CS 1511 Homework 17

Mathew Varughese, Justin Kramer, Zach Smith

Friday, March 22

32.)

The language QNR = { (a, p) | a is not a quadratic residue modulo p where p is a prime.}

From Euler's criterion, we know that there are (p+1)/2 quadratic residues and (p-1)/2 quadratic nonresidues.

In the private coin protocol, the verifier takes a random number r mod p and a random bit b ∈ {0,1} and sends the prover r^2 mod p if b = 0 and sends the prover ar^2 mod p if b = 1.

If a is a quadratic residue, then the prover has a 1/2 chance of guessing b correctly. Otherwise, the prover is certain of the value of b.

We know from Euler's criterion that if a is not a quadratic residue, then $|\ S\ |$ will be equal to (p-1)/2. If it is a quadratic residue, $|\ S\ |$ will be equal to (p+1)/2. With the set S being the set of quadratic or non-quadratic residues.