- Congruence *Modulo Reduction Property*: Let $d \geq 1$, $d|m$, 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.

- ***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]}

- 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: :
  $\forall\, a, b,\ \ [a]+[b]=[a+b], \qquad [a]\cdot[b]=[ab].$
- **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 $0+2\equiv 2 \bmod 3$.

- 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.

↳ Examples of Modular Exponentiation

- **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}?

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:**

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

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

③Since 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:**

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

②By 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.

- **Example**: Solve the linear congruence equation **6x≡3 (mod 9).**
- **Solution**: Using the ***equivalence class method*** modulo ***m***:

① **gcd(6,9)=3|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,…,8**.

③ The test results show that ***x*=2,5,8** are solutions to the equation **6x≡3 (mod 9),*x*=2** is the particular solution, and ***x*=2+9*k*** (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 of the Existence and Uniqueness of Modular Inverses

- **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 $ax \equiv 1(\mathrm{mod})$, 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***.

↳ Direct Observation Method for Modular Inverses

- ***Direct Observation Method***: This method involves testing each integer x from 1 to $m-1$, computing $ax \pmod m$, and identifying the value of x that yields a remainder of 1. Such an x satisfies the $ax \pmod m = 1$ and is the modular inverse of a mod m.
- **Example:** Find the modular inverse of **5** modulo **7**.
  - **Solution 1:** Using the ***direct observation method*** to find an integer x such that $5x \equiv 1 \pmod 7$.

    ① Try values of x from 1 to 6. When $x=3$, $5 \times 3 \pmod 7 = 1$, satisfied $5x \equiv 1 \pmod 7$.

    ② Verify that $x=3$ is correct: $5^{-1} \equiv 3 \pmod 7$.

↳ Trial Method for Modular Inverses (e.g.)

- **Solution 2:** Use the ***trial method*** to solve the congruence $ax \equiv 1 \pmod{m}$ and find the modular inverse of a mod m.

① Since **gcd(5,7)=1**, the modular inverse of *5* modulo *7* exists.

② solve $ax \equiv 1$(mod), try values of x(1 to 6) compute $5x \pmod 7$.

③ when $x=3$, $5 \times 3 = 15 \pmod 7 = 1$.

④ Therefore, the modular inverse of **5** modulo **7** is **3**, that is, $5^{-1} \equiv 3 \pmod 7$.

↳ Trial Method for Modular Inverses (e.g.)

- **Solution 3: Use the** ***Euclidean Algorithm***. Since **gcd(5,7)=1**,we solve the equation **5x +7y=1.**

  ①**7=1×5+2,5=2×2+1,then 1=5−2×2.**

  ②**2=7−1×5, 1=5−2×2, we have 3×5−2×7=1,** which is the modular inverse of 5 modulo 7,then **5×3≡1(mod 7)** holds.

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

- 《孙子算经》 “物不知数”问题: 今有物, 不知其数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

$$x \equiv 2 \pmod 7$$

- **Theorem 8.14 (Chinese Remainder Theorem).**

  Let m_1, m_2,…,m_k be pairwise coprime positive integers. Then the system of linear congruences $x \equiv a_i \pmod{m_i}$, i=1,2, … ,k has an integer solution, and the solution is **unique modulo**, that is, **any two solutions are congruent modulo** m**.**

Proof of the Chinese Remainder Theorem

- **Proof of *Existence of Solution*: $x \equiv a_i \pmod{m_i}$, $i=1,2, \ldots ,k$. m_1, m_2, …, m_k** are pairwise coprime positive integers:

① Compute $M= m_1m_2\ldots,m_k$.

② Define $M_i= M / m_i$, Since M_i is the product of all moduli except m_i . Since the moduli are pairwise coprime, we have **gcd(m_i ,M_i)=1.**

③ Because M_i and m_i coprime, by the theorem on the existence of modular inverses, there exists an integer m_i' such that $M_i m_i' \equiv 1$ **mod m_i.**

④ Construct a partial solution for each congruence as $x_i = a_i M_i m_i'$, where each x_i satisfies the congruence $x \equiv a_i \bmod m_i$, but not affect m_j **($j \neq i$).**

⑤ The final solution x is the sum of all x_i ,$x = \sum_{i=1}^{k} x_i$.

- Proof of *Existence of Solution*: $x \equiv a_i \pmod{m_i}$, $i=1,2,\ldots,k$. m_1, m_2, …, m_k are pairwise coprime positive integers:

  ⑥ To show that this x satisfies each individual congruence $x \equiv a_i \bmod m_i$:

  Let $x=\sum_{j=1}^{k} x_j$, two cases on $x \bmod m_i$:

  (a) For $j=i$, $x_i = a_i M_i m_i'$, and the result modulo m_i is a_i , since $M_i\ m_i' \equiv 1 \bmod m_i$.

  (b) When $j \neq i$,because M_j includes m_i as a factor (since all m_i are pairwise coprime), we have $M_j m_j' \equiv 0 \bmod m_i$.

  Thus, all x_j for $j \neq i$ contribute 0 modulo m_i, and only x_i determines the value of $x \bmod m_i$, yielding $x \equiv a_i \bmod m_i$.

- **Proof of** ***Uniqueness of the Solution***: To prove that the solution x is unique modulo $M = m_1m_2\ldots m_k$, it is sufficient to show that any two solutions x and y are congruent modulo M, i.e., $x \equiv y \pmod{M}$.

①Suppose there exist two solutions x and y that satisfy all the congruences in the system. That is, for every i, $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$.

②Since both x and y yield the same remainder modulo each m_i, it follows that $x \equiv y \pmod{m_i}$. This implies that each m_i divides $(x - y)$.

③Because $m_1, m_2, \ldots, m_k$ are pairwise coprime, it follows from the properties of coprime integers that their product $M = m_1m_2\ldots m_k$ also divides $(x - y)$.

④ $M \mid (x-y)$ means $x \equiv y \pmod{M}$, which proves that the solution is *unique modulo M*.

↳ Chinese Remainder Theorem: Solving Linear Congruences

- **Solving a System of Linear Congruences $x \equiv a_i \pmod{m_i}$, $i=1,2, \ldots ,k$** where the positive integers $m_1, m_2,\ldots,m_k$ are *pairwise coprime*.
- **Solution:** *Using the Chinese Remainder Theorem.*

(1) Compute the product of all moduli: $M = m_1 m_2 \ldots m_k$.

(2) For each i=1,2,…,k compute $M_i = M / m_i$, $i=1, 2,\ldots, k$.

(3) Find the modular inverse of each M_i modulo m_i, denoted as M_i^{-1} .

(4) Compute the final solution: $x = \sum_{i=1}^{k} a_i M_i M_i^{-1} \bmod M$.

By following the above steps, one can solve a system of linear congruences. In particular, when the moduli are pairwise coprime, the **Chinese Remainder Theorem** provides an efficient method for finding the solution.

- **Example**: Solve the "*Problem of the Unknown Quantity*," that is, find the positive integer solution to the following system of equations:
  $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.
- **Solution:**
  ① $m_1=3$, $m_2=5$, $m_3=7$, $M=105$.
  ② $M_1=M/m_1=105/3=35$, $M_2=M/m_2=105/5=21$, $M_3=M/m_3=105/7=15$.
  ③ Solve $M_1^{-1}=2$, $M_2^{-1}=1$, $M_3^{-1}=1$.
  ④ Final solutions $x=(2\cdot 35\cdot 2+3\cdot 21\cdot 1+2\cdot 15\cdot 1) \bmod 105=23$.
  Solution is $105k+23$, $k=0,1,2,\ldots$. Least number is 23.
- **Finding the Modular Inverse by Observation:**
  ① Find the inverse of $M_1=35$ modulo m1=3, i.e., find M_1^{-1} such that $M_1 \cdot M_1^{-1} \equiv 1 \bmod 3$.
  ② ($35 \equiv 2 \bmod 3$), we need to make $2\cdot M_1^{-1} \equiv 1 \bmod 3$ M_1^{-1} .
  ③ By simple trial, we find that $M_1^{-1}=2$ satisfies the condition.

- 8.4.1 Linear Congruences

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

- Let $m_1,m_2,…,m_k$ be integers greater than **1** and pairwise coprime, and define $m=m_1m_2…m_k$. For any integer $0 \le x<m$, define $x_i=x \bmod m_i$, $i=1,…,k$. $(x_1,x_2,…,x_k)$ is called the *modular representation of x* with respect to the moduli $m_1,…,m_k$, or simply the **modular representation** of x. It is denoted as: $x=(x_1,x_2,…,x_k)$.
- **Modular Representation Operations**

  Let $x=(x_1,x_2,…,x_k)$, $y=(y_1,y_2,…,y_k)$, then

  $x+y=((x_1+y_1) \bmod m_1,\ (x_2+y_2) \bmod m_2,\ …,\ (x_k+y_k) \bmod m_k)$.

  $x-y=((x_1-y_1) \bmod m_1,\ (x_2-y_2) \bmod m_2,\ …,\ (x_k-y_k) \bmod m_k)$.

  $xy=(x_1y_1 \bmod m_1,\ x_2y_2 \bmod m_2,\ …,\ x_ky_k \bmod m_k)$.

Advantages of Representing an Integer *x* by Its Remainders Modulo a Set of Moduli:

- When an integer x is represented by its remainders with respect to a set of pairwise coprime moduli $m_1, m_2, \ldots, m_k$, computations involving x can be carried out independently under each modulus.
- The results can then be combined using the **Chinese Remainder Theorem.**
- This approach improves **computational efficiency**, enhances **distributed processing capability**, and increases **algorithmic flexibility.**

Challenges in Large Integer Arithmetic and Corresponding Solutions:

- *Computational Complexity*: Operations on large integers (such as addition, multiplication, and exponentiation) are very time-consuming using traditional methods.
- *Memory Constraints*: Representing large integers using modular decomposition allows more efficient use of memory by storing smaller components.
- *Parallel Processing*: The modular representation of large integers enables computations to be performed independently under each modulus, supporting parallel processing.
- *Security*:Enhances the efficiency of computations in cryptographic applications.

- **Example:** Let m_1=9, m_2=7, m_3=5, m=9×7×5=315, Arithmetic operations within the range of **0** to **314** can be performed using arithmetic modulo **9, 7, 5.**
- **Solve:** Let x=20, y=13, then x=(2, 6, 0), y=(4, 6, 3).

  $x+y$=((2+4)mod 9, (6+6)mod 7, (0+3)mod 5)=(6, 5, 3).

  $x-y$=((2−4)mod 9, (6−6)mod 7, (0−3)mod 5)=(7, 0, 2).

  xy=(2×4 mod 9, 6×6mod 7, 0×3mod 5)=(8, 1, 0).

  Find the smallest positive integer solution:

$$\begin{cases} z \equiv 6 \pmod 9 \\ z \equiv 5 \pmod 7 \\ z \equiv 3 \pmod 5 \end{cases} \qquad \begin{cases} z \equiv 7 \pmod 9 \\ z \equiv 0 \pmod 7 \\ z \equiv 2 \pmod 5 \end{cases} \qquad \begin{cases} z \equiv 8 \pmod 9 \\ z \equiv 1 \pmod 7 \\ z \equiv 0 \pmod 5 \end{cases}$$

Compute as:

$M_1=35,\ M_1\equiv -1 \pmod 9,\ M_1^{-1}=-1,$

$M_2=45,\ M_2\equiv 3 \pmod 7,\ M_2^{-1}=5,$

$M_3=63,\ M_3\equiv 3 \pmod 5,\ M_3^{-1}=2,$

Then

$x+y=(6\times(-1)\times 35+5\times 5\times 45+3\times 2\times 63) \bmod 315=33.$

$x-y=(7\times(-1)\times 35+0\times 5\times 45+2\times 2\times 63) \bmod 315=7.$

$xy=(8\times(-1)\times 35+1\times 5\times 45+0\times 2\times 63) \bmod 315=260.$

Objective :

Key Concepts :