Notes on Quadratic Reciprocity

Steven J. Miller*

October 2, 2002

Abstract

1 Arithmetic Modulo p

Let $\mathbb{Z}$ denote the integers, and define $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. We often read $\mathbb{Z}/n\mathbb{Z}$ as the **integers modulo** n.

Definition 1.1 (Congruence) *$x \equiv y$ mod n means $x - y$ is a multiple of n.*

Definition 1.2 (Equivalence Relation) *Let R be a binary operation on a set S. We say R is an equivalence relation if the following hold:*

1. $\forall x \in S$, $R(x,x)$ is true;
2. $\forall x, y \in S$, $R(x,y)$ is true if and only if $R(y,x)$ is true;
3. $\forall x, y, z \in S$, $R(x,y)$ and $R(y,z)$ true imply $R(x,z)$ is true.

Exercise 1.3
1. *Let S be any set, and let $R(x,y)$ be $x = y$. Prove R is an equivalence.*
2. *Let $S = \mathbb{R}$ and let $R(x,y)$ be $x \leq y$. Prove R is an equivalence.*
3. *Let $S = \mathbb{Z}/n\mathbb{Z}$ and let $R(x,y)$ be $x \equiv y$. Prove R is an equivalence.*

We define addition by $x, y \in \mathbb{Z}/n\mathbb{Z}$, then $x+y$ is the unique number $z \in \mathbb{Z}/n\mathbb{Z}$ such that $n|(x+y-z)$. In other words, z is the unique number in $\mathbb{Z}/n\mathbb{Z}$ such that $x + y \equiv z$.

$\mathbb{Z}/n\mathbb{Z}$ is a finite group under addition; in fact, it is a finite ring.

Exercise 1.4 *Prove we can multiply elements of $\mathbb{Z}/n\mathbb{Z}$, and that every non-zero element has a multiplicative inverses if and only if n is prime.*

*E-mail: `millerj@cims.nyu.edu` or `sjmiller@math.princeton.edu`

Try and solve in $\mathbb{Z}$ the equation $2x + 1 = 2y$. The left hand side is odd, the right hand side is even. Thus, there are no solutions. Really, what we did above is just arithmetic mod 2 or arithmetic in $\mathbb{Z}/2\mathbb{Z}$.

Now consider a harder problem: $x^2 + y^2 + z^2 = 8n + 7$. This never has a solution. Look modulo 8. The RHS is 7 modulo 8. What are the squares mod 8? $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 1$, $4^2 \equiv 0$, and then the pattern repeats (as modulo 8, k and $(8-k)$ have the same square). We see there is no way to add three squares and get 7. Thus, there are no solutions to $x^2 + y^2 + z^2 = 8n + 7$.

General Idea: First, try and solve the equation modulo different primes. If you cannot solve it for some prime, then you cannot solve it over the integers.

1.1 Group Theory Review

A group G is a set of elements g_i satisfying the four conditions below, relative to some binary operation. We often use multiplicative notation $(g_1 g_2)$ or additive notation $(g_1 + g_2)$ to represent the binary operation. For definiteness, we use multiplicative notation below; however, one could replace xy with $b(x, y)$ below.

If the elements of G satisfy the following four properties, then G is a group.

1. (Identity) $\exists e \in G$ s.t. $\forall g \in G : eg = ge = g$. We often write $e = 1$ for multiplicative groups, and $e = 0$ for additive groups.

2. (Associativity) $\forall x, y, z \in G : (xy)z = x(yz)$.

3. (Inverse) $\forall x \in G, \exists y \in G$ s.t. $xy = yx = e$. We write $y = x^{-1}$ for multiplication, $y = -x$ for addition.

4. (Closure) $\forall x, y \in G : xy \in G$.

If **commutation** holds ($\forall x, y \in G$, $xy = yx$), we say the group is **Abelian**. Non-abelian groups exist and are important.

Exercise 1.5 *Consider the group of $N \times N$ matrices with real entries and non-zero determinant. Prove this is a group under matrix multiplication, and show this group is not commutative.*

H is a **subgroup** of G if H is a group and its elements form a subset of those of G. The identity of H is the same as the identity of G. Once one has shown the elements of H are closed (ie, under the binary operation, $b(x, y) \in H$ if $x, y \in H$), then associativity in H follows from closure in H and associativity in G.

1.2 Algebra Review

Consider arithmetic in the ring $\mathbb{Z}/n\mathbb{Z}$.

Definition 1.6 $\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$ *$\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ are the invertible (under multiplication) elements in the ring $\mathbb{Z}/n\mathbb{Z}$; ie, x is in $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ if there is a y such that $xy \equiv 1$ mod n.*

Note: if $\gcd(x, n) > 1$ (ie, x and n have a common prime divisor p), then you cannot invert x (there is no y with $xy \equiv 1 \bmod n$). Why? $xy \equiv 1 \bmod n$ means $xy = 1 + \lambda n$ for some integer λ. But if $p|x$ and $p|n$, then $p|1$ which is absurd.

Exercise 1.7 (Euclidean Algorithm) *If $\gcd(x, n) = 1$, there is an multiplicative inverse to x mod n.*

The cardinality (number of elements in the set) of $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ is the number of $x \in \{0, 1, 2, \ldots, n-1\}$ such that $\gcd(x, n) = 1$. We denote the number of such x by $\phi(x)$, the Euler totient function. A good reference is H. Davenport, *The Higher Arithmetic*. Note that if p is prime, $\phi(p) = p - 1$. This implies that $\left|\left(\mathbb{Z}/p\mathbb{Z}\right)^*\right| = p - 1 = \mathbb{Z}/p\mathbb{Z} - \{0\}$. In other words, we have a field if n is a prime, as every non-zero element is invertible.

$\left(\mathbb{Z}/n\mathbb{Z}\right)^*$, for any n, is a finite Abelian group (we have inverses under multiplication, and order of multiplication doesn't matter). Finite Abelian Groups is a trivial subject: the Structure Theorem for Finite Abelian Groups says any such group can be decomposed as a product of cyclic groups.

For $n = p$ a prime, $\left(\mathbb{Z}/n\mathbb{Z}\right)^*$ is a cyclic group of order $p - 1$.

Definition 1.8 (order) *The order of x in a group G, ord(x), is the least positive power m such that $x^m = e$, where $e \in G$ is the identity of the group.*

Exercise 1.9 *Prove that, in a finite group, every element has finite order. Hint: use the pidgeonhole principle.*

1.3 Lagrange's Theorem

Theorem 1.10 (Lagrange) *Let H be a sub-group of a finite group G. Then $|H|$ divides $|G|$. In particular, taking H to be the sub-group generated by $x \in G$, ord(x) $|$ ord(G).*

We first prove two useful lemmas.

Lemma 1.11 (Cayley) *Let H be a sub-group of G, andlet $h \in H$. Then $hH = H$.*

Proof: by closure hH falls within H. We only need to show that hh_i can never equal hh_j for two different elements $i \neq j$. If $hh_i = hh_j$, since a unique h^{-1} exists we could pre-multiply the equation $hh_i = hh_j$ by h^{-1} to give $h_i = h_j$, giving a contradiction. Therefore $hh_i \neq hh_j$ if $i \neq j$. As H is finite, $hH = H$. $\square$

Lemma 1.12 *Let H be a sub-group of a finite group G. Then either $g_iH = g_jH$ or the two sets are disjoint.*

Proof: assume there is some element in both. Then $g_ih_1 = g_jh_2$. Multiplying on the right by $h_i^{-1} \in H$ (since H is a sub-group) gives $g_i = g_jh_2h_1^{-1}$. As H is a sub-group, $\exists h_3 \in H$ such that $h = h_2h_1^{-1}$. Thus $g_i = g_jh_3$. Therefore, as $h_3H = H$, $g_iH = g_jh_3H = g_jH$, and we see if the two sets have one element in common, they are identical. □

Definition 1.13 (coset) *We call a set gH a* coset *(actually, a left coset) of H.*

We now prove Lagrange's Theorem.
Clearly

$$G = \bigcup_{g \in G} gH \tag{1.1}$$

Why do we have an equality? As $g \in G$ and $H \subset G$, every set on the right is contained in G. Further, as $e \in H$, given $g \in G$, $g \in gH$. Thus, G is a subset of the right side, proving equality.

There are only finitely many elements in G. As we go through all g in G, we see if the set gH equals one of the sets already in our list (recall we've shown two cosets are either identical or disjoint). If the set equals something already on our list, we do not include it; if it is new, we do. Continuing this process, we obtain

$$G = \bigcup_{i=1}^{k} g_iH \tag{1.2}$$

for some finite k. If $H = \{e\}$, k is the number of elements of G; in general, however, k will be smaller.

Each set g_iH has $|H|$ elements. Thus, $|G| = k|H|$, proving $|H|$ divides $|G|$.

Applying Lagrange's Theorem to $(\mathbb{Z}/p\mathbb{Z})^*$ gives

Corollary 1.14 (Fermat's Little Theorem) *For any prime p, if $\gcd(a,p) = 1$, then $a^{p-1} \equiv 1$ mod p.*

Proof: $\left|(\mathbb{Z}/p\mathbb{Z})^*\right| = p - 1$.

Exercise 1.15 *Prove that if $a^{n-1} \not\equiv 1$ mod n then n is composite.*

1.4 Legendre Symbol

From now on, p and q will always be odd primes.

Definition 1.16 (Legendre Symbol $\left(\frac{\cdot}{p}\right)$) *The Legendre Symbol $\left(\frac{a}{p}\right)$ is 1 if a is a non-zero square mod p, 0 if $a = 0$, and -1 otherwise (ie, if a is not a square mod p).*

Note a is a square mod p if there exists an $x \in \{0, 1, \ldots, p-1\}$ such that $a \equiv x^2$ mod p. For p an odd prime, half the non-zero numbers are squares, half are not.

Exercise 1.17 (Euler's Criterion) *$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ mod p for odd p. Hint: $a^{\frac{p-1}{2}}$ squared is $a^{p-1} \equiv 1$, so $a^{\frac{p-1}{2}} \equiv \pm 1$ mod p.*

The Legendre symbol is a function on $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We can extend the Legendre symbol to all integers. We only need to know a mod p, and we define $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$.

Initially the Legendre symbol is define only when the bottom is prime. We now extend the definition to all n as follows: let $n = p_1 \cdot p_2 \cdots p_t$ be the product of t distinct primes. Then $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right)$. Note this is *not* the same as saying that if a is a square (a quadratic residue) mod n, then a is a square mod p_i for each prime divisor.

The main result (which allows us to calculate the Legendre symbol quickly and efficiently) is the celebrated

Theorem 1.18 (Quadratic Reciprocity) *For m, n odd and relatively prime, $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.*

Gauss gave at least four proofs of this deep result. If either p or q is equivalent to 1 mod 4, then one has $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, ie, p is a square root modulo q if and only if q is a square root modulo p.

2 Eisenstein's Proof of Quadratic Reciprocity

2.1 Preliminaries

Theorem 2.1 (Quadratic Reciprocity) *Let p and q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{2.3}$$

As p and q are distinct, odd primes, both $\left(\frac{q}{p}\right)$ and $\left(\frac{p}{q}\right)$ are ± 1. The difficulty is figuring out which signs are correct, and how the two signs are related.

We use Euler's Criterion, proved previously:

Lemma 2.2 (Euler's Criterion)

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \ \textit{mod}\ p. \tag{2.4}$$

The idea behind Eisenstein's proof is as follows: $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)$ is -1 to a power. Further, we only need to determine the power mod 2. Eisenstein shows many expressions are equivalent, mod 2, to this power. Eventually, we arrive at an expression which is trivial to calculate (mod 2).

2.2 First Stage

Consider all even multiples of q by an $a \leq p-1$: $\{2q, 4q, 6q, \ldots, (p-1)q\}$. Denote a generic multiple by aq. Recall $[x]$ is the greatest integer less than or equal to x. By integer division,

$$aq = \left[\frac{aq}{p}\right] p + r_a,\ 0 \leq r_a < p-1. \tag{2.5}$$

Thus, r_a is the least non-negative number equivalent to qa mod p.

The numbers $(-1)^{r_a} r_a$ are equivalent to even numbers in $\{0, \ldots, p-1\}$. If r_a is even this is clear; if r_a is odd, then $(-1)^{r_a} r_a \equiv p - r_a$ mod p, and as p and r_a are odd, this is even.

Lemma 2.3 *If* $(-1)^{r_a} r_a \equiv (-1)^{r_b} r_b$, *then* $a = b$.

Proof: We quickly get $\pm r_a \equiv r_b$ mod p. If the plus sign holds, then $r_a \equiv r_b$ mod p implies $qa \equiv qb$ mod p. As q is invertible mod p, we get $a \equiv b$ mod p, which yields $a = b$ (as a and b are even integers between 0 and $p-1$).

If the minus sign holds, then $r_a + r_b \equiv 0$ mod p, or $qa + qb \equiv 0$ mod p. Multiplying by q^{-1} mod p now gives $a + b \equiv 0$ mod p. As a and b are even integers between 0 and $p-1$, $0 < a + b \leq 2(p-1)$. The only integer strictly between 0 and $2p$ which is equivalent to 0 mod p is p; however, p is odd and $a+b$ is even. Thus, the minus sign cannot hold, and the elements are all distinct. $\Box$.

Lemma 2.4

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{a\,even} r_a}. \tag{2.6}$$

Proof: For each even a, $qa \equiv r_a$ mod p. Thus, mod p:

$$\begin{aligned}
\prod_{a \text{ even}} qa &\equiv \prod_{a \text{ even}} r_a \\
q^{\frac{p-1}{2}} \prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} r_a \\
\left(\frac{q}{p}\right) \prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} r_a,
\end{aligned} \tag{2.7}$$

where the above follows from the fact that we have $\frac{p-1}{2}$ choices for an even a (to get $q^{\frac{p-1}{2}}$ and Euler's Criterion (to replace $q^{\frac{p-1}{2}}$ with $\left(\frac{q}{p}\right)$).

As a ranges over all even number from 0 to $p-1$, so too do the numbers $(-1)^{r_a} r_a$ mod p. Thus, mod p,

$$\begin{aligned}
\prod_{a \text{ even}} a &\equiv \prod_{a \text{ even}} (-1)^{r_a} r_a \\
\prod_{a \text{ even}} a &= (-1)^{\sum_{a \text{ even}} r_a} \prod_{a \text{ even}} r_a.
\end{aligned} \tag{2.8}$$

Combining gives

$$\left(\frac{q}{p}\right)(-1)^{\sum_{a \text{ even}} r_a} \prod_{a \text{ even}} r_a \equiv \prod_{a \text{ even}} r_a. \tag{2.9}$$

As each r_a is invertible mod p, so is the product. Thus,

$$\left(\frac{q}{p}\right)(-1)^{\sum_{a \text{ even}} r_a} \equiv 1 \bmod p. \tag{2.10}$$

As $\left(\frac{q}{p}\right)$ is its own inverse, the Lemma now follows by multiplying both sides by $\left(\frac{q}{p}\right)$. $\square$.

Therefore, it is sufficient to determine $\sum_{a \text{ even}} r_a \bmod 2$.

We make one last simplification. By integer division, we have

$$\begin{aligned}
\sum_{a \text{ even}} qa &= \sum_{a \text{ even}} \left(\left[\frac{qa}{p}\right]p + r_a\right) \\
&= \sum_{a \text{ even}} \left[\frac{qa}{p}\right]p + \sum_{a \text{ even}} r_a.
\end{aligned} \tag{2.11}$$

As we are summing over even a, the Left Hand Side above is even. Thus, the Right Hand Side is even, so

$$\begin{aligned}
\sum_{a \text{ even}} \left[\frac{qa}{p}\right]p &\equiv \sum_{a \text{ even}} r_a \bmod 2 \\
p\sum_{a \text{ even}} \left[\frac{qa}{p}\right] &\equiv \sum_{a \text{ even}} r_a \bmod 2 \\
\sum_{a \text{ even}} \left[\frac{qa}{p}\right] &\equiv \sum_{a \text{ even}} r_a \bmod 2,
\end{aligned} \tag{2.12}$$

where the last line follows from the fact that p is odd, so mod 2, dropping the factor of p from the Left Hand Side doesn't change the parity.

We have shown

Lemma 2.5 *It is sufficient to calculate* $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$

2.3 Second Stage

Consider the rectangle with vertices at $A = (0,0)$, $B = (p,0)$, $C = (p,q)$ and $D = (0,q)$. The upward slopping vertical is given by the equation $y = \frac{q}{p}x$. As p and q are distinct odd primes, there are no pairs of integers (x,y) on the line AC.

We now interpret $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$. Consider the vertical line with x coordinate a. Then $\left[\frac{qa}{p}\right]$ gives the number of pairs (x, y) with x-coordinate equal to a and y-coordinate an integer at most $\left[\frac{qa}{p}\right]$. Thus, $\sum_{a \text{ even}} \left[\frac{qa}{p}\right]$ is the number of integer pairs (in the rectangle $ABCD$) with even x-coordinate that are below the line AC.

We add some additional points: $E = (\frac{p}{2}, 0)$, $F = (\frac{p}{2}, \frac{q}{2})$, $G = (0, \frac{q}{2})$ and $H = (\frac{p}{2}, q)$. We prove

Lemma 2.6 *The number of integer pairs under the line AC (inside the rectangle) with even x-coordinate is congruent mod 2 to the number of integer pairs under the line AF.*

Let $a > \frac{p}{2}$ be an even integer. The integer pairs on the line $x = a$ are $(a, 0)$, $(a, 1), \ldots, (a, q)$. There are $q + 1$ pairs. As q is odd, there are an even number of integer pairs on the line $x = a$. As there are no integer pairs on the line AC, for a fixed $a > \frac{p}{2}$, mod 2 there are the same number of integer pairs *above* AC as there are *below* AC.

Further, the number of integer pairs *above* AC is equivalent mod 2 to the number of integer pairs below AF on the line $x = p - a$. To see this, consider the map which takes (x, y) to $(p - x, q - y)$. As $a > \frac{p}{2}$ and is even, $p - a < \frac{p}{2}$ and is odd. Further, every odd $a < \frac{p}{2}$ is hit (given $a_{odd} < \frac{p}{2}$, start with the even number $p - a_{odd} > \frac{p}{2}$).

Let $\#FCH_{even}$ be the number of integer pairs (x, y) in triangle FCH with x even.

Let $\#EBCH$ be the number of integer pairs in the rectangle $EBCH$; $\#EBCH \equiv 0 \bmod 2$ (we've shown each vertical line has an even number of pairs).

Let $\#AFE_{even}$ be the number of integer pairs (x, y) in the triangle AFE with x even, and let $\#AFE$ be the number of integer pairs in the triangle AFE.

We need to calculate $\sum_{a \text{ even}} \left[\frac{qa}{p}\right] \bmod 2$:

$$\begin{aligned} \sum_{a \text{ even}} \left[\frac{qa}{p}\right] &= \#AFE_{even} + \#EBCH - \#FCH \\ &\equiv \#AFE_{even} + \#EBCH + \#FCH \\ &= \#AFE_{even} + \#FCH + \#EBCH \\ &= \#AFE + \#EBCH \\ &= \#AFE. \end{aligned} \tag{2.13}$$

Therefore, $\mu = \sum_{a \text{ even}} \left[\frac{qa}{p}\right] \equiv \#AFE \bmod 2$, and we have

$$\left(\frac{q}{p}\right) = (-1)^{\mu}. \tag{2.14}$$

Reversing the rolls of p and q, we see that

$$\left(\frac{p}{q}\right) = (-1)^{\nu}, \tag{2.15}$$

where $\nu \equiv \#AFG \bmod 2$, with $\#AFG$ equal to the number of integer pairs in the triangle AFG.

Now, $\mu + \nu = \#AFE + \#AFG$, which is the number of integer pairs in the rectangle $AEFG$. There are $\frac{p-1}{2}$ choices for x and $\frac{q-1}{2}$ choices for y, giving $\frac{p-1}{2}\frac{q-1}{2}$ pairs of integers in the rectangle $AEFG$.

Thus,

$$\begin{aligned}
\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) &= (-1)^{\mu+\nu} \\
&= (-1)^{\#AFE+\#AFG} \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}, \qquad (2.16)
\end{aligned}$$

which completes the proof of Quadratic Reciprocity. $\square$.