# 第三课时　同余的表示

一、概念

1. 同余的定义　设 $m$ 是正整数，$a$、$b$ 是整数．若 $m\mid(a-b)$，则称 $a$ 和 $b$ 关于模 $m$ 同余，记作 $a\equiv b(\bmod m)$．
2. 同余的基本性质
   （1）$a\equiv a(\bmod m)$
   （2）若 $a\equiv b(\bmod m)$，则 $b\equiv a(\bmod m)$
   （3）若 $a\equiv b(\bmod m)$，则 $b\equiv c(\bmod m)$，则 $a\equiv c(\bmod m)$
   （4）若 $a\equiv b(\bmod m)$ 且 $c\equiv d(\bmod m)$，则 $a+c\equiv b+d(\bmod m)$ 且 $ac\equiv bd(\bmod m)$
   （5）若 $a\equiv b(\bmod m)$，则对任意的正整数 $n$ 有 $a^n\equiv b^n(\bmod m)$ 且 $an\equiv bn(\bmod mn)$

3. 剩余类的概念

同余类或剩余类：把全体整数分为这样的若干个两两不相交的集合，使得在同一个集合中的任意两个数对模 $n$ 一定同余，而属于不同集合中的两个数对模 $n$ 一定不同余.每一个这样的集合称为模 $n$ 的同余类或模 $n$ 的剩余类. $M_i=\{x\mid x\in Z,x\equiv i(\bmod n)\}$

4. 剩余类性质：

（1）模 n 共有__n__个不同的剩余类；

（2）在任意取定的 $n$+1 个整数中，必有两个数对模 $n$ 同余；

（3）若 i 与 $n$ 互素，则同余类 $M_i$ 中的所有数都和 $n$ 互素；

（4）同余类 $M_i$ 中的所有数与 n 的最大公约数相等.

5. 完全剩余系：在 n 个剩余类中各任取一个数作为代表，这样的 n 个数称为模 n 的一个完全剩余系，简称模 n 的完系.例如：0,1,2，…，n-1 是模 n 的一个完系，这称作模 n 的最小非负完系.

缩同余类：性质 3 中同余类 $M_i$ 中的所有数都和 n 互素，这样的同余类称为模 n 的缩同余类.

我们将模 n 的缩同余类的个数记作 $\varphi(n)$，称为欧拉函数.若 $p$ 是素数时，有 $\varphi(p)=p-1$.

一般地：设正整数 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则 $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

特别地：对素数 $p$ 有 $\varphi(p)=p-1,\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

缩剩余系：在模 n 的 $\varphi(n)$ 个缩同余类中各取一个数作为代表，这样的 $\varphi(n)$ 个数称为模 n 的一个缩剩余系，简称模 n 的缩系.不超过 n 且与 n 互素的 $\varphi(n)$ 个正整数称为模 n 的最小正缩系.

## 二、经典例题

例 1　证明：完全平方数模 4 同余 0 或 1.

证明：若 $a=4k$，则 $a^2\equiv 0^2\equiv 0 \pmod 4$

若 $a=4k+1$，则 $a^2\equiv 1^2\equiv 1 \pmod 4$

若 $a=4k+2$，则 $a^2\equiv 2^2\equiv 0 \pmod 4$

若 $a=4k+3$，则 $a^2\equiv 3^2\equiv 1 \pmod 4$

综上，命题得证

例 2　(1)计算 $3^{300}$ 的个位数字；

(2)计算 $15^{100}$ 除以 17 的余数.

(1)解：$3^{300}$
$\equiv (3^4)^{75}$
$\equiv 1^{75}$
$\equiv 1 \pmod{10}$

(2)解：$15^{100}$
$\equiv (-2)^{100}$
$\equiv [(-2)^4]^{25}$
$\equiv (-1)^{25}$
$\equiv -1 \pmod{17}$

例 3　求 $2001\times 2002+2003\times 2004+2005\times 2006$ 除以 45 的余数.

解：$2001\times 2002+2003\times 2004+2005\times 2006$
$\equiv 21\times 22+23\times 24+25\times 26$
$\equiv -24\times 22+23\times 24+50\times 13$
$\equiv 674$
$\equiv 44 \pmod{45}$

例 4　求证:对于任何正整数 $k$,均有 $7\,|\,2^{3k+1}+3^{6k}+5^{6k}+3$.

证明：对 $k$ 归纳，即证 $7\,|\,2^{3k+1}\cdot 7+3^{6k}(3^6-1)+5^{6k}(5^6-1)$

$\because 3^6-1=(3^3)^2-1=26\times 28$　$\therefore 7\,|\,3^6-1$，$7\,|\,5^6-1$

$\therefore 7\,|\,2^{3k+1}\cdot 7+3^{6k}(3^6-1)+5^{6k}(3^6-1)$

$\therefore 7\,|\,2^{3k+1}+3^{6k}+5^{6k}+3 \Rightarrow 7\,|\,2^{3(k+1)+1}+3^{6(k+1)}+5^{6(k+1)}+3$

又 $\because$ $k=0$ 时，$2^{3k+1}+3^{6k}+5^{6k}+3=7$，$7\,|\,7$，成立

$\therefore$ 对于 $k\geq 0$，均有 $7\,|\,2^{3k+1}+3^{6k}+5^{6k}+3$

$\therefore$ 命题得证

三、巩固练习

1.证明:完全平方数模 3 同余 0 或 1.

证明: 记 $a \bmod 3$ 为 $\bar{a}$, 且 $\bar{a} \in [0,2]$

$\therefore \overline{a^2} \in \{\overline{0^2}, \overline{1^2}, \overline{2^2}\}$

$\therefore \overline{a^2} \in \{0,1\}$

2 证明:完全平方数模 8 同余 0,1,或 4.

证明: 记 $a \bmod 8$ 为 $\bar{a}$, 且 $\bar{a} \in [0,1]$

$\therefore \overline{a^2} \in \{\overline{0^2}, \overline{1^2}, \overline{2^2}, \overline{3^2}, \overline{4^2}, \overline{5^2}, \overline{6^2}, \overline{7^2}\}$

$\therefore \overline{a^2} \in \{0,1,4\}$

3.证明:整数的四次幂模 16 同余 0 或 1.

证明: 记 $a \bmod 16$ 为 $\bar{a}$, $\bar{a} \in [0,15]$

$\therefore \overline{a^2} \in \{0,1,4,9\}$

$\therefore \overline{a^4} \in \{0,1\}$

4. (1)求所有整数 $x$ ,使得 $5x \equiv 4 \pmod{11}$ ;

(2)所有整数 $x$ ,使得 $6x \equiv 1 \pmod{8}$ .

(1)解: $5x \pmod{11}$

$= 5 \pmod{11} \cdot x \pmod{11}$

$= 4 \pmod{11}$

$= 15 \pmod{11}$

$\therefore x = 3 \pmod{11}$

(2)解: $6x = 8a+1$ , $a \in Z$

$\because$ $6x$ 为偶, $1+8a$ 为奇

$\therefore$ 无解

5.已知正整数 $n \leq 100$ ,使得 $1+2+3+\cdots+n$ 的结果为 8 的倍数,求满足要求的 $n$ 的个数.

解: $8 \mid \frac{(n+1)n}{2}$

$\therefore 16 \mid n(n+1)$

$\because (n, n+1) = 1$

$\therefore 16 \mid (n+1)$ 或 $16 \mid n$

$\because n+1 \leq 101$ , $n \leq 100$

$\therefore [\frac{101}{16}] = 6$ , $[\frac{100}{16}] = 6$

$\therefore$ 有12个

6. “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?”

解: $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$

$\therefore \begin{cases} 35x \equiv 70 \pmod{105} \\ 21x \equiv 63 \pmod{105} \\ 15x \equiv 30 \pmod{105} \end{cases}$

$\therefore x \equiv 23 \pmod{105}$