ENEE/CMSC/MATH 456
Cyclic Groups Class Exercise

From Wikipedia:

Definition [edit]

Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The **Legendre symbol** is a function of a and p defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a non-quadratic residue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases}$$

Legendre's original definition was by means of the explicit formula

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad \text{and} \quad \left(\frac{a}{p}\right) \in \{-1, 0, 1\}.$$

By Euler's criterion, which had been discovered earlier and was known to Legendre, these two definitions are equivalent.[2] Thus Legendre's contribution lay in introducing a convenient *notation* that recorded quadratic residuosity of *a* mod *p*. For the sake of comparison, Gauss used the notation *a*R*p*, *a*N*p* according to whether *a* is a residue or a non-residue modulo *p*. For typographical convenience, the Legendre symbol is sometimes written as (*a* | *p*) or (*a*/*p*). The sequence (*a* | *p*) for *a* equal to 0, 1, 2,... is periodic with period *p* and is sometimes called the **Legendre sequence**, with {0,1,−1} values occasionally replaced by {1,0,1} or {0,1,0}.[3] Each row in the following table can be seen to exhibit periodicity, just as described.

1. Prove that $a \in Z_p^*$ (where p is an odd prime) is a quadratic residue iff $a^{\frac{p-1}{2}}\ mod\ p = 1$.

   Hint: For the backwards direction, use the fact that Z_p^* is a cyclic group, and thus has some generator g.

ENEE/CMSC/MATH 456
Cyclic Groups Class Exercise

2. Let p be an odd prime, such that $p \equiv 3 \ mod \ 4$. For quadratic residues $a \in Z_p^*$, show an efficient algorithm for computing the square roots of a.

Hint: Use the fact from the previous problem that for any $x \in Z_p^*$ $x^{\frac{p-1}{2}} \equiv \pm 1 \ mod \ p$ and use the fact that $2 \cdot \frac{p+1}{4} = \frac{p-1}{2} + 1$.