1 Background

In this section, we examine a few topics that will be necessary in the main paper of which the reader may be unaware.

1.1 Primitive Roots

Definition. *A number g is a primitive root modulo m if every number a coprime to n is congruent to some power of g modulo n. This k is called the index of a to the base g modulo n.*

The primitive residue classes modulo n have many useful properties, but we will not examine them very thoroughly - we only state without proof that n has a primitive root if it is of the form $2, 4, p^k,$ or $2p^k$ where p is an odd prime and $k \geq 1$, and if an integer n has a primitive root, then it has $\phi(\phi(n))$ of them. Additionally, the lowest power of a primitive root a modulo n that is equivalent to 1 modulo n is $\phi(n)$.

1.2 Quadratic Residues

Quadratic Residue. *Let a and n be integers such that $(a, n) = 1$. If the congruence*

$$x^2 \equiv a \pmod{n}$$

has solutions x, then a is a quadratic residue of n. If there are no such solutions, then a is a quadratic non-residue modulo n.

It should be noted that the condition $(a, n) = 1$ allows us to consider only the so-called *primitive* residue classes modulo n, or those classes that are relatively prime to n when searching for quadratic residues.

We now have a result related to quadratic residues.

Theorem. *The product of two quadratic residues a and b modulo n is always a quadratic residue of n, and the product of two quadratic non-residues α and β modulo n is always a quadratic non-residue.*

Proof. Suppose that two integers a and a both relatively prime to n are quadratic residues modulo n. Thus $x^2 \equiv a \pmod{n}$ and $y^2 \equiv b \pmod{n}$ for some x and y. Because a and b are relatively prime to n, we can say $x^2y^2 = (xy)^2 \equiv ab \pmod{n}$, which gives us our first result.

Now suppose there is an x such that $x^2 \equiv \alpha \pmod{n}$, but no y such that $y^2 \equiv \beta \pmod{n}$, and there exists some z such that $z^2 \equiv \alpha\beta \pmod{n}$. This gives us $z^2 \equiv x^2\beta \pmod{n}$, and thus $\left(\frac{z}{x}\right)^2 \equiv \beta \pmod{n}$, which contradicts our assumption that β is a non-quadratic residue. $\square$

Note that we do not address the product of two non-residues - we will state without proof that for primes, the product of two non-residues is a residue, and that the issue is more complex for composite numbers.

1.2.1 Legendre's Symbol, Euler's Criterion, and Jacobi's Symbol

We define Legendre's Symbol $\left(\frac{a}{p}\right)$ as a symbol given the value 1 if a is a quadratic residue of p and the value -1 if a is a quadratic non-residue of p, where p is a prime.

It is, of course, possible to compute Legendre's Symbol directly by trying every congruence class of p, but luckily there is a more elegant way, given by Euler:

Euler's Criterion. *If $(a, p) = 1$ and p is an odd prime, then*

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

Proof. The result can be broken into two results:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ if and only if } a \text{ is a quadratic residue of } p$$

and

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \text{ if and only if } a \text{ is a quadratic non-residue of } p$$

We begin with the second of these. Let a be a quadratic non-residue of a prime p, and b be some natural number less than p. $bx \equiv a$ has a unique solution $x = b^{-1}$, because $(b, p) = 1$. However, $b \not\equiv b^{-1} \pmod{p}$, because otherwise $b^2 \equiv a \pmod{p}$ contradicts the assumption that a is a quadratic non-residue. Thus all natural numbers less than p can be paired into $\frac{p-1}{2}$ pairs (m, n) such that $mn \equiv a \pmod{p}$.

Multiplying these pairs together, we have a product of $\frac{p-1}{2}$ integers all equivalent to a modulo p, which will be equivalent to $a^{\frac{p-1}{2}}$ modulo p and equal to $(p-1)!$. By Wilson's Theorem, we also have $(p-1)! \equiv -1 \pmod{p}$, and so when a is a quadratic non-residue of p, $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Now let a be such that $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. By Wilson's Theorem, $a^{\frac{p-1}{2}} \equiv (p-1)! \pmod{p}$, and thus this implies that the product of all natural numbers $b < p$ produce $\frac{p-1}{2}$ factors equivalent to a. If any b exists such that $bx \equiv a \pmod{p}$ has its unique solution x equivalent to b, then b will not be able to form a product equivalent to a when paired with any other factor of $(p-1)!$, which is a contradiction. Thus there is no b such that $b^2 \equiv a \pmod{p}$, and a is a quadratic non-residue.

Now let a be a quadratic residue of p. We can pick a natural number $b < p$ such that $b^2 \equiv a \pmod{p}$, and thus $b^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$. By Fermat's Theorem, we have $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Finally, we examine the case that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ for some arbitrary a relatively prime to p. Let b be a primitive root modulo p such that a can be written as b^j for some j. From this we have $b^{j \cdot \frac{p-1}{2}} \equiv 1 \pmod{p}$. Because the least power of b that is equivalent to 1 modulo p is $p-1$, $p-1 \mid j \cdot \frac{p-1}{2}$. Thus j

must be even, and $\frac{j}{2}$ is an integer. Thus we have that $(b^{\frac{j}{2}})^2 \equiv a \pmod{p}$, and thus a must be a quadratic residue.

$\square$

You may have noticed that the Legendre Symbol is only defined for a prime p. We define an analogue for composites, *Jacobi's Symbol*, $\left(\frac{a}{n}\right)$, as $\prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$ for n an odd integer, $(a, n) = 1$, and $n = \prod_i p_i^{\alpha_i}$.

Recalling that we never addressed the case of the product of two quadratic non residues of a composite number, it makes intuitive sense that the Jacobi symbol occasionally incorrectly takes the value 1 for a quadratic non-residue, given it is the product of two non-residues. However, it never incorrectly identifies a quadratic residue. Thus it can be used to quickly determine that something is not a quadratic residue modulo n, but cannot prove something as a quadratic residue mod n.

It should be noted that the smallest module M containing two integers a and b is the one generated by $d = (a, b)$. The proof is trivial.

1.3 A Few Small Results

Theorem. *If k is the least positive integer such that $a^k \equiv 1 \pmod{n}$, $a^j \equiv 1 \pmod{n}$, and $k < j$, then $k \mid j$.*

Proof. Let k be the least power such that $a^k \equiv 1 \pmod{n}$. $j = k + m$, with $m \in \mathbb{N}$. if $k \nmid m$, then $m = qk + r$, $0 < r < m$, and $j = (q+1)k + r$. However, $a^j = a^{(q+1)k}a^r \equiv a^r \equiv 1 \pmod{n}$ contradicts the minimality of k. Thus k must divide j. $\square$