MATH 772
SUMMER 2006
HOMEWORK 1

Due Monday June 26, 2006.

1. (5 pt) Let p be a prime integer. Characterize (and find the number of) units in the ring $\mathbb{Z}/p^n\mathbb{Z}$. Use this to find a formula for the number of units in $\mathbb{Z}/n\mathbb{Z}$ where $n > 2$.

2. Find all primes p such that:
   a) (5 pt) -7 is a square mod(p).
   b) (5 pt) $\frac{3}{5}$ is a square mod(p).

3. (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 $U(\mathbb{Z}/2^n\mathbb{Z})$)?

4. Let d be a square-free integer (that is, d is divisible by no square except 1) and consider the ring $R := \mathbb{Z}[\omega]$ where ω is given by

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

These rings are called the *quadratic rings of integers*. If $d > 0$ the quadratic ring of integers is called *real* and if $d < 0$ then the quadratic ring of integers is called *imaginary*.

We define the *norm* (N) by $N(a + b\omega) = (a + b\omega)(a + b\overline{\omega})$ where

$$\overline{\omega} = \begin{cases} -\sqrt{d} \text{ if } d \equiv 2, 3 \text{mod}(4) \\ \frac{1-\sqrt{d}}{2} \text{ if } d \equiv 1 \text{mod}(4) \end{cases}$$

Verify the following properties of the norm.
   a) (5 pt) $N(R) \subseteq \mathbb{Z}$.
   b) (5 pt) $N(x) = 0$ if and only if $x = 0$.
   c) (5 pt) $N(xy) = N(x)N(y)$.
   d) (5 pt) $x \in U(R)$ if and only if $N(x) = \pm 1$.

5. (5 pt) Consider the family of quadratic rings of integers defined above. Show that if R is an imaginary quadratic ring of integers, 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.