Math 152, Spring 2006
Problem Set 4
Due: Friday, May 5

1. (Problem 1.9 in Cox)

   (a) Prove the reciprocity step for $n = 3$:
   If $p > 3$ is a prime,

   $$p \,|\, x^2 + 3y^2,\ \gcd(x, y) = 1 \iff p \equiv 1\ (3)$$

   (Hint: use quadratic reciprocity and Lemma 1.7 from Cox stating that $p|x^2 + ny^2$ with $\gcd(x, y) = 1$ if and only if the Legendre symbol $\left(\frac{-n}{p}\right) = 1$)

   (b) Prove the analogous statement to part (a) with $n = 2$:
   If $p > 2$ is a prime,

   $$p \,|\, x^2 + 2y^2,\ \gcd(x, y) = 1 \iff p \equiv 1, 3\ (8)$$

2. (Problem 1.15 in Cox) Find congruence classes mod 84 for primes p for which

   $$\left(\frac{-21}{p}\right) = 1$$

   Note: this gives the congruence conditions, and hence solve the reciprocity step, for primes of the form $x^2 + 21y^2$.

3. Recall that Gauss' Lemma stated that

   $$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

   where μ is the number of elements in the set

   $$\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

   which are congruent to a negative least residue. (Again, least residues are the set of residues mod p of the form $(-(p-1)/2, \ldots, 0, 1, \ldots, (p-1)/2)$.)

   (a) Compute μ for $a = 7$ and $p = 17$ and verify that Gauss' Lemma holds in this special case.

(b) Prove Gauss' Lemma by first demonstrating the following congruence is true:

$$\left(\frac{p-1}{2}\right)!\, a^{(p-1)/2} \equiv (-1)^{\mu} \left(\frac{p-1}{2}\right)! \pmod p$$

(c) Use Gauss' Lemma to show that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7\ (8) \\ -1 & \text{if } p \equiv 3, 5\ (8) \end{cases}$$

(d) Prove "Fact II" from class: If p is an odd prime, $\gcd(a,p) = 1$, then

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right)$$

(Hint: This is included in a problem about Gauss' Lemma)