# Lecture 2-1: Math I

## –Cryptographic Algorithms and Protocols


Instructor: Xiujie Huang 黄秀姐

Office: Nanhai Building, Room 411

E-mail: t_xiujie@jnu.edu.cn

Department of Computer Science

School of Information Science and Technology

Jinan University

# Outline

# Outline

# Modular Arithmetic

## Modular Arithmetic, 模运算(求余数运算)

Let $a$ and $b$ be two integers, $m$ is a positive integer. If $m$ divides $b - a$, i.e., $m|(b - a)$, then denote $a \equiv b \pmod{m}$.

- The phrase $a \equiv b \pmod{m}$ is called a congruence, and read as *$a$ is congruent to $b$ modulo $m$*.
- The integer $m$ is called the *modulus*.

# Modular Arithmetic

## Modular Arithmetic, 模运算(求余数运算)

Let $a$ and $b$ be two integers, $m$ is a positive integer. If $m$ divides $b-a$, i.e., $m|(b-a)$, then denote $a \equiv b \pmod{m}$.

- The phrase $a \equiv b \pmod{m}$ is called a congruence, and read as *$a$ is congruent to $b$ modulo $m$*.
- The integer $m$ is called the *modulus*.
- $a \bmod m$ denotes the remainder when $a$ is divided by $m$. Hence, $a \bmod m$ is one of the elements in the set $\{0, 1, 2, \cdots, m-1\}$.
- If $a$ is replaced by $a \bmod m$, we say that $a$ is reduced modulo $m$.

# Modular Arithmetic

## Modular Arithmetic, 模运算(求余数运算)

Let $a$ and $b$ be two integers, $m$ is a positive integer. If $m$ divides $b-a$, i.e., $m|(b-a)$, then denote $a \equiv b \pmod{m}$.

- The phrase $a \equiv b \pmod{m}$ is called a congruence, and read as *$a$ is congruent to $b$ modulo $m$*.
- The integer $m$ is called the *modulus*.
- $a \bmod m$ denotes the remainder when $a$ is divided by $m$. Hence, $a \bmod m$ is one of the elements in the set $\{0, 1, 2, \cdots, m-1\}$.
- If $a$ is replaced by $a \bmod m$, we say that $a$ is reduced modulo $m$.

## Examples

$5 \equiv 25 \pmod{4}$, $3 \equiv 11 \pmod{4}$, $3 \equiv (-1) \pmod{4}$, $(-7) \equiv 1 \pmod{4}$

# Modular Arithmetic

## Modular Arithmetic, 模运算(求余数运算)

Let $a$ and $b$ be two integers, $m$ is a positive integer. If $m$ divides $b - a$, i.e., $m|(b-a)$, then denote $a \equiv b \pmod{m}$.

- The phrase $a \equiv b \pmod{m}$ is called a congruence, and read as *$a$ is congruent to $b$ modulo $m$*.
- The integer $m$ is called the *modulus*.
- $a \bmod m$ denotes the remainder when $a$ is divided by $m$. Hence, $a \bmod m$ is one of the elements in the set $\{0, 1, 2, \cdots, m-1\}$.
- If $a$ is replaced by $a \bmod m$, we say that $a$ is reduced modulo $m$.

## Examples

$5 \equiv 25 \pmod{4}$, $3 \equiv 11 \pmod{4}$, $3 \equiv (-1) \pmod{4}$, $(-7) \equiv 1 \pmod{4}$

$25 \bmod 4 = 1$, $11 \bmod 4 = 3$, $(-1) \bmod 4 = 3$, $(-7) \bmod 4 = 1$

# Modular Arithmetic

## Modular Arithmetic, 模运算(求余数运算)

Let $a$ and $b$ be two integers, $m$ is a positive integer. If $m$ divides $b-a$, i.e., $m|(b-a)$, then denote $a \equiv b \pmod{m}$.

- The phrase $a \equiv b \pmod{m}$ is called a congruence, and read as *$a$ is congruent to $b$ modulo $m$*.
- The integer $m$ is called the *modulus*.
- $a \bmod m$ denotes the remainder when $a$ is divided by $m$. Hence, $a \bmod m$ is one of the elements in the set $\{0, 1, 2, \cdots, m-1\}$.
- If $a$ is replaced by $a \bmod m$, we say that $a$ is reduced modulo $m$.

## Examples

$5 \equiv 25 \pmod{4}$, $3 \equiv 11 \pmod{4}$, $3 \equiv (-1) \pmod{4}$, $(-7) \equiv 1 \pmod{4}$

$25 \bmod 4 = 1$, $11 \bmod 4 = 3$, $(-1) \bmod 4 = 3$, $(-7) \bmod 4 = 1$

$1 = [5 \bmod 4] = [25 \bmod 4] = [(-7) \bmod 4]$, $3 = [11 \bmod 4] = [(-1) \bmod 4]$

# Modular Arithmetic

## Modular Arithmetic, 模运算(求余数运算)

Let $a$ and $b$ be two integers, $m$ is a positive integer. If $m$ divides $b-a$, i.e., $m|(b-a)$, then denote $a \equiv b \pmod{m}$.

- The phrase $a \equiv b \pmod{m}$ is called a congruence, and read as *$a$ is congruent to $b$ modulo $m$*.
- The integer $m$ is called the *modulus*.
- $a \bmod m$ denotes the remainder when $a$ is divided by $m$. Hence, $a \bmod m$ is one of the elements in the $\boxed{\text{set } \{0, 1, 2, \cdots, m-1\}}$.
- If $a$ is replaced by $a \bmod m$, we say that $a$ is reduced modulo $m$.

## Examples

$5 \equiv 25 \pmod{4}$, $3 \equiv 11 \pmod{4}$, $3 \equiv (-1) \pmod{4}$, $(-7) \equiv 1 \pmod{4}$

$25 \bmod 4 = 1$, $11 \bmod 4 = 3$, $(-1) \bmod 4 = 3$, $(-7) \bmod 4 = 1$

$1 = [5 \bmod 4] = [25 \bmod 4] = [(-7) \bmod 4]$, $3 = [11 \bmod 4] = [(-1) \bmod 4]$

Bad notations: $5 = 9 \bmod 4$, $(-7) = 25 \bmod 4$ ✗

# Arithmetic Modulo $m$, $(\mathbb{Z}_m = \{0, 1, \cdots, m-1\}, +, \times)$

# Arithmetic Modulo $m$, $(\mathbb{Z}_m = \{0, 1, \cdots, m-1\}, +, \times)$

**Arithmetic Modulo $m$, $(\mathbb{Z}_m, +, \times)$, has properties as follows.**

1. addition is closed and associative.
2. $0$ is an additive identity.
3. addition is commutative.
4. the additive inverse of any $a$ is $m - a$.
5. multiplication is closed and associative.
6. $1$ is a multiplicative identity.
7. multiplication is commutative.
8. the distributive property is satisfied.

# Arithmetic Modulo $m$, $(\mathbb{Z}_m = \{0, 1, \cdots, m-1\}, +, \times)$

**Arithmetic Modulo $m$, $(\mathbb{Z}_m, +, \times)$, has properties as follows.**

1. addition is closed and associative.
2. $0$ is an additive identity.
3. addition is commutative.
4. the additive inverse of any $a$ is $m - a$.
5. multiplication is closed and associative.
6. $1$ is a multiplicative identity.
7. multiplication is commutative.
8. the distributive property is satisfied.

- p1,2,4 say that $(\mathbb{Z}_m, +)$ is a group; p1,2,4 + p3, $(\mathbb{Z}_m, +)$ is an abelian group.

# Arithmetic Modulo $m$, $(\mathbb{Z}_m = \{0, 1, \cdots, m-1\}, +, \times)$

**Arithmetic Modulo $m$, $(\mathbb{Z}_m, +, \times)$, has properties as follows.**

1. addition is closed and associative.
2. $0$ is an additive identity.
3. addition is commutative.
4. the additive inverse of any $a$ is $m - a$.
5. multiplication is closed and associative.
6. $1$ is a multiplicative identity.
7. multiplication is commutative.
8. the distributive property is satisfied.

- p1,2,4 say that $(\mathbb{Z}_m, +)$ is a group; p1,2,4 + p3, $(\mathbb{Z}_m, +)$ is an abelian group. p1-8 say that $(\mathbb{Z}_m, +, \times)$ is a ring.

# Arithmetic Modulo $m$, $(\mathbb{Z}_m = \{0, 1, \cdots, m-1\}, +, \times)$

**Arithmetic Modulo $m$, $(\mathbb{Z}_m, +, \times)$, has properties as follows.**

1. addition is closed and associative.
2. $0$ is an additive identity.
3. addition is commutative.
4. the additive inverse of any $a$ is $m - a$.
5. multiplication is closed and associative.
6. $1$ is a multiplicative identity.
7. multiplication is commutative.
8. the distributive property is satisfied.

- p1,2,4 say that $(\mathbb{Z}_m, +)$ is a group; p1,2,4 + p3, $(\mathbb{Z}_m, +)$ is an abelian group. p1-8 say that $(\mathbb{Z}_m, +, \times)$ is a ring.
- If $(\mathbb{Z}_m - \{0\}, \times)$ is also a (multiplicative) group, then $(\mathbb{Z}_m, +, \times)$ is a field. That is, each non-zero element in $\mathbb{Z}_m$ has multiplicative inverse that is an element $a' \in \mathbb{Z}_m$ such that $aa' \equiv a'a \equiv 1 (\bmod m)$.

# Outline

# Group

## Group $(G, '+')$

- $'+'$ is closed;
- $'+'$ is associative;
- There is a unique identity, usually denoted by $0$ and called "zero";
- Any element has a unique inverse.

If $'+'$ is commutative, then $G$ is called *Abelian Group*.

## Examples of Group

$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Z}_m, \oplus)$ (R, x), (Q, x)

# Ring

## Ring $(R,' +',' \cdot')$

- $(R,' +')$ is an Abelian group, the additive identity is denoted by $0$;
- $(R,' \cdot')$ satisfies
  - $'\cdot'$ is closed;
  - $'\cdot'$ is associative;
  - There is a unique multiplicative identity, denoted by $1$;
  - $'\cdot'$ is commutative.
- $'+'$ and $'\cdot'$ satisfy distributive property.

## Examples of Ring

$(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}_m, \oplus, \odot)$

# Field

## Field $(R,'+','\cdot')$

If the non-zero elements of the ring $(R,'+','\cdot')$ form a group under multiplication $'\cdot'$, then $R$ is a field. In other words,

1. $(R,'+')$ is an Abelian group, the additive identity is denoted by $0$;
2. $(R-\{0\},'\cdot')$ is an Abelian group satisfying
   - $'\cdot'$ is closed;
   - $'\cdot'$ is associative;
   - There is a unique multiplicative identity, denoted by $1$;
   - $'\cdot'$ is commutative;
   - Any element in $R-\{0\}$ has a unique multiplicative inverse.
3. $'+'$ and $'\cdot'$ satisfy distributive property.

## Examples of Field

$(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{Z}_m,\oplus,\odot)$ if $m$ is primitive.

# Outline

# Congruence Equations

# Congruence Equations

**Theorem 2.1 (on Page 23)**

The congruence $ax \equiv b(\bmod\ m)$ has a unique solution $x \in \mathbb{Z}_m$ for every $b \in \mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

# Congruence Equations

## Theorem 2.1 (on Page 23)

The congruence $ax \equiv b(\bmod m)$ has a unique solution $x \in \mathbb{Z}_m$ for every $b \in \mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

## Some Useful Definitions

- The greatest common divisor of $a$ and $m$ is denoted by $\gcd(a, m)$.
- Any integer $p > 1$ is prime if it has no positive divisors other than $1$ and $p$.
- Integers $a \geq 1$ and $m \geq 2$ are said to be relatively prime, if $\gcd(a, m) = 1$. (若$a$和$m$的最大公因数为1，则称整数$a \geq 1$和$m \geq 2$互素or 互质.)

# Congruence Equations

## Theorem 2.1 (on Page 23)

The congruence $ax \equiv b(\bmod m)$ has a unique solution $x \in \mathbb{Z}_m$ for every $b \in \mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

## Some Useful Definitions

- The greatest common divisor of $a$ and $m$ is denoted by $\gcd(a, m)$.
- Any integer $p > 1$ is prime if it has no positive divisors other than $1$ and $p$.
- Integers $a \geq 1$ and $m \geq 2$ are said to be relatively prime, if $\gcd(a, m) = 1$. (若$a$和$m$的最大公因数为1，则称整数$a \geq 1$和$m \geq 2$互素or 互质.)

## Examples

- In $\mathbb{Z}$, $2x = 10$ has a unique solution $x = 5$, $4x = 10$ has no solution.
- In $\mathbb{Z}_{26}$, $3x \equiv 6(\bmod 26)$ has a unique solution $x = 2$.
- However, in $\mathbb{Z}_{26}$,$2x \equiv 1(\bmod 26)$ has no solution, and $2x \equiv 6(\bmod 26)$ has solutions $x = 3$ and $x = 16$.

# Outline

# Euler phi-function, $\phi(\cdot)$

## Definitions

- The number of integers in $\mathbb{Z}_m$ that are relatively prime to $m$ is denoted by $\phi(m)$ and called Euler phi-function.
- The collection of integers in $\mathbb{Z}_m$ that are relatively prime to $m$ is denoted by $\mathbb{Z}_m^*$, that is,

$$\boxed{\mathbb{Z}_m^* = \{a | a \in \mathbb{Z}_m \text{ and } \gcd(a, m) = 1\}}$$

# Euler phi-function, $\phi(\cdot)$

## Definitions

- The number of integers in $\mathbb{Z}_m$ that are relatively prime to $m$ is denoted by $\phi(m)$ and called Euler phi-function.
- The collection of integers in $\mathbb{Z}_m$ that are relatively prime to $m$ is denoted by $\mathbb{Z}_m^*$, that is,

$$\mathbb{Z}_m^* = \{a | a \in \mathbb{Z}_m \text{ and } \gcd(a, m) = 1\}$$

- $\phi(m) = |\mathbb{Z}_m^*|$.

# Euler phi-function, $\phi(\cdot)$

## Definitions

- The number of integers in $\mathbb{Z}_m$ that are relatively prime to $m$ is denoted by $\phi(m)$ and called Euler phi-function.
- The collection of integers in $\mathbb{Z}_m$ that are relatively prime to $m$ is denoted by $\mathbb{Z}_m^*$, that is,

$$\boxed{\mathbb{Z}_m^* = \{a | a \in \mathbb{Z}_m \text{ and } \gcd(a, m) = 1\}}$$

- $\boxed{\phi(m) = |\mathbb{Z}_m^*|}$.

## Examples: $m = 7$ and $m = 9$

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
- $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$, $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$
- $\phi(7) = 6, \phi(9) = 6$

# Euler phi-function, $\phi(\cdot)$

## Theorem 2.2 (on Page 23)

Suppose

$$m = \prod_{i=1}^{n} p_i^{e_i}, \tag{4.1}$$

integer prime factorization
整数素数分解

where $\{p_i\}$ are distinct primes and $e_i > 0$. Then

$$\phi(m) = \prod_{i=1}^{n} \left( p_i^{e_i} - p_i^{e_i - 1} \right). \tag{4.2}$$

## Examples

- $m = 7$, $m = 9$, $m = 26$, $m = 60$

# Euler phi-function, $\phi(\cdot)$

## Theorem 2.2 (on Page 23)

Suppose

$$m = \prod_{i=1}^{n} p_i^{e_i}, \tag{4.1}$$

where $\{p_i\}$ are distinct primes and $e_i > 0$. Then

$$\boxed{\phi(m) = \prod_{i=1}^{n} \left(p_i^{e_i} - p_i^{e_i - 1}\right).} \tag{4.2}$$

## Examples

- $m = 7,\ m = 9,\ m = 26,\ m = 60$
- $\phi(7) = 6, \phi(9) = 6, \phi(26) = 12, \phi(60) = 16$

# Outline

# Multiplicative inverse

## Definition of Multiplicative inverse

- Suppose $a \in \mathbb{Z}_m$. The multiplicative inverse of $a$ modulo $m$, denoted $a^{-1} \bmod m$, is an element $a' \in \mathbb{Z}_m$ such that

$$aa' \equiv a'a \equiv 1 \pmod{m}.$$

# Multiplicative inverse

## Definition of Multiplicative inverse

- Suppose $a \in \mathbb{Z}_m$. The multiplicative inverse of $a$ modulo $m$, denoted $a^{-1} \mod m$, is an element $a' \in \mathbb{Z}_m$ such that

$$aa' \equiv a'a \equiv 1 (\mod m).$$

## Example

- In $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $2^{-1} \mod 9 = 5$ since $(2 \times 5) \equiv 10 \equiv 1 (\mod 9)$.
- What is $3^{-1} \mod 9$?

# Multiplicative inverse

## Definition of Multiplicative inverse

- Suppose $a \in \mathbb{Z}_m$. The multiplicative inverse of $a$ modulo $m$, denoted $a^{-1} \mod m$, is an element $a' \in \mathbb{Z}_m$ such that

$$aa' \equiv a'a \equiv 1(\mod m).$$

## Example

- In $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $2^{-1} \mod 9 = 5$ since $(2 \times 5) \equiv 10 \equiv 1(\mod 9)$.
- What is $3^{-1} \mod 9$? It does not exist.

# Multiplicative inverse

## Definition of Multiplicative inverse

- Suppose $a \in \mathbb{Z}_m$. The multiplicative inverse of $a$ modulo $m$, denoted $a^{-1} \mod m$, is an element $a' \in \mathbb{Z}_m$ such that

$$aa' \equiv a'a \equiv 1 (\mod m).$$

## Example

- In $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $2^{-1} \mod 9 = 5$ since $(2 \times 5) \equiv 10 \equiv 1 (\mod 9)$.
- What is $3^{-1} \mod 9$? It does not exist.

## Theorems

The integer $a \in \mathbb{Z}_m$ has a multiplicative inverse modulo $m$ if and only if $\gcd(a, m) = 1$.
That is, any integer in $\mathbb{Z}_m^* = \{a | a \in \mathbb{Z}_m \& \gcd(a, m) = 1\}$ is invertible.
If a multiplicative inverse exists, it is unique modulo $m$.

# Multiplicative inverse

**Examples: $m = 9$**

- in $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, $1^{-1} \bmod 9 = 1$, $2^{-1} \bmod 9 = 5$, $4^{-1} \bmod 9 = 7$, $8^{-1} \bmod 9 = 8$.

# Multiplicative inverse

**Examples: $m = 9$**

- in $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, $1^{-1} \mod 9 = 1$, $2^{-1} \mod 9 = 5$, $4^{-1} \mod 9 = 7$, $8^{-1} \mod 9 = 8$.

**Consider the case of $m = 26$, $\mathbb{Z}_{26} = \{0, 1, 2, \cdots, 25\}$**

- $1^{-1} = 1$, $3^{-1} = 9$, $5^{-1} = 21$, $7^{-1} = 15$, $11^{-1} = 19$, $17^{-1} = 23$, $25^{-1} = 25$; $\phi(26) = 12$
- $2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24?$
- $\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

# Summary

# Homework 1-1

Exercises: 2.1, 2.8, 2.9.

# Thanks for your attention!

# Questions?