初等数论
第四章 二次剩余

中山大学　计算机学院

考虑模为素数的二次同余方程：

$$ay^2 + by + c \equiv 0 \bmod p$$

其中$p \nmid a$. 如果p为2, 很容易验证这个方程是否有解, 所以一般都假设$p > 2$.
由于$p \nmid a \Longrightarrow p \nmid 4a$，所以上述二次同余方程和

$$4a^2y^2 + 4aby + 4ac \equiv 0 \bmod p$$

等价，或者表示为：

$$(2ay + b)^2 \equiv (b^2 - 4ac) \bmod p$$

这样，令$x = 2ay + b$, 我们有二次同余方程：

$$x^2 \equiv (b^2 - 4ac) \bmod p$$

设素数$p > 2$, 如果$x^2 \equiv a \bmod p$有解，则称a是一个模p的平方剩余(二次剩余). 否则，称a是一个模p的平方非剩余(二次非剩余).

例如，$1^2 \equiv 1 \bmod 3$，所以1是模3的平方剩余
0,1,2都不能使得$x^2 \equiv -1 \bmod 3$成立，所以-1是一个模3的平方非剩余.
$2^2 \equiv 4 \bmod 7$，所以4是模7的平方剩余.
$4^2 \equiv 2 \bmod 7$，所以2是模7的平方剩余.
0,1,2,3,4,5,6 均不能使得$x^2 \equiv 5 \bmod 7$成立，所以5是模7的平方非剩余.

对同余方程$x^2 \equiv a \bmod p$，如果$p \mid a$,则$x^2 \equiv a \bmod p$只有唯一解$x \equiv 0 \bmod p$. 所以，下面讨论中都假设$(a, p) = 1$.

习惯上, $x \equiv 0 \bmod p$即不是模p的二次剩余, 也不是非二次剩余.

定理

设p是奇素数. 在模p的简化剩余系中, 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, 则$x^2 \equiv a \bmod p$的解数为2.

证明: 因为p是奇素数, 所以模p的简化剩余系可以写成:

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

对于$\mathcal{C}$中任意一个简化剩余i都有

$$(-i)^2 \equiv i^2 \bmod p$$

这样, a是模p二次剩余当且仅当

$a \equiv 1^2 \bmod p$, 或$a \equiv 2^2 \bmod p$, 或$a \equiv 3^2 \bmod p$, $\cdots$, 或$a \equiv \left(\frac{p-1}{2}\right)^2 \bmod p$.

也就是说, 在模p的简化剩余系中可能成为二次剩余的数至多是$\frac{p-1}{2}$个.

如果这些平方的结果两两不同余, 那么$\mathcal{C}$中二次剩余的数有确$\frac{p-1}{2}$个.

证明(续)：

当
$$1 \le i, j \le \frac{p-1}{2} \quad 且 \quad i \ne j$$
时，我们有
$$i^2 \not\equiv j^2 \bmod p$$
成立．否则$p \mid (i-j)$或$p \mid (i+j)$，矛盾．

所以，$a \equiv 1^2 \bmod p$，或$a \equiv 2^2 \bmod p$，或$a \equiv 3^2 \bmod p$，$\cdots$，或$a \equiv \left(\frac{p-1}{2}\right)^2 \bmod p$．

就给出了模p的全部二次剩余，一共$\frac{p-1}{2}$个．

简化剩余系中剩下的$\frac{p-1}{2}$个数也就是模p的二次非剩余了．

根据这个分析，当a是模p的二次剩余时，则在$1 \sim \frac{p-1}{2}$之间一定有一个且仅有一个整数i使得$i^2 \equiv a \bmod p$成立．这样，$x^2 \equiv a \bmod p$的解就是$x \equiv \pm i \bmod p$，解数为2．

$\diamond$

例如，求$p=11$的二次剩余和二次非剩余：

$$\mathcal{C}=\{-5,-4,-3,-2,-1,1,2,3,4,5\}$$

j	1	2	3	4	5
$d\equiv j^2 \bmod p$	1	4	9	5	3

所以，$\{1,2,3,4,5,6,7,8,9,10\}$中1,3,4,5,9是二次剩余，2,6,7,8,10是二次非剩余.

根据这个表还可以看出$x^2\equiv 9 \bmod p$的解是$\pm 3 \bmod 11$.

定理

设p是奇素数，且$(a,p)=1$. a是模p的平方剩余当且仅当$a^{\frac{p-1}{2}} \equiv 1 \bmod p$. a是模p的平方非剩余当且仅当$a^{\frac{p-1}{2}} \equiv -1 \bmod p$

证明：因为先说明$(a,p)=1$，所以有$a^{p-1} \equiv 1 \bmod p$. 又因为p是奇数，所以

$$(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \bmod p,$$

即

$$p \,|\, (a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1).$$

因为p是素数，因此要么$p \,|\, (a^{\frac{p-1}{2}}-1)$，要么$p \,|\, (a^{\frac{p-1}{2}}+1)$.
这表明，$a^{\frac{p-1}{2}} \equiv 1 \bmod p$与$a^{\frac{p-1}{2}} \equiv -1 \bmod p$必有一个成立.
注意到，二者不能同时成立. 令$t=a^{\frac{p-1}{2}}$，如果同时有$p \,|\, (t-1), p \,|\, (t+1)$，则有$t=kp+1=k'p-1$，即$p(k'-k)=2$，从而$p \cdot |k'-k|=2$，但已经假设了$p$是$\geq 3$的素数.矛盾.

所以，如果我们能够证明a是模p的平方剩余 $\Longleftrightarrow$ $a^{\frac{p-1}{2}} \equiv 1 \bmod p$,那么自然有$a$是模$p$的平方非剩余 $\Longleftrightarrow$ $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

证明(续1)： 先证明必要性"$\Longrightarrow$"：
如果a是模p的二次剩余，则必有i使得$i^2 \equiv a \bmod p$成立，因而有

$$(i^2)^{\frac{p-1}{2}} \equiv i^{p-1} \equiv a^{\frac{p-1}{2}} \bmod p$$

成立. 又因为$p \nmid i$, 所以$(i,p)=1$, 从而有

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

再证明充分性"$\Longleftarrow$"：
如果$a^{\frac{p-1}{2}} \equiv 1 \bmod p$, 这时必有$p \nmid a$, 从而$(p,a)=1$, 即$a$是模$p$的一个简化剩余.
任取非零整数c, 满足

$$-\frac{p-1}{2} \le c \le \frac{p-1}{2},$$

考虑同余式$cx \equiv a \bmod p$. 我们知道, 如果x遍历模p简化剩余系

$$\mathcal{C} = \{-\frac{p-1}{2}, -\left(\frac{p-1}{2}-1\right), -\left(\frac{p-1}{2}-2\right), \cdots, -1, 1, 2, \cdots, \frac{p-1}{2}-1, \frac{p-1}{2}\},$$

则cx也会遍历模p的一个简化剩余系. 这就表明, 在集合$\mathcal{C}$中存在唯一的元素, 记作x_c, 使得$cx_c \equiv a \bmod p$.

证明(续2)：

如果a不是二次剩余，则对于任意满足上述条件的c都有$x_c \neq c \bmod p$.
这样可以将

$$\mathcal{C} = \{-\frac{p-1}{2}, -\left(\frac{p-1}{2}-1\right), -\left(\frac{p-1}{2}-2\right), \cdots, -1, 1, 2, \cdots, \frac{p-1}{2}-1, \frac{p-1}{2}\},$$

的$p-1$个数按照c和x_c分对, 每一对都满足$cx_c \equiv a \bmod p$. 于是, 我们有

$$\left(-\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}+1\right) \cdots (-2) \cdot (-1) \cdot 1 \cdot 2 \cdots (\frac{p-1}{2}-1) \cdot (\frac{p-1}{2}) \equiv a^{\frac{p-1}{2}} \bmod p$$

证明(续2)：

如果a不是二次剩余，则对于任意满足上述条件的c都有$x_c \neq c \bmod p$.

这样可以将

$$\mathcal{C} = \{-\frac{p-1}{2}, -\left(\frac{p-1}{2}-1\right), -\left(\frac{p-1}{2}-2\right), \cdots, -1, 1, 2, \cdots, \frac{p-1}{2}-1, \frac{p-1}{2}\},$$

的$p-1$个数按照c和x_c分对, 每一对都满足$cx_c \equiv a \bmod p$. 于是, 我们有

$$\left(-\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}+1\right) \cdots (-2) \cdot (-1) \cdot 1 \cdot 2 \cdots (\frac{p-1}{2}-1) \cdot (\frac{p-1}{2}) \equiv a^{\frac{p-1}{2}} \bmod p$$

另外，注意到

$$\frac{p-1}{2}+1 \equiv -\frac{p-1}{2} \bmod p$$

$$\frac{p-1}{2}+2 \equiv -\frac{p-1}{2}+1 \bmod p$$

$$\frac{p-1}{2}+3 \equiv -\frac{p-1}{2}+2 \bmod p$$

$$\cdots$$

$$p-1 \equiv -1 \bmod p$$

证明(续3)：
所以，我们有

$$(p-1)! \equiv a^{\frac{p-1}{2}} \bmod p$$

由于已知条件

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

从而

$$(p-1)! \equiv 1 \bmod p.$$

而由Wilson定理，

$$(p-1)! \equiv -1 \bmod p,$$

所以，矛盾，故a是模p的二次剩余.$\diamond$
这个结论被称为欧拉判别条件

欧拉判别条件的简化证明

定理

设$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$, $n\le p$, 且$x^p-x=f(x)q(x)+r(x)$.
那么同余方程$f(x)\equiv 0 \bmod p$有n个解当且仅当$r(x)$的系数都是p的倍数.

$$\begin{aligned} x^p-x &= x^p-a^{\frac{p-1}{2}}x+a^{\frac{p-1}{2}}x-x \\ &= x((x^2)^{\frac{p-1}{2}}-a^{\frac{p-1}{2}})+(a^{\frac{p-1}{2}}-1)x \\ &= x\cdot q(x)\cdot(x^2-a)+(a^{\frac{p-1}{2}}-1)x \end{aligned}$$

其中$q(x)=(x^2)^{\frac{p-1}{2}-1}+(x^2)^{\frac{p-1}{2}-2}a^{\frac{p-1}{2}}+\ldots+(a^{\frac{p-1}{2}})^{p-1}$是整系数多项式.

a是模p的二次剩余, 或者说$x^2\equiv a \bmod p$有两个解, 当且仅当余式$(a^{\frac{p-1}{2}}-1)x$的系数$(a^{\frac{p-1}{2}}-1)$被p整除, 即当且仅当

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

示例：判别137是否是模227的二次剩余
根据欧拉判别条件，需要计算：

$$137^{\frac{227-1}{2}} \bmod 227$$

即$137^{113} \bmod 227$
这可以通过模重复平方计算法得出，最后可得：

$$137^{\frac{227-1}{2}} \equiv -1 \bmod 227$$

故137是模227的平方非剩余.

二次剩余小结

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

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

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

示例：
$a=-1$是模p二次剩余的充要条件是$(-1)^{\frac{p-1}{2}}\equiv 1 \bmod p$, 即$p\equiv 1 \bmod 4$.

示例：
判断同余方程$x^2\equiv 16 \bmod 51$的解数.
由于$51=3\times 17$, 同余方程

$$x^2\equiv 16 \bmod 51 \qquad (1)$$

和同余方程组

$$\begin{cases} x^2\equiv 16 \bmod 3 \\ x^2\equiv 16 \bmod 17 \end{cases} \qquad (2)$$

等价，考虑(1)的解数，只需考虑(2)的解数。

同余方程组(2)又等价于

$$\begin{cases} x^2 \equiv 1 \bmod 3 \\ x^2 \equiv -1 \bmod 17 \end{cases} \qquad (2')$$

显然, 1是模3的二次剩余, 从而第一个同余方程有2个解，分别是$x \equiv 1, 2 \bmod 3$. 使用欧拉判别法判断, -1是模17的二次剩余, 从而第二个同余方程有2个解, 可以检查分别是$x \equiv 4 \bmod 17, x \equiv 13 \bmod 17$), 把它们组合在一起就构成4个同余方程:

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 4 \bmod 17 \end{cases} \qquad \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 13 \bmod 17 \end{cases}$$

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 4 \bmod 17 \end{cases} \qquad \begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 13 \bmod 17 \end{cases}$$

它们每个都有一个解，所以原来的同余方程(1)有4个解.

示例：
判断同余方程$x^2 \equiv -63 \bmod 187$的解数.
类似上例，可以判断与之等价的同余方程组:

$$\begin{cases} x^2 \equiv -63 \bmod 11 \\ x^2 \equiv -63 \bmod 17 \end{cases}$$

这个同余方程组等价于:

$$\begin{cases} x^2 \equiv 3 \bmod 11 \\ x^2 \equiv 5 \bmod 17 \end{cases} \qquad (2)$$

检查

$$\{1, 2, 3, 4, 5, 6, 7, 8\}$$

中的每个的数平方都不与5同余, 所以$x^2 \equiv 5 \bmod 17$无解, 从而原同余方程无解.
也可以通过计算

$$5^{\frac{17-1}{2}} \equiv 5^8 \equiv (5^2)^4 \equiv 8^4 \equiv (8^2)^2 \equiv (-4)^2 \equiv -1 \bmod 17$$

来判断$x^2 \equiv 5 \bmod 17$无解.

定理

设p是奇素数，$(a_1,p)=1,(a_2,p)=1$，则：

- 如果a_1,a_2都是模p的二次剩余，则a_1a_2也是.
- 如果a_1,a_2都是模p的二次非剩余，则a_1a_2是模p的二次剩余
- 如果a_1,a_2一个是模p的二次剩余，一个是模p的二次非剩余，则a_1a_2是模p的二次非剩余.

这是因为

$$(a_1a_2)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}\equiv 1 \bmod p,$$

如果a_1,a_2都是模p的二次剩余，或者都是二次非剩余，以及

$$(a_1a_2)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}a_2^{\frac{p-1}{2}}\equiv -1 \bmod p,$$

如果a_1,a_2一个是模p的二次剩余，一个是模p的二次非剩余.

2. 勒让德(Legendre)符号

设p是素数，定义Legendre符号如下：

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

例如

$$0^2 \equiv 0 \bmod 5, 1^2 \equiv 1 \bmod 5, 2^2 \equiv 4 \bmod 5, 3^2 \equiv 4 \bmod 5, 4^2 \equiv 1 \bmod 5$$

由此

$$\left(\frac{1}{5}\right) = 1, \left(\frac{4}{5}\right) = 1, \left(\frac{2}{5}\right) = -1, \left(\frac{3}{5}\right) = -1, \left(\frac{5}{5}\right) = 0$$

$\left(\frac{a}{p}\right) = 1 \iff a$是模$p$的二次剩余;

$\left(\frac{a}{p}\right) = -1 \iff a$是模$p$的二次非剩余.

根据二次剩余的欧拉判别条件, 如果p是奇数, $a \in \mathbb{Z}$, 则:

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

由此我们可以计算勒让德符号, 例如:

$$\because 2^{\frac{17-1}{2}} \equiv 1 \mod 17 \quad \therefore \left(\frac{2}{17}\right) = 1$$

即2是模17的二次剩余

$$\because 3^{\frac{17-1}{2}} \equiv -1 \mod 17 \quad \therefore \left(\frac{3}{17}\right) = -1$$

即3是模17的二次非剩余

设p是奇素数:

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

对于奇素数p, 可能的情况有两种:

$$p \equiv 1 \bmod 4, \qquad p \equiv 3 \bmod 4$$

对于前者, 有$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$, 从而

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

对于后者, 有$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1$ 从而

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

从而

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

设p是奇素数.

- $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$
  这是因为下面的两个同余式等价(一个的解也是另外一个的解)
  $$x^2 \equiv a + p \bmod p \iff x^2 \equiv a \bmod p$$
  即a是模p的二次剩余当且仅当$a+p$是模p的二次剩余. 一般地, $\left(\frac{a+kp}{p}\right) = \left(\frac{a}{p}\right)$.
- $a \equiv b \bmod p \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
  这是因为
  $$a = kp + b \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{kp+b}{p}\right) = \left(\frac{b}{p}\right).$$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
  这是因为
  $$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \mod p$$
- $(a,p) = 1 \Longrightarrow \left(\frac{a^2}{p}\right) = 1$
  由上一条即得. 另外, 如果$p \mid a$, 则$\left(\frac{a^2}{p}\right) = 0$.

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

以$r_1, r_2, \ldots, r_m$表示所有那些模p后大于$\frac{p}{2}$的数．以$s_1, s_2, \ldots, s_k$表示所有那些模p后小于$\frac{p}{2}$的数的数．这样，我们有$k+m=\frac{p-1}{2}$,即:

$$\frac{p}{2}<r_i<p, \quad 1\leq s_j<\frac{p}{2}.$$

进一步，我们还有

$$1\leq p-r_i<\frac{p}{2},$$

也即

$$1\leq p-r_1, p-r_2, \ldots, p-r_m<\frac{p}{2}.$$

我们知道
$$s_j \not\equiv p - r_i \bmod p,$$
其中$j=1,2,\ldots,k, i=1,2,\ldots,m$. 否则, 存在整数$q_i$和$q_j$, 满足$1\le q_i, q_j \le \frac{p-1}{2}$, 使得$s_j = aq_j$, $r_i = aq_i$, 并且
$$aq_j = p - aq_i, \quad 即 \quad aq_j + aq_i \equiv 0 \bmod p.$$
于是, $q_i + q_j \equiv 0 \bmod p$, 但是$2 \le q_i + q_j \le \frac{p-1}{2} + \frac{p-1}{2} < p$, 矛盾.
这表明,
$$s_1, s_2, \ldots, s_k, p - r_1, p - r_2, \ldots, p - r_m$$
这$\frac{p-1}{2}$个数恰好是$1,2,3,\ldots,\frac{p-1}{2}$的一个置换, 从而
$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv 1a \cdot 2a \cdot \cdots \cdot \frac{p-1}{2}a \equiv s_1 s_2 \ldots s_k r_1 r_2 \ldots r_m$$
$$\equiv (-1)^m s_1 s_2 \ldots s_k (p-r_1)(p-r_2)\ldots(p-r_m) \equiv (-1)^m 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \bmod p$$
即得
$$\left(\frac{a}{p}\right) = (-1)^m$$

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

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

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$a=2, 1\le j\le \frac{p-1}{2}$时，有$2\le 2j\le p-1$，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

$$T \equiv m \bmod 2$$

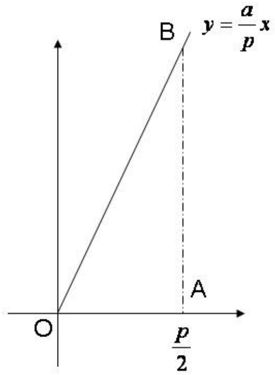
即

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

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.

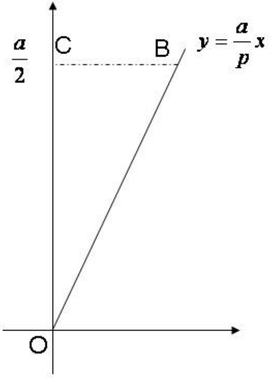


整数

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

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

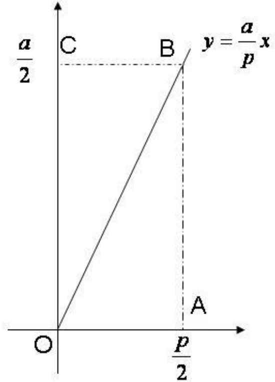


整数

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

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S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.