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 \( a \) with \( (a, p) = 1 \).

Proof: Let \( \Gamma = \frac{1}{2}(p-1) \). For \( (p, k) = 1 \), by Lagrange's Theorem, \( x^k \equiv k \pmod{p} \) has, at most, \( 2 \) solutions. If a solution exists then \( 2 \) solutions exist since \( (p-x) \equiv x \pmod{p} \) 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 \( x \in \mathbb{Z} \) then
\[ a^\Gamma \equiv (x^2)^\Gamma \equiv x^{2\Gamma} \equiv x^{p-1} \equiv 1 \pmod{p} \] by Fermat's Little Theorem.
FURTHERMORE, \((a^c)^2 \equiv a^{p-1} \equiv 1 \pmod{p}\)

so \(a^c \equiv \pm 1 \pmod{p}\). Since \(a^c \equiv 1 \pmod{p}\)

has, at most, \(r\) solutions by Lagrange’s Theorem

and all \(r\) quadratic residues are solutions.

We must have \(a^c \equiv -1 \pmod{p}\) when

\(a\) is not a quadratic residue

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

Another argument can be made

with primitive roots (Assignment 3).

Euler’s criterion gives us that

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

and so

the Legendre symbol has a multiplicative property,

\(\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)\).

Also, \(\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod{p} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}\)

which we showed last week, when \(p \equiv 1 \pmod{4}\)

\((r!)^2 \equiv -1 \pmod{p}\).

\[\$4.3\] Gauss’ Lemma

For \(a \in \mathbb{C}\) and \(n \in \mathbb{N}\), we define the "numerically least residue" of \(a \pmod{n}\) is
\( \bar{a} \in \mathbb{Z} \) SUCH THAT \( a \equiv \bar{a} \pmod{n} \) AND
\[-\frac{1}{2}n < \bar{a} \leq \frac{1}{2}n. \]
WE CAN DO THIS BECAUSE THERE
ARE \( n \) DISTINCT RESIDUES IN \( (-\frac{n}{2}, \frac{n}{2}] \), SO \( a \)
IS EQUIVALENT TO ONE OF THEM.

For odd \( p \),
LET \( (a, p) = 1 \) AND LET \( a_j := \bar{a}_j \) FOR \( j \in \mathbb{N} \).
WHERE \( \bar{a}_j \) IS DEFINED \( \pmod{p} \).

**Gauss' Lemma** \( \left( \frac{a}{p} \right) = (-1)^L \) WHERE
\( L := \# \{ a_j | a_j < 0 \text{ for } j \leq \frac{p-1}{2} \}. \) (Odd \( p \)).

**Example** Consider \( \left( \frac{4}{5} \right) \). \( a = 4 \) so \( a_1 = \frac{4}{1} = 4 \).
\( a_2 = 4/2 = -2 \), \( \left( \frac{p-1}{2} \right) = 2 \) so \( L = 2 \) AND \( \left( \frac{4}{5} \right) = (-1)^2 = 1 \).

**Proof:** Again let \( \gamma = \left( \frac{a}{p} \right) \). First note
\( |a_1, |a_2|, \ldots, |a_{\gamma}| \) IS A REORDERING OF
OF \( 1, 2, \ldots, \gamma \) SINCE \( |s|/|a_r| = \gamma \) AND
THEY ARE ALL DISTINCT SINCE \( a_j \neq a_k \pmod{p} \).

IF \( j \neq k \), So \( a_j \neq a_k \) IF \( j \neq k \).
IF \( a_j = a_k \) THEN \( a_j = a_k \pmod{p} \) SO
\( j = k \pmod{p} \) SO \( j + k \geq p \), WHICH IS IMPOSSIBLE
FOR \( 1 \leq j, k \leq \frac{p-1}{2} \). So \( a_j \neq a_k \) FOR \( j \neq k \).

\( |a_j| \neq |a_k| \) FOR \( j \neq k \).

So \( a_1, a_2, \ldots, a_\gamma = (-1)^L \gamma! \) BUT \( a_1 \ldots a_\gamma \equiv (a_1)(a_2) \ldots (a_\gamma) \pmod{p} \)