5.1

Let $p \equiv 3 \pmod 4$ be prime, let r, y be integers and $r \ge 2$

Suppose that α and γ are nonzero integers such that $\gamma \equiv \alpha^{2^r y} \pmod p$,

then $\gamma^{\frac{p+1}{4}} \equiv \alpha^{2^{r-1} y} \pmod p$.

proof:

$$\gamma^{\frac{p+1}{4}} \equiv (\alpha^{2^r y})^{\frac{p+1}{4}} \equiv \alpha^{2^{r-2}(p+1)y} \equiv \alpha^{2^{r-2}(p-1)y} \cdot \alpha^{2^{r-1}y} \equiv \alpha^{2^{r-1}y} \pmod p$$

Suppose that there is an efficient way to find $L_\alpha(\beta)$ for any given β.

If $\beta \equiv \alpha^x \pmod p$ and $x = x_0 + 2x_1 + 4x_2 + \cdots$, where $0 \le x_i \le 1$.

then x_0 and x_1 can be determined We also claim that x_r for $r \ge 2$ can also be found.

Assume $x_0, x_1, \cdots, x_{r-1}$ with $r \ge 2$ are known, then

$$\beta_r \equiv \beta \cdot \alpha^{-(x_0 + 2x_1 + \cdots + 2^{r-1}x_{r-1})} \equiv \alpha^{2^r(x_r + 2x_{r+1} + \cdots)} \pmod p$$

Apply Lemma 5.1 $r-1$ times

$$\beta_r^{\left(\frac{p+1}{4}\right)^{r-1}} \equiv \alpha^{2(x_r + 2x_{r+1} + \cdots)} \pmod p$$

$$2x_r \equiv L_\alpha\left(\beta_r^{\left(\frac{p+1}{4}\right)^{r-1}}\right) \pmod 4$$

$\therefore x_r$ can be found

That means: for primes $p \equiv 3 \pmod 4$

Finding $L_\alpha(\beta) \bmod 4$ is "easy" $\Rightarrow$ Finding $L_\alpha(\beta)$ is "easy"

However, we believe finding $L_\alpha(\beta)$ is "hard", so is finding $L_\alpha(\beta) \bmod 4$

Bit Commitment

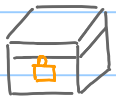
Think:

A: I have a method to predict the outcome of football games (for simplicity, win or lose),
do you want to buy it?

B: Sure, if you can prove by predicting the result of the game this weekend.

A: No way! You will simply make your bets without paying me.

Solution:

A [Result 0 or 1] $\longrightarrow$  $\longrightarrow$ B

A writes down the result, put it in a box, lock it

then A sends the locked box to B

(Remark: While B cannot open the box, A cannot change his prediction.)

A  $\longrightarrow$ B

After the game, A sends the key to B and B can verify the prediction of A.

Algorithm to implement in mathematical way:

1) A and B agree on a large prime $p \equiv 3 \pmod 4$ and a primitive root α.

2) A chooses integer $1 < x < p-1$ (key) such that x_1 which is the prediction.

3) A sends $\beta \equiv \alpha^x \pmod p$ (locked box) to B

(Remark: Assume B cannot compute $L_\alpha(\beta) \pmod 4$)

4) After the game, A sends x to B, B can compute x_1 to verify the prediction of A.
and also check $\beta \equiv \alpha^x \pmod p$ to make sure A has not changed his prediction by sending another x since the above equation has a unique solution modulo $p-1$.