HOMEWORK 4

DUE 14 FEBRUARY 2012

1. These are two identities used by Euler.

(a) Prove that
$$(x^2 + ny^2)(s^2 + nt^2) = (sx \pm nty)^2 + n(tx \mp sy)^2.$$

(b) Generalize the above to find an identity of the form
$$(ax^2 + cy^2)(as^2 + ct^2) = (?)^2 + ac(?)^2.$$

2. Let n be a positive integer. Prove or disprove and salvage if possible the following statement.

Suppose $N = a^2 + nb^2$ for some integers a, b with $(a, b) = 1$. Assume that $q = x^2 + ny^2$ is a prime divisor of N. Then there exist integers c, d with $(c, d) = 1$ such that $\frac{N}{q} = c^2 + nd^2$.

3. Same as above for $n = 3$ and $q = 4$. (*Hint: you should be able to just adapt your proof from exercise* 2.)

4. Extra credit Prove that if an odd prime p divides $a^2 + 3b^2$ for some relatively prime integers a and b, then p itself can be written as $p = x^2 + 3y^2$ with $(x, y) = 1$. The argument is more complicated because the descent step fails for $p = 2$. Thus, if it fails fro some odd prime p, you have to produce an *odd* prime $q < p$ for which it also fails. *Hint: exercise* 3 *should help.*

5. If p is a prime and $p \equiv 1 \pmod 3$, prove that there exist integers $(a, b) = 1$ such that $p \mid a^2 + 3b^2$.

Note that Exercises 4 and 5 prove that a prime p can be written as $p = x^2 + 3y^2$ for some integers x, y if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

6. Compute $\left(\frac{a}{5}\right)$ for $-10 \le a \le 10$.

7. Compute $\left(\frac{a}{7}\right)$ for $-10 \le a \le 10$.

8. Let p be a prime number. Show that for any integers a, n we have
$$\left(\frac{a + np}{p}\right) = \left(\frac{a}{p}\right).$$

9. Let p be an odd prime number. Show that every reduced residue system $\pmod p$ contains exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic nonresidues $\pmod p$.