Mathematics 124 Fall 2003

HOMEWORK ASSIGNMENT # 7
DUE, Friday, November 21

Collaboration: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate, CA, or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class.
Show all your working, and write up your solutions as neatly as possible.

1. **Negative Fields of Class Number One**. Suppose that $p \equiv 3 \mod 4$ is prime. Let $K = \mathbb{Q}(\sqrt{-p})$, and let R be the ring of integers of K, so

$$R = \mathbb{Z}\left[\frac{(1+\sqrt{-p})}{2}\right].$$

   (a) (3 points) Let $q \in \mathbb{Z}$ be prime. Suppose there exists an element $\alpha \in R$ with $N(\alpha) = q$. Prove that

$$q \geq \frac{p+1}{4}.$$

   (b) (3 points) Suppose that $q \neq p$ is an odd prime, and that

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

   Prove there exist integers m, n such that $m^2 + pn^2$ is divisible by q but not by q^2.

   (c) (4 points) Let m, n be as in part (b). Let I be the ideal $I = (m + n\sqrt{-p}, q)$. Prove that any element in R can be written in the form $k + i$, where $i \in I$, and k is an integer such that $0 \leq k < q$.

   (d) (3 points) Prove that I is a prime ideal.

   (e) (4 points) Suppose that I is principal. Show that $I = (\alpha)$, where $\alpha \in R$ is an element such that $N(\alpha) = q$.

   (f) (2 points) Conclude that if all ideals of R are principal, then

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

   for all odd primes q with $4q < p + 1$.

   (g) (1 point) Use this criterion to prove that when $p = 23$, 31 and 47, the ring R is not a principal ideal domain. When $p = 23$, explicitly construct an ideal that is not principal.