DUE DATE: APR. 15, 2008

1. By associating each pair $(a, b) \in \mathbb{Z}^2$ with the Gaussian integer $\alpha = a + bi \in \mathbb{Z}[i]$ we see that the number of ways that we can write an integer n as a sum $n = a^2 + b^2$ of two squares is the same as the number of Gaussian integers of norm exactly n, i.e., that

$$\#\left\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 = n\right\} = \#\left\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = n\right\}.$$

The purpose of this question is to use unique factorization in the Gaussian integers to count the number of such α.

Recall that by unique factorization any Gaussian integer α can be written as

$$\alpha = u\pi_1^{s_1} \cdots \pi_m^{s_m}$$

where u is a unit and $\pi_1, \ldots, \pi_\ell$ are primes in $\mathbb{Z}[i]$.

(a) Suppose that p is a prime in $\mathbb{Z}$, $p \equiv 1 \pmod 4$ and that π_1 and π_2 are two distinct primes in $\mathbb{Z}[i]$ with $N(\pi_1) = N(\pi_2) = p$.

Let e be a nonnegative integer. Find a formula in terms of e for the number of pairs (s_1, s_2) with $s_1, s_2 \geq 0$ such that $N(\pi_1^{s_1}\pi_2^{s_2}) = p^e$. (The answer isn't complicated – the hard part is understanding the question).

(b) If q is a prime in $\mathbb{Z}$, $q \equiv 3 \pmod 4$ then q is still prime in $\mathbb{Z}[i]$. Given $f \geq 0$ how many possibilities are there for integers $t \geq 0$ such that $N(q^t) = q^{2f}$? (This is even easier).

(c) If $p = 2$, and given any $f \geq 0$, how many possibilities are there for $t \geq 0$ such that $N((1+i)^t) = 2^f$?

(d) Given a positive integer n let's factor it as

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_0^{f_0} q_1^{2f_1} q_2^{2f_2} \cdots q_\ell^{2f_\ell}$$

where $p_i \equiv 1 \pmod 4$ for all i, $q_0 = 2$ and $q_i \equiv 3 \pmod 4$ for $i \geq 1$.

Putting parts (a), (b), and (c) together, how many possible expressions are there of the form

$$\alpha = u\pi_{1,1}^{s_{1,1}}\pi_{1,2}^{s_{1,2}}\pi_{2,1}^{s_{2,1}}\pi_{2,2}^{s_{2,2}} \cdots \pi_{k,1}^{s_{k,1}}\pi_{k,2}^{s_{k,2}}(1+i)^{t_0} q_1^{t_1} q_2^{t_2} \cdots q_\ell^{t_\ell}$$

with $N(\alpha) = n$? (In the notation above, u is a unit and for each i the elements $\pi_{i,1}$ and $\pi_{i,2}$ are two distinct primes such that $N(\pi_{i,1}) = N(\pi_{i,2}) = p_i$.)

2. Suppose that $I = \langle a, b\rangle$ and $J = \langle c, d\rangle$ are two ideals in a ring R.

(a) Show that $I \subseteq J$ if and only if $a, b \in J$.

(b) Show that $I = J$ if and only if $a, b \in J$ and $c, d \in I$.

3. The prime $p = 13$ factors as $13 = (2+3i)(2-3i)$ in $\mathbb{Z}[i]$. Let $I_1 = \langle 2+3i\rangle$, $I_2 = \langle 2-3i\rangle$ in $\mathbb{Z}[i]$. Let's use the homomorphism theorems and the Chinese remainder theorem to try and understand the ring $\mathbb{Z}[i]/\langle 13\rangle$.

(a) Show that $I_1 \cap I_2 = \langle 13\rangle$ in $\mathbb{Z}[i]$ (This should be a straightforward argument using unique factorization and the fact that $\mathbb{Z}[i]$ is a P.I.D.).

(b) By part (a) and the Chinese remainder theorem,

$$\frac{\mathbb{Z}[i]}{\langle 13\rangle} = \frac{\mathbb{Z}[i]}{\langle 2+3i\rangle} \oplus \frac{\mathbb{Z}[i]}{\langle 2-3i\rangle},$$

and it would be nice to know what the quotients $\frac{\mathbb{Z}[i]}{\langle 2+3i\rangle}$ and $\frac{\mathbb{Z}[i]}{\langle 2-3i\rangle}$ are.

Let $\phi\colon \mathbb{Z}[x] \longrightarrow \mathbb{Z}[i]$ be the homomorphism given by $\phi(f(x)) = f(i)$. The kernel of ϕ is the ideal $\ker\phi = \langle x^2+1\rangle$.

Find the ideal $J_1 = \phi^{-1}(I_1)$ of $\mathbb{Z}[x]$.

(c) Show that the ideals J_1 and $\langle 13, x-8\rangle$ are the same ideal in $\mathbb{Z}[x]$.

(d) By the third homomorphism theorem, $\mathbb{Z}[x]/J_1$ is isomorphic to $\mathbb{Z}[i]/\langle 2+3i\rangle$. Using part (c) show that $\mathbb{Z}[x]/J_1 \simeq \mathbb{Z}/13\mathbb{Z}$.

(e) Similarly, let $J_2 = \phi^{-1}(I_2)$. Show that $J_2 = \langle 13, x-5\rangle$, and again conclude that $\mathbb{Z}[i]/\langle 2-3i\rangle \simeq \mathbb{Z}/13\mathbb{Z}$.

(f) Conclude that $\dfrac{\mathbb{Z}[i]}{\langle 13\rangle} = \dfrac{\mathbb{Z}}{13\mathbb{Z}} \oplus \dfrac{\mathbb{Z}}{13\mathbb{Z}}$.

Bonus mini-question: Explain why $\mathbb{Z}[i]/\langle 13\rangle$ is the same ring as $\mathbb{Z}[x]/\langle 13, x^2+1\rangle$ which is the same ring as $F[x]/\langle x^2+\bar{1}\rangle$, where $F = \mathbb{Z}/13\mathbb{Z}$. Since $(x-\bar{5})\cdot(x-\bar{8}) = x^2+\bar{1}$ in $F[x]$, use the Chinese remainder theorem to see that

$$\frac{\mathbb{Z}[i]}{\langle 13\rangle} \simeq F \oplus F.$$