第3章 二次剩余

二次剩余理论

二次剩余的判断

模 p^l 的一元二次同余方程的解的结构

3.1 Legendre符号（1）：Euler判别法

定义 3.1.1 设a为整数，p为素数，并且$p \nmid a$，如果同余$x^2 \equiv a \pmod p$有解，则称a是模p的二次剩余；否则称a是模p的二次非剩余。

定理 3.1.1 设 p 为奇素数，在模 p 的一个缩系中，恰有 $\frac{p-1}{2}$ 个模 p 的二次剩余，$\frac{p-1}{2}$ 个模 p 的二次非剩余；在模 p 的意义下，$1^2, 2^2, \cdots, (\frac{p-1}{2})^2$ 即为全部模 p 的二次剩余。

证明：注意到模 p 的二次剩余只可能为

$$1^2, 2^2, \cdots, (p-2)^2, (p-1)^2。$$

例 **2** 求模 **11** 的二次剩余及二次非剩余。

解：由上定理证明知，

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ \left(\frac{11-1}{2}\right)^2$$

为模 **11** 的二次剩余，即 **1**，**4**，**9**，**5**，**3**；

而 **2**，**6**，**7**，**8**，**10** 为模 **11** 的二次非剩余。

定义 3.1.2 设 p 为奇素数，对每个整数 a，定义 **Legendre** 符号如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{如果} p\nmid a\text{，且} a \text{是模} p \text{的二次剩余}\\ -1 & \text{如果} p\nmid a\text{，且} a \text{是模} p \text{的二次非剩余}\\ 0 & \text{如果} p\mid a\end{cases}$$

二次同余方程 $x^2\equiv a(\bmod p)$ 有无解的问题，可以归结为如何计算 **Legendre** 符号 $\left(\frac{a}{p}\right)$ 的值

定理 3.1.2(Euler 判别法) 设 p 为奇素数，则

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

证明：利用 Fermat 小定理将定理证明转换成证明

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

和

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

例 3 判断 3 是不是模 29 的二次剩余。

解：

$$\left(\frac{3}{29}\right) \equiv 3^{\frac{29-1}{2}} \pmod{29}$$

定理 3.1.3 若奇素数 $p \nmid ab$，则 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$。

证明：利用 **Euler** 判别法。

定理 3.1.4 对于奇素数 p 而言，模 p 的两个二次剩余之积为二次剩余，两个二次非剩余之积为二次剩余，而一个二次剩余与一个二次非剩余之积为二次非剩余。

例 4 模 5 的二次剩余为 1，4，二次非剩余为 2，3。

两个二次剩余之积

$4\times1\equiv4(\bmod 5)$，$1\times1\equiv1(\bmod 5)$，$4\times4\equiv1(\bmod 5)$

均为二次剩余；

两个二次非剩余之积

$2\times3\equiv1(\bmod 5)$，$2\times2\equiv4(\bmod 5)$，$3\times3\equiv4(\bmod 5)$

均为二次剩余；

一个二次剩余与一个二次非剩余之积

$2\times1\equiv2(\bmod 5)$，$2\times4\equiv3(\bmod 5)$，

$3\times1\equiv3(\bmod 5)$，$3\times4\equiv2(\bmod 5)$

均为二次非剩余。

3.2 Legendre符号（2）：二次互反律

若$a=\pm 2^m q_1^{l_1}\cdots q_s^{l_s}$，则

$$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^m\left(\frac{q_1}{p}\right)^{l_1}\cdots\left(\frac{q_s}{p}\right)^{l_s},$$

即我们只要能计算出

$$\left(\frac{\pm 1}{p}\right),\left(\frac{2}{p}\right),\left(\frac{q}{p}\right),$$ q为奇素数，

就可以计算任意的$\left(\frac{a}{p}\right)$。

定理 3.2.1 (1) $\left(\frac{a}{p}\right)=\left(\frac{a+p}{p}\right)$;

(2) 当 $p\nmid a$ 时，$\left(\frac{a^2}{p}\right)=1$;

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

(4) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 & 当p\equiv 1(\bmod 4)\\ -1 & 当p\equiv 3(\bmod 4)\end{cases}$。

定理 3.2.2(Gauss 引理) 设 p 为奇素数，$p \nmid a$，若 $\frac{1}{2}(p-1)$ 个数

$a, 2a, \cdots, \frac{1}{2}(p-1)a$ 模 p 的最小正余数中有 m 个大于 $\frac{p}{2}$，

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

例 1 $p=5$，$a=8$，

定理 3.2.3 设 p 为奇素数，则

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & 当 p \equiv \pm 1 \pmod 8 \\ -1 & 当 p \equiv \pm 3 \pmod 8 \end{cases}。$$

证明：直接利用 **Gauss** 引理，注意此时 $a = 2$，则

$$2,\ 2\times 2,\ 3\times 2,\ \cdots,\ \frac{p-1}{2}\times 2$$

都在 **0** 与 p 之间。

定理 **3.2.4**（二次互反律）设 p,q 为不同的奇素数，则

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

证明：获取 **Gauss** 引理中 m 的奇偶性信息，将定理归结成下式的证明：

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]+\sum_{l=1}^{\frac{q-1}{2}}[\frac{lp}{q}]=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

二次剩余的概念	欧拉	**1754**	
二次互反律	欧拉	**1783**	
严格证明	高斯	**1796**	**7**
		1963	**152**

我们将利用二次互反律来有效地计算 **Legendre** 符号。通常我们会利用它如下的变形：

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

例 **2** 计算$\left(\frac{15}{227}\right)$。

解：**227** 为一个素数，$15=3\times5$，从而利用 **Legendre** 符号的性质可得

$$\left(\frac{15}{227}\right)=\left(\frac{3}{227}\right)\left(\frac{5}{227}\right),$$

又$3,5,227$为互不相同的奇素数，利用二次互反律可得

$$\left(\frac{3}{227}\right)=(-1)^{\frac{3-1}{2}\times\frac{227-1}{2}}\left(\frac{227}{3}\right)=-\left(\frac{227}{3}\right)=-\left(\frac{-1}{3}\right)=-(-1)^{\frac{3-1}{2}}=1,$$

$$\left(\frac{5}{227}\right)=(-1)^{\frac{5-1}{2}\times\frac{227-1}{2}}\left(\frac{227}{5}\right)=\left(\frac{227}{5}\right)=\left(\frac{2}{3}\right)=(-1)^{\frac{5^2-1}{8}}=-1,$$

所以

$$\left(\frac{15}{227}\right)=\left(\frac{3}{227}\right)\left(\frac{5}{227}\right)=-1。$$

例 **3** 求所有以 **3** 为其二次剩余的奇素数。

解：求所有以 **3** 为其二次剩余的奇素数，即求使

$$\left(\frac{3}{p}\right)=1$$

成立的所有奇素数 p。

由二次互反律可得

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}=\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}},$$

由于

$$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1 & 当 p\equiv 1 \pmod 3\\ \left(\frac{-1}{3}\right)=-1 & 当 p\equiv -1 \pmod 3\end{cases},$$

$$(-1)^{\frac{p-1}{2}}=\begin{cases}1 & 当 p\equiv 1 \pmod 4\\ -1 & 当 p\equiv 3 \pmod 4\end{cases},$$

$$\left(\frac{3}{p}\right)=1 \Leftrightarrow \begin{cases}p\equiv 1 \pmod 3\\ p\equiv 1 \pmod 4\end{cases} 或 \begin{cases}p\equiv -1 \pmod 3\\ p\equiv 3 \pmod 4\end{cases}$$

利用孙子定理即可得 $p\equiv \pm 1 \pmod{12}$，即模 **12** 同余于± 1的所以奇素数是所有以 **3** 为其二次剩余的奇素数。

3.3 Jacobi符号

定义 **3.3.1** 设m为大于 **1** 的奇数，$m=\prod_{i=1}^{s} p_i$，其中p_i为素数且可以重复出现，$a \in Z$，定义 **Jacobi** 符号

$$\left(\frac{a}{m}\right)=\prod_{i=1}^{s}\left(\frac{a}{p_i}\right),$$

其中$\left(\frac{a}{p_i}\right)$为 **Legendre** 符号。

定理 3.3.1 (1) 当$(a,m)>1$时，$\left(\frac{a}{m}\right)=0$；当$(a,m)=1$时，$\left(\frac{a}{m}\right)$取值$\pm 1$;

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

(3) 若m'也是一个大于 **1** 的奇数，则$\left(\frac{a}{mm'}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$;

(4) 当$(a,m)=1$时，$\left(\frac{a^2}{m}\right)=1$，$\left(\frac{a}{m^2}\right)=1$;

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

(6) $\left(\frac{1}{m}\right)=1$。

定理 **3.3.2** 设m为大于 **1** 的奇数，则

$$\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}=\begin{cases}1 & m\equiv 1\pmod 4\\ -1 & m\equiv 3\pmod 4\end{cases}。$$

证明：设$m=p_1p_2\cdots p_s$， p_i是奇素数。由定义 **3.3.1** 及定理 **3.2.1** 可得

$$\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_s}\right)=(-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_s-1}{2}},$$

故只需证明 $\sum_{i=1}^{s}\frac{p_i-1}{2}\equiv\frac{m-1}{2}=\frac{1}{2}\left(\prod_{i=1}^{s}p_i-1\right)\pmod 2$。

因为 $(p_1-1)(p_2-1)\equiv 0\pmod 4$，

所以 $p_1p_2-1\equiv p_1-1+p_2-1\pmod 4$，

$$\frac{p_1p_2-1}{2}\equiv\frac{p_1-1}{2}+\frac{p_2-1}{2}\pmod 2。$$

以此为基础利用数学归纳法即可完成证明。

定理 **3.3.3** 设m为大于 **1** 的奇数，则

$$\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}=\begin{cases}1 & m\equiv\pm1(\bmod 8)\\ -1 & m\equiv\pm3(\bmod 8)\end{cases}。$$

证明：由 **Jacobi** 符号的定义及 **Legendre** 符号的性质可得

$$\left(\frac{2}{m}\right)=\prod_{i=1}^{s}\left(\frac{2}{p_i}\right)=\prod_{i=1}^{s}(-1)^{\frac{p_i^2-1}{8}}=(-1)^{\sum_{i=1}^{s}\frac{p_i^2-1}{8}},$$

$$\sum_{i=1}^{s}\frac{p_i^2-1}{8}\equiv\frac{1}{8}\left(\prod_{i=1}^{s}p_i^2-1\right)(\bmod 8),$$

从而定理得证。

定理 3.3.4 设m,n为两个大于 **1** 的奇数，且$(m,n)=1$，则

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

证明：令$m=\prod_{i=1}^{s}p_i$，$n=\prod_{j=1}^{t}q_j$，则由 **Jacobi** 符号和 **Legendre** 符号的定义、性质以及定理 **3.3.2** 中归纳证明的结论即可。

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

m与n互素

$$\left(\frac{\pm 1}{m_1}\right) \quad \left(\frac{2}{m_2}\right)$$

例 **1** 求$\left(\frac{339}{1979}\right)$

解：容易验证 **1979** 是一个素数，所以$\left(\frac{339}{1979}\right)$也是一个 **Legendre** 符号。

下面我们先利用 **Legendre** 符号的二次互反律来求解它的值。

由于 **339** 可分解为3×113，所以

$$\left(\frac{339}{1979}\right)=\left(\frac{3}{1979}\right)\left(\frac{113}{1979}\right),$$

下面我们分别来计算$\left(\frac{3}{1979}\right)$和$\left(\frac{113}{1979}\right)$。

$$\left(\frac{3}{1979}\right)=(-1)^{\frac{3-1}{2}\times\frac{1979-1}{2}}\left(\frac{1979}{3}\right)=-\left(\frac{2}{3}\right)=-(-1)^{\frac{3^2-1}{8}}=1$$

$$\left(\frac{113}{1979}\right)=(-1)^{\frac{113-1}{2}\times\frac{1979-1}{2}}\left(\frac{1979}{113}\right)=\left(\frac{58}{113}\right)$$

所以，$\left(\frac{339}{1979}\right)=\left(\frac{3}{1979}\right)\left(\frac{113}{1979}\right)=1\times(-1)=-1$。

接着我们利用 **Jacobi** 符号的二次互反律来进行计算。

易知 **339** 与 **1979** 为互素的奇数，故可直接利用 **Jacobi** 符号的二次互反律得

$$\left(\frac{339}{1979}\right)=(-1)^{\frac{339-1}{2}\times\frac{1979-1}{2}}\left(\frac{1979}{339}\right)=-\left(\frac{284}{339}\right) \qquad 1979=5\times339+284$$

Jacobi 符号与 Legendre 符号具有本质差别：

Jacobi 符号 $\left(\frac{a}{m}\right)=1$

不表示

二次同余方程 $x^2 \equiv a(\bmod m)$ 一定有解。

例 2 **Jacobi 符号** $\left(\frac{-1}{9}\right)=(-1)^{\frac{9-1}{2}}=1$，

但是易验证 $x^2 \equiv -1(\bmod 9)$ 是无解的。

对于 **Jacobi** 符号而言，前面关于 **Legendre** 符号的 **Guass** 引理、**Euler** 判别条件均是不成立的。

依据 **Euler** 判别法，我们给出一个素性检验的方法

Solovay-Strassen 素性检验，其描述如下：

设$n>2$是一个奇数，

(1) 随机均匀地选取整数$a\in\{1,2,3,\cdots,n-1\}$**;**

(2) 计算(a,n)**;**

(3) 如果$(a,n)\neq 1$，则n不是素数**;**

(4) 计算$\left(\dfrac{a}{n}\right)$和$a^{\frac{n-1}{2}}\bmod n$**;**

(5) 如果$\left(\dfrac{a}{n}\right)\equiv a^{\frac{n-1}{2}}\bmod n$，则$n$可能是素数；否则，$n$不是素数。

利用下面的定理知该算法判定n是素数的正确概率至少为 **50**%，出错的概率小于 **50**%。

定理 **3.3.5** 若$n>2$是一个奇合数，则至少有 **50**%的$a\in Z_n^*$，使得

$$\left(\frac{a}{n}\right)\equiv a^{\frac{n-1}{2}} \bmod n$$

不成立。

下面给出**Blum**数的一些有趣性质，它们在公钥密码学和密码协议中非常有用。

定理 **3.3.6** 设$n = pq$为 **Blum** 数，则

(1) $\left(\frac{-1}{n}\right)=1$**;**

(2) 若$\left(\frac{a}{n}\right)=1$，则要么$a$为模$n$的二次剩余，要么$-a$为模$n$的二次剩余。

当整数n是两个奇素数p和q的乘积时，由二次剩余的性质定理**3.1.1**知，模p的一个缩系中，模p的二次剩余和二次非剩余各占一半，对模q有同样的结论。

整数a为模n的二次剩余，当且仅当a同时是模p和模q的二次剩余。

所以，在模n的一个缩系中，有一半满足$\left(\frac{a}{n}\right)=-1$;

另一半满足$\left(\frac{a}{n}\right)=1$，而在这一半$a$中，只有一半满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1$，另一半满足$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$，它们分别对应着模$n$的二次剩余和二次非剩余。

例 3 $n=21=3\times7$ 为一个 **Blum** 数，

在模 **3** 的缩系$1,2$中，**2** 为模 **3** 的二次非剩余，**1** 为模 **3** 的二次剩余；

在模 **7** 的缩系$1,2,3,4,5,6$中，**3, 5, 6** 为模 **7** 的二次非剩余，**1, 2, 4** 为模 **7** 的二次剩余；

在模 **21** 的缩系$1,2,4,5,8,10,11,13,16,17,19,20$中，

有 **6** 个数a：**2, 8, 10, 11, 13, 19** 满足$\left(\frac{a}{21}\right)=-1$，

有 **6** 个数a：**1, 4, 5, 16, 17, 20** 满足$\left(\frac{a}{21}\right)=1$，

这 **6** 个数中有 **3** 个数a：**1, 4, 16** 满足$\left(\frac{a}{3}\right)=\left(\frac{a}{7}\right)=1$，它们就是模 **21** 的二次剩余，其余 **3** 个数a：**5, 17, 20** 满足$\left(\frac{a}{3}\right)=\left(\frac{a}{7}\right)=-1$，它们是模 **21** 的二次非剩余。

定理 **3.3.7** 设 p 为 **Blum** 素数，a 为模 p 的二次剩余，则 a 模 p 的两个平方根为 $\pm a^{\frac{p+1}{4}}$。

例 **4** $p=7$为一个 **Blum** 素数，**2** 为模 **7** 的一个二次剩余，由定理 **3.3.7** 知，**2** 模 **7** 的两个平方根为

$$2^{\frac{7+1}{4}}=4,$$

和

$$-2^{\frac{7+1}{4}}=-4\equiv 3(\bmod 7).$$

$q=47\equiv 3(\bmod 4)$也是一个 **Blum** 素数，由$\left(\frac{24}{47}\right)=1$知 **24** 是模 **47** 的一个二次剩余，利用定理 **3.3.7** 易知 **24** 模 **47** 的两个平方根为

$$24^{\frac{47+1}{4}}\equiv 27(\bmod 47),$$

$$-24^{\frac{47+1}{4}}\equiv -27\equiv 20(\bmod 47)。$$

定理 3.3.8 设$n=pq$为 **Blum** 数，a为模n的二次剩余，若u,v为a模n的两个不同的平方根，即$u\not\equiv \pm v \pmod n$，则

$$\left(\frac{u}{n}\right)=-\left(\frac{v}{n}\right)。$$

例 **5** 整数$n=1457=31\times 47$，满足$31\equiv 47\equiv 3(\bmod 4)$，即$n$是一个 **Blum** 数。由

$$\left(\frac{1575}{1457}\right)=\left(\frac{1575}{31}\right)\left(\frac{1575}{47}\right)$$

$$=\left(\frac{25}{31}\right)\left(\frac{24}{47}\right)$$

$$=1\times 1$$

$$=1$$

知 **1575** 是模 **1457** 的一个二次剩余。

下面我们来求 **1575** 模 **1457** 的平方根。即求解同余方程

$$x^2\equiv 1575(\bmod 1457)，$$

利用定理 **3.3.7** 求出 **24** 模 **47** 的平方根为± 27，**25** 模 **31** 的平方根为± 5，故上述方程组等价于

$$\begin{cases} x \equiv 5 \pmod{31} \\ x \equiv 27 \pmod{47} \end{cases}, \quad \begin{cases} x \equiv -5 \pmod{31} \\ x \equiv -27 \pmod{47} \end{cases},$$

$$\begin{cases} x \equiv -5 \pmod{31} \\ x \equiv 27 \pmod{47} \end{cases}, \quad \begin{cases} x \equiv 5 \pmod{31} \\ x \equiv -27 \pmod{47} \end{cases}$$

利用孙子定理即可求出 **1575** 模 **1457** 的平方根为

$$\pm 5 \times 47 \times 2 \pm 27 \times 31 \times 44 \pmod{1457},$$

即$\pm 67, \pm 584$。其中 **67** 和 **584** 即为 **1575** 模 **1457** 的两个不同的平方根，它们的 **Jacobi** 符号的值分别为