1. Prove that $x^2 \equiv y \pmod{p}$ has exactly two solutions in the cyclic multiplicative group Z_p^* if p is a prime number and $y \in QR_p$. (Hint: use the generator representation, i.e. $x \equiv g^k \pmod{p}$ to reach a conclusion)
2. Prove that the set $S = \{g, g^3, g^5, \ldots, g^{p-2}\}$ is a set of quadratic non-residues (i.e. they are not square of any number in Z_p^*), where g is a primitive root in Z_p^* and p is a prime number. (Hint: you can prove that all the quadratic residues are in $Z_p^* - S$).