Math 568 Homework 1
Spring 2009
Due: Thursday, January 22

1. Remember that there is a norm map $N : \mathbb{Z}[i] \to \mathbb{Z}$ which is given by $N(a+bi) = a^2+b^2$. It is easy to check that for any $\alpha, \beta \in \mathbb{Z}[i]$ we have $N(\alpha\beta) = N(\alpha)N(\beta)$.

   (a) Show that an element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$. Use this to compute the units of $\mathbb{Z}[i]$.

   (b) Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$, then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$ which is congruent to 3 modulo 4.

2. Show that $\mathbb{Z}[i]$ is a principal ideal domain. Proceed as follows:

   (a) Let I be an ideal of $\mathbb{Z}[i]$ and let $\alpha \in I - \{0\}$ be an element such that $N(\alpha)$ is minimized. Consider the multiples $\gamma\alpha$ for $\gamma \in \mathbb{Z}[i]$. Show that these are the vertices of an infinite family of squares which fill up the complex plane. (One such square has vertices $0, \alpha, i\alpha$, and $(1+i)\alpha$.)

   (b) Show with a geometric argument that if I contained anything besides the $\gamma\alpha$, then this would contradict the minimality of $N(\alpha)$.

3. (a) Show that if $p \in \mathbb{Z}$ is a prime with $p \equiv 1 \mod 4$, then -1 is a square modulo p.

   (b) Show that an element p as in (a) cannot be irreducible in $\mathbb{Z}[i]$.

   (c) Prove that any prime p with $p \equiv 1 \mod 4$ is a sum of two squares.

4. Let I be the ideal generated by 2 and $1+\sqrt{-3}$ in the ring $\mathbb{Z}[\sqrt{-3}] = \{a+b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Show that $I \neq (2)$, but $I^2 = 2I$. Conclude that ideals in $\mathbb{Z}[\sqrt{-3}]$ do not factor uniquely into prime ideals. Show moreover that I is the unique prime ideal containing (2) and conclude that (2) is not a product of prime ideals.

5. (a) Suppose all roots of a monic polynomial $f \in \mathbb{Q}[x]$ have absolute value 1. Show that the coefficient of x^r has absolute value $\leq \binom{n}{r}$, where n is the degree of f and $\binom{n}{r}$ is the binomial coefficient.

   (b) Show that there are only finitely many algebraic integers α of fixed degree n, all of whose conjugates (including α) have absolute value 1.

   (c) Show that α as in (b) must be a root of unity.