Quadratic Reciprocity

Matias Relyea
heyanlong@gmail.com

July 10, 2022

Contents

A Brief History

1. 1801: First proof of Quadratic Reciprocity by Gauss in Section IV of *Disquisitiones Arithmeticae*
   (a) "Aureum Theorema" - "The Golden Theorem"
2. Gauss proved Quadratic Reciprocity 7 more times before his death in 1855, and, in Section V of *Disquisitiones Arithmeticae*, developed theory that could be used to consider higher reciprocity. (namely Genus Theory)
3. Euler also contributed by considering Fermat's Theorem on the Sum of Two Squares, and derived results that proved useful when stating Quadratic Reciprocity
4. Exactly 334 proofs as of now

Preliminaries

Quadratic Congruences

A Quadratic Congruence is a congruence of the form

$$x^2 \equiv a \pmod{m},$$

where $m \in \mathbb{Z}^+$. We consider m to be prime.

Preliminaries (continued)

Quadratic Characters

Definition

An integer a is called a *quadratic residue modulo* p if it is a solution to the congruence $x^2 \equiv a \pmod{p}$, and is called a *quadratic nonresidue modulo* p otherwise.

Alternatively, we call a the quadratic character modulo p.

Preliminaries (continued)

Example of Quadratic Residues and Nonresidues

As an example, consider $p = 7$. Looking at all possible values for a, namely all residues modulo p, we have the set $\{0, 1, 2, 3, 4, 5, 6\}$. Squaring each residue, we can determine whether it is a quadratic residue or nonresidue modulo 7. Squaring each of these residues, we can determine which values of a are residues and which are nonresidues.
Therefore, the quadratic residues are $1, 2$, and 4, and the quadratic nonresidues are $3, 5$, and 6.

Preliminaries (continued)

Legendre Symbol

Definition

If $\gcd(a, p) = 1$, then the Legendre Symbol is defined as follows:

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

We use the Legendre Symbol to denote whether some integer a is a quadratic residue or nonresidue modulo p.

Some facts about the Legendre Symbol

These are several important facts that will be used. (proofs can be found in my paper)

$$a \equiv b \pmod{p} \iff \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

$$\left(\frac{0}{p}\right) = 0 \qquad \left(\frac{a^2}{p}\right) = 1 \qquad a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Preliminaries (continued)

Quadratic Reciprocity

Theorem

For odd primes p and q,

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

We can rewrite this as

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

so depending on the value of $\frac{p-1}{2} \cdot \frac{q-1}{2}$, the relationship between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ is down to sign.

Why Quadratic Reciprocity is useful

Using the simplification in the previous slide, we can notice that

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

With this fact, we can compute Legendre Symbols with any integer numerator.

Example

As an example, consider the Legendre Symbol $\left(\frac{11}{29}\right)$. Since

Example

As an example, consider the Legendre Symbol $\left(\frac{11}{29}\right)$. Since $29 \equiv 1 \pmod 4$,

Example

As an example, consider the Legendre Symbol $\left(\frac{11}{29}\right)$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$.

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$,

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right).$$

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right).$$

Again, we have

Example

As an example, consider the Legendre Symbol $\left(\frac{11}{29}\right)$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $\left(\frac{7}{11}\right)$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right).$$

Again, we have

$$-\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right).$$

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right).$$

Again, we have

$$-\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right).$$

4 is a square, so

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right).$$

Again, we have

$$-\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right).$$

4 is a square, so $-(\frac{4}{7}) = -1$,

Example

As an example, consider the Legendre Symbol $(\frac{11}{29})$. Since $29 \equiv 1 \pmod 4$, by Quadratic Reciprocity, we have

$$\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right).$$

Reducing mod 11, we have $(\frac{7}{11})$. Since $7 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, we have

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right).$$

Again, we have

$$-\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right).$$

4 is a square, so $-(\frac{4}{7}) = -1$, and so

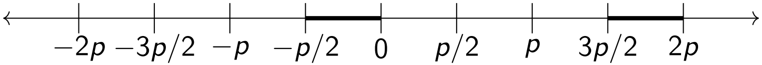
$$\left(\frac{11}{29}\right) = -1.$$

Before we can proceed, we must provide some background for Gauss' Lemma. Consider some set $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ of multiples of a. Our goal is to reduce this set modulo p so that the coefficient of a lies within the interval $[1, \frac{p-1}{2})$, or so its individual elements lie within the interval $(-\frac{p}{2}, \frac{p}{2})$.

Proof of Quadratic Reciprocity

Gauss' Lemma

Before we can proceed, we must provide some background for Gauss' Lemma. Consider some set $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ of multiples of a. Our goal is to reduce this set modulo p so that the coefficient of a lies within the interval $[1, \frac{p-1}{2})$, or so its individual elements lie within the interval $(-\frac{p}{2}, \frac{p}{2})$.



Proof of Quadratic Reciprocity

Gauss' Lemma (continued)

After reducing the elements of S modulo p within the specified interval, we call the new elements in a set T the set of *least residues modulo p*. Those that are negative are *least negative residues modulo p*. We state the following theorem. We let $\mu(a, p)$ be the number of least negative residues modulo p.

Proof of Quadratic Reciprocity

Gauss' Lemma (continued)

After reducing the elements of S modulo p within the specified interval, we call the new elements in a set T the set of *least residues modulo p*. Those that are negative are *least negative residues modulo p*. We state the following theorem. We let $\mu(a, p)$ be the number of least negative residues modulo p.

Lemma (Gauss' Lemma)

Let $\gcd(a, p) = 1$. *Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)},$$

where $\mu(a, p)$ *denotes the number of least negative residues modulo p.*

Proof of Quadratic Reciprocity (continued)

Sketch of proof of Gauss' Lemma (continued)

1. To prove Gauss' Lemma, we construct the set S as before.

Proof of Quadratic Reciprocity (continued)

Sketch of proof of Gauss' Lemma (continued)

1. To prove Gauss' Lemma, we construct the set S as before.
2. We then construct the set T of least residues modulo p from S, and prove three properties:

Proof of Quadratic Reciprocity (continued)

Sketch of proof of Gauss' Lemma (continued)

1. To prove Gauss' Lemma, we construct the set S as before.
2. We then construct the set T of least residues modulo p from S, and prove three properties: all elements, when reduced modulo p, are distinct,

Proof of Quadratic Reciprocity (continued)

Sketch of proof of Gauss' Lemma (continued)

1. To prove Gauss' Lemma, we construct the set S as before.
2. We then construct the set T of least residues modulo p from S, and prove three properties: all elements, when reduced modulo p, are distinct, no elements of S reduce to 0 modulo p,

Proof of Quadratic Reciprocity (continued)

Sketch of proof of Gauss' Lemma (continued)

1. To prove Gauss' Lemma, we construct the set S as before.
2. We then construct the set T of least residues modulo p from S, and prove three properties: all elements, when reduced modulo p, are distinct, no elements of S reduce to 0 modulo p, and no element of T is the additive inverse of another.

Proof of Quadratic Reciprocity (continued)

Sketch of proof of Gauss' Lemma (continued)

1. To prove Gauss' Lemma, we construct the set S as before.
2. We then construct the set T of least residues modulo p from S, and prove three properties: all elements, when reduced modulo p, are distinct, no elements of S reduce to 0 modulo p, and no element of T is the additive inverse of another.
3. We then take the product from 1 to $\frac{p-1}{2}$ of elements of S and T and equate them modulo p, obtaining our result.

Lemma

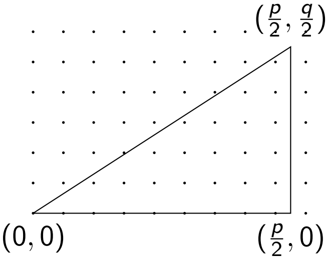
Let $\gcd(a,p)=1$*. Then*

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

We will not prove this statement here. However, it is important to note that this explicitly determines $\mu(a,p)$, and is fundamental in the proof of Quadratic Reciprocity.

Proof of Quadratic Reciprocity using Lattice Points

We begin by letting p and q be odd primes. We then consider the two integers $\frac{p-1}{2}$ and $\frac{q-1}{2}$. We begin by constructing a triangle $T(q, p)$ with vertices at $(0,0), (\frac{p}{2}, 0)$, and $(\frac{p}{2}, \frac{q}{2})$.



We want to count the number of non-side-intersecting points (or the number of points bounded within $T(q, p)$).

Proof of Quadratic Reciprocity using Lattice Points (continued)

Starting from $x = 1$ and going to $x = 5$ in the diagram, we see that there are

$$1 + 1 + 2 + 3 + 3 + 4 + 5 = 19$$

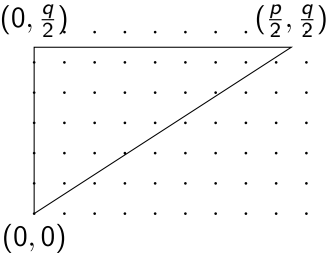
points. In general, the sum of all points until the kth column is

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$$

points.

Proof of Quadratic Reciprocity using Lattice Points (continued)

Now we consider the triangle $T'(p,q)$ with vertices at $(0,0), (0,\frac{q}{2})$, and $(\frac{p}{2},\frac{q}{2})$.



We want to count the number of non-side-intersecting points again, but in a different way.

Proof of Quadratic Reciprocity using Lattice Points (continued)

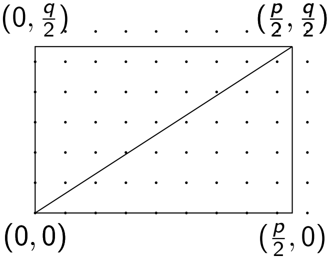
Starting from $y = 1$ and going to $y = 5$, we see that there are also 19 points. However, in general, since we're counting by rows, there are

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor$$

points.

Proof of Quadratic Reciprocity using Lattice Points (continued)

Now we consider the rectangle that is formed by connecting the two triangles. Then we have



Again, we want to count the number of points in this rectangle, but there are

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Proof of Quadratic Reciprocity using Lattice Points (continued)

We calculate the number of points in a different way.

$$\left\lfloor \frac{p}{2} \right\rfloor \left\lfloor \frac{q}{2} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

Thus we have that

$$\begin{aligned}\{\text{number of points in } R(q,p)\} &= \frac{p-1}{2} \cdot \frac{q-1}{2} \\ &\equiv \mu(q,p) + \mu(p,q) \pmod{2}.\end{aligned}$$

Then by Gauss' Lemma,

$$\{\text{number of points in } R(q,p)\} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

■

Thank You!

Thank you for listening!