# 整 数 论

第一卷 第二分册

张德馨 著

中国人民解放军洛阳外国语学院翻印

1980

# 第 五 章

# 平 方 剩 余

## § 1．平方剩余和平方非剩余

一元二次同余式的一般形式是

$$ax^2+bx+c\equiv 0 \pmod m, \qquad (1)$$

这里是 $a\not\equiv 0 \pmod m$.

若用$4a$乘(1)式的两边和模$m$，则得

$$4a^2x^2+4abx+4ac\equiv 0 \pmod{4am}. \qquad (2)$$

(1)式的根很明显也是(2)式的根，(2)式的根很明显也是(1)式的根。不过(1)式是以$m$为模的，(2)式是以$4am$为模的。故由(1)式的一个根可以得出(2)式的$4a$个根。又若$x_1$为(2)式的一个根，则

$$x_1+km,\ k=0,\ 1,\ 2,\ \cdots,\ 4a-1,$$

也都是(2)式的根，这$4a$个数对于(2)式来说是不同余根，对于(1)式来说则是一个根。所以恒是(2)式的$4a$个根和(1)式的一个根相对应。

(2)式可以写成

$$(2ax+b)^2\equiv b^2-4ac \pmod{4am}.$$

若令

$$y=2ax+b,$$

$$D=b^2-4ac,$$

则得

$$y^2\equiv D \pmod{4am}. \qquad (3)$$

若(3)式没有解，则(2)式不能有解，当然(1)式也没有解。

若(3)式的一个根是$y_1$，则(2)和(1)式的根应该是

$$x_1=\frac{y_1-b}{2a}.$$

故若$2a\nmid(y_1-b)$，则(1)式没有和$y_1$对应的根；若$2a\mid(y_1-b)$，则(1)式有一个根$x_1$。这样就可从(3)式的全部的根找出(2)式的全部根，因而也就得出(1)式的全部的根。

所以我们得到下面的

**定理1**．形状为(1)的同余式恒可以化成形状为(3)的同余式。也可以说，一个一般的三项的二次同余式像(1)恒可以化成一个二项的二次同余式像(3)。

在从(1)变成(3)的过程中有时可以作一些简化如下：

Ⅰ．若$(a, m)=1$，则必有一个$\alpha$，能使

$$a\alpha\equiv 1 \pmod{m}.$$

找出这个$\alpha$来。用$\alpha$乘(1)式，并因$(\alpha, m)=1$，所以得

$$x^2+b_1x+c_1\equiv 0 \pmod{m}.$$

所以(2)式变成

$$4x^2+4b_1x+4c_1\equiv 0 \pmod{4m},$$

即

$$(2x+b_1)^2\equiv b_1^2-4c \pmod{4m}.$$

所以(3)式变成

$$y^2\equiv D \pmod{4m}.$$

Ⅱ．若(1)式的$b$是偶数，$b=2l$，则只用$a$乘(1)式就行。这样(2)式变成

$$a^2x^2+2alx+ac\equiv 0 \pmod{am},$$

即

$$(ax+l)^2\equiv l^2-ac \pmod{am}.$$

所以(3)式变成

$$y^2\equiv D \pmod{am}.$$

若(1)式的 $b$ 是奇数，而 $m$ 也是奇数，则可把(1)式写成

$$ax^2+(b+m)x+c\equiv 0 \pmod{m},$$

这样 $x$ 的系数也就变成偶数了。

Ⅱ．若在 $b=2l$ 的同时，还有 $(a, m)=1$，则(2)式可以变成

$$a^2x^2+2alx+ac\equiv 0 \pmod{m},$$

或

$$x^2+2alx+\alpha c\equiv 0 \pmod{m},$$

这里是 $a\alpha\equiv 1 \pmod{m}$.

所以(3)式变成

$$y^2\equiv D \pmod{m}.$$

总结以上所讲，我们得到下列的结论：

解一般的二次同余式的问题归结到如何解

$$x^2\equiv a \pmod{m} \qquad (4)$$

这样形状的同余式，而这样的同余式的解法又归结到如何解同余式

$$x^2\equiv a \pmod{p^\alpha}, \qquad (5)$$

这里 $p$ 是质数，$\alpha$ 是正整数。

在(5)式内，若 $p\mid a$，$a=p^\beta u$，$(u, p)=1$，则得

$$x^2\equiv p^\beta u \pmod{p^\alpha}. \qquad (6)$$

若 $\beta\geqslant\alpha$，则

$$x^2\equiv 0 \pmod{p^\alpha}$$

当然恒有解。若 $\beta<\alpha$，$\beta$ 是偶数，$\beta=2k$，则可令 $x=p^k y$。

所以(6)式变成

$$p^{\beta}y^2\equiv p^{\gamma}u \pmod{p^{\alpha}},$$

就是

$$y^2\equiv u \pmod{p^{\alpha-\beta}}, \tag{7}$$

这里是$(u, p)=1$。若$\beta<\alpha$，$\beta$是奇数，$\beta=2l+1$，则可令$x=p^{l+1}y$。所以(6)式变成

$$p^{\beta+1}y^2\equiv p^{\gamma}u \pmod{p^{\alpha}},$$

即

$$py^2\equiv u \pmod{p^{\alpha-\beta}}.$$

这个同余式很明显没有解，因为无论$y$是什么数，$py^2$和模恒有一公约数$p$，而$u$和$p$是互质的。

因此我们得到下面的

**定理2**．在(6)式内，若$\beta\geqslant\alpha$，则它恒有解；若$\beta<\alpha$，$\beta$是奇数，则它没有解；若$\beta<\alpha$，$\beta$是偶数，则它变成形状为(7)的同余式了。

(7)和(5)的形式相同；若$(a, p)=1$，则内容也相同。因此我们将在(5)式内设$(a, p)=1$，也就是在(4)式内设$(a, m)=1$。以下我们将只讨论这种形式的同余式。

**定义1**．若$(a, m)=1$，

$$x^2\equiv a \pmod{m} \tag{8}$$

有解，则$a$叫作模$m$的平方剩余，否则叫作模$m$的平方非剩余。

比方每一个平方数都是任意模的平方剩余。

在不至于发生误解的情况下，平方剩余和平方非剩余也有时可以简称为剩余和非剩余。

摆在我们面前现在有两个问题：

Ⅰ．在$m$给定后，哪些数是$m$的平方剩余？对于每一个平方剩余$a$，相应的同余式(8)有多少解？

## Ⅰ．在 $a$ 给定后，有哪些数作模以 $a$ 为平方剩余？

### §2．质数模的平方剩余

质数模2的平方剩余很明显是1．以下我们设质数 $p>2$．

**定理3．** 若 $a$ 是模 $p$ 的平方剩余，则

$$x^2\equiv a \pmod p \qquad (1)$$

有两个解．

证明．$a$ 既是平方剩余，所以必有一数 $x_1$ 可使

$$x_1^2\equiv a \pmod p.$$

又因 $(-x_1)^2\equiv x_1^2\equiv a \pmod p$，

所以 $-x_1$ 也能满足(1)式．

$x_1$ 和 $-x_1$ 对于模 $p$ 不是同余的．假设

$$x_1\equiv -x_1 \pmod p,$$

则得 $2x_1\equiv 0 \pmod p$．

因为 $(2,\ p)=(x_1,\ p)=1$，

所以这是不可能的．所以

$$x_1\not\equiv -x_1 \pmod p.$$

故(1)式有

$$x\equiv x_1 \pmod p$$

和

$$x\equiv -x_1 \pmod p$$

这两个解．

又因(1)式是以质数 $p$ 为模的二次同余式，所以它的根数不能多于2．故(1)式恰有两个根．

**定理 4**. 模 $p$ 的平方剩余和非剩余各有 $\frac{p-1}{2}$ 个.

证明. 若

$$x^2 \equiv a \pmod{p} \tag{1}$$

有根，则它的根逃不出下列 $p-1$ 个数：

$$\pm 1, \pm 2, \cdots, \pm \frac{p-1}{2}.$$

这些数的平方就是下列 $\frac{p-1}{2}$ 个数：

$$1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2.$$

在这些数当中没有两个是同余的. 假设

$$1 \leqslant l < k \leqslant \frac{p-1}{2},$$

而

$$k^2 \equiv l^2 \pmod{p},$$

则得

$$k^2 - l^2 = (k+l)(k-l) \equiv 0 \pmod{p}. \tag{2}$$

因为 $1 < k+l < p-1$,

$$1 \leqslant k-l < \frac{p-1}{2},$$

所以(2)式是不可能的. 所以

$$k^2 \not\equiv l^2 \pmod{p}.$$

所以模 $p$ 有 $\frac{p-1}{2}$ 个平方剩余. 其余的 $\frac{p-1}{2}$ 类剩余当然是平方非剩余.

**定理 5** (Euler 的判别标准). 若 $a$ 是模 $p$ 的平方剩余，则

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

若 $b$ 是模 $p$ 的平方非剩余，则

$$b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

证明．$a$ 既是平方剩余，所以必有一数 $r$，可使

$$r^2 \equiv a \pmod{p}.$$

所以 $$a^{\frac{p-1}{2}} \equiv r^{p-1} \equiv 1 \pmod{p}.$$

因为 $$x^{p-1} \equiv 1 \pmod{p}$$

有 $p-1$ 个根，就是 $p$ 的简化剩余系，故由

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p},$$

得

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p} \qquad (1)$$

和

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \qquad (2)$$

它们各有 $\frac{p-1}{2}$ 个根．因为平方剩余都能满足(1)式，而一个数又不能同时满足(1)式和(2)式，这样会产生

$$2 \equiv 0 \pmod{p},$$

这是不可能的，所以平方非剩余都能满足(2)式．所以

$$b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

**定理 6**．对于同一质数 $p$ 来说：

剩余×剩余＝剩余，

剩余×非剩余＝非剩余，

非剩余×非剩余＝剩余。

证明．设$a_1$和$a_2$都是平方剩余．故必有二数$r_1$和$r_2$，可使

$$r_1^2 \equiv a_1 \pmod{p},$$

$$r_2^2 \equiv a_2 \pmod{p}.$$

所以　　$(r_1 r_2)^2 \equiv a_1 a_2 \pmod{p}$．

这就是说，$a_1 a_2$是一个平方剩余，因为$r_1 r_2$可以满足

$$x^2 \equiv a_1 a_2 \pmod{p}.$$

模$p$的简化剩余系是

$$1, 2, \cdots, p-1.$$

若$a$是平方剩余，则因$(a, p)=1$，故$p-1$个数

$$a, 2a, \cdots, (p-1)a$$

也是模$p$的简化剩余系．因为在这里边是$a$乘剩余等于剩余，而剩余和非剩余又各占半数，故$a$乘非剩余等于非剩余。

若$b$是平方非剩余，则因$(b, p)=1$，故

$$b, 2b, \cdots, (p-1)b$$

也是模$p$的简化剩余系．因为在这里边有半数是$b$这个非剩余乘剩余等于非剩余，所以另外那半数是$b$这个非剩余乘非剩余等于剩余。

## § 3．Legendre 符号

**定义 2**．Legendre 符号$\left(\frac{a}{p}\right)$的定义如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{若 } a \text{ 是 } p \text{ 的平方剩余},\\ -1, & \text{若 } a \text{ 是 } p \text{ 的平方非剩余}.\end{cases}$$

$\left(\frac{a}{p}\right)$可以读作 $a$ 对于 $p$ 的 Legendre 符号，$a$ 和 $p$ 分别叫作 Legendre符号的分子和分母.

故若$(n, p)=1$，恒是$\left(\frac{n^2}{p}\right)=1$，特别是$\left(\frac{1}{p}\right)=1$.

若能很快地得出，$\left(\frac{a}{p}\right)$是等于 1 或 $-1$，则就很快地决定了

$$x^2\equiv a \pmod p$$

有解或没有解.

由定义 2 和定理 5 可得

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p.$$

**定理 7.** 若

$$a_1\equiv a_2 \pmod p,$$

则

$$\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right).$$

证明. 因为

$$\left(\frac{a_1}{p}\right)\equiv a_1^{\frac{p-1}{2}}\equiv a_2^{\frac{p-1}{2}}\equiv\left(\frac{a_2}{p}\right) \pmod p,$$

故 $$\left(\frac{a_1}{p}\right)-\left(\frac{a_2}{p}\right)\equiv 0 \pmod p.$$

因为 $$\left|\left(\frac{a_1}{p}\right)-\left(\frac{a_2}{p}\right)\right|\leqslant 2,$$

而 $p>2$，故只能是

$$\left(\frac{a_1}{p}\right)=\left(\frac{a_2}{p}\right).$$

**定理 8**．若

$$A=a_1a_2\cdots a_n,$$

则
$$\left(\frac{A}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right).$$

证明．

$$\left(\frac{A}{p}\right)\equiv A^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}\cdots a_n^{\frac{p-1}{2}}$$

$$\equiv\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)\pmod p.$$

由此定理可知，若 $a=b^2c$，则

$$\left(\frac{a}{p}\right)=\left(\frac{b^2c}{p}\right)=\left(\frac{b^2}{p}\right)\left(\frac{c}{p}\right)=\left(\frac{c}{p}\right).$$

故在 Legendre 符号的分子内，若有平方数作因数，则可把它约掉．

**定理 9**．

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

换个说法是：若 $p=4n+1$，则 $-1$ 是平方剩余；若 $p=4n+3$，则 $-1$ 是平方非剩余．

证明．因为

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\pmod p,$$

所以同余号前后必须同时是1或同时是$-1$，否则就会得$p\mid 2$，这是不可能的，因为$p>2$。故若

$$p=4n+1,\ 则\left(\frac{-1}{p}\right)=1,$$

$$p=4n+3,\ 则\left(\frac{-1}{p}\right)=-1.$$

## §4. 互倒定律

**定理10(Gauss引理)**。若$p>2$，$(q,\ p)=1$，则

$$q,\ 2q,\ \cdots,\ \frac{p-1}{2}q$$

代表$\frac{p-1}{2}$类不同的剩余。若把这些数用和它们同余的最小正整数来代替，则必得

$$0<r_1<r_2<\cdots<r_{\frac{p-1}{2}}<p.$$

若在这里边有$\mu$个大于$\frac{p}{2}$，则

$$\left(\frac{q}{p}\right)=(-1)^{\mu}.$$

证明。设$n=\frac{p-1}{2}-\mu$。故

$$r_{n+1},\ r_{n+2},\ \cdots,\ r_{n+\mu}$$

都大于$\frac{p}{2}$。故

$$p-r_{n+1},\ p-r_{n+2},\ \cdots,\ p-r_{n+\mu}$$

都小于$\frac{p}{2}$。现在我们要证明在下列$\frac{p-1}{2}$个数内：

$$r_1,\ r_2,\ \cdots,\ r_n,\ p-r_{n+1},\ \cdots p-r_{n+\mu}$$

没有两个是同余的。这当然只证明 $r_k$ 和 $p-r_\lambda$ 不同余就行了。假设

$$r_k\equiv p-r_\lambda \pmod p,$$

则得 $$r_k+r_\lambda\equiv 0 \pmod p.$$

因为 $$r_k=sq,\ r_\lambda=tq,$$

所以 $$(s+t)q\equiv 0 \pmod p.$$

所以 $$s+t\equiv 0 \pmod p.$$

因为 $s$ 和 $t$ 都大于零小于 $\frac{p}{2}$，所以这个同余式是不可能的。

所以

$$r_k\not\equiv p-r_\lambda \pmod p.$$

所以 $$1\cdot 2\cdots\frac{p-1}{2}\,q^{\frac{p-1}{2}}\equiv r_1r_2\cdots r_{n+\mu} \pmod p.$$

而 $$1\cdot 2\cdots\frac{p-1}{2}=r_1r_2\cdots r_n(p-r_{n+1})\cdots(p-r_{n+\mu})$$

$$\equiv r_1r_2\cdots r_{n+\mu}(-1)^\mu \pmod p.$$

所以 $$r_1r_2\cdots r_{n+\mu}(-1)^\mu q^{\frac{p-1}{2}}\equiv r_1r_2\cdots r_{n+\mu} \pmod p,$$

$$(-1)^\mu q^{\frac{p-1}{2}}\equiv 1 \pmod p,$$

$$q^{\frac{p-1}{2}}\equiv(-1)^\mu \pmod p,$$

$$\left(\frac{q}{p}\right)\equiv(-1)^\mu \pmod p.$$

因为 $p>2$，所以

$$\left(\frac{q}{p}\right)=(-1)^\mu.$$

**定理11.**

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

换一个说法：若 $p=8n\pm1$，则2是平方剩余；若 $p=8n\pm3$，则2是平方非剩余.

证明. 用2乘1，2，…，$\frac{p-1}{2}$得

$$2,\ 4,\ 6,\ \cdots,\ p-1.$$

这些数的形状是$2r$. 若$2r>\frac{p}{2}$，则 $r>\frac{p}{4}$. 所以在这里边大于$\frac{p}{2}$的数有

$$\frac{p-1}{2}-\left[\frac{p}{4}\right]\text{个}.$$

令 $$\mu=\frac{p-1}{2}-\left[\frac{p}{4}\right].$$

若 $p=8n+1$，则 $\mu=4n-2n=2n$.

若 $p=8n+3$，则 $\mu=4n+1-2n=2n+1$.

若 $p=8n+5$，则 $\mu=4n+2-(2n+1)=2n+1$.

若 $p=8n+7$，则 $\mu=4n+3-(2n+1)=2n+2$.

所以若 $p=8n\pm1$，则 $\mu$ 是偶数，2是平方剩余；若 $p=8n\pm3$，则 $\mu$ 是奇数，2是平方非剩余. 又因

$$\text{若}p=8n\pm1,\ \text{则}\frac{p^2-1}{8}=8n^2\pm2n\equiv0\pmod 2,$$

$$\text{若}p=8n\pm3,\ \text{则}\frac{p^2-1}{8}=8n^2\pm6n+1\equiv1\pmod 2,$$

故得 $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

**定理12**（互倒定律）．若 $p$，$q$ 是两个不同的奇质数，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \qquad (1)$$

Euler 在1783年最先提出这个定理，Gauss在1796年最先把它严格地证明了．这个定理说明了，在 $p$，$q$ 这两个质数当中，只要有一个的形式是 $4n+1$，那么就得

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right).$$

若 $p$，$q$ 的形式都是 $4n+3$，则

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right).$$

证明．以下我们令

$$p'=\frac{p-1}{2},\quad q'=\frac{q-1}{2}.$$

若以 $p$ 为模，则

$$q,\ 2q,\ \cdots,\ p'q$$

代表 $p'$ 类不同的剩余．设

$$\left.\begin{aligned} q&=\left[\frac{q}{p}\right]p+r_1,\\ 2q&=\left[\frac{2q}{p}\right]p+r_2,\\ &\cdots\cdots\cdots\cdots\\ p'q&=\left[\frac{p'q}{p}\right]p+r_{p'}, \end{aligned}\right\} \qquad (2)$$

这里是　$0<r_x<p$，$x=1,\ 2,\ \cdots,\ p'$．

设在下列数

$$r_1,\ r_2,\ \cdots,\ r_{p'}$$