5 Quadratic Reciprocity Law

5.1 Primitive roots and solutions of congruences

In Corollary 3.6, we see that if \(d|(p-1)\), where \(p\) is a prime, then
\[
x^d \equiv 1 \pmod{p}
\]
is solvable and has exactly \(d\) solutions. In this section, we study an extension of this result.

**Theorem 5.1** Suppose \(m = 1, 2, 4, p^\alpha\) or \(2p^\alpha\), where \(p\) is an odd prime. Let \((a, m) = 1\) and let \(d = (\varphi(m), n)\). The congruence
\[
x^n \equiv a \pmod{m}
\]
is solvable if and only if
\[
a^{\varphi(m)/d} \equiv 1 \pmod{m}.
\]
In the case when the congruence is solvable, there are exactly \(\left(\frac{n}{\varphi(m)}\right)\) solutions.

**Proof**

We may assume that \(n \leq \varphi(m)\) by Euler’s Theorem. If
\[
x^n \equiv a \pmod{m}
\]
has a solution, then let \(g^k\) be its solution where \(g\) is a primitive root modulo \(m\). Hence
\[
a^{\varphi(m)/d} \equiv g^{kn(\varphi(m)/d)} \equiv (g^{\varphi(m)})^{kn/d} \equiv 1 \pmod{m}.
\]

Conversely, suppose
\[
a^{\varphi(m)/d} \equiv 1 \pmod{m}.
\]
Let \(a = g^\ell\). Note that from our assumption and the fact that \(g\) is a primitive root, we must have
\[
\varphi(m)|((\ell\varphi(m))/d).
\]
Hence \(d|\ell\).

Now consider the linear congruence
\[
u \equiv \ell \pmod{\varphi(m)}.
\]
Note that since \( d = (n, \varphi(m)) \) divides \( \ell \), the above congruence is solvable by Theorem 1.40. Now, let \( s = g^u \). Then
\[
s^n = g^{nu} = g^{nu + \varphi(m)v} \equiv g^\ell \equiv a \pmod{m}
\]
and hence
\[
x^n \equiv a \pmod{m}
\]
is solvable.

By specifying \( n = 2 \) and \( m = p \) we see that

**Theorem 5.2 (Euler’s Criterion)** The congruence equation
\[x^2 \equiv a \pmod{p}\]
is solvable if and only if
\[a^{(p-1)/2} \equiv 1 \pmod{p}.
\]

### 5.2 The Legendre Symbol

Let \( a \) be any integer relatively prime to \( p \), where \( p \) is an odd prime. The Legendre symbol is defined by
\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } x^2 \equiv a \pmod{p} \text{ is solvable,} \\
-1 & \text{otherwise.}
\end{cases}
\]

From the Euler Criterion, we see immediately that
\[a^{(p-1)/2} \equiv \left( \frac{a}{p} \right) \pmod{p}.
\]
This is because \( a^{p-1} \equiv 1 \pmod{p} \) and so \( a^{(p-1)/2} \equiv \pm 1 \pmod{p} \).

When \( p \mid n \) we simply define
\[
\left( \frac{n}{p} \right) = 0.
\]

From Euler’s Criterion, we obtain immediately that the Legendre symbol \( \left( \frac{n}{p} \right) \) is a completely multiplicative function of \( n \), i.e.,
\[
\left( \frac{mn}{p} \right) = \left( \frac{m}{p} \right) \left( \frac{n}{p} \right).
\]

In the subsequent sections, we will learn an algorithm in computing the Legendre symbol, thereby allowing us to determine the solvability of the congruence
\[x^2 \equiv a \pmod{p}.
\]
**Definition 5.3** For \((a, p) = 1\), we say that \(a\) is a quadratic residue modulo \(p\) if \(x^2 \equiv a \pmod{p}\) is solvable. Otherwise, we say that \(a\) is a quadratic non-residue modulo \(p\).

### 5.3 Gauss Lemma

In this section, we give an elementary proof of the Gauss Lemma.

**Theorem 5.4** Let \(p\) be a prime and let \(a\) be an integer such that \((a, p) = 1\). Consider

\[ S := \{a, 2a, \ldots, \frac{p-1}{2}a\} \]

and let

\[ T := \{s \pmod{p} | s \in S\}, \]

with elements in \(T\) between 0 and \(p - 1\). Suppose there are \(m\) elements in \(T\) which are greater than \(p/2\), then

\[ \left( \frac{a}{p} \right) = (-1)^m. \]

**Proof**

Let \(r_1, r_2, \ldots, r_m\) be elements in \(T\) exceeding \(p/2\). Let \(s_1, s_2, \ldots, s_k\) be the remaining elements in \(T\). Note that

\[ m + k = \frac{p-1}{2}. \]

Now, \(r_j > p/2\) implies that \(0 < p - r_j < p/2\).

Note that since \((\mathbb{Z}/p\mathbb{Z})^*\) is a group, multiplication by \(a\) induces a bijection on this group and hence, no two \(s_i\)'s coincide and no two \(p - r_j\) coincide. It remains to show that no \(p - r_j\) coincides with \(s_i\). Let

\[ r_j \equiv \rho a \pmod{p} \quad \text{and} \quad s_i \equiv \sigma a \pmod{p}, \]

with \(\rho < p/2, \sigma < p/2\) and \(\rho \neq \sigma\). If

\[ -r_j \equiv s_i \pmod{p}, \]

then

\[ a(\rho + \sigma) \equiv 0 \pmod{p}. \]

This implies that \(p|(\rho + \sigma)\). Since \(|\rho + \sigma| < p\), this is impossible.

Now, since \(m + k = (p - 1)/2\), \(p - r_i, 1 \leq i \leq n\) and \(s_j, 1 \leq j \leq k\), are distinct and less than \(p/2\) and that they are all less than \(p/2\), we conclude that

\[ \{p - r_1, p - r_2, \ldots, p - r_m, s_1, s_2, \ldots, s_k\} = \{1, 2, \ldots, \frac{p - 1}{2}\}. \]
Multiplying the elements on both sides, we find that
\[ (-r_1)(-r_2) \cdots (-r_m) \cdot s_1 \cdots s_k \equiv \left( \frac{p - 1}{2} \right)! \pmod{p}. \]

But
\[ r_1 \cdot r_2 \cdots r_m \cdot s_1 \cdots s_k \equiv (-1)^m a^{(p-1)/2} \left( \frac{p - 1}{2} \right)! \pmod{p} \]
as the \( r_i \)'s and \( s_j \)'s are congruent to elements in \( S \), we conclude that
\[ a^{(p-1)/2} \equiv (-1)^m \pmod{p}, \]
and hence,
\[ \left( \frac{a}{p} \right) = (-1)^m. \]

\[ \square \]

### 5.4 Proofs of Gauss’ Quadratic Reciprocity Law

Let \( a = -1 \) then \( m = (p-1)/2 \) since \( a \not\in S \) for all \( s \in S \). From Euler’s Criterion or Gauss Lemma (Theorem 5.4), we deduce that
\[ \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2}. \]

This is the first part of Gauss’ quadratic reciprocity law.

Let \( a = 2 \) and \( p \equiv 1 \pmod{4} \). Set \( p = 4\ell + 1 \). We have \( S = \{1, 2, \cdots, 2\ell\} \).

Therefore \( 2S = \{2, 4, \cdots, 2\ell, 2\ell + 2, \cdots, 4\ell\} \). Hence \( m = \ell \). In other words
\[ \left( \frac{2}{p} \right) = \begin{cases} 1 & \text{if } p = 8\ell + 1 \\ -1 & \text{if } p = 8\ell + 5. \end{cases} \]

Similarly, we have
\[ \left( \frac{2}{p} \right) = \begin{cases} 1 & \text{if } p = 8\ell + 7 \\ -1 & \text{if } p = 8\ell + 3. \end{cases} \]

In short, we may write
\[ \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8}. \]

We now prove the final part of Gauss’ quadratic reciprocity law. First, we need a lemma.

**Lemma 5.5** For odd positive integer \( m \), we have
\[ \frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{1 \leq j \leq (m-1)/2} \left( \sin^2 x - \sin^2 \frac{2\pi j}{m} \right). \]
5.4 Proofs of Gauss’ Quadratic Reciprocity Law

Proof

It is known that

$$\cos mx + i \sin mx = (\cos x + i \sin x)^m = \sum_{k=0}^{m} A_k (\cos x)^{m-k} (\sin x)^k i^k.$$  

Comparing the imaginary parts of both sides, we conclude that

$$\sin mx = \sum_{\ell=0}^{(m-1)/2} A_{2\ell+1} \sin^{2\ell+1} x \cos^m x (\sin^2 x - \sin^2 \frac{2\pi j}{m}).$$

Hence

$$\frac{\sin mx}{\sin x}$$

is a polynomial in \(\sin^2 x\) of degree \((m - 1)/2\). We note that the function

$$\frac{\sin mx}{\sin x}$$

vanishes when \(x = 2\pi j/m\) for \(1 \leq j \leq (m - 1)/2\). Hence

$$\frac{\sin mx}{\sin x} = C \prod_{1 \leq j \leq (m-1)/2} \left( \sin^2 x - \sin^2 \frac{2\pi j}{m} \right).$$

The constant \(C\) can be found by letting \(x\) tends to 0. The left hand side is \(m\) and the right hand side becomes

$$C(-1)^{(m-1)/2} \prod_{1 \leq j \leq (m-1)/2} \sin^2 \frac{2\pi j}{m}.$$

Using the fact that

$$\sin(\pi - x) = \sin x,$$

we find that

$$\prod_{1 \leq j \leq (m-1)/2} \sin^2 \frac{2\pi j}{m} = \prod_{k=1}^{m-1} \sin \frac{k\pi}{m}.$$

But

$$\prod_{k=1}^{m-1} \sin \frac{k\pi}{m} = \frac{1}{2^{m-1} m-1} \prod_{k=1}^{m-1} e^{-ik\pi/m} (\omega^k - 1),$$

where \(\omega = e^{2\pi i/m}\). Now,

$$\prod_{k=1}^{m-1} e^{-ik\pi/m} = i^{-(m-1)},$$

and using the equation

$$x^m - 1 = \prod_{k=1}^{m} (x - \omega^k),$$
we deduce that
\[ m(-1)^{m-1} = \prod_{k=1}^{m-1} (\omega^k - 1). \]

Hence,
\[ \prod_{k=1}^{m-1} \sin \frac{k\pi}{m} = \frac{m}{2^{m-1}}. \]

This implies that \( C = (-4)^{(m-1)/2} \) and the proof is complete. \( \square \)

The main part of Gauss’ quadratic reciprocity law states that for odd distinct primes \( p, q \)
\[ \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}. \]

Let \( S = \{1, 2, \ldots, (p - 1)/2\} \). Write
\[ [qs]_p = [e_s(q)s_q]_p, \]
where \( s_q \in S \) and
\[ e_s(q) = \begin{cases} 1 & \text{if } qs = s_q \in S \\ -1 & \text{if } qs \notin S. \end{cases} \]

Note that \( e_s(q) = -1 \) precisely when \( qs \) exceeds \( p/2 \). Hence, if \( m \) is the number of elements in \( qS = \{1 \leq qs \pmod{p} \leq p|s \in S\} \) that exceeds \( p/2 \), then
\[ \left( \frac{q}{p} \right) = (-1)^m = \prod_{s \in S} e_s(q). \]

Now, define
\[ F([m]_p) = \sin \frac{2\pi m}{p}. \]

Note that \( F \) is well defined on \((\mathbb{Z}/p\mathbb{Z})^*\) since \( F([m + kp]_p) = F([m]_p) \) because \( \sin(2\pi(m + kp)/p) = \sin(2\pi m/p) \). Therefore, the relation
\[ [qs]_p = [e_s(q)s_q]_p \]
yields
\[ \sin \frac{2\pi}{p} qs = F([qs]_p) = F([e_s(q)s_q]_p) = e_s(q) \sin \frac{2\pi}{p} s_q. \]

Since \( s \to s_q \) is a bijection of \( S \), we conclude that
\[ \left( \frac{q}{p} \right) = \prod_{s \in S} e_s(q) = \prod_{s \in S} \frac{\sin \frac{2\pi}{p} qs}{\sin \frac{2\pi}{p} s_q} = \prod_{s \in S} \frac{\sin \frac{2\pi}{p} qs}{\sin \frac{2\pi}{p} s}. \]
Applying Lemma 5.5, we deduce that
\[ \left( \frac{q}{p} \right) = \prod_{s \in S} (-4)^{(q-1)/2} \prod_{t \in T} \left( \sin^2 \frac{2 \pi s}{p} - \sin^2 \frac{2 \pi t}{q} \right), \]
where \( T = \{1, 2, \ldots, (q - 1)/2\} \). Hence
\[ \left( \frac{q}{p} \right) = (-4)^{(q-1)(p-1)/4} \prod_{s \in S} \prod_{t \in T} \left( \sin^2 \frac{2 \pi s}{p} - \sin^2 \frac{2 \pi t}{q} \right). \]
Interchanging the role of \( p \) and \( q \), we deduce that
\[ \left( \frac{p}{q} \right) = (-4)^{(q-1)(p-1)/4} \prod_{t \in T} \prod_{s \in S} \left( \sin^2 \frac{2 \pi t}{q} - \sin^2 \frac{2 \pi s}{p} \right). \]
Therefore,
\[ \left( \frac{p}{q} \right) \quad \text{and} \quad \left( \frac{q}{p} \right) \]
agrees up to sign and the sign is given by \((-1)^{(p-1)(q-1)/4}\) by looking at the products
\[ \prod_{s \in S} \prod_{t \in T} \left( \sin^2 \frac{2 \pi s}{p} - \sin^2 \frac{2 \pi t}{q} \right) \quad \text{and} \quad \prod_{t \in T} \prod_{s \in S} \left( \sin^2 \frac{2 \pi t}{q} - \sin^2 \frac{2 \pi s}{p} \right). \]
We have thus completed the proof of the quadratic reciprocity law and we summarize the result as follow:

**Theorem 5.6** Let \( p \) and \( q \) be distinct primes. Then we have
\[ \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \]
\[ \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} \]
\[ \left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{(p-1)(q-1)/4}. \]

**Example 5.1**
Show that \( x^2 \equiv 10 \pmod{89} \) is solvable.

**Solutions.** We compute
\[ \left( \frac{10}{89} \right) = \left( \frac{2}{89} \right) \left( \frac{5}{89} \right) = (-1)^{(89^2-1)/8} \left( \frac{5}{89} \right) = \left( \frac{89}{5} \right) = 1. \]

### 5.5 The Jacobi Symbol

In this section, we discuss an extension of the Legendre symbol.
**Definition 5.7** Let \( Q \) be a positive odd integer so that 
\[ Q = q_1 q_2 \cdots q_s \]
where \( q_i \) are not necessarily distinct. The Jacobi symbol is defined by
\[
\left( \frac{P}{Q} \right) = \prod_{j=1}^{s} \left( \frac{P}{q_j} \right)
\]
where the expressions on the right hand side involving \( q_j \) are the Legendre symbols.

We observe that if \( Q \) is prime then the Jacobi symbol is simply the Legendre symbol. We also note that if \( (P, Q) > 1 \), then
\[
\left( \frac{P}{q_j} \right) = 0
\]
for some \( j \) and hence
\[
\left( \frac{P}{Q} \right) = 0.
\]

Now if \( P \) is a quadratic residue modulo \( Q \), then
\[ x^2 \equiv P \pmod{q_j} \]
is solvable and hence
\[
\left( \frac{P}{q_j} \right) = 1.
\]
The converse, however, is not true. Although
\[
\left( \frac{2}{15} \right) = 1,
\]
the congruence
\[ x^2 \equiv 2 \pmod{15} \]
is not solvable.

From the definition of the Jacobi symbol and the properties of the Legendre symbol, it is immediate that
\[
\left( \frac{P}{Q} \right) \left( \frac{P'}{Q} \right) = \left( \frac{P}{QQ'} \right)
\]
\[
\left( \frac{P}{Q} \right) \left( \frac{P'}{Q} \right) = \left( \frac{PP'}{Q} \right)
\]
\[
\left( \frac{P^2}{Q} \right) = 1 \text{ and } \left( \frac{P}{Q^2} \right) = 1
\]
Finally, we observe that if \( P \equiv P' \pmod{Q} \), then
\[
\left( \frac{P}{Q} \right) = \left( \frac{P'}{Q} \right).\]
The main result we want to show in this section is

**Theorem 5.8** If \( Q \) is odd positive integer, then

\[
\left( \frac{-1}{Q} \right) = (-1)^{\frac{Q-1}{2}} \\
\left( \frac{2}{Q} \right) = (-1)^{\frac{a^2-1}{2}} \\
\left( \frac{P}{Q} \right) \left( \frac{Q}{P} \right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}}.
\]

**Proof**

To prove the first equality, we observe that

\[
\frac{ab - 1}{2} = \frac{(a - 1)}{2} + \frac{(b - 1)}{2} = \frac{(a - 1)(b - 1)}{2}.
\]

The numerator of the right hand side is divisible by 4 if both \( a \) and \( b \) are odd. Hence,

\[
\frac{ab - 1}{2} \equiv \left( \frac{a - 1}{2} + \frac{b - 1}{2} \right) \pmod{2}.
\]

Hence if \( Q = q_1q_2 \cdots q_s \), then

\[
\sum_{j=1}^{s} \left( \frac{q_j - 1}{2} \right) \equiv \left( \frac{Q - 1}{2} \right) \pmod{2}.
\]

This implies that

\[
\left( \frac{-1}{Q} \right) = \prod_{j=1}^{s} \left( \frac{-1}{q_j} \right) = (-1)^{\sum_{j=1}^{s} (q_j - 1)/2} = (-1)^{\frac{Q-1}{2}}.
\]

The proof of the second equality is similar except that we used the relation

\[
\frac{a^2b^2 - 1}{8} = \frac{(a^2 - 1)}{8} + \frac{(b^2 - 1)}{8} = \frac{(a^2 - 1)(b^2 - 1)}{8}
\]

and observe that the numerator of the right hand side is divisible by 64.

The proof of the last equality follows in exactly the same way as the proof of the first equality.

With the Jacobi symbol, we can now calculate Legendre symbol without having to factorize integers (except for factoring \(-1\) and 2).

In the next two sections, we will give another proof of the Gauss Lemma using results from group theory.
5.6 The Transfer

Let $G$ be a finite group and $H$ be a subgroup of $G$. Let $X = G/H$ and fix a set of representatives for $X$, namely,

$$R = \{x_1, \cdots, x_m\}$$

where $m = |X|$. Write the elements in $X$ as $[x_j]$ instead of $x_jH$.

The group $G$ acts on $X$ via

$$g \cdot [x_i] = [gx_i].$$

Now, because we insist that the representative for the cosets in $X$ to be from $R$ we must write $[gx_i]$ as $[x_j]$ for some $1 \leq j \leq m$. Since $[gx_i] = [x_j]$ for some $j$ we could view $G$ as acting on $\{1, 2, \cdots, m\}$ and we write

$$g \circ i = j.$$

In other words, we have

$$[gx_i] = [x_{gi}].$$

From the above, we conclude that

$$gx_i = x_{gi}h_{g,[x_i]}$$

for some $h_{g,[x_i]} \in H$. We define the transfer of $g$ to be

$$\text{Ver}(g) = \prod_{[x] \in X} h_{g,[x]} \pmod{[H,H]}$$

where where $[H,H]$ is the commutator subgroup of $H$, namely, the group generated by $\{h_1h_2h_1^{-1}h_2^{-1} | h_1, h_2 \in H\}$.

It appears that $\text{Ver}(g)$ depends on our choice of set of representatives $R$. We will show that this is not the case.

**Theorem 5.9** The map $\text{Ver} : G \to H/[H,H]$ is independent of the choice of representatives of $x \in X$ and it is a homomorphism.

**Proof**

Let $R^* = \{x^*_1, x^*_2, \cdots, x^*_m\}$ be another fixed set of coset representatives and suppose we have

$$[x^*_i] = [x_i].$$

This means that

$$x^*_i = x_i h_{[x_i]}$$

for some $h_{[x_i]} \in H$. Now,

$$g[x^*_i] = [gx^*_i] = [gx_i] = [x_{gi}] = [x^*_{gi}].$$

If we write

$$gx^*_i = x^*_{gi}h^*_{g,[x^*_i]}$$
for some \( h_{g,[x_i^*]} \in H \), then the corresponding transfer is defined by

\[
\text{Ver}^*(g) = \prod_{[x] \in X} h_{g,[x]}^* \quad (\text{mod } [H,H]).
\]

Note that

\[
gx_i^* = gx_i h_{[x_i]} = x_{g[x_i]} h_{g,[x_i]} h_{[x_i]} = x_{g[x_i]} h_{[x_i]}^{-1} h_{g,[x_i]} h_{[x_i]}.
\]

This implies that

\[
h_{g,[x_i^*]} = h_{[x_{g[x_i]}]}^{-1} h_{g,[x_i]} h_{[x_i]}.
\]

Therefore,

\[
\text{Ver}^*(g) = \prod_{[x_i] \in X} h_{[x_{g[x_i]}]}^{-1} h_{g,[x_i]} h_{[x_i]} \quad (\text{mod } [H,H]) = \text{Ver}(g)
\]

since

\[
ab = abb^{-1}a^{-1}ba = ba \quad (\text{mod } [H,H])
\]

and

\[
\prod_{[x_i] \in X} h_{[x_{g[x_i]}]}^{-1} h_{[x_i]} = 1 \quad (\text{mod } [H,H]).
\]

Therefore the transfer is independent of the coset representatives.

Next,

\[
st[x_i] = [stx_i] = [x_{st[x_i]}].
\]

Hence,

\[
stx_i = x_{st[x_i]}h_{st,[x_i]}.
\]

Now,

\[
s(tx_i) = s(x_{t[x_i]}) h_{t,[x_i]} = x_{t[x_i]} h_{s,[x_{t[x_i]}]} h_{t,[x_i]}.
\]

Therefore,

\[
\text{Ver}(st) = \prod_{[x_i] \in X} h_{st,[x_i]} \quad (\text{mod } [H,H]) = \prod_{[x_i] \in X} h_{s,[x_{t[x_i]}]} h_{t,[x_i]} \quad (\text{mod } [H,H])
\]

\[
= \prod_{[x_i] \in X} h_{s,[x_{t[x_i]}]} h_{t,[x_i]} \quad (\text{mod } [H,H]) = \text{Ver}(s)\text{Ver}(t).
\]

Hence Ver is a homomorphism.

\[\square\]

Our next task to compute \( \text{Ver}(s) \) for a single element \( s \in G \). We consider the cyclic subgroup \( C \) generated by \( s \) and let \( C \) acts on \( X \), namely,

\[
s^j[x] = [s^jx].\]
Note that $X$ is a disjoint union of orbits $O_\alpha$ under the action of $C$. If $|O_\alpha| = f_\alpha$ and $[x_\alpha] \in O_\alpha$ then the elements in the orbit are
\[
\{[s^j x_\alpha]| j = 0, 1, \ldots, f_\alpha - 1\}.
\]

We can now choose our coset representatives $R$ to contain
\[
\{s^j x_\alpha| j = 0, 1, \ldots, f_\alpha - 1\}
\]
for each orbit $O_\alpha$. Note that if $0 \leq j \leq f_\alpha - 2$,
\[
s[s^j x_\alpha] = [s^{j+1} x_\alpha]
\]
and since $s^{f_\alpha} x_\alpha \in R$, we have
\[
s(s^j x_\alpha) = s^{j+1} x_\alpha h_{s,[s^j x_\alpha]}
\]
with $h_{s,[s^j x_\alpha]} = 1$. When $j = f_\alpha - 1$, we find that
\[
s(s^{f_\alpha-1} x_\alpha) = s^{f_\alpha} x_\alpha = x_\alpha h_{s,[s^{f_\alpha-1} x_\alpha]}.
\]
\[\text{(5.2)}\]

Therefore,
\[
\text{Ver}(s) = \prod_{[x] \in X} h_{s,[x]} = \prod_{\alpha} \prod_{j=0}^{f_\alpha-1} h_{s,[s^j x_\alpha]} = \prod_{\alpha} h_{s,[s^{f_\alpha-1} x_\alpha]} = \prod_{\alpha} x_\alpha^{1-s^{f_\alpha} x_\alpha},
\]
where we have used (5.2).

Hence we have

**THEOREM 5.10** Let $s \in G$ and let $O_\alpha$ be the orbits of $X$ under the action of the cyclic subgroup generated by $s$. Suppose $[x_\alpha]$ is an element in $O_\alpha$, then
\[
\text{Ver}(s) = \prod_{\alpha} h_{\alpha} = \prod_{\alpha} (x_\alpha)^{-1} s^{f_\alpha} x_\alpha \quad \text{(mod } [H, H]).
\]

We have already seen that the map Ver is a homomorphism from $G$ to $H/[H, H]$. If $G$ is abelian then $[H, H]$ is trivial and we have a homomorphism from $G$ to $H$ given by
\[
\text{Ver}(s) = \prod_{\alpha} s^{f_\alpha} = s \sum_{\alpha} f_\alpha = s^m,
\]

since
\[
\sum_{\alpha} f_\alpha = m
\]
where $m = |X|$.
5.7 Gauss Lemma via the transfer

Let $G = (\mathbb{Z}/p\mathbb{Z})^*$ and $H = \{[\pm 1]_p\}$. Let the coset representatives of $H$ in $G$ be $S := \{1, 2, \cdots, (p - 1)/2\}$. Now, for $a \in G$,

$$\text{Ver}([a]_p) = [a]_p^{(p-1)/2}.$$

We now compute Ver from its definition. Note that for $[s]_p \in S$ and $[a]_p \in G$,

$$[as]_p = [s_a e_s(a)]_p$$

where

\[
e_s(a) = \begin{cases} 1 & \text{if } [as]_p = [sa]_p \text{ for some } s_a \in S, \\ -1 & \text{otherwise.} \end{cases}
\]

Hence,

$$\text{Ver}([a]_p) = [-1]^m_p$$

where $m$ is the number of elements $s$ such that $[as]_p \not\in S$. Comparing with the previous computation of Ver(s), we conclude that

$$\left(\frac{a}{p}\right)_p \equiv [a]_p^{(p-1)/2} = \text{Ver}([a]_p) = [-1]^m_p,$$

where $m$ is the number of elements $s$ such that $[as]_p \neq [s']_p$ for all $s' \in S$. In other words, $m$ is the number of elements in $S$ such that $[as]_p = [-sa]_p = [p - sa]_p$, or the number of elements in $S$ such that the least positive residues of $as \pmod{p}$ exceeds $p/2$. This proves Gauss Lemma and shows that Gauss Lemma corresponds to computing $\text{Ver}([a]_p)$ in two different ways.

5.8 The Legendre Symbol and primes of the form $x^2 + y^2$

In this section, we give an explicit form of $x$ and $y$ that satisfy

$$x^2 + y^2 = p$$

where $p$ is a prime, $p \equiv 1 \pmod{4}$. This would certainly imply that

**Theorem 5.11** Let $p$ be an odd prime such that $p \equiv 1 \pmod{4}$. Then $p$ is a sum of two squares.

We first need two lemmas.

**Lemma 5.12** Let $p$ be an odd prime. We have

$$\sum_{m \pmod{p}} \left(\frac{m}{p}\right) = 0.$$

---

1 Adapted from “Number Theory” by G.E. Andrews
Quadratic Reciprocity Law

Proof
Note that using primitive roots modulo $p$, we see that if $g$ is a primitive root modulo $p$, then the even powers of $g$ are quadratic residues and the odd powers of $g$ are quadratic non-residues. Therefore there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues. Therefore in the sum

$$\sum_{m \pmod{p}} \left( \frac{m}{p} \right),$$

there are $(p-1)/2$ terms which take the value 1 and $(p-1)/2$ terms which take the value $-1$. In other words,

$$\sum_{m \pmod{p}} \left( \frac{m}{p} \right) = 0.$$

\[\square\]

Lemma 5.13 Let $p$ be an odd prime. We have

$$\sum_{m \pmod{p}} \left( \frac{(m-a)(m-b)}{p} \right) = \begin{cases} p-1 & \text{if } a \equiv b \pmod{p} \\ -1 & \text{if } a \not\equiv b \pmod{p}. \end{cases}$$

Proof
Note first by replacing $m$ by $m+a$, we find that

$$\sum_{m \pmod{p}} \left( \frac{(m-a)(m-b)}{p} \right) = \sum_{m \pmod{p}} \left( \frac{(m)(m-(b-a))}{p} \right)$$

$$= \sum_{m \pmod{p}} \left( \frac{(m)(m-(b-a))}{p} \right)$$

since $\left( \frac{m}{p} \right) = 0$ when $p|m$. Let $m'$ be such that $m'm \equiv 1 \pmod{p}$. Then

$$\sum_{m \pmod{p}} \left( \frac{m(m-(b-a))}{p} \right) = \sum_{m \pmod{p}} \left( \frac{m'^2}{p} \right) \left( \frac{m(m-(b-a))}{p} \right)$$

$$= \sum_{m \pmod{p}} \left( \frac{m'm}{p} \right) \left( \frac{m'm-(b-a)}{p} \right)$$

$$= \sum_{m \pmod{p}} \left( \frac{1-m'(b-a)}{p} \right)$$

$$= \sum_{m' \pmod{p}} \left( \frac{1-m'(b-a)}{p} \right) - 1$$

$$= -1$$
by Lemma 5.12. Note that number -1 in the second last line is added so that we could sum over complete residues $m' \pmod{p}$. \hfill \Box

Let

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

Note that $S(0) = 0$ by Lemma 5.12 and $S(m + Np) = S(m)$ for any integer $N$.

Let $k \not\equiv 0 \pmod{p}$. Then

$$S(m) = \sum_{n \pmod{p}} \left( \frac{k^4}{p} \right) \left( \frac{n(n^2 - m)}{p} \right) = \sum_{n \pmod{p}} \left( \frac{k^2 n}{p} \right) \left( \frac{k^2 n^2 - k^2 m}{p} \right) = \left( \frac{k}{p} \right) \sum_{n \pmod{p}} \left( \frac{kn}{p} \right) \left( \frac{(kn)^2 - k^2 m}{p} \right) = \left( \frac{k}{p} \right) S(k^2 m).$$

Hence, we have

$$S^2(k^2 m) = S^2(m). \tag{5.3}$$

If $u$ is a quadratic residue modulo $p$, then $u \equiv k^2 \pmod{p}$ for some integer $k$ and

$$S^2(u) = S^2(k^2 \cdot 1) = S^2(1) \tag{5.4}$$

by setting $m = 1$ in (5.3).

If $v$ is a non-residue, then $v = \ell^2 j \ell$ where $\ell$ is a fixed primitive root modulo $p$. This is because all quadratic non-residues are odd powers of primitive roots modulo $p$. Then by (5.3),

$$S^2(v) = S^2(\ell^2 j \ell^2) = S^2(\ell). \tag{5.5}$$

We note that we can replace $\ell$ by any quadratic non-residue modulo $p$.

There are $(p - 1)/2$ quadratic residues and $(p - 1)/2$ quadratic non-residues and hence by (5.4) and (5.5), we deduce that

$$\sum_{m \pmod{p}} S^2(m) = S^2(0) + \frac{p-1}{2} (S^2(1) + S^2(\ell)) = \frac{p-1}{2} (S^2(1) + S^2(\ell))^2,$$

since $S^2(0) = 0.$
Now,
\[
\sum_{m \equiv \ell \pmod{p}} S^2(m) = \sum_{m \equiv \ell \pmod{p}} \sum_{s \equiv t \pmod{p}} \left( \frac{s(s^2 - m)}{p} \right) \left( \frac{t(t^2 - m)}{p} \right)
\]
\[
= \sum_{s,t} \left( \frac{st}{p} \right) \left( \frac{(m - s^2)(m - t^2)}{p} \right)
\]
\[
= \sum_{s,t} \left( \frac{st}{p} \right) \sum_{m} \left( \frac{(m - s^2)(m - t^2)}{p} \right).
\]

By Lemma 5.13, we deduce that
\[
\frac{p - 1}{2} (S^2(1) + S^2(\ell)) = \sum_{s \equiv t \pmod{p}} \left( \frac{st}{p} \right) (p - 1) + \sum_{s \equiv t \pmod{p}} \left( \frac{st}{p} \right) (-1)
\]
\[
= \sum_{s,t} \left( \frac{st}{p} \right) (p - 1) - \left\{ \sum_{s,t} \left( \frac{st}{p} \right) - \sum_{s,t} \left( \frac{st}{p} \right) \right\}
\]
\[
= p \sum_{s,t} \left( \frac{st}{p} \right),
\]
where we have used Lemma 5.12 in the last equality. Next,
\[
\sum_{s,t} \left( \frac{st}{p} \right) = \sum_{s,t} \left( \frac{st}{p} \right) + \sum_{s,t} \left( \frac{st}{p} \right)
\]
\[
= \sum_{t \equiv \ell \pmod{p}} \left( \frac{t^2}{p} \right) + \sum_{t \equiv -\ell \pmod{p}} \left( \frac{-t^2}{p} \right) = 2(p - 1)
\]

Hence we conclude that
\[
\left( \frac{S(1)}{2} \right)^2 + \left( \frac{S(\ell)}{2} \right)^2 = p.
\]

Now, if \(2 | S(m)\) then we would have found integers \(x\) and \(y\) such that
\[
x^2 + y^2 = p.
\]
To show that $2|S(m)$ for all integers $m$, we observe that

$$S(m) = \sum_{n=1}^{(p-1)/2} \left( \frac{n(n^2 - m)}{p} \right) + \sum_{n=(p+1)/2}^{p-1} \left( \frac{n(n^2 - m)}{p} \right)$$

$$= \sum_{n=1}^{(p-1)/2} \left( \frac{n(n^2 - m)}{p} \right) + \sum_{n=1}^{(p-1)/2} \left( \frac{(p-n)((p-n)^2 - m)}{p} \right)$$

$$= 2 \sum_{n=1}^{(p-1)/2} \left( \frac{n(n^2 - m)}{p} \right),$$

where the last equality follows for the fact that $p \equiv 1 \pmod{4}$.

**Remark 5.14** Recently, H.H. Chan, L. Long and Y.F. Yang showed the following observation:

Let $p \equiv 1 \pmod{6}$. Suppose $a$ is any integer such that $x^3 \equiv a \pmod{p}$ is not solvable. Then

$$3p = x^2 + xy + y^2,$$

with

$$x = \sum_{a=1}^{p} \left( \frac{a^3 + 1}{p} \right) \quad \text{and} \quad y = \left( \frac{a}{p} \right) \sum_{a=1}^{p} \left( \frac{a^3 + a}{p} \right).$$

### 5.9 Appendix : Primes of the form $x^2 + y^2$, a second approach

In this section, we give another proof of Theorem 5.11. This proof is due to D. Zagier and is motivated by the work of R. Heath-Brown, who is in turn motivated by Liouville.

Consider the set

$$S = \{(x, y, z) \in \mathbb{Z}^+ | x^2 + 4yz = p\}.$$

Note that $S$ is non-empty. This is because if $p = 4k + 1$, then $(1, 1, k) \in S$. Define the map on $S$ by

$$\alpha : (x, y, z) \rightarrow \begin{cases} 
(x + 2z, z, y - x - z) & \text{if } x < y - z, \\
(2y - x, y, x - y + z) & \text{if } y - z < x < 2y, \\
(x - 2y, x - y + z, y) & \text{if } x > y.
\end{cases}$$

We can check that this is a map on $S$ by checking that each expression in the image satisfies $x^2 + 4yz = p$. For example,

$$(x + 2z)^2 + 4z(y - x - z) = p$$

if $x^2 + 4yz = p$. 

We next check that $\alpha$ is an involution. This again can be checked by considering the three cases as listed in the definition of $\alpha$. For example, if $x < y - z$, then
\[ \alpha(x, y, z) = (x + 2z, z, y - x - z) = (x', y', z') \]
and $x + 2z > 2z$ or $x' > 2y'$. Hence
\[ \alpha(x', y', z') = (x' - 2y', x' - y' + z', y') = (x, y, z). \]
The rest of the cases can be verified in a similar way.

Our next step is to show that the only fixed point of $\alpha$ is $(1, 1, k)$ where $p = 1 + 4k$. If we use the definition of $\alpha$, we find that the only possible case where a fixed point exists for $\alpha$ is when $y - z < x < 2y$ since $x, y, z$ are all positive integers. This implies that the fixed point must be of the form $(u, u, w)$. But this would mean that $u^2 + 4uw = p$ and that $u|p$, or $u = 1$ or $p$. Now, $u \neq p$ for otherwise, the left hand side would be greater than the right hand side. Hence $u = 1$ and $w = k$ and the only fixed point of $\alpha$ is $(1, 1, k)$. For any involution $\beta$, we find that the number of elements in $S$ is the sum of the number of elements in
\[ \{s, \beta(s) \mid \beta(s) \neq s\} \]
and
\[ \{t \mid \beta(t) = t\}. \]
Since there is only one fixed point for $\alpha$, we conclude that the number of elements in $S$ is odd.

We next consider a simple involution
\[ \sigma(x, y, z) = (x, z, y). \]
Since the number of elements in $S$ is odd, $\sigma$ must have a fixed point, say $(x_0, y_0, z_0)$. But this is a fixed point of $\sigma$ means that $y_0 = z_0$ and thus, we conclude that
\[ x_0^2 + 4y_0^2 = p \]
and this completes the proof of Theorem 5.11.