Discrete Mathematics 2025 Spring

同济经管 TONGJI SEM

魏可佶 kejiwei@tongji.edu.cn

CAMEA 中国高质量MBA教育认证 AACSB ACCREDITED EQUIS ACCREDITED

- 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

8.1 Prime Numbers

- 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:** $20 \bmod 6 = 2$, $-13 \bmod 4 = 3$, $10 \bmod 2 = 0$

  $b \mid a$ 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 $|a| \leq |b|$.

- **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 $p|a_1a_2...a_k$, 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 $0\le s_i\le r_i$, $i=1,2,\dots,k$.

↳ Common Methods of Prime Factorization

- **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**

- **Example:** How many positive factors does **21560** have?
  - **Solution:**

① Using trial division, we obtain the prime factorization: $21560=2^3\times5\times7^2\times11$.

② According to the Fundamental Theorem of Arithmetic and the property regarding the number of prime factors, the number of positive divisors of 21560 is $(3+1)\times(1+1)\times(2+1)\times(1+1)=48$.

- **Example:** How many trailing zeros are there in the binary representation of **10!** ?
  - **Solution:** According to:

    ① The number of trailing zeros in a binary number indicates the highest power of 2 that divides the number.

    ② In the binary representation of a decimal number, each trailing zero means the number is divisible by 2 one more time.

    10!=1 × 2×3× 2^2 ×5×(2×3) ×7× 2^3 × 3^2 × (2×5) has the prime factorization： **$10!=2^8\times3^4\times5^2\times7$**

    Therefore, the binary representation of **10!** has **8 trailing zeros**.

- **Theorem 8.4 (Infinitude of Primes):** There are infinitely many prime numbers.
- **Proof:** We use proof by contradiction.

①Assume that there are only finitely many prime numbers, and denote them as $p_1, p_2, \ldots, p_n$. Now construct a new number Q, where $Q = p_1 p_2 \ldots p_n + 1$.

②Clearly, none of the primes p_i divides Q, since dividing Q by any p_i leaves a remainder of 1, for $1 \le i \le n$.

③According to the Fundamental Theorem of Arithmetic, either Q is a new prime number, or it must have a prime factor that is not in the known list of primes.

④This contradicts the assumption that the number of primes is finite. Therefore, there must be ***infinitely many prime numbers***.

- ***Mersenne numbers*** (named after Marin Mersenne) are a special class of natural numbers defined as: $M_n = 2^n - 1$, n is the exponent used to generate the Mersenne number.
  If $M_n = 2^n - 1$ is a prime number, then M_n is called a ***Mersenne prime***.
- Properties of Mersenne Numbers and Mersenne Primes

(1)All Mersenne primes are prime numbers, they are a special form of primes.

(2)If M_n is a Mersenne prime, then n itself must also be a prime number (this is a necessary condition).

(3)If n is a composite number, then the Mersenne number M_n is definitely composite. For example： $M_6=2^6-1=63=7\times9$.

- The GIMPS official website(www.mersenne.org) publishes the latest discovered Mersenne prime and the discovery process.
- On October 21, 2024, GIMPS discovered a new Mersenne prime, $2^{136279841}-1$, with 41 million digits—surpassing the previous record by over 16 million digits.
- **Example: $M_5 = 2^5-1=31$** is a prime number, **$M_{11}=2^{11}-1=2047=23\times 89$** is a composite number.

- The study of the ***distribution of prime numbers*** focuses on the patterns and regularities in how primes appear among natural numbers. The ***Prime Number Theorem*** provides an approximate description of the frequency of prime numbers.
- The ***prime counting function*** $\pi(n)$ represents the number of prime numbers less than or equal to n.
- **Example:**

  $\pi(0)=\pi(1)=0$, $\pi(2)=1$, $\pi(3)=\pi(4)=2$, $\pi(5)=\pi(6)=3$,
  $\pi(7)=\pi(8)=\pi(9)=\pi(10)=4$ (2、3、5、7).

- **Theorem 8.5 (Prime Number Theorem):**
  - As n approaches infinity, the ratio of the number of primes less than or equal to n, denoted $\pi(n)$, to $\frac{n}{ln(n)}$ approaches 1.

    Mathematically, this is written as: $\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{ln(n)}} = 1$.
  - This can also be equivalently stated as: $\pi(n)$ is asymptotically equal to $\frac{n}{ln(n)}$, i.e., $\pi(n) \sim \frac{n}{ln(n)}$.
- The Prime Number Theorem tells us that there are approximately $\frac{n}{ln(n)}$ prime numbers between 1 and n.

- **Theorem 8.6 (Factor Property of Composite Numbers):**
  If a is a composite number, then it must have a proper factor less than or equal to $\sqrt{a}$.
- **Proof:**

① By the property of composite numbers (a composite number a has at least one nontrivial factor), we can write $a=bc$, where $1<b<a$ and $1<c<a$.

② Clearly, at least one of b or c must be less than or equal to $\sqrt{a}$. Otherwise, $bc>=a$, which is a contradiction.

.

- **Corollary:** If a is a composite number, then it must have a prime factor less than or equal to $\sqrt{a}$.
- **Proof：** ①By the fact that "any composite number can be factored into a product of prime numbers," composite number a must have at least one prime factor d such that $1<d<a$.

②If $d \le \sqrt{a}$, the result is proven.

③Suppose $d>\sqrt{a}$, since d is a factor of a, there exists another integer e such that $a=d \times e$.

④If $d>\sqrt{a}$,and $e > \sqrt{a}$,then $d \times e > \sqrt{a} \times \sqrt{a} = a$,which contradicts the fact that $d \times e = a$, **therefore,** e must be less than or equal to$\sqrt{a}$.

⑤Since d is a prime factor of a, and a cannot have two factors greater than $\sqrt{a}$, our initial assumption that $d> \sqrt{a}$ must be false. Thus, any prime factor d of a must satisfy $d \le \sqrt{a}$ 。

- ***Prime Testing Algorithms*** can be broadly categorized into two types: **deterministic tests** and **probabilistic tests**. **Trial Division** and the **Sieve of Eratosthenes** are common deterministic algorithms.
- ***Trial Division*****:** For a given number a, divide it by all positive integers less than or equal to $\sqrt{a}$. If a has no divisors in this range (i.e., none divide it evenly), then a is a prime number, otherwise, it is composite.
- ***Sieve of Eratosthenes*****:** To find all prime numbers less than or equal to n, start from 2 and consider all numbers less than or equal to $\sqrt{a}$ as potential prime candidates. Then eliminate all multiples of these candidates. The numbers that remain after the elimination process are the prime numbers.

- **Example:** Determine whether 157 and 161 are prime numbers.
- **Solution:**

① $\sqrt{157}$, $\sqrt{161}$ are less than 13. The prime numbers less than 13 are: 2, 3, 5, 7, 11.

② Since $2 \nmid 157$, $3 \nmid 157$, $5 \nmid 157$, $7 \nmid 157$, $11 \nmid 157$, we conclude that 157 is a prime number.

③ Since $2 \nmid 161$, $3 \nmid 161$, $5 \nmid 161$, $7 \mid 161$ ($161 = 7 \times 23$), we conclude that 161 is a composite number.

- **The Sieve of Eratosthenes** for finding all prime numbers less than or equal to 100.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Divisible by 2
Divisible by 3
Divisible by 5
Divisible by 7

```
// Original sieve method using the isPrime function to check for prime numbers.
#include <stdio.h>
#define N 100
int main() {  int i, j;    int prime[N+1];

// Assume all numbers are prime: 0 represents a prime number, 1 represents a non-prime number
    for(i = 2; i <= N; i++) {
        prime[i] = 0;          }
    for(i = 2; i*i <= N; i++) {

// If i is a prime number, eliminate all multiples of i
    if(prime[i] == 0) {
            for(j = i*i; j <= N; j += i) {
                prime[j] = 1;    }    }  }


// print prime
    printf("Prime numbers up to %d:\n", N);
    for(i = 2; i <= N; i++) {
        if(prime[i] == 0) {
            printf("%d ", i);
        }    }
    printf("\n");
    return 0;   }
```

8.1 Prime Numbers • Brief summary

同济经管 TONGJI SEM

Objective :

Key Concepts :

Discrete Mathematics 2025 Spring

同济经管 TONGJI SEM

魏可佶 kejiwei@tongji.edu.cn

CAMEA 中国高质量MBA教育认证 AACSB ACCREDITED EQUIS ACCREDITED

- 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

8.2 Greatest Common Divisor and Least Common Multiple

- **Common divisor** and **Greatest common divisor (GCD)**
- **Common multiple** and **Least common multiple (LCM)**
- **Euclidean algorithm** (for finding the GCD)
- **Relatively prime (coprime)**

Greatest common divisor and least common multiple

- A *common factor* (or divisor) refers to an integer that can divide two or more integers simultaneously.
- A *common multiple* refers to a shared multiple of two or more integers.
- **Definition 8.4:**

(1)Let ***a*** and ***b*** be two integers, not both zero. The greatest integer ***d*** such that d divides both ***a*** and ***b*** is called the *greatest common divisor* (gcd) of ***a*** and ***b***, denoted as **gcd(*a*,*b*)**.

(2) The *least common multiple* (lcm) of two positive integers ***a*** and ***b*** is the smallest positive integer divisible by both ***a*** and ***b***, denoted as **lcm(*a*,*b*)**.

- **example: gcd(12,18)=6, lcm(12,18)=36.**
- **gcd-lcm relation**
  - For any positive integer ***a***: **gcd(0,*a*)=*a*, gcd(1,*a*)=1, lcm(1,*a*)=*a***
  - For positive integers ***a*** and ***b***: $a.b=gcd(a,b)\cdot lcm(a,b)$

- **Theorem 8.7:**

  (1) If $a|m$, $b|m$, then $\mathbf{lcm}(a,b)|m$.

  * If a and b are two factors of an integer m, then $\mathbf{lcm}(a,b)$ is also a factor of m.

  (2) **If $d|a$, $d|b$, then $d|\mathbf{gcd}(a,b)$.**

  * If two integers a and b have a common factor d, then d is also a factor of their greatest common divisor.

- **Proof:**

  (1) Since $a|m$ and $b|m$, we know that m is a common multiple of a and b, and $\mathbf{lcm}(a,b)$ is the least common multiple of a and b. Therefore, m must be a multiple of $\mathbf{lcm}(a,b)$, meaning there exists an integer n such that $m=\mathbf{lcm}(a,b)\cdot n$. Thus, $\mathbf{lcm}(a,b)|m$ holds.

■ **Proof:(2)**

① Since $d|a$ and $d|b$, we know that d is a common divisor of a and b.

② The greatest common divisor $\gcd(a,b)$ is the largest integer that can divide both a and b, and it is also a common divisor of a and b.

③ By the transitivity of divisibility, d must also divide $\gcd(a,b)$.This is because any integer that divides both a and b must also divide their common divisors, especially the greatest common divisor.