University of Chicago

Elementary Number Theory

Several Proofs of the Law of Quadratic Reciprocity

Andrew Dong

Abstract

In this paper we will discuss the law of quadratic reciprocity and several proofs of it primarily using tools from elementary number theory. Namely, we will be considering Gotthold Eisenstein's proof using counting of lattice points and Yegor Ivanovich Zolotarev's lemma which allows for application of the Chinese remainder theorem. We will also provide background on the history of the theorem and its importance to the field of number theory.

supervised by
Professor Ngo Bao Chau
special thanks to Minh-Tam Trinh

November 19, 2015

Introduction

The Law of Quadratic Reciprocity is a theorem related to modular arithmetic where the restrictions for solvability of quadratic equations modulo prime numbers can be found. In particular, the Law of Quadratic Reciprocity states that

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

where p and q are odd prime numbers and $\frac{p}{q}$ denotes the Legendre symbol (which we will discuss in a further section).

The Law of Quadratic Reciprocity makes it possible to determine whether any quadratic equation $x^2 \equiv a$ mod (p) has a solution when p is an odd prime.

The theorem was first conjectured by Leonhard Euler and Adrien-Marie Legendre, though it was only proved later by Carl Freidrich Gauss in the *Disquisitiones Arithmeticae*. There are now many proofs available for the Law of Quadratic Reciprocity. This paper will closely examine two put forth by Eisenstein and Zolotarev.

Legendre Symbol

The Legendre symbol is a multiplicative function with values 1, -1, and 0 that is a quadratic character modulo a prime number p. It can be thought of as an arithmetic function f(n) of a positive integer n such that f(Id) = Id and for gcd(a,b) = 1, f(ab) = f(a)f(b). The value of a Legendre symbol on a nonzero quadratic residue mod p is 1 and on a non-quadratic residue is -1, whereas it's value on zero is 0.

It is formally defined as follows:

Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p defined as

$$\frac{a}{p} = \begin{cases} 1 \text{ if a is a quadratic residue modulo p and a} \neq 0 \\ \text{-1 if a is a quadratic non-residue modulo p,} \\ 0 \text{ if a} \equiv 0 \text{ mod(p)} \end{cases}$$

Zolotarev's Lemma

An important lemma regarding the Legendre symbol is Zolotarev's Lemma. It states that the Legendre symbol $\frac{a}{p}$ for an integer a modulo an odd prime number p where p does not divide a can be computed as the sign of a permutation.

Formally, it claims that

$$(\frac{a}{p}) = \epsilon(\pi_a)$$

where ϵ signifies the signature of a permutation and π_a is the permutation of the nonzero residue classes mod p induced by multiplication by a.

Proof 1

For any finite group G of order n, we can determine the signature of the permutation π_g made by left-multiplication by the element g of G. The permutation π_g will be even, unless there are an odd number of orbits of even size. Suppose n is even. Now, in order for π_g to be an odd permutation, if g has order k then $\frac{n}{k}$ must be odd. This is equivalent to saying that the subgroup $< g >$ must have an odd index.

Applying this to the group of nonzero numbers mod p, which is a cyclic group of order p-1, we see that the jth power of a primitive root modulo p has as its index the gcd, i = (j,p-1).

Thus, for a nonzero number mod p to be a quadratic non-residue p must be an odd power of a primitive root. □

From the proof of Zolotarev's lemma, we come to a better understanding of it's statement. The lemma allows us to know that i is odd when j is odd, and j is odd when i is odd.

Another proof of Zolotarev's lemma can be deduced from Gauss's lemma.

Recall that Gauss's lemma makes the claim that for any odd prime p, if a is an integer that is coprime to a, then the integer multiplies of a up to $\frac{p-1}{2}$a and their least positive residues modulo p are all distinct. Furthermore, if n is the number of residues greater than $\frac{p}{2}$, then

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

where $\frac{a}{p}$ is the Legendre symbol.

We now consider a proof of Zolotarev's Lemma using Gauss's lemma in an attempt to bridge the connection between these two claims.

Proof 2 Consider the Legendre symbol $\frac{a}{p}$ and the set 1,2,...,p-1 arranged as a matrix of two rows such that the sum of two elements in each column is zero mod (p).

Now apply a permutation f: $x \to ax$ mod (p).

Following our permutation we will see that the columns still have the property that the sum of any two elements in a column is zero mod (p).

Now apply a second permutation g which inverts any column in which the upper member before the application of permutation f was a lower member.

To return to the original matrix we apply a third permutation h, where $h^{-1} = $ fg. h is an even permutation.

Recall the statement's of Zolotarev and Gauss's lemmas.

Zolotarev's lemma makes the claim that $\frac{a}{p} = 1$ if and only if an initial permutation f is even.

Gauss's lemma states that $\frac{a}{p} = 1$ if and only if g is an even permutation.

Since h is an even permutation, we have that the two lemmas are equivalent. □

We should now have sufficient prerequisites for understanding the tools used in Eisenstein and Zolotarev's proofs of the Quadratic Reciprocity theorem. Any further clarification will be brought up as needed. We begin with a look at Eisenstein's proof.

Eisenstein's Proof of Quadratic Reciprocity

Recall that in order to show the quadratic reciprocity theorem we must show that for p and q distinct odd primes we have

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

Proof

Eisenstein asks us to consider a set a = 2,4,6,...,p-1. He then defines r as the remainder mod (p) of an arbitrary multiple qa.

We should have that the the list of numbers $(-1)^r r$ agrees with the list of numbers a up to multiples of p since each number $(-1)^r r$ has even least positive residue. If ∀ q, a, $a\prime$ we have

$$(-1)^{qa}qa \equiv (-1)^{qa\prime)qa\prime}$$

we must have it that $a \equiv \pm a\prime$. Since the elemnts of a are each distinct, we will have that $a + a\prime \equiv 0$ which is impossible since $0 < a + a\prime < 2p$ and $a_a\prime$ is even.

We see that

$$q^{\frac{p-1}{2}} \prod a \equiv \prod r \text{mod p and} \prod a \equiv (-1)^{\sum r} \prod r \text{mod p}$$

from which it follows that $q^{\frac{p-1}{2}} \equiv (-1)^{\sum r}$ mod (p). By Euler's Criterion which claims that $(\frac{q}{p}) \equiv q^{\frac{p-1}{2}}$ mod p we have that this results in

$$(\frac{q}{p}) = (-1)^{\sum r}$$

We can see that

$$\sum qa = p \sum [\frac{qa}{p}] + \sum r,$$

where [ ] is the greatest integer function. Since the elements of a are even and p is odd, we get that $\sum r \equiv \sum [\frac{qa}{p}]$. mod (2) and thus

$$(\frac{q}{p}) = (-1)^{\sum \frac{qa}{p}}$$

From here Eisenstein uses a geometric representation of the exponent $\sum \frac{qa}{p}$ in $(\frac{q}{p}) = (-1)^{\sum \frac{qa}{p}}$ to transform it while still maintaining it's equality. Here he uses that the exponent is the number of integer lattice points with even abscissa's lying in the interior triangle which is taken to be one half of a rectangle split by it's diagonal running through the origin. Since the number of lattice points on each abscissa (or point on an axis) is even, the number $[\frac{qa}{p}]$ of lattice points below the diagonal is equal to the number $[\frac{qa}{p}]$ of lattice points above the diagonal. This is also the same as the number of points lying below the diagonal on the odd abscissa p-a.

Since we've found a one-to-one correspondence between even abscissas in the upper and lower triangles (recall our rectangle has been split into two triangles), we now know that $\sum [\frac{qa}{p} \equiv \mu$ mod (2) where μ is the number of points inside a smaller triangle partitioned inside one of our two upper and lower triangles such that μ is has hypotenuse 1/2 that of it's parent triangle. Now we get the equality $\frac{q}{p} = (-1)^{\mu}$

We can follow the logic of this proof with p and q reversed and obtain that $\frac{p}{q} = (-1)^{\hat{\mu}}$ where $\hat{\mu}$ is simply the upper relative of μ. Since we know that the total number of points in our two parent triangles is known to be $\frac{p-1}{2}, \frac{q-1}{2}$ we conclude that

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

.

□

This is quite a beautiful proof, and is even clearer with a pictorial representation.

Quadratic Reciprocity and Zolotarev's Lemma

Proof

Consider the set Z/p = 0,1,...,p-1 where $p > 1$ and is odd. This set has both ring structure and linear ordering. Now suppose that p and q are both odd integers and are relatively prime. Thus by the Chinese remainder theorem ∃ a unique ring isomorphism

$$Z/pq \mapsto Z/pxZ/q$$

If we assign Z/p and Z/q a lexicographic order, then there is also a unique linear isomorphism

$$(Z/pxZ/q)_l \mapsto Z/pq$$

which takes an element $(x, y) \in (Z/pxZ/q)$ to $(qx + y) \in 0, 1, ..., pq - 1$.

From these two isomorphisms we see that the composite α of the functions

$$(Z/pxZ/q) \mapsto Z/pq \mapsto Z/pxZ/q$$

is simply

$$(x, y) \mapsto (qx + y) \mapsto (qx + y, y)$$

.

Therefore we see that α is a juxtaposition of q row permutations each corresponding to a fixed y. The sign of the permutation $x \mapsto qx + y$ is

$$sign((-) + y) * sign(q(-)) = sign(q(-)) = (\frac{q}{\lfloor})$$

Since the permutation (-) + q is even, we have that

$$sign(\alpha) = (\frac{q}{p})^q = (q/p)$$

where the second equation is true since q is odd.

We can now consider the reverse isomorphisms and analyze their composition, let's call it β.

$$(Z/pxZ/q) \mapsto Z/pq \mapsto Z/pxZ/q$$

which takes

$$(x, y) \mapsto (x, x + py)$$

and we can calculate sign(β) = ($\frac{p}{q}$.

Notice that $\beta^{-1} \circ \alpha$ is unique and order preserving, this gives a permutation on the set (Z/p x Z/q) and all that we need to show is that the sign of the permutation is $(-1)^{\frac{p-1}{q-1}}$.

Recall that a permutation σ on a linear ordered set has sign

$$sign(\sigma) = (-1)^{I(\sigma)}$$

where $I(\sigma)$ is the total number of inversions.

Here, we have that $\sigma = \beta^{-1}\alpha$ so we are considering the pair of pairs (i,j)$(i\prime, j\prime)$ where (i,j) < $(i\prime, j\prime)$ in lexicographic ordering but (i,j) > $(i\prime, j\prime)$ in reverse lexicographic ordering. The total number of inversions for which this occurs is

$$I(\sigma) = \frac{p(p-1)}{2} \frac{q(q-1}{2}$$

where

$$(-1)^{I(\sigma} = (-1)^{\frac{p(p-1)}{2} \frac{n(n-1}{2}}$$

Thus we've shown that

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

for p and q distinct odd primes. □

Conclusion

In this paper we have shown two different proofs of the quadratic residue theorem using mostly tools from elementary number theory. In the future it may be interesting to consider other proofs using algebraic number theory. Among these one proof in particular which uses Cyclotomic field setup and the Frobenius automorphism seems promising.

Before ending this paper I would like to thank Minh-Tam Trinh in helping me better understand the relationship between Zolotarev's Lemma and Gauss' Lemma, Franz Lemmermeyer for his book ***Reciprocity Laws: From Euler to Eisenstein***, Kenneth Ireland and Michael Rosen for their book ***A Classical Introduction to Modern Number Theory*** and of course my professor Ngo Bao Chau for his supervision of the paper. Since this paper is still an early draft I hope to in the future clarify my explanations and further explore proofs of the quadratic reciprocity law.