Math 218: Elementary Number Theory

Homework 14 : Due November 18

3.3 #8 (a) Find a and b so that $x^2 + ax + b \equiv 0 \bmod 15$ has more than two solutions.

(b) Find a and b so that $x^2 + ax + b \equiv 0 \bmod 15$ has exactly two solutions.

(c) Find a and b so that $x^2 + ax + b \equiv 0 \bmod 15$ has no solutions.

(d) What sort of general condition can you come up with for a and b which fit into the situation described in (a) or (b) or (c)? ?

3.4 #5abc Solve $x^3 + x - 3 \equiv 0 \bmod 7^3$ by starting with solutions mod 7 and building up like we did with Example 3.4.4.

3.6 #5. Let $p = 23$. It is quick work to determine that 1, 4, 9, and 16 are quadratic residues mod 23. On Monday 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 #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.

3.8 #6. For what odd primes is 5 a quadratic residue? (Prove your answer!)