

QUADRATIC RECIPROCITY

JORDAN SCHESSLER

Abstract. *The goals of this project are to have the reader(s) gain an appreciation for the usefulness of Legendre symbols and ultimately recreate Eisenstein's slick proof of Gauss's Theorema Aureum of quadratic reciprocity.*

1. QUADRATIC RESIDUES AND LEGENDRE SYMBOLS

Definition 0.1. Let $m, n \in \mathbb{Z}$ with $(m, n) = 1$ (recall: the gcd (m, n) is the nonnegative generator of the ideal $m\mathbb{Z} + n\mathbb{Z}$). Then m is called a **quadratic residue mod n** if $m \equiv x^2 \pmod{n}$ for some $x \in \mathbb{Z}$, and m is called a **quadratic nonresidue mod n** otherwise.

Prove the following remark by considering the kernel and image of the map $x \mapsto x^2$ on the group of units $(\mathbb{Z}/n\mathbb{Z})^\times = \{m + n\mathbb{Z} : (m, n) = 1\}$.

Remark 1. For $2 < n \in \mathbb{N}$ the set $\{m + n\mathbb{Z} : m \text{ is a quadratic residue mod } n\}$ is a subgroup of the group of units of order $\leq \varphi(n)/2$ where $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ is the Euler totient function. If $n = p$ is an odd prime, then the order of this group is equal to $\varphi(p)/2 = (p - 1)/2$, so the equivalence classes of all quadratic nonresidues form a coset of this group.

Definition 1.1. Let p be an odd prime and let $n \in \mathbb{Z}$. The **Legendre symbol** (n/p) is defined as

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a quadratic residue mod } p \\ -1 & \text{if } n \text{ is a quadratic nonresidue mod } p \\ 0 & \text{if } p|n. \end{cases}$$

The law of quadratic reciprocity (the main theorem in this project) gives a precise relationship between the "reciprocal" Legendre symbols (p/q) and (q/p) where p, q are distinct odd primes. We'll prove quadratic reciprocity in section 2, and we'll see applications thereof to Diophantine equations and computations of Legendre symbols in section 3. In the meantime, use remark 1 to establish the following proposition.

Proposition 2. *Let p be an odd prime and let $m, n \in \mathbb{Z}$. Then*

$$(1.1) \quad \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right)$$

and

$$(1.2) \quad m \equiv n \pmod{p} \Rightarrow \left(\frac{m}{p}\right) = \left(\frac{n}{p}\right).$$

Show the following lemma by recalling that an element of a finite group has order dividing the size of the group.

Lemma 3 (Fermat's Little Theorem). *Let p be an odd prime and let $n \in \mathbb{Z}$ with $(n, p) = 1$. Then*

$$(1.3) \quad n^{p-1} \equiv 1 \pmod{p}.$$

Now apply lemma 3 to get the proceeding fundamental result about Legendre symbols (Hint: factor $n^{p-1} - 1 = (n^{(p-1)/2} - 1)(n^{(p-1)/2} + 1)$ and use the fact that the group of units of a finite field is cyclic).

Theorem 4 (Euler's Criterion). *Let p be an odd prime and let $n \in \mathbb{Z}$ with $(n, p) = 1$. Then*

$$(1.4) \quad \left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}.$$

Next, plug in $n = -1$ into theorem 4 to get the following immediate consequence.

Corollary 5. *Let p be an odd prime. Then*

$$(1.5) \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

2. QUADRATIC RECIPROCITY

Flesh out the sketch of the proof for the crucial lemma which follows where for $x \in \mathbb{R}$ we take $\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leq x\}$

Lemma 6 (Eisenstein). *Let p be an odd prime and let $n \in \mathbb{Z}$ with $(n, p) = 1$. Then*

$$(2.1) \quad \left(\frac{n}{p}\right) = (-1)^s$$

where

$$s = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2kn}{p} \right\rfloor.$$

Sketch. For each $k \in \{1, \dots, (p-1)/2\}$ define

$$r_k := 2kn - p \left\lfloor \frac{2kn}{p} \right\rfloor \equiv \left\lfloor \frac{2kn}{p} \right\rfloor \pmod{2}.$$

Then

$$\begin{aligned} n^{(p-1)/2} \prod_{k=1}^{(p-1)/2} (2k) &\equiv \prod_{k=1}^{(p-1)/2} r_k = (-1)^{\sum_k r_k} \prod_{k=1}^{(p-1)/2} [(-1)^{r_k} r_k] \\ &\equiv (-1)^{\sum_k r_k} \prod_{k=1}^{(p-1)/2} (2k) \pmod{p}, \end{aligned}$$

so by theorem 4 we get

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \equiv (-1)^{\sum_k r_k} = (-1)^s \pmod{p}.$$

□

Deduce the following corollary which is traditionally established with a result called Gauss's lemma.

Corollary 7. *Let p be an odd prime. Then*

$$(2.2) \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. Note that

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{4k}{p} \right\rfloor = \#\{k \in \mathbb{N} : p/4 < k \leq p/2\} = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor,$$

so if $p = 8m \pm 1$, then

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{4k}{p} \right\rfloor = \lfloor 4m \pm 1/2 \rfloor - \lfloor 2m \pm 1/4 \rfloor = 2m \equiv 0 \equiv \frac{p^2 - 1}{8} \pmod{2},$$

and if $p = 8m \pm 3$, then

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{4k}{p} \right\rfloor = \lfloor 4m \pm 3/2 \rfloor - \lfloor 2m \pm 3/4 \rfloor = 2m \pm 1 \equiv 1 \equiv \frac{p^2 - 1}{8} \pmod{2}.$$

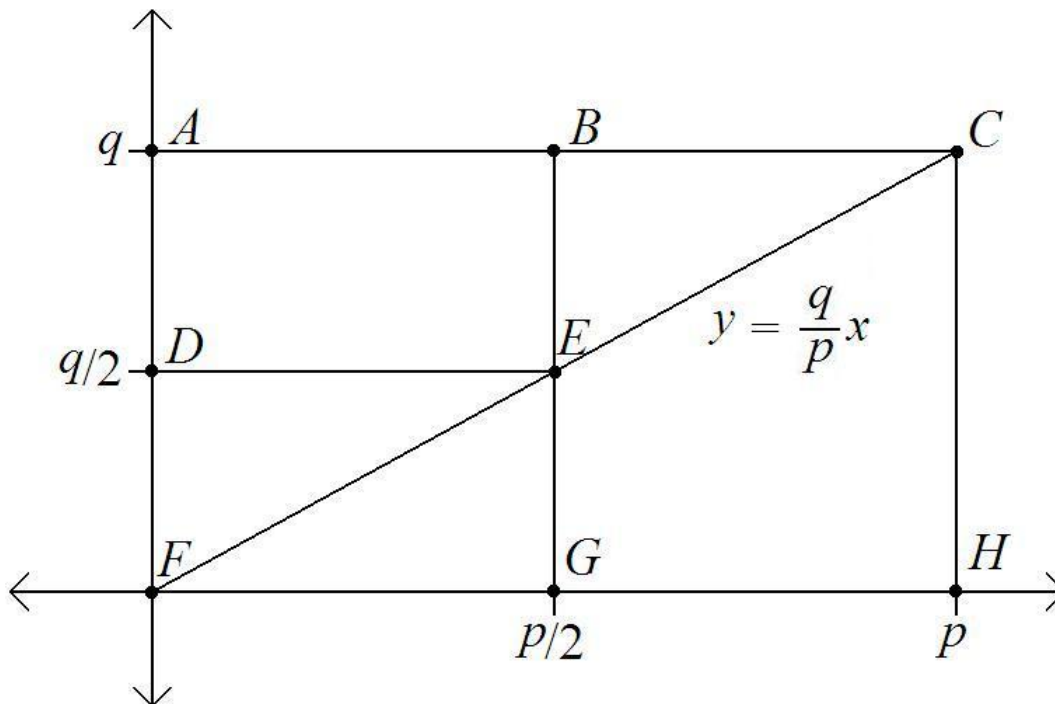
□

Finally, fill in the details of the following proof (originally suggested by Eisenstein) of the quadratic reciprocity theorem (originally proved by Gauss).

Theorem 8 (Quadratic Reciprocity). *Let p, q be distinct odd primes. Then*

$$(2.3) \quad \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{[(p-1)/2][(q-1)/2]}.$$

Sketch. Consider the following diagram in the (x, y) -plane.



Let μ be the number of lattice points (i.e., points in the plane with integer coefficients) in the interior of the triangle EFG . Note that number of lattice points with odd x -coordinates

in EFG is equal to the number of lattice points with even x -coordinates in BCE , which has the same parity as the number of lattice points with even x -coordinates in $CEGH$. Hence

$$\mu \equiv \#\{P : P \text{ is a lattice point in } CFH \text{ and has even } x\text{-coordinate}\} \pmod{2},$$

but for each positive integer $m < p$, the number of lattice points in CFH with x -coordinate m is $\lfloor mq/p \rfloor$, so

$$\mu \equiv \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2kq}{p} \right\rfloor \pmod{2}.$$

Therefore lemma 6 now implies

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

A symmetric argument shows that

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

where ν is the number of lattice points in DEF . Thus the statement follows from the observation

$$\mu + \nu = \#\{P : P \text{ is a lattice point in } DEGF\} = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

□

3. EXAMPLES AND APPLICATIONS

Remark 9. For a fixed odd prime p , we can reasonably obtain the quadratic residues mod p by simply squaring the integers $1, \dots, (p-1)/2$ and reducing modulo p . On the other hand, the inverse problem of determining those primes p for which a fixed integer n is a quadratic residue mod p requires reciprocity as the next example illustrates.

Example 10. To determine all odd primes p for which 5 is a quadratic residue mod p we note that

$$\left(\frac{p}{5}\right) \left(\frac{5}{p}\right) = (-1)^{[(p-1)/2][(5-1)/2]} = 1,$$

so $(5/p) = 1 \Leftrightarrow (p/5) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{5}$.

Exercise 11. Determine all odd primes p for which $n = 3$ is a quadratic residue mod p . Do the same for $n = 7$ and $n = 6$.

The reciprocity law can also be utilized to compute Legendre symbols with “large” arguments as seen in the following example.

Example 12. Suppose we wanted to compute $(21/53)$. We could start squaring the integers $1, \dots, 26$ and reducing modulo 53, but this would be laborious. It’s easier to accomplish this by repeated applications of theorem 8 and proposition 2; e.g.,

$$\begin{aligned} \left(\frac{21}{53}\right) &= \left(\frac{3}{53}\right) \left(\frac{7}{53}\right) = \left(\frac{53}{3}\right) (-1)^{1 \cdot 26} \left(\frac{53}{7}\right) (-1)^{3 \cdot 26} = \left(\frac{2}{3}\right) \left(\frac{4}{7}\right) \\ &= (-1) \left(\frac{2}{7}\right)^2 = (-1)(-1)^{(7^2-1)/4} = (-1)(-1)^{12} = -1. \end{aligned}$$

Exercise 13. Use the techniques of the above example to compute (143/409).

Another use of quadratic reciprocity includes (as one would expect) finding integer solutions to degree two polynomial equations. Prove the next lemma, which follows easily from the reciprocity law.

Lemma 14. *Let p, q be distinct odd primes with $p \equiv 3 \equiv q \pmod{4}$. Then the equation*

$$(3.1) \quad x^2 - qy^2 = p$$

has no solutions in integers x, y .

We can in turn apply this lemma along with a little algebraic number theory to deduce the following theorem. Read the outline of the proof and try to justify the tools used.

Theorem 15. *Let p be a prime. Then $p \equiv 1 \pmod{12}$ if and only if the equation*

$$(3.2) \quad x^2 - 3y^2 = p$$

has a solution in integers x, y .

Proof. (\Leftarrow) If equation 3.2 has integer solutions, then $p \equiv 1 \pmod{4}$ by the contrapositive of lemma 14, but also $p \equiv 1 \pmod{3}$ since p is a quadratic residue mod 3, whence $(3, 4) = 1$ implies $p \equiv 1 \pmod{12}$ as needed.

(\Rightarrow) Now suppose $p \equiv 1 \pmod{12}$. Then 3 is a quadratic residue modulo p by exercise 11, so there are integers m, n such that

$$mp = n^2 - 3 = (n - \sqrt{3})(n + \sqrt{3}).$$

Thus p divides the product $(n - \sqrt{3})(n + \sqrt{3})$ in the ring $\mathbb{Z}[\sqrt{3}]$, but p does not divide $n \pm \sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$, so p is not a prime element in $\mathbb{Z}[\sqrt{3}]$. Hence p is not an irreducible element in $\mathbb{Z}[\sqrt{3}]$ since $\mathbb{Z}[\sqrt{3}]$ is a UFD, so there are $x, y, s, t \in \mathbb{Z}$ such that neither $x + y\sqrt{3}$ nor $s + t\sqrt{3}$ is a unit in $\mathbb{Z}[\sqrt{3}]$ with

$$p = (x + y\sqrt{3})(s + t\sqrt{3}).$$

Moreover, the norm map $N : \mathbb{Z}[\sqrt{3}] \rightarrow \mathbb{Z}$ given by $a + b\sqrt{3} \mapsto a^2 - 3b^2$ is multiplicative, so

$$p^2 = N(p) = (x^2 - 3y^2)(s^2 - 3t^2),$$

but this implies $x^2 - 3y^2 = \pm p$ since units have norm ± 1 and p is a prime in \mathbb{Z} . Therefore $p = x^2 - 3y^2$ since otherwise $p = 3y^2 - x^2 \equiv -1 \pmod{3}$, which is a contradiction. \square

REFERENCES

- [1] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2th ed., Springer, 2000.
- [2] Reinhard C. Laubenbacher and David J. Pengelley, *Eisenstein's Misunderstood Geometric Proof of the Quadratic Reciprocity Theorem*, The College Mathematics Journal, Vol. 25, No. 1, (Jan., 1994), pp. 29-34.