HOMEWORK 8

DUE 11 MARCH 2015

SHOW ALL YOUR WORK.

Solve the following problems, and turn in the solutions to *seven* of them.

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. 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 for 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. (a) Compute $\left(\dfrac{a}{5}\right)$ and $\left(\dfrac{a}{7}\right)$ for $-10 \leq a \leq 10$.

(b) Let p be a prime number. Show that for any integers a, n we have

$$\left(\frac{a+np}{p}\right) = \left(\frac{a}{p}\right).$$

7. 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 $\pmod{p}$.

8. Determine whether the integer A is a quadratic residue or nonresidue modulo p for the following integers.

(a) $A = 500, p = 4219$.

(b) $A = 2003, p = 2011$.

(c) $A = 1903, p = 2011$.

9. Let p and q be distinct odd primes. Set $p^* = (-1)^{\frac{p-1}{2}} p$. Prove that

$$\left(\frac{p^*}{q}\right) = 1 \iff p \equiv \pm a^2 \pmod{4q} \text{ for some } \textit{odd} \text{ integer } a.$$

10. (a) Determine whether 888 is a quadratic residue or nonresidue modulo the prime 1999 using exclusively the Legendre symbol.

(b) Determine whether 888 is a quadratic residue or nonresidue modulo 1999 by factoring $888 = 2 \cdot 4 \cdot 111$ and using Jacobi symbols.

(c) Same for $a = -104$ modulo the prime $p = 997$.

11. Use quadratic reciprocity to determine the congruence classes in $(\mathbb{Z}/84\mathbb{Z})^\times$ with $\left(\dfrac{-21}{p}\right) = 1$. This solves the reciprocity step when $n = 21$, i.e. it tells us when $p \mid a^2 + 21b^2$ for some relatively prime integers a, b.