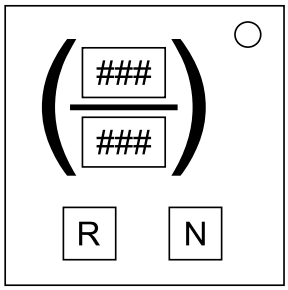
On the Subject of the Legendre Symbol



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:

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

(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.)

An interesting fact about the number of quadratic residues modulo an odd prime is as follows, the proof of which is left as an exercise to the reader:

Proposition 1. If p is an odd prime, then exactly half of the integers between 1 and p-1 inclusive are quadratic residues modulo p; the rest are nonresidues.

Properties of the Legendre Symbol

The Legendre symbol has several properties that offer a way to compute it.

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:

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

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

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

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:

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

By iteratively applying these properties, 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 by either listing out the first few perfect squares and checking their remainders by hand (Proposition 1 can help here) or 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:

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