Mathematics 437/537 – Homework #4

due Monday, October 30, 2006 at the beginning of class

1. (NZM 3.2 – *20) Show that $(x^2-2)/(2y^2+3)$ is never an integer when x and y are integers.

2. Given any non-zero integer a, define a function f_a from the odd integers to $\{-1,0,1\}$ by the Jacobi symbol $f_a(x) = \left(\frac{a}{x}\right)$. Prove that f_a is periodic with period $4|a|$ (perhaps not the least period).

3. (NZM 3.3 – *13 (H)) Let the reduced residues modulo an odd prime p be divided up into two nonempty sets S_1, S_2 so that the product of two elements in the same set is in S_1 and the product of an element in S_1 and an element in S_2 is in S_2. Prove that S_1 consists of the quadratic residues and S_2 consists of the quadratic nonresidues modulo p.

4. (NZM 3.3 – *21) Let m be a positive odd integer and let $\mathcal{G}$ denote the set of those reduced residue classes $a \pmod m$ such that $a^{(m-1)/2} \equiv \left(\frac{a}{m}\right) \pmod m$. Show that if $a, b \in \mathcal{G}$ then $ab \in \mathcal{G}$ and if $a \in \mathcal{G}$ and $a\bar{a} \equiv 1 \pmod m$, then $\bar{a} \in \mathcal{G}$. (Thus $\mathcal{G}$ is a subgroup of the multiplicative group of reduced residue classes (mod m).)

5. (NZM 3.3 – *14) Suppose that p is a prime with $p \equiv 1 \pmod 4$ and that $a^2 + b^2 = p$ with a odd and positive. Show that $\left(\frac{a}{p}\right) = 1$.

6. (NZM 3.3 – *15(H)) Suppose that p is a prime, $p \geq 7$. Show that $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = 1$ for at least one number in the set $\{1, 2, \ldots, 9\}$.

7. (NZM 3.3 – 9) For which positive integers n do there exist integers x and y with $(x, n) = 1$, $(y, n) = 1$ and $x^2 + y^2 \equiv 0 \pmod n$?

8. Use the algorithm given by the proof in class of Fermat's Lemma 2.13 (NZM p.54) to compute x and y such that $x^2 + y^2 = p$, where p is the prime 100049. You may use a calculator or computer but show the sequence of successive a_k, b_k and m_k with $a_k^2 + b_k^2 = m_k p$.

9. (based on NZM 2.1 – 56) Let p be a prime number and suppose that x is an integer with $x^2 \equiv -2 \pmod p$. Show that $a^2 + 2b^2 = p$ has a solution.

10. Show that a prime number p can be expressed in the form $a^2 + 2b^2$ if and only if $p = 2$ or $p \equiv 1$ or $3 \pmod 8$. (See NZM, 2.1 – 57–60, but you need not slavishly follow their hints).