Discrete Mathematics 2025 Spring

同济经管
TONGJI SEM

魏可佶 kejiwei@tongji.edu.cn

- 8.1 Prime Numbers
- 8.2 Greatest Common Divisor and Least Common Multiple
- 8.3 Congruence
- 8.4 Linear Congruence Equations and the Chinese Remainder Theorem
- 8.5 Euler's Theorem and Fermat's Little Theorem

- The Division Algorithm
- Prime and Composite Numbers
- The Fundamental Theorem of Arithmetic (Prime Factorization)
- Primality Testing – Sieve Method

- **Definition 8.1:** Let a and b be two integers, with $b \neq 0$. If there exists an integer c such that $a=bc$, then:
  (1) We say that ***a* is divisible by *b***, or ***b* divides *a***, denoted as $b \mid a$.
  (2) We say that ***a* is a multiple of *b***, and that ***b* and *c*** are **factors (or divisors) of *a***.
  (3) If b does **not** divide a, we write $b \nmid a$.
- **Example:** The number **6** has **8** factors: $\pm 1, \pm 2, \pm 3$ and ± 6.
- We usually consider only the **positive factors** of positive integers.
  - *Trivial factors*: 1 and the number itself.
  - *Proper factors*: All factors other than 1 and the number itself.
  - **Example:** 2 and 3 are proper factors of 6.

- **Theorem 8.1:** ***Division Algorithm***

  Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

- **Definition 8.2:** Quotient and Remainder of the Division Algorithm

  In the division algorithm, the quotient can be expressed as $q=a \text{ div } d$, and the remainder can be expressed as $r=a \bmod d$.

- **Examples:** 20 mod 6=2, –13 mod 4=3, 10 mod 2=0

  $b|a$ if and only if $a \bmod b = 0$.

- **Theorem 8.2:** Properties of Divisibility

(1) *Linear Combination* Property of Divisibility：

If $a \mid b$ and $a \mid c$, then $\forall x, y$, we have $a \mid (xb+yc)$.

(2) *Transitivity* of Divisibility： **If $a \mid b$ and $b \mid c$, then $a \mid c$.**

(3) *Multiplicative* Property of Divisibility：

Let $m \neq 0$, then $a \mid b$ *if and only if* $ma \mid mb$.

(4) *Antisymmetry* of Divisibility： **if $a \mid b$ and $b \mid a$, then $a = \pm b$.**

(5) *Absolute Value* Property of Divisibility：

if $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

同济经管
TONGJI SEM

- **Definition 8.3:** Prime Numbers and Composite Numbers
  - ***Prime Number***: A positive integer greater than 1 that is divisible only by 1 and itself.
  - ***Composite Number***: A positive integer greater than 1 that is not a prime.
- **Example:** 2, 3, 5, 7, and 11 are prime numbers, while 4, 6, 8, and 9 are composite numbers.
- Properties of Prime and Composite Numbers

  (1) A number $a>1$ is **composite** if and only if $a=bc$, where $1<b<a$, $1<c<a$.

  This means that a composite number has at least one nontrivial factor (i.e., a factor other than 1 and itself).

Properties of Prime and Composite Numbers

(2) Every composite number has a prime factor.

(3) If $d>1$, p is a prime, and $d|p$, then $d=p$.

This emphasizes a fundamental property of **prime numbers**: a prime number p has exactly two positive divisors, 1 and itself.

(4) Let p be a prime number. If $p|ab$, then $p|a$ or $p|b$.

- This distributive property of primes is also known as the ***Prime Divisor Theorem or Euclid's Lemma***. It states that if a prime number p divides the product of two integers ab, then p must divide at least one of those integers.
- Generalized Form: Let p be a prime number. If $p|a_1a_2 \ldots a_k$, then there exists some $1 \le i \le k$ such that $p|a_i$.
  Note: If d is not a prime, then $d|ab$ *does **not necessarily** imply* $d|a$ *or* $d|b$.

- **Theorem 8.3:** ***Fundamental Theorem of Arithmetic***
  - Every integer $a>1$ can be uniquely written as a product of two or more prime numbers, with the prime factors arranged in non-decreasing order.
  - The prime factorization of an integer a takes the formal form:

  $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where: $p_1,p_2,\dots,p_k$ are distinct prime numbers and $r_1,r_2,\dots,r_k$ are positive integers.
- **Examples:** $30=2\times3\times5$, $117=3^2\times13$, $1024=2^{10}$
- **Corollary on Determining Factor Relationships:**

  Let $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, where: $p_1,p_2,\dots,p_k$ are distinct prime numbers and , $r_1,r_2,\dots,r_k$ are positive integers. Then, a positive integer d is a **divisor** of a if and only if $d = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, where $0\le s_i\le r_i$, $i=1,2,\dots,k$.

- **Trial Division:** Start with the smallest prime number 2 and try dividing the integer by successive primes until a prime factor is found.
- **Sieve of Eratosthenes:** Generate a sufficiently large list of numbers, then starting from the smallest prime, repeatedly mark off its multiples. The unmarked numbers are prime.
- In the fields of cryptography and information security, more efficient algorithms are often required for ***factoring large integers***, such as:
  - **Fermat's Method**
  - **Elliptic Curve Factorization**
  - **Number Field Sieve**