

# 同余、中国剩余定理

李辉



## Table of Contents

- 同余
- <u>欧拉定理</u>
- 模逆元
- 同余方程(组)
- 欧几里德扩展算法
- 中国剩余定理



## 同余

### Definition Congruence(同余)

Let a, b, m be integers, with  $m \neq 0$ . Say a is **congruent** to b modulo m ( $a \equiv b \mod m$ ) if  $m \mid (a - b)$ .

#### **Example**

$$3 \equiv 27 \mod 12$$
$$-3 \equiv 11 \mod 7$$



#### Basic properties:

• Congruence compatible with usual arithmetic operations of addition and multiplication.

If 
$$a \equiv b \pmod{m}$$
 and  $c \equiv d \pmod{m}$ ,  $a + c \equiv b + d \pmod{m}$   $ac \equiv bd \pmod{m}$ 

$$4 + 12 \equiv 26 + 1 \pmod{11}$$
  
 $4 \times 12 \equiv 26 \times 1 \pmod{11}$ 



#### Proof.

$$a = b + mk$$

$$c = d + ml$$

$$a + c = b + d + m(k + l)$$

$$ac = bd + bml + dmk + m^{2}kl$$

$$= bd + m(bl + dk + mkl)$$



#### Likewise,

• if  $a \equiv b \pmod{m}$ , then  $a^k \equiv b^k \pmod{m}$ 

#### However, the follows are **NOT TRUE**:

- If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  $a^c \equiv b^d \pmod{m}$ .
- If  $ax \equiv bx \pmod{m}$ , then  $a \equiv b \pmod{m}$ .



#### **Example**

$$4^{12} \neq 4^1 \, (mod \, 11)$$

$$8^2 \neq 3^7 \, (mod \, 5)$$

$$5 \times 2 \equiv 2 \times 2 \pmod{6}$$



## 欧拉定理

**Definition** Residue System

A **complete residue system mod** m is a collection of integer  $a_1a_2\cdots a_m$  such that  $a_i\neq a_j \ mod \ m$  if  $i\neq j$  and any integer n is congruent to some  $a_i \ mod \ m$ .

A **Reduced residue system mod** m is a collection of integer  $a_1a_2\cdots a_m$  such that  $a_i\neq a_j \ mod \ m$  if  $i\neq j$  and  $\gcd(a_i,m)=1$  for all i, and any integer n coprime to m must be congruent to some  $a_i \ mod \ m$ .



#### **Example**

If m=9

• Compete Residue System: {1,2,3,4,5,6,7,8,9}

• Reduced Residue System: {1,2,4,5,7,8}

If m=10

• Compete Residue System: {1,2,3,4,5,6,7,8,9,10}

• Reduced Residue System: {1,3,7,9}



#### **Definition Euler's Totient Function**

The number of elements in a reduced residue system mod m is called **Euler's Totient Function**  $\phi(m)$ .

$$\phi(9) = 6$$
  
 $\phi(10) = 4$ 



#### **Theorem Euler's Theorem**

lf

$$gcd(a,m) = 1$$
,

then

$$a^{\phi(m)} \equiv 1 \mod m$$
.

#### Example

$$3^{\phi(10)} = 81 \equiv 1 \mod 10.$$



#### Proof.

• need a lemma.

Lemma If gcd(a,m)=1 and  $r_1r_2\cdots r_k$  is a reduced residue system mod  $m,k=\phi(m)$ , then  $ar_1\,ar_2\cdots ar_k$  is also a reduced residue system mod m.

#### **Example**

Reduced residue system mod 10:

$$s = \{1,3,7,9\}$$
  
 $7s = \{7,1,9,3\}$ 



Proof of the lemma.

We shall show that  $ar_i$  are all coprime to m and distinct mod m. Since gcd(r,m) and gcd(a,m)=1, so, gcd(ar,m)=1. Also, if  $ar_i\equiv ar_j \ mod \ m$ , then  $m|ar_i-ar_j=a(r_i-r_j)$ .

If gcd(a, m) = 1, then  $m|r_i - r_j \Rightarrow r_i \equiv r_j \mod m$ , which won't be true unless i = j.



Proof of Euler' theorem.

Choose a reduced residue system  $r_1r_2\cdots r_k\ mod\ m$  with  $k=\phi(m)$ . By lemma,  $ar_1\ ar_2\cdots ar_k$  is also a reduced residue system. These two must be permutation of each other mod m. So,

$$\begin{array}{c} r_1r_2\cdots r_k\equiv ar_1\,ar_2\cdots ar_k\,mod\,m\\ r_1r_2\cdots r_k\equiv a^{\phi(m)}r_1\,r_2\cdots r_k\,mod\,m\\ a^{\phi(m)}\equiv 1\,mod\,m, \end{array}$$

because

$$gcd(r_1r_2\cdots r_k,m)=1.$$



## **Corollary Fermat's little Theorem**

If p is a prime and a is an integer, then  $a^p \equiv a (mod \ p)$ 

Proof.

$$\phi(p) = p - 1$$
 ...



$$3^5 \equiv 3 \mod 5$$

$$2^{11}\equiv 2\,mod\,11$$



#### Excise004

What is the last digit of  $27^{123456789}$ ?



## 模逆元

### Definition Inverse of elements mod m

If gcd(a,m)=1, then there is a unique integer  $b \mod m$  such that  $ab \equiv 1 \mod m$ . The b is denoted as  $\frac{1}{a}$  or  $a^{-1} \mod m$ .

$$\frac{1}{5}$$
 mod  $7 = 5^{-1}$  mod  $7 = 3$ .



#### Existence

Since gcd(a, m) = 1, ax + my = 1 for some integers x, y, so  $ax \equiv 1 \mod m$ .

Set b = x.

Uniqueness

If  $ab_1 \equiv 1 \, mod \, m$  and  $ab_2 \equiv 1 \, mod \, m$ , then

 $ab_1 \equiv ab_2 \mod m \Rightarrow m|a(b_1 - b_2).$ 

Since gcd(m, a) = 1,  $m|b_1 - b_2 \Rightarrow b_1 \equiv b_2 \mod m$ .



#### **Theorem Wilson's Theorem**

If p is a prime then  $(p-1)! \equiv -1 \mod p$ 

$$4! = 24 \equiv -1 \mod 5$$



Proof. need a lemma.

Lemma The congruence  $x^2 \equiv 1 \mod p$  has only the solutions  $x \equiv \pm 1 \mod p$ .

Proof.

$$x^{2} \equiv 1 \mod p$$

$$\Rightarrow p | (x^{2} - 1)$$

$$\Rightarrow p | (x + 1)(x - 1)$$

$$\Rightarrow p | x \pm 1$$

$$\Rightarrow x \equiv \pm 1 \mod p$$



Proof of Wilson's Theorem

Assume that p is odd, note that

$$x^2 \equiv 1 \mod p \Rightarrow \gcd(x, p) = 1$$

x has inverse and  $x \equiv x^{-1} \mod p$ .

 $\{1,2,\cdots,p-1\}$  is a reduced residue system mod p.

Pair up elements a with inverse  $a^{-1} \mod p$ .

Only sigletons will be 1 and -1.

$$\equiv (a_1 a_1^{-1})(a_2 a_2^{-1}) \cdots (a_k a_k^{-1})(1)(-1) \bmod p$$

$$\equiv -1 \bmod p$$



## 同余方程(组)

#### **Definition Congruence equation**

A **congruence equation** is of the form  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \equiv 0 \bmod m$  where  $\{a_n, a_{n-1}, \dots, a_0\}$  are integers.

Solution of the congruence equation are integers or residue classes  $\mod m$  that satisfy the equation.



#### **Example**

 $x^2 \equiv -1 \mod 13.$ 

Answer is  $\{5,8\}$ .

 $x^2 \equiv 1 \, mod \, 15.$ 

Answer is  $\{\pm 1, \pm 4 \mod 15\}$ .



Definition Linear Congruence Equation A congruence equation of degree 1 ( $ax \equiv b \mod m$ )

Theorem Let g = gcd(a, m), then there is a solution to  $ax \equiv b \mod m$  if and only if g|b. If it has solutions, then it has exactly g solutions mod m.



#### **Example**

 $4x \equiv 5 \ mod \ 10$  has no solution, because  $g = gcd(4,10) \nmid 5$ .  $4x \equiv 6 \ mod \ 10$  has solution x = 4. In fact, it has g = 2 solutions. The other solution is x = 9.



Proof.

Suppose  $g \nmid b$ .

Suppose  $x_0$  is a solution  $\Rightarrow ax_0 = b + mk$  for some integer k.

Since g|a, g|m, g divides  $ax_0 - mk = b$ , which is a contradict.

So g|b.



 $g=ax_0+my_0$  for integer  $x_0,y_0$ . Let b=b'g, multiply by b' to obtain  $b=b'g=b'(ax_0+my_0)$   $=a(b'x_0)+m(b'y_0)$   $\Rightarrow a(b'x_0)\equiv b\ (mod\ m)$ So,  $x=b'x_0$  is a solution.



Prove that there are exactly g solutions.

Suppose there is one solution  $x_1$ .

Then

$$ax \equiv b \equiv ax_1 \mod m$$
$$a(x - x_1) \equiv 0 \pmod m$$

$$a(x - x_1) = mk$$
 for some integer  $k$   
 $g = gcd(a, m) \Rightarrow a = a'g, m = m'g$ 

So,

$$gcd(a', m') = 1.$$



Then

$$a'g(x - x_1) = m'gk$$

 $\Rightarrow a'(x - x_1) = m'k \text{ for some } k.$ 

So,

$$m'|x-x_1$$
,

Then

$$x \equiv x_1 \mod m'$$
.

So, all solutions are

$$x_1, x_1 + m', x_1 + 2m', \dots, x_1 + (g-1)m'.$$



## 欧几里德扩展算法

## **Extended Euclidean Algorithm** is used to

obtain

$$a^{-1} \mod n$$

when gcd(a, n) = 1.



$$41 = 1 \times 23 + 18$$
  
 $23 = 1 \times 18 + 5$   
 $18 = 3 \times 5 + 3$   
 $5 = 1 \times 3 + 2$   
 $3 = 1 \times 2 + 1$   
 $2 = 2 \times 1$ 



$$1 = 3 - 1 \times 2 = 3 - (5 - 1 \times 3)$$

$$= -1 \times 5 + 2 \times 3$$

$$= -1 \times 5 + 2 \times (18 - 3 \times 5)$$

$$= 2 \times 18 - 7 \times 5$$

$$= 2 \times 18 - 7 \times (23 - 1 \times 18)$$

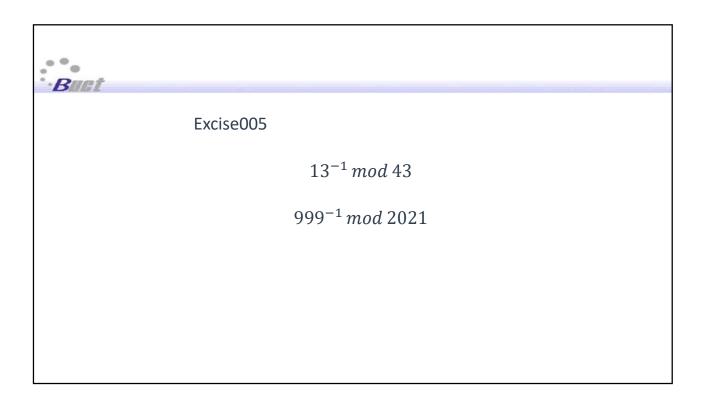
$$= -7 \times 23 + 9 \times 18$$

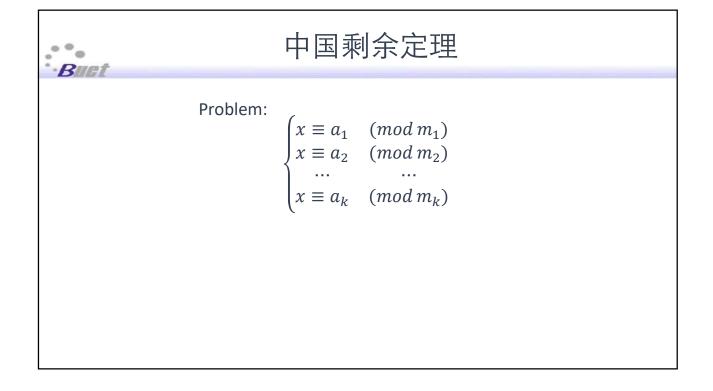
$$= -7 \times 23 + 9 \times (41 - 1 \times 23)$$

$$= 9 \times 41 - 16 \times 23,$$
So,
$$23^{-1} \mod 41 = -16 \text{ or } 25.$$



#### The pseudocode:







## Example

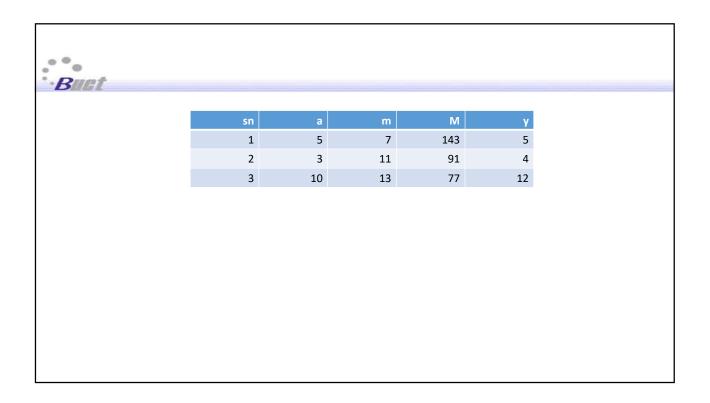
$$\begin{cases} x \equiv 5 & (mod 7) \\ x \equiv 3 & (mod 11) \\ x \equiv 10 & (mod 13) \end{cases}$$



### Solution (Chinese Remainder Theorem)

$$M_i = \frac{\prod m_i}{m_i}$$
$$y_i = M_i^{-1} \mod m_i$$

$$x = \sum a_i M_i y_i \, mod \, (\prod m_i)$$





So, the result ( $\Sigma aMy$ ) is 894 mod 1001.

$$\begin{cases} 894 \equiv 5 & (mod 7) \\ 894 \equiv 3 & (mod 11) \\ 894 \equiv 10 & (mod 13) \end{cases}$$



## Excise006

$$\begin{cases} x \equiv 1 & (mod 7) \\ x \equiv 3 & (mod 11) \\ x \equiv 5 & (mod 13) \\ x \equiv 7 & (mod 19) \end{cases}$$