Math 218: Elementary Number Theory

Homework 16 : Due December 6

3.6 #5. Let $p = 23$. It is quick work to determine that 1, 4, 9, and 16 are quadratic residues mod 23. On Wednesday in class we will learn Corollary 3.6.3 which will tell you whether -1 is a quadratic residue or nonresidue mod 23. Starting with only those values and Theorem 3.6.2, determine all the quadratic residues and nonresidues mod 23. As the book says, try to do this with as few computations as possible. No credit will be given if you just square the numbers 1 through $\frac{p-1}{2}$.

3.6 #6. (a) If a is a quadratic residue mod p, prove that the multiplicative inverse of a is also a quadratic residue.

(b) If a is a quadratic nonresidue mod p, what is $\left(\frac{a^{-1}}{p}\right)$, i.e. is the multiplicative inverse of a a quadratic residue or quadratic nonresidue? Why or why not?

(c) If a is a quadratic residue mod p, is the additive inverse of a a quadratic residue? Why or why not? Same question if a is a quadratic nonresidue.

3.6 #7. Either prove or disprove the following statement: The sum of the quadratic residues mod p is divisible by p if $p > 3$.

3.6 #9. Prove that $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$.

1. For this problem, assume p is a prime ≥ 7.

   (a) Prove that at least one of 2, 5, and 10 is a quadratic residue of p.

   (b) Prove that there are always two consecutive numbers in Z_p which are quadratic residues of p.