初等数论
第四章 二次剩余

中山大学 数据科学与计算机学院

二次剩余

考虑模素数二次同余方程：

$$x^2 \equiv a \bmod p,$$

其中p是奇素数, $(a, p) = 1$.

1. 定义：二次(平方)剩余，二次(平方)非剩余
2. 定理：在模p的一个简化剩余系中, 恰有$\frac{p-1}{2}$个模p二次剩余, 恰有$\frac{p-1}{2}$个模p二次非剩余; 如果a是模p二次剩余, 那么$x^2 \equiv a \bmod p$的解数为2.
3. 列举：集合

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

   给出了模p的全部二次剩余.
4. 欧拉判别条件：a是模p的平方剩余 $\iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$; a是模p的平方非剩余 $\iff a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

勒让德(Legendre)符号

设p是素数，定义Legendre符号如下：

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{如果}a\text{是模}p\text{的平方剩余}\\ -1 & \text{如果}a\text{是模}p\text{的平方非剩余}\\ 0 & \text{如果}p|a\end{cases}$$

根据二次剩余的欧拉判别条件, 如果p是奇素数, $a\in\mathbb{Z}$, 则$a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\bmod p$.

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{if } p\equiv 1 \bmod 4\\ -1 & \text{if } p\equiv 3 \bmod 4\end{cases}$$

- $(\frac{a+kp}{p})=(\frac{a}{p})$, $a\equiv b \bmod p\Longrightarrow(\frac{a}{p})=(\frac{b}{p})$
- $(\frac{ab}{p})=(\frac{a}{p})(\frac{b}{p})$, $(a,p)=1\Longrightarrow(\frac{a^2}{p})=1$.

高斯引理

引理（Gauss引理）

设p是奇素数，a是整数，且$(a,p)=1$. 如果在整数

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

中模p后大于$\frac{p}{2}$的个数是m，则$\left(\frac{a}{p}\right)=(-1)^m$.

Gauss引理的一个直接应用就是$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$，或者

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

当a是奇数时，

$$\left(\frac{a}{p}\right)=(-1)^{T(a,p)}=(-1)^{\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]}.$$

Gauss引理的一个直接应用就是计算$\left(\frac{2}{p}\right)$.
采用Gauss引理中的符号, 取$a=2$, 可以看到

$$1 \leq j < \frac{p}{4} \Longrightarrow 1 < 2j < \frac{p}{2}, \quad \frac{p}{4} < j < \frac{p}{2} \Longrightarrow \frac{p}{2} < 2j < p$$

所以

$$m = \frac{p-1}{2} - \left[\frac{p}{4}\right] \quad 即 \quad m = \begin{cases} l & p = 4l+1 \\ l+1 & p = 4l+3 \end{cases}$$

将$l=2k-1$和$l=2k$分别带入, 可以进一步得到

$$m = \begin{cases} 2k-1 & p = 8k-3 \\ 2k & p = 8k-1 \end{cases} \quad 和 \quad m = \begin{cases} 2k & p = 8k+1 \\ 2k+1 & p = 8k+3 \end{cases}.$$

所以有

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

对于$1 \le j \le \frac{p-1}{2}$, 利用向下取整符号$[\cdot]$, 整数$(ja)$可以进一步表示为:

$$ja = p\left[\frac{ja}{p}\right] + (ja \bmod p).$$

两边对j求和得

$$a\sum_{j=1}^{\frac{p-1}{2}} j = p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right] + \sum_{j=1}^{\frac{p-1}{2}}(ja \bmod p) = pT + \sum_{j=1}^{\frac{p-1}{2}}(ja \bmod p).$$

而

$$\sum_{j=1}^{\frac{p-1}{2}}(ja \bmod p) = s_1 + \ldots + s_k + r_1 + \ldots + r_m$$

$$= s_1+\ldots+s_k+(p-r_1)+\ldots+(p-r_m)-mp+2(r_1+\ldots+r_m) = \sum_{j=1}^{\frac{p-1}{2}} j-mp+2(r_1+\ldots+r_m).$$

利用等差数列求和公式$S_n = \frac{n(a_1+a_n)}{2}$, 我们有

$$a\cdot\frac{\frac{p-1}{2}\cdot(1+\frac{p-1}{2})}{2} = pT + \frac{\frac{p-1}{2}\cdot(1+\frac{p-1}{2})}{2} - mp + 2(r_1+\ldots+r_m).$$

整理后, 可得

$$\frac{p^2-1}{8}(a-1)=p(T-m)+2(r_1+\ldots+r_m),$$

即

$$\frac{p^2-1}{8}(a-1)\equiv T+m \bmod 2.$$

要注意到p是奇素数, 而且模2下正负号是一样的, 因此有$p(T-m)\equiv T+m \bmod 2$. 易见, 当$a=2, 1\leq j\leq \frac{p-1}{2}$时, 有$2\leq 2j\leq p-1$, 进而有$[\frac{2j}{p}]=0$. 于是,

$$T=\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{2j}{p}\right]=0$$

从而, 当$a=2$时,

$$m\equiv\frac{p^2-1}{8} \bmod 2.$$

这样就有

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

当a是奇数时, $a-1$是偶数, 于是

$$\frac{p^2-1}{8}(a-1) \equiv T + m \bmod 2 \Longrightarrow 0 \equiv T + m \bmod 2$$

因为模2下正负号是一样的, 所以有

$$T \equiv m \bmod 2$$

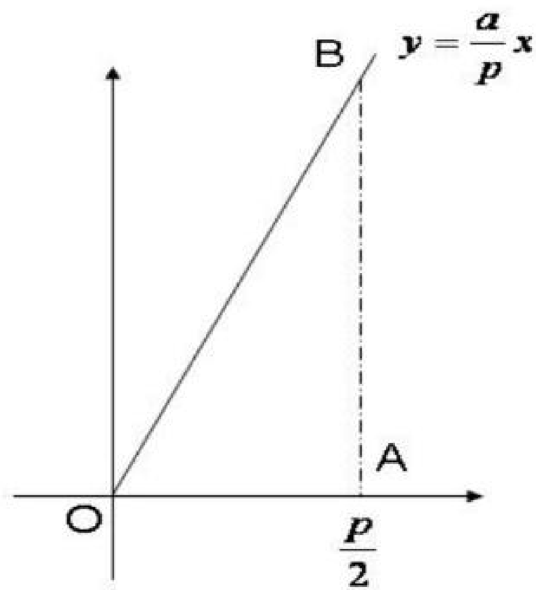
即

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] \equiv m \bmod 2$$

所以有

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]}.$$

设a是正数, 考虑$T(a,p)=\sum_{j=1}^{\frac{p-1}{2}}[\frac{ja}{p}]$的几何意义.

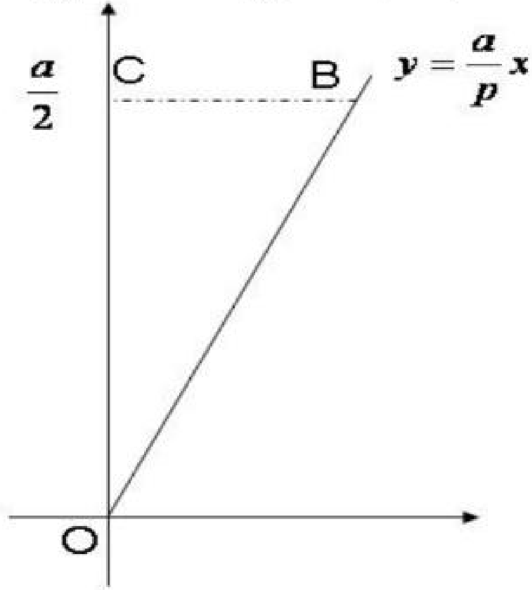


整数

$$[\frac{a}{p}\cdot 1],[\frac{a}{p}\cdot 2],\ldots,[\frac{a}{p}\cdot\frac{p-1}{2}]$$

分别是x取$1,2,\ldots,\frac{p-1}{2}$时对应的竖线(垂线)上的整点(横纵坐标均为整数)的个数. 显然, AB上没有整点(因为$\frac{p}{2}$不是整数), OB上除O外无整点(因为$\frac{a}{p}$不是整数), 这样$T(a,p)$就是三角形OAB内部的整点的个数.

如果a也是奇素数，则可以考虑$(\frac{p}{a})$. 于是$(\frac{p}{a}) = (-1)^{T(p,a)} = (-1)^{\sum_{j=1}^{\frac{a-1}{2}}[\frac{jp}{a}]}$.

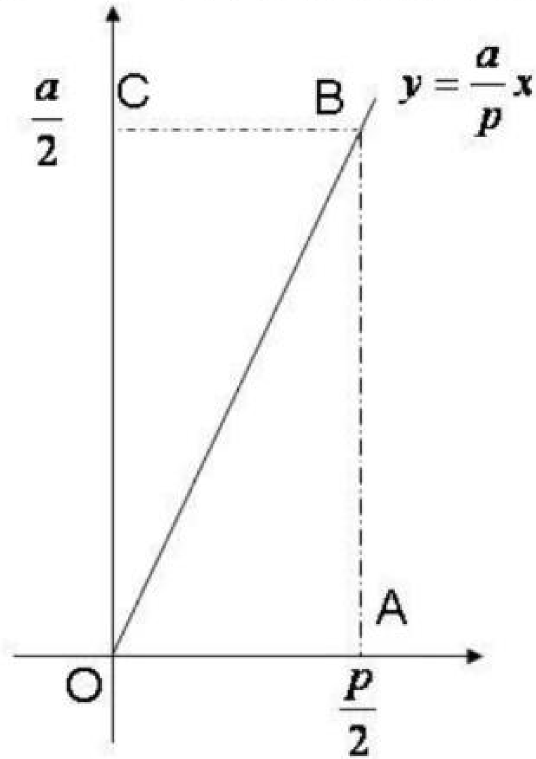


整数

$$[\frac{p}{a}\cdot 1], [\frac{p}{a}\cdot 2], \ldots, [\frac{p}{a}\cdot\frac{a-1}{2}]$$

分别是y取$1, 2, \ldots, \frac{a-1}{2}$时对应的横线(水平线)上的整点(横纵坐标均为整数)的个数. 显然, CB上没有整点(因为$\frac{a}{2}$不是整数), OB上除O外无整点(因为$\frac{a}{p}$不是整数), 这样$T(p,a)$就是三角形OCB内部的整点的个数.

这样, $T(a,p)+T(p,a)$就是矩形$OABC$内部的整点个数.



这个矩形内部的整点个数显然是$\frac{p-1}{2}\cdot\frac{a-1}{2}$, 所以,

$$T(a,p)+T(p,a)=\frac{p-1}{2}\cdot\frac{a-1}{2}$$

所以, 当a,p都是奇素数时, $(\frac{a}{p})\cdot(\frac{p}{a})=(-1)^{T(a,p)}\cdot(-1)^{T(p,a)}=(-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}$.
这就是著名的(Gauss)二次互反律.

定理（二次互反律）

设$p \neq q$均为奇素数，则

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

定理（二次互反律）

设$p \neq q$均为奇素数, 则

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

推论

设$p \neq q$均为奇素数, 如果p, q只要有一个是$4k+1$型整数, 则$(\frac{p}{q}) = (\frac{q}{p})$.
当且仅当p, q都是$4k+3$型整数时, $(\frac{p}{q}) = -(\frac{q}{p})$.

定理（二次互反律）

设$p \neq q$均为奇素数, 则

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

推论

设$p \neq q$均为奇素数, 如果p, q只要有一个是$4k+1$型整数, 则$(\frac{p}{q}) = (\frac{q}{p})$.
当且仅当p, q都是$4k+3$型整数时, $(\frac{p}{q}) = -(\frac{q}{p})$.

利用这个推论, 结合$\left(\frac{-1}{p}\right)$和$\left(\frac{2}{p}\right)$的性质, 可以更好地计算勒让得符号.

计算$(\frac{137}{227})$
事实上，227是素数，

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) =$$

计算$(\frac{137}{227})$
事实上，227是素数，

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) = (\frac{-1}{227})(\frac{2 \cdot 3^2 \cdot 5}{227})$$

计算$(\frac{137}{227})$
事实上，227是素数，

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) = (\frac{-1}{227})(\frac{2 \cdot 3^2 \cdot 5}{227})$$

$$= (-1)(\frac{2}{227})(\frac{3^2}{227})(\frac{5}{227})$$

计算$(\frac{137}{227})$
事实上，227是素数,

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) = (\frac{-1}{227})(\frac{2 \cdot 3^2 \cdot 5}{227})$$

$$= (-1)(\frac{2}{227})(\frac{3^2}{227})(\frac{5}{227}) \quad (\because (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}})$$

$$= (-1)(\frac{2}{227})(\frac{5}{227})$$

计算$(\frac{137}{227})$
事实上，227是素数,

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) = (\frac{-1}{227})(\frac{2\cdot 3^2 \cdot 5}{227})$$

$$= (-1)(\frac{2}{227})(\frac{3^2}{227})(\frac{5}{227}) \quad (\because (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}})$$

$$= (-1)(\frac{2}{227})(\frac{5}{227}) \quad (\because p \nmid a \Longrightarrow (\frac{a^2}{p}) = 1)$$

$$= (-1)(-1)(\frac{5}{227})$$

计算$(\frac{137}{227})$
事实上，227是素数，

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) = (\frac{-1}{227})(\frac{2\cdot 3^2 \cdot 5}{227})$$

$$= (-1)(\frac{2}{227})(\frac{3^2}{227})(\frac{5}{227}) \quad (\because (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}})$$

$$= (-1)(\frac{2}{227})(\frac{5}{227}) \quad (\because p \nmid a \Longrightarrow (\frac{a^2}{p}) = 1)$$

$$= (-1)(-1)(\frac{5}{227}) \quad (\because 227 = 28 \cdot 8 + 3, (\frac{2}{p}) = -1 \text{ if } p \equiv \pm 3 \bmod 8)$$

计算$(\frac{137}{227})$
事实上，227是素数，

$$137 \equiv -90 \bmod 227 \Longrightarrow (\frac{137}{227}) = (\frac{-90}{227}) = (\frac{-1}{227})(\frac{2 \cdot 3^2 \cdot 5}{227})$$

$$= (-1)(\frac{2}{227})(\frac{3^2}{227})(\frac{5}{227}) \quad (\because (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}})$$

$$= (-1)(\frac{2}{227})(\frac{5}{227}) \quad (\because p \nmid a \Longrightarrow (\frac{a^2}{p}) = 1)$$

$$= (-1)(-1)(\frac{5}{227}) \quad (\because 227 = 28 \cdot 8 + 3, (\frac{2}{p}) = -1 \text{ if } p \equiv \pm 3 \bmod 8)$$

对于$(\frac{5}{227})$，因为5模4余1，所以$(\frac{5}{227}) = (\frac{227}{5})$，而$227 \equiv 2 \bmod 5$，于是

$$(\frac{227}{5}) = (\frac{2}{5}) = -1(\because 5 \equiv -3 \bmod 8).$$

最终，$(\frac{137}{227}) = -1$

上述计算$(\frac{137}{227})$其实就是相当于判断同余式$x^2 \equiv 137 \bmod 227$是否有解.

示例: 判断$x^2 \equiv -1 \bmod 365$是否有解? 如果有, 解数多少?

上述计算$(\frac{137}{227})$其实就是相当于判断同余式$x^2 \equiv 137 \bmod 227$是否有解.

示例: 判断$x^2 \equiv -1 \bmod 365$是否有解? 如果有, 解数多少?
无法直接使用勒让得符号的方法, 因为365不是素数, 所以勒让得符号$(\frac{-1}{365})$没有定义.
但是$365 = 7 \cdot 73$, 5和73互素, 这时原同余式等价于下面的同余方程组.

$$\begin{cases} x^2 \equiv -1 \bmod 5 \\ x^2 \equiv -1 \bmod 73 \end{cases}$$

这样要判断原同余式的解, 只需要判断这个同余式组的解的情况.
这里5和73都是素数, 所以:
可以使用勒让得符号判断$x^2 \equiv -1 \bmod 5$有解$(\because (\frac{-1}{5}) = 1)$,
可以使用勒让得符号判断$x^2 \equiv -1 \bmod 73$有解$(\because (\frac{-1}{73}) = 1)$
所以同余式组有解, 解数为4,
故原同余式有解, 解数为4.

3模p的勒让德符号

设p是大于3的奇素数, 那么3模p的勒让德符号可以使用二次互反律来确定.

$$\left(\frac{3}{p}\right)=\begin{cases}\left(\frac{p}{3}\right) & \text{如果 } p\equiv 1 \bmod 4\\ (-1)\left(\frac{p}{3}\right) & \text{如果 } p\equiv -1 \bmod 4\end{cases}$$

而

$$\left(\frac{p}{3}\right)=\begin{cases}\left(\frac{1}{3}\right)=1 & \text{如果 } p\equiv 1 \bmod 3\\ \left(\frac{-1}{3}\right)=-1 & \text{如果 } p\equiv -1 \bmod 3\end{cases}$$

于是, 3是模p的二次剩余当且仅当

$$\begin{cases}p\equiv 1 \bmod 4\\ p\equiv 1 \bmod 3\end{cases}\qquad\qquad \begin{cases}p\equiv -1 \bmod 4\\ p\equiv -1 \bmod 3\end{cases}$$

这等价于$p\equiv \pm 1 \bmod 12$.
相反地, 当$p\equiv \pm 5 \bmod 12$时, 那么3是模p的二次非剩余.

3. 雅可比(Jacobi)符号

设$m m = p_1 p_2 \ldots p_s$是奇素数p_i的乘积, 对于任意整数a, 定义雅可比(Jacobi)符号为

$$\left(\frac{a}{m}\right) \triangleq \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \cdots \cdot \left(\frac{a}{p_s}\right)$$

其中$\left(\frac{a}{p_i}\right)$是模$p_i$的勒让得符号.
显然, 根据这个定义, 当m本身就是素数时, 雅可比符号就是勒让得符号.

雅可比(Jacobi)符号的基本性质

- 如果$(m,n)>1$, 则
$$\left(\frac{m}{n}\right)=\left(\frac{n}{m}\right)=0.$$
- $\left(\frac{a+m}{m}\right)=\left(\frac{a}{m}\right)$, 类似地, $\left(\frac{a+km}{m}\right)=\left(\frac{a}{m}\right)$
$$\left(\frac{a+m}{m}\right)=\left(\frac{a+m}{p_1p_2\cdots p_s}\right)=\left(\frac{a}{p_1}\right)\cdots\cdots\left(\frac{a}{p_s}\right)=\left(\frac{a}{m}\right)$$
- $\left(\frac{ab}{m}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$
- 如果$(a,m)=1$, 则
$$\left(\frac{a^2}{m}\right)=1$$
- $\left(\frac{1}{m}\right)=1$

当$m=p_1p_2\dots p_s$是奇素数的乘积时, 我们有

$$\begin{aligned} m &= (1+2\cdot\frac{p_1-1}{2})(1+2\cdot\frac{p_2-1}{2})\dots(1+2\cdot\frac{p_s-1}{2}) \\ &= 1+2\cdot\frac{p_1-1}{2}+\dots+2\cdot\frac{p_s-1}{2}+4\cdot(\dots). \end{aligned}$$

于是

$$m\equiv 1+2\cdot\frac{p_1-1}{2}+2\cdot\frac{p_2-1}{2}+\dots+2\cdot\frac{p_s-1}{2} \bmod 4.$$

所以

$$m-1\equiv 2\cdot(\frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_s-1}{2}) \bmod 4$$

$$\frac{m-1}{2}\equiv\frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_s-1}{2} \bmod 2$$

即存在某一整数k使得

$$\frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_s-1}{2}=2k+\frac{m-1}{2}.$$

- $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$
  这是因为

$$\begin{aligned}
\left(\frac{-1}{m}\right) &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_s}\right) \\
&= (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\ldots(-1)^{\frac{p_s-1}{2}} \\
&= (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\frac{p_s-1}{2}} \\
&= (-1)^{\frac{m-1}{2}}
\end{aligned}$$

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

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$$

所以, 在这种意义下, 勒让德符号是雅克比符号的特殊情形.

类似地, 设$m = p_1p_2\dots p_s$,是奇素数的乘积, 则$m^2 = p_1^2p_2^2\dots p_s^2$, 于是有

$$m^2 \equiv p_1^2p_2^2\dots p_s^2 \bmod 16.$$

这是因为

$$\begin{aligned} m^2 &= (1+8\cdot\frac{p_1^2-1}{8})(1+8\cdot\frac{p_2^2-1}{8})\dots(1+8\cdot\frac{p_s^2-1}{8}) \\ &= 1+8\cdot\frac{p_1^2-1}{8}+\dots+8\cdot\frac{p_s^2-1}{8}+64\cdot(\dots). \end{aligned}$$

于是

$$m^2-1 \equiv 8\cdot\frac{p_1^2-1}{8}+8\cdot\frac{p_2^2-1}{8}+\dots+8\cdot\frac{p_s^2-1}{8} \bmod 16$$

所以

$$\frac{m^2-1}{8} \equiv \frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\dots+\frac{p_s^2-1}{8} \bmod 2$$

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

这是因为

$$\begin{aligned}
\left(\frac{2}{m}\right) &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_s}\right) \\
&= (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\ldots(-1)^{\frac{p_s^2-1}{8}} \\
&= (-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\frac{p_s^2-1}{8}} \\
&= (-1)^{\frac{m^2-1}{8}}
\end{aligned}$$

回忆

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

所以, 在这种意义下, 勒让德符号是雅克比符号的特殊情形.

雅克比符号的互反律

设m,n都是奇素数的乘积, 且$(m,n)=1$, 则

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

证明: 设$m=p_1p_2\dots p_r, n=q_1q_2\dots q_s$, 其中$p_i,q_j$均为奇素数, 且$p_i\neq q_j$, 则

$$\left(\frac{n}{m}\right)=\prod_{i=1}^{r}\left(\frac{n}{p_i}\right)=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)$$

$$=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

$$=\left(\prod_{i=1}^{r}\prod_{j=1}^{s}(\frac{p_i}{q_j})\right)\cdot\left(\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\right)$$

$$=\left(\frac{m}{n}\right)\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

可以看到

$$\left(\frac{m}{n}\right)\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}=\left(\frac{m}{n}\right)(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\sum_{j=1}^{s}\frac{q_j-1}{2}}$$

再注意到

$$\left(\sum_{i=1}^{r}\frac{p_i-1}{2}\right)\equiv\frac{m-1}{2} \bmod 2 \quad \text{以及} \quad \left(\sum_{i=1}^{r}\frac{q_i-1}{2}\right)\equiv\frac{n-1}{2} \bmod 2.$$

所以

$$\left(\frac{m}{n}\right)(-1)^{\sum_{i=1}^{r}\frac{p_i-1}{2}\cdot\sum_{j=1}^{s}\frac{q_j-1}{2}}=\left(\frac{m}{n}\right)(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$$

雅克比符号的上述几个性质表明:

计算雅克比符号(包括勒让德符号)的值, 并不需要求素因数分解式.

在密码学中将会提到, 正是由于这一原因, (教科书式的)RSA加密会泄露明文的至少一比特信息.

示例: 计算

$$(\frac{105}{317}) = (\frac{307}{105}) = (\frac{2}{105}) = 1$$

利用雅克比符号的基本性质, 不必计算$(\frac{105}{317}) = (\frac{3}{317})(\frac{5}{317})(\frac{7}{317})$.

以上的雅克比符号性质虽然都和勒让德符号类似, 但不能忽视两者之间的本质区别:
雅克比符号$(\frac{n}{m}) = 1$不表示二次同余方程

$$x^2 \equiv n \bmod m$$

一定有解.
例如: $(\frac{3}{119}) = 1$, 但$x^2 \equiv 3 \bmod 9$ 无解.

同样的, 对雅克比符号来说, 没有欧拉判别条件$(\frac{n}{m}) = n^{\frac{m-1}{2}} \bmod m$.
也不存在类似勒让德符号的Gauss引理, 即不存在等式$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{\frac{p-1}{2}} [\frac{aj}{p}]}$成立.

4. 模素数的二次同余方程求解

计算勒让德符号可以判定二次同余方程$x^2 \equiv a \bmod p$解的存在性, 其中p是奇素数. 如果二次同余方程的解是存在的, 应该怎么求解? 下面给出求解的一般思路是.

4. 模素数的二次同余方程求解

计算勒让德符号可以判定二次同余方程$x^2 \equiv a \bmod p$解的存在性, 其中p是奇素数. 如果二次同余方程的解是存在的, 应该怎么求解? 下面给出求解的一般思路是.

- 将$p-1$写成是2的幂和一个奇数的乘积形式, 即$p-1 = 2^t \cdot s$, 其中$s \geq 1$.
- 首先应用欧拉定理和欧拉判别条件，我们发现较容易求出同余方程

$$y^{2^{t-1}} \equiv 1 \bmod p$$

  的一个形如$a^{-1}x_{t-1}^2$的解. 如果$t=1$, 则$x_0 \bmod p$就是原二次同余式的一个解.
- 如果$t>1$, 在$a^{-1}x_{t-1}^2$基础上, 能够比较容易地求出同余方程

$$y^{2^{t-2}} \equiv 1 \bmod p$$

  的一个形如$a^{-1}x_{t-2}^2$的解. 如果$t=2$, 则求解工作可以结束.
- 如果$t>2$, 在$a^{-1}x_{t-2}^2$基础上, 继续类似的求解运算, 即求出同余方程

$$y^{2^{t-3}} \equiv 1 \bmod p$$

  的一个形如$a^{-1}x_{t-3}^2$的解;

- 一般地, 如果求出了同余方程

$$y^{2^{t-k}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-k}^2$的解, 且$t > k$, 可以类似的求出同余方程

$$y^{2^{t-k-1}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-k-1}^2$的解.

- 继续下去, 我们一定能求出同余方程

$$y^2 \equiv 1 \bmod p$$

的一个形如$a^{-1}x_1^2$的解, 从而最终能够比较容易地求出

$$y \equiv 1 \bmod p$$

的一个形如$a^{-1}x_0^2$的解.

- 至此, 将完成原二次同余方程的求解, 即一个解$x_0 \bmod p$, 另一个是$-x_0 \bmod p$.

具体求解时，先任意选取模p的一个平方非剩余n，计算$b=(n^s \bmod p)$，从而有

$$b^{2^t}=(n^s)^{2^t}=n^{s\cdot 2^t}=n^{p-1}\equiv 1 \bmod p$$

$$b^{2^{t-1}}=(n^s)^{2^{t-1}}=n^{s\cdot 2^{t-1}}=n^{\frac{p-1}{2}}\equiv -1 \bmod p$$

给定$p-1=2^t\cdot s$，同余方程$y^{2^{t-1}}\equiv 1 \bmod p$的一个形如$a^{-1}x_{t-1}^2$的解(其中的$x_{t-1}$)是

$$x_{t-1}=(a^{\frac{s+1}{2}} \bmod p).$$

这是因为

$$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv (a^{-1}(a^{\frac{s+1}{2}})^2)^{2^{t-1}}=(a^{-1}a^{s+1})^{2^{t-1}}=a^{s\cdot 2^{t-1}}\equiv a^{\frac{p-1}{2}}\equiv 1 \bmod p.$$

下面是找出方程$y^{2^{t-2}}\equiv 1 \bmod p$的一个形如$a^{-1}x_{t-2}^2$的解的方法.
由于$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv 1 \bmod p$，而且$(a^{-1}x_{t-1}^2)^{2^{t-1}}=[(a^{-1}x_{t-1}^2)^{2^{t-2}}]^2$
所以必定有

$$(a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-1}^2)^{2^{t-2}}\equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$, 则令$x_{t-2} = x_{t-1}$, 且有

$$(a^{-1}x_{t-2}^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-2}^2$是同余方程$y^{2^{t-2}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \bmod p$, 则令$x_{t-2} = x_{t-1} \cdot b^{2^0} = x_{t-1} \cdot b$, 且有

$$\begin{aligned}(a^{-1}x_{t-2}^2)^{2^{t-2}} &= (a^{-1}x_{t-1}^2 b^2)^{2^{t-2}} = (a^{-1}x_{t-1}^2)^{2^{t-2}}(b^2)^{2^{t-2}} \\ &= (a^{-1}x_{t-1}^2)^{2^{t-2}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-2}^2$是同余方程$y^{2^{t-2}} \equiv 1 \bmod p$的解.

所以, 不论$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \bmod p$还是$(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \bmod p$, 总能利用方程

$$y^{2^{t-1}} \equiv 1 \bmod p$$

一个形如$a^{-1}x_{t-1}^2$的解, 计算出方程

$$y^{2^{t-2}} \equiv 1 \bmod p$$

的一个形如$a^{-1}x_{t-2}^2$的解.

类似地, 必定有

$$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$, 则令$x_{t-3} = x_{t-2}$, 且有

$$(a^{-1}x_{t-3}^2)^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-2}^2)^{2^{t-3}} \equiv -1 \bmod p$, 则令$x_{t-3} = x_{t-2} \cdot b^{2^1}$, 则$x_{t-3}^2 = x_{t-2}^2 \cdot b^{2^2}$, 且有

$$\begin{aligned}(a^{-1}x_{t-3}^2)^{2^{t-3}} &= (a^{-1}x_{t-2}^2 b^{2^2})^{2^{t-3}} = (a^{-1}x_{t-2}^2)^{2^{t-3}}(b^{2^2})^{2^{t-3}} \\ &= (a^{-1}x_{t-2}^2)^{2^{t-3}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-3}^2$是同余方程$y^{2^{t-3}} \equiv 1 \bmod p$的解.

类似地, 必定有

$$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p \quad 或 \quad (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p.$$

case 1: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$, 则令$x_{t-4} = x_{t-3}$, 且有

$$(a^{-1}x_{t-4}^2)^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv 1 \bmod p$$

即$a^{-1}x_{t-4}^2$是同余方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.

case 2: 如果$(a^{-1}x_{t-3}^2)^{2^{t-4}} \equiv -1 \bmod p$, 则令$x_{t-4} = x_{t-3} \cdot b^{2^2}$, 则$x_{t-4}^2 = x_{t-3}^2 \cdot b^{2^3}$, 且有

$$\begin{aligned}(a^{-1}x_{t-4}^2)^{2^{t-4}} &= (a^{-1}x_{t-3}^2 b^{2^3})^{2^{t-4}} = (a^{-1}x_{t-3}^2)^{2^{t-4}}(b^{2^3})^{2^{t-4}} \\ &= (a^{-1}x_{t-3}^2)^{2^{t-4}} b^{2^{t-1}} \equiv 1 \bmod p\end{aligned}$$

即$a^{-1}x_{t-4}^2$是方程$y^{2^{t-4}} \equiv 1 \bmod p$的解.

示例: 求解$x^2 \equiv 186 \bmod 401$
计算$(\frac{186}{401}) = 1$, 说明原方程有解.

$$a = 186, p = 401, p-1 = 2^4 \cdot 25, t = 4, s = 25, a^{-1} \equiv 235 \bmod 401.$$

取一个模p的非平方剩余$n = 3$, 计算$b = n^s = 3^{25} \equiv 268 \bmod 401$
计算$y^{2^{t-1}} \equiv 1 \bmod p$的解:

$$x_{t-1} = (a^{\frac{s+1}{2}}), \quad x_3 = (186^{\frac{25+1}{2}} \bmod 401) = 103$$

$$a^{-1}x_3^2 = (235 \cdot 103^2 \bmod 401) = 98$$

计算$y^{2^{t-2}} \equiv 1 \bmod p$的解:

$$\because (a^{-1}x_3^2)^{2^{t-2}} \equiv 98^4 \equiv -1 \bmod 401$$

$$\therefore x_{t-2} = x_{t-1}b, \quad x_2 = (x_3 b \bmod p) = (103 \cdot 268 \bmod 401) = 336$$

$$a^{-1}x_{t-2}^2 = (235 \cdot 336^2 \bmod 401) = 400 \equiv -1 \bmod 401$$

计算$y^{2^{t-3}} \equiv 1 \bmod p$的解:

$$\because (a^{-1}x_2^2)^{2^{t-3}} \equiv (-1)^2 \equiv 1 \bmod 401$$

$$\therefore x_{t-3} = x_{t-2}, \quad x_1 = x_2 = 336$$

$$a^{-1}x_{t-3}^2 = (235 \cdot 336^2 \bmod 401) = 400 \equiv -1 \bmod 401$$

计算$y^{2^{t-4}} \equiv 1 \bmod p$, 即$y \equiv 1 \bmod p$ 的解:

$$\because (a^{-1}x_1^2)^{2^{t-4}} \equiv -1 \bmod 401$$

$$\therefore x_{t-4} = x_{t-3}b^{2^{3-1}}, \quad x_0 = (x_1 b^4 \bmod 401) = (336 \cdot 268^4 \bmod 401) = 304$$

这就是我们要求的原方程的解: $x \equiv \pm 304 \bmod 401$.

对于$4k+3$形式的素数p, 不需要像上述那样繁琐的计算.
如果$x^2 \equiv a \bmod p$有解, 其中$p=4k+3$, k为正整数. 求其解.
因为$x^2 \equiv a \bmod p$有解, 根据欧拉判别条件, 我们有

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

从而有

$$a^{\frac{4k+2}{2}} \equiv 1 \bmod p \Longrightarrow a^{2k+1} \equiv 1 \bmod p.$$

于是

$$a^{2k+1}a \equiv a \bmod p$$

即

$$(a^{k+1})^2 \equiv a \bmod p$$

其中$k+1=\frac{p+1}{4}$. 所以, 原方程的解就是

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

设p和q都是形如$4k+3$形式的素数, 且$x^2 \equiv a \bmod p$和$x^2 \equiv a \bmod q$都有解, 则二次同余方程

$$x^2 \equiv a \bmod pq$$

有解, 并且可以通过中国剩余定理求解获得.

$$\begin{cases} x \equiv a^{\frac{p+1}{4}} \bmod p \\ x \equiv a^{\frac{q+1}{4}} \bmod q \end{cases}$$

$$\begin{cases} x \equiv -a^{\frac{p+1}{4}} \bmod p \\ x \equiv a^{\frac{q+1}{4}} \bmod q \end{cases}$$

$$\begin{cases} x \equiv a^{\frac{p+1}{4}} \bmod p \\ x \equiv -a^{\frac{q+1}{4}} \bmod q \end{cases}$$

$$\begin{cases} x \equiv -a^{\frac{p+1}{4}} \bmod p \\ x \equiv -a^{\frac{q+1}{4}} \bmod q \end{cases}$$

在密码学中, 著名的Rabin公钥加密体制就依赖于二次同余方程$x^2 \equiv a \bmod pq$求解.