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

    ① Using trial division, we obtain the prime factorization:
    $21560=2^3\times 5\times 7^2\times 11.$

    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.

$10!=1\times 2\times 3\times 2^2\times 5\times(2\times 3)\times 7\times 2^3\times 3^2\times(2\times 5)$ has the prime factorization： $10!=2^8\times 3^4\times 5^2\times 7$

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: $\boldsymbol{M_n = 2^n} - 1$, $\boldsymbol{n}$ is the exponent used to generate the Mersenne number.
  If $\boldsymbol{M_n = 2^n} - 1$ is a prime number, then $\boldsymbol{M_n}$ 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 $\boldsymbol{M_n}$is a Mersenne prime, then $\boldsymbol{n}$ itself must also be a prime number (this is a necessary condition).

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

↳ Great Internet Mersenne Prime Search(GIMPS)

- 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, $2^{2136279841}-1$, 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.

同济经管 TONGJI SEM

- 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 $\boldsymbol{a}$ is a composite number, then it must have a prime factor less than or equal to $\sqrt{\boldsymbol{a}}$.
- **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 $\boldsymbol{d}$ such that $\mathbf{1}<\boldsymbol{d}<\boldsymbol{a}$.

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

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

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

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

- *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 $\boldsymbol{a}$, divide it by all positive integers less than or equal to $\sqrt{\boldsymbol{a}}$. If $\boldsymbol{a}$ 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 $\boldsymbol{n}$, start from 2 and consider all numbers less than or equal to $\sqrt{\boldsymbol{a}}$ 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

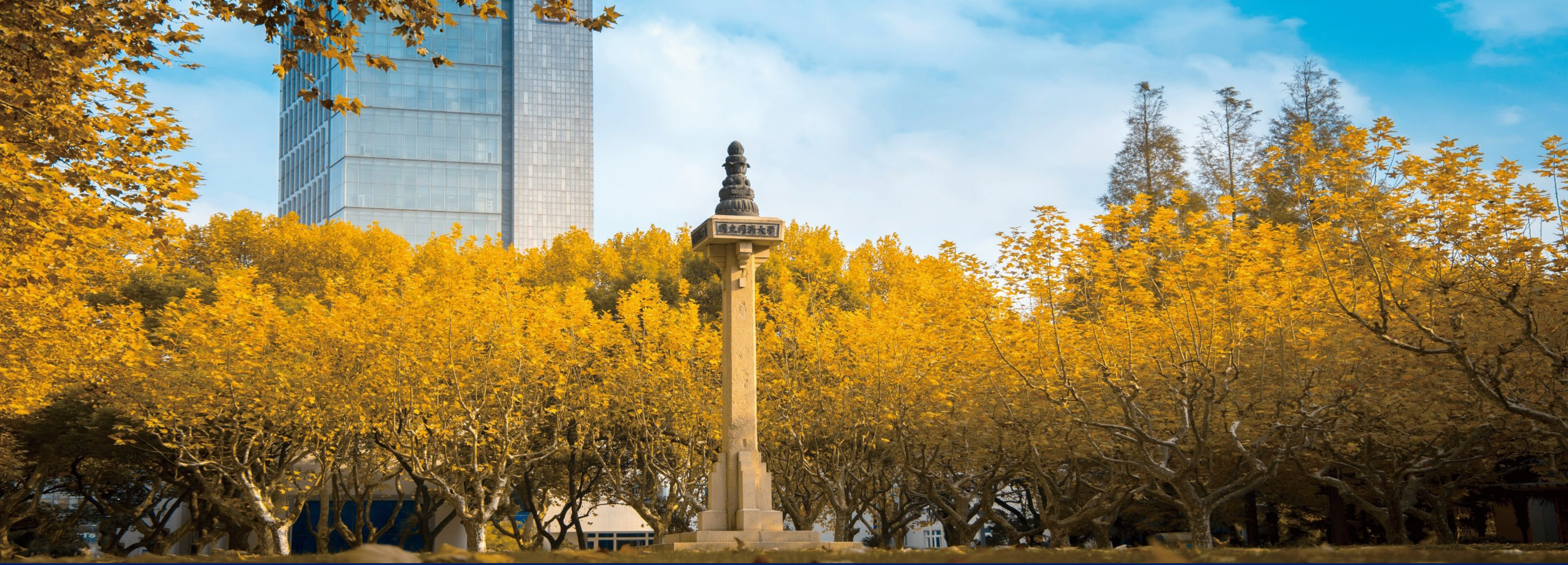
↳ Prime testing algorithms - The Sieve of Eratosthenes (C code)

```
// 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

Objective :

Key Concepts :



Discrete Mathematics 2025 Spring

魏可佶 kejiwei@tongji.edu.cn

同济经管 TONGJI SEM

- **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.
- **Definition8.4:**

(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 $\text{lcm}(a,b)$.

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

- **Theorem 8.7:**

  (1) If $a|m$, $b|m$, then lcm(a,b)$|m$.

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

  (2) If $d|a$, $d|b$, then $d|$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 lcm(a,b) is the least common multiple of a and b. Therefore, m must be a multiple of lcm(a,b), meaning there exists an integer n such that m=lcm(a,b)$\cdot n$. Thus, 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.

↳ Divisibility properties of LCM and GCD

- ***Prime factorization***, based on the Fundamental Theorem of Arithmetic, calculates the **gcd** by multiplying common prime factors with the smallest exponent, and the **lcm** by multiplying them with the largest exponent.
- The **gcd** and **lcm** of two non-negative integers ***a*** and ***b*** can be calculated as:

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_n^{e_n}\ , \quad b = p_1^{f_1} \cdot p_2^{f_2} \cdot \cdots \cdot p_n^{f_n}$$

$$\gcd(a, b) = p_1^{min(e_1,f_1)} \cdot p_2^{min(e_2,f_2)} \cdot \cdots \cdot p_n^{min(e_n,f_n)}$$

$$\mathrm{lcm}(a, b) = p_1^{max(e_1,f_1)} \cdot p_2^{max(e_2,f_2)} \cdot \cdots \cdot p_n^{max(e_n,f_n)}$$

- **Example:** Find the greatest common divisor and least common multiple of 45, 75, and 90.

Solve: $45=3^2\times5^1$, $75=3^1\times5^2$, $90=2^1\times3^2\times5^1$

$\gcd(45,75,90)= 3^1\times5^1=15$

$\mathrm{lcm}(45,75,90)= 2^1\times3^2\times5^2=2\times9\times25=450.$

- **Theorem 8.8: let $a=qb+r$**, where a, b, q, r are integers.

  Then, $\gcd(a,b) = \gcd(b,r)$.

- Prove ⇒: "If d is a common divisor of a and b, then d is also a common divisor of b and r ".

  ① Let d be a common divisor of a and b, so we have $a=dm$ and $b=dn$, where m and n are integers. The equation $a=qb+r$ can be rewritten as: $dm=q(dn)+r$, $r=dm-q(dn)=d(m-qn)$.

  ②Since $m-qn$ is an integer, $d|r$. Therefore, since d divides both a and b ($d|a$ and $d|b$), d is also a common divisor of b and r.

- Prove $\Leftarrow$:

"if d is a common divisor of b and r, then d is also a common divisor of a and b":

①Let d be a common divisor of b and r, so we have $b=dk$ and $r=dl$, where k and l are integers. The equation $a=qb+r$ can be rewritten as: $a=q(dk)+dl=d(qk+l)$.

②Since $qk+l$ is an integer, d divides a. Therefore, since d is a common divisor of b and r ($d|b$ and $d|r$), d is also a common divisor of a and b.

↳ Euclidean Algorithm (Successive Division Method): Finding the GCD

■ *Successive Division Method*

① Input two non-negative integers a and b (assume $a>b$, otherwise swap a and b), and $b\neq 0$.

② According to the **Euclidean division theorem**, find q and r such that $a=bq+r$, where $0\le r<b$。

③ Assign the value of b to a, and the value of r to b.

④ Repeat steps ② and ③ until the remainder $r=0$. When $r=0$, the current value of b is the greatest common divisor **gcd(*a*,*b*)**.

⑤The final non-zero value of b is the greatest common divisor of a and b.

■ **Example:** Find the greatest common divisor of 414 and 662.

Solve： $a=b\times q+r$

①$662=414\times 1+248$. ②$414=248\times 1+166$. ③$248=166\times 1+82$.

④$166=82\times 2+2$. ⑤$82=2\times 41+0$

$gcd(662,414)=2$

- **Theorem 8.9:** (Bézout's Theorem):
  Let a and b not both be zero, then there exist integers x and y such that $\gcd(a,b) = xa+yb$.
- **Proof:**
  ①Let $a=r_0$, $b=r_1$, and apply the Euclidean algorithm:
  $r_i=q_{i+1}r_{i+1}+r_{i+2}$, $i=0, 1,\ldots,k-2$, $r_{k-1}=q_k r_k$, $\gcd(a,b)=r_k$.
  ② Rewrite as $r_{i+2}= r_i-q_{i+1}r_{i+1}$, $i=k-2,k-3,\ldots,0$.
  ③ By performing backward substitution, r_k can be expressed as a linear combination of a and b.