1 Background

1.1 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 $x^2 y^2 = (xy)^2 \equiv ab \pmod{n}$, 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.

1.1.1 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:

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

<div align="center">and</div>

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

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 $a^{p-1}2$ modulo p and equal to $(p-1)!$. By Wilson's Theorem, we also have $(p-1)! \equiv -1 \pmod{p}$, and so $\qquad\square$

1.2 Modules

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. $\qquad\square$