Quadratic Reciprocity For Non-Mathematicians

Ahmar Arshad

Received June 29, 2023
Accepted November 05, 2023
Electronic access November 30, 2023

Quadratic reciprocity deals with the solvability of quadratic equations modulo prime numbers. It deals with solving the congruence $x^2 \equiv a(mod p)$. Quadratic reciprocity is an important and interesting part of mathematics with many practical uses in computer science and cryptography. For example, the first probabilistic public-key encryption scheme relies on calculations that can only be done efficiently using the law of quadratic reciprocity. This paper presents a proof of quadratic reciprocity. To make the paper self-contained and accessible for high school readers unfamiliar with number theory, we have included all necessary background, including novel explanations and examples. This sets our paper apart from the majority of expository work on the subject, which assumes greater mathematical knowledge on the reader's part.

Introduction

Quadratic reciprocity is a fundamental theorem of number theory, the part of mathematics that focuses on whole numbers. It was initially formulated by Euler and Legendre in the 18th century and given two complete proofs by Gauss in 1801. Euler was studying earlier results of Fermat relating to Pell's equation, which led him to the preliminary form of the law of quadratic reciprocity. However, it wasn't until Gauss published a proof of the quadratic reciprocity that it became a theorem. It was the first nontrivial result in number theory; it had no uses then, but applications of it were found later in the 20th century. Quadratic reciprocity is a theorem in number theory that has greatly advanced our understanding of prime numbers and congruences. It deals with the solvability of quadratic equations modulo prime numbers; in particular, this concept is often used to determine whether congruences of the form $x^2 \equiv a \pmod{p}$ have a solution. However, it is difficult to grasp without the prerequisite knowledge. The purpose of this text is to explain quadratic reciprocity and the prerequisite knowledge in a way that can be understood by readers who may not have an extensive background in mathematics. There are many proofs of quadratic reciprocity and many texts explaining them; however, many of these texts were written for experienced mathematicians and are quite difficult to understand. This expository note differs from others in that, unlike other reviews on quadratic reciprocity, its target audience is high schoolers interested in the topic who may not possess the prerequisite knowledge.

The general topics covered are modular arithmetic, quadratic residues, quadratic reciprocity, and Hensel's lemma. Modular arithmetic and congruences (section 3) are essential for learning about quadratic reciprocity, as quadratic reciprocity is based on the solvability of congruences. Fermat's theorem (Section 4) is key to our understanding of congruences and will be utilized to solve congruences involving prime numbers throughout this text. Prime moduli and power quadratic residues (sections 5 and 6) are essential to quadratic reciprocity, as they provide useful information regarding quadratic congruences and their solutions. Hensel's lemma (Section 8) is not directly used in the proof of quadratic reciprocity presented; however, it is quite useful in dealing with modular arithmetic and the applications of quadratic reciprocity.

The reader should be familiar with derivatives/higher derivatives (only used in the section regarding Hensel's lemma) and prime factorization of integers. However, the reader does not have to be familiar with multivariable calculus, differential equations, or linear algebra, as this text does not utilize these areas of mathematics. Additionally, this text utilizes basic proof techniques like contradiction and induction, but they are used in a way such that readers unfamiliar with these techniques will likely be able to understand the relevant passages. Learning Objectives: After reading this paper, the reader should

- Understand modular arithmetic (which is used in cryptography/computer science) and be able to apply it
- Understand what quadratic residues and non-residues are
- Be able to follow the proof of the law of quadratic reciprocity and be able to apply it to calculate legendre symbols modulo prime numbers
- Understand the connection between calculus and number theory through the use of the Taylor expansion in the proof of Hensel's lemma
- Be familiar with the structure of mathematical proofs.

Modular Arithmetic, Congruence, and Integers

Modular arithmetic is quite similar to normal arithmetic: it is arithmetic on remainders when numbers are divided by a fixed positive integer called a modulus. When doing modular arithmetic, every number is divided by the modulus m, which must be a positive integer and denoted by $a \equiv b \pmod{m}$. To repeat, the integer m is greater than 1, and the remainder upon division by m is always in the range $0, \ldots, m-1$. We are setting a fixed positive integer m and then reducing everything to its remainder by dividing by m. For example, if $m = 5$, then $2+4 \equiv 1 \pmod{5}$. Similarly, $5 \cdot 7 \equiv 3 \pmod{8}$. Thus, in modular arithmetic, there are only finitely many values, in contrast to the infinite range of integers. In modular arithmetic, numbers are generally related by congruences (denoted by $\equiv$), which are essentially the equal signs of the modular world.

Definition 1 Let integers a and b be integers. We say that a divides b if there is an integer c so that $b = ac$. This is written $a|b$; we refer to a as a divisor of b and b as a multiple of a. If a does not divide b, when we write $a \nmid b$.

Definition 2 Let m be a positive integer, which we call the modulus. Then we say that a and b are equivalent modulo m if a-b is a multiple of m. In other words, if a and b, when divided by m, result in the same reminder, then they are congruent modulo m. This is denoted as $a \equiv b \pmod{m}$.

Example 3.1 $19 \equiv 7(mod 4)$ because the difference 19-7=12 is a multiple of 4. By the same logic, we know that $19 \equiv 7(mod 2)$, (mod 6), and (mod 3) as well

In modular arithmetic, the operations of addition, subtraction, and multiplication remain much the same, with the exception that new relations like $1+4 \equiv 0 \pmod{5}$ now result. However, the operation of division is much different, as we will see later in this text. While the functions other than division don't change much, they are not exactly equivalent to their non-modular counterparts. For example, $4+7 = 11$, while $4+7 \equiv 11 \equiv 5 \pmod{6}$, and $16 \cdot 7 = 112$, while $16 \cdot 7 \equiv 112 \equiv 2 \pmod{10}$. Modular arithmetic is key to understanding the other topics in this text: quadratic reciprocity and many of the topics surrounding it, such as Fermat's little theorem, Hensel's lemma, and quadratic residues, are extensions of modular arithmetic and congruences.

The following simple theorem allows us to replace numbers in modular arithmetic.

Theorem 1 If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$.

Proof. If $a \equiv b \pmod{m}$, then we can write a=b+tm, and if $c \equiv d \pmod{m}$, then we can write c=d+sm. This means that

$$a+c = b+tm+d+sm \equiv b+d \pmod{m}$$

Theorem 2 If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. As in the proof of theorem 1, we can write a=b+tm and c=d+sm. Then, multiplying the two gives us

$$ac = (b+tm)(d+sm) = bd+bsm+tmd+tsm^2 \equiv bd \pmod{m},$$

completing the proof.

Lemma 3 Fix an integer m. Then x and y have the same remainder when divided by m if and only if $x \equiv y \pmod{m}$.

Proof. Suppose that $x \equiv y$ and x=am+r, where the remainder r is in the range $0, \ldots m-1$. Then y=x+sm for some integer s, and so y=am+r+sm=(a+s)m+r, showing that y has the same remainder. On the other hand, if x=am+r, then $x \equiv r$, and if y has the same remainder, then $x \equiv r \equiv y$

Definition 3 Let m,n be two nonzero integers. A common divisor of m and n is an integer d so that $d|m$ and $d|n$. The greatest common divisor of m and n is denoted gcd(m,n) or just (m,n). If (m,n)=1 then we say that m and n are coprime.

Example 3.2 16 and 9 are co-prime to each other. The only positive factors of 16 are 1, 2, 4, 8, and 16, and the only factors of 9, are 1, 3, and 9, meaning that the only common factor they share in 1.

The following lemma allows us to confirm the existence of modular inverses (discussed later in this section) and will be used in the proof of Euclid's lemma.

Lemma 4 Let m and n be non-zero integers. Then there exist integers x and y so that xm+ny=(m,n). In particular, if (m,n)=1, there exists an integer x so that $xm \equiv 1 \pmod{n}$.

Proof. Consider the smallest positive combination b=xm+yn where m and n are integers. Then, b must divide x because if it didn't, we could write x=bs+r where r must be less than b. This means we could express r as a smaller combination of x and y, which cannot be true because b is already the smallest combination of x and y. If d is any other common divisor of m and n, then $b = xm+yn \equiv 0 \pmod{d}$, because $m \equiv 0 \pmod{d}$ and $n \equiv 0 \pmod{d}$. So d has to divide b, which means that $d \leq b$, proving that b is the greatest common divisor of x and y. Since b=xm+yn where b is the gcf of x and y, when b=1, we can write 1=xm+yn. Then, we can write xm=1-yn. Because $yn \equiv 0 \pmod{n}$, we get $xm \equiv 1 \pmod{n}$. Euclid's lemma is extremely useful for dividing prime numbers and prime factorization. This will be extremely important for working with prime moduli, which are the basis of quadratic reciprocity and the theorems surrounding it.

Lemma 5 (Euclid's lemma) Suppose that p is prime and $p|ab$. Then $p|a$ or $p|b$. In particular, if $p \nmid a$ and $p \nmid b$, then $p \nmid ab$.

Proof. Because p is prime, the greatest common denominator of a and p is 1. By lemma 4, we can write 1=ax+py. Then, we can multiply both sides of the equation by b, giving us b=bax+bpy. since $p|ab$, $p|bax$, and p must divide bpy. Because p divides both of these terms, it must also divide their sum, b, completing the proof.

Definition 4 Let (m,n)=1 and let x be an integer so that $xm \equiv 1 \pmod{n}$ (such an x must exist by the previous lemma). Then we say that x is the inverse of m modulo n, i.e. $x = m^{(-1)} \pmod{n}$.

Example 3.3 $3^{(-1)} = 7 \pmod{1}0$ because $(3)(7) = 21 \equiv 1 \pmod{10}$. Similarly, $3 = 3^{(-1)} \pmod{8}$ because $(3)(3) = 9 \equiv 1 \pmod{8}$.

The reverse Euclidean algorithm is an efficient method of finding these modular inverses; however, it is unnecessary for the proof of quadratic reciprocity presented in this text.

Modular arithmetic is essential to understanding Quadratic reciprocity. The law of quadratic reciprocity is a theorem about congruences, so it would not exist if not for modular arithmetic. The rest of this text also contains theorems and lemmas based on modular arithmetic and congruences.

Fermat's Little Theorem

Fermat's little theorem simplifies the process of dealing with prime powers, which are quite prevalent in the proofs and applications of quadratic reciprocity.

Definition 5 Let m be a positive integer. A set of integers $r_1, \ldots, r_k$ is called a reduced residue system modulo m if the following are all true:

- Every r_i is coprime with m, for i=1, ...,k.
- No two r_i, r_j with $i \neq j$ are equivalent modulo m.
- Every integer n that is coprime to m is equivalent modulo m to exactly one r_i

Each individual number in a reduced residue set is often called a residue.

For any prime p, the set $1, 2, \ldots, p-1$ is a reduced residue system. This is because every natural number less than p is co-prime to it. Any other integer not divisible by p is equivalent to exactly one number in the range. $(1, 2, \ldots, p-1)$ modulo p. The following lemma is quite useful as it provides us with a straightforward method of determining a reduced residue system for some prime p.

Lemma 6 Suppose that p is prime and $p \nmid a$. Then $\{a, 2a, \ldots, (p-1)a\}$ is a reduced residue system.

Proof. Since $p \nmid a$, we know that (a,p)=1, and so we have an inverse for a modulo p, say $ax \equiv 1 \pmod{p}$. Now, the prime number p will not divide ja for $j = 1 \ldots p-1$ (by the fundamental theorem of arithmetic) because it does not divide either factor j or a. So, the first condition for a reduced residue set is satisfied, (ja,p)=1. If $ja \equiv ka \pmod{p}$, we can multiply by the inverse x and use our theorems from Section 4 to infer $j = j_1 \equiv jax \equiv kax \equiv k_1 = k \pmod{p}$. So, no two of the residues ja,ka are equivalent. Also, if n is any integer coprime to p, then nx is coprime to p (by the fundamental theorem of arithmetic) because p does not divide either n or x, so it is equivalent to some j in the range $(1, 2, \ldots p-1)$. This means that $n \equiv n_1 \equiv nx_a \equiv ja$, so every integer coprime to p is equivalent to some number in the set $a, 2a \ldots (p-1)a$.

The following result is extremely useful when dealing with congruence modulo p and primes in general. It will be essential to many of the proofs in this text.

Theorem 7 Fermat's little theorem: Suppose that p is a prime number, and a is any integer. Then $a^p \equiv a \pmod{p}$. If in addition we know that (a,p)=1, then $a^{(p-1)} \equiv 1 \pmod{p}$.

Proof. : If $(a, p) \neq 1$, then a is divisible by p. This means that $a \equiv 0 \pmod{p}$. Additionally, $a^p \equiv 0 \pmod{p}$, meaning that $a^p \equiv a \equiv 0 \pmod{p}$. To prove this theorem when (a,p)=1, we can look at the sequence $a, 2a \ldots a(p-1)$. By lemma 6, we know that $a, 2a, \ldots, (p-1)a$ is a reduced residue system as well, so when every term in the sequence is multiplied by some number a, every term will remain distinct modulo p, so the set will still be a reduced residue system modulo p). All the terms of any reduced residue system modulo p, when multiplied together, must result in the same product modulo p; this is because any reduced residue set modulo p can be obtained by adding or subtracting some multiple of p from every term in any other reduced residue system modulo p, and $p \equiv 0 \pmod{p}$. Adding $0 \pmod{p}$ to every term will not affect its product modulo p. Thus, we can write $a \cdot 2a \ldots \cdot a(p-1) \equiv 1 \cdot 2 \ldots \cdot (p-1) \pmod{p}$ (both sides of the congruence are products of every term in a reduced residue system modulo p). Then, we can factor out an a from each term, giving us $a^{(p-1)}(1 \cdot 2 \ldots \cdot (p-1))$ (each term in the sequence was multiplied by a, and there were p-1 terms in the sequence, so, because we factored out an a from each term, we have to multiply by $a^{(p-1)}$). Then, we can rewrite $(1 \cdot 2 \ldots \cdot (p-1))$ as (p-1)!, giving us $(p-1)! \equiv a^{(p-1)\cdot(p-1)!} \pmod{p}$. Then, we can divide both sides of the congruence by (p-1)!, giving us $a^{(p-1)} \equiv 1 \pmod{p}$ (This is supported by lemma 4) because p does not divide any integer in the set $1, 2, \ldots p-1$, meaning that it does not divide (p-1)!, so there is some inverse of (p-1)! modulo p), completing the proof.

Fermat's Theorem is essential to the proof of Euler's criterion, which is necessary for proving quadratic reciprocity and calculating Legendre symbols.

Prime Modulus

If we take an integer-coefficient polynomial and examine its values modulo p, we obtain a polynomial modulo p. While the introduction of congruences makes polynomials more difficult to work with, we can still transfer some of our knowledge of polynomials over real numbers. The degree of a congruence $f(x) \equiv 0(mod\, p), where f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{(n-2)}x^{(n-2)} \ldots a_0$ is n so long as a isn't divisible by p.

Definition 6 Consider the integer-coefficient polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{(n-2)}x^{(n-2)} \ldots a_0$. Let j be the largest integer such that $a_j \not\equiv 0 \pmod{m}$; the degree of the congruence

$f(x) \equiv 0 \pmod{m}$ is equal to j. If no such value of j exists (all coefficients in the function are congruent to $0 \pmod{m}$), then the congruence has no degree. For example, the degree of the congruence $9x^3 + 5x^2 + 6x - 2 \equiv 0 \pmod{3}$ is 2.

A congruence like $x \equiv 1 \pmod{2}$ has infinitely many integer solutions (all odd integers). but only 1 solutions modulo 2 (namely 1). The following theorem can be used to determine the maximum number of solutions a congruence can have based on its degree. This result is somewhat similar to the fundamental theorem of algebra.

Theorem 8 If the polynomial congruence $f(x) \equiv 0 \pmod{p}$ is of degree n, then there are at most n solutions $\pmod{p}$

Proof. If a congruence has a degree of 0, then it has 0 solutions because the congrence $f(x) \pmod{p}$ could be written as $a \pmod{p} where a (\not\equiv) 0 \pmod{p}$. If a congruence only is of degree 1, then it only has one solution. We will assume that this is true for all degrees $< n$ (this will be our induction hypothesis). We assume by way of contradiction that $f(x) \equiv 0 \pmod{p}$, of degree n, has more than n solutions. Then, let $f(x) \equiv 0 \pmod{p}$ be a congruence of degree n that has more than n solutions. The leading term of f(x) is $a_n x^n$, and the solutions to the congruence are $b_1, b_2, b_3 \ldots b_n, b_{(n+1)}$ where each solution is unique. Then let

$$g(x) = f(x) - a_n(x-b_1)(x-b_2)(x-b_3)...(x-b_n).$$

g(x) must have a lower degree than f(x) because $a_n x^n$ is the leading term in f(x), and $a_n x^n - a_n x^n = 0$, so g(x) must be at least one degree lower than f(x). The polynomial g(x) must have at least n solutions (because $b_1, b_2 \ldots b_n$ must be solutions). We can look at two cases: where every coefficient in g(x) is divisible by p, and where not every coefficient of g(x) is divisible by p. In the first case, every integer x satisfies the congruence $g(x) \equiv 0 \pmod{p}$. Additionally, as stated earlier, $x = b_{(n+1)}$ is a solution to the congruence $f(x) \equiv 0 \pmod{p}$. Plugging $x = b_{(n+1)}$ to the equation above gives us $0 = 0 - a_n(b_{(n+1)} - b_1)(b_(n+1) - b_2)...(b_{(n+1)} - b_n) \pmod{p}$), or $a_n(b_{(n+1)} - b_1)(b_{(n+1)} - b_2)\ldots(b_{(n+1)} - b_n) \equiv 0 \pmod{p}$. However, $b_{(n+1)} \not\equiv b_1, b_2 \ldots b_n \pmod{p}$, meaning that the congruence is false, thus disproving the statement that every coefficient of g(x) is divisible by p.

Then, we must look at the second case, in which at least one coefficient of g(x) is not divisible by p (meaning that the degree of the congruence $g(x) \equiv 0 \pmod{p}$ has a degree less than n). Since we know that the congruence $g(x) \equiv 0$ can have at most n-1 solutions by induction because its degree is at most n-1, we obtain a contradiction because all of the numbers $b_1, b_2, \ldots, b_n$ are solutions to $g(x) \equiv 0$. Thus, the congruence $f(x) \equiv 0 \pmod{p}$ of degree n can have at most n solutions.

Quadratic Residues

It is important to understand Quadratic Residues before learning about the law of quadratic reciprocity because its purpose is to relate to quadratic congruences modulo a prime. Quadratic residues are used to determine whether quadratic congruences have solutions.

Definition 7 An integer a is a quadratic residue modulo m if the congruence $x^2 \equiv a \pmod{m}$ has a solution; otherwise, a is a quadratic non-residue.

Example 6.1 3 is a quadratic residue modulo 11 because $3 \equiv 25 = 5^2 \pmod{1}1$. Conversely, 8 is not a quadratic residue modulo 11. We can take the residue set 0,1,2,3,4,5,6,7,8,9,10, square each of them, and reduce them modulo 11, giving us 0,1,4,9,5,3,3,5,9,4,1=0,1,3,4,5,9. 8 is not in this final set, meaning that it isn't a quadratic residue modulo 11. Additionally, the residues repeat after they reach $(\frac{p-1}{2})^2$ For example, taking the residues of x^2 modulo 11, we get 1,4,9,5,3,3,5,9,4,1. The residues modulo 11 repeat after reaching 5^2, which is equal to $(\frac{p-1}{2})^2$

It is important to note that while all perfect squares are quadratic residues modulo any m, not all quadratic residues are perfect squares. For example, $3^2 \equiv 9 \pmod{11}$ (this works for any perfect square), while $21 \equiv 4 \pmod{17}$ even though 21 is not a perfect square. The following lemma shows that there are as many quadratic residues as there are non-residues modulo p. This is quite useful in general when working with quadratic residues and will aid in the proof of other theorems in this text.

Lemma 9 Let p be an odd prime. Then there are exactly (p-1)/2 quadratic residues mod p, and they are

$$1 = 1^2, 2^2, 3^2, \ldots, (\frac{(p-1)}{2})^2$$

All of these residues are distinct mod p, and any quadratic residue mod p must be equivalent to one of these. There are (p-1)/2 quadratic nonresidues.

Proof. By construction all the numbers $1, 2^2, 3^2, \ldots, ((p-1)/2)^2$ are perfect squares so they are quadratic residues. Also if any a is chosen with (a,p)=1 and $a \equiv b^2$, then b is either in the range $1, 2, \ldots, (p-1)/2$ or it is in the range $(p+1)/2, \ldots, p-2, p-1$. But these are the negatives of the integers in the original range, so if b=p-k, we can take b'=k and then $a = b^2 = (-b)^2 \equiv (p-b) \equiv k^2 \pmod{p}$. So, all the quadratic residues are in that range.

It remains to show that none of the $1, 2^2, 3^2, \ldots, ((p-1)/2)^2$ are repeats. If $m \neq n$ and $m^2 \equiv n^2$, then using sum of squares we have $(m-m)(m+n) \equiv 0 \pmod{p}$. This means that $m \equiv norm + n \equiv 0$. But the numbers $1, 2, \ldots, (p-1)/2$ are distinct (mod p) (their difference is at most $(p-1)/2 - 1 = (p-3)/2 < p$) and their sum m+n is likewise bounded by $2 * \frac{(p-1)}{2} = p-1$. So neither $m \equiv n$ or $m + n \equiv 0$. Thus it is impossible for $m^2 \equiv n^2$

$(\text{mod } p)$ if m,n are distinct integers from the list $1, 2, \ldots, (p-1)/2$.

This shows there are exactly (p-1)/2 quadratic residues. As there are p-1 nonzero residues mod p, there must exist $p-1-\frac{(p-1)}{2} = \frac{(p-1)}{2}$ quadratic nonresidues.

Definition 8 If a and p are coprime, and if a is a quadratic residue modulo p, then we define $(\frac{a}{p}) = 1$; if a,p are coprime and a is a quadratic non-residue modulo p, we define $(\frac{a}{p}) = -1$. Finally, if $p|a$, we define $(\frac{a}{p}) = 0$.

Legendre symbols are used to communicate whether quadratic congruences have solutions. Using the theorems and lemma surrounding these symbols, we can more easily determine whether quadratic congruences have a solution and relate the solvability of different quadratic congruences to each other. It is also important to note that the Legendre symbol $(\frac{a}{p})$ is p-periodic, so $(\frac{a}{p}) = (\frac{(a+p)}{p})$ (This is a consequence of the results in section 4). For example, $(\frac{3}{7}) = (\frac{10}{7}) = -1$.

The following result is quite useful when working with Legendre symbols. It has many practical restrictions, but it theoretically can be used to calculate any Legendre symbol.

Theorem 10 Euler's Criterion: Let p be an odd prime and a be an integer coprime to p. Then, $(\frac{a}{p}) \equiv a^{\frac{(p-1)}{2}} \pmod{p}$.

Proof. By Fermat's theorem, we know that for any a coprime to p, $a^(p-1) \equiv 1 \pmod{p}$ Factoring this, we get

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

Then, we can write

$$(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1) \equiv 0 \pmod{p}$$

This means that every integer must satisfy either $a^{\frac{(p-1)}{2}} - 1 \equiv 0 \pmod{p}$ or $a^{(\frac{(p-1)}{2})} + 1 \equiv 0 \pmod{p}$. Then, by theorem 8, we know that each of these congruences has at most $\frac{(p-1)}{2}$ solutions. There are $\frac{(p-1)}{2}$ quadratic residues modulo p; we will show that all of them are solutions to the congruence $a^{(\frac{(p-1)}{2})} - 1 \equiv 0 \pmod{p}$. If a is a quadratic residue, then $a \equiv b^2 \pmod{p}$. p cannot divide b because p does not divide a (since a is a quadratic residue modulo p). So, we get $a^{(\frac{(p-1)}{2})} \equiv (b^2)^{(\frac{(p-1)}{2})} = b^{(p-1)} \equiv 1 \pmod{p}$. This means that all $\frac{(p-1)}{2}$ quadratic residues must be a solution to the congruence $a^{(\frac{(p-1)}{2})} \equiv (\frac{a}{p}) \equiv 1 \pmod{p}$ If a is a quadratic non-residue, then it must satisfy either $a^{(\frac{(p-1)}{2})} \equiv 1$ or $a^{(\frac{(p-1)}{2})} \equiv -1 \pmod{p}$.

However, we have already established $\frac{(p-1)}{2}$ solutions to the congruence $a^{(\frac{(p-1)}{2})} \equiv 1$, and we know that it can have a maximum of $\frac{(p-1)}{2}$ solutions (by theorem 8), so there must be $\frac{(p-1)}{2}$ solutions to the congruence $a^{(\frac{(p-1)}{2})} \equiv -1 \pmod{p}$ (because $(p-1) - (\frac{(p-1)}{2}) = (\frac{(p-1)}{2})$. When $(\frac{a}{p}) = 0$ (a is divisible by p), $a^{(\frac{(p-1)}{2})} \equiv 0 \pmod{p}$. This means that the congruence $a^{(\frac{(p-1)}{2})} \equiv (\frac{a}{p}) \pmod{p}$ is always true, proving Euler's criterion.

For small primes p, Euler's criterion is a reliable method of determining the value of a Legendre symbol. For example, without this extremely useful theorem, it would be quite strenuous to determine whether or not 6 is a quadratic residue modulo 37. Instead of plugging in 37 different values into the congruence $x^2 \equiv 6 \pmod{37}$, we can simply determine the value of $6^{(\frac{(37-1)}{2})} \pmod{37}$. We know that $6^2 \equiv -1 \pmod{37}$, so $6^{18} \equiv -1^9 \equiv -1 \pmod{37}$, meaning that $(\frac{6}{37}) = -1$. Additionally, because the Legendre symbol is periodic, we know that

$$(\frac{-31}{37}) = (\frac{6}{37}) = (\frac{43}{37}) = (\frac{80}{37}) = -1$$

Euler's criterion can be extremely useful, but it cannot be used to determine the values of Legendre symbols involving very large primes. For example, take the largest prime number, $2^8 2,589,933 - 1$. Euler's criterion could never be used to calculate the value of $(\frac{7}{2^{82,539,933}})$ by hand. However, the weakness of Euler's criterion is solved by the law of quadratic reciprocity. The following lemma shows that Legendre symbols are multiplicative. This fact is extremely useful for simplifying Legendre symbols.

Lemma 11 Let p be an odd prime. Then, $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$

Proof. By Euler's criterion, we know that $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}}, (\frac{b}{p}) \equiv b^{\frac{p-1}{2}} and (\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}}$

Then means that $(\frac{a}{p})(\frac{b}{p}) \equiv a^{\frac{p-1}{2}}.b^{\frac{p-1}{2}}$. Since $a^{\frac{p-1}{2}}.b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}}$

$$(\frac{a}{p})(\frac{b}{p}) \equiv (\frac{ab}{p})$$

Because the only possible values of a Legendre symbol are -1, 0, and 1, both sides of the congruence lie within the set -1,0,1. This means that the difference of both sides must lie in the set -2,0,2. p is an odd prime, so it can only divide the difference of both sides if the difference is zero, meaning that they are equal. Thus, we can replace the congruence sign in the previous equation with an equal sign, giving us

$$(\frac{a}{p})(\frac{b}{p}) \equiv (\frac{ab}{p})$$

In view of the previous lemma, we say that Legendre symbols are multiplicative. This is quite useful in conjunction with Euler's criterion. It allows us to divide Legendre symbols into multiple parts that are easier to calculate and multiply them. For example, to determine the value of $(\frac{27}{11})$, instead of calculating 27^5, we can calculate $(\frac{3}{11})(\frac{3}{11})(\frac{3}{11})$, which only requires us to determine the value of 3^5. Since $3^5 \equiv 1 \pmod{11}$, we know that

$$(\frac{27}{11}) = (\frac{3}{11})(\frac{3}{11})(\frac{3}{11}) = 1^3 = 1$$

The following theorem allows us to Legendre symbols involving negative values.

Theorem 12 If p is an odd prime, then $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ Proof. This theorem is essentially an extension of the fact that $(\frac{a}{p}) \equiv a^{(\frac{(p-1)}{2})} \pmod{p}$ (Euler's Criterion). We know that $(\frac{-1}{p})$ and $-1^{\frac{p-1}{2}}$ are equal to ± 1. If they are congruent, then their difference must be divisible by p, but p is odd, so their difference must be equal to 0 (because the only possible values of their difference are (-2, 0, and 2). Two quantities with a difference of 0 must be equal to each other, so we can write

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

It is important that we are able to easily calculate the values of Legendre symbols involving -1 because it makes it much easier to work with Legendre symbols involving negative numbers. As established earlier, $(\frac{64}{11}) = 1$; we can easily calculate the value of $(\frac{-64}{11})$ by determining the value of $(\frac{-1}{p})$. We know that $(\frac{-64}{11}) = (\frac{64}{11})(\frac{-1}{11})$, so

$$(\frac{-64}{11}) = 1(-1^5) = -1 \tag{1}$$

While Euler's criterion, in principle, can find all Legendre symbols modulo p, the following theorem is a more precise result we will use in the proof of Quadratic Reciprocity.

For the proof of the following result, known as lemma of Gauss, we follow the proof laid out in [1] adding details for ease of reading.

Theorem 13 Lemma of Gauss: Take some prime p and some integer a that is coprime to p. Consider the sequence $a, 2a, 3a, \ldots (\frac{p-1}{2})a$ and their least positive reminders modulo p.If x denotes the number of these remainder that exceed $\frac{p}{2}$, then $(\frac{a}{p}) = (-1)^x$ Proof. This proof is somewhat lengthy, but the idea is to show that $(-1)^x$ and $a^{(\frac{(p-1)}{2})}$ are equivalent modulo p and then use Euler's criterion to show $(-1)^x \equiv (\frac{a}{p})$. As in the proof of Theorem 12, this will show that $(-1)^x = (\frac{a}{p})$. Let $o_1, o_2, o_3, \ldots, o_x$ denote the number of remainders that exceed $\frac{p}{2}$ and let $u_1, u_2, u_3, \ldots, u_y$ represent the remainders that do not exceed $\frac{p}{2}$. Each of the terms in each sequence is distinct, and there are $\frac{p-1}{2}$ terms, so $x + y = \frac{p-1}{2}$. To prove that the terms are distinct, take two terms in the sequence a_j and a_k. j and k must be distinct integers between 1 and $\frac{p-1}{2}$ because a_j and a_k are terms in the sequence a,2a, ... a $\frac{p-1}{2}$. If a_j and a_k are equivalent (mod p), then $a(j-k) \equiv 0 \pmod{p}$. This can only be true of $j - k = 0$ since j and k are both less than p. If $j - k = 0$, then j=k, so no two terms in the sequence can be equivalent. Because Each o_i is greater than $\frac{p}{2}$, we have $p - o_i < \frac{p}{2}$.

The first step in the proof is to show that no p-o_i is equal to any u_i. To prove this, let $o_i \equiv za \pmod{p}$ and $u_i \equiv va \pmod{p}(o_i$ and u_i are congruent to some multiple of a modulo p because they are derived from the sequence $a, 2a, 3a, \ldots, (\frac{p-1}{2})a$. So, if $p - o_i = u_i$, then $p - za \equiv va \pmod{p}$. We can rewrite this as $a(z+v) \equiv 0 \pmod{p}$. $a \not\equiv 0 \pmod{p}$, so the previous equation would imply that $z + v \equiv 0 \pmod{p}$. However, this cannot be true because $1 \leq z \leq \frac{p-1}{2}$ and $1 \leq v \leq \frac{p-1}{2}$ (meaning that p cannot divide z+v).

To review, none of the numbers $p - o_1, p - o_2, \ldots, p - o_x, u_1, u_2, \ldots, u_y$ are repeats. We also know that they all fall in the range $1 \leq m \leq \frac{p-1}{2}$, and there are $x + y = \frac{p-1}{2}$ of them. Thus the list $p - o_1, p - o_2, \ldots, p - o_x, u_1, u_2, \ldots, u_y$ is simply a re-arrangement of the sequence $1, 2, \ldots \frac{p-1}{2}$.

Then, take the sequence $p - o_1, p - o_2, p - o_3, \ldots p - o_x, u_1, u_2, u_3, \ldots, u_y$. Each term in this sequence must be greater than 0 and less than $\frac{p}{2}$ (because $o_i > \frac{p}{2}$ and $u_i < \frac{p}{2}$). This means that

$$(p-o_1)(p-o_2)\ldots(p-o_x)(u_1)(u_2)\ldots(u_y) = (1)(2)\ldots((\frac{p-1}{2}).$$

Since $p - o_i \equiv -o_i \pmod{p}$, we can rewrite the equation above as a congruence:

$$-o_1 \cdot -o_2 \cdot \ldots - o_x \cdot u_1 \cdot u_2 \cdot \ldots u_y \equiv 1 \cdot 2 \cdot \ldots \frac{p-1}{2} \pmod{p}.$$

Then, we can rewrite this as

$$(-1^x)o_1 \cdot o_2 \cdot \ldots o_x \cdot u_1 \cdot u_2 \cdot \ldots u_y \equiv 1 \cdot 2 \cdot \ldots \frac{p-1}{2} \pmod{p}.$$

Because each of the remainders $o_1, \ldots, o_x, u_1, \ldots, u_y$ is equivalent to exactly one of the terms in the sequence $a, 2a, \ldots, \frac{p-1}{2} * a$ the product $o_1 * o_2 * \ldots * o_x * u_1 * \ldots u_y$ is equivalent to the product $a * 2a * \ldots (\frac{p-1}{2})a$ modulo p, so we can write

$$(-1)^x a \cdot 2a \ldots \frac{p-1}{2}a \equiv 1 \cdot 2 \cdot \ldots \frac{p-1}{2} \pmod{p}.$$

Simplifying this gives us

$$(-1^x)(a^{\frac{p-1}{2}}) \equiv 1 \pmod{p}$$

Then we can write $(-1)^x \equiv a^{\frac{p-1}{2}}$. Thus, by Euler's criterion, we get

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

The only possible values of a Legendre symbol are 1 ,0,-1, and the only possible values of $-1^x are 1, -1$. The only possible values of their difference are -2,0,2 and because they are equivalent modulo p, their difference must be equivalent to 0 modulo p. This means that the difference must be zero (note that this is essentially the method used in theorem 12). Thus, we get

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

Definition 9 For any number m, [m] equals the integer less than or equal to m and is known as the floor of m.

The floor function is used to round down. For example, [5.78]=5. If we rounded 5.78 to the nearest integer, we would get 6, but because we are rounding the down using the floor function, we get an answer of 5. Additionally, $m = [\frac{m}{q}]q \cdot + r$ where r is the remainder when m is divided by q. For example, $15 = [\frac{15}{4}] \cdot 4 + 3$.

Consider some s that is equal to $1+2+\ldots x$ for any integer x. The average term in the sequence $1,2,\ldots xis\frac{x+1}{2}$, and there are x terms in this sequence. Thus, $s = \frac{(x)(x+1)}{2}$. For example, $1,2,\ldots 100 = \frac{(100)(101)}{2} = 5050$. This result will be used in the proof of the following theorem.

The following theorem is essentially a sequel of Gauss's lemma. It builds on the same idea and is extremely important to proving quadratic reciprocity.

Theorem 14 If p is an odd prime and (a,2p)=1, then $\frac{2}{p} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$.

Additionally, $\frac{a}{p} = (-1)^t$ where $t = \sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}]$

Proof. We are going to build on the lemma of Gauss and show that the number x from the lemma is equal to t plus a multiple of 2, and since raising -1 to an even power results in 1, the result follows. We are going to calculate the sum $\sum_{j=1}^{\frac{(p-1)}{2}} ja = a+2a+\ldots(\frac{(p-1)}{2})a$ in two different ways, and the equation between them will provide the relation we need. Recall the situation in the proof of Theorem 13: we have formed the products $a,2a,\ldots(\frac{(p-1)}{2})a$ and taken their remainders mod p, arranged into $o_1,o_2,\ldots,o_x,u_1,u_2,\ldots,u_y$ according to whether they are greater than $\frac{p}{2}$ or less than $\frac{p}{2}$. As shown in the previous proof, we know there are no repeats in this list and that $p-o_1,p-o_2,\ldots,p-o_x,u_1,u_2,\ldots,u_y$ is actually just a rearrangement of the list $1,2,\ldots\frac{(p-1)}{2}$. More specifically, we will take each of the products ja and write it in the form $ja = [\frac{ja}{p}] * p + r$ according to the discussion after Definition 9. Those remainders greater than $\frac{p}{2}$ will be in the list $o_1,o_2,\ldots,o_x$ and those remainders less than $\frac{p}{2}$ will be in the list $u_1,u_2,\ldots u_y$ and others will be among the u_i. So,

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] + \sum_{j=1}^{x} o_i + \sum_{j=1}^{y} u_i$$

(this equation is breaking up $\frac{ja}{p}$ into its quotient and remainder) where $\sum_{j=1}^{\frac{p-1}{o}} i$ runs overall values for which o_i is defined and $\sum_{j=1}^{y} u_i$ runs over all values for which u_i is defined. The sequence $p-o_i,p-o_2,\ldots p-o_x,u_1,u_2,\ldots u_y$ has no repeats and is a rearrangement of the sequence $1,2,\ldots\frac{p-1}{2}$, so we can write

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{x} (p-o_i) + \sum_{j=1}^{y} u_i$$

and then we can break up $\sum_{j=1}^{x}(p-o_i)$ into $\sum_{j=1}^{x} p - \sum_{j=1}^{x} o_i$. So we get

$$\sum_{j=1}^{\frac{p-1}{2}} j = xp - \sum_{j=1}^{x} o_i + \sum_{j=1}^{y} u_i$$

Then, using subtraction, we get

$$\sum_{j=1}^{\frac{p-1}{2}} (ja-j) = p(\sum_{j=1}^{\frac{p-1}{2}} [\frac{ja}{p}] - x) + 2\sum_{j=1}^{x} o_i$$

Note that

$$\sum_{j=1}^{\frac{p-1}{2}} (ja-j) = (a-1) + (2a-2) + \ldots + \left(a\frac{p-1}{2} - \frac{p-1}{2}\right)$$
$$= (a-1)\left(1+2+3+\ldots+\frac{p-1}{2}\right).$$

$\sum_{j=1}^{\frac{p-1}{2}} j$ is the sum of all integers between 1 and $\frac{p-1}{2}$ (inclusive), so we can write

$$\sum_{j=1}^{\frac{p-1}{z}} j = \frac{\left(\frac{p-1}{z}\right)\left(\frac{p-1}{z}+1\right)}{2} = \frac{p^2-1}{8}.$$

This summation gives us

$$(a-1)\left(p^2-1\right)/8 = p\left(\sum; \left[\frac{j}{p}\right]\right) - px + 2\sum o_i.$$

Then, simplifying this $(\mod 2)$, using $p \equiv 1 (\mod 2)$ we get

$$\frac{(e-1)\left(p^2-1\right)}{8} \equiv \Sigma_{/}\left[\frac{ia}{p}\right] - x (\mod 2).$$

Now we can outline two cases: if a is odd, we get $a-1$ even, and so $t = \sum_l \left[\frac{la}{p}\right]$ differs from x by a multiple of 2, so, by Gauss's Lemma,

$$(-1)^t = (-1)^x = \left(\frac{a}{p}\right).$$

If $a = 2$, then $aj = 2j \leq p-1$ for all $j = 1,\ldots,\frac{(p-1)}{2}$, so the quotients $\left[\frac{ia}{p}\right]$ are all 0 . Thus in this case, using $a-1 \equiv 1$, we get $\frac{p^2-1}{8} \equiv -x \equiv x (\mod 2)$. So

$$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{(p^2-1)/8},$$

completing the proof. This result has two aspects. First, we get an alternate expression for the number x in the statement of Gauss's lemma, valid for any odd number a. This alternate expression is absolutely critical for our method of proving Quadratic Reciprocity. Secondly, we obtain the precise value of $\left(\frac{\mathrm{f}}{\mathrm{p}}\right)$ as a power of -1 , which we will simplify even further in the sequel. While this isn't considered a part of the *QR* law, it's still a useful result for simplifying Legendre symbols involving even numbers. The following lemma simplifies the task of dealing with Legendre symbols involing two, and its proof provides and example of a use case of theorem 14.

Lemma 15 if p is an odd prime then $\left(-\frac{2}{p}\right) = 1$ when $p \equiv 1,7(\bmod p)$, and $\left(\frac{2}{p}\right)$ = -1 when $p \equiv 3,5(\bmod 8)$. Proof. By theorem 14, we know that $\underset{p}{p)} = (-1)^{\frac{p^2-1}{14}}$, so $\frac{p^2-1}{8} \equiv 0$ (mod 2) (because -1 to any even power is equal to 1). Then, we can multiply both sides of the congruence by 8 and adjust the modulus, giving us $p^2 - 1 \equiv 0$ (mod 16). Then, we can plug in $p \equiv 130(\bmod 16)$ and $7^2 - 1 \equiv 0 \pmod{16}$. This means that $\left(-\frac{1}{p} = 1\right.$ when $p \equiv 1,7(\bmod 16)$ and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3,5(\bmod 16)$. Then, because 16 is divisible by 8 , we get $\frac{2}{p} = 1$ when $p \equiv 1,7(\bmod 8)$ and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3,5(\bmod 8)$, completing the proof.

Law of Quadratic Reciprocity

Using the multiplicatively of Legendre symbols and factoring, we can find the value of any Legendre symbol (excluding $\left(\frac{2}{p}\right)$, even those of the form $\left(\frac{m}{q}\right)$ where m is not prime. We can do this by factoring $\left(\frac{m}{q}\right)$ into symbols of the form $\left(\frac{1}{q}\right)$ where p is prime. The law of quadratic reciprocity states that $\left(\frac{b}{q}\right) = \left(\frac{q}{p}\right)$ unless both q and p are equivalent to 3 modulo 4 , in which case either $\left(\frac{p}{q}\right)$ or $\left(\frac{\mathrm{q}}{\mathrm{p}}\right)$ is equal to 1 while the other is not. For example, take the Legendre symbol $\left(\frac{13}{17}\right)$. Because $13 \geq 3$ (mod 4), we know that $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$; calculating the values of both Legendre symbols confirms this (both are equal to 1). While it is true in this case, a Legendre symbol and its reciprocal are not always equal. For example, take $\left(\frac{7}{11}\right)$. Both 7 and 11 are equivalent to 3 modulo 4 , so $\left(\frac{7}{11}\right) \neq \left(\frac{11}{7}\right)$. We confirm this by calculating the value of both Legendre symbols: $7^{\frac{11-1}{2}} \equiv -1$ (mod 11) while $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = 4^{\frac{7-1}{2}} \equiv 1(\bmod p)$. So, $\left(\frac{7}{11}\right) = -1$ and $\left(\frac{11}{7}\right) = 1$.

Theorem 16 Low of Quadrotic Reciprocity:

$$\left(\frac{0}{q}\right)\left(\frac{0}{p}\right) = (-1)^{\frac{p-1q-1}{2}}$$

where p and q are distinct odd primes. Proof. With Gauss's Lemma and its sequel (theorems 13 and 14), we have already laid most of the technical groundwork for the proof of Quadratic Reciprocity. What remains is comparatively simple, although it may be difficult to determine the motivation at first glance. For ease of reading, we will cover a brief outline of the proof beforehand. By Theorem 14. We know that $\underset{q}{(p)} = (-1)^t$ where $t = \sum_{y=1}^{\frac{(Q-1)}{2}} [py/q]$ and we know that $\left(\frac{q}{p}\right) = (-1)^5$, where $s = \sum_{x=1}^{\frac{(p-1)}{2}} [qx/p]$. Thus $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s+t}$. We will mark out a rectangular grid of exactly $(\frac{(p-1)}{2}) * (\frac{(q-1)}{2})$ points and divide it by a straight line into a subset with s points and another subset with t points. The result will then follow.

Let H be the set of ordered pairs (x,y) such that $1 \leq x \leq \frac{p-1}{2}$, and $1 \leq y \leq \frac{q-1}{2}$. The set H is just a rectangular grid of lattice points in the first quadrant, with its bottom left corner at $(1,1)$ and its top right corner at $(\frac{(p-1)}{2}, \frac{(q-1)}{2})$. There are $\frac{p-1}{2}$ such values of x and $\frac{q-1}{2}$ values of y, meaning that this set has $\frac{(p-1)(q-1)}{4}$ elements.

Imagine that all these points are plotted in the plane; we will divide them into those that lie above the line $y = \frac{g}{p}x$ and those that lie below. Separate H into two subsets, H_1 and H_2, where H_1 contains all points (x,y) such that $qx > py$ (those that lie below the line) and H_2 contains all points (x,y) such that $qx < py$ (those that lie above the line). If $qx = py$, then, by Euclid's lemma, $p \mid qx$. p cannot divide q because they are distinct primes, so if $qx = py$, then $p \mid x$; however, this cannot be true due to the range restriction placed on x (because x is less than p). If (x,y) is in the set H_1, then $1 \leq x \leq \frac{(p-1)}{2}$ and $1 \leq y < (\frac{q}{p})x$, just by the range restriction on x and rearrangement of the inequality $qx > py$. Also, any point satisfying these inequalities belongs to H_1, so the number of points in set H_1 is equal to

$$\sum_{x=1}^{\frac{p-1}{z}} \left[\frac{qx}{p}\right]$$

We get this by looking at the graph formed by inequalities that define H_1. The number of integers in the interval $[1, (\frac{q}{p})x)$ is equal to the number of integers in the range $[1, [(\frac{q}{p})x]]$ because $[(\frac{q}{p})x]$ is the largest integer in that range. 50 the number of integers in $[1, (\frac{q}{p})x)$ is $[(\frac{q}{p})x]$.

Then, we sum up the value of $\frac{\alpha x}{p}$ for every x-value in the interval to get the total amount of elements in subset H_1 Then, we can set up H_2 in the same way, so H_2 consists of ordered pairs (x,y) such that $1 \leq y \leq \frac{q-1}{2}$ and $1 \leq x \leq \frac{py}{q}$. Since H_2 is defined by reversing the roles of p and q, we know that the

number of points in H_2 is equal to

$$\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$$

Recall that the total number of points in H is $\frac{p-1}{2}\frac{p-1}{2}$ as calculated in the beginning of this proof. Thus, the number of ordered pairs in the set H is equal to

$$\sum_{z=1}^{\frac{p-1}{2}} \frac{qz}{p} + \sum_{z=1}^{\frac{q-1}{2}} \frac{pz}{q} = \frac{p-1}{2}\frac{q-1}{2}$$

Then, we can raise -1 to the power of both sides, giving us Finally, by theorem 14, we get

$$(-1)^{\sum_{z=1}^{\frac{p-1}{2}} \frac{qz}{p} + \sum_{z=1}^{\frac{q-1}{2}} \frac{pz}{q}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Finally, by theorem 14, we get

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

One of the most convenient uses for this theorem is the simplification of complex Legendre Symbols. Returning to our previous example, take $2^{82,589,933}$. This integer is extremely large, having over $20,000,000$ digits. Using the law of quadratic reciprocity, we can easily calculate the value of the Legendre $\left(\frac{7}{82.589.933}\right)$. Using Euler's criterion, we would have to calculate value of $7^{\frac{2^{82.589.933}-1}{2}}$ which is not feasible. By the law of quadratic reciprocity, $(\frac{7}{2^{82.589.933}}) = (\frac{2^{82.589.933}}{7}) \cdot (-1)^{\frac{2^{82.589.933}-1}{2}\frac{7-1}{2}}$. For the rest of this calculation, we will let $p = 2^{82,589,933} - 1$. Then, $\left(\frac{p}{7}\right) = \left(\frac{-4}{7}\right)$ because $p \equiv -4 (\bmod 7)$, and $\left(\frac{-4}{7}\right) = -1$. Additionally, $p \equiv -1 \pmod 4$, so $\frac{p-1}{2} \equiv 2 (\bmod 4)$, meaning that $\frac{p-1}{2}$ can be written in the form $4k+2$. This means that $\frac{p-1}{2}$ is an odd number. Thus, $-1^{\frac{p-1}{2}\frac{2-1}{2}} = -1$ because $\frac{p-1}{2} - \frac{7-1}{2}$ is equal to the product of two odd numbers, meaning that it must be odd, and -1 to an even power is always equal to -1 . Finally, we can write $\left(\frac{7}{2^{82,589,933}}\right) = (-1)(-1) = (1)$. Although this calculation was a little tedious, it was made possible by the law of quadratic reciprocity.

Hensel's Lemma

In this section, we present a self-contained proof of Hensel's lemma, which provides us a method of "lifting" the solutions of congruence modulo some prime p to solutions of a congruence modulo p^k for some integer $k > 1$. Before we derive the main result, we develop a few lemmas that are important for dealing with polynomials. This section, unlike the others in this text, includes calculus. Recall that if f is a function, then $f^{(b)}$ is the j th derivative (this notation will be used later in this section).

The following results prowdes a method of proving two functions are equal as long as all their derivatives are equal. It will be used in the proof of Hensel's lemma.

Lemma 17 suppose that $f(x)$ and $g(x)$ are two polynomials with degrees less than or equal to N. If there is a point such thot $f^{(j)}(a) = g^{(b)}(a)$ for all values of $0 \leq j \leq N$, then the polynomiols f and g are equal.

Proof. If $N = 0$, then both $f(x)$ and $g(x)$ are constants, so if they are equal at one point, they are equal everywhere. Then, assume that this lemma holds for polynomials of degrees less than or equal to $N-1$. If the polynomials f and g are of degrees less than or equal to N, then polynomials $f'(x)$ and $g'(x)$ are of degrees less than or equal to $N-1$. Then, let $h = f'(x)$ and $k = g'(x)$. polynomials h and k are of degrees less than or equal to $N-1$, and

$$h^{(j)}(a) = f^{(j+1)}(a) = g^{(j+1)}(a) + k^{(h)}(a)$$

for all values $0 \leq j \leq N-1$. By induction, we know that $h = k$, so that $f' = g'(x)$, meaning that $f(x)$ and $g(x)$ can only differ by a constant. This means that $f(x) = g(x) + C$ for some constant C. However, $f(a) = g(a)$, so $f(a) = g(a) = g(a) + C$, so $C = 0$. Thus, $f(x) = g(x)$, completing the proof.

The following expansion is a familiar expansion from calculus; however, the proof in this text will remain purely algebraic.

Lemma 18 For any polynomial f with degree N,

$$f(x) = \sum_{i=0}^{N} \frac{f^u(a)}{u!}(x-a)^u$$

for all values of x, given that a is any real number.

Proof. Let $g(x) = \sum_{k=0}^{N} \frac{f^{(x)}(a)}{w}(x-a)^w$. This means that $g(x)$ is a polynomial of degree N (Because $(x-a)^u$ will be of degree N when $u = N$). Then, to prove this lemma, we need to prove that $f^{(b)}(a) = g^{(i)}(a)$ for all values $0 \leq j \leq N$ (because lemma 17 will teccosh. This means that

$$g^{(j)}(a) = \frac{f^{(j)}(a)}{f} \cdot j!(a-a)^0 = f^{(h)}(a).$$

Because this works for $0 \leq j \leq N$, lemma 17 tells us that $f(x) = g(x)$, completing the proof. The product of any two consecutive integers is always even because the two integers must be even. By the same logic, the product of any three consecutive integers must always be divisible by $3! = 6$ because one of the integers must be even, and one of the other integers must be divisible by 3 . The following result is a generalization

of this observation, although the proof is different. This lemma will be used to prove that the coefficients of a polynomial used in the proof of Hensel's lemma are whole numbers.

Lemma 19 The product of any n consecutive positive integers is alwoys divisible by $n!$! Proof. We can express the product of any n consecutive integers as $a\cdot(a+1)\cdot(a+2)$...- $(a+n-1)$ where a is the first term in the sequence of consecutive integers. If the product of n consecutive integers is divisible by n !, then

$$\frac{a\langle(a+1)\cdot(a+2)-(a+n-1)}{n!}$$

must be an integer.

$$a\cdot(a+1)\cdot(a+2)\ldots\cdot(a+n-1)=\frac{(a+n-1)!}{(a-1)!}$$

so we can rewrite the previous fraction as

$$\frac{(a+n-1))}{(a-1)(n)}$$

This fraction is equal to the binomial coefficient $\begin{pmatrix} a+n-1 \\ n \end{pmatrix}$, meaning it must be equal to an integer because binomial coefficients are always integers.

Hensel's lemma enables us to "extend" the solutions of congruences so that they apply to congruences with a modulus of a higher degree. This lemma makes the process of finding the solution to congruences with a modulus of the form pk much more efficient.

Theorem 20 Hensel's Lemma: Let $f(x)$ be o polynomial with integrol coefficients of degree N, and let a and b be positive integers such that $f(a)\equiv 0 \pmod{p^b}$. If $f'(a)\not\equiv 0 \pmod{p}$, there must be a unique d such that $f\left(a+dp^b\right)\equiv 0 \pmod{p}^{b+1}$

Proof. Using the Taylor expansion (lemma 18) to rewrite $f(x)$, we get

$$f(x)=\sum_{n=0}^{N}\frac{f^{(n)}(a)}{n!}(x-a)^n,$$

where a is the point we are expanding at. We can then rewrite this as

$$f(x)=f(a)+f'(a)\left(\frac{(x-a)}{1!}\right)+f''(a)\frac{(x-a)^2}{2!}\cdots$$

We want to find some d such that $f(d)\equiv 0 \pmod{p^{b+1}}$. Then, to find the value of $f\left(a+dp^b\right)$, we can plug $x=a+dp^b$ into the Taylor expansion above, giving us

$$f\left(a+dp^b\right)=f(a)+f'(a)\frac{dp^b}{1!}+f''(a)\frac{a^2p^{2b}}{2!}\cdots$$

We want $f\left(a+dp^b\right)$ to be congruent to 0 (mod p^{b+1}), so we can write

$$f(a)+f'(a)\frac{dy^b}{1!}+f''(a)\frac{d^2p^{2b}}{2!}\cdots\equiv 0\left(\bmod p^{b+1}\right).$$

If we can find some value of d for which this is true, we will have proved Hensel's lemma. Every term in this Taylor expansion beyond the second term has p^{2b} as a divisor, and $2b\geq b+1$, so we can rewrite the sum of every term in the sequence beyond the second term as

$$\left(p^{2b}\right)\left(\sum_{n=2}^{N}\frac{f^{(n)}(a)}{n!}d^n p^{b(n-2)}\right).$$

If $\frac{f^{(\mathrm{N})}(a)}{\mathrm{n!}}$ is an integer, then the sum above must be congruent to 0 ($\bmod\ p^b+1$). To prove that $\frac{f^{(n)}(a)}{n!}$ is an integer, let zx^m be a term in $f(x)$. The nth derivative of zx^m is equal to $(zx^{m-n})(m-1)(m-2)\ldots(m-n)$. By lemma 19, the product of any n consecutive terms must be divisible by n !, so $(m-1)(m-2)\ldots(m-n)$ must be divisible by $n!$!, proving that $\frac{f^*(a)}{n!}$ is an integer. This means that all the terms in the Taylor sequence beyond the second term are congruent to $0\left(\bmod p^{b+1}\right)$, so we can write

$$f(a)+f'(a)\frac{dp^b}{1!}\equiv 0\left(\bmod p^{b+1}\right)$$

$$f(a)=tp^b, \text{ so}$$

$$f(a)+f'(a)dp^b=tp^b+f'(a)dpb\equiv 0\left(\bmod p^{b+1}\right)$$

yields

$$t+df'(a)\equiv 0(\bmod p).$$

Then, we can write

$$df'(a)\equiv=t(\bmod p)$$

substituting in $t=\frac{f(\alpha)}{p^b}$ gives us

$$df'(a)\equiv\frac{-f(a)}{p^b}(\bmod p).$$

Some value of d that satisfies this congruence will exist as long as $f'(a)\geqslant 0(\bmod p)$ $f'(a)$ not being equivalent to $0(\bmod p)$ also guarantees the existence of its inverse modulo p (referred to later in this section as $f*(a)$)

The main use of Hensel's lemma is to solve congruences with moduli of a high degree. Given the congruence $f(a)\equiv 0\left(\bmod p^b\right)$, as long $f'(a)\geq 0(\bmod p)$, we can find some d such that $f\left(a+dp^b\right)\equiv 0\left(\bmod p^{b+1}\right)$ using the values of $a, f(a)$, and $f'(a)$. As established in the proof of Hensel's lemma,

$$df'(a)\equiv\frac{-f(a)}{p^b}(\bmod p).$$

To find the value of $a+dp^b$, normally, we would divide both sides of the congruence by $f'(a)$, but, in this case, we cannot guarantee that $\frac{f(a)}{f'(x)}$ is a whole number. Instead, because we are working with congruences, we can multiply both sides of the congruence by some $f'(a)$ such that $f^*(a)\cdot f'(a) \equiv 1 \pmod{p}$. This gives us

$$df'(a)f^*(a) \equiv \frac{-f(a)f'(a)}{p^b},$$

and $f*(a)\cdot f'(a) \equiv 1 (\bmod p)$, so we get

$$d \equiv \frac{f(a)f^*(a)}{p^b} (\bmod p).$$

Then, we can multiply both sides of the congruence by p^b and add a to both sides, giving us

$$a+dp^b \equiv a-f(a)f^*(a) (\bmod p).$$

This congruence is satisfied if both sides of the congruence are equal, so when trying to lift a congruence, we use the equation

$$a+dp^b = a-f(a)f'(a).$$

This equation is quite useful as it allows us to "lift" the solution of congruence of some degree to a higher degree. With repeated use of this process, you can find a solution of congruence with a modulus of any degree without having to test every possible value. For example, consider the congruence

$$f(x) = x^3-5x+1 \equiv 0 (\bmod 27).$$

To find the solutions to this congruence, we would normally have to plug in all values between 0 and 27 . Hensel's lemma makes this process much easier, requiring us to only plug in values between 0 and 3. $f(0) = 1 \not\equiv 0(mod3), f(1) = -3 \equiv 0(mod3), f(2) = -1 \not\equiv 0(mod3), and f(3) = 13 \not\equiv 0(mod3)$. The only solution to the congruence modulo 3 is 1, so we can lift this root to find solutions to the same congruence modulo 9 and 27 $f'(x) = 3x^2-5 so f'(1) = -2 \equiv 1 \pmod 3$. Normally, we would have to find the inverse of $f'(1)$ modulo 3, but $f'(1) \equiv 1 \pmod 3$, so $f*(1) \equiv 1 \pmod 3$. Then, we get $1-(-3)(1) = 4$, meaning that 4 is a solution to the congruence $x^3-5x+1 \equiv 0 \pmod 9$. Then, we can lift this solution again; $f(4) = 64-20+1 = 45$ and $f'(4) = 48-5 = 43 \equiv 7 \pmod 9$. This inverse of f'(4) modulo 9 is 4, so we get $4-(4)(45) = -176 \equiv 13 \pmod{27}$, meaning that 13 is a solution to the congruence $x^3-5x+1 \equiv 0 \pmod{27}$. We can test this by plugging 13 into the congruence, giving us $13^3-5(13)+1 = 2133 = 79(27) \equiv 0 \pmod{27}$. It is important to note that we can only lift roots if $f'(a) \not\equiv 0 \pmod p$.

Conclusion

It is remarkable that such varied and rich results can be derived using very little beyond ordinary addition and multiplication.The proofs of quadratic reciprocity given here are quite elementary, given that they require no complex analysis. However, as shown by this paper, they involve the use of extensive mathematical terminology and inference. From modular arithmetic to Quadratic Reciprocity, the study of integers and number theory involves the use of a variety of methods and constructs.

Number theory is not a "solved" field; many unsolved problems are still present (such as the Riemann zeta hypothesis), so the reader should not hesitate to pursue number theory further. In addition, there are many topics in number theory, like the Chinese remainder theorem and linear congruences, that haven't been covered in this text, which can be found in works like Introduction to Analytic Number Theory by Tom. M. Apostol[2].

Readers interested in further pursuing the topics presented in this paper should consult books like "An Introduction to the Theory of Numbers" by Ivan Nivan, Hubert S. Zuckerman, and Hugh L. Montgomery, and "Algebraic Number Theory" by Kenneth Ireland and Michael Rosen. The present paper has not covered some fundamental parts of number theory (namely the prime number theorem), but the reader can find an in-depth discussion of these un-solved topics in books like Unsolved Problems in Number Theory[3].

Acknowledgements

I would like to acknowledge and thank Doctoral Student at Cambridge University (UK) Lukas Kofler for his advice and guidance in writing this paper. Additionally, I would like to thank Mr. Cryster for his generous assistance in composing and refining this paper.

References

1 Ivan Niven and Herbert S. Zuckerman, *An introduction to the theory of numbers*, 1960.

2 A. Tom M., *Introduction to Analytic Number Theory | SpringerLink*, https://link.springer.com/book/10.1007/978-1-4757-5579-4.

3 R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, NY, 2004, pp. 1–2.