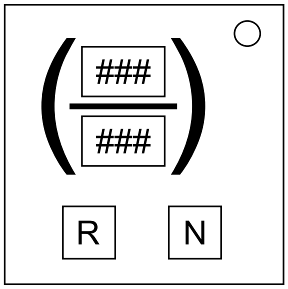
On the Subject of the Legendre Symbol



For those of you who were afraid of fractions in grade school, be thankful you didn't have to deal with these.

- Each display shows a whole number between 1 and 999.
- The number on the top display is guaranteed to be less than the number on the bottom display.
- The number on the bottom display is guaranteed to be a three-digit prime number.
- To disarm this module, let q and m be the numbers on the top and bottom displays respectively. If q is a quadratic residue modulo m, press the button labeled "R." Otherwise, press the button labeled "N."
- Pressing the wrong button will administer a strike and cause the numbers on the displays to change.

Useful Notes on Quadratic Residues

An integer q is said to be a quadratic residue modulo m if it is congruent to some perfect square modulo m, that is, if there exists some integer x such that $x^2 \equiv q \pmod{m}$. If no such value exists, then q is said to be a quadratic nonresidue modulo m.

For example, since perfect squares leave remainders of 0, 1, 4, 5, 6, and 9 when divided by 10, any number that also leaves one of these remainders when divided by 10 (including said remainders themselves) is a quadratic residue modulo 10. Any other number is a quadratic nonresidue.

In the special case where the modulus is an odd prime p, quadratic residuosity can be described using the Legendre symbol, defined as follows:

$$\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{if q is a quadratic residue modulo p, but not a multiple of p} \\ -1 & \text{if q is a quadratic nonresidue modulo p} \\ 0 & \text{if q is a multiple of p} \end{cases}$$

(The notion of a "multiple" in the above definition includes negative numbers and zero. For example, 14, 49, 0, and -21 are all considered to be multiples of 7.)

Note that the third case should never apply in the context of this module, since the Legendre symbol on the module is guaranteed to satisfy $0 < q < p$. The third case is only enumerated here for the sake of mathematical completeness.

Properties of the Legendre Symbol

The Legendre symbol has several interesting properties, including but not limited to the following:

1. **Periodicity.** Let p be an odd prime. If $a \equiv b \pmod{p}$, then:

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

2. **Total Multiplicativity.** Let p be an odd prime. Then for all integers a, b:

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

This can also be extended to three or more factors, a fact easily proven by induction.

3. **Quadratic Reciprocity.** Let p and q be distinct odd primes. Then:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}$$

Since a Legendre symbol consisting of two distinct primes can only take on values of ±1 (a prime number can't be a multiple of a different prime), and since multiplying by ±1 is the same as dividing by ±1, this property can be rewritten as follows:

If $p \equiv 1 \pmod{4}$ or $q \equiv 1 \pmod{4}$, then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Otherwise, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

4. **First Supplement to Quadratic Reciprocity.** Let p be an odd prime. Then:

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

5. **Second Supplement to Quadratic Reciprocity.** Let p be an odd prime. Then:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$$

Computing a Legendre Symbol's Value

By iteratively applying the properties on the previous page, it is possible to express the value of a Legendre symbol in terms of other Legendre symbols with smaller moduli.

Eventually, these moduli will become small enough that the Legendre symbols' values can be computed either by listing out the first few perfect squares and checking their remainders by hand (see the section below) or by recognizing a perfect square in a Legendre symbol's "top" argument, which automatically gives said Legendre symbol a value of +1 by definition.

For example, here's one way to show that 14 is NOT a quadratic residue modulo 41. New terms generated using one of the five rules above are marked accordingly:

$$\left(\frac{14}{41}\right) = \underset{\text{(rule 2)}}{\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)} = \underset{\text{(rule 5)}}{(-1)^{\frac{41^2-1}{8}}} \cdot \underset{\text{(rule 3)}}{\left(\frac{41}{7}\right)} = (-1)^{210} \cdot \underset{\text{(rule 1)}}{\left(\frac{-1}{7}\right)} = 1 \cdot \underset{\text{(rule 4)}}{(-1)^{\frac{7-1}{2}}} = (-1)^3 = \boxed{-1}$$

Since the Legendre symbol evaluates to -1, it follows by definition that 14 is not a quadratic residue modulo 41.

There are multiple ways in which one may apply these rules to arrive at a final answer, some of which are faster and more efficient than others, but they will all lead to the same answer. Experiment with different algorithms to find one that best suits your needs.

Listing Out Quadratic Residues

When listing out quadratic residues modulo p (where p is an odd prime) by hand, it may help to know that exactly half of the integers between 1 and p-1 inclusive are quadratic residues modulo p, while the rest are nonresidues. (The proof of this statement is left as an exercise to the reader.)

The table below lists examples of this for various small odd primes:

p	Quadratic residues modulo p between 1 and p-1 inclusive
3	1
5	1, 4
7	1, 2, 4
11	1, 3, 4, 5, 9
13	1, 3, 4, 9, 10, 12