Number Theory: II

李昂生

Discrete Mathematics
U CAS
17th April, 2018

Outline

1. Background
2. Relatively prime （互素）
3. Solving congruences （解同余式）
4. Euler’s function （欧拉函数）
5. Algebraic fundamental theorem （代数基本定理）
6. Primitive roots （原根）
7. Exercises

General views

- Further understanding of the concept of numbers
- From number theory to advanced mathematics, the base of mathematics
- From mathematics to research projects in computer science

Greatest Common Divisor

Definition 1

Given integers a, b, the *greatest common divisor* (GCD, for short) of a and b is the largest natural number d such that both $d|a$ and $d|b$ hold.

We use (a, b) to denote the greatest common divisor of a and b.

Definition 2

Given integers a and b, we say that a, b are *relatively prime*, if

$$(a, b) = 1.$$

Least Common Multiple

Definition 3

Given a, b, we define the *least common multiple* (LCM, for short) of a and b to be the least natural number x such that both $a|x$ and $b|x$ hold.

We use $[a, b]$ to denote the least common multiple of a and b.

Understanding

Suppose

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}, \ \alpha_j \geq 0$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_l^{\beta_l}, \ \beta_j \geq 0$$

For each j,

$$\gamma_j = \min\{\alpha_j, \beta_j\}$$
$$\delta_j = \max\{\alpha_j, \beta_j\}$$

Then:

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_l^{\gamma_l} \tag{1}$$

$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_l^{\delta_l} \tag{2}$$

Theorem

For $\alpha, \beta \geq 0$,
$\gamma = \min\{\alpha, \beta\}$, $\delta = \max\{\alpha, \beta\}$, then

$$\alpha + \beta = \gamma + \delta.$$

Therefore,

Theorem 4

Let a, b be natural numbers. Then,

$$ab = (a, b) \cdot [a, b].$$

The Euclidean Algorithm

Lemma 5

Given natural numbers a and b, suppose that

$$a = qb + r,\ 0 \leq r < b.$$

Then:

$$x|a\ \&x|b \iff x|b\ \&\ x|r, \tag{3}$$

giving

$$(a, b) = (b, r). \tag{4}$$

The Algorithm $\mathcal{E}$

Let $a \geq b$ be natural numbers. Let $r_0 = a$, $r_1 = b$. Suppose that

$$\begin{aligned} r_0 &= q_0 r_1 + r_2, 0 < r_2 < r_1 \\ r_1 &= q_1 r_2 + r_3, 0 < r_3 < r_2 \\ \ldots & \\ r_{k-2} &= q_{k-2} r_{k-1} + r_k, 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k-1} r_k + r_{k+1},\ r_{k+1} = 0. \qquad (5) \end{aligned}$$

Therefore,

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_k, r_{k+1}) = (r_k, 0) = r_k. \qquad (6)$$

The time complexity

For $a \geq b$, if $a = qb + r$ with $0 \leq r < b$, then $a \geq b + r > 2r$.
Therefore, for each $j \geq 1$,

$$r_{j+2} < \frac{1}{2} \cdot r_j.$$

The number k in the Euclidean algorithm $\mathcal{E}$ is at most $2 \log b$.
The complexity for each division is $O(\log^2 b)$.
The total time complexity of $\mathcal{E}$ is

$$O(\log^3 b).$$

The space complexity

In each division, we will need to restore the current r_j and r_{j+1}, for which the space complexity is

$$O(\log_2 a).$$

Bézout Theorem

Theorem 6

For natural numbers a and b, there exist integers s and t satisfying the following Bézout identity

$$(a, b) = sa + tb, \tag{7}$$

in which s and t are called the Bézout coefficients.

Proof.

$(a, b) = r_k$,
$r_k = r_{k-2} - q_{k-2}r_{k-1}$, and each r_j can be expressed by a linear combination of r_{j-1} and r_{j-2}. This leads to

$$(a, b) = r_k = sa + tb$$

for some integers s and t. □

Relatively prime and multiplication inverse

For natural numbers a, m, if a and m are relatively prime, then there exist s and t such that

$$sa + tm = 1.$$

Therefore

$$sa \equiv 1 \bmod m.$$

This means that $s \bmod m$ is the multiplication inverse of a modulo m, written

$$a^{-1} = s \bmod m.$$

Understanding

- Primality is hard
- Relative primality is easy
  Why? The idea of relativity
- **The Key**:

$$\textit{Relatively prime} = \textit{Inverse} \tag{8}$$

The role of relatively prime

Theorem 7

Let a, b, c, m be natural numbers.

(1) *If $(a, b) = 1$ and $a|bc$, then $a|c$.*

(2) *If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$.*

Proof.

For (1). $(a, b) = 1$ means that a and b do not share any prime factor, so that if $a|bc$, then every factor of a is a factor of c, giving rise to $a|c$.

For (2). Since $(c, m) = 1$, c^{-1} modulo m exists. Using $ac \equiv bc$, we have $acc^{-1} \equiv bcc^{-1}$, implying $a \equiv b \bmod m$. □

Linear congruence

For natural number m, a linear congruence is an equation of the following form:

$$ax \equiv b \pmod{m}. \tag{9}$$

Remark:
If $a^{-1} \bmod m$ exists and equals s, that is, $a^{-1} = s \bmod m$, then the linear congruence has a solution

$$x = a^{-1} b \equiv sb \bmod m. \tag{10}$$

Equivalence

More importantly, this becomes the only case that a linear congruence has a solution.

Theorem 8

Let a, m be integers and $m > 1$. Then:

$$a^{-1} \bmod m \textit{is defined} \iff (a, m) = 1, \tag{11}$$

where a^{-1} is for modulo m.

Proof.

If $a^{-1} \bmod m$ exists and equal s, then $a \cdot s \equiv 1 \bmod m$, so there is a t such that

$$a \cdot s - 1 = t \cdot m.$$

So $a \cdot s - t \cdot m = 1$, $(a, m) = 1$ follows. □

Special attention

The theorem provides the **KEY** for us to solve

- linear congruence
- systems of linear congruences

Question is, however, what happens for non-linear congruence?

Chinese Remainder Theorem

Theorem 9

Let $m_1, m_2, \cdots, m_k$ be natural numbers greater than 1 that are pairwise relatively prime.
Then for every k-tuple $(a_1, a_2, \cdots, a_k)$, the system of linear congruences of the following form

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{12}$$

has a unique solution modulo m $(= \prod_{i=1}^{k} m_i)$.

Uniqueness

Assume $0 \le x, y < m$.
Suppose that

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{13}$$

$$\begin{cases} y \equiv a_1 \pmod{m_1} \\ \dots \\ y \equiv a_k \pmod{m_k} \end{cases} \tag{14}$$

Uniqueness - continued

Then, there exist $t_1, t_2, \cdots, t_k$ such that

$$\begin{cases} m_1 t_1 = x - y \\ \dots \\ m_k t_k = x - y \end{cases} \tag{15}$$

which implies that

$$m | (x - y)$$

giving $x = y$.

Existence

For $j \in [k] = \{1, 2, \cdots, k\}$, define

$$M_j = \frac{m}{m_j}.$$

Then $(M_j, m_j) = 1$.
Let s_j be such that

$$s_j M_j \equiv 1 \pmod{m_j}, j = 1, 2, \cdots, k. \tag{16}$$

Let

$$x = a_1 s_1 M_1 + a_2 s_2 M_2 + \cdots + a_k s_k M_k.$$

Then for each j,

$$x \equiv a_j \pmod{m_j}.$$

Theorem

(1) For prime p,

$$\phi(p) = p - 1. \tag{17}$$

(2) For natural number n,

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}), \tag{18}$$

where the production is over all prime factors p of n.

(3) If $(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n). \tag{19}$$

Theorem - continued

(4) If p is prime,

$$\phi(p^k) = p^k - p^{k-1}. \tag{20}$$

(5) If $p_1, p_2, \cdots, p_k$ are distinct primes, and $n = p_1 p_2 \cdots p_k$, then

$$\phi(n) = \prod_{i=1}^{k} (p_i - 1). \tag{21}$$

(6) If $n = m_1 m_2 \cdots m_k$ for distinct numbers that are relatively prime, then for each k-tuple $(r_1, \cdots, r_k) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$, there is a unique $r \in \Phi(n)$ such that for each i,
$r \equiv r_i \mod m_i$.
(Chinese Remainder Theorem revisit)

Theorem - continued

(7)

$$\sum_{m|n} \phi(m) = n. \tag{22}$$

(8) (Fermat's Theorem) For prime p, for each a, with $1 \leq a < p$,

$$a^{p-1} \equiv 1 \bmod p. \tag{23}$$

(Using this, it is easy to compute $a^n \bmod p$.)

(9) For each natural number n and each $a \in \Phi(n)$,

$$a^{\phi(n)} \equiv 1 \pmod{n}. \tag{24}$$

Prof of (1)

Let p be prime. Clearly, for each x, if $1 \leq x < p$, then $(x, p) = 1$. This gives $\phi(p) = p - 1$.

Proof of (2)

Given n, suppose that $p_1, \cdots, p_k$ are all the distinct prime factors of n. Let $L_0 = \{1, 2 \cdots, n\}$. In L_0, the numbers of the form ip_1 for i from 1 to some number n_1 that are not relatively prime to n are deleted from L_0 . This cancels $\frac{1}{p_1}$ fraction of the numbers in L_0. Let L_1 be the set of the remaining elements of L_0 after the cancellation of the form ip_1. Then the size of L_1 is $n(1 - \frac{1}{p_1})$. In L_1, there are numbers of the form ip_2, which are not relatively prime to n. We cancel these numbers, giving a remaining set L_2. Then the size of L_2 is $n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})$. Repeating the procedure, we get a set L_k such that

- In L_k, there is no number x of the form mp_i for any $i \in \{1, 2, \cdots, k\}$ and any m. Therefore, every $x \in L_k$ is relatively prime to n.
- $|L_k| = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$.

(2) follows.

Proof of (2) - again

We will give another proof of the result by inclusion/exclusion principle in combinatorics.

Proof of (3)

(3) If $(m, n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$.

Proof.
By (2),

$$\begin{aligned} \phi(mn) &= m \cdot n \prod_{p|mn} (1 - \frac{1}{p}) \\ &= (m \prod_{p|m} (1 - \frac{1}{p})) \cdot (n \prod_{p|n} (1 - \frac{1}{p})), \end{aligned} \tag{25}$$

where p is a prime and the second equation is due to the fact that m and n share no common prime factor.

□

Proof of (4)

Proof.

By A(2),

$$\begin{aligned}\phi(p^k) &= p^k(1-\frac{1}{p}) \\ &= p^k - p^{k-1}\end{aligned}$$

□

Proof of (5)

Combining (1) and (3),

$$\begin{aligned}\phi(n) &= \prod_{i=1}^{k} \phi(p_i) \\ &= \prod_{i=1}^{k} (p_i - 1).\end{aligned}$$

Proof of (6)

Proof.

Clearly,

$$|\mathbb{Z}_n| \quad = \quad |\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}|. \tag{26}$$

There is a one-to-one map between $\mathbb{Z}_n$ and $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$. This means that a large number in $\mathbb{Z}_n$ can be encoded by a k-tuple in $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ in which each coordinate is small. Clearly, the function defined below is such a map:

$$\begin{array}{rcl} \mathbb{Z}_n & \rightarrow & \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \\ r \in \mathbb{Z}_n & \mapsto & (r \bmod m_1, \cdots, r \bmod m_k) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}. \end{array}$$

The proof of the one-to-oneness of the map uses the assumption that $m_1, \cdots, m_k$ are pairwise relatively prime.

□

Proof of (7)

Proof.

Let $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ be the prime factoring of n. Set $\phi(1) = 1$. By (4),

$$\phi(1) + \phi(p^1) + \phi(p^2) + \cdots + \phi(p^k) = p^k. \tag{27}$$

By (3),

$$\begin{aligned} n &= p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l} \\ &= \prod_{i=1}^{k} (\phi(1) + \phi(p_i) + \cdots + \phi(p_i^{k_i}) \cdot \\ &= \sum_{0 \le \alpha_i \le k_i, i=1,2,\cdots,l} \phi(p_1^{\alpha_1}) \phi(p_2^{\alpha_2}) \cdots \phi(p_l^{\alpha_l}) \\ &= \sum_{m|n} \phi(m). \end{aligned} \tag{28}$$

Proof of (8)

Proof.

By (1), $\Phi(p) = \{1, 2, \cdots, p-1\}$.

For $a \in \Phi(p)$, define the set

$$a \cdot \Phi(p) = \{a \cdot 1, a \cdot 2, \cdots, a \cdot (p-1)\}.$$

Since $(a, p) = 1$,

$$a \cdot \Phi(p) = \Phi(p).$$

By multiplying the elements in the two sets,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Since $((p-1)!, p) = 1$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

For (9)

By the proof of (8). That is:
For every $a \in \Phi(n)$,

$$a \cdot \Phi(n) = \Phi(n)$$

and

$$a^{\phi(n)} \cdot \prod_{x \square \Phi(n)} x = \prod_{x \square \Phi(n)} x \pmod{n}$$

giving

$$a^{\phi(n)} = 1 \pmod{n}$$

due to the fact that $(\prod_{x \square \Phi(n)} x)$ is relatively prime to n.

Group revisit

A set G with an operation $*$, satisfying:

- Closure
- Identity and inverse
- Associativity

Finite groups

1. $(\mathbb{Z}_n, +)$
2. $(\mathbb{Z}_2, +)$: here + is XOR
3. S_n: the set of permutations on $[n] = \{1, 2, \cdots, n\}$, $*$ is function composition.
4. $(\mathbb{Z}_2)^n$: n-bit strings with $*$ being bitwise XOR
5. $\mathbb{Z}_n^{\square} = \{k \mid 1 \leq k < n, (k, n) = 1\}$.
   Inverse is found by Euclidean algorithm. We know: $\phi(p) = p - 1$, and $|\mathbb{Z}_n^{\square}| = \phi(n)$.

Finite Group Fundamental Theorem

Theorem 11

If G is a finite group, and H is a subgroup of G, then

$$|H| \mid |G|. \tag{29}$$

Proof.

For $a \in G$, define $aH = \{ax \mid x \in G\}$.

1. $|aH| = |H|$
2. For $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$.
3. the union of aH for all a's is G.

Therefore, G is partitioned into several parts each of which has size $|H|$. $|H|$ divides $|G|$.

□

Fermat's Little Theorem - Revisit

Consider $G = \langle \mathbb{Z}_n^{\square}, \cdot \rangle$. Recall $\mathbb{Z}_n^{\square} = \Phi(n)$, and that G is a group. For $x \in \Phi(n)$, set

$$H = \{x^l \mid l \in \mathbb{Z}\}.$$

Then
1) H is a subgroup of G,
2) $|H|$ is the least $k > 0$ such that $x^k = 1 \pmod{n}$.
Therefore,

- $x^{|H|} = 1 \pmod{n}$, by definition, and
- $|H|\ |\phi(n)$, implying $x^{\phi(n)} \equiv 1 \pmod{n}$. (by finite group fundamental theorem)

Order

Definition 12

Let $\langle G, \cdot \rangle$ be a finite group. For every $x \in G$, we define the **order** of x in G to be the least natural number k such that $x^k = 1$.

Therefore, for a finite group $\langle G, \cdot \rangle$,

1) Every $x \in G$ has an order, and
2) For every $x \in G$, the order of x in G divides the size $|G|$ of G.

Cyclic group and generator

Definition 13

Let $\langle G, \cdot \rangle$ be a group (finite or infinite). If there is an element $g \in G$ such that

$$G = \{g^l \mid l \geq 0\}, \tag{30}$$

then $\langle G, \cdot \rangle$ is called a **cyclic group**.
In this case, we call g a **generator** of $\langle G, \cdot \rangle$ (or simply G).

Fields

Definition 14

A *field* is a set $\mathbb{F}$ (finite or infinite) with two operations, namely, addition + and multiplication $\cdot$, written $(\mathbb{F}, +, \cdot)$, such that the following properties are satisfied:

1) Associativity, commutativity, and distributive laws all hold to both + and $\cdot$.
2) Identity and inverse hold for both + and $\cdot$.

Examples:

- $\mathbb{Q}$: Rational numbers with + and ×
- $\mathbb{R}$: Real numbers with + and ×
- $\mathbb{C}$: Complex numbers with + and ×.

Finite Fields

- Prime fields
  $$\mathbb{Z}_p, \text{ or written as } \mathrm{GF}(p),$$
  for each prime p. In Particular, we have $\mathrm{GF}(2)$, for which $+$ is XOR and multiplication $\cdot$ is AND
- Non-prime fields
  $$\mathrm{GF}(p^k),$$
  which is
  $$\mathrm{GF}(p) \times \cdots \times \mathrm{GF}(p),$$
  for k times.
  – elements are of the form $(a_1, a_2, \cdots, a_k)$ with operation $+$ to be the coordinate plus mod p,
  – the multiplication $\times$ is unusual, which we don't usually use in Computer Science

In CS, sometimes we use the finite $GF(2^k)$.

Algebraic Fundamental Theorem

Theorem 15

For a prime p, in the field $\mathbb{Z}_p$, for any polynomial $P(x)$ of degree k, if $P(x) \not\equiv 0$, then $P(x)$ has at most k roots in $\mathbb{Z}_p$.

By induction on k. $k = 0$ is the trivial case.
For $k > 0$. Suppose by induction that the theorem holds for all $k^{\prime} < k$.
Suppose to the contrary that
$\pi(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots a_1 x + a_0$ for $a_k \neq 0 \pmod{p}$ has $k + 1$ distinct roots $x_1, x_2, \cdots, x_{k+1} \in \mathbb{Z}_p$.

Proof

Set

$$\pi^{\Box}(x) = \pi(x) - a_k(x - x_1)\cdots(x - x_k).$$

Then,

- $\pi^{\Box}(x)$ has degree $\leq k - 1$
- $\pi^{\Box}(x_{k+1}) = -a_k(x_{k+1} - x_1)\cdots(x_{k+1} - x_k) \not\equiv 0 \pmod{p}$
- However, $\pi^{\Box}(x)$ has k roots $x_1, x_2, \cdots, x_k$. A contradiction.

General field

The algebraic fundamental theorem holds for the polynomials over all fields.

Algebraic Fundamental Theorem- continued

The Theorem holds for all fields.
Significance is many-fold.
In particular, it leads to new mathematics of the following form:
According to the Algebraic Fundamental Theorem, we have:
For any finite field $\mathbb{F}$ of size p, $\mathbb{Z}_p$ for prime p say. Let $P(x)$ be a polynomial of degree d, that is implicitly given.
Here $d << p$.

The tester $\mathcal{T}$

We test whether or not $P(x)$ is identically zero as follows.
Tester $\mathcal{T}$:

(1) Randomly and uniformly picks an element $a \in \mathbb{F}$, written $a \in_{\mathrm{R}} \mathbb{F}$, in which R stands for Randomly.

(2) If $P(a) = 0$, then accepts, and rejects otherwise.

Key The tester $\mathcal{T}$ queries only one value of P at her randomly picked point a.

The tester $\mathcal{T}$- Proofs

Completeness If $P \equiv 0$, then
$\mathcal{T}$ accepts with probability 1.
Soundness Otherwise.
Then, the probability that $\mathcal{T}$ accepts is at most

$$\frac{k}{p},$$

which is small.
Remark:
(i) $\frac{k}{p}$ could be arbitrarily small, since k is much less than p
(ii) $\mathcal{T}$ can principally decide whether or not $P \equiv 0$ by simply reading one value of P.
(iii) This leads to a research project in the current state of the art, which could be called local algorithms.

Definition

Definition 16

Given a natural number n, and an element $a \in \mathbb{Z}_n^{\square} = \Phi(n)$, we say that a is a *primitive root module n*, if:

$$\mathbb{Z}_n^{\square} = \{a^l \mid l \geq 0\}. \tag{31}$$

Remark: A primitive root module n is an element in the finite group $\mathbb{Z}_n^{\square}$ having order $\phi(n)$, and is a generator of the group $\mathbb{Z}_n^{\square}$.

Primitive Root Theorem

Theorem 17

For every prime p, there is a primitive root r modulo p, that is, r generates the finite group $\mathbb{Z}_p^{\square}$, or equivalently,

$$\mathbb{Z}_p^{\square} = \{r^l \mid l \geq 0\}.$$

Proof of the Primitive Root Theorem - I

Fix a prime p. We consider $\mathbb{Z}_p^{\star} = \Phi(p)$.
For $m \in \Phi(p)$, we define the *order of m in $\mathbb{Z}_p^{\star}$* to be the least $k > 0$ such that $m^k \equiv 1 \pmod{p}$. We use $\mathrm{order}(m)$ to denote the order of m.
By the Finite Group Theorem, we have that for every $m \in \Phi(p)$,

$$\mathrm{order}(m) | (p-1). \tag{32}$$

Given k with $1 \leq k \leq p-1$, define $R(k)$ to be the set of all the elements $m \in \Phi(p)$ having order k.
Let

$$r(k) = |R(k)|.$$

Clearly, if $k \not| (p-1)$, then $R(k) = \emptyset$ and $r(k) = 0$.

Proof of the Primitive Root Theorem - II

For $m \in R(k)$, meaning m has order k, we have

$$m^k \equiv 1 \pmod{p},$$

so that m is a root of the degree k polynomial:

$$P(x) \equiv x^k - 1.$$

According to the Algebraic Fundamental Theorem, for every $k|(p-1)$, there are at most k residues r in $\mathbb{Z}_p^{\square}$ that are the roots of $P(x)$, i.e., $r^k \equiv 1 \pmod{p}$.

Proof of the Primitive Root Theorem - III

(1) Given $s \in R(k)$, that is, s has order k, then the elements in

$$\{1, s, \cdots, s^{k-1}\}$$

are all distinct, and all are roots of the polynomial $P(x)$.

- If $0 \leq i < j \leq k-1$, then $s^i \neq s^j$ in $\mathbb{Z}_p^{\square}$.
- For $0 \leq i \leq k-1$,

$$(s^i)^k = (s^k)^i = 1^i = 1,$$

in $\mathbb{Z}_p^{\square}$.

Therefore, $\{1, s, \cdots, s^{k-1}\}$ are all the roots of $x^k - 1$ in $\mathbb{Z}_p^{\square}$.

Proof of the Primitive Root Theorem - IV

(2) If $s \in \mathbb{Z}_p^{\square}$ has order k, then

$$x^k - 1$$

has roots

$$\{1, s, \cdots, s^{k-1}\}$$

in $\mathbb{Z}_p^{\square}$.
Let s be fixed as above.
For $0 \leq l \leq k-1$, if $l \notin \Phi(k)$, then $(l, k) = d > 1$,

$$(s^l)^{\frac{k}{d}} = (s^k)^{\frac{l}{d}} \equiv 1 \pmod{p},$$

implying that s^l has order $\leq \frac{k}{d} < k$.

Proof of the Primitive Root Theorem - V

(3) If s^l has order k, then $l \in \Phi(k)$, so that

$$r(k) \leq \phi(k).$$

(4)

$$\sum_{k|(p-1)} r(k) = p - 1.$$

(5)

$$\sum_{k|(p-1)} \phi(k) = p - 1.$$

(6) For every $k|(p-1)$, $r(k) \leq \phi(k)$.
(4) + (5) + (6): For every $k|(p-1)$, $r(k) = \phi(k)$ (otherwise, $\sum_{k|(p-1)} r(k) < \sum_{k|(p-1)} \phi(k) = p - 1$) so

$$r(p-1) = \phi(p-1) > 0.$$

There exists a primitive root for $\mathbb{Z}_p^{*}$.

Discrete Logarithm

Given prime p, and a primitive root r module p, and a, e with $1 \leq a \leq p-1$ and $0 \leq e \leq p-1$, if:

$$r^e \equiv a \pmod{p},$$

then we call e the *discrete logarithm of a modulo p to the base r*, written

$$e \equiv \log_r a \pmod{p}.$$

- Computing discrete logarithm is hard, but useful in cryptography
- Quantum computer computes the discrete logarithm in polynomial time

Exercises

1. Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.
2. Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.
3. Find all solutions, if any, to the system of congruences $x \equiv 7 \pmod{9}$, $x \equiv 4 \pmod{12}$, and $x \equiv 16 \pmod{21}$.
4. Let $m_1, m_2, \cdots, m_k$ be pairwise relatively prime integers greater than 1. Show that for any integers a and b, if $a \equiv b \pmod{m_i}$ holds for all i with $1 \leq i \leq k$, then $a \equiv b \pmod{m}$, for $m = \prod_{i=1}^{k} m_i$.
5. Show that for appropriately large n, $\phi(n) = \Omega(\frac{n}{\log n})$.
6. Review all the proofs in this lecture

谢谢！