



# 信息安全数学基础

## 第二章 同余

熊虎

电子科技大学



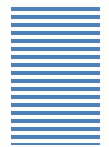
## 第二章 同余



### ➤ 2.1 同余的概念和基本性质

### 2.2 同余类与剩余系

### 2.3 同余方程与中国剩余定理



## 2.1 同余的概念和基本性质



**定义2.1.1**（同余）给定3个整数 $a, b, m$ ，如果 $m|(a - b)$ ，  
则称 $a$ 模 $m$ 同余于 $b$ 或 $a, b$ 模 $m$ 同余，记作 $a \equiv b(\text{mod } m)$ ；  
若 $m \nmid (a - b)$ ，则称 $a, b$ 模 $m$ 不同余。

**注：**由于 $m|(a - b)$ 等价于 $(-m)|(a - b)$ ，所以在后续内容中，总假定 $m$ 是一个正整数。



## 2.1 同余的概念和基本性质



### 定理2.1.1

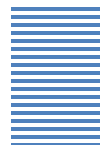
(1)  $a \equiv b \pmod{m}$  当且仅当存在整数  $k$ , 使得  $a = km + b$ 。

**证明思路：** 利用同余和整除的定义可直接验证。

**证明：**  $a \equiv b \pmod{m}$  根据同余的定义有  $m | (a - b)$ , 不妨设

$a - b = km$ , 故  $a = km + b$ 。反之  $a = km + b$ , 则有

$a - b = km$ , 所以  $m | (a - b)$ 。故  $a \equiv b \pmod{m}$ 。



## 2.1 同余的概念和基本性质



### 定理2.1.1

(2) 设  $a = k_1m + r_1$ ,  $b = k_2m + r_2$ ,  $0 \leq r_1 < m$ ,  $0 \leq r_2 < m$ ,  $a \equiv b \pmod{m}$  当且仅当  $r_1 = r_2$ 。

证明:  $a - b = (k_1 - k_2)m + (r_1 - r_2)$ ,  $a \equiv b \pmod{m}$ , 根据同余定义有  $m | (a - b)$

所以  $m | (r_1 - r_2)$ , 又  $0 \leq r_1 < m$ ,

$0 \leq r_2 < m$ , 故有  $r_1 - r_2 = 0$ , 即  $r_1 = r_2$ 。反之, 由  $r_1 = r_2$

可知  $a - b = (k_1 - k_2)m$ , 所以  $m | (a - b)$ 。故  $a \equiv b \pmod{m}$ 。



## 2.1 同余的概念和基本性质



**例2.1.1**  $39 \equiv 29 \pmod{10}$ , 因为  $10 \mid (39 - 29)$ 。

同样  $55 \equiv 3 \pmod{26}$ 。

**例2.1.2** 某月的1号为星期二, 问该月的25号为星期几?

**解:** 因为  $25 \equiv 4 \pmod{7}$ , 而根据已知条件该月的4号为星期五, 所以25号为星期五。



## 2.1 同余的概念和基本性质



**定理2.1.2** 设 $a, b, c, m$  是正整数,

自反性:  $a \equiv a \pmod{m}$  ;

对称性: 若 $a \equiv b \pmod{m}$ , 则 $b \equiv a \pmod{m}$  ;

传递性: 若 $a \equiv b \pmod{m}, b \equiv c \pmod{m}$ , 则 $a \equiv c \pmod{m}$ 。

**证明思路:** 直接利用同余定义验证。



## 2.1 同余的概念和基本性质



**定理2.1.3** 设 $a, b, d, a_1, a_2, b_1, b_2, m$ 为正整数, 则

(1) 若 $a_1 \equiv a_2 \pmod{m}$ ,  $b_1 \equiv b_2 \pmod{m}$ , 则

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m}。$$

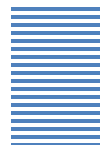
证明:

若 $a_1 \equiv a_2 \pmod{m}$ ,  $b_1 \equiv b_2 \pmod{m}$ , 则 $m|a_1 - a_2$ ,

$m|b_1 - b_2$ , 所以 $m|(a_1 - a_2) + (b_1 - b_2) = m|(a_1 + b_1) - (a_2 + b_2)$ 。

故 $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ 。



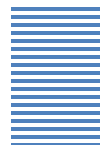


## 2.1 同余的概念和基本性质



(2) 若  $a_1 \equiv a_2 \pmod{m}$ ,  $b_1 \equiv b_2 \pmod{m}$ , 则  
 $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$ 。

证明:  $m \mid (a_1 - a_2) - (b_1 - b_2) = (a_1 - b_1) - (a_2 - b_2)$ ,  
故  $(a_1 - b_1) \equiv (a_2 - b_2) \pmod{m}$ 。



## 2.1 同余的概念和基本性质



### 定理2.1.3

(3) 若  $a_1 \equiv a_2 \pmod{m}$ ,  $b_1 \equiv b_2 \pmod{m}$ , 则

$$a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

证明:

若  $a_1 \equiv a_2 \pmod{m}$ ,  $b_1 \equiv b_2 \pmod{m}$ , 则  $a_1 = k_1 m + a_2$ ,  
 $b_1 = k_2 m + b_2$ , 所以  $a_1 b_1 = (k_1 k_2 m + k_1 b_2 + k_2 a_2) m + a_2 b_2$ , 故  
 $a_1 b_1 \equiv a_2 b_2 \pmod{m}$ .



## 2.1 同余的概念和基本性质



### 定理2.1.3

(4) 若  $ad \equiv bd \pmod{m}$ ，且  $d$  和  $m$  互素，则  $a \equiv b \pmod{m}$ 。

证明：若  $ad \equiv bd \pmod{m}$ ，则  $m | ad - bd = m | (a - b)d$ ，又  $d$  和  $m$  互素，所以  $m | a - b$ ，故  $a \equiv b \pmod{m}$ 。

(5) 若  $a \equiv b \pmod{m}$ ， $d$  是  $a, b, m$  的任意公因数，则

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}。$$

证明：若  $a \equiv b \pmod{m}$ ，则  $m | a - b$ ，从而  $\frac{m}{d} | \frac{a}{d} - \frac{b}{d}$ ，故

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}。$$



## 2.1 同余的概念和基本性质



### 定理2.1.3

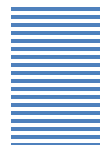
(6) 若  $a \equiv b \pmod{m}$ ,  $d|m$ ,  $d > 0$ , 则  $a \equiv b \pmod{d}$ 。

证明: 若  $a \equiv b \pmod{m}$ , 则  $m|a-b$ , 又  $d|m$ , 所以  $d|a-b$ , 故  $a \equiv b \pmod{d}$ 。

(7) 若  $a \equiv b \pmod{m_i}$ ,  $i = 1, 2, \dots, k$ , 则

$$a \equiv b \pmod{\text{lcm}[m_1, m_2, \dots, m_k]}。$$

证明: 若  $a \equiv b \pmod{m_i}$ ,  $i = 1, 2, \dots, k$ , 则  $m_i|a-b$ ,  $i = 1, 2, \dots, k$ , 所以  $\text{lcm}[m_1, m_2, \dots, m_k]|a-b$ , 故  $a \equiv b \pmod{\text{lcm}[m_1, m_2, \dots, m_k]}$ 。



## 2.1 同余的概念和基本性质



**例2.1.3**  $30 \equiv 3(\text{mod } 9)$  ,  $47 \equiv 2(\text{mod } 9)$  , 则

$$77 \equiv 30 + 47 \equiv 3 + 2 \equiv 5(\text{mod } 9)$$

$$1410 \equiv 30 \cdot 47 \equiv 3 \cdot 2 \equiv 6(\text{mod } 9)$$

由于3是30, 3, 9的公因数, 所以

$$\frac{30}{3} \equiv \frac{3}{3}(\text{mod } \frac{9}{3}) , \text{ 即 } 10 \equiv 1(\text{mod } 3)$$

由于  $3|9$ , 所以

$$47 \equiv 2(\text{mod } \frac{9}{3}) , \text{ 即 } 47 \equiv 2(\text{mod } 3)$$



## 2.1 同余的概念和基本性质



**例2.1.4** 计算  $3^{801} \pmod{10}$

**解：** 因为  $3^2 \equiv 9 \pmod{10}$ ,  $3^3 \equiv 7 \pmod{10}$ ,  $3^4 \equiv 1 \pmod{10}$ ,

又  $801 = 4 \times 200 + 1$ , 所以

$$3^{801} = 3^{4 \times 200 + 1} = (3^4)^{200} \times 3 \equiv 1 \times 3 \pmod{10} = 3 \pmod{10}$$

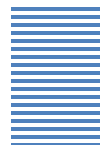
**例2.1.5** 设  $n$  是一个十进制整数, 设  $n = (a_k a_{k-1} \cdots a_0)_{10}$ , 则

(1)  $3|n$  的充要条件是  $3 | \sum_{i=0}^k a_i$ ; (2)  $9|n$  的充要条件是  $9 | \sum_{i=0}^k a_i$ ;

**证明：**  $n$  的十进制表示形式为

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$$

因为  $10 \equiv 1 \pmod{3}$ , 所以  $n = \sum_{i=0}^k a_i \pmod{3}$ , 因此  $3|n$



## 2.1 同余的概念和基本性质



的当且仅当  $3 \mid \sum_{i=0}^k a_i$ 。对于9的情形同理可证。

**例2.1.6** 设  $n = 6789$ ，则  $n$  可被3整除，但不能被9整除。

解：因为  $\sum_{i=0}^k a_i = 6 + 7 + 8 + 9 = 30$ ，又  $3 \mid 30$ ， $9 \nmid 30$ ，

所以  $3 \mid 6789$ ， $9 \nmid 6789$ 。



谢谢！