1.6 二次剩余（讲述模p（奇素数）的二次剩余）

一.勒让德（Lengedre）符号

根据定义 对于$(a,p)=1$，a是模p的二次剩余，是指存在整数b，使得：$a\equiv b^2 \pmod p$，换句话说，$\alpha=\bar{a}$是$\mathbb{Z}_p^*$中的平方元素（$\alpha=\beta^2$，其中$\beta=\bar{b}\neq 0$），否则a叫做模p的二次非剩余.

Thm 1. 设p是奇素数，g是模p的一个原根，则

1）模p的二次剩余共有$\frac{p-1}{2}$个，它们（在模p的意义下）是

$$\{g^{2i}: 0\le i\le \frac{p-3}{2}\}$$

模p的二次非剩余也共有$\frac{p-1}{2}$个，它们是$\{g^{2i+1}: 0\le i\le \frac{p-3}{2}\}$

2）模p的两个二次剩余相乘是二次剩余，二次剩余和二次非剩余相乘是二次非剩余，两个二次非剩余相乘是二次剩余.

证：在Th 5.14中，取$k=2$，$\varphi(p)=p-1$，则$d=(2,p-1)=2$

因此a是模p的二次剩余当且仅当$2\mid \mathrm{ind}_g(a)$，即$\mathrm{ind}_g(a)$为偶数，所以a是模p的二次非剩余当且仅当$\mathrm{ind}_g(a)$为奇数.

从而⑴⑵成立.

def. 对于奇素数p和$a\in\mathbb{Z}$，定义Lengedre符号为：

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

采用Lengedre符号，则Thm 6.1的⑵可以表示成：

当$a,b\in\mathbb{Z}$，$p\nmid ab$时，$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

事实上，此式在$p\mid ab$时也成立.（因为等式两边均为0）

引理6.2 1）对 $\forall a,b\in\mathbb{Z}$，$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

2）若 $a\equiv b \pmod p$，则 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

3）同余方程 $x^2\equiv a \pmod p$ 的模 p 解数为 $1+\left(\frac{a}{p}\right)$

证：只需证3）

以 N 表示 $x^2\equiv a \pmod p$ 模 p 解的个数

若 a 是模 p 的二次剩余，则 $N=2$ $\left(\frac{a}{p}\right)=1$

若 a 是模 p 的二次非剩余，则 $N=0$ $\left(\frac{a}{p}\right)=-1$

若 $p\mid a$，则 $N=1$ $\left(\frac{a}{p}\right)=0$

所以 $N=1+\left(\frac{a}{p}\right)$ 均成立

Thm 6.3 Euler判别法则

设 p 为奇素数，则对每一个整数 a，$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p$

证：当 $p\mid a$ 时，$\left(\frac{a}{p}\right)=0\equiv a^{\frac{p-1}{2}} \pmod p$

当 $p\nmid a$ 时，

①若 a 是模 p 的二次剩余，则 $a\equiv g^{2i} \pmod p$，

其中 g 是模 p 的原根，于是 $\left(\frac{a}{p}\right)=1$，而

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

②若 a 是模 p 的二次非剩余，则 $a\equiv g^{2i+1} \pmod p$

从而 $\left(\frac{a}{p}\right)=-1$，而 $a^{\frac{p-1}{2}}\equiv g^{(p-1)i}\equiv 1\cdot(-1)\equiv -1 \pmod p$

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

推论6.4 设 p 为奇素数，则

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

证：$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \pmod p$ 同余式两边取值为 ±1，而 $p\geq 3$

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

引理6.5 Gauss引理

设p为奇素数，$(a,p)=1$，记$r=\frac{p-1}{2}$，令μ是$a, 2a, \cdots, ra$当中模p的最小正剩余大于$\frac{p}{2}$的个数，则$\left(\frac{a}{p}\right)=(-1)^{\mu}$

证：设$a, 2a, \cdots, ra$被p除的余数中小于$\frac{p}{2}$的为$b_1, b_2, \cdots, b_\lambda$，大于$\frac{p}{2}$的为$c_1, c_2, \cdots, c_\mu$，于是$\lambda+\mu=r$，且

$$1\le b_i \le \frac{p-1}{2} \ (1\le i\le \lambda), \ \frac{p+1}{2}\le c_j \le p-1 \ (1\le j\le \mu)$$

由于$a, 2a, \cdots, ra$模p彼此不同余，从而$p-c_j \ (1\le i\le \mu)$也两两不同，并且$1\le p-c_j\le\frac{p-1}{2} \ (1\le j\le\mu)$，进而每一个$p-c_j$和$b_i$也彼此不同，因为$c_j\equiv xa$，$b_i\equiv ya \pmod p$

其中$x, y\in\mathbb{Z}$，$1\le x, y\le r\le\frac{p-1}{2}$，如果$p-c_j\equiv b_i \pmod p$

则$(x+y)a\equiv 0 \pmod p$ 但$1\le x+y\le p-1$，$(a,p)=1$

故$(x+y)a\equiv 0 \pmod p$ 不可能成立

这表明$\lambda+\mu=r$个整数$b_1, b_2, \cdots, b_\lambda, p-c_1, p-c_2, \cdots, p-c_\mu$两两不同，并且均在$1, 2, \cdots, r$之中，从而它们就是$1, 2, \cdots, r$.

于是 $r! = b_1 b_2\cdots b_\lambda (p-c_1)\cdots(p-c_\mu)$

模p之后成为 $r! \equiv (-1)^{\mu} b_1 b_2\cdots b_\lambda c_1 c_2\cdots c_\mu \pmod p$

$$\equiv (-1)^{\mu} a\cdot 2a\cdot\cdots\cdot(ra) \pmod p$$

$$\equiv (-1)^{\mu} a^r\cdot r! \pmod p$$

$$\therefore \left(\frac{a}{p}\right)\equiv a^r\equiv(-1)^{\mu} \pmod p$$

因此$\left(\frac{a}{p}\right)=(-1)^{\mu}$

可以用Gauss引理来计算$\left(\frac{-1}{p}\right)$，取$a=-1$，则$\{a, 2a, \cdots, ra\}=\{-1, -2, \cdots, -r\}$其中$r=\frac{p-1}{2}$，它们被$p$除的余数$p-1, p-2, \cdots, p-r=\frac{p+1}{2}$，均大于$\frac{p}{2}$，于是$\mu=r$，即$\left(\frac{-1}{p}\right)=(-1)^r=(-1)^{\frac{p-1}{2}}$

推论6.6 设p为奇素数，则

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

证：当$a=2$时，$2,4,\cdots,2r=p-1$均小于p

则Gauss引理中的μ是满足$\frac{p+1}{2}\le 2i\le p-1$的整数$i$的个数.

当$p=8m+1$时，满足$4m+1\le 2i\le 8m$的整数i为$2m+1,2m+2,\cdots,4m$.

即$\mu=2m$，从而$\left(\frac{2}{p}\right)=(-1)^{\mu}=1$

当$p=8m+3$时，满足$4m+2\le 2i\le 8m+2$的i为$2m+1,2m+2,\cdots,4m+1$

即$\mu=2m+1$，从而$\left(\frac{2}{p}\right)=(-1)^{\mu}=-1$

类似可证：$p=8m+5$和$p=8m+7$时，$\left(\frac{2}{p}\right)$分别为-1和1

例1. 证明形如$4m+1$的素数有无穷多个.

证：首先，这样的素数存在，如$p=5, 29\cdots\cdots$

接着，假设这样的素数只有有限多个，它们是$p_1,p_2,\cdots,p_s\ (s\ge1)$.

考虑正整数$n=4(p_1p_2\cdots p_s)^2+1$

由于n是大于2的奇数，则n必有素因子p，且$p\ge3$，于是

$$0\equiv n=4(p_1p_2\cdots p_s)^2+1 \pmod p$$

即$(2p_1p_2\cdots p_s)^2\equiv-1 \pmod p$

从而$\left(\frac{-1}{p}\right)=1$，即$p\equiv1 \pmod 4$

但$p\mid n$，p不能为$p_1,p_2,\cdots,p_s$，于是p为求的形如$4m+1$的素数.

因而假设不成立，也即形如$4m+1$的素数有无穷多个.

例 2. 设p为奇素数，$(a,p)=1$，则

1) $\sum_{x=0}^{p-1}\left(\frac{x^2+ax}{p}\right)=-1$

2) $\sum_{x=0}^{p-1}\left(\frac{x^2+a}{p}\right)=-1$

证明：1) 证法一

$$\sum_{x=0}^{p-1}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x^2}{p}\right)\left(\frac{1+ax^{-1}}{p}\right)$$

$$=\sum_{x=1}^{p-1}\left(\frac{1+ax^{-1}}{p}\right)$$

$$=\sum_{y=1}^{p-1}\left(\frac{1+y}{p}\right)$$ （当x遍历模p缩系时，$y=ax^{-1}$也如此）

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

$$=\sum_{\delta=1}^{p-1}\left(\frac{\delta}{p}\right)-\left(\frac{1}{p}\right)=0-1=-1$$

$\sum_{\delta=1}^{p-1}\left(\frac{\delta}{p}\right)=0$是因为左边和式中1和$-1$各有$\frac{p-1}{2}$个.

证法2

当x遍历模p缩系时，ax也如此，所以

$$\sum_{x=0}^{p-1}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{(ax)^2+a(ax)}{p}\right)$$

$$=\sum_{x=1}^{p-1}\left(\frac{a^2(x^2+x)}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x^2+x}{p}\right)$$

这表明$\sum_{x=0}^{p-1}\left(\frac{x^2+ax}{p}\right)$与$a$无关$((a,p)=1)$，记为$A$

$$\text{于是 } (p-1)A=\sum_{a=1}^{p-1}\sum_{x=1}^{p-1}\left(\frac{x^2+ax}{p}\right)=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{a=1}^{p-1}\left(\frac{x+a}{p}\right)$$

$$=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left[\sum_{a=0}^{p-1}\left(\frac{x+a}{p}\right)-\left(\frac{x}{p}\right)\right]$$

$$=\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\left(0-\left(\frac{x}{p}\right)\right)$$

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

从而$A=-1$

2) $\sum_{x=0}^{p-1}\left(1+\left(\frac{x^2+a}{p}\right)\right)$ 等于二元二次同余方程 $y^2\equiv x^2+a \pmod p$ 的模p解的个数。这里 $(x,y)=(\alpha,\beta)$ 和 (α',β') 是模p同一个解是指 $\alpha\equiv\alpha'$ 且 $\beta\equiv\beta' \pmod p$)，此同余方程可写为

$(y+x)(y-x)\equiv a \pmod p$，对每个 $b\not\equiv 0 \pmod p$，令 $y+x\equiv b \pmod p$，

则 $y-x\equiv ab^{-1} \pmod p$

从而给出同余方程的一个解 $y\equiv\frac{1}{2}(b+ab^{-1})$，$x\equiv\frac{1}{2}(b-ab^{-1}) \pmod p$

易知b和解是一一对应的，于是同余方程模p解数为 $p-1$，

即 $p-1=\sum_{x=0}^{p-1}\left(1+\left(\frac{x^2+a}{p}\right)\right)=\sum_{x=0}^{p-1}1+\sum_{x=0}^{p-1}\left(\frac{x^2+a}{p}\right)=p+\sum_{x=0}^{p-1}\left(\frac{x^2+a}{p}\right)$

$\therefore \sum_{x=0}^{p-1}\left(\frac{x^2+a}{p}\right)=-1$

二、平方和问题

Thm 6.7 (Euler-Gauss) 对于素数 $p\equiv 1 \pmod 4$，存在整数A和B，使得 $p=A^2+B^2$.

证：取模p的一个原根g，如下定义一个函数：对 $a\in\mathbb{Z}$.

$$\chi(a)=\begin{cases} i^{\mathrm{ind}_g(a)}, & 若\ p\nmid a \\ 0, & 若\ p\mid a \end{cases}$$

这里 $i=\sqrt{-1}\in\mathbb{C}$，由指数 $\mathrm{ind}_g(a)$ 的性质可知：

1) $a\equiv b \pmod p$ 时，$\chi(a)=\chi(b)$，即 $\chi(a)$ 是模p同余类的函数.

2) $\chi(ab)=\chi(a)\chi(b)$

当 $p\mid ab$ 时，两端均为0；

当 $p\nmid ab$ 时，$\mathrm{ind}(ab)\equiv\mathrm{ind}(a)+\mathrm{ind}(b) \pmod{p-1}$

由 $p\equiv 1 \pmod 4$ 知 $\mathrm{ind}(ab)\equiv\mathrm{ind}(a)+\mathrm{ind}(b) \pmod 4$

而 $i^4=1$，所以 $\chi(ab)=i^{\mathrm{ind}(ab)}=i^{\mathrm{ind}(a)+\mathrm{ind}(b)}=\chi(a)\chi(b)$

3) $\chi(a)^2=\left(\frac{a}{p}\right)$

当 $p\mid a$ 时，两端均为 0.

当 $p\nmid a$ 时，$\chi(a)^2=(-1)^{ind(a)}=\begin{cases}1, & 若ind(a)为偶数\\ -1, & 若ind(a)为奇数\end{cases}=\left(\frac{a}{p}\right)$

4) $\sum_{w=0}^{p-1}\chi(w)=0$

因为 $\exists a$，使得 $\chi(a)\neq 0$，则 $\chi(a)\sum_{w=0}^{p-1}\chi(w)=$

$\sum_{w=0}^{p-1}\chi(a)\chi(w)=\sum_{w=0}^{p-1}\chi(aw)=\sum_{w=0}^{p-1}\chi(w)$

因此 $\sum_{w=0}^{p-1}\chi(w)=0$

现考虑复数 $\alpha=\sum_{x=0}^{p-1}\chi(x)\chi(1-x)\in\mathbb{C}$，该复数有形式 $A+Bi$.

其中 $A,B\in\mathbb{Z}$，下面证明复数 α 的绝对值平方 $\alpha\bar{\alpha}$ 等于 p，于是得到所希望的结果 $A^2+B^2=p$.

由 2) 知，当 $(a,p)=1$ 时，

$$\overline{\chi(a)}=i^{-ind(a)}=i^{ind(a^{-1})}=\chi(a^{-1})$$

所以 $\alpha\bar{\alpha}=\sum_{x,y=2}^{p-1}\chi(x)\chi(1-x)\overline{\chi(y)}\,\overline{\chi(1-y)}$

$$=\sum_{x,y=2}^{p-1}\chi\left(\frac{x}{y}\right)\chi\left(\frac{1-x}{1-y}\right)$$

$$=\sum_{\substack{x,y=2\\x=y}}^{p-1}\chi(1)\chi(1)+\sum_{\substack{x,y=2\\x\neq y}}^{p-1}\chi\left(\frac{x}{y}\right)\chi\left(\frac{1-x}{1-y}\right)$$

$$=p-2+\sum_{y,\delta=2}^{p-1}\chi(\delta)\chi\left(\frac{1-\delta y}{1-y}\right)\quad 令\ \left(\delta=\frac{x}{y}\right)$$

$$=p-2+\sum_{\delta=2}^{p-1}\chi(\delta)\sum_{y=2}^{p-1}\chi\left(\frac{1-\delta y}{1-y}\right)$$

令 $w=\frac{1-\delta y}{1-y}$，则 $y=\frac{w-1}{w-\delta}$，当 y 遍历 $2,3,\cdots,p-1$ 时，w 遍历

$\{0,1,2,\cdots,p-1\}$ 中除去 1 和 δ 以外的元素. 所以

$$\alpha\bar{\alpha}=p-2+\sum_{\delta=2}^{p-1}\chi(\delta)\sum_{\substack{w=0\\ w\neq 1,\delta}}^{p-1}\chi(w)$$

$$=p-2+\sum_{\delta=2}^{p-1}\chi(\delta)(-\chi(1)-\chi(\delta))$$

$$=p-2-\sum_{\delta=2}^{p-1}\chi(\delta)-\sum_{\delta=2}^{p-1}\chi^2(\delta)$$

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

$$=p-2+1+1=p$$

这就证明了$A^2+B^2=\alpha\bar{\alpha}=p$.

$i=\sqrt{-1}$，Gauss研究：哪些正整数n可以表示成两个整数的平方和，即方程$x^2+y^2=n$有整数解(x,y)，Gauss将方程写成$(x+iy)(x-iy)=n$，即$\alpha\bar{\alpha}=n$，$(\alpha=x+iy)$. 从而研究$x^2+y^2=n$的整数解可以考虑集合$R=\{a+bi:a,b\in\mathbb{Z}\}^*$，该集合对于通常的加、减、乘运算成环，称作高斯整数环，每个$a+bi$ $(a,b\in\mathbb{Z})$叫做Gauss整数，由$(*)$可知：$x^2+y^2=n$有整数解当且仅当n是某个Gauss整数α的绝对值的平方.

因此：

Lemma 6.8 设正整数n和m都是两个整数的平方和，则mn也是两个整数的平方和.

证：由假设知$n=\alpha\bar{\alpha}$，$m=\beta\bar{\beta}$，其中α和β是Gauss整数

于是$nm=\alpha\bar{\alpha}\beta\bar{\beta}=(\alpha\beta)\overline{\alpha\beta}$，所以$mn$为两个整数的平方和.

由Lemma 6.8可知，将$n=p_1p_2\cdots p_s$表成素数乘积，如果每个p_i均是两整数平方和，则n也是整数平方和. 但是反命题不成立，例如：$18=3^2+3^2$，18的素因子3不是二整数平方和. 为了叙述Gauss关于二整数平方和的完整结论，我们引入以下符号：

1) 对每个正整数n和素数p，用$p^e \| n$表示$p^e | n$但$p^{e+1} \nmid n$.
从而e即n的标准分解式中p的指数 $(e \geq 0)$

2) n可唯一表示成$n = m^2 n'$，其中n'是无平方因子的整数，即$n' = 1$或为不同素数之积，叫做n的无平方因子部分.

定理6.9 (Gauss) 对于正整数n，以n'表示n的无平方因子部分，则下列三者等价.

1) n是两个整数的平方和

2) n'没有素因子$p \equiv 3 \pmod 4$

3) 对每个素数$p \equiv 3 \pmod 4$，$p^e \| n$，则e必为偶数.

证：易知(2)，(3)等价.

"(1) ⇒ (3)"

设$n = A^2 + B^2$，$(A, B \in \mathbb{Z})$ 若$p \equiv 3 \pmod 4$是n的素因子$p^e \| n$，则$e \geq 1$. 于是$A^2 + B^2 = n \equiv 0 \pmod p$

即$A^2 \equiv -B^2 \pmod p$，如果$B \not\equiv 0 \pmod p$，则

$A \not\equiv 0 \pmod p$ 且$\left(\frac{A}{B}\right)^2 \equiv -1 \pmod p$

所以$\left(\frac{-1}{p}\right) = 1$，但这与$p \equiv 3 \pmod 4$矛盾，于是$B \equiv 0 \equiv A \pmod p$

令$A = pA'$，$B = pB'$，则$A', B' \in \mathbb{Z}$，而$n = A^2 + B^2 = p^2(A'^2 + B'^2)$

从而$p^2 | n$ $(e \geq 2)$ 并且$n_0 = A'^2 + B'^2$

以上证明了：若$p | n$，则$p^2 | n$，且$n_0 = \frac{n}{p^2}$ 也是二整数平方和.

如果又有$p | n_0$，则有$p^2 | n_0$ (即若$p^3 | n$，则$p^4 | n$)

由此可知：对每个素数$p \equiv 3 \pmod 4$，$p^e \| n$的e必是偶数

"(2) ⇒ (1)"

由2) 知$n = m^2 n'$，n'的素因子为2或$p \equiv 1 \pmod 4$

素数$p \equiv 1 \pmod 4$均是二整数平方和 (Thm 6.7).

而$2 = 1^2 + 1^2$，从而n'是二整数平方和 (引理6.8)

$\therefore n = m^2 n'$也是二整数平方和.

三、二次互反律

Thm 6.10 设p和q是不同的奇素数，则

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

$$=\begin{cases}1, & 若\ p\equiv 1 \pmod 4\ 或\ q\equiv 1 \pmod 4\\ -1, & 若\ p\equiv q\equiv 3 \pmod 4\end{cases}$$

换句话说，当$p\equiv q\equiv 3 \pmod 4$时，$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$，否则$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$

例1 同余方程$x^2\equiv 219 \pmod{383}$是否有解.

383是素数，$219=3\times 73$

$$\left(\frac{219}{383}\right)=\left(\frac{3}{383}\right)\left(\frac{73}{383}\right)=-\left(\frac{383}{3}\right)\left(\frac{383}{73}\right) \quad (二次互反律)$$

$$=-\left(\frac{2}{3}\right)\left(\frac{18}{73}\right) \quad (383\equiv 2 \pmod 3 \quad 383\equiv 18 \pmod{73})$$

$$=-\left(\frac{2}{3}\right)\left(\frac{2}{73}\right) \quad \left(\left(\frac{9}{73}\right)=\left(\frac{3}{73}\right)^2=1\right)$$

$$=-(-1)\cdot 1=1$$

从而$x^2\equiv 219 \pmod{383}$有整数解.

例2 决定$\left(\frac{-3}{p}\right)=-1$的全部奇素数$p$.

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

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

$$\therefore \left(\frac{-3}{p}\right)=-1 \Leftrightarrow \left(\frac{p}{3}\right)=-1 \Leftrightarrow p\equiv 2 \pmod 3$$

例7 决定所有素数 p，使6为模 p 的二次剩余

解：$\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}}\left(\frac{p}{3}\right)$

$\because (-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}}=\begin{cases}1, & 若 p\equiv 1,3 \pmod 8\\ -1, & 若 p\equiv 5,7 \pmod 8\end{cases}$

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

$\therefore \left(\frac{6}{p}\right)=1 \Leftrightarrow \begin{cases}p\equiv 1,3 \pmod 8\\ p\equiv 1 \pmod 3\end{cases}$ 或 $\begin{cases}p\equiv 5,7 \pmod 8\\ p\equiv 2 \pmod 3\end{cases}$

$\Leftrightarrow p\equiv 1,19,23,5 \pmod{24}$ （中国剩余定理）