同余

Congruent

刘铎

liuduo@bjtu.edu.cn

同余

- 设 n 是正整数，a 和 b 是整数，如果 $n|(a-b)$，则称 a **模 n 同余于 b**，或 **a 与 b 模 n 同余（congruent）**，记作 $a \equiv b \pmod{n}$，n 称为**模（modulus）**
- 例
  - $70 \equiv 5 \pmod{13}$
  - $-19 \equiv 6 \pmod{25}$

同余

- 定理

  以下命题等价：

  (a) a 与 b 模 n 同余；

  (b) $a \bmod n = b \bmod n$；

  (c) $a = b+kn$，其中 k 是整数。

- 注：$b|a$ 当且仅当 $a \bmod b = 0$，

  当且仅当 $a \equiv 0 \pmod{b}$ 。

同余

- 定理

若$a \equiv b \pmod{n}$，$c \equiv d \pmod{n}$，则

$$a \pm c \equiv b \pm d \pmod{n},$$

$$ac \equiv bd \pmod{n}。$$

$$\begin{aligned} ac - bd &= ac - bc + bc - bd \\ &= (a-b)c + b(c-d) \end{aligned}$$

同余

+ （mod 4）	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

× （mod 4）	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

End