QUADRATIC RECIPROCITY

MARIA CHRYSAFIS

Contents

1. Introduction

Quadratic reciprocity deals with the fundamental question of characterizing which numbers can be expressed as perfect squares under some modulus. That is:

Definition 1.1. We say that an integer a is a quadratic residue modulo n iff there exists an x for which: $x^2 \equiv a \pmod{n}$.

If n is not a prime power, then we can reduce determining if a is quadratic residue to determining if it is a quadratic residue modulo various prime powers. To see this, suppose that $n = n_1 \cdot n_2$, where $\gcd(n_1, n_2) = 1$. Then, a is a quadratic residue modulo n iff it is a quadratic residue modulo n_1 and n_2, by the Chinese Remainder Theorem.
Instead of focusing on prime powers, we'll focus on primes.

Proposition 1.2. *There are $\frac{p-1}{2}$ quadratic residues in the range $[0, p-1] \cap \mathbb{Z}$.*

Proof. Let us imagine the multiset of quadratic residues, taken modulo p: $\{0^2, 1^2, 2^2, 3^2, \ldots, (p-1)^2\}$. We know that we have some repeated elements, namely

$$x^2 \equiv y^2 \implies (x-y)\cdot(x+y) \equiv 0 \implies x \equiv y \text{ or } x \equiv -y.$$

This tells us that the multiset repeats elements x^2 and $(p-x)^2 \equiv x^2$. That is, if p is an odd prime ($p \neq 2$), then each element in the multiset is repeated twice, with the exception if 0^2, which occurs only once. It thereby follows that there must be $\frac{p-1}{2}$ quadratic residues in the range $[0, p-1]$. ■

Definition 1.3. There's a useful notation called the Legendre symbol: $\left(\frac{a}{p}\right)$. It is denoted:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{p}|\text{a} \\ 1 & \text{a is a quadratic residue modulo p.} \\ -1 & \text{a is not a quadratic residue modulo p.} \end{cases}$$

This notation lends way to some interesting properties:

Date: March 20, 2022.

Proposition 1.4 (Euler's Criterion)**.**

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

Proof. It is easy to show that it holds when $p = 2$. In the ensuing paragraphs, we will assume that p is an odd prime. Trivially, if $p|a$, then we know that $a^{(p-1)/2} \equiv 0 \pmod{p}$ for all primes p. Now suppose that a is a quadratic residue modulo p:

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

We know by Fermat's Little Theorem that if $\gcd(x, p) = 1$, then $x^{p-1} \equiv 1 \pmod{p}$. Hence it follows that Euler's criterion holds for quadratic residues.
What about for quadratic nonresidues? We know that $a^{(p-1)/2} \equiv 1$ for exactly $\frac{p-1}{2}$ values of $a \in [1, p-1]$ and likewise, $a^{(p-1)/2} \equiv -1$ for $\frac{p-1}{2}$ values of $a \in [1, p-1]$. Since, by 1.2, there are $\frac{p-1}{2}$ nonresidues and residues and since Euler's crition holds for quadratic residues, it must be the case that $a^{(p-1)/2} \equiv -1$ for nonresidues. Thus, Euler's criterion stand true. ∎

There are two immediate and important consequences of this:

Corollary 1.5. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Corollary 1.6. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *if* $a \equiv b \pmod{p}$.

2. Gauss Sums Proof

Perhaps the most elementary and well-known proof of Quadratic reciprocity utilizes Gauss sums. We define:

Definition 2.1. $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta_p^{at}$.

For our purposes, ζ_p is a primitive pth root of unity. It doesn't matter which root of unity exactly, so you can assume $\zeta_p = e^{2\pi i/p}$ if you prefer.

Lemma 2.2. $g_a = \left(\frac{a}{p}\right) g_1$.

Proof.

$$\left(\frac{a}{p}\right) g_1 = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right)\left(\frac{a}{p}\right) \zeta_p^t = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta_p^t.$$

Instead of iterating over t, we can iterate over at, equivalently:

$$\left(\frac{a}{p}\right) g_1 = \sum_{t=0}^{p-1} \left(\frac{at^2}{p}\right) \zeta_p^{at} = \sum_{t=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{t^2}{p}\right) \zeta_p^{at} = \sum_{t=0}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{at} = g_a,$$

from which the desired follows. ∎

Lemma 2.3. $g_1^2 = (-1)^{(p-1)/2}\, p$.

Proof.

$$g_1^2 = \sum_{s=0}^{p-1}\sum_{r=0}^{p-1}\left(\frac{r}{p}\right)\left(\frac{s}{p}\right)\zeta_p^{s+r} = \sum_{s=1}^{p-1}\sum_{r=1}^{p-1}\left(\frac{rs}{p}\right)\zeta_p^{s+r}.$$

Instead of iterating over r, we can iterate over sr:

$$g_1^2 = \sum_{s=1}^{p-1}\sum_{r=1}^{p-1}\left(\frac{s^2r}{p}\right)\zeta_p^{s+sr} = \sum_{s=1}^{p-1}\sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\zeta_p^{s+sr} = \sum_{r=1}^{p-1}\left(\frac{r}{p}\right)\sum_{s=1}^{p-1}\zeta_p^{s(r+1)}.$$

We know that the sum of the roots of unity is 0. Therefore,

$$g_1^2 = (p-1)\left(\frac{p-1}{p}\right) - \sum_{r=1}^{p-2}\left(\frac{r}{p}\right) = p(-1)^{(p-1)/2},$$

from which the desired follows. ■

Theorem 2.4 (Quadratic Reciprocity Theorem)**.** *For odd primes p, q:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Proof. Notice that:

$$g_1^{q-1} = \left(\left(\frac{p-1}{p}\right)p\right)^{(q-1)/2} \equiv \left(\frac{\left(\frac{p-1}{p}\right)p}{q}\right) \pmod q.$$

We also have another expression for g_1^q straight from the definition of g_1 :

$$g_1^q = \left(\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta_p^t\right)^q = \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)^q\zeta_p^{tq} \equiv g_q \pmod q.$$

Putting this all together, we have that:

$$g_1\left(\frac{\left(\frac{p-1}{p}\right)p}{q}\right) \equiv g_q \equiv \left(\frac{q}{p}\right)g_1 \pmod q.$$

It thereby follows that:

$$\left(\frac{\left(\frac{p-1}{p}\right)p}{q}\right) \equiv \left(\frac{q}{p}\right) \Longrightarrow \left(\frac{p}{q}\right)\left(\frac{\left(\frac{p-1}{p}\right)}{q}\right) \equiv \left(\frac{q}{p}\right) \Longrightarrow \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

The Quadratic Reciprocity theorem follows. ■

3. Evaluating the Sign of the Gauss Sum

Recall earlier that we found g_1^2, but we were unable to find g_1 itself (that is, evaluate the sign of g_1). To do this, we note that we can instead find $\sum_{i=0}^{n-1}\zeta_n^{i^2}$. This is precisely the trace of the matrix $\mathbf{A}$ formed by:

$$a_{i,j} = \zeta_n^{ij}.$$

To evaluate the trace, we will find the eigenvalues and their multiplicities of the matrix $\mathbf{A}$. Before, we start, some preliminaries:

Lemma 3.1. $\prod_{s=1}^{n-1}(1-\zeta_n^s)=n$.

Proof. Recall that:

$$\prod_{s=0}^{n-1}(x-\zeta_n^s)=x^n-1,$$

by the definition of roots of unity. As an immediate consequence, we know that:

$$\prod_{s=1}^{n-1}(x-\zeta_n^s)=\frac{x^n-1}{x-1}=\sum_{i=0}^{n-1}x^i.$$

If we let $x=1$, then we see that:

$$\prod_{s=1}^{n-1}(1-\zeta_n^s)=n.$$

■

Lemma 3.2. $(\det(\mathbf{A}))^2=(-1)^{n(n-1)/2}\,n^n$.

Proof. Since the rows of $\mathbf{A}$ are geometric series, $\mathbf{A}$ is a Vandermonde matrix and therefore we can compute the Vandermonde determinant. It immediately follows that:

$$\det(\mathbf{A})=\prod_{r=0}^{n-1}\prod_{s=r+1}^{n}(\zeta_n^r-\zeta_n^s).$$

We'd like r,s to be symmetrical, that way the expression is more workeable. This motivates the idea to work with $(\det(\mathbf{A}))^2$:

$$\begin{aligned}(\det(\mathbf{A}))^2&=(-1)^{n(n-1)/2}\prod_{r=0}^{n-1}\prod_{s\neq r}(\zeta_n^r-\zeta_n^s)\\&=(-1)^{n(n-1)/2}\prod_{u=0}^{n-1}\zeta_n^u\prod_{v\neq 0}(1-\zeta_n^v).\end{aligned}$$

By 3.1, we can reduce the expression to the following:

$$(-1)^{n(n-1)/2}\prod_{u=0}^{n-1}n\zeta_n^u=(-1)^{n(n-1)/2}n^n.$$

from which the desired follows. ■

However, crucially, the sign of the determinant remains unknown. To deduce the sign, we will need to utilize a new method.

Proposition 3.3. *Assuming n is odd,* $\prod_{r=0}^{n-1}\prod_{s=r+1}^{n}\eta_n^{r+s}=1$.

Proof.

$$\prod_{r=0}^{n-1}\prod_{s=r+1}^{n}\eta_n^{r+s}=\prod_{s=0}^{n-1}\prod_{r=0}^{s-1}\eta_n^{r+s}=\prod_{s=0}^{n-1}\eta_n^{s^2+s\cdot(s-1)/2}=\prod_{s=0}^{n-1}\eta_n^{n(n-1)^2/2}.$$

Since n is odd, this evaluates to 1, as per the desired. ■

Lemma 3.4. *When n is odd,* $\det(\mathbf{A})=i^{n(n-1)/2}n^{n/2}$.

Proof. Recall, as before that

$$\det(\mathbf{A}) = \prod_{r=0}^{n-1} \prod_{s=r+1}^{n} \left(\zeta_n^r - \zeta_n^s\right).$$

If we let $\eta_n = e^{\pi i/n}$, then we have:

$$\begin{aligned}\det(\mathbf{A}) &= \prod_{r=0}^{n-1} \prod_{s=r+1}^{n} \left(\eta_n^{2r} - \eta_n^{2s}\right) \\ &= \prod_{r=0}^{n-1} \prod_{s=r+1}^{n} \left(\eta_n^{r+s}\left(\eta_n^{r-s} - \eta_n^{s-r}\right)\right).\end{aligned}$$

We know that $e^x - e^{-x} = \cos(x) + i\sin(x) - \cos(-x) - i\sin(-x) = 2i\sin(x)$. Therefore, we can reduce the expression to:

$$\det(\mathbf{A}) = \prod_{r=0}^{n-1} \prod_{s=r+1}^{n} \eta_n^{r+s} \cdot 2i\sin\left(\frac{(r-s)\pi}{n}\right).$$

Using 3.3, we can reduce it to:

$$\det(\mathbf{A}) = i^{n(n-1)/2} \prod_{r=0}^{n-1} \prod_{s=r+1}^{n} 2\sin\left(\frac{(r-s)\pi}{n}\right).$$

We already know the square of $\det(\mathbf{A})$, so we don't need to evaluate the inner summand. Instead, we can immediately deduce that $\det(\mathbf{A}) = i^{n\cdot(n-1)/2} n^{n/2}$, since we know that the inner expression is positive. ■

We want to find the trace of $\mathbf{A}$.

Lemma 3.5. *For odd n, $|tr(\mathbf{A})|^2 = n$.*

Proof. We know that, by definition,

$$\operatorname{tr}(\mathbf{A}) = \sum_{r=0}^{n-1} \zeta_n^{r^2} \Longrightarrow \operatorname{tr}(\mathbf{A})^2 = \sum_{r=0}^{n-1} \sum_{s=0}^{n-1} \zeta_n^{r^2+s^2}.$$

Since the sum of quadratic residues equals the sum of nonquadratic residues and $\left(\frac{-p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)$:

$$\operatorname{tr}(\mathbf{A}) = \sum_{r=0}^{n-1} \sum_{s=0}^{n-1} \zeta_n^{r^2-s^2} = \sum_{r=0}^{n-1} \sum_{s=0}^{n-1} \zeta_n^{(r+s)(r-s)} = \sum_{r=0}^{n-1} \sum_{s=0}^{n-1} \zeta_n^{r^2+2rs},$$

if we iterate over $r+s$ instead. It follows that:

$$\operatorname{tr}(\mathbf{A}) = \sum_{r=0}^{n-1} \zeta_n^{r^2} \sum_{s=0}^{n-1} \zeta_n^{2rs} = n + \sum_{r=1}^{n-1} \zeta_n^{r^2} \sum_{s=0}^{n-1} \zeta_n^{2rs} = n.$$

■

We would like to determine the coefficient of $\operatorname{tr}(\mathbf{A})$:

Lemma 3.6.

$$tr(\mathbf{A}) = \begin{cases} \sqrt{n} & \textit{if } n \equiv 1 \pmod 4 \\ i\sqrt{n} & \textit{if } n \equiv 3 \pmod 4 \end{cases}.$$

Proof. Let's try to evaluate $\mathbf{A}^2$. The element (r,s) is:

$$\sum_{t=0}^{n-1} \zeta_n^{t(r+s)} = \begin{cases} n & \text{if } r+s \equiv 0 \pmod n \\ 0 & \text{if } r+s \not\equiv 0 \pmod n \end{cases}.$$

It immediately follows that $\mathbf{A}^4 = \mathbf{I}n^2$, so the eigenvalues of $\mathbf{A}^2$ are $\pm\sqrt{n}$. Say we have an eigenvalue of $\mathbf{A}^2$ of $(x_0, x_1, \ldots, x_{n-1})$. Then, we know that for the eigenvalue n:

$$\mathbf{A}\mathbf{x} = n\mathbf{x} \Longrightarrow x_k = x_{n-k}.$$

The dimension of the eigenspace corresponding to n is $\frac{n+1}{2}$, so that corresponding to $-n$ must be $\frac{n-1}{2}$. If a, b, c, d are the multiplicities of $\sqrt{n}, -\sqrt{n}, i\sqrt{n}, -i\sqrt{n}$, then, because of the eigenvalues of $\mathbf{A}^2$:

$$a + b = \frac{n+1}{2}, c + d = \frac{n-1}{2}.$$

We also know that:

$$|\operatorname{tr}(\mathbf{A})|^2 = ((a-b)^2 + (c-d)^2)n \Longrightarrow (a-b)^2 + (c-d)^2 = 1.$$

This thereby implies that either $a = b$ and $c - d = \pm 1$ or $c = d$ and $a - b = \pm 1$. Coupled with our previous equation, we can deduce that if $n \equiv 1 \pmod 4$, then $c - d = 0, a - b = \pm 1$ and if $n \equiv 3 \pmod 4$, then $c - d = \pm 1, a - b = 0$.
We also know the determinant of the aforementioned matrix:

$$\det(\mathbf{A}) = \left(\sqrt{n}\right)^a \left(-\sqrt{n}\right)^b \left(\sqrt{n}i\right)^c \left(-\sqrt{n}i\right)^d = n^{n/2}(-1)^{b+d} i^{c+d} = n^{n/2} i^{2b+c+3d} = n^{n/2} i^{n(n-1)/2}.$$

If $n \equiv 1 \pmod 4$, then $c = d$, so $c + 3d$ is a multiple of 4 and $i^{2b} = (-1)^b = i^{n(n-1)/2} = (-1)^{n(n-1)/4}$. Then,

$$a - b = (a+b) - 2b = \frac{n+1}{2} - 2b \equiv \frac{n+1}{2} - \frac{n(n-1)}{2} \equiv \frac{-n^2+2n+1}{2} \equiv \frac{-(n-1)^2}{2} + 1 \equiv 1 \pmod 4.$$

It therefore follows that $a - b = 1$. In the case where $n \equiv 1 \pmod 4$, we see that $\operatorname{tr}(\mathbf{A}) = \sqrt{n}$.
If $n \equiv 3 \pmod 4$, then $a = b$ and $c - d = \pm 1$, so:

$$c - d = (c+d) - 2d = \frac{n-1}{2} - 2d \equiv \frac{n-1}{2} = \frac{n-1}{2} - \frac{n(n-3)}{2} \equiv 1 \pmod 4.$$

Hence, if $n \equiv 3 \pmod 4$, then $\operatorname{tr}(\mathbf{A}) = i\sqrt{n}$. ∎

As desired, we have found the sign of the quadratic gauss sum g_1.

4. Resources Used

I used the following resources:

- `https://www.math.purdue.edu/~jlipman/MA598/GaussSumSign.pdf`
- Number Theory Euler Circle Book

Euler Circle, Palo Alto, CA 94306
Email address: `maria.chrysafis.junior@gmail.com`