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.

(a) If a is a quadratic residue then a^{(p-1)/2} mod p = 1.
To show this, we assume a is a QR so a = x^2 for some x \in Z^*_p.
So a^{(p-1)/2} = (x^2)^{(p-1)/2} = x^{p-1} = 1.
where the last equality holds by the "generalized theorem" since p-1 is the order of Z^*_p.

(b) If a^{(p-1)/2} mod p = 1 then a is a QR.
Since Z^*_p is cyclic, it has some generator g and a = g^i for some i \in Z_{p-2}. So g^{i * (p-1)/2} = 1 = g^0.
By a theorem we saw in class, this means that i * (p-1)/2 = 0 mod p-1.
By definition of modulo, this means that (p-1) | i * (p-1)/2.
Rearranging, we get that 2 * (p-1)/2 | i * (p-1)/2, which implies that 2|i. So a = g^i and i is even.
Therefore, a is a QR with square root plus or minus g^{i/2}.

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 $2 \cdot \frac{p+1}{4} = \frac{p-1}{2} + 1$.

Assume a is a QR. So a = x^2 mod p.
Consider a ^{(p+1)/4} = x^{2 * (p+1)/4} = x^{(p-1)/2 + 1} = plus or minus x.