

Name:

Problem 1: Let p be an odd prime, $\gcd(a, p) = 1$, and suppose that the equation

$$x^2 \equiv a \pmod{p}$$

does have a solution. In other words a is a quadratic residue of p . What is the value of

$$\left(\frac{a}{p}\right)?$$

Solution:

The *Legendre symbol*, when p is an odd prime and $\gcd(a, p) = 1$ is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p. \end{cases}$$

Since here $x^2 \equiv a \pmod{p}$ has a solution, a is a quadratic residue of p , and

$$\left(\frac{a}{p}\right) = 1.$$