- ***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 ⇐ :**

"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*≠0.**

② According to the **Euclidean division theorem**, find ***q*** and ***r*** such that ***a*=*bq*+*r***, where **0≤*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 ×q+r**

**①662=414×1+248. ②414=248×1+166. ③248=166×1+82.**

**④166=82×2+2. ⑤82=2×41+0**

***gcd*(662,414)=2**

## ↳ Bézout's Identity: A Bridge Between GCD and Linear Combinations



- **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:
  $r_i=q_{i+1}r_{i+1}+r_{i+2}$, $i=0, 1,\ldots,k-2$, $r_{k-1}=q_kr_k$, $\gcd(a,b)=r_k$.

  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 $b$.

- **Example:** Calculate **gcd(119,544)**and find the values of ***x*** and ***y*** that satisfy the equation **119*x*+544*y*=gcd(119,544)** through the backward substitution process.
- **Solve:** ①Apply the Euclidean algorithm.

We begin by performing the division steps of the Euclidean algorithm:

$544=119\times4+68$

$119=68\times1+51$

$68=51\times1+17$

$51=17\times3+0$

- **Solve:** ②Use backward substitution to find $x$ and $y$.

  Now, we work backwards to express 17 as a linear combination of 119 and 544. From the last division:

  $119x+544y=\gcd(119,544)=17$

  $17=68-51\times1$

  $17=68-(119-68\times1)\times1$

  $17=68\times2-119$

  $17=(544-119\times4)\times2-119$

  $17=544\times2-119\times8-119$

  $17=544\times2-119\times9$

- The GCD of **119** and **544** is **17**, which can be expressed as a linear combination: $119\times(-9)+544\times2=17$

## The Necessary and Sufficient Condition for Coprimality



- Two integers $a$ and $b$ are *coprime* if $\gcd(a,b)=1$.
- A set of integers $a_1, a_2, \ldots, a_n$ is *pairwise coprime* if every pair of distinct elements is coprime, i.e., $\gcd(a_i, a_j)=1$ for all $i \neq j$ .
- **For example**, 8 and 15 are coprime, while 8 and 12 are not coprime.The numbers 4, 9, 11, and 35 are pairwise coprime.
- **Theorem 8.10:** The necessary and sufficient condition for two integers $a$ **and** $b$ **to be coprime** is that there exist integers $x$ and $y$ such that $xa+yb=1$.

## The Necessary and Sufficient Condition for Coprimality

- **Necessity:** If integers $a$ and $b$ are coprime, then there exist integers $x$ and $y$ such that the equation $ax + by = 1$ holds.
- **Proof:**

  ①By the definition of coprimeness, $\gcd(a,b)=1$.

  ②By Bézout's Theorem, since $\gcd(a,b)=1$, there must exist integers $x$ and $y$ such the $ax+by=gcd(a,b)$.

  ③Substituting $\gcd(a,b)=1$, we get $ax+by=1$, thus finding the values of $x$ and $y$ that satisfy the condition.

- **Sufficiency:** Proving that the equation $ax + by = 1$ holds is a sufficient condition for $a$ and $b$ to be coprime.

- **Proof:**

①Suppose there exist integers $x$ and $y$ such that the equation $ax + by=1$ holds, meaning $a$ and $b$ can be expressed as a linear combination to generate the smallest positive integer 1.

②Let $d$ be a common divisor of $a$ and $b$ , so $a=d\cdot m$ and $b=d\cdot n$, where $m$ and $n$ are integers. The equation $ax + by=1$ can be rewritten as $d\cdot(mx+ny)=1$.

③Since only 1 multiplied by 1 results in 1 among positive integers, $d$ must be 1.

④Therefore, since $a$ and $b$ have no common divisors greater than 1, we have $\gcd(a,b)=1$, and by the definition of coprimeness, $a$ and $b$ are coprime.

## ↳ Coprime Divisibility Transfer Theorem



- **Theorem 8.11**: Let $a|c$, $b|c$, $a$ and $b$ be coprime. Then, $ab|c$.
- **Proof:**

①By the necessary and sufficient condition for coprimeness, there exist integers x and y such tha $xa+yb=1$.

②Multiplying both sides by $c$, we get $cxa+cyb=c$. Since $a|xa$ and $b|c$, we have $ab|cxa$.

③Similarly, since $b|yb$ and $a|c$, we have $ab|cyb$. Thus, we have $ab|cxa+cyb$, which simplifies to $ab|c$.

# 8.2 Greatest Common Divisor and Least Common Multiple

- Brief summary

**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

# 8.3 Congruence

- Congruence
- Modular Arithmetic
- Equivalence Class modulo m

- **Definition 8.5 :** Let ***m*** be a positive integer, and ***a*** and ***b*** be integers.
  - If $m|(a-b)$, then ***a*** is said to be ***congruent*** to ***b*** modulo ***m***, or ***a*** is congruent to ***b*** modulo ***m***, denoted as $a \equiv b \pmod{m}$.
  - If ***a*** is ***not congruent*** to ***b*** modulo ***m***, we write $a \not\equiv b \pmod{m}$.
- The ***necessary and sufficient conditions*** for $a \equiv b \pmod{m}$. :

  (1) $a \bmod m = b \bmod m$.

  (2) $a \equiv b \pmod{m}$ if and only if $a-b$ is a multiple of ***m***, i.e., $a=b+km$, where ***k*** is an integer.
- **Example：** $5 \equiv 17 \pmod 6$ , $264 \equiv 249 \pmod 5$ , $24 \not\equiv 16 \pmod 6$ .

- Congruence modulo $m$ satisfies the properties of an *equivalence relation*.

  That is, for all integers $a,b,c \in Z$, the following hold:

  ① **Reflexivity:** $a \equiv a \pmod{m}$

  ② **Transitivity:** $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

  ③ **Symmetry:** $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

  - Shorthand notation for the equivalence relation modulo $m$:

    $a_1 \equiv a_2 \equiv \ldots \equiv a_k \pmod{m}$.

- *Closure of Algebraic Operations* under Congruence Modulo $m$

  If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, then:

  ① $a \pm c \equiv b \pm d \pmod{m}$ (Additive and subtractive property)

  ② $ac \equiv bd \pmod{m}$ (Multiplicative property)

  ③ $a^k \equiv b^k \pmod{m}$ , where $k$ is a non-negative integer (Exponentiation property)

- Congruence *Modulo Reduction Property*: Let $d \geq 1$, $d \mid m$, then $a \equiv b \pmod{m} \Rightarrow a \equiv b \pmod{d}$.
  *When $d$ is a divisor of $m$, a congruence modulo $m$ implies a congruence modulo the smaller modulus $d$.
- *Scaling Property of Congruence* : Let $d \geq 1$, then $a \equiv b \pmod{m} \Leftrightarrow da \equiv db \pmod{dm}$.
  *The congruence relation is scalable under multiplication: if you multiply both sides by the same factor $d$, the congruence remains valid modulo $dm$.
- *Multiplicative Inverse Property* of Congruence: Let $c$ and $m$ be coprime,then $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{m}$.
  * If $c$ is relatively prime to $m$, then multiplying both sides by $c$ preserves the congruence modulo $m$.

## ↳ Equivalence Classes and Quotient Set of Congruence



- ***Congruence Class Modulo m*: An equivalence class under the congruence relation modulo *m*. The class of an integer a modulo m is denoted by $[a]_m$ , or simply $[a]$.**
- **The *quotient set* of the integers Z under the modulo *m* congruence relation is denoted by $Z_m$ ,which is the set of all congruence classes modulo *m*.**
- **Example: Partitioning the set of integers under the congruence relation modulo *m*=3, we obtain the following equivalence classes:**

**[0]: The set of integers with remainder 0, {...,−6,−3,0,3,6,9,12,...}.**

**[1]: The set of integers with remainder 1, {...,−5,−2,1,4,7,10,13,...}.**

**[2]: The set of integers with remainder 2, {...,−4,−1,2,5,8,11,14,...}.**

The *quotient set* is: $Z_3$={[0],[1],[2]}

## ↳ Addition and Multiplication on the Quotient Set $Z_m$

- On the quotient set $Z_m$ operations of **addition, subtraction, and multiplication** are defined between equivalence classes, ***resulting in a new equivalence class***.
- The operations of addition and multiplication are defined as follows: :

  $\forall\ a, b,\ \ [a]+[b]=[a+b],\quad [a]\cdot[b]=[ab].$
- **Example:** Write out the addition and multiplication operations on $Z_3$

  Solve: $Z_3=\{[0],[1],[2]\}$, where $[i]=\{3k+i \mid k\in Z\}$, $i=0,1,2$.
  - **All possible results of addition on Z3:**

    **[0]+[0]=[0]:** Because $0+0\equiv 0 \bmod 3$.

    **[0]+[1]=[1]:** Because $0+1\equiv 1 \bmod 3$.

    **[0]+[2]=[2]:** Because $0+2\equiv 2 \bmod 3$.

## ↳ Addition and Multiplication on the Quotient Set $Z_m$



- All possible results of ***addition*** on **Z3**

**[1]+[1]=[2]:** Because 1+1≡2 mod 3.

**[1]+[2]=[0]:** Because 1+2≡0 mod 3.

**[2]+[2]=[1]:** Because 2+2≡1 mod 3.

- All possible results of ***multiplication*** on **Z3**：

**[0]×[0]=[0]:** Because 0×0≡0 mod 3.

**[0]×[1]=[0]:** Because 0×1≡ **0** mod 3.

**[0]×[2]=[0]:** Because 0×2≡ **0** mod 3.

**[1]×[1]=[1]:** Because 1×1≡1 mod 3

**[1]×[2]=[2]:** Because 1×2≡2 mod 3.

**[2]×[2]=[1]:** Because 2×2≡1 mod 3.

- **Example:** What is the units digit of $3^{455}$? How can we determine the units digit of $a^n$?
- **Solution:**

①**Use the cyclic nature of modular arithmetic** to find the pattern of the units digit of $3^n$ Since the units digit corresponds to modulo 10, we can compute $3^n$ **mod 10** to determine the cycle length $k$, **such that** $3^k \equiv 1 \bmod 10$.

②We find that the units digit of $3^n$ follows a repeating pattern **3, 9, 7, 1, repeat every $k$=4 powers.**

③To find the units digit of $3^{455}$, **note that 455 mod 4 =3,** Therefore, the units digit corresponds to the 3rd number in the cycle, which is **7.**

④For any $a^n$ , the units digit can be found using: $a^n \equiv a(n \bmod k) \bmod 10$ where $k$ is the length of the cycle of a mod **10.**

What are the last two digits (the tens and units digits) of $3^{455}$ ?

# 8.3 Congruence • Brief summary

**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

- 8.4.1 Linear Congruences
  - Modular Inverses
- 8.4.2 The Chinese Remainder Theorem
- 8.4.3 Arithmetic Operations with Large Integers

- *Linear Congruence Equation*: $ax \equiv c \pmod{m}$, where $m>0$.
- *Solution to the linear congruence equation*: The integers that satisfy the equation.
- **Example: $3x \equiv 4 \pmod 7$'s solution $x \equiv 6 \pmod 7$, such as 6,13,20,−1**

  $2x \equiv 1 \pmod 4$ has no solution.
- **Theorem 8.12:** The necessary and sufficient condition for the equation $ax \equiv c \pmod m$ to have a solution is that $\gcd(a,m) \mid c$.
- **Number of solutions:**

  $\gcd(a,m)=1$, the equation has a unique solution, >1, there are gcd(a,m) distinct solutions.
- **Method for calculating the solutions:**

  The solutions can be found by direct observation or by using the multiplicative inverse of a modulo $m$.

- **Proof of Necessity:**

① Suppose the equation $ax \equiv c \pmod{m}$ has a solution, then $ax-c=km$, $ax-km=c$, $k$ is integer.

② Bezout's identity, if $d=gcd(a,m)$, then there exist integers $u$ and $v$ such that $au+mv=d$.

③ Since both $c$ and $d$ can be expressed as linear combinations of a and $m$, $d$ must divide $c$. Therefore, $(a,m)|c$.

- **Proof of Sufficiency:**

① Suppose $gcd(a,m)|c$, there exists an integer $k$ such that $c=d*k$, where $d=gcd(a,m)$.

② By Bezout's identity, if $d=gcd(a,m)$, then there exist integers u and $v$ such that $au+mv=d$.

③ Replacing $d$ with $c=d.\ k, a(uk)+m(vk)=c$. This shows that there exists an integer $x=uk$ such that $ax-c$ is a multiple of $m$, or equivalently, there exists an $x$ such that $ax \equiv c \pmod{m}$. Therefore, if $gcd(a,m)|c$, the equation $ax \equiv c \pmod{m}$ must have a solution.

## ↳ Equivalence Class Method for Linear Congruences



- **Example**: Solve the linear congruence equation $6x \equiv 3 \pmod 9$.
- **Solution**: Using the *equivalence class method* modulo $m$:

① $\gcd(6,9)=3 \mid 3$ , which satisfies the necessary and sufficient condition for a solution.

② In modulo 9, any integer belongs to one of the equivalence classes from 0 to 8. We only need to check whether $x$ satisfies the given congruence equation for $x=0,1,2,\ldots,8$.

③ The test results show that $x=2,5,8$ are solutions to the equation $6x \equiv 3 \pmod 9$, $x=2$ is the particular solution, and $x=2+9k$ (where $k$ is any integer) are the valid solutions.

- **Note**: Choosing $x=-4,-3,-2,-1,0,1,2,3,4$ will produce the same set of solutions.

- **Definition 8.6 :** If $ab \equiv 1 \pmod{m}$, then $b$ *is* called the modular inverse of $a$ modulo $m$, denoted as $a^{-1} \pmod{m}$ or $a^{-1}$.
  - $a^{-1} \pmod{m}$ is the solution to the equation $ax \equiv 1 \pmod{m}$.
- **Theorem 8.13:** (**Existence and Uniqueness Theorem** )

  (1) The necessary and sufficient condition for the modular inverse of a modulo $m$ to exist is that $a$ and $m$ are coprime and $m > 1$(*Existence*).

  (2) If $a$ and $m$ are coprime and $m>1$, then the modular inverse of $a$ modulo $m$ is unique (*Uniqueness*).

- **Proof (1) (existence):** The necessary and sufficient condition for the existence of the modular inverse of a modulo $m$ is that $a$ and $m$ are coprime.
- **Sufficiency:**
  ① $a,m$ coprime, then there exist integers $x$ *and* $y$ such that $ax+my=1$.
  ② $ax-1=my$ is equivalent to $ax\equiv 1 \bmod m$, showing that $x$ is the modular inverse of a modulo $m$.
- **Necessity:**
  ① Suppose there exists an integer $b$ such that $ab\equiv 1 \bmod m$, Then there exists an integer such that $ab-1=km$.
  ② Rearranging gives $ab-km=1$ which shows that 1 can be expressed as an integer linear combination of $a$ and $m$.
  This is only possible when $\gcd(a,m)=1$.

■ **Proof(2) (Uniqueness):** Suppose $a$ and $m$ are coprime, then the modular inverse of a modulo $m$ is unique.

① Suppose $a$ has two modular inverses modulo $m$, say $b_1$ and $b_2$, such that: $ab_1 \equiv 1 \pmod{m}$, $ab_2 \equiv 1 \pmod{m}$. This means there exist integers $k$ and $l$ such that: $ab_1 = 1 + km$、$ab_2 = 1 + lm$. Subtracting the two equations gives: $a(b_1 - b_2) = (k - l)m$.

② Therefore $a(b_1 - b_2) \equiv 0 \pmod{m}$.

③ Since $a$ and $m$ are coprime, this implies that $b_1 - b_2$ must be divisible by $m$, that is, $b_1 \equiv b_2 \pmod{m}$.

④ Hence, if two integers $b_1$ and $b_2$ are both modular inverses of $a$ modulo $m$, they must be congruent modulo $m$, that is, **the modular inverse is unique modulo $m$.**

## ↳ Trial Methods for Modular Inverse



- ***Trial Method*: This method directly uses the definition of a modular inverse by solving the congruence equation $ax \equiv 1 \pmod{m}$ to find the modular inverse of $a$ modulo $m$.**

- **Main steps:**

① Verify the necessary condition for the existence of the inverse by ensuring that $\gcd(a,m)=1$.

② Set up the congruence equation $ax \equiv 1 \pmod{}$ , where $x$ is the modular inverse of a that we are looking for.

③ Try values of **x:** For each integer x from 1 to m−1, compute $ax \pmod{m}$ .

④ **Identify the solution:** The value of x that satisfies $ax \pmod{m}=1$ the modular inverse of a, denoted as $a^{-1} \bmod m$.

## ↳ Euclidean Algorithm for Modular Inverses



- ***Euclidean Algorithm*: This method uses the Extended Euclidean Algorithm to find integers $x$ and $y$ such that $ax + my = \gcd(a,m)$. When $\gcd(a,m)=1$, the value of $x$ is the modular inverse of a modulo $m$.**

- **Main steps:**

  ① Apply the Extended Euclidean Algorithm to find integers $x$ and $y$ such that: $ax+my=\gcd(a,m)$ .

  ② If a and m are coprime, i.e., then $x$ is the modular inverse of $a$ mod $m$.

  ③ If $x$ is negative, add $m$ repeatedly until $x$ becomes positive, to ensure that x lies within the standard range modulo $m$.