PRIMES AND QUADRATIC RECIPROCITY

ANGELICA WONG

Abstract. We discuss number theory with the ultimate goal of understanding quadratic reciprocity. We begin by discussing Fermat's Little Theorem, the Chinese Remainder Theorem, and Carmichael numbers. Then we define the Legendre symbol and prove Gauss's Lemma. Finally, using Gauss's Lemma we prove the Law of Quadratic Reciprocity.

1. Introduction

Prime numbers are especially important for random number generators, making them useful in many algorithms. The Fermat Test uses Fermat's Little Theorem to test for primality. Although the test is not guaranteed to work, it is still a useful starting point because of its simplicity and efficiency.

An integer is called a quadratic residue modulo p if it is congruent to a perfect square modulo p. The Legendre symbol, or quadratic character, tells us whether an integer is a quadratic residue or not modulo a prime p. The Legendre symbol has useful properties, such as multiplicativity, which can shorten many calculations. The Law of Quadratic Reciprocity tells us that for primes p and q, the quadratic character of p modulo q is the same as the quadratic character of q modulo p unless both p and q are of the form $4k+3$.

In Section 2, we discuss interesting facts about primes and "fake" primes (pseudoprimes and Carmichael numbers). First, we prove Fermat's Little Theorem, then show that there are infinitely many primes and infinitely many primes congruent to 1 modulo 4. We also present the Chinese Remainder Theorem and using both it and Fermat's Little Theorem, we give a necessary and sufficient condition for a number to be a Carmichael number. In Section 3, we define quadratic residues and the Legendre symbol, then examine the quadratic character of -1 modulo p (which depends only on whether p is 1 or 3 modulo 4). We show the multiplicative property of the Legendre symbol and prove Gauss's Lemma. Then, using the properties of the Legendre symbol and Gauss's Lemma, we give a neat proof of the Law of Quadratic Reciprocity.

2. General Facts About Primes and Prime-Look-Alikes

Proposition 2.1. *$f(x) = x^p$ is the identity automorphism of $\mathbb{Z}/p\mathbb{Z}$.*

Proof. First, we want to show that f is a field automorphism of $\mathbb{Z}/p\mathbb{Z}$; that is, that f preserves multiplication and addition. That $f(xy) = (xy)^p = x^p y^p = f(x)f(y)$ follows from the commutativity of multiplication.

We want to show that $(x+y)^p \equiv x^p + y^p \pmod{p}$. The binomial theorem gives $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$. It suffices to show that each term of the expansion

Date: August 11, 2008.

except the first and last is zero modulo p; this follows from the fact that $p|\binom{p}{i}$ if and only if $1 \leq i \leq p-1$. This fact is true because $p|p!$ but $p \nmid i!(p-i)!$ for such i, so $p|\frac{p!}{i!(p-i)!} = \binom{p}{i}$. Therefore, $(x+y)^p \equiv x^p + y^p \pmod{p}$.

Now to show f is the identity, let p be a prime. By induction on x, we show that $x^p \equiv x \pmod{p}$. This is clearly true for $x \equiv 0 \pmod{p}$. Assume the claim for x. Applying the conclusion that $(x+y)^p \equiv x^p + y^p \pmod{p}$ to the $x+1$ case, we have $(x+1)^p \equiv x^p + 1^p$. But this is just $x+1$ by the induction hypothesis. So $x^p \equiv x \pmod{p}$ holds for all x. □

Corollary 2.2 (Fermat's Little Theorem)**.** *If p is prime, then for all x such that $x \not\equiv 0 \pmod{p}$, $x^{p-1} \equiv 1 \pmod{p}$.*

Proof. For $x \not\equiv 0 \pmod{p}$, we may multiply both sides of the equality $x^p \equiv x \pmod{p}$ by x^{-1}, yielding $x^p \cdot x^{-1} \equiv x^{p-1} \equiv 1 \pmod{p}$. □

Theorem 2.3. *There exist infinitely many primes.*

Proof. Suppose for a contradiction that there are only finitely many primes; call them $p_1, \ldots, p_k$. Consider the number $x = p_1 \cdots p_k + 1$. If x is not a prime, there exists some prime p_i such that p_i divides x. This implies $x \equiv 0 \pmod{p_i}$, but this is impossible since $x \equiv 1 \pmod{p_i}$ from the definition of x. Therefore x must be prime. Since x is greater than each prime p_i, this is a contradiction. Thus, there must exist infinitely many primes. □

Theorem 2.4. *There are infintely many primes congruent to 1 modulo 4.*

Proof. Suppose for a contradiction that there are only finitely many primes congruent to 1 modulo 4; call them $p_1, ..., p_k$. Let us consider the numbers $x = 2p_1 \cdots p_k$ and $N = x^2 + 1$. Because x is divisible by 2, $x^2 \equiv 0 \pmod{4}$, so $N \equiv 1 \pmod{4}$. Note that $N \equiv 1 \pmod{p_i}$ for each p_i.

Assume N is not prime; then there exists a prime q such that q divides N. Since $q|(x^2+1)$, $x^2 \equiv -1 \pmod{q}$, so $x^4 \equiv 1 \pmod{q}$. Since 4 is the smallest such exponent, Theorem 2.2 implies that 4 divides $q-1$, so $q \equiv 1 \pmod{4}$. Thus, $q = p_i$ for some i, but this is a contradiction: $N \equiv 0 \pmod{q}$ while $N \equiv 1 \pmod{p_i}$ for all i. It follows that N is prime. But since N is greater than each p_i and $N \equiv 1 \pmod{4}$, this is again a contradiction. Since either assuming N is prime or assuming N is composite leads to a contradiction, there must be infinitely many primes congruent to 1 modulo 4. □

Fermat's Little Theorem can be used to test for primality. If there exists a such that $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime. Choosing a randomly and testing this equality yields an efficient randomized primality test known as the Fermat Test. Unfortunately, there exist non-prime numbers that always pass the Fermat Test (see Definition 2.6).

Definition 2.5. An odd composite number n such that $b^{n-1} \equiv 1 \pmod{n}$ is called a **pseudoprime** to the base b.

Note that a pseudoprime to the base b may pass the Fermat Test when the randomly chosen number is equal to b. The smallest pseudoprime is 341, which is pseudoprime to the base 2 [1].

Definition 2.6. An odd composite number n is called **Carmichael** if $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

The difference between a pseudoprime and a Carmichael number is that a pseudoprime passes the Fermat Test for some numbers a, but Carmichael numbers pass the Fermat Test for all numbers a. In other words, a Carmichael number is pseudoprime to every base. The smallest Carmichael number is 561.

Theorem 2.7 (Chinese Remainder Theorem)**.** *If* $\gcd(a, b) = 1$ *then for all* $\alpha, \beta \in \mathbb{Z}$ *there exists a unique* $\gamma \pmod{ab}$ *such that*

$$\gamma \equiv \alpha \pmod{a}$$

$$\gamma \equiv \beta \pmod{b}.$$

Proof. We know $x \equiv \alpha \pmod{a}$ if and only if $x = \alpha + ka$ for some k. We want to show that there exists an integer k such that $\alpha + ka \equiv \beta \pmod{b}$. Since $\gcd(a, b) = 1$, the Euclidean algorithm gives integers r, s such that $1 = ra+sb$. Multiplying both sides of this equation by $(\beta-\alpha)$, we get $(\beta-\alpha)-(\beta-\alpha)ra = (\beta-\alpha)sb$. Taking $k = r(\beta - \alpha)$, we get $ka \equiv (\beta - \alpha) \pmod{b}$, and thus $\alpha + ka \equiv \beta \pmod{b}$.

In order to prove uniqueness modulo ab, we first prove that if $y \equiv 0 \pmod{a}$ and $y \equiv 0 \pmod{b}$, then $y \equiv 0 \pmod{ab}$. Since $a|y$ and $b|y$, then $\operatorname{lcm}(a, b)|y$. In addition, since $\gcd(a, b) = 1$, this implies that $\operatorname{lcm}(a, b) = ab$. Therefore, $y \equiv 0 \pmod{ab}$. Now, let $x \equiv \alpha \pmod{a}$, $x \equiv \beta \pmod{b}$, and $x' \equiv \alpha \pmod{a}$, $x' \equiv \beta \pmod{b}$. Subtracting x' from x, we get $x - x' \equiv 0 \pmod{a}$ and $x - x' \equiv 0 \pmod{b}$ so by above we have $x - x' \equiv 0 \pmod{ab}$, as desired. □

Proof that 561 is a Carmichael number. We need to show that for all a, $a^{560} \equiv 1 \pmod{561}$. We know 561 factors as $561 = 3 \cdot 11 \cdot 17$. Therefore, by the Chinese Remainder Theorem it suffices to show

$$\begin{aligned} a^{560} &\equiv 1 \pmod{3} \\ a^{560} &\equiv 1 \pmod{11} \\ a^{560} &\equiv 1 \pmod{17}. \end{aligned}$$

By Fermat's Little Theorem, since 3 is prime, we know $a^2 \equiv 1 \pmod{3}$. So, $a^{560} \equiv (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod{3}$. Similarly, since $a^{10} \equiv 1 \pmod{11}$, $a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11}$, and since $a^{16} \equiv 1 \pmod{17}$, $a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}$. Therefore, 561 is a Carmichael number. □

Proposition 2.8. *If* $x = p_1 \cdot p_2 \cdots p_k$ *where* p_i *are distinct primes and* $(p_i-1)|(x-1)$ *for all* i*, then* x *is a Carmichael number.*

Proof. Examining the proof that 561 is Carmichael, we see that the same proof works for any x satisfying the hypotheses of the proposition. Consider the Carmichael number 561, which is equal to $3 \cdot 11 \cdot 17$. The key to our proof was using Fermat's Little Theorem for the primes $3, 11$, and 17 to show that $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, and $a^{16} \equiv 1 \pmod{17}$. We were then able to show that $a^{560} \equiv 1 \pmod{3}$ because $(3-1)|560$ and $a^{560} \equiv a^{(3-1)280} \equiv 1 \pmod{3}$. We used the same approach for 11 and 17. □

The converse of the above proposition is true as well [3].

3. Quadratic Reciprocity

Definition 3.1. An integer k is a **quadratic residue** modulo n if it is congruent to a perfect square modulo n; that is, there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv k \pmod{n}$.

Definition 3.2. The **Legendre symbol** $\left(\frac{a}{p}\right)$ for an integer a and an odd prime p is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } (\exists x)\ x^2 \equiv a \pmod{p} \\ 0 & \text{if } a \equiv 0 \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

For nonzero a, the Legendre symbol equals 1 when a is a quadratic residue modulo p and -1 when a is not a quadratic residue modulo p. The Legendre symbol is also known as the **quadratic character** of a modulo p.

Lemma 3.3. *If p is an odd prime and $P = \frac{1}{2}(p-1)$, then $a^P \equiv \left(\frac{a}{p}\right) \pmod{p}$.*

Proof. Case 1. Say $a \equiv 0$. Then $a^P \equiv 0 = \left(\frac{0}{p}\right)$.

Case 2. Say a is a nonzero quadratic residue. Then it suffices to show that $a^P \equiv \left(\frac{a}{p}\right) = 1$. Let $a \equiv b^2$ for some b. Then $a^P \equiv b^{2P} \equiv b^{p-1}$. But we know that $b^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Thus, $a^P \equiv \left(\frac{a}{p}\right)$.

Case 3. Say a is a not a quadratic residue. Then it suffices to show that $a^P \equiv \left(\frac{a}{p}\right) = -1$. Consider $(a^P)^2 = a^{2P}$. Substituting for P we have $a^{2P} = a^{p-1}$, but by Fermat's Little Theorem this is congruent to 1. Thus a^P is a square root of 1 modulo p, so a^P must be congruent to 1 or -1. Consider the polynomial $a^P - 1 \equiv 0$. This is a degree P polynomial so it can have at most P roots. By Case 2, for any quadratic residue a, $a^P = 1$, so each quadratic residue is a root of this polynomial. Since the function $x \mapsto x^2$ is two-to-one on $(\mathbb{Z}/p\mathbb{Z})^*$, exactly half of the nonzero elements modulo p are quadratic residues. Thus, the P quadratic residues are exactly the P roots of the polynomial $x^P - 1$, so if a is not a quadratic residue, $a^P \equiv -1 = \left(\frac{a}{p}\right)$. □

Proposition 3.4. *The Legendre symbol is multiplicative: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Proof. Write $\left(\frac{a}{p}\right)$ as a^P and $\left(\frac{b}{p}\right)$ as b^P. Then, $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = a^P \cdot b^P = (ab)^P = \left(\frac{ab}{p}\right)$. □

Lemma 3.5. *Let p be prime. Then the quadratic character of -1 modulo p depends only on whether p is 1 or 3 modulo 4, that is,*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod{4} \\ -1 & \textit{if } p \equiv 3 \pmod{4} \end{cases}$$

Proof. Case 1. $p \equiv 1 \pmod{4}$. If $a|(p-1)$ then there exists an x such that $x^a \equiv 1 \pmod{p}$, but $x^b \not\equiv 1 \pmod{p}$ for any $0 < b < a$ (see [2] for a proof of this fact). Since $4|(p-1)$, there exists an x such that $x^4 \equiv 1 \pmod{p}$, but $x^2 \not\equiv 1 \pmod{p}$. We know $(x^2)^2 \equiv 1$; therefore, x^2 is either 1 or -1. We have already ruled out

$x^2 \equiv 1 \pmod{p}$, so it must be the case that $x^2 \equiv -1 \pmod{p}$. Thus, -1 is a quadratic residue modulo p.

Case 2. $p \equiv 3 \pmod{4}$. Suppose for a contradiction that $\left(\frac{-1}{p}\right) \neq -1$, that is, there exists an x such that $x^2 \equiv -1 \pmod{p}$. Then, taking the square of both sides of the equation, we have $x^4 \equiv 1$. By Fermat's Little Theorem, we know that $x^{p-1} \equiv 1 \pmod{p}$. Substituting $p-1 = 4k+2$, we have $x^{4k+2} \equiv 1$. We can rewrite this as $x^{4k+2} = x^{4k} \cdot x^2 = (x^4)^k \cdot x^2 = 1^k \cdot x^2 = -1$. But this is a contradiction since $x^{4k+2} = 1$. Thus, -1 is not a quadratic residue modulo p. □

Lemma 3.6 (Gauss's Lemma)**.** *Let $a \not\equiv 0 \pmod{p}$ where p is a prime greater than 2. Let $P = \frac{1}{2}(p-1)$. Form the numbers $a, 2a, 3a, \ldots, Pa$ and reduce each of these numbers to fall within the interval $\left(-\frac{p}{2}, \frac{p}{2}\right)$ by taking them modulo p. Let ν be the number of negative numbers in the resulting set. Then $\left(\frac{a}{p}\right) = (-1)^\nu$. In other words, a is a quadratic residue if ν is even, and a non-residue if ν is odd.*

Proof. Express the numbers $a, 2a, \ldots, Pa$ as congruent to $\pm1, \pm2, \ldots, \pm P$. No number in the set $1, 2, \ldots, P$ will occur more than once, whether positive or negative: if a number occured twice with the same sign, it would mean that two of the numbers in $a, 2a, \ldots, Pa$ were congruent to one another modulo p, which cannot happen since multiplication by a is injective. If the same number occured twice with opposite signs, it would mean that the sum of two numbers in $a, 2a, \ldots, Pa$ was congruent to zero modulo p, which also cannot happen. Therefore, we have that $\{a, 2a, \ldots, Pa\} = \{\pm1, \pm2, \ldots, \pm P\}$ with a definite sign for each number. We get $(a)(2a)\cdots(Pa) \equiv (\pm1)(\pm2)\cdots(\pm P) \pmod{p}$. Canceling $P!$ we get $a^P \equiv (\pm1)(\pm1)\cdots(\pm1) = (-1)^\nu$ where ν is the number of negative signs above. Therefore, $a^P \equiv \left(\frac{a}{p}\right) = (-1)^\nu$ by Lemma 3.3. □

Theorem 3.7 (Law of Quadratic Reciprocity)**.** *Let p and q be two different odd primes. The quadratic character of p $\pmod{q}$ is the same as the quadratic character of q $\pmod{p}$ unless both p and q are of the form $4k+3$, in which case the characters are opposite.*

Another way of saying this is that if p and q are prime numbers, then the product of their Legendre symbols is $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. This product depends only on the parity of the exponent, and is only -1 when both p and q are of the form $4k+3$. There are two cases in proving this theorem: one where $p \equiv q \pmod{4}$ and one where $p \not\equiv q \pmod{4}$. We will need one lemma for each case, but their proofs are very similar.

Lemma 3.8. *Let a be any natural number, and p and q be odd primes. If $p \equiv q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Proof. Using Gauss's Lemma, we know $\left(\frac{a}{p}\right)$ is determined by ν, the number of the integers $a, 2a, \ldots, Pa$ (where $P = \frac{p-1}{2}$) that lie between $\frac{1}{2}p$ and p, or between $\frac{3}{2}p$ and $2p$, etc. (These intervals correspond to values between $-\frac{p}{2}$ and 0 when reduced modulo p as in Gauss's Lemma.) Since Pa is the largest multiple of a that is less than $\frac{1}{2}pa$, the last interval that we have to consider is $((b-\frac{1}{2})p, bp)$, where b is $\frac{1}{2}a$ or $\frac{1}{2}(a-1)$ (whichever is an integer). Thus ν is the number of multiples of a that lie in the intervals $(\frac{1}{2}p, p)$, $(\frac{3}{2}p, 2p)$, ..., $(b - \frac{1}{2}p, bp)$. Dividing through by a, we get the new intervals $(\frac{p}{2a}, \frac{p}{a})$, $(\frac{3p}{2a}, \frac{2p}{a})$, ..., $(\frac{(2b-1)p}{2a}, \frac{bp}{a})$, and ν is now the number of integers in the union of these intervals. Now write p as $4ak + r$ and substitute for p yielding $(2k + \frac{r}{2a}, 4k + \frac{r}{a})$, $(6k + \frac{3r}{2a}, 8k + \frac{2r}{a})$, ..., $(\frac{(2b-1)(4ak+r)}{2a}, 4bk + \frac{br}{a})$. We can disregard the $2k$ and $4k$, etc. and consider $(\frac{r}{2a}, \frac{r}{a})$, $(\frac{3r}{2a}, \frac{2r}{a})$, ..., $(\frac{(2b-1)r}{2a}, \frac{br}{a})$ because changing the endpoints of an interval by an even integer does not change the parity of the number of integers in the interval, and it is only the parity of ν that determines $\left(\frac{a}{q}\right)$. It is now clear from the form of these intervals that the parity of ν depends only on r, and not on the specific prime p which leaves the remainder r when divided by $4a$; thus, $\left(\frac{a}{p}\right)$ depends only on the remainder of p modulo $4a$. □

Lemma 3.9. *Let a be any natural number, and p be an odd prime. If $p \equiv -q \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.*

Proof. Write q as $4ak' - r$. So, $q = 4a(k' - 1) + (4a - r)$. Applying the same method from Lemma 3.8, we know that the remainder of q modulo $4a$ completely determines $\left(\frac{a}{p}\right)$. In order to find the number of integers in the intervals in the case, we need to replace r by $4a - r$. After simplification, and again removing even integers from both ends of the interals, we have the intervals $(-\frac{r}{2a}, -\frac{r}{a})$, $(-\frac{3r}{2a}, -\frac{2r}{a}), \ldots, (-\frac{(2b-1)r}{2a}, -\frac{br}{a})$. Since these intervals are exactly the negatives of the intervals $(\frac{r}{2a}, \frac{r}{a})$, $(\frac{3r}{2a}, \frac{2r}{a})$, ..., $(\frac{(2b-1)r}{2a}, \frac{br}{a})$ the number of integers in the union of the intervals is the same in both cases. Thus, we have the same result, $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. □

Proof of Quadratic Reciprocity. Suppose p and q are odd primes.

Case 1. Let $p \equiv q \pmod 4$; then $p - q = 4a$ for some a and we have the following equalities:

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

In the above equalitites we can disregard the 4 since multiplying by a quadratic residue does not change the quadratic character of $\left(\frac{a}{q}\right)$ or of $\left(\frac{-a}{q}\right)$.

Taking the product of the Legendre symbols, we have

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

By Lemma 3.8, since $p \equiv q \pmod{4a}$, the expression on the right simplifies to $\left(\frac{a}{p}\right)^2\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)$. Then, by Lemma 3.5,

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

which is exactly what we needed.

Case 2. Let $p \not\equiv q \pmod 4$; then one of p or q is congruent to 1 (mod 4) and the other congruent to 3 (mod 4). Thus $p \equiv -q \pmod 4$, so $p + q = 4k$ for some k, and we have

$$\left(\frac{p}{q}\right) = \left(\frac{4k-q}{q}\right) = \left(\frac{4k}{q}\right) = \left(\frac{4}{q}\right)\left(\frac{k}{q}\right) = \left(\frac{k}{q}\right).$$

Similarly, $\left(\frac{q}{p}\right) = \left(\frac{k}{p}\right)$. Since $p \equiv -q \pmod{4k}$, $\left(\frac{k}{p}\right) = \left(\frac{k}{q}\right)$ by Lemma 3.9. Therefore $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{k}{p}\right)\left(\frac{k}{p}\right) = \left(\frac{k}{p}\right)^2 = 1$, as we wanted. □

References

[1] Bach, Eric, and Jeffrey Schallit. Algorithmic Number Theory: Efficient Algorithms. United States of America: Integre Technical Publishing Co., Inc., 1996.

[2] Davenport, H. The Higher Arithmetic: An Introduction to the Theory of Numbers. Cambridge: Cambridge University Press, 1982.

[3] Korselt. Probléme Chinois. L'intermédiaire des mathématiciens, 6, 142 - 143, 1899.

[4] Joyner, D., Kreminski, R., Turisco, J. Applied Abstract Algebra: Rough Draft. `http://web.ew.usna.edu/~wdj/book/node37.html`. Johns Hopkins University Press, 2002.