Math 748 Homework 1

Due Monday, September 11

1. This problem leads to finding all primes p that are representable as the sum of two squares.

   (a) Show that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ implies $p \equiv 1 \bmod 4$.

   (b) Show that $\mathbb{Z}[i]$ is Euclidean, i.e., that there exists $N : \mathbb{Z}[i] \to \mathbb{Z}$ such that given nonzero $\alpha, \beta \in \mathbb{Z}[i]$, there are $\gamma, \delta \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \delta$ with $N(\delta) < N(\beta)$. (This implies that $\mathbb{Z}[i]$ is a PID.)

   (c) Show that if $p \equiv 1 \bmod 4$ then p is not a prime element in $\mathbb{Z}[i]$. You may assume the fact that $p \equiv 1 \bmod 4$ implies -1 is a square mod$p$.

   (d) Use parts (b) and (c) to conclude that if $p \equiv 1 \bmod 4$ then $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. You may assume the fact that in a PID an irreducible element is prime (in any integral domain it is true that a prime element is irreducible).

2. Find all p that can be represented as $a^2 - 2b^2$ for some $a, b \in \mathbb{Z}$. Find infinitely many such representations for $p = 7$ (give a recursive description of your infinite family).

3. Find a prime $p > 5$ that does not remain prime in $\mathbb{Z}[\sqrt{-5}]$ yet for which there is no representation $p = a^2 + 5b^2$ with $a, b \in \mathbb{Z}$. This shows that the proof outlined in problem 1 makes essential use of the fact that $\mathbb{Z}[i]$ is a PID.