HW5

This is due Friday, March 14

1. Prove that if p is an odd prime then $x^2 \equiv 2 \bmod p$ has a solution iff $p \equiv 1$ or $7 \bmod 8$.(Hint:Use theorem 3.3).

2. Prove that $x^2 \equiv 16 \bmod p$ has a solution for all prime p. (Hint:Use theorems 2.37, 3.3).

3. Which of the following congruences have solutions and how many:

$$x^2 \equiv 2 \bmod 59$$

$$x^2 \equiv -2 \bmod 59$$

4. Let g be a primitive root(i.e. $g^{p-1} \equiv 1$ and $g^s \not\equiv 1$ for $0 < s < p-1$). Prove that quadratic residues(i.e. solutions of all equations $x^2 \equiv a$ $a \in \mathbb{Z}_p \setminus \{0\}$) are congruent to $g^2, g^4, g^6, \ldots, g^{p-1}$ and that non residues to $g, g^3, g^5, \ldots, g^{p-2}$. Count the number of residues and non residues.

5. Determine how many solutions each of the following congruences has:

$$x^{12} \equiv 16 \bmod 17$$

$$x^{20} \equiv 13 \bmod 17$$

$$x^{48} \equiv 9 \bmod 17$$

$$x^{11} \equiv 9 \bmod 17$$

(Hint: Use theorem 2.37)