The Legendre Symbol as the Sign of a Permutation

R. C. Daileda

October 20, 2020

Let p be an odd prime. Recall that if $p \nmid a$ then the *Legendre symbol* is defined to be

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

If r is a primitive root modulo p, we have seen that

$$\left(\frac{a}{p}\right) = (-1)^{\operatorname{ind}_r(a)}. \tag{1}$$

Left multiplication by $a+p\mathbb{Z}$ yields a permutation $\lambda_a : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$. We define $\sigma(a)$ to be the sign of the permutation λ_a. That is, if λ_a is the product of n transpositions, then $\sigma(a) = (-1)^n$. The goal of this note is to provide an elementary proof of the following fact.

Theorem 1. *Let p be an odd prime and suppose $p \nmid a$. Then $\sigma(a) = \left(\frac{a}{p}\right)$.*

Before turning to the proof, we consider $\sigma(a)$ more closely. Let $x + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. The cycle of λ_a containing $x + p\mathbb{Z}$ is just

$$x + p\mathbb{Z}, ax + p\mathbb{Z}, a^2x + p\mathbb{Z}, \ldots, a^{m-1}x + p\mathbb{Z},$$

where $m = \left|a + p\mathbb{Z}\right|$ is the multiplicative order of a modulo p. This is just the coset

$$(x + p\mathbb{Z})\langle a + p\mathbb{Z}\rangle.$$

By Lagrange's theorem there are exactly $\frac{p-1}{m}$ disjoint cosets of $\langle a + p\mathbb{Z}\rangle$. Thus, λ_a is the product of $\frac{p-1}{m}$ disjoint m-cycles.

An m-cycle has sign $(-1)^{m-1}$, since

$$(x_1\, x_2\, \ldots\, x_m) = (x_1\, x_2)(x_1\, x_3)\cdots(x_1\, x_m).$$

It follows that

$$\sigma(a) = \operatorname{sgn}(\lambda_a) = ((-1)^{m-1})^{(p-1)/m}, \tag{2}$$

where m is the multiplicative order of a modulo p. Since $a \equiv r^{\operatorname{ind}_r(a)} \pmod p$, we find that

$$m = \frac{p-1}{(p-1, \operatorname{ind}_r(a))}.$$

Thus (2) becomes

$$\sigma(a) = (-1)^{(m-1)(p-1,\operatorname{ind}_r(a))}. \tag{3}$$

We can now prove Theorem 1.

Proof of Theorem 1. As above, let m be the multiplicative order of a modulo p. If m is odd, then (3) shows that $\sigma(a) = 1$. Since $(p-1, \mathrm{ind}_r(a))m = p-1$ and $p-1$ is even, we conclude that $(p-1, \mathrm{ind}_r(a))$ is even. In particular, $2 | \mathrm{ind}_r(a)$. But this means that $\left(\frac{a}{p}\right) = 1$, by (1). Hence $\sigma(a) = 1 = \left(\frac{a}{p}\right)$ in this case.

Now suppose that m is even. Then (3) becomes

$$\sigma(a) = (-1)^{(p-1, \mathrm{ind}_r(a))}.$$

If $\mathrm{ind}_r(a)$ is even, then 2 divides $(p-1, \mathrm{ind}_r(a))$. Hence

$$\sigma(a) = (-1)^{(p-1, \mathrm{ind}_r(a))} = 1 = (-1)^{\mathrm{ind}_r(a)} = \left(\frac{a}{p}\right).$$

If $\mathrm{ind}_r(a)$ is odd, then $(p-1, \mathrm{ind}_r(a))$ is odd, and we have

$$\sigma(a) = (-1)^{(p-1, \mathrm{ind}_r(a))} = -1 = (-1)^{\mathrm{ind}_r(a)} = \left(\frac{a}{p}\right).$$

Thus $\sigma(a) = \left(\frac{a}{p}\right)$ whenever m is even as well. This finishes the proof.

□

A more elegant, but less illuminating, proof can be given using character theory. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is an abelian group, it is isomorphic to its dual. As $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of even order, it follows that there is a unique character of $(\mathbb{Z}/p\mathbb{Z})^\times$ of order 2. The Legendre symbol fits this description. But $\sigma(r) = (-1)^{(p-1, \mathrm{ind}_r(r))} = -1$, so σ also has order 2 in the character group. Thus $\left(\frac{\cdot}{p}\right) = \sigma(\cdot)$.