信息安全数学基础5—二次剩余（《数论讲义》第4章）

杨礼珍

同济大学计算机科学与技术系, 2018

Outline

作业

- 阅读：
  - 《数论讲义》第4章的1-4、6节（定理1）、7节。
  - 《密码学原理与实践》的P140-144关于勒让得(Legendre)符号和雅可比(Jacobi)符号的计算部分。
- 作业：《数论讲义》第4章习题（编号前缀s4.）1、2、3、4。
- 本章主要内容：勒让德符号和雅可比符号的计算。
- 本章内容在密码学中的应用：用于产生随机素数的素性测试算法，RSA的安全性分析。

定义

定义： 设$m > 1$，若

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

有解，则n叫做模数m的**二次剩余**；若无解，则n叫做模数m的**二次非剩余**。

例： 因为$0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv -1, 3^2 \equiv -1, 4^2 \equiv 1 \pmod{5}$，所以$1, 4$是模数5的二次剩余，2,3是模数5的非二次剩余。

定义： 设p为奇素数，$(p, n) = 1$，令

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & ，若n是模数p的二次剩余， \\ -1 & ，若n是模数p的二次非剩余. \end{cases}$$

函数$\left(\frac{n}{p}\right)$叫做**勒让德符号**。

例：

$$\left(\frac{1}{5}\right) = 1, \left(\frac{2}{5}\right) = -1, \left(\frac{3}{5}\right) = -1, \left(\frac{4}{5}\right) = 1.$$

定义： 设m是一个正奇数，$m = p_1p_2\ldots p_t, p_i(i = 1,\ldots,t)$是素数，$(n,m) = 1$，则

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{t}\left(\frac{n}{p_i}\right)$$

叫做**雅可比符号**。

雅可比符号是勒让德符号的推广，勒让得符号是雅可比符号的特殊情况。

本章主要内容是勒让得符号和雅可比符号的计算，其中《数论讲义》

- 第1节讨论模数为奇素数时的二次剩余，
- 第2－4节讨论勒让得符号的计算，给出了2个计算方法。
- 第7节讨论雅可比符号的计算。由雅可比符号的计算法则，可以通过两种方法有效计算勒让得符号。

1-2节的部分定理不采用课本的证明，而利用了$\mathbb{Z}_p^*$存在原根来证明。

勒让德符号
基本性质

性质:若$n \equiv n' \not\equiv 0 \pmod p$，则$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right)$。(由定义易得)

当p为奇素数时，我们知道$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$存在原根，设$g$是其中一个原根，那么

$$\mathbb{Z}_p^* = \langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{p-2} \pmod p\}$$

设$n \equiv g^i \pmod p$。如果

$$x^2 \equiv n \equiv g^i \pmod p \tag{2}$$

有解，设解$x \equiv g^j \pmod p$，那么有

$$\begin{aligned} &(g^j)^2 \equiv g^i \pmod p \Leftrightarrow 2j \equiv i \pmod{p-1} \\ &\Rightarrow \exists k, i = (p-1)k + 2j \Rightarrow i\text{为偶数} \end{aligned}$$

反之，若i为偶数，$g^{\frac{i}{2}}$是二次同余式(2)的解。因此有

定理*: 设p为奇素数，g是模p的原根，$n \equiv g^i \pmod p$。勒让德符号

$$\left(\frac{n}{p}\right) = (-1)^i = \begin{cases} 1 & \text{，当且仅当}i\text{为偶数} \\ -1 & \text{，当且仅当}i\text{为奇数} \end{cases}$$

《数论讲义》第1节定理1:$\mathbb{Z}_p^*$中，分别有$\frac{1}{2}(p-1)$个模数p的二次剩余和非二次剩余，且

$$1, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \pmod{p} \tag{3}$$

就是$\mathbb{Z}_p^*$中的全部二次剩余。

证明:设g是模数p的原根。由定理*知道，$g^i \in \mathbb{Z}_p^*$是模数p的二次剩余当且仅当i为偶数。因此$\mathbb{Z}_p^* = \{g^0, g^1, g^2, \ldots, g^{p-2} \pmod{p}\}$中二次剩余和非二次剩余的数量都是$\frac{p-1}{2}$个。

显然(3)中的元素都是模数p的二次剩余。现证明(3)中的元素关于模数p两两不同余，那么(3)包含了$\mathbb{Z}_p^*$中的全部二次剩余。

设$1 \le j < i \le \frac{p-1}{2}$，若$j^2 \equiv i^2 \pmod{p}$，那么有

$$(j-i)(j+i) \equiv 0 \pmod{p}$$

因为$1 < j+i < p$，故$p | j-i$，与所设$1 \le j < i \le \frac{p-1}{2}$矛盾。因此$j^2 \not\equiv i^2 \pmod{p}$。

欧拉判别条件(《数论讲义》第1节定理2):设p是奇素数，勒让德符号

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p \tag{4}$$

证明:设g是模数p的原根，$n \equiv g^i \pmod p$。那么$n^{\frac{p-1}{2}} \equiv g^{\frac{i(p-1)}{2}} \pmod p$对模数$p$的阶为

$$\frac{p-1}{(p-1, \frac{i(p-1)}{2})} = \begin{cases} 1 & ,\ \text{当}i\text{为偶数} \\ 2 & ,\ \text{当}i\text{为奇数} \end{cases}$$

因此

$$n^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p & ,\ \text{当}i\text{为偶数} \\ -1 \pmod p & ,\ \text{当}i\text{为奇数} \end{cases}$$

上式第2个同余式成立的原因是$\mathbb{Z}_p^*$中阶为2的元素的数量为$\phi(2) = 1$个，而$-1 \equiv p-1 \pmod p$的阶为2。
结合定理*，得到(4)。

《数论讲义》第2节定理1:对于给定的奇素数p，勒让德符号$\left(\frac{n}{p}\right)$是一个完全积性函数，即

$$\left(\frac{mn}{p}\right)=\left(\frac{m}{p}\right)\left(\frac{n}{p}\right).$$

证明:设g是模数p的原根，$m\equiv g^i \pmod p$，$n\equiv g^j \pmod p$，那么$mn\equiv g^{i+j} \pmod p$。由定理*得到

$$\left(\frac{mn}{p}\right)=\begin{cases}1 & \text{当且仅当} i+j\text{为偶数} \quad \Leftrightarrow i,j\text{奇偶相同} \quad \Leftrightarrow \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=1\\ -1 & \text{当且仅当} i+j\text{为奇数} \quad \Leftrightarrow i,j\text{奇偶不同} \quad \Leftrightarrow \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)=-1\end{cases}$$

由此得证。

《数论讲义》第2节定理2:对于每一个奇素数p，我们有

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

证明: 由欧拉判定准则有

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

故

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

勒让德符号
高斯引理和二次互反律

高斯利用高斯引理，证明了著名的二次互反律—这是经典数论中最出色的定理之一。由高斯引理还可给出$\left(\frac{2}{p}\right)$的计算公式。

高斯引理(《数论讲义》第3节定理1): 设p是一个奇素数，$(p,n)=1$，且$\frac{1}{2}(p-1)$个数

$$n, 2n, \dots, \frac{(p-1)n}{2} \pmod p \tag{5}$$

中有m个大于$\frac{1}{2}p$，则

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

例: $p=7, n=10$，则

$$10, 2\cdot 10, 3\cdot 10 \equiv 3, 6, 2 \pmod 7,$$

其中有一个$>\frac{7}{2}$。故$m=1$，而得$\left(\frac{10}{7}\right)=-1$。

高斯引理证明:以$a_1,\ldots,a_l$表示(5)中所有小于$\frac{1}{2}p$的数，$b_1,\ldots,b_m$表示(5) 中所有大于$\frac{1}{2}p$的数，显然，$l+m=\frac{1}{2}(p-1)$，且

$$\prod_{s=1}^{l}a_s\prod_{t=1}^{m}b_t\equiv\prod_{k=1}^{\frac{1}{2}(p-1)}kn=(\frac{p-1}{2})!n^{\frac{p-1}{2}}\pmod p. \tag{6}$$

$p-b_t$也在1和$\frac{1}{2}(p-1)$之间，故$a_s,p-b_t(s=1,\ldots,l,t=1,\ldots,m)$是1和$\frac{1}{2}(p-1)$之间的$\frac{1}{2}(p-1)$个数。现证这$\frac{1}{2}(p-1)$ 个数各不相同，这只需证$a_s\neq p-b_t$。如果$a_s=p-b_t$，即$a_s+b_s=p$，则有

$$xn+yn\equiv 0\pmod p\left(1\leq x,y\leq\frac{p-1}{2}\right)\Rightarrow x+y\equiv 0\pmod p,$$

此不可能，故

$$\begin{aligned}&\prod_{s=1}^{l}a_s\prod_{t=1}^{m}(p-b_t)=\left(\frac{p-1}{2}\right)!\\ \equiv\quad&(-1)^m\prod_{s=1}^{l}a_s\prod_{t=1}^{m}b_t\equiv(-1)^m(\frac{p-1}{2})!n^{\frac{p-1}{2}}\pmod p\text{（由(6)）}\\ \Rightarrow\quad&n^{\frac{p-1}{2}}\equiv(-1)^m\pmod p=\left(\frac{n}{p}\right)\text{（由欧拉判别条件）}\end{aligned}$$

《数论讲义》第2节定理3:对于每一个奇素数p，我们有

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & ,若p\equiv\pm1 \pmod 8),\\ -1 & ,若p\equiv\pm3 \pmod 8).\end{cases}$$

证明:在高斯引理中取$n=2$，则

$$2,2\cdot2,2\cdot3,\ldots,\frac{p-1}{2}\cdot2$$

已在0和p之间。现在求出适合

$$\frac{p}{2}<2k<p \quad 即 \quad \frac{p}{4}<k<\frac{p}{2}$$

的k的个数，即得$m=[\frac{p}{2}]-[\frac{p}{4}]$。
令$p=8a+r,r=1,3,5,7$，则得

$$m=2a+[\frac{r}{2}]-[\frac{r}{4}]\equiv0,1,1,0 \pmod 2),$$

故

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

二次互反律(《数论讲义》第4节): 设$p>2,q>2$是两个素数，$p\neq q$，则

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$$

证明:首先，我们利用高斯引理来计算$\left(\frac{q}{p}\right)$。当$1\leq k\leq\frac{p-1}{2}$，有

$$kq=q_kp+r_k,q_k=\left[\frac{kq}{p}\right],1\leq r_k\leq p-1,$$

令

$$a=\sum_{s=1}^{l}a_s,b=\sum_{t=1}^{m}b_t,$$

此处a_s,b_t的涵义见高斯引理(取$n=q$)的证明，则得

$$a+b=\sum_{k=1}^{\frac{p-1}{2}}r_k \tag{7}$$

由高斯引理的证明知，$a_s,p-b_t(s=1,\ldots,l,t=1,\ldots,m)$正好是$1,2,\ldots,\frac{1}{2}(p-1)$的各数，故有

$$\frac{p^2-1}{8}=1+2+\ldots+\frac{p-1}{2}=a+mp-b, \tag{8}$$

二次互反律证明(续):又

$$\frac{p^2-1}{8}q=\sum_{k=1}^{\frac{p-1}{2}}kq=p\sum_{k=1}^{\frac{p-1}{2}}q_k+\sum_{k=1}^{\frac{p-1}{2}}r_k=p\sum_{k=1}^{\frac{p-1}{2}}q_k+a+b \tag{9}$$

(9)式减去(8)式得

$$\frac{p^2-1}{8}(q-1)=p\sum_{k=1}^{\frac{p-1}{2}}q_k-mp+2b,$$

上式两边模2并移位得到

$$m\equiv\sum_{k=1}^{\frac{p-1}{2}}q_k \pmod 2 \Rightarrow \left(\frac{q}{p}\right)=(-1)^m=(-)^{\sum_{k=1}^{\frac{p-1}{2}}q_k}=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]}$$

$$\text{同理可证}\quad \left(\frac{p}{q}\right)=(-1)^{\sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]}$$

即得

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]+\sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]}$$

二次互反律证明(续): 剩下来，只需证明

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] + \sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}] = \frac{p-1}{2} \cdot \frac{q-1}{2} \tag{10}$$

作以

$$(0,0), (0, \frac{q}{2}), (\frac{p}{2}, 0), (\frac{p}{2}, \frac{q}{2})$$

为顶点的长方形，那么经原点的对角线上无整点（整点即二坐标均为整数的点），因若此对角线上有整点(x, y)，则

$$xq - yp = 0.$$

即得$p|x, q|y$，而此类型的点在长方形的外面。长方形内的整点总数为$\frac{p-1}{2} \cdot \frac{q-1}{2}$，其中对角线之下的整点数为

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]$$

而对角线之上的整点数为

$$\sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]$$

故得到(10)

总结我们得到的计算勒让得符号的计算法则。设p, q是奇素数，

方法1 欧拉判别条件：$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p$

方法2 利用以下法则计算：

- 基本性质：若$n \equiv n' \not\equiv 0 \pmod p$，则$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right)$。
- 完全积性：$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$
- 二次互反律：$p \neq q$，则
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \text{ 或 } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{(p-1)(q-1)}{4}}$$
- $$\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & ,\text{若} p \equiv 1 \pmod 4, \\ -1 & ,\text{若} p \equiv 3 \pmod 4. \end{cases}$$
- $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & ,\text{若} p \equiv \pm 1 \pmod 8, \\ -1 & ,\text{若} p \equiv \pm 3 \pmod 8. \end{cases}$$

利用以上所给计算法则，给出几个勒让得符号的计算例子。

例1:设$p=593, n=438$，计算$\left(\frac{438}{593}\right)$.

解:因为$438=2\cdot 3\cdot 73$，故

$$\begin{aligned}
\left(\frac{438}{593}\right) &= \left(\frac{2}{593}\right)\cdot\left(\frac{3}{593}\right)\cdot\left(\frac{73}{593}\right) \text{(完全积性)}\\
&= (-1)^{\frac{593^2-1}{8}}\cdot\left(\frac{3}{593}\right)\cdot\left(\frac{73}{593}\right)\\
&= \left(\frac{3}{593}\right)\cdot\left(\frac{73}{593}\right)\\
&= (-1)^{\frac{(3-1)(593-1)}{4}}\left(\frac{593}{3}\right)\cdot(-1)^{\frac{(73-1)(593-1)}{4}}\left(\frac{593}{73}\right) \text{(二次互反律)}\\
&= \left(\frac{593}{3}\right)\cdot\left(\frac{593}{73}\right)=\left(\frac{2}{3}\right)\cdot\left(\frac{9}{73}\right) \text{(基本性质)}\\
&= \left(\frac{2}{3}\right)\cdot\left(\frac{3\cdot 3}{73}\right)=\left(\frac{2}{3}\right)\cdot\left(\frac{3}{73}\right)^2\\
&= -1\cdot\left((-1)^{\frac{(3-1)(73-1)}{4}}\left(\frac{73}{3}\right)\right)^2\\
&= -1\cdot\left(\frac{1}{3}\right)^2=-1
\end{aligned}$$

勒让得符号
总结

例1:设$p = 593, n = 438$，计算$\left(\frac{438}{593}\right)$.
解: 或者直接利用欧拉判别条件计算：

$$\begin{aligned}\left(\frac{438}{593}\right) &\equiv 438^{\frac{593-1}{2}} \pmod{593} \\ &\equiv -1 \pmod{593} \\ &= -1\end{aligned}$$

例2:求以3为二次剩余的所有素数$p(>3)$。

解:由二次互反律,

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

因

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

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

故

$$\left(\frac{3}{p}\right)=\begin{cases}1, & 若 p\equiv 1 \pmod 3, p\equiv 1 \pmod 4,\\ & 即 p\equiv 1 \pmod{12}(由中国剩余定理得到),\\ 1, & 若 p\equiv -1 \pmod 3, p\equiv -1 \pmod 4,\\ & 即 p\equiv -1 \pmod{12}(由中国剩余定理得到),\\ -1, & 若 p\equiv -1 \pmod 3, p\equiv 1 \pmod 4,\\ & 即 p\equiv 5 \pmod{12}(由中国剩余定理得到),\\ -1, & 若 p\equiv 1 \pmod 3, p\equiv -1 \pmod 4,\\ & 即 p\equiv -5 \pmod{12}(由中国剩余定理得到).\end{cases}$$

综上所述

$$\left(\frac{3}{p}\right)=\begin{cases}1, & 若 p\equiv \pm 1 \pmod{12},\\ -1, & 若 p\equiv \pm 5 \pmod{12}.\end{cases}$$

例3:求以5为二次剩余的所有素数$p(\neq 5)$。

解:由二次互反律得到$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$，及有

$$\left(\frac{1}{5}\right)=1,\left(\frac{2}{5}\right)=(-1)^{\frac{5^2-1}{8}}=-1,\left(\frac{3}{5}\right)=\left(\frac{-2}{5}\right)=-1,\left(\frac{4}{5}\right)=1,$$

可知

$$\left(\frac{p}{5}\right)=\begin{cases}1, & 若 p\equiv\pm1 \pmod 5,\\ -1, & 若 p\equiv\pm2 \pmod 5;\end{cases}$$

例4:求以10为二次剩余的所有素数p。

解:由完全积性得到$\left(\frac{10}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)$，又

$$\left(\frac{2}{p}\right)=\begin{cases}1 & ,若 p\equiv\pm1 \pmod 8,\\ -1 & ,若 p\equiv\pm3 \pmod 8.\end{cases}$$

由例3和中国剩余定理可以算出：

$$\left(\frac{10}{p}\right)=\begin{cases}1, & 若 p\equiv\pm1,\pm3,\pm9,\pm13 \pmod{40},\\ -1, & 若 p\equiv\pm7,\pm11,\pm17,\pm19 \pmod{40};\end{cases}$$

第6节二次同余式的解法和解数

我们将会在椭圆曲线的计算中运用到以下定理。

定理1： 二次同余式

$$x^2 \equiv n \pmod{p},\ p\text{是奇素数，}\ p \nmid n. \tag{11}$$

设$\left(\frac{n}{p}\right) = 1$，则有

1. 当$p \equiv 3 \pmod{4}$时，$\pm n^{\frac{1}{4}(p+1)}$为(11)的解；
2. 当$p \equiv 5 \pmod{8}$，

$$\begin{cases} n^{\frac{1}{4}(p-1)} \equiv 1 \pmod{p}\text{时} & \pm n^{\frac{1}{8}(p+3)}\text{为(11)的解；} \\ n^{\frac{1}{4}(p-1)} \equiv -1 \pmod{p}\text{时} & \pm \left(\frac{p-1}{2}\right)! \cdot n^{\frac{1}{8}(p+3)}\text{为(11)的解.} \end{cases}$$

雅可比符号(《数论讲义》第7节)

计算勒让得符号$\left(\frac{n}{p}\right)$，可以直接利用欧拉判别条件，或者可能需要把n分解成标准分解式，而这是没有有效算法的。避开这个问题的办法是引进也雅可比(Jacobi)符号，

定义： 设m是一个正奇数，$m = p_1 p_2 \dots p_t, p_i (i = 1, \dots, t)$是素数，$(n, m) = 1$，则

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{t} \left(\frac{n}{p_i}\right)$$

叫做**雅可比符号**。

显然，雅可比符号是勒让德符号的推广。

雅可比符号(《数论讲义》第7节)

雅可比符号的计算法则，容易由勒让得符号的计算法则推出，下面的定理1是容易推出的。

定理1:设m, m_1为正奇数，

1. 若$n \equiv n_1 \pmod{m}$和$(n, m) = 1$，则
$$\left(\frac{n}{m}\right) = \left(\frac{n_1}{m}\right)$$
2. 若$(n, m) = (n, m_1) = 1$，则
$$\left(\frac{n}{m}\right)\left(\frac{n}{m_1}\right) = \left(\frac{n}{mm_1}\right)$$
3. 若$(n, m) = (n_1, m) = 1$，则
$$\left(\frac{n}{m}\right)\left(\frac{n_1}{m}\right) = \left(\frac{nn_1}{m}\right)$$

定理2: $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.
证明:因为

$$
\begin{aligned}
m = \prod_{i=1}^{t} p_i &= \prod_{i=1}^{t}(1 + p_i - 1) \\
&= 1 + \sum_{i=1}^{t}(p_i - 1) + \sum_{1\le i<j\le t}(p_i - 1)(p_j - 1) + \ldots \\
&\equiv 1 + \sum_{i=1}^{t}(p_i - 1) \pmod 4
\end{aligned}
$$

因此

$$\frac{m-1}{2} \equiv \sum_{i=1}^{t}\frac{(p_i - 1)}{2} \pmod 2.$$

于是

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{t}\left(\frac{-1}{p_i}\right) = \prod_{i=1}^{t}(-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{t}\frac{p_i-1}{2}} = (-1)^{\frac{m-1}{2}}.$$

定理3: $\left(\frac{2}{m}\right) = (-1)^{\frac{1}{8}(m^2-1)}$.
证明:因为

$$m^2 = \prod_{i=1}^{t}(1 + p_i^2 - 1) = 1 + \sum_{i=1}^{t}(p_i^2 - 1) + \sum_{1\le i<j\le t}(p_i^2 - 1)(p_j^2 - 1) + \dots$$

因为p_i和2互素，因此为奇数，那么$p_i^2 - 1 \equiv 0 \pmod 8 (i = 1, \dots, t)$，
故得

$$m^2 - 1 \equiv \sum_{i=1}^{t}(p_i^2 - 1) \pmod{8^2},$$

即

$$\frac{m^2-1}{8} \equiv \sum_{i=1}^{t}\frac{p_i^2-1}{8} \pmod 8 \Longrightarrow \frac{m^2-1}{8} \equiv \sum_{i=1}^{t}\frac{p_i^2-1}{2} \pmod 2.$$

于是

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

定理4: 若m与n是二个正奇数，且$(m,n)-1$，则

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

证明: 设$m=\prod_{i=1}^{t}p_i, n=\prod_{j=1}^{s}q_j, p_1,\ldots,p_t,q_1,\ldots,q_s$均为素数，则

$$\begin{aligned}
\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\\
&= \prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\\
&= (-1)^{\sum_{i=1}^{t}\sum_{j=1}^{s}\frac{p_i-1}{2}\frac{q_j-1}{2}}\\
&= (-1)^{\sum_{i=1}^{t}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}}\\
&\equiv (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\text{(在定理2中已证}\textstyle\sum_{i=1}^{t}\frac{p_i-1}{2}\equiv\frac{1}{2}(m-1)\pmod{2}\text{)}
\end{aligned}$$

有效计算$\left(\frac{n}{m}\right)$的几条计算法则：

- 基本性质：若$n \equiv n' \not\equiv 0 \pmod{m}$，则$\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$。
- 完全积性：$\left(\frac{nn'}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)$
- 二次互反律：设$(n, m) = 1$，则

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$$

特别地，如果$n = 2^k t$且t为一个奇数，那么：

$$\left(\frac{n}{m}\right) = \left(\frac{2}{m}\right)^k \left(\frac{t}{m}\right)$$

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

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

例:

$$
\begin{aligned}
\left(\frac{7411}{9283}\right) &= \left(\frac{9283}{7411}\right) \quad \text{由二次互反律} \\
&= \left(\frac{1872}{7411}\right) \quad \text{基本性质} \\
&= \left(\frac{2}{7411}\right)^4 \left(\frac{117}{7411}\right) \quad \text{由完全积性} \\
&= \left(\frac{117}{7411}\right) \\
&= \left(\frac{7411}{117}\right) \quad \text{由二次互反律} \\
&= \left(\frac{40}{117}\right) \quad \text{由基本性质} \\
&= \left(\frac{2}{117}\right)^3 \left(\frac{5}{117}\right) \quad \text{由完全积性} \\
&= \left(\frac{5}{117}\right) \\
&= \left(\frac{117}{5}\right) \quad \text{由二次互反律} = \left(\frac{2}{5}\right) = -1
\end{aligned}
$$

计算$\left(\frac{n}{m}\right)$的一般过程：

- 把n写成如下形式$n = 2^k t$且t是奇数，根据性质完全积性和$\left(\frac{2}{m}\right)$的计算法则把问题归结为计算$\left(\frac{t}{m}\right)$
- 如果$t < m$，那么根据二次互反律归结为计算$\left(\frac{m}{t}\right)$，否则根据基本性质归结为计算$\left(\frac{s}{m}\right)$，其中$s = t \bmod m$
- 继续以上过程直到得到最终结果

所需要的时间复杂度为$O((\log(m))^2)$。