二次同余式与平方剩余

定义

二次同余式

4.1 一般二次同余式

二次同余式的一般形式是

$$ax^2+bx+c\equiv 0 \pmod m, \tag{4.1}$$

其中 $a\not\equiv 0 \pmod m$.

因为正整数 m 有素因数分解式 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, 所以二次同余式 (4.1) 等价于同余式组

$$\begin{cases} ax^2+bx+c\equiv 0 & (\bmod\ p_1^{\alpha_1}),\\ \quad\vdots \\ ax^2+bx+c\equiv 0 & (\bmod\ p_k^{\alpha_k}).\end{cases}$$

因此, 只需讨论模为素数幂 p^α 的同余式

$$ax^2+bx+c\equiv 0 \pmod{p^\alpha}, \qquad p\nmid a. \tag{4.2}$$

将同余式 (4.2) 的两端同乘以 $4a$, 得到

$$4a^2x^2+4abx+4ac\equiv 0 \pmod{p^\alpha}$$

或

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

令 $y=2ax+b$, 有

$$y^2\equiv b^2-4ac \pmod{p^\alpha}.$$

特别地, 当 p 是奇素数时, $(2a,p)=1$. 上述同余式等价于同余式 (4.2).

平方剩余

定义 4.1.1 设 m 是正整数. 若同余式

$$x^2\equiv a \pmod m, \qquad (a,m)=1 \tag{4.3}$$

有解，则 a 叫做模 m 的**平方剩余(或二次剩余)**；否则，a 叫做模 m 的**平方非剩余(或二次非剩余)**.

模p为奇素数的判别法

欧拉判别法

定理 4.2.1 (欧拉判别条件) 设 p 是奇素数，$(a,p)=1$，则

(i) a 是模 p 的平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}}\equiv 1 \pmod p; \tag{4.5}$$

(ii) a 是模 p 的平方非剩余的充分必要条件是

$$a^{\frac{p-1}{2}}\equiv -1 \pmod p. \tag{4.6}$$

并且当 a 是模 p 的平方剩余时, 同余式 (4.4) 恰有二解.

推论

推论 设 p 是奇素数, $(a_1,p)=1$, $(a_2,p)=1$, 则

(i) 如果 a_1, a_2 都是模 p 的平方剩余, 则 $a_1\cdot a_2$ 是模 p 的平方剩余.

(ii) 如果 a_1, a_2 都是模 p 的平方非剩余, 则 $a_1\cdot a_2$ 是模 p 的平方剩余.

(iii) 如果 a_1 是模 p 的平方剩余, a_2 是模 p 的平方非剩余, 则 $a_1\cdot a_2$ 是模 p 的平方非剩余.

二次平方剩余系

定理 4.2.2 设 p 是奇素数，则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为 $\frac{p-1}{2}$, 且 $\frac{p-1}{2}$ 个平方剩余与序列

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2 \tag{4.7}$$

中的一个数同余, 且仅与一个数同余.

勒让得符号

定理

4.3.1 勒让得符号之运算性质

定理 4.2.1 给出了整数 a 是否是模奇素数 p 二次剩余的判别法则, 但需要作较复杂的运算, 需要一种更简单的判别法则和计算方法.

定义 4.3.1 设 p 是素数. 定义**勒让得 (Legendre) 符号** 如下:

$$\left(\frac{a}{p}\right)=\begin{cases}1, & 若\ a\ 是模\ p\ 的平方剩余;\\ -1, & 若\ a\ 是模\ p\ 的平方非剩余;\\ 0, & 若\ p\mid a.\end{cases} \tag{4.8}$$

由此, 对于 $(a,p)=1$, 有

$$\begin{aligned}\left(\frac{a}{p}\right)=1 &\iff x^2\equiv a \pmod p\ 有解\\ \left(\frac{a}{p}\right)=-1 &\iff x^2\equiv a \pmod p\ 无解\end{aligned} \tag{4.9}$$

定理 4.3.2 设 p 是奇素数，则

(1) $\left(\frac{1}{p}\right)=1$;

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

性质

定理 4.3.3 设 p 是奇素数，则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$;

(ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) 设 $(a,p)=1$, 则 $\left(\frac{a^2}{p}\right)=1$.

子主题 3

相关定理

定理 4.2.2 设 p 是奇素数，则模 p 的简化剩余系中平方剩余与平方非剩余的个数各为 $\frac{p-1}{2}$, 且 $\frac{p-1}{2}$ 个平方剩余与序列

$$1^2,\ 2^2,\ \cdots,\ \left(\frac{p-1}{2}\right)^2 \tag{4.7}$$

中的一个数同余, 且仅与一个数同余.

高斯引理

引理 4.3.1 (Gauss) 设 p 是奇素数. a 是整数, $(a,p)=1$. 如果整数

$$a\cdot 1,\ a\cdot 2,\ \cdots,\ a\cdot\frac{p-1}{2}$$

中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数是 m, 则

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

推论

定理 4.3.4 设 p 是奇素数,

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

(ii) 若 $(a,2p)=1$, 则 $\left(\frac{a}{p}\right)=(-1)^{T(a,p)}$, 其中 $T(a,p)=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{a\cdot k}{p}\right]$.

求解定理

推论 设 p 是奇素数, 那么

$$\left(\frac{2}{p}\right)=\begin{cases}1, & 若\ p\equiv\pm 1 \pmod 8;\\ -1, & 若\ p\equiv\pm 3 \pmod 8.\end{cases}$$

二次互反律

定理 4.4.1 (二次互反律) 若 p, q 是互素奇素数，则

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

辅助

以二次互反律配合以下两个辅助定理

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

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

即能迅速地计算勒让德符号，从而解决二次剩余的判别问题。

例如判别37是否是模89的二次剩余：

$$\left(\frac{37}{89}\right)\left(\frac{89}{37}\right)=(-1)^{\frac{(37-1)(89-1)}{4}}=1$$

所以 $\left(\frac{37}{89}\right)=\left(\frac{89}{37}\right)=\left(\frac{89-37-37}{37}\right)=\left(\frac{15}{37}\right)=\left(\frac{3}{37}\right)\left(\frac{5}{37}\right)=\left(\frac{37}{3}\right)\left(\frac{37}{5}\right)=\left(\frac{1}{3}\right)\left(\frac{2}{5}\right)=-1$

因此37不是模89的二次剩余。

雅可比符号

弱化条件

在勒让得符号的计算中，要求模p为素数此外，在二次互反律的应用中，也要求α = q为素数．这些都是很强的条件，因此，希望这些条件可以弱化，只要求模m为奇整数，α为任意整数．

定义

定义 4.5.1 设 $m=p_1\cdots p_r$ 是奇素数 p_i 的乘积. 对任意整数 a, 定义**雅可比 (Jacobi) 符号** 为

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right). \tag{4.23}$$

雅可比符号形式上是勒让得符号的推广, 但所蕴涵的意义已经不同. 与式 (4.10) 作比较, 对于 $(a,m)=1$, 有

$$\begin{aligned}\left(\frac{a}{m}\right)=1 &\Longleftarrow x^2\equiv a \pmod m\ 有解\\ \left(\frac{a}{m}\right)=-1 &\Longrightarrow x^2\equiv a \pmod p\ 无解\end{aligned} \tag{4.24}$$

雅可比符号为 -1, 可判断 a 是模 m 平方非剩余; 但雅可比符号为 1, 却不能判断 a 是模 m 平方剩余. 例如, 3 是模 119 平方非剩余, 但

$$\left(\frac{3}{119}\right)=\left(\frac{3}{7}\right)\left(\frac{3}{17}\right)=(-1)(-1)=1.$$

定理

定理 4.5.1 设 m 是正奇数，则

(i) $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$;

(ii) $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$;

(iii) 设 $(a,m)=1$, 则 $\left(\frac{a^2}{m}\right)=1$.

引理

引理 4.5.1 设 $m=p_1\cdots p_r$ 是奇数，则

$$\frac{m-1}{2}\equiv\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2} \pmod 2;$$

$$\frac{m^2-1}{8}\equiv\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8} \pmod 2.$$

推论

定理 4.5.2 设 m 是奇数，则

(i) $\left(\frac{1}{m}\right)=1$;

(ii) $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$;

(iii) $\left(\frac{2}{m}\right)\equiv(-1)^{\frac{m^2-1}{8}}$;

二次互反

定理 4.5.3 设 m,n 都是奇数，则

$$\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{m}{n}\right).$$

模平方根

具体求解

模 p 平方根

设p是形为4k +3的素数．讨论此情形的模p平方根

定理 4.6.1 设 p 是形为 $4k+3$ 的素数. 如果同余式

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

有解, 则其解是

$$x\equiv\pm a^{\frac{p+1}{4}} \pmod p.$$

证明

解 因为 p 是形为 $4k+3$ 的素数, 所以存在奇数 q 使得 $p-1=2q$. 现在同余式

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

有解, 则有

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

或者

$$a^q\equiv 1 \pmod p.$$

两端同时乘以 a, 得到

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

因此, 同余式的解为式 (4.25).

模p平方根

p为奇素数

定理 4.6.3 设 p 是奇素数，$p-1=2^t\cdot s$，$t\geqslant 1$，其中 s 是奇整数. 设 n 是模 p 平方非剩余，$b:=n^s \pmod p$，如果同余式

$$x^2\equiv a \pmod p \tag{4.28}$$

有解，则 $a^{-1}x_{t-k-1}^2$ 满足同余式

$$y^{2^{t-k-1}}\equiv 1 \pmod p, \qquad k=0,1,\cdots,t-1, \tag{4.29}$$

解定理

150 第 4 章 二次同余式与平方剩余

这里，$x_{t-1}:=a^{\frac{s+1}{2}} \pmod p$，

$$x_{t-k-1}=x_{t-k}b^{j_{k-1}2^{k-1}},\quad 其中\ j_{k-1}=\begin{cases}0, & 如果\ (a^{-1}x_{t-k}^2)^{2^{t-k-1}}\equiv 1 \pmod p;\\ 1, & 如果\ (a^{-1}x_{t-k}^2)^{2^{t-k-1}}\equiv -1 \pmod p.\end{cases} \tag{4.30}$$

特别，x_0 是同余式 (4.28) 的解.

模m平方根

条件

本节讨论模 m 为合数的二次同余式

$$x^2\equiv a \pmod m,\quad (a,m)=1.$$

有解的条件及解的个数.

当 $m=2^\delta p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 时, 同余式等价于同余式组

$$\begin{cases}x^2\equiv a & (\bmod\ 2^\delta),\\ x^2\equiv a & (\bmod\ p_1^{\alpha_1}),\\ \quad\vdots\\ x^2\equiv a & (\bmod\ p_k^{\alpha_k}).\end{cases}$$

解定理

p^a

因此, 先讨论模为奇素数幂 p^α 的二次同余式

$$x^2\equiv a \pmod{p^\alpha},\qquad (a,p)=1,\ \alpha>0 \tag{4.33}$$

有解的条件及解的个数.

定理 4.6.4 设 p 是奇素数. 则同余式 (4.33) 有解的充分必要条件是 a 为模 p 平方剩余, 且有解时, 式 (4.33) 的解数是 2.

推论

推论 设 p 是奇素数, 则对于任意的整数 a, 同余式 (4.33) 的解数是

$$T=1+\left(\frac{a}{p}\right).$$

a的分情况

定理 4.6.5 设 $\alpha>1$, 则同余式 (4.34) 有解的必要条件是

(i) 当 $\alpha=2$ 时, $a\equiv 1 \pmod 4$;

(ii) 当 $\alpha\geqslant 3$ 时, $a\equiv 1 \pmod 8$.

若上述条件成立, 则式 (4.34) 有解. 进一步, 当 $\alpha=2$ 时, 解数是 2; 当 $\alpha\geqslant 3$ 时, 解数是 4.

x^2+y^2 = p

定理

定理 4.7.1 设 p 是素数, 那么

$$x^2+y^2=p$$

有解的充分必要条件就是 $p=2$ 或 -1 为模 p 平方剩余, 即 $p=2$ 或 $p=4k+1$.