Number Theory (I)

Cunsheng Ding

HKUST, Hong Kong

November 7, 2015

Contents

Prime Factorization

Definition 1

We call an integer n composite if n is not prime.

Theorem 2 (Fundamental Theorem of Arithmetic)

Every natural number $n > 1$ can be written as a product of primes uniquely up to order.

Proof.

We prove this theorem by strong mathematical induction. Suupose that the conclusion is true for all natural numbers m with $2 \leq m < n$. If n is a prime, the conclusion is obviously true. If n is composite, Then $n = n_1 n_2$ for some n_1 and n_2, where $1 < n_1 < n$ and $1 < n_2 < n$. By the induction hypothesis, n_1 and n_2 both are the product of prime numbers, so is $n = n_1 n_2$. $\square$

Prime Factorization

The following follows from Theorem 2.

Theorem 3 (Canonical Form)

Every natural number $n \geq 2$ can be factorized into

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t},$$

where $p_1, p_2, \ldots, p_t$ are pairwise distinct primes, $e_1, e_2, \ldots, e_t$ are natural numbers, and t is also a natural number.

Example 4

$$n = 120 = 2^3 \times 3 \times 5.$$

The Factorization Problem

Factorization Problem

Factorize n into the product of prime powers.

Comments

- This is a fundamental problem in mathematics and computer science (especially, in cryptography).
- Many algorithms for solving the factorization problem have been developed so far.
- It is open if there is a polynomial-time algorithm for solving the factorization problem.

Fermat's Factorization Method

Theoretical basis

If an odd integer n can be expressed as $n = a^2 - b^2$ is odd, then n is factorized into $n = (a+b)(a-b)$.
On the other hand, if an odd integer $n = cd$, then indeed $n = \left(\frac{c+d}{2}\right)^2 - \left(\frac{c-d}{2}\right)^2$.

Basic method

One tries various values of a, hoping that $a^2 - N = b^2$, a square.

Complexity of this method

Fermat's factorization method is very inefficient.

Some Basic Results about Primes

The following theorem was proved in the lecture about mathematical induction.

Theorem 5 (Euclid)

There are infinitely many primes.

We present the following result without giving a proof.

Theorem 6 (Dirichlet)

Let a and b be integers with $\gcd(a, b) = 1$. Then there are infinitely many primes of the form $ax + b$.

Congruence Modulo n

Definition 7

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. We say that $\underline{a \text{ is congruent to } b \text{ modulo } n}$ if $n \mid (a-b)$ (i.e., n divides $(a-b)$), and write $a \equiv b \pmod{n}$.

Example 8

$30 \equiv -2 \pmod{2}$ and $16 \equiv 6 \pmod{5}$.

Proposition 9

For any modulus $n \in \mathbb{N}$, the congruence relation is an equivalence relation on $\mathbb{Z}$.

Proof.

It is trivial and omitted. $\square$

Congruence Classes Modulo n

Definition 10

Let $n \in \mathbb{N}$. For each i with $0 \leq i \leq n-1$, the <u>congruence class $\bar{i}$ modulo n</u> is defined by

$$\bar{i} = \{x \in \mathbb{Z} \mid x \equiv i \pmod{n}\} = \{jn + i \mid j \in \mathbb{Z}\}.$$

We define

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}.$$

Remark

The set $\bar{i}$ is the equivalence class containing i with respect to the congruence relation.

Congruence Classes Modulo n

Proposition 11

The congruence classes $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$ *form a partition of* $\mathbb{Z}$.

Proof.

Define a binary relation R_n on $\mathbb{Z}$ by $(a, b) \in R_n$ if and only if $a \equiv b \pmod{n}$. It is easy to verify that R_n is an equivalence relation, and the congruence classes are in fact the equivalence classes. The desired conclusion then follows. $\square$

The Euler Totient Function $\phi(n)$

Definition 12

For any $n \in \mathbb{N}$, $\phi(n)$ is defined by

$$\phi(n) = |\{1 \leq i < n \mid \gcd(i, n) = 1\}|.$$

Example 13

Let $n = 15$. Then

$$\{1 \leq i < 15 \mid \gcd(i, 15) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Hence, $\phi(15) = 8$.

The Euler Totient Function $\phi(n)$

Theorem 14

Let $n = \prod_{i=1}^{t} p_i^{e_i}$ be the canonical factorization of n. Then

$$\phi(n) = \prod_{i=1}^{t} (p_i - 1) p_i^{e_i - 1}.$$

Sketch of proof.

The first step is to prove that $\phi(nm) = \phi(n)\phi(m)$ if $\gcd(m, n) = 1$. The second step is to prove the conclusion of the theorem is true for $t = 1$. $\square$

Euler's Theorem

Theorem 15

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof.

Define $R = \{1 \le i < n \mid \gcd(i, n) = 1\}$. By definition, $|R| = \phi(n)$. Since $\gcd(a, n) = 1$, the sets $aR := \{ar \bmod n \mid r \in R\}$ and R are equal. It then follows that

$$\left(\prod_{x \in R} x\right) \bmod n = \left(a^{\phi(n)} \prod_{x \in R} x\right) \bmod n.$$

Note that the integer $\prod_{x \in R}$ is relatively prime to n. The desired conclusion then follows. $\square$

When $n = p$ is a prime, Euler's Theorem is called Fermat's Theorem.

The Multiplicative Order

Definition 16

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $\gcd(a, n) = 1$, the least $\ell \in \mathbb{N}$ such that $a^\ell \equiv 1 \pmod{n}$ is called the order of a modulo n, and is denoted by $\mathrm{ord}_n(a)$.

Proposition 17

Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $\gcd(a, n) = 1$. Then $\mathrm{ord}_n(a)$ exists and divides $\phi(n)$.

Proof.

The conclusion on the existence follows from Euler's Theorem. Let $\phi(n) = q \times \mathrm{ord}_n(a) + r$, where $0 \le r < \mathrm{ord}_n(a)$. Suppose that $r > 0$. We have

$$a^r = a^{\phi(n) - q \times \mathrm{ord}_n(a)} \equiv 1 \pmod{n}.$$

This is contrary to the assumption that $\mathrm{ord}_n(a)$ is the order of a modulo n. $\square$

The Multiplicative Order

Proposition 18

Let $a \in \mathbb{Z}$ *and* $n \in \mathbb{N}$*. Let* $\gcd(a, n) = 1$*. If* $a^k \equiv 1 \pmod{n}$ *for some* $k \in \mathbb{N}$*, then* $\mathrm{ord}_n(a) \mid k$*.*

Proof.

Let $k = k_1 \mathrm{ord}_n(a) + k_0$, where $0 \le k_0 < \mathrm{ord}_n(a)$. Then

$$a^k = a^{k_1 \mathrm{ord}_n(a)} a^{k_0} = (a^{\mathrm{ord}_n(a)})^{k_1} a^{k_0} \equiv a^{k_0} \pmod{n}.$$

Hence $a^{k_0} \equiv 1 \pmod{n}$ and $k_0 = 0$. $\square$

The Multiplicative Order

We will need the following result later.

Proposition 19

Let $a \in \mathbb{Z}$ *and* $n \in \mathbb{N}$ *with* $\gcd(a,n) = 1$. *Then* $\mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{\gcd(k, \mathrm{ord}_n(a))}$, *where* $k \in \mathbb{N}$.

Proof.

Let $r = \frac{\mathrm{ord}_n(a)}{\gcd(k, \mathrm{ord}_n(a))}$. It is straightforward to verify that $a^{kr} \equiv 1 \pmod{n}$. Suppose that $a^{kj} \equiv 1 \pmod{n}$ for some $j \in \mathbb{N}$. By Proposition 18, $\mathrm{ord}_n(a) \mid kj$. Consequently,

$$\frac{\mathrm{ord}_n(a)}{\gcd(k, \mathrm{ord}_n(a))} \mid \frac{k}{\gcd(k, \mathrm{ord}_n(a))} j.$$

Since $\frac{\mathrm{ord}_n(a)}{\gcd(k, \mathrm{ord}_n(a))}$ and $\frac{k}{\gcd(k, \mathrm{ord}_n(a))}$ are coprime, r must divide j. $\square$

Primitive Roots

Definition 20

Let $n \in N$. If there is an integer $a \in \mathbb{N}$ such that $\gcd(a, n) = 1$ and $\mathrm{ord}_n(a) = \phi(n)$, then a is called a primitive root of n or modulo n.

Example 21

3 is a primitive root modulo 7.

Question 1

When does n have a primitive root? How many? How to find them?

Existence of Primitive Roots

A proof of the following theorem can be found in most books on elementary number theory (e.g., the reading material posted on the course web page).

Theorem 22

There is a primitive root modulo n if and only if $n = 1, 2, 4, p^e$, *or* $2p^e$, *where p is an odd prime.*

The Number of Primitive Roots

Theorem 23

If there is a primitive root modulo n, then the total number of primitive roots modulo n is $\phi(\phi(n))$.

Proof.

Let g be a primitive root modulo n. By definition, $\mathrm{ord}_n(g) = \phi(n)$. We now claim that the integers $1, g, g^2, \cdots, g^{\phi(n)-1}$ are coprime to n, and distinct modulo n.

- If we had $g^i \equiv g^j \pmod{n}$ for $0 \le i < j \le \phi(n) - 1$, then we would have $g^{j-i} \equiv 1 \pmod{n}$, where $0 < j - i < \phi(n)$. This is contrary to the fact that $\mathrm{ord}_n(g) = \phi(n)$.

If a is a primitive root modulo n, then $a \equiv g^k \pmod{n}$. By proposition 19, $\mathrm{ord}_n(a)$ is equal to

$$\frac{\mathrm{ord}_n(g)}{\gcd(k, \mathrm{ord}_n(g))} = \frac{\phi(n)}{\gcd(k, \phi(n))}.$$

Hence, a is a primitive root if and only if $\gcd(k, \phi(n)) = 1$. $\square$

Finding a Primitive Root Modulo p

Rule of Thumb

Most primes p have a small primitive root. For example, for the primes less than 100000, approximately 37.5% have 2 as a primitive root, and approximately 87.4% have a primitive root of value 7 or less.

Remark

For primes of reasonable size, many programming languages for mathematics have commands for finding primitive roots.

Primality Testing: Probabilistic Tests

Primality Testing Problem

Use some algorithm to test if a given positive integer n is a prime.

Probabilistic Tests

A test whose conclusion is true with certain level of probability.

- **Fermat primality test:** "Given n, choose some integer a coprime to n and calculate $a^{n-1} \bmod n$. If the result is different from 1, then n is composite. If it is 1, then n may or may not be prime."
- **Miller-Rabin primality test:** "Given n, choose some positive integer $a < n$. Let $2^s d = n - 1$, where d is odd. If $a^d \not\equiv 1 \pmod{n}$ and $a^{d2^r} \not\equiv -1 \pmod{n}$ for all $0 \le r \le s - 1$, then n is composite and a is a witness for the compositeness. Otherwise, n may or may not be prime."

Primality Testing: Deterministic Tests

Deterministic Tests

A test whose conclusion is true.

- **Wilson test:** "n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$." This is inefficient.
- **Pocklington primality test (not known to be polynomial time):** It is based on the Pocklington Theorem:
  "Let $n > 1$ be an integer, and suppose there exist numbers a and q such that
  - q is prime, $q \mid (n-1)$ and $q > \sqrt{n} - 1$;
  - $a^{n-1} \equiv 1 \pmod{n}$;
  - $\gcd(a^{(n-1)/q} - 1, n) = 1$.

  Then n is prime."
- **AKS primality test runs in $O((\log n)^{12})$ (polynomial time, 2002):**
  "$n > 2$ is prime if and only if the polynomial congruence $(x-a)^n \equiv (x^n - a) \pmod{n}$ holds for all integers a coprime to n (or even for some integer a, in particular for $a = 1$)."