Quadratic Reciprocity

Mauritz Fasth, Jiachen Mi, Olle Rehnquist, Erik Wettergren

May 2023

1 Introduction

Among the first things one learns in algebra is to find the zeroes of polynomials over the real numbers. One might pose a similar problem of finding zeroes of polynomials over $\mathbb{Z}/p\mathbb{Z}$, the set of integers modulo a prime p. However, we will instead consider the somewhat easier problem of determining when a polynomial has a zero. For linear congruences $ax \equiv b \pmod{p}$ the answer is simply that there exist a solution if and only if p does not divide a or p divides a and b. For 2nd degree equations the situation becomes much more interesting. As we know from the real numbers, we can complete the square to reduce the problem to finding for which $a \in \mathbb{Z}/p\mathbb{Z}$ there exists $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$. This is what we want to solve in this essay and is the same question that many brilliant mathematicians such as Fermat, Euler, Legendre and Gauss asked themselves and at the heart of the topic lies The Law of Quadratic Reciprocity.

Due to the non-trivial nature of this topic, we have to assume familiarity with the fundamental results in number theory (for instance Fermat's Little Theorem and The Chinese Remainder Theorem) that one might learn about in any book on Elementary Number Theory, such as *Elementary Number Theory* by Rosen.

1.1 Notation

We will throughout this essay use standard notation, with one exception. We will sometimes use the denser notation $\mathbb{Z}_p$ to denote $\mathbb{Z}/p\mathbb{Z}$. We write $\mathbb{Z}_p^*$ for the nonzero elements of $\mathbb{Z}_p$. Also, when we are working in the integers and say *prime*, we are always referring to a positive prime. In the section on Cubic Residues we will occasionally use the term *rational prime* when talking about primes in $\mathbb{Z}$.

1.2 Pedagogy

Mathematics is not a spectator sport. We therefore encourage mathematical inquiry and have accordingly chosen to develop a lot of the theory through series of instructive exercises that we hope will bring more clarity to the reader. Furthermore, presenting proofs of theorems strips the reader of the satisfaction one gets from proving them oneself. Some of the topics later on will be on a higher level and so the reader should not expect to understand everything at once. The section on cubic residues in particular will require patience.

2 Quadratic Residues

We are very comfortable solving quadratic equations over the real numbers, so a natural question to ask is when the equation $x^2 = a$ has a solution in $\mathbb{Z}_p$. This endeavour is essentially trivial for a fixed p since the problem is a finite one, but the question can be reversed: given a, for which primes p is a a square?

Definition 2.1. Let p be a prime and $a \in \mathbb{Z}_p^*$. Then a is called a *quadratic residue* modulo p if there exists $x \in \mathbb{Z}_p$ such that $x^2 = a$ in $\mathbb{Z}_p$. Otherwise a is called a *quadratic non-residue* modulo p.

Example 2.1. It is easy to see that 5 is a quadratic residue modulo 11 since $4^2 \equiv 5 \pmod{11}$, while 2 is a quadratic non-residue modulo 3 (simply try to square all numbers in $\mathbb{Z}_3$).

The reader is now encouraged to engage in inquiry, that is to try small cases for p and make conjectures.

Exercise 2.1. Try to conjecture when -1 is a quadratic residue by numerically investigating $p = 3, 5, 7, 11, 13$ and 17. Can you make any attempts of proving your conjecture?

Some of the theory of quadratic residues will be developed through a series of exercises below and the following theorem, which is easily proved, might be useful for the reader.

Theorem 2.1 (Division Algorithm for Polynomials)**.** For any $A(x), B(x) \in \mathbb{Z}_p[x]$, such that $B(x) \neq 0$, there exists $Q(x), R(x) \in \mathbb{Z}_p[x]$ such that $A(x) = B(x)Q(x) + R(x)$ and either $R(x) = 0$ or $\deg(B) > \deg(R)$.

Exercise 2.2. Prove that a polynomial over $\mathbb{Z}_p$ of degree n has at most n zeroes. Hint: Use the division algorithm for polynomials.

Exercise 2.3. List the perfect squares in $\mathbb{Z}_5$ and $\mathbb{Z}_{13}$. How many are there? Verify your conjecture for the general case. Hint: $a^2 = (-a)^2$ and the previous exercise.

We saw in the last exercise that there are exactly $\frac{p-1}{2}$ quadratic residues and equally many quadratic non-residues. We shall now apply it to a problem.

Example 2.2. Show that for every prime p there exist $a, b \in \mathbb{Z}$ such that p divides $a^2 + b^2 + 1$.

Proof. The condition holds if and only if $a^2 \equiv -b^2 - 1 \pmod{p}$. Note that both sides, which are independent of each other, can attain exactly $\frac{p-1}{2} + 1$ values, as a consequence of the result obtained in the last exercise. Hence there must be some overlap so that $a^2 \equiv -b^2 - 1$ for some integers a, b. (Why?) □

Theorem 2.2. If a, b are both quadratic residues, then their product is a quadratic residue. If one is a quadratic residue and the other a quadratic non-residue the product is a quadratic non-residue. If both are quadratic non-residues the product is a quadratic residue.

Proof. Suppose that $a, b \in \mathbb{Z}_p$ are quadratic residues modulo p. Then there exists $x, y \in \mathbb{Z}_p$ such that $x^2 = a$ and $y^2 = b$ in $\mathbb{Z}_p$, thus $ab = (xy)^2$ is a quadratic residue in $\mathbb{Z}_p$.

If a is a quadratic residue and b is a quadratic nonresidue in $\mathbb{Z}_p$, suppose for the sake of contradiction that ab is a quadratic residue. Then there exists $x, y \in \mathbb{Z}_p^*$ such that $a = x^2$ and $ab = y^2$ in $\mathbb{Z}_p$. This implies that $b = (x/y)^2$, a contradiction, hence ab must be a quadratic nonresidue.

Suppose a, b are both quadratic nonresidues in $\mathbb{Z}_p$. Then the map from $\mathbb{Z}_p^*$ to itself defined by $x \mapsto a \cdot x$ is trivially a bijection. Since we know that there are exactly $\frac{p-1}{2}$ quadratic residues by a previous exercise and that the product of a with a quadratic residue always results in a quadratic nonresidue, we conclude that ab is a quadratic residue. $\square$

In this exercise, we find out that the property of being a quadratic residue behaves in some sense like multiplication of -1 and 1, where -1 is identified with quadratic non-residues and 1 is identified with quadratic residues. This motivates the following definition:

Definition 2.2. The *Legendre symbol* is defined for $a \in \mathbb{Z}$ and a positive odd prime p as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue,} \\ -1 & \text{if } a \text{ is a quadratic non-residue.} \end{cases}$$

The reader should, using Theorem 2.2, verify that this definition is natural. We have already proved our first proposition about it, namely that for $a, b \in \mathbb{Z}$ not divisible by p, it is the case that: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Hence, by unique prime factorisation, it is sufficient to classify the quadratic residues of all primes together with -1. Now more exercises follow.

Exercise 2.4. When is $5n^2 - 2$ a perfect square? Can you use the theory of quadratic residues that we have developed so far?

Exercise 2.5. Suppose $a^2 \equiv -1 \pmod{p}$, where p is an odd prime. What can you say about the order of a? What can you hence deduce about the residue of p modulo 4? What about the converse of your result?

Note how polynomials played an important part in some of the earlier exercises. The following is a crucial result that we advise the reader to try to prove for themselves, although we will include a proof due to its significance:

Theorem 2.3 (Euler's Criterion)**.** Let p be an odd prime and a an integer not divisible by p. Then

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

Proof. Consider the polynomial $x^{p-1} - 1$ in $\mathbb{Z}_p[x]$. By Fermat's Little Theorem, all $a \in \mathbb{Z}_p^*$ are zeroes of this polynomial. However

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1).$$

This implies that either $a^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod{p}$. But if $a \equiv b^2 \pmod{p}$ for some integer b then $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$ and since there are exactly $\frac{p-1}{2}$ quadratic residues and $x^{\frac{p-1}{2}} - 1$ has degree $\frac{p-1}{2}$, exactly the quadratic non-residues must have $a^{\frac{p-1}{2}}$ congruent to -1 by Exercise 2.2. We see that this aligns with our definition of the Legendre symbol, and thus, we are done. $\square$

3 The Law of Quadratic Reciprocity

We are now ready to treat the first case in understanding quadratic residues completely, by proving the so-called First Supplementary Law.

Exercise 3.1 (First Supplementary Law)**.** Prove that -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod 4$. Hint: Use Euler's Criterion.

We shall now state the main theorem which allows us to in principle determine whenever a number is a quadratic residue, together with the Second Supplementary Law.

Theorem 3.1 (Second Supplementary Law)**.** Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Theorem 3.2 (The Law of Quadratic Reciprocity)**.** Let p, q be odd distinct primes. Then

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

Take a second to appreciate the beautiful theorem above, which eventually gave rise to one of the most profound results in number theory: Artin's Reciprocity Law, which is far too difficult for this essay to even state. We will however give a couple of proofs of Quadratic Reciprocity, although in a later section.

Let us now familiarise ourselves with calculations using the Legendre symbol by use of an example and some exercises:

Example 3.1. We shall prove a criterion for when 3 is a quadratic residue modulo an odd prime p. But notice that

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}}.$$

If p is congruent to 1 mod 3 then $\left(\frac{p}{3}\right) = 1$ and for 3 to be a quadratic residue modulo p we need $p \equiv 1 \pmod 4$. If p is congruent to 2 mod 3 and $\left(\frac{p}{3}\right) = -1$ instead, we get that $p \equiv 3 \pmod 4$. Hence, by the Chinese Remainder Theorem, 3 is a quadratic residue if and only if $p \equiv 1$ or $11 \pmod{12}$.

Exercise 3.2. Determine, using the law of quadratic reciprocity, if 51 is a quadratic residue modulo 101.

Exercise 3.3. Determine a criterion for when 5 is a quadratic residue modulo an odd prime p.

This is a good point to take a step back and see what our theory can accomplish so far. We do this by proving the following theorem.

Theorem 3.3 (Pépin's Test)**.** The number $p = 2^{2^n}+1$ is prime, where n is a positive integer, if and only if $3^{\frac{p-1}{2}} \equiv -1 \pmod p$.

Proof. If $p = 2^{2^n}+1$ is prime we see that that $p = (2^2)^{2^{n-1}}+1 \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$. Hence $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}} = -1$ and so by Euler's Criterion $3^{\frac{p-1}{2}} \equiv -1 \pmod p$. If on the other hand $3^{\frac{p-1}{2}} \equiv -1 \pmod p$ we see that the order of 3 modulo p divides $p-1 = 2^{2^n}$ but not $\frac{p-1}{2} = 2^{2^n-1}$ and is therefore equal to $p-1$. Since $p-1 \mid \phi(p)$ we get that $\phi(p) = p-1$ and so p is prime. □

Notice that the primality test above is very useful since we can easily calculate $3^{\frac{p-1}{2}} \pmod p$ using repeated squaring. Unfortunately, the rate at which the numbers $2^{2^n}+1$ (so-called Fermat numbers) grow makes it computationally hard to use anyways.

Exercise 3.4. Prove that the sum of quadratic residues modulo a prime p is congruent to 0 if and only if $p \neq 2$ or 3.

Exercise 3.5. What can you say about the product of all quadratic residues modulo p? Hint: Think about inverses and consider two cases.

Exercise 3.6. Figure out the condition for $3, 5, 7, 11$ and 13 being quadratic residues modulo p. What is the modular condition for p? Prove that for distinct odd primes p, q there exists an odd $\alpha \in \mathbb{Z}$ such that $\left(\frac{q}{p}\right) = 1 \iff p \equiv \pm\alpha^2 \pmod{4q}$. Hint: Consider different cases based on residues modulo 4.

3.1 The Jacobi Symbol

A remark that we would like to make is that a troublesome part of calculating the Legendre symbol is that we first need to perform a prime factorisation, which is computationally hard. This motivates us to generalise the symbol into the *Jacobi Symbol.* Note that we use the same notation as for the Legendre symbol.

Definition 3.1. The *Jacobi Symbol* is defined for $a \in \mathbb{Z}$ and a positive odd integer $n = p_1 p_2 \cdots p_k$ where $p_1, \ldots, p_k$ are not necessarily distinct primes, as the product of the Legendre Symbols of the primes:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right).$$

It is a straightforward exercise, although worthwhile, to prove that for any $a, b \in \mathbb{Z}$ and m, n positive odd integers

1. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$,
2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$,
3. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$,
4. $\left(\frac{2}{n}\right) = (-1)^{\frac{p^2-1}{8}}$.

Even a corresponding reciprocity law can be easily deduced:

Exercise 3.7. Prove that for odd relatively prime positive integers m, n,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Exercise 3.8. Prove that if for an integer a and a positive odd integer n, $\left(\frac{a}{n}\right) = -1$, then there does not exist an integer x such that $x^2 \equiv a \pmod{n}$.

Exercise 3.9. Prove or disprove that $\left(\frac{a}{n}\right) = 1$ implies the existence of an integer x such that $x^2 \equiv a \pmod{n}$. Hint: It is false, but spend some time thinking about exactly when this fails AND give an explicit counterexample.

Now we have developed a tool that allows us to calculate the Legendre symbol (since it aligns with the Jacobi symbol when it is defined) using only the division algorithm by constantly flipping the symbol using the reciprocity law, which for a computer is much easier than factorising.

Exercise 3.10. Determine whether 153 is a quadratic residue modulo 191. Hint: 191 is a prime.

4 Applications to Mathematical Olympiads

In this section, we apply the theory that we have developed to some Olympiad-style problems. The most generally applicable idea is to **consider prime divisors** which we exemplify below.

Example 4.1. Find all positive integers n such that $2^n - 1 \mid 3^n - 1$.

Solution. We first observe that $n = 1$ is a solution. Otherwise, we know that there will be a prime dividing $2^n - 1$. If n is even then $3 \mid 2^n - 1$ (prove this!) and naturally 3 does not divide $3^n - 1$. Now suppose that $2^n - 1 \mid 3^n - 1$ where $n > 1$ is a positive odd integer and let p be any prime (necessarily odd and not equal to 3) dividing $2^n - 1$ and therefore $3^n - 1$. Hence $(3^{\frac{n+1}{2}})^2 \equiv 3 \pmod{p}$. But

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2}}.$$

For this to be equal to 1 we realise that either $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$ or $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$. This gives us that $p \equiv \pm 1 \pmod{12}$. Now we know there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$ and $4^2 \equiv 4 \pmod{12}$, so

$$2^n - 1 = 2 \cdot 4^k - 1 \equiv 7 \pmod{12}.$$

This contradicts the fact that all primes dividing $2^n - 1$ had residue ± 1 modulo 12. The only solution is therefore $n = 1$. □

The following harder example demonstrates the same principle.

Example 4.2 (Iran TST 2013 (modified))**.** Prove that there does not exist an integer n such that $3n + 2$ is not a power of 2 and $\frac{a^2+b^2+c^2}{3(ab+bc+ca)} = n$, for integers $a, b, c \in \mathbb{Z}^+$.

Proof. Suppose for contradiction that $\frac{a^2+b^2+c^2}{3(ab+bc+ca)} = n \in \mathbb{Z}^+$. Then by rewriting, we get that:

$$(a + b + c)^2 = (3n + 2)(ab + bc + ca).$$

Now we notice that there must exist an odd prime p congruent to 2 modulo 3 such that it divides $3n + 2$ with an odd exponent (make sure that you understand why). Hence since p must divide the right hand side by an even exponent $p \mid ab+bc+ca$ and consequently $p \mid ab-b(a+b)-a(a+b)$ which is equivalent to $p \mid 4a^2 + 4ab + 4b^2$. We can write this as

$$p \mid (2a + b)^2 + 3b^2,$$

which implies that -3 is a quadratic residue modulo p. However,

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = (-1)^{p-1} \cdot \left(\frac{2}{3}\right) = -1,$$

which is a contradiction. Hence there exists no integer n such that $3n + 2$ is not a power of two and $\frac{a^2+b^2+c^2}{3(ab+bc+ca)} = n$. □

The requirement that $3n+2$ is not a power of two is rather unpleasant and even unnecessary, but we have left out the details for the sake of brevity.

Below more exercises for the reader follow and we advise the reader to keep these ideas in mind:

1. Consider prime divisors.
2. Use modular reduction.
3. Complete the square.
4. Look at orders.

Exercise 4.1. Find all positive integers x, y such that $y^2 - 5 \mid x^2 + 1$.

Exercise 4.2. Solve for $x \in \mathbb{Z}$ and n an even positive integer: $10^n + 89 = x^2$.

Exercise 4.3. Prove that if the last digit of $x^2 + xy + y^2$ is zero (in base 10) then the second to last digit is zero as well.

Exercise 4.4. Prove that $2^n + 1$ has no prime factor of the form $8k - 1$ where $k \in \mathbb{Z}$.

Exercise 4.5. Prove that all numbers are *cubic residues* modulo a prime p if and only if $p \equiv 2 \pmod 3$.

Exercise 4.6. Let p be an odd prime and A, B distinct non-empty subsets of $\{1, \ldots, p-1\}$ satisfying:

1. $A \cup B = \{1, \ldots, p-1\}$,
2. if both a, b are in A or in B then $ab \in A$,
3. if $a \in A$ and $b \in B$ or vice versa then $ab \in B$.

Determine all possible sets A and B.

Exercise 4.7. Let a and b be positive integers such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

Exercise 4.8. An odd prime p is defined to be a *Sophie Germain-prime* if and only if $2p + 1$ is a prime as well. Prove that for a Sophie Germain-prime $p \equiv 1 \pmod 4$, 2 is a primitive root modulo $2p + 1$.

Exercise 4.9. For a positive integer a define $x_1 = a$ and $x_{k+1} = 2x_k + 1$ for positive integers k. Let $y_k = 2^{x_k} - 1$ and determine the largest positive integer n such that $y_1, \ldots, y_n$ are all primes for some positive integer a.

5 Proofs of Quadratic Reciprocity

The Quadratic Reciprocity Law was by Gauss called the Golden Theorem and he produced eight proofs of it during his lifetime. This abundance of proofs most likely stemmed from the feeling that none of them were sufficiently deep. Many of the more than 200 known proofs may involve transparent and elegant arguments, but tend to use clever, seemingly God-given tricks that do not explain the deep reason as to why one should expect such a theorem to be true. For this however, one needs to introduce more heavy machinery in the form of algebraic number theory, which, unfortunately, is beyond the scope of this essay. The theorem is in itself quite unexpected, since the Chinese Remainder Theorem essentially tells us that life modulo p is unrelated to life modulo q, whereas the plethora of reciprocity theorems stemming from

Quadratic Reciprocity shows us that, in fact, they are. This should serve as an indication that some clever combinatorial argument is not the underlying reason for the validity of the theorem.

Nevertheless, we want to give the reader two proofs of quadratic reciprocity, due to their beauty. The first will be presented to the reader while the latter will be discovered by guided inquiry through exercises.

5.1 Combinatorial proof

For this proof, we will start off by giving a combinatorial interpretation of the Legendre symbol. Consider the map $x \mapsto ax + b$ modulo p, for $a, b \in \mathbb{Z}_p$, where a is a non-zero residue modulo p. Then the sign of our permutation π of the elements mod p is the same as $\left(\frac{a}{p}\right)$, since $\text{sgn}(\pi) = \prod_{0 \le i < j < p} \frac{\pi(i) - \pi(j)}{i-j} \equiv \prod_{0 \le i < j < p} \frac{ai+b-(aj+b)}{i-j} \equiv \prod_{0 \le i < j < p} \frac{a(i-j)}{i-j} \equiv a^{\frac{p(p-1)}{2}} \pmod{p}$. From Fermat's little theorem $(a^p)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}$, which according to Euler's criterion is the same as $\left(\frac{a}{p}\right)$.

We will now use this fact to formulate a proof of the law of quadratic reciprocity. Consider the set of all pairs (i, j), wherein $i \in \mathbb{Z}_p$ and $j \in \mathbb{Z}_q$, for two odd primes p and q. We turn our attention to the following two possible permutations: $\pi_p : (i, j) \mapsto (i, i + pj)$ and $\pi_q : (i, j) \mapsto (qi+j, j)$, and note that they each have the signs $\text{sgn}(\pi_p) = \left(\frac{p}{q}\right)$ and $\text{sgn}(\pi_q) = \left(\frac{q}{p}\right)$ respectively, by the result above. We consider the permutation $\pi_{pq} = \pi_p \pi_q^{-1}$ mapping $(j+qi, j)$ to $(i, i + pj)$, which has the sign $\text{sgn}(\pi_{pq}) = \text{sgn}(\pi_p)\text{sgn}(\pi_q^{-1}) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$. Since each element in $\mathbb{Z}_{pq}$ has a unique representation as $j + qi$, where $0 \le i < p$ and $0 \le j < q$, we can interpret our set of pairs as containing elements in $\mathbb{Z}_{pq}$, where an element in $\mathbb{Z}_{pq}$ corresponds to the pair of its p-reduction and q-reduction. Thus the permutation π_{pq} is the same as $j+qi \mapsto i+pj$.

Since this permutation is the same as π_{pq}, it has the same sign as well. However, this must be the same as $(-1)^n$, where n is the number of inversions. This corresponds to the number of pairs (i, j) and (i', j') such that $j + qi > j' + qi'$ and $i + pj < i' + pj'$. This is in turn the same as $i' < i$ and $j < j'$ (can you tell why?), meaning in turn that $n = \binom{q}{2}\binom{p}{2} = \frac{q(q-1)}{2}\frac{p(p-1)}{2}$. Since both p and q are odd, the sign of our permutation becomes $(-1)^{\frac{q(q-1)}{2}\frac{p(p-1)}{2}} = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$. This in turn gives us that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$. We have thus proven the law of quadratic reciprocity for odd primes p and q. A separate proof is required for the case wherein one of our primes isn't odd, which is presented in the second proof down below.

5.2 Eisenstein's Geometric Proof

A variation of this proof was first discovered by Gauss, although Eisenstein's form below is far more elegant.

Exercise 5.1. Consider the set $A = \{2, 4, \ldots, p-1\}$ of even residues modulo a prime p. Let r_a be the remainder modulo p of qa for every $a \in A$ where q is an odd prime. Show that $(-1)^{r_a} r_a$ is a permutation of A up to multiples of p.

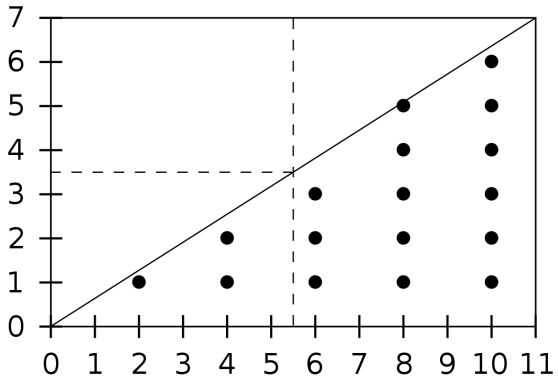
Exercise 5.2. Hence show, using an argument similar to the proof of Fermat's Little Theorem, that $q^{\frac{p-1}{2}} \equiv (-1)^{\sum_{a \in A} r_a}$.

Exercise 5.3. Show that $(-1)^{\sum_{a\in A} r_a} = (-1)^{\sum_{a\in A}\left\lfloor \frac{qa}{p}\right\rfloor}$. Hint: by the Division Algorithm:

$$\sum_{a\in A} qa = p\sum_{a\in A}\left\lfloor \frac{qa}{p}\right\rfloor + \sum_{a\in A} r_a.$$

Exercise 5.4. Prove the second supplementary theorem of the Law of Quadratic Reciprocity, namely that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ using the last exercise. Hint: What values can $\left\lfloor \frac{2a}{p}\right\rfloor$ take?

Remember that we have already earlier proved the First Supplementary Law of Quadratic Reciprocity, namely that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, so we are now ready to attack the Golden Theorem using some geometry.



Exercise 5.5. Consider a lattice of points $(x, y) \in \mathbb{Z}^2$ where for two distinct odd primes p, q the line segment connecting $(0, 0)$ and (p, q) is drawn. Prove firstly that no lattice points between these two points lie on the line segment.

Exercise 5.6. Prove that for an even x-coordinate $p > a > p/2$, the parity of the number of lattice points with x-coordinate a under the line is the same as over the line.

Exercise 5.7. Hence prove that the parity of the number of lattice points with the odd x-coordinate $p - a$ under the line is the same as the parity of the number of lattice points under the line with x-coordinate a using symmetry.

Exercise 5.8. Deduce, by counting of the number of lattice points with x-coordinate a under the line, that

$$(-1)^{\sum_{a\in A}\left\lfloor \frac{qa}{p}\right\rfloor} = (-1)^{\sum_{a=1}^{\frac{p-1}{2}}\left\lfloor \frac{qa}{p}\right\rfloor}.$$

Exercise 5.9. Convince yourself that $\sum_{a=1}^{\frac{p-1}{2}}\left\lfloor \frac{qa}{p}\right\rfloor + \sum_{a=1}^{\frac{q-1}{2}}\left\lfloor \frac{pa}{q}\right\rfloor = \frac{p-1}{2}\cdot\frac{q-1}{2}$ by counting lattice points.

Exercise 5.10. Put everything together to prove the Law of Quadratic Reciprocity.

Make sure that you have studied the proof well enough to be able to reproduce it, not by memorising it word by word, but rather by understanding the principles. Notice that the proof contains only very simple ideas, which does not mean that it is easily discovered. Quite on the contrary, it is a surprising proof strategy.

6 Cubic Residues (Advanced Section)

To conclude this essay, we would like to give the reader a taste of how quadratic reciprocity generalises. We will here study cubic residues, that is solutions to the equation $x^3 \equiv a \pmod{p}$, though will unfortunately not include any proofs to avoid being too technical. For the interested reader we recommend the excellent exposition in Chapter 1 Section 4 of *Primes of the form* $x^2 + ny^2$ by Cox.

Remember that the Legendre symbol took the values of the second roots of unity in the quadratic case. This might hint at us that the natural setting for cubic residues is actually the set of *Eisenstein Integers*

$$\mathbb{Z}[\omega] := \{a + b\omega | a, b \in \mathbb{Z}\}$$

where $\omega = e^{\frac{2\pi i}{3}}$.

Reading Question. Look up the definition of a ring if you are not already familiar with it. Verify that $\mathbb{Z}$ is one. Verify that $\mathbb{Z}[\omega]$ is one.

One of our most important tools will henceforth be the *norm* of a number $\alpha = a+b\omega \in \mathbb{Z}[\omega]$, defined as $N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2$.

Exercise. Show that the norm is multiplicative: $N(\alpha\beta) = N(\alpha)N(\beta)$. Hint: No messy algebra is needed. Use the multiplicativity of the complex conjugate.

Reading Question. Look up the definitions of a Euclidean Domain, Principle Ideal Domain and Unique Factorisation Domain. Prove that $\mathbb{Z}[\omega]$ is one using a similar argument to the proof of the same fact for $\mathbb{Z}$.

The exercise above is optional. If the reader is completely unfamiliar with these notions the reader will just have to trust us when we say that the properties of the Eisenstein integers are very similar to those of the integers. We now give some important definitions, assuming already the definitions of divisibility which are analogous to the rational case.

Definition 6.1. Let α, β be Eisenstein integers. Then

1. α is a *unit* if there exists $\gamma \in \mathbb{Z}[\omega]$ such that $\alpha\gamma = 1$,
2. α, β are *associates* if one is a unit multiple of the other,
3. α is a prime if it is a non-unit and for any $x, y \in \mathbb{Z}[\omega]$, $\alpha \mid xy$ implies $\alpha \mid x$ or $\alpha \mid y$,
4. α is *irreducible* if for any $x, y \in \mathbb{Z}[\omega]$, $\alpha = xy$ implies that exactly one of x, y is a unit.

Exercise 6.1. Prove that the notion of irreducible and prime coincides in $\mathbb{Z}[\omega]$ using an argument similar to in the integers. Give an example of a ring where this is not true.

Exercise 6.2. Show that $\alpha \in \mathbb{Z}[\omega]$ is a unit if and only if $N(\omega) = 1$. Hence determine all units in the ring.

Next, we want to determine what happens with rational primes when inserted into the Eisenstein integers.

Exercise 6.3. Prove that if p is a rational prime, then

1. 3 *ramifies*, that is $3 = -\omega^2(1-\omega)^2$, where $1-\omega$ is a prime

2. $p \equiv 2 \pmod 3$ implies that p is an Eisenstein prime (We say that p is *inert*). Hint: The norm's multiplicativity is very useful.

3. $p \equiv 1 \pmod 3$ implies that $p = \pi\bar{\pi}$ where π is a Gaussian prime (We say that p *splits*). Hint: Show that p divides a number of the form $x^2 + 3 = (x - \sqrt{3}i)(x + \sqrt{3}i)$.

Exercise 6.4. Prove that if π is an Eisenstein prime, then for any Eisenstein integer a not divisible by π

$$a^{N(\pi)-1} \equiv 1 \pmod \pi.$$

Hint: The proof of Fermat's little theorem generalises nicely.

Wishful thinking makes us want to have a corresponding Euler's Criterion, which makes the following definition natural.

Definition 6.2. For a prime π not dividing 3 and $a \in \mathbb{Z}[\omega]$ not divisible by π we define the *cubic character* $\left(\frac{a}{\pi}\right)_3$ to be the unique cube root of unity which is congruent to $a^{\frac{N(\pi)-1}{3}}$ modulo π.

Exercise 6.5. Justify the definition above by demonstrating firstly that $a^{\frac{N(\pi)-1}{3}}$ must be congruent to $1, \omega$ or ω^2. Show that the condition that π does not divide 3 was necessary for the cube roots of unity to be distinct.

Exercise 6.6. Prove the multiplicativity of the cubic character.

Exercise 6.7. Prove that for a prime π not dividing 3 and Eisenstein integer a not divisible by π: $\left(\frac{a}{\pi}\right)_3 = 1$ if and only if $x^3 \equiv a \pmod \pi$ has a solution. Hint: This is very similar to the quadratic case.

The final definition that we need is that a prime π not dividing 3 is called primary if and only if $\pi \equiv 2 \pmod 3$.

Exercise 6.8. Show that a given prime not dividing 3 has exactly one associate which is primary. This means that "primary" is the equivalent of "positive" in the integers.

We are now ready to state the main theorem:

Theorem 6.1 (The Law of Cubic Reciprocity)**.** Let π_1 and π_2 be primary primes in $\mathbb{Z}[\omega]$ such that $N(\pi_1) \neq N(\pi_2)$. Then

$$\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3.$$

As for Quadratic Reciprocity there are supplementary laws, but we will not state them here. We will not give a proof of this theorem either, though one can be found in *A Classical Introduction to Modern Number Theory* by Ireland and Rosen (a proof using so-called Gauss sums).

We shall now shortly touch on when a is a cubic residue modulo a prime p in $\mathbb{Z}$. The reader should already have proved in Exercise 4.5 that all numbers relatively prime to p are cubic residues if $p \equiv 2 \pmod 3$. If not, we know that p splits in $\mathbb{Z}[\omega]$ and so there exists a prime π such that $N(\pi) = p$. Here we can not avoid being a bit technical, so the reader might want to look up some of the terminology that we use.

Let t be a number whose square is -3 modulo p (which we know exists due to quadratic reciprocity). Then consider the map $\phi : \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \to \mathbb{Z}/p\mathbb{Z}$ defined by

$$\phi(a + b\omega) = a + b \cdot \frac{t-1}{2}.$$

This can be easily verified to be an homomorphism and since all field homomorphisms are injective and since both fields have the same cardinality ($N(\pi) = p$), we conclude that this is indeed a field isomorphism. Furthermore, we see that ϕ maps $a + 0\omega$ to a, $a \in \mathbb{Z}$. Therefore a is a cubic residue modulo p in $\mathbb{Z}$ if and only if $\left(\frac{a}{\pi}\right)_3 = 1$ which can be determined using the cubic reciprocity theorem in $\mathbb{Z}[\omega]$.

We hope that this method of generalisation, the starting point for algebraic number theory, has been insightful, even though some of the material might be a bit too advanced for the reader at this point.

7 Further Reading

As has already been emphasised, quadratic reciprocity is an incredibly beautiful result and is probably the most important and nontrivial theorem of Elementary Number Theory. There are also many generalisations, most notably Artin's Reciprocity Theorem which is too difficult to state here but is the starting point for the ambitious Langlands program. The interested reader should consult the following literature.

1. *Elementary Number Theory* by Rosen - This book introduces number theoretic theorems and notions such as order, the Chinese Remainder Theorem and so on, which are prerequisites for this essay.

2. *Abstract Algebra* by Dummit and Foote - This will be preliminaries for some of our other recommendations.

3. *Modern Olympiad Number theory* by Aditya Khurmi - A book primarily aimed at Olympiad competitors.

4. *The Quadratic Reciprocity Law* by Lemmermeyer - Contains a huge list of proofs of quadratic reciprocity together with detailed descriptions of some proofs and some historical remarks.

5. *Primes of the form* $x^2 + ny^2$ by David A. Cox - The author develops class field theory, beginning with a discussion of quadratic, cubic and biquadratic reciprocity.

6. *A Classical Introduction to Modern Number Theory* by Ireland and Rosen - An excellent introduction to primarily algebraic number theory. Especially chapters 5-9 might be of interest considering the topic of this essay. Nonetheless, there is a lot of other interesting number theory in it as well.