Legendre symbol

Learning Objectives. By the end of class, students will be able to:

- Define the Legendre symbol
- Prove basic facts about the Legendre symbol
- Use the definition and basic facts to find the Legendre symbol for specific examples.

Read: Strayer Section 4.2 through Example 4

Turn in: Exercise 12 Use Euler's Criterion to evaluate the following Legendre symbols

(a) $\left(\dfrac{11}{23}\right)$

Solution: $\left(\dfrac{11}{23}\right) \equiv 11^{(23-1)/2} \equiv 11^{11} \pmod{23}$ By Euler's Criterion. Then

$$11^{11} \equiv (11^2)^5(11) \equiv 6^5(11) \equiv (6^2)(6^3)(11) \equiv (13)(9)(11) \equiv (-90)(11) \equiv -1 \pmod{23}$$

(b) $\left(\dfrac{-6}{11}\right)$

Solution: $\left(\dfrac{-6}{11}\right) \equiv (-6)^{(11-1)/2} \equiv (-6)^5 \pmod{11}$ By Euler's Criterion. Then

$$(-6)^5 \equiv ((6)^2)^2(-6) \equiv 3^2(-6) \equiv -54 \equiv 1 \pmod{11}$$

Definition 1 (Legendre symbol)**.** Let p be an odd prime number and let $a \in \mathbb{Z}$ with $p \nmid a$. The *Legendre symbol*, denoted $\left(\dfrac{a}{p}\right)$, is

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

Theorem 1 (Euler's Criterion)**.** Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. Then

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

We will not prove this today, but we will use it to go over the solution to the reading assignment and to prove the following proposition.

Proposition 1. Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then

Learning outcomes:
Author(s): Claire Merriman

(a) $\left(\frac{a^2}{p}\right) = 1$

(b) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

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

Proof Let p be an odd prime number and $a, b \in \mathbb{Z}$ with $p \nmid a$ and $p \nmid b$. Then a^2 is a quadratic residue modulo p, by definition, so $\left(\frac{a^2}{p}\right) = 1$ by the definition of the Legendre symbol.

If $a \equiv b \pmod{p}$, then either both a and b are quadratic residues modulo p or both a and b are quadratic nonresidues modulo p. Thus $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

For the last part, **??** gives

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

■

Remark 1. Some sources define $\left(\frac{a}{p}\right) = 0$ when $p \mid a$. In this case, Let p be an odd prime and $a \in \mathbb{Z}$. If $p \mid a$, then $a^{(p-1)/2} \equiv 0^{(p-1)/2} \equiv 0 \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Theorem 2. Let p be an odd prime number. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}.$$

Proof Let p be an odd prime number. Then from **??**, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. Since both values are ± 1, we can say $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

If $p \equiv 1 \pmod{4}$, then there exists $k \in \mathbb{Z}$ such that $p = 4k+1$. Thus, $\frac{p-1}{2} = 2k$ and

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2k} = 1.$$

If $p \equiv 3 \pmod{4}$, then there exists $k \in \mathbb{Z}$ such that $p = 4k+3$. Thus, $\frac{p-1}{2} = 2k+1$ and

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2k+1} = -1.$$

■