## 5.2. The Legendre Symbol

我們已經把解一般的二次 congruence equation 一步一步的化簡到解 $x^2 \equiv a \pmod{p}$, 其中 $p$ 為奇質數且 $p \nmid a$ 的情形. 本節我們將探討何時 $x^2 \equiv a \pmod{p}$ 有解. 至於若有解如何找解, 我們留待下一章學習更多方法後再處理.

由於我們只關注 $x^2 \equiv a \pmod{p}$ 何時有解, 何時無解, 我們介紹一個符號稱 (Legendre symbol) 來表示其有解或無解.

**Definition 5.2.1.** 給定奇質數 $p$ 以及 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 若 $x^2 \equiv a \pmod{p}$ 有解, 我們稱 $a$ 是一個 *quadratic residue* modulo $p$ 並以 $\left(\frac{a}{p}\right) = 1$ 表示之. 反之, 若 $x^2 \equiv a \pmod{p}$ 無解, 我們稱 $a$ 是一個 *quadratic nonresidue* modulo $p$ 並以 $\left(\frac{a}{p}\right) = -1$ 表示之.

首先要注意的是 Legendre symbol 不要和分數搞混. 在本講義中的分數如三分之二的平方我們會用 $(\frac{2}{3})^2$ 或 $(2/3)^2$ 這兩種方法表示, 括號比較小. 而 Legendre symbol $\left(\frac{2}{3}\right)$ 的括號比較大. 另外依定義 Legendre symbol 的分母一定是一個奇質數且分子一定和分母互質 (有的書規定不同, 這裡為了不讓同學搞混我們嚴格如此規定). 例如在本講義中 $\left(\frac{5}{6}\right)$ 或 $\left(\frac{6}{3}\right)$ 這樣的符號是沒意義的.

接下來我們來看 Legendre symbol 直接依定義所得之性質.

**Lemma 5.2.2.** 假設 $p$ 是一個奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$.

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

(2) 若 $b \in \mathbb{Z}$ 滿足 $b \equiv a \pmod{p}$, 則 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

**Proof.** (1) 要判斷 $a^2$ 是否為 quadratic residue modulo $p$, 也就是要判斷 $x^2 \equiv a^2 \pmod{p}$ 是否有解. 然而很容易知道 $x = a$ 是 $x^2 \equiv a^2 \pmod{p}$ 的解, 故知 $\left(\frac{a^2}{p}\right) = 1$.

(2) 要判斷 $b$ 是否為 quadratic residue modulo $p$, 也就是要判斷 $x^2 \equiv b \pmod{p}$ 是否有解. 然而依假設 $b \equiv a \pmod{p}$ 故要解 $x^2 \equiv b \pmod{p}$ 就等同於解 $x^2 \equiv a \pmod{p}$. 故知 $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$. □

其實 $x^2 \equiv a \pmod{p}$ 要不然有解要不然就無解. 所以若僅將 Legendre symbol 看成只是一個符號表示有解無解就太小看它了. 若要定符號, 我們也可以將有解定為 1 無解定為 0, 或其他相異的兩個數, 為何要將有解定為 1；無解定為 $-1$ 呢? 說實話若僅想用兩個數字來表示有解或無解的情況, 那真的是怎麼定值都可以, 然而如此一來這樣的符號頂多僅讓我們方便表達有解或無解的情況, 沒有什麼太大的意義. Legendre symbol 之所以要將有解定為 1 無解定為 $-1$, 主要是我們可以將它們看成整數的 1 和 $-1$ 來做乘法運算. 其原因就是下面這一個定理.

**Theorem 5.2.3** (Euler's Criterion)**.** 假設 $p$ 是一個奇質數且 $a\in\mathbb{Z}$ 滿足 $p\nmid a$.

(1) 若 $x^2\equiv a \pmod p$ 有解, 則 $a^{(p-1)/2}\equiv 1 \pmod p$.

(2) 若 $x^2\equiv a \pmod p$ 無解, 則 $a^{(p-1)/2}\equiv -1 \pmod p$.

**Proof.** (1) 若 $x^2\equiv a \pmod p$ 有解且 $x=c$ 為其一解, 即 $c^2\equiv a \pmod p$. 此時

$$a^{\frac{p-1}{2}}\equiv (c^2)^{\frac{p-1}{2}}\equiv c^{p-1} \pmod p.$$

由於 $a$ 和 $p$ 互質, 所以 $x^2\equiv a \pmod p$ 之解 $c$ 亦與 $p$ 互質. 因此利用 Fermat's Little Theorem (3.3.4) 知 $c^{p-1}\equiv 1 \pmod p$, 故得證 $a^{(p-1)/2}\equiv 1 \pmod p$.

(2) 考慮 $S=\{1,2,\dots,p-1\}$ 這一個 reduced residue system modulo $p$. 對任意 $k\in S$, 由於 $k$ 和 $p$ 互質, 故由 Theorem 4.3.4 知 $kx\equiv a \pmod p$ 在 modulo $p$ 之下有唯一解. 由於 $a$ 和 $p$ 互質, 故知其解必也與 $p$ 互質. 換句話說, 給定 $k\in S$ 必存在唯一的 $k'\in S$ 滿足 $kk'\equiv a \pmod p$. 要注意此時 $k'\neq k$, 否則會得到 $k^2\equiv a \pmod p$, 此與 $x^2\equiv a \pmod p$ 無解的假設相矛盾. 另一方面也要注意因為 $k'x\equiv a \pmod p$ 在 modulo $p$ 之下其解唯一且已知 $x=k$ 為其一解, 所以不可能找到另一個 $\ell\in S$ 使得 $k'\ell\equiv a \pmod p$. 因此對於 $S$ 中的元素, 我們可以將之兩兩配對, 也就是對任意 $k\in S$ 將 $k$ 和滿足 $kk'\equiv a \pmod p$ 唯一的 $k'\in S$ 相配對. 如此一來我們共有 $(p-1)/2$ 對. 由於每一對相乘在 modulo $p$ 之下和 $a$ congruent, 故可得

$$(p-1)!=1\cdot 2\cdots p-1\equiv a^{\frac{p-1}{2}} \pmod p.$$

不過 Wilson's Theorem (3.4.3) 告訴我們 $(p-1)!\equiv -1 \pmod p$, 故得證 $a^{(p-1)/2}\equiv -1 \pmod p$. □

如果大家不健忘的話, 當初在證明 Wilson's Theorem 我們是將 $S=\{1,\dots,p-1\}$ 中之元素依 $kk'\equiv 1 \pmod p$ 來配對. 所以 Wilson's Theorem 和 Euler's Criterion 的證明有異曲同工之妙.

當 $p\nmid a$ 時 $a^{(p-1)/2}$ 在 modulo $p$ 之下之值不是 1 就是 $-1$. 這是因為若令 $b=a^{(p-1)/2}$, 則 $b^2=a^{p-1}\equiv 1 \pmod p$, 也就是說 $x=b$ 為 $x^2\equiv 1 \pmod p$ 之一根. 因此由 Lemma 3.4.2 知 $b\equiv\pm 1 \pmod p$. 不過因為 $p$ 是奇質數, 不可能有 $1\equiv -1 \pmod p$ 的情況發生, 所以 Theorem 5.2.3 也告訴我們可以由 $a^{(p-1)/2}$ modulo $p$ 為 1 或 $-1$ 來判斷 $x^2\equiv a \pmod p$ 是否有解. 也就是說若 $a^{(p-1)/2}\equiv 1 \pmod p$, 則 $\left(\frac{a}{p}\right)=1$; 而若 $a^{(p-1)/2}\equiv -1 \pmod p$, 則 $\left(\frac{a}{p}\right)=-1$. 這就是 Legendre symbol 取 1 和 $-1$ 為值的理由. 我們有以下之結論.

**Corollary 5.2.4.** 假設 $p$ 是一個奇質數且 $a\in\mathbb{Z}$ 滿足 $p\nmid a$. 則

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

所以今後我們要知道 $x^2\equiv a \pmod p$ 有解或無解, 只要去算 $a^{(p-1)/2}$ 除以 $p$ 的餘數是 1 或 $p-1$. 若餘數是 1 則有解, 若餘數是 $p-1$ 則無解. 不過這個方法在實際狀況下仍很費事, 因為要計算 $a^{(p-1)/2}$ 一般來說當 $p$ 很大時仍很很麻煩. 不過這個 criterion 在證明一般抽象的定理時就很管用了. 我們有以下有關 Legendre symbol 的重要性質.

**Proposition 5.2.5.** 假設 $p$ 是一個奇質數且 $a,b\in\mathbb{Z}$ 滿足 $p\nmid a$ 且 $p\nmid b$. 則

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

**Proof.** 由 Corollary 5.2.4 知

$$\left(\frac{ab}{p}\right)\equiv(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\pmod{p}.$$

由於 $\left(\frac{ab}{p}\right)$ 和 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ 之值要不是 1 就是 $-1$, 所以他們在 modulo $p$ 之下同餘表示必相等 (否則又會得 $p|2$ 之矛盾). 故得 $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Proposition 5.2.5 可以推出很令人吃驚的結果. 例如假設 $x^2\equiv a\pmod{a}$ 和 $x^2\equiv b\pmod{p}$ 皆有解且設 $x=c$ 和 $x=c'$ 分別為其一解. 那麼我們很容易推得 $x^2\equiv ab\pmod{p}$ 必有解. 因為 $x=cc'$ 就是其中之一解; 而若 $x^2\equiv a\pmod{a}$ 和 $x^2\equiv b\pmod{p}$ 其中有一個無解或是皆無解, 要利用解方程式的方法來探討 $x^2\equiv ab\pmod{p}$ 是否有解推論起來就比較麻煩. 不過若利用 Proposition 5.2.5, 我們很快的便知若 $x^2\equiv a\pmod{p}$ 有解但 $x^2\equiv b\pmod{p}$ 無解 (即 $\left(\frac{a}{p}\right)=1$, $\left(\frac{b}{p}\right)=-1$), 則 $x^2\equiv ab\pmod{p}$ 便無解 (因為此時 $\left(\frac{ab}{p}\right)=1\times(-1)=-1$). 更令人訝異的是若 $x^2\equiv a\pmod{p}$ 和 $x^2\equiv b\pmod{p}$ 皆無解, 我們可以知 $x^2\equiv ab\pmod{p}$ 必有解 (因為此時 $\left(\frac{ab}{p}\right)=(-1)\times(-1)=1$). 這個結果是很難用有解無解這樣的角度來判斷的.

Proposition 5.2.5 另一個好處是對任意整數 $a$ 我們可以分解成 $a=(-1)^m2^{n_0}q_1^{n_1}\cdots q_r^{n_r}$, 其中 $q_i$ 為奇質數 (且 $p\neq q_i$ 因 $p\nmid a$), $m\in\{0,1\}$, $n_i\geq 0$. 因此可得

$$\left(\frac{a}{p}\right)=\left(\frac{-1}{p}\right)^m\left(\frac{2}{p}\right)^{n_0}\left(\frac{q_1}{p}\right)^{n_1}\cdots\left(\frac{q_r}{p}\right)^{n_r}.$$

也就是說給定一奇質數 $p$, 我們只要知道 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ ($q$ 為任意與 $p$ 相異的奇質數) 之值, 那麼對任意與 $p$ 互質的整數 $a$, 就可以算出 $\left(\frac{a}{p}\right)$ 之值了.

我們從原來要了解一般二次的 congruence equation 解的情形, 一路化簡到現在只要了解 $x^2\equiv -1\pmod{p}$, $x^2\equiv 2\pmod{p}$ 和 $x^2\equiv q\pmod{p}$ (其中 $q$ 是與 $p$ 相異的奇質數), 這三種簡單形式的情形. 這就是解決數學問題常遇到的由繁化簡的過程, 值得大家細細體會其中的演化. 另一件有趣的是 Legendre symbol 和 Euler's Criterion 幫助我們將一個原本解二次 congruence equation 的問題換成另外一個和解方程式完全無關的方法來處理. 接下來我們就是要利用這樣的方式來處理 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$, 而不再直接探討 $x^2\equiv -1,2,q\pmod{p}$ 有解或是無解.

**Exercise 5.3.** 假設 $p$ 為奇質數且 $a,b,c\in\mathbb{Z}$ 皆與 $p$ 互質。試利用 Legendre symbol 的性質（Lemma 5.2.2, Proposition 5.2.5），求以下 Legendre symbol 的值：

(1) 已知 $ab\equiv 1 \pmod p$，求 $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$。

(2) 已知 $ax^2\equiv c \pmod p$ 無解，求 $\left(\frac{a}{p}\right)\left(\frac{c}{p}\right)$。

**Exercise 5.4.** 假設 $p$ 是一奇質數。

(1) 試求 $\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots+\left(\frac{p-1}{p}\right)$（Hint: 利用在 modulo $p$ 之下共有 $\frac{p-1}{2}$ 個 quadratic residue）.

(2) 若已知 $\left(\frac{-1}{p}\right)=1$，試求 $\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots+\left(\frac{(p-1)/2}{p}\right)$.

## 5.3. Quadratic Reciprocity Law

我們僅剩下要討論 $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ 和 $\left(\frac{q}{p}\right)$ 之值. 在這節中 $p$ 和 $q$ 永遠表示兩相異奇質數, 我們就不另加說明了.

**5.3.1. 求 $\left(\frac{-1}{p}\right)$.** 我們首先探討 $\left(\frac{-1}{p}\right)$ 的取值情形. 或許大家會疑惑當 $a$ 是一個負整數時, 一定可以找到一正整數 $b$ 使得 $a\equiv b \pmod p$, 因此利用 Lemma 5.2.2(2) 我們有 $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$, 所以只要探討正整數的情況就好了為何還要考慮負的情況呢? 沒錯, 一般來說我們只要知道正整數的情形就足夠了, 不過考慮負整數也有其方便性. 例如我們要求 $\left(\frac{97}{101}\right)$. 因為 $97\equiv -4=(-1)\times 2^2 \pmod{101}$, 利用 Lemma 5.2.2 以及 Proposition 5.2.5 馬上可得 $\left(\frac{97}{101}\right)=\left(\frac{-1}{101}\right)$. 另一方面在 modulo $p$ 之下是否有元素像複數中的 $i$ 一樣滿足 $i^2=-1$ 原本也就是一個有趣的問題. 所以了解 $\left(\frac{-1}{p}\right)$ 之值事實上是必要的.

Euler's Criterion 雖然在算一般的 $\left(\frac{a}{p}\right)$ 不是很好用, 不過在算 $\left(\frac{-1}{p}\right)$ 就很好用了.

**Theorem 5.3.1.** 假設 $p$ 是奇質數, 則

$$\left(\frac{-1}{p}\right)=\begin{cases} 1, & \text{當 } p\equiv 1 \pmod 4;\\ -1, & \text{當 } p\equiv -1 \pmod 4.\end{cases}$$

**Proof.** 利用 Corollary 5.2.4 我們知

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

若 $p\equiv 1 \pmod 4$, 表示存在 $k\in\mathbb{N}$ 使得 $p=4k+1$, 故得 $(-1)^{(p-1)/2}=(-1)^{2k}=1$. 因此得證 $\left(\frac{-1}{p}\right)=1$. 若 $p\equiv -1 \pmod 4$, 表示存在 $k\in\mathbb{N}$ 使得 $p=4k-1$, 故得 $(-1)^{(p-1)/2}=(-1)^{2k-1}=-1$. 因此得證 $\left(\frac{-1}{p}\right)=-1$. □

要注意由於 $p$ 是奇質數, 因此 $p$ 在 modulo 4 之下要不然和 1 同餘要不然就和 $-1$ 同餘, 所以 Theorem 5.3.1 給了 $\left(\frac{-1}{p}\right)$ 完整的答案. 今後我們要知道 $x^2 \equiv -1 \pmod{p}$ 是否有解時, 只要看 $p$ 在 modulo 4 之情形就可以知道答案. 例如剛才我們想知道 $x^2 \equiv 97 \pmod{101}$ 是否有解, 由 $\left(\frac{97}{101}\right) = \left(\frac{-1}{101}\right)$ 以及 $101 \equiv 1 \pmod{4}$ 馬上知道 $x^2 \equiv 97 \pmod{101}$ 是有解的.

**5.3.2. 求 $\left(\frac{2}{p}\right)$.** 接下來我們要探討 $\left(\frac{2}{p}\right)$ 的取值情形. 會將 2 和一般的奇質數分開討論的原因是因為 2 是唯一的偶質數, 其表現在很多狀況是和奇質數不同的, 事實上我們在前面已經看到許多在 2 的情況和一般奇質數有很大不同的情形例如 $x^2 \equiv a \pmod{2^n}$ 和 $x^2 \equiv a \pmod{p^n}$ 這兩種 congruence equation 其解的形態就完全不同.

我們還是要用 Euler's criterion 的精神來求 $\left(\frac{2}{p}\right)$ 而不是直接探討 $x^2 \equiv 2 \pmod{p}$ 何時有解. 然而 Euler's criterion 並不能直接套用來求 $\left(\frac{2}{p}\right)$, 主要原因是我們這裡的 $p$ 是一般的奇質數而不是特定的奇質數, 所以根本無法估計 $2^{(p-1)/2}$ 在 modulo $p$ 之下為 1 或 $-1$. 我們必須推導出另外的方法可以幫助我們求 $2^{(p-1)/2}$ 在 modulo $p$ 之情形.

**Lemma 5.3.2** (Gauss's Lemma)**.** 假設 $p$ 是奇質數且 $a \in \mathbb{Z}$ 滿足 $p \nmid a$. 考慮集合 $S = \{a, 2a, \ldots, \frac{p-1}{2}a\}$. 若 $S$ 中共有 $n$ 個元素其除以 $p$ 的餘數大於 $(p-1)/2$, 則

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

**Proof.** 我們將 $S$ 中的元素除以 $p$ 的餘數分成 $r_1, \ldots, r_n$ 及 $s_1, \ldots, s_m$ 兩部份, 其中 $r_i > (p-1)/2$；而 $s_j \leq (p-1)/2$. 若將 $S$ 中的元素全部乘在一起，在 modulo $p$ 之下會有

$$\frac{p-1}{2}! \times a^{\frac{p-1}{2}} \equiv (r_1 \cdots r_n) \times (s_1 \cdots s_m) \pmod{p}. \tag{5.1}$$

為了要求出 $a^{\frac{p-1}{2}}$ 在 modulo $p$ 之下與 $(-1)^n$ 同餘，我們需進一步了解 $r_1, \ldots, r_n$ 以及 $s_1, \ldots, s_m$.

首先因為 $a$ 與 $p$ 互質，所以 $a, 2a, \ldots, \frac{p-1}{2}a$ 在 modulo $p$ 之下皆不同餘，因此它們除以 $p$ 的餘數 $r_1, \ldots, r_n$ 以及 $s_1, \ldots, s_m$ 皆兩兩相異，也就是說共有 $n+m = \frac{p-1}{2}$ 元素。另一方面，若令集合 $T = \{p-r_1, \ldots, p-r_n, s_1, \ldots, s_m\}$，則 $T$ 中的元素也是兩兩相異的。這是因為若 $p - r_i = s_j$，依定義 $r_i, s_j$ 分別為 $ka, la$ 除以 $p$ 的餘數，其中 $1 \leq k, l \leq \frac{p-1}{2}$，所以 $p - r_i = s_j$ 表示 $p - ka \equiv la \pmod{p}$，亦即 $(k+l)a \equiv 0 \pmod{p}$。然而 $1 \leq k+l \leq p-1$，不可能滿足 $p \mid k+l$，所以任意的 $p - r_i$ 皆不可能等於 $s_j$。由於 $T$ 中的元素皆介於 1 到 $\frac{p-1}{2}$ 之間，且兩兩相異又共有 $n+m = \frac{p-1}{2}$ 元素，因此知 $T = \{1, 2, \ldots, \frac{p-1}{2}\}$。現將 $T$ 中元素全部乘在一起，在 modulo $p$ 之下會有

$$((p-r_1)\cdots(p-r_n)) \times (s_1 \cdots s_m) \equiv (-1)^n (r_1 \cdots r_n) \times (s_1 \cdots s_m) \equiv \frac{p-1}{2}! \pmod{p}. \tag{5.2}$$

結合式子 (5.1)、(5.2)，得

$$(-1)^n(r_1\cdots r_n)\times(s_1\cdots s_m)\times a^{\frac{p-1}{2}}\equiv(r_1\cdots r_n)\times(s_1\cdots s_m)\pmod p.$$

因為 $(r_1\cdots r_n)\times(s_1\cdots s_m)$ 與 $p$ 互質，故得證 $(-1)^n\times a^{\frac{p-1}{2}}\equiv 1 \pmod p$，亦即 $a^{\frac{p-1}{2}}\equiv(-1)^n \pmod p$. □

若 $\{a,2a,\ldots,\frac{p-1}{2}a\}$ 中共有 $n$ 個元素除以 $p$ 的餘數大於 $(p-1)/2$, 則由 Corollary 5.2.4 以及 Lemma 5.3.2 知

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

故由 $\left(\frac{a}{p}\right)$ 的取值為 $\pm1$, 得

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

Gauss's Lemma 將繁複 $a^{\frac{p-1}{2}}$ 的計算換成計算 $\{a,2a,\ldots,\frac{p-1}{2}a\}$ 中有多少個除以 $p$ 的餘數大於 $(p-1)/2$, 確實將問題簡化了. 我們可以利用它來計算 $\left(\frac{2}{p}\right)$.

**Theorem 5.3.3.** 假設 $p$ 是奇質數, 則

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

**Proof.** 考慮 $S=\{2,2\times2,\ldots,\frac{p-1}{2}\times2\}$, 我們得 $S=\{2,4,\ldots,p-1\}$. 也就是說 $S$ 中的元數除以 $p$ 所得餘數所成的集合恰為 $S$, 即小於 $p$ 的正偶數所成之集合. 由於 $p$ 是奇數, 我們將之分成 $p\equiv\pm1,\pm3 \pmod 8$ 四種情形來討論. 看看 $S$ 中有多少元素大於 $(p-1)/2$.

當 $p=8k+1$ (即 $p\equiv1 \pmod 8$) 時, $(p-1)/2=4k$. 因此 $S$ 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1=8k$ 且大於 $4k$ 的偶數之個數. 知其共有 $(8k-4k)/2=2k$. 故由 Corollary 5.2.4 以及 Lemma 5.3.2 知

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

當 $p=8k-1$ (即 $p\equiv-1 \pmod 8$) 時, $(p-1)/2=4k-1$. 因此 $S$ 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1=8k-2$ 且大於 $4k-1$ 的偶數之個數. 知其共有

$$(8k-2-(4k-2))/2=2k.$$

故由 Corollary 5.2.4 以及 Lemma 5.3.2 知

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

當 $p=8k+3$ (即 $p\equiv3 \pmod 8$) 時, $(p-1)/2=4k+1$. 因此 $S$ 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1=8k+2$ 且大於 $4k+1$ 的偶數之個數. 知其共有 $(8k+2-4k)/2=2k+1$. 故由 Corollary 5.2.4 以及 Lemma 5.3.2 知

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

當 $p=8k-3$ (即 $p\equiv -3 \pmod 8$) 時, $(p-1)/2=4k-2$. 因此 $S$ 中大於 $(p-1)/2$ 的元素個數即為小於等於 $p-1=8k-4$ 且大於 $4k-2$ 的偶數之個數. 知其共有

$$(8k-4-(4k-2))/2=2k-1.$$

故由 Corollary 5.2.4 以及 Lemma 5.3.2 知

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

□

有了 Theorem 5.3.3, 給定一奇質數 $p$, 我們將很容易知道 $x^2\equiv 2 \pmod p$ 是否有解. 例如因為 $101\equiv 5\equiv -3 \pmod 8$, 故知 $x^2\equiv 2 \pmod{101}$ 無解. 而 $23\equiv -1 \pmod 8$ 故知 $x^2\equiv 2 \pmod{23}$ 有解. 事實上 $5^2\equiv 2 \pmod{23}$, 故知 $x\equiv \pm 5 \pmod{23}$ 為 $x^2\equiv 2 \pmod{23}$ 之解.

**Exercise 5.5.** 試分別利用 Euler's Criterion 以及 Gauss's Lemma 計算以下 Legendre symbols:

$$\text{(a)}\ \left(\frac{11}{23}\right) \qquad \text{(b)}\ \left(\frac{-6}{11}\right).$$

**Exercise 5.6.** 利用 Theorem 5.3.1 以及 Theorem 5.3.3，將奇質數 $p$ 依 modulo 8 分類求 $\left(\frac{-2}{p}\right)$。

**Exercise 5.7.** 假設 $p$ 是一奇質數, 試利用 Gauss's Lemma 依照分類方式求 Legendre symbol 的值。

(1) 將 $p$ 依照 modulo 4 分類，求 $\left(\frac{-1}{p}\right)$（不要用 Theorem 5.3.1）。

(2) 將 $p$ 依照 modulo 12 分類，求 $\left(\frac{3}{p}\right)$。

**Exercise 5.8.** 以下我們要用反證法證明 $4k+1$ 形式的質數有無窮多個. 假設 $p_1,\ldots,p_r$ 是所有 $4k+1$ 形式的質數, 試證明若 $q$ 是一質數且 $q|4p_1^2\cdots p_r^2+1$, 則 $q\equiv 1 \pmod 4$ (即 $q$ 亦為 $4k+1$ 形式). 依此得矛盾而得證 $4k+1$ 形式的質數有無窮多個.