同 余（续 1）

定义五：如果一个模 m 的剩余类 k_r 中任一数与 m 互质，则称 k_r 是与模 m 互质的剩余类；在与模 m 互质的每个剩余类中任取一个数（共 $\varphi(m)$ 个）所组成的数组，称为模 m 的一个简化剩余系.

例如，取 m=6，在模 6 的六个剩余类中，

$k_1=\{\cdots,-11,-5,1,7,13,\cdots\}$,

$k_5=\{\cdots,-7,-1,5,11,17,\cdots\}$是与模 6 互质的剩余类.数组 1，5；7，－7；1，－1；等等都是模 6 的简化剩余类.

由此定义，不难得到：

定理三: $a_1,a_2,\cdots,a_{\varphi(m)}$ 是模 m 的简化剩余系

$\Leftrightarrow (a_i,m)=1$, 且$a_i\not\equiv a_j(\mathrm{mod}\,m)(i\neq j,i,j=1,2,\cdots\varphi(m))$.

定理四：在模 m 的一个完全剩余系中，取出所有与 m 互质的数组成的数组，就是一个模 m 的简化剩余系.

这两个定理，前者是简化剩余系的判别方法，后者是它的构造方法.显然，模 m 的简化剩余系有无穷多个，但常用的是“最小简化剩余系”，即由 1，2，…，m－1 中与 m 互质的那些数组成的数组.由定理不难证得简化剩余系的如下性质定理.

定理五：设 $a_1,a_2,\cdots,a_{\varphi(m)}$ 是模 m 的简化剩余系.若（k,m）=1，则 $ka_1,ka_2,\cdots,ka_{\varphi(m)}$ 也是模 m 的简化剩余系.

下面介绍两个有关欧拉函数的重要结论.其证明略.

定理六：（欧拉定理）若（a,m）=1，则 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$

特别地，（费马小定理）若 m=p 为质数， $p\nmid a$ ，则 $a^{p-1}\equiv 1(\mathrm{mod}\,p)$.

定理七：（威尔逊定理）设 p 素数，则（p－1）！ $\equiv -1(\mathrm{mod}\,p)$.

定理八：（欧拉函数值计算公式）令 m 的标准分解式为

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

则
$$\varphi(m)=m\prod_{i=1}^{k}(1-\frac{1}{p_i}).$$

例如，30=2・3・5，则 $\varphi(30)=30(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=8.$

读者应认识到：由于任何整数都属于模 m 的某一剩余类，所以，在研究某些整数性质时，选取适当的（模）m，然后在模 m 的每个剩余类中取一个“代表数”（即组成一个完全剩余系），当弄清了这些代表数的性质后，就可弄清对应的剩余类中所有数的性质，进而弄清全体整数的性质，这就是引入剩余类和完全剩余系的目的.

III.同余方程

设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 为 x 的整系数多项式.类似于多项式和代数方程式的有关定义，我们有

定义六：同余式 $f(x)\equiv 0(\mathrm{mod}\,m), a_n\not\equiv 0(\mathrm{mod}\,m)$ 叫做一元 n 次同余方程.例如，

$9x^7-3x^5+5x^2-3\equiv 0(\mathrm{mod}\,3)$ 是七次同余方程.

定义七：若 c 使得 $f(c)\equiv 0(\mathrm{mod}\,m)$ 成立,则 $x\equiv c(\mathrm{mod}\,m)$ 叫做同余方程 $f(x)\equiv 0(\mathrm{mod}\,m)$ 的一个解.

显然，同余方程的解是一些剩余类，而不仅是一个或 n 个类.例如， $x\equiv 1(\mathrm{mod}\,5),$ $x\equiv 4(\mathrm{mod}\,5)$ 都是二次同余方程 $x^2\equiv 1(\mathrm{mod}\,5)$ 的解.

1．一次同余方程

$ax\equiv b(\mathrm{mod}\,m)$（其中 $m\nmid a$）称为一次同余方程.关于它的解，有如下共知的结论：

定理九：若（a,m）=1，则 $ax\equiv b(\mathrm{mod}\,m)$ 有一个解.

定理十：若（a,m）=d>1， $d\nmid b$，则 $ax\equiv b(\mathrm{mod}\,m)$ 无解，其中 $a\not\equiv 0(\mathrm{mod}\,m)$.

定理十一：若（a,m）=d>1，d|b，则 $ax\equiv b(\mathrm{mod}\,m)$ 有 d 个解.并且，若 $\alpha x=\beta(\mathrm{mod}\,m_1)$ 的一个解为 $x\equiv r(\mathrm{mod}\,m_1)$, 则 d 个解为： $x\equiv r+km_1(\mathrm{mod}\,m), k=0,1,\cdots,d-1$，

其中 $\alpha=\frac{a}{d},\beta=\frac{b}{d},m_1=\frac{m}{d}.$

下面介绍一次同余方程

$ax\equiv b(\mathrm{mod}\,m),(a,m)=1$ （*）

的解法.

【解法 1】因（a,m）=1，则存在二数 s,t，使得 as+mt=1，即 $as=1(\mathrm{mod}\,m)$，由此有

$asx \equiv bs(\mathrm{mod}\, m)$,于是$x \equiv bs(\mathrm{mod}\, m)$为（*）的解.

【解法 2】先把（*）变形成$x \equiv \frac{b}{a}(\mathrm{mod}\, m)$($\frac{b}{a}$仅只是形式上的记号），然后用与 m 互质的数陆续乘右端的分子分母，直至把分母绝对值变成 1（通过分子分母各对模 m 取余数）而得到解.

【解法 3】得用欧拉定理.因$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$,由$ax \equiv b(\mathrm{mod}\, m)$可得$a^{\varphi(m)}x \equiv b \cdot a^{\varphi(m)-1}(\mathrm{mod}\, m)$,从而有解　　$x \equiv b \cdot a^{\varphi(m)-1}(\mathrm{mod}\, m).$

2．一次同余方程组

定义八：若数 r 同时满足 n 个同余方程：$f_k(x) \equiv 0(\mathrm{mod}\, m_k), k = 1,2,\cdots,n.$则$r$叫做这 n 个同余方程组成的同余方程组的解.

定理十二：对同余方程组

$$\begin{cases} x \equiv c_1(\mathrm{mod}\, m_1), \\ x \equiv c_2(\mathrm{mod}\, m_2). \end{cases}$$

记$(m_1, m_2) = d, [m_1, m_2] = M.$

①若$d \nmid c_1 - c_2$，则此同余方程组无解；

②若$d \mid c_1 - c_2$，则此同余方程组有对模 M 的一类剩余解.

Ⅳ.模 m 的阶和中国剩余定理

（1）模 m 的阶

定义九：设 m>1 是一个固定的整数，a 是与 m 互素的整数，则存在整数 k，1≤k＜m，使得$a^k \equiv 1(\mathrm{mod}\, m)$.我们将具有这一性质的最小正整数（仍记为 k）称为 a 模 m 的阶.

a 模 m 的阶具有如下性质：

①设$(a,m) = 1, k$是a模m的阶，u, v是任意整数，则$a^u \equiv a^v(\mathrm{mod}\, m)$的充要条件是$u \equiv v(\mathrm{mod}\, k)$.

特别地，$a^u \equiv 1(\mathrm{mod}\, m)$的充分必要条件是 k|u.

【简证】充分性显然.

必要性.设$u > v$,记$l = u - v$,则由$a^u \equiv a^v(\mathrm{mod}\, m)$及$(a,m) = 1$易知$a^l \equiv 1(\mathrm{mod}\, m).$用带余除法，$l = kq + r$，这里$0 \le r < k$，故$a^{kq} \cdot a^r \equiv 1(\mathrm{mod}\, m)$，即$a^r \equiv 1(\mathrm{mod}\, m)$。由$0 \le r < k$及 k 的定义知，必须 r=0，所以$u \equiv r(\mathrm{mod}\, k).$

②设$(a,m) = 2, a$模 m 的阶为 k，则数列$a, a^2, a^3, \cdots,$模 m 是周期的，且最小正周期是

k，而 k 个数 $a, a^2, \cdots, a^k$ 模 m 互不同余.

③设 $(a,m)=1$,则 a 模 m 的阶整除欧拉函数 $\varphi(m)$. 特别地，若 m 是素数 p，则 a 模 p 的阶整除 p－1.

（2）中国剩余定理（即孙子定理）

设 $n \geq 2, m_1, m_2, \cdots, m_n$ 是两两互质的正整数，记 M=$\prod_{i=1}^{n} m_i, M_i = \frac{M}{m_i}(i=1,2,\cdots,n)$ 则

同余方程组　$x \equiv c_i (\mathrm{mod}\, m_i)(i=1,2,\cdots,n)$

有且只有解　$x \equiv \sum_{i=1}^{n} M_i \alpha_i c_i (\mathrm{mod}\, M).$　（△）

其中 $M_i \alpha_i \equiv 1(\mathrm{mod}\, m_i), i=1,2,\cdots,n.$　（△△）

【证明】由 $(m_i, m_j)=1(i \neq j)$ 知，$(M_i, m_j)=1$，因此每一个同余方程 $M_{iy} \equiv 1(\mathrm{mod}\, m_i)$（$i$=1，2，…n）都有解，于是必存在 α_i，使得 $M_i \alpha_i \equiv 1(\mathrm{mod}\, m)$。又因 $M = m_i M_i, m_i \mid M_i (i \neq j),$ 所以对模 $m_i (i=1,2,\cdots,n)$ 有 $M_1\alpha_1 c_1 + \cdots + M_i \alpha_i c_i + \cdots + M_n \alpha_n c_n \equiv M_i \alpha_i c_i \equiv c_i (\mathrm{mod}\, m_i).$ 故（△△）是（△）的解.

若 x_1, x_2 是适合（△）的任意两个解，则 $x_1 = x_2 (\mathrm{mod}\, m_i), i=1,2,\cdots,n,$ 因 $(m_i, m_j)=1(i \neq j).$ 故 $x_1 \equiv x_2 (\mathrm{mod}\, m_1 m_2 \cdots m_n)$，即 $x_1 \equiv x_2 (\mathrm{mod}\, M),$ 因此，（△△）是（△）的惟一解.