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

Note that we do not address the product of two non-residues.

1.1.1 Legendre's Symbol 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.

1.1.2 Euler's Criterion

1.2 Modules