MATH 772
SPRING 2011
HOMEWORK 2

Due Monday October 2, 2011.

1. Find all primes p such that:
   a) (5 pt) -7 is a square mod(p).
   b) (5 pt) $\frac{2}{5}$ is a square mod(p).

2. (5 pt) Show that if p is an odd prime then the units of $\mathbb{Z}/p^n\mathbb{Z}$ form a cyclic group. What happens in the case that $p = 2$ (what is the group structure of $U(\mathbb{Z}/2^n\mathbb{Z})$)?

3. (5 pt) Consider the family of quadratic rings of integers $R := \mathbb{Z}[\omega]$ where ω is given by

$$\omega = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3 \bmod(4); \\ \frac{1+\sqrt{d}}{2}, & \text{if } d \equiv 1 \bmod(4). \end{cases}$$

Show that if R is an imaginary quadratic ring of integers ($d < 0$), then $U(R) = \pm 1$ unless $d = -1$ or $d = -3$. What happens in these last two cases? By way of contrast, show that $U(\mathbb{Z}[\sqrt{2}])$ is infinite.

4. (5 pt) Let R be an integral domain with quotient field K. We define the *integral closure* of R to be

$$\overline{R} = \{\alpha \in K | p(\alpha) = 0 \text{ for some monic } p(x) \in R[x]\}.$$

We say that R is integrally closed if $R = \overline{R}$ (that is, R already contains all of its integral elements from K). Prove that any UFD is integrally closed.

5. (5 pt) Let R be an integral domain with quotient field K and $p \in R$ a nonzero prime element. Show that p is also a prime element of $R[x]$.

6. (5 pt) Let F be a field extension of degree n over $\mathbb{Q}$. Suppose that $\omega \in F$ is a root of a monic polynomial in $\mathbb{Z}[x]$. Show that ω is a root of a monic polynomial in $\mathbb{Z}[x]$ of degree no more than n and, in particular, show that the minimal polynomial of ω (over $\mathbb{Q}$) may be taken to be monic and in $\mathbb{Z}[x]$.

7. (5 pt) Let d be a square-free integer. Show that the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ is given by

$$R = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod(4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod(4). \end{cases}$$