同　　余

知识、方法、技能

同余是数论中的重要概念，同余理论是研究整数问题的重要工作之一.本讲介绍同余的基本概念，剩余类和完全剩余系，同余方程，整数模的阶和中国剩余定理.

Ⅰ.基本概念

定义一：设 m 是一个给定的正整数.如果两个整数 a,b 用 m 除所得的余数相同，则称 a,b 对模 m 同余，记为 $a\equiv b(\mathrm{mod}\,m)$；否则，记为 $a\not\equiv b(\mathrm{mod}\,m)$.

例如，15≡7（mod 4），$-2\not\equiv 12$（mod 7）.

同余有如下两种等价定义法：

定义一* 若 m|(a－b)，则称 a、b 对模 m 同余.

定义一**若 a=b+mt(t∈Z)，则称 a、b 对模 m 同余.

同余的基本性质：

（1） $a\equiv 0(\mathrm{mod}\,m)\Leftrightarrow m\mid a.$

（2） $a\equiv a(\mathrm{mod}\,m)$(反身性)

$a\equiv b(\mathrm{mod}\,m)\Leftrightarrow b\equiv a(\mathrm{mod}\,m)$(对称性)

$\left.\begin{array}{l}a\equiv b(\mathrm{mod}\,m)\\ b\equiv c(\mathrm{mod}\,m)\end{array}\right\}\Leftrightarrow a\equiv c(\mathrm{mod}\,m)$(传递性)

（3）若 $a\equiv b(\mathrm{mod}\,m),c\equiv d(\mathrm{mod}\,m)$,则

① $a\pm c\equiv b\pm d(\mathrm{mod}\,m);$

② $ac\equiv bd(\mathrm{mod}\,m).$

（4）若 $a_i\equiv b_i(\mathrm{mod}\,m),i=0,1,2,\cdots,n.$则,$a_nx^n+\cdots+a_1x+a_0=b_nx^n+\cdots+b_1x+b_0(\mathrm{mod}\,m).$

特别地，设 $f(x)=a_nx^n+\cdots+a_1x+a_0(a_i\in Z)$,若$a\equiv b(\mathrm{mod}\,m)$，则 $f(a)\equiv f(b)(\mathrm{mod}\,m).$

（5）若 $ac\equiv bc(\mathrm{mod}\,m)$,则$a\equiv b(\mathrm{mod}\dfrac{m}{(m,c)})$.特别地，又若（c,m）=1，则 $a\equiv b(\mathrm{mod}\,m).$

【证明】因 $m \mid c(a-b)$, 这等价于 $\frac{m}{(m,c)} \mid \frac{c}{(m,c)}(a-b)$. 又因若（a,b）$= d \Rightarrow (\frac{a}{d}, \frac{b}{d})$ =1

（d≠0）及 b|ac，且（b,c）=1 $\Rightarrow b \mid a$,

从而有 $\frac{m}{(m,c)} \mid (a-b)$.

这个性质说明同余式两边的同一非零因数，不能像等式那样“约去”，只有当这非零因数与模互质时，才可“约去”.

（6） $a \equiv b(\mathrm{mod}\, m)$, 而 $d \mid m(d>0)$, 则 $a \equiv b(\mathrm{mod}\, d)$.

（7）设 $a \equiv b(\mathrm{mod}\, m)$,

①若 c>0，则 $ac \equiv bc(\mathrm{mod}\, mc)$;

②d 为 a、b、m 的任一公约数，则 $\frac{a}{d} \equiv \frac{b}{d}(\mathrm{mod}\frac{m}{d})$.

（8）若 $a \equiv b(\mathrm{mod}\, m_1), a \equiv b(\mathrm{mod}\, m_2)$ 且 $(m_1, m_2) = 1$, 则 $a \equiv b(\mathrm{mod}\, m_1 m_2)$.

（9）若 $a \equiv b(\mathrm{mod}\, m)$, 则 $(a, m) = (b, m)$.

Ⅱ.剩余类和完全剩余系

若按对某一模 m 的余数进行分类，就可以引入所谓的剩余类和完全剩余系的概念.

定义二：设 m∈N*，把全体整数按其对模 m 的余数 r（0≤r≤m－1）归于一类，记为 k_r，每一类 k_r（r=0,1,⋯,m－1）均称模 m 的剩余类（又叫同余类）.同一类中任一数称为该类中另一数的剩余.

剩余类 k_r 是数集 $k_r = \{qm + r \mid m$是模, r是余数, $q \in Z\}$, 也即 $k_r = \{a \mid a \in Z$且$a \equiv r(\mathrm{mod}\, m)\}$, 它是一个公差为 m 的（双边无穷）等差数列.

根据定义，剩余类具有如下性质：

（1） $Z = k_0 \cup k_1 \cup k_2 \cdots \cup k_{m-1}$, 而 $k_i \cap k_j = \phi(i \neq j)$;

（2）对任一数 n∈Z，有惟一的 r_0 使 $n \in k_{r_0}$ ；

（3）对任意的 a,b∈Z，a,b $\in k_r \Leftrightarrow a \equiv b(\mathrm{mod}\, m)$.

定义三：设 $k_0, k_1, \cdots, k_{m-1}$ 是模 m 的（全部）剩余类.从每个 k_r 中任取一个数 a_r,这 m 个数 $a_0, a_1, \cdots, a_{m-1}$ 组成的一个组称为模 m 的一个完全剩余系，简称完系.

例如，取 m=4，则有 $k_0=\{\cdots,-8,-4,0,4,8\cdots\}, k_1=\{\cdots,-7,-3,1,5,9,\cdots\}$，$k_2$={…，－6，－2，2，6，10，…}，$k_3$={…，－5，－1，3，7，11，…}.数组 0，1，2，3；－8，5，2，－1 等等都是模的 4 的一个完全剩余系.

显然，模 m 的完全剩余系有无穷多个.但最常用的是下面两种：

（1）非负数最小完全剩余系：0，1，2，…，m－1；

（2）绝对值最小完全剩余系：它随 m 的奇偶性不同而略有区别.

当 $m=2k+1$ 时,为 $-k,-(k-1),\cdots,-1,0,1,\cdots,(k-1),k.$（对称式）

当 $m=2k$ 时,为 $-(k-1),-(k-2),\cdots,-1,0,1,(k-1),k.$ 或 $-k,-(k-1),\cdots,-1,0,1,\cdots,(k-1).$

由定义不难得到如下判别完全剩余系的方法：

定理一：m 个整数 $a_1,a_2,\cdots,a_m$ 是模 m 的一个完系 $\Leftrightarrow$ 当 $i\neq j$ 时，$a_i\not\equiv a_j(\mathrm{mod}\,m)$

定理二：设 $(b,m)=1$，c 为任意整数.若 $a_1,a_2,\cdots,a_n$ 为一个完系，则 $ba_1+c,ba_2+c,\cdots,ba_m+c$ 也是模 m 的一个完全剩余系.

特别地，任意 m 个连续整数构成模 m 的一个完全剩余系.

【证明】只需证明：当 $i\neq j$ 时,$ba_i+c\equiv ba_j+c(\mathrm{mod}\,m)$. 而这可用反证法得证.下略.

设 m 为一正整数，由于在 0，1，…，m－1 中与 m 互质的数的个数是由 m 惟一确定的一个正整数，因此，可给出如下定义.

定义四：m 为一正整数，把 0，1，…，m－1 与 m 互质的数的个数叫做 m 的欧拉函数，记为 $\varphi(m)$.

显然，$\varphi(m)$ 的定义域是正整数 N*，前 n 个值为：

$\varphi(1)=0,\varphi(2)=1,\varphi(3)=2,\varphi(4)=2,\varphi(5)=4,\varphi(6)=2,\varphi(7)=6,\cdots$，当 m=p 为质数时，$\varphi(p)=p-1.$

设 k 是模的一个剩余类.若 a、b∈k，则 $a\equiv b(\mathrm{mod}\,m)$. 于是由性质 9 知，（$a$,m）=（b,m）. 因此，若（$a$,m）=1，则 k 中的任一数均与 m 互质.这样，又可给出如下定义.