Number Theory (II)

Cunsheng Ding

HKUST, Hong Kong

November 10, 2015

Contents

The Discrete Logarithm Modulo p

Definition 1

Let p be a prime and a be a primitive root of p. Then any integer b with $1 \leq b \leq p-1$ can be uniquely expressed as $b = a^i \bmod p$, where $0 \leq i \leq q-2$. The index i is called the discrete logarithm of b to the base a, and denoted by $\log_a(b)$.

Example 2

2 is a primitive root of 11. It is easily verified that $\log_2(6) = 9$.

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

The Discrete Logarithm Problem Modulo p

Conclusion

Let a be a primitive root of a prime p. Given a and p, it is easy to compute $a^i \bmod p$ for any $i \in \mathbb{N}$.

Fast exponentiation algorithm

Let $i = 48$. The brute force computation of $a^{48} \bmod p$ takes 47 multiplication. However, Noticing that $i = 2^5 + 2^4$. We have

$$a^{48} \bmod p = ((((a^2)^2)^2)^2)^2 \times (((a^2)^2)^2)^2 \bmod p.$$

This takes only 10 multiplications.

The Discrete Logarithm Problem Modulo p

Definition 3 (Discrete Logarithm Problem Modulo p)

Let p be a prime and a be a primitive root of large prime p. The problem is to compute $\log_a(b)$ for any b with $1 \leq b < p-1$.

Comments

- The discrete logarithm problem (DLP) is believed to be hard in the computational sense for large prime p. But it is still open if this is a hard problem.
- The DLP has many applications, and is a fundamental problem in mathematics and computer science.

Diffie-Hellman Key Exchange Protocol

Protocol parameters

Let p be large prime with at least 130 digits, and α be a primitive root of p.

DH protocol

Step 1: Alice picks up her private number X_A with $1 \leq X_A < p$ at random. Bob picks up his private number X_B with $1 \leq X_B < p$ at random.

Step 2: Alice computes $Y_A = \alpha^{X_A} \bmod p$ and Bob computes $Y_B = \alpha^{X_B} \bmod p$.

Step 3: Alice and Bob exchange their Y_A and Y_B via a public communication channel.

Step 4: Alice computes $Y_B^{X_A} \bmod p$, and Bob computes $Y_A^{X_B} \bmod p$.

$k := Y_B^{X_A} \bmod p = Y_A^{X_B} \bmod p$ is the common secret number established by Alice and Bob.

Security of the Diffie-Hellman Key Exchange Protocol

Question 1

Suppose an adversary has intercepted Y_A and Y_B in the communication channel, and has knowledge of p and α. Can he/she compute the secret number k?

Statement

If the discrete logarithm problem modulo p is hard, it should be computationally infeasible for the adversary to compute the secret number.

Linear Congruences Modulo n

Proposition 4

If $\gcd(a, n) = 1$*, then the equation* $ax \equiv b \pmod{n}$ *has a solution, and the solution is unique modulo n.*

Proof.

Since $\gcd(a, n) = 1$, a has the multiplicative inverse modulo n, denoted by a^{-1}.
Then $x = a^{-1}b$ is a solution of the congruence $ax \equiv b \pmod{n}$.
We now prove the uniqueness of the solution. Let x_1 and x_2 be two solutions of the equation $ax \equiv b \pmod{n}$. Then we have

$$ax_1 \equiv b \pmod{n} \text{ and } ax_2 \equiv b \pmod{n}.$$

It then follows that $a(x_1 - x_2) \equiv 0 \pmod{n}$. Multiplying both sides of the equation with a^{-1} yields $x_1 \equiv x_2 \pmod{n}$. $\square$

Linear Congruences Modulo n

Proposition 5

The equation $ax \equiv b \pmod{n}$ *has a solution if and only if* $\gcd(a, n)$ *divides* b.

Proof.

Let $g = \gcd(a, n)$. If there is a solution x to the equation $ax \equiv b \pmod{n}$, then n divides $ax - b$. Hence, g divides $ax - b$. Since g divides a, it must divide b. Conversely, suppose that g divides b. Then x is a solution to $ax \equiv b \pmod{n}$ if and only if x is a solution to

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{n}{g}}. \tag{1}$$

Note that $\frac{a}{g}$ and $\frac{n}{g}$ are relatively. Let $\frac{a}{g}^{-1}$ denote the inverse of $\frac{a}{g}$ modulo $\frac{n}{g}$. Then $x = \frac{a}{g}^{-1}\frac{b}{g}$ is a solution of (1). □

The Original Chinese Remainder Problem

Sun Zi Suanjing (Problem 26, Volume 3), the first century A.D.

> *"We have a number of things, but do not know exactly how may. If we count them by threes we have two left over. If we count them by fives we have three left over. If we count them by sevens we have two left over. How many things are there?"*

In modern terminology the problem is to find a positive integer x such that

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

Question 2

How do you solve this problem?

Sun Zi's Solution

The first step is to compute a value for the following s_0, s_1 and s_2:

$$s_0 \equiv 0 \pmod 5 \equiv 0 \pmod 7 \equiv 1 \pmod 3,$$
$$s_1 \equiv 0 \pmod 3 \equiv 0 \pmod 7 \equiv 1 \pmod 5,$$
$$s_2 \equiv 0 \pmod 5 \equiv 0 \pmod 3 \equiv 1 \pmod 7.$$

He took $s_0 = 70, s_1 = 21$ and $s_2 = 15$. Since 5 and 7 divide s_0, s_0 must be of the form $7 \times 5 \times k = 35k$, where k is an integer. Hence s_0 mod $3 = 2k$ mod 3, and $k = 2$ gives $s_0 = 70$. s_1 and s_2 were similarly computed. The second step is to compute

$$s_0' = 2s_0 = 140, \quad s_1' = 3s_1 = 63, \quad s_2' = 2s_2 = 30.$$

The last step is to compute $x = (s_0' + s_1' + s_2')$ mod $105 = 23$.

The Chinese Remainder Problem in General

Chinese Remainder Problem

Let $m_1, m_2, \cdots, m_n$ be n positive integers that are pairwise relatively prime. Find an integer x such that

$$x \equiv r_i \pmod{m_i}, \quad i = 1, 2, \cdots, n, \tag{2}$$

where $r_1, r_2, \cdots, r_n$ are any set of integers with $0 \le r_i < m_i$.

Question 3

1. *Does the set of congruences have a solution?*
2. *Is the solution unique?*
3. *How do you find a specific solution x?*

Chinese Remainder Theorem

Theorem 6 (Chinese Remainder Theorem)

For any set of integers $\{r_1, r_2, \ldots, r_n\}$*, the Chinese Remainder Problem has a unique solution* x *with* $0 \leq x < M$*, where* $M = \prod_{i=1}^{n} m_i$*.*

Proof of the uniqueness of the solution x

Let x_1 and x_2 be two solutions. Then $x_1 - x_2 \equiv \pmod{m_i}$ for all i. This means that $m_i \mid (x_1 - x_2)$ for all i. It then follows that the least common multiple $\mathrm{lcm}\{m_1, m_2, \ldots, m_n\}$ divides $x_1 - x_2$. It is easy to show that

$$\mathrm{lcm}\{m_1, m_2, \ldots, m_n\} = \prod_{i=1}^{n} m_i = M.$$

Whence $x_1 - x_2 \equiv 0 \pmod{M}$.

Remark

We will prove the CRP has a solution in two different ways subsequently.

An Existence Proof of the CRT

Proof.

Define a function f from $\mathbb{Z}_M$ to $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$ by

$$f(x) = (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_n).$$

Due to the uniqueness of the solution x to the Chinese Remainder Problem, this function is one-to-one. Note that

$$|\mathbb{Z}_M| = |\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}|.$$

The function f is a one-to-one correspondence. Hence, the CRP has a solution. □

Remark

This existence proof does not give the specific solution. In the next slide, we will give a constructive proof, which can be developed into an algorithm for computing the solution x.

Chinese Remainder Algorithm

Theorem 7

Let $m_1, \cdots, m_n$ be n positive integers that are pairwise relatively prime. For any set of integers $r_1, \cdots, r_n$ with $0 \le r_i < m_i$, there is an unique integer $0 \le x < M$ such that

$$x \equiv r_i \pmod{m_i}, \quad i = 1, 2, \cdots, n. \tag{3}$$

Furthermore,

$$x = \left(\sum_{i=1}^{n} r_i u_i M_i \right) \bmod M, \quad M = \prod_{i=1}^{n} m_i, \quad M_i = \frac{M}{m_i}$$

and u_i is the multiplicative inverse of M_i mod m_i, i.e., $u_i M_i \equiv 1 \pmod{m_i}$.

Chinese Remainder Algorithm

Proof.

Recall that

$$x = \left(\sum_{i=1}^{n} r_i u_i M_i\right) \bmod M, \quad M = \prod_{i=1}^{n} m_i, \quad M_i = \frac{M}{m_i}$$

and u_i is the multiplicative inverse of $M_i \bmod m_i$.
Note that $M_j \bmod m_i = 0$ for all (i, j) with $i \neq j$. We have then

$$x \bmod m_i = r_i u_i M_i \bmod m_i = r_i \bmod m_i = r_i$$

for all i. □

Some Applications of the Chinese Remainder Theorem

Some applications

- Solving the discrete logarithm problem (Pholig-Hellman algorithm).
- Cryptography (secret sharing, speeding up the decryption of RSA).
- Signal processing.
- Coding theory.
- Computing.

Reference

C. Ding, D. Pei, A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography,* World Scientific, Singapore, 1996.

The Base b Representation of n

Definition 8

Let $b \geq 2$ and $n \geq 0$ be nonnegative integers. The **base-b representation** of n is defined to be the following sequence

$$n = (n_{k-1} n_{k-2} \cdots n_1 n_0)_b$$

if and only if for some $k \geq 1$

$$n = n_{k-1} b^{k-1} + n_{k-2} b^{k-2} + \cdots + n_1 b + n_0,$$

where each $n_i \in \{0, 1, \cdots, b-1\}$.

Remarks

The representation is **unique** if and only if we require that $n_{k-1} \neq 0$.

The Base b Representation of n

Popular bases

Base b is called

- **binary** if $b = 2$ (computer science and communication engineering);
- **ternary** if $b = 3$;
- **octal** if $b = 8$;
- **decimal** if $b = 10$ (school base); and
- **hexadecimal** if $b = 16$ (computer science).
  - In this case, we use $A = 10$, $B = 11$, $C = 12$, $D = 13$, $E = 14$, and $F = 15$ in the hexadecimal representation.

The Base b Representation of n

Examples

1. $17 = (10001)_2$, as $17 = 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 0 \times 2 + 1$.
2. $4879 = (4879)_{10}$, as $4879 = 4 \times 10^3 + 8 \times 10^2 + 7 \times 10 + 9$.
3. $10705679 = (A35B0F)_{16}$, as

$$10705679 = 10 \times 16^5 + 3 \times 16^4 + 5 \times 16^3 + 11 \times 16^2 + 0 \times 16 + 15.$$

The Base b Representation of n

How to determine the base-b representation

Suppose that
$$n = n_{k-1}b^{k-1} + n_{k-2}b^{k-2} + \cdots + n_1 b + n_0.$$

Then $n_0 = n \bmod b$ and for each $i \geq 1$ we have
$$n_i = \left(\left(n - \sum_{j=0}^{i-1} n_j b^j \right) \div b^i \right) \bmod b.$$