§4.1 Legendre’s Symbol

We’ve already dealt with solving the equation \( ax \equiv b \pmod{n} \), so let’s step it up to solving \( ax^2 + bx + c \equiv 0 \pmod{n} \). This is a good deal more complicated. However, if we let \( y = 2ax + b \) and \( d = b^2 - 4ac \) we get
\[
y^2 - d = 4a^2x^2 + 4abx + b^2 - b^2 + 4ac = 4a(x^2 + bx + c) \equiv 0 \pmod{4an}
\]
If \( ax^2 + bx + c \equiv 0 \pmod{n} \), so we can instead deal with the equation \( y^2 \equiv d \pmod{4an} \), and we can then consider the more general question: “For which \( \frac{d}{4a}x^2 \) does \( x^2 \equiv d \pmod{n} \) have a solution in \( x \)?” Such solutions are called \( \text{Quadratic Residues} \pmod{n} \).

For example, \( \pmod{5} \) the squares are
\[
0^2, 1^2, 2^2, 3^2, 4^2 \quad \text{so} \quad x^2 \equiv d \pmod{5} \quad \text{iff} \quad d \equiv 0, 1, 4 \pmod{5}.
\]

**Definition:** For \( p \) prime, and \((a, p) = 1\)
THE LEGENDRE SYMBOL

\( \left( \frac{a}{p} \right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \\ -1 & \text{otherwise} \end{cases} \)

So \( \left( \frac{4}{5} \right) = 1 \), \( \left( \frac{3}{5} \right) = -1 \).

Clearly if \( a \equiv a' \pmod{p} \) then by definition \( \left( \frac{a}{p} \right) = \left( \frac{a'}{p} \right) \).

§ 4.2 EULER'S CRITERION:

Euler's Criterion: If \( p \) is an odd prime then

\( \left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p} \) for all \( a \) with \( (a, p) = 1 \).

Proof: Let \( r = \frac{1}{2}(p-1) \). For \( (p, k) = 1 \) by Lagrange's theorem, \( x^k \equiv k \pmod{p} \) has, at most, \( k \) solutions. If a solution exists then \( k \) solutions exist since \( (p-x) \not\equiv x \pmod{p} \) is also a solution.

Every \( x = 1, 2, 3, \ldots, (p-1) \) is a solution to \( x^2 \equiv k \) for some \( k \), so there must be \( \frac{(p-1)}{2} \) distinct nonzero quadratic residues.

If \( a \equiv x^2 \pmod{p} \) for some \( x \in \mathbb{F}_p \) then

\( a^r \equiv (x^2)^{r/2} \equiv x^{2r/2} \equiv x \equiv 1 \pmod{p} \) by Fermat's Little Theorem.