Math 331: Homework 6, Due Oct 12

The *Gaussian Integers*, denoted $\mathbb{Z}[i]$ is the set

$$\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$$

where i is the complex number $i = \sqrt{-1}$. Addition and multiplication in $\mathbb{Z}[i]$ is inherited from $\mathbb{C}$.

1. Given $a + bi \in \mathbb{Z}[i]$, define the *norm* of $a + bi$ to be

   $$N(a + bi) = a^2 + b^2$$

   Show that this norm is multiplicative. In other words, show that for any $z_1, z_2 \in \mathbb{Z}[i]$, you have

   $$N(z_1 z_2) = N(z_1)N(z_2)$$

   Solution: This is just a matter of computing:

   $$\begin{aligned} N((a+bi)(c+di)) &= N((ac-bd)+(ad+bc)i) = (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ N(a+bi)N(c+di) &= (a^2+b^2)(c^2+d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \end{aligned}$$

2. Find all the units in $\mathbb{Z}[i]$. Justify your answer.

   Solution: We can use our knowledge of complex numbers. The multiplicative inverse of $a + bi$ is $(a - bi)/(a^2 + b^2)$. Thus a unit must have $a^2 + b^2 = 1$. In order for this to be the case, we must either have $a = \pm 1, b = 0$ or $a = 0$, $b = \pm 1$. Thus our units are: $\{\pm 1, \pm i\}$.

3. We will say that a number in $x \in \mathbb{Z}[i]$ is *prime* if you have $x = yz$ (where $y, z \in \mathbb{Z}[i]$) then either y or z is a unit.

   (a) Show that 2 is not prime in $\mathbb{Z}[i]$.
   Solution: $2 = (1 - i)(1 + i)$

   (b) Show that $1 - i$ is prime in $\mathbb{Z}[i]$.
   Solution: Notice that $z \in \mathbb{Z}[i]$ is a unit if and only if $N(z) = 1$. In this case $N(1 - i) = 2$ and therefore if $z = xy$ then $N(z) = 2 = N(x)N(y)$. Thus, either x or y is a unit. $1 - i$ must be prime.

   (c) Show that 3 is prime in $\mathbb{Z}[i]$.
   Solution: If $x \in \mathbb{Z}[i]$ is such that $x|3$ then $N(x)|9$ and thus $N(x) = 3$ or $N(x) = 9$. If $N(x) = 9$ then x is an associate of 3 (x is a unit times 3). If $N(x) = 3$ and $x = a + bi$ then we have $a^2 + b^2 = 3$, which has no integer solutions.

4. (a) Find all the divisors of 10 in $\mathbb{Z}[i]$.
   Solution: Here are the prime divisors:

   $$1 + i, 1 - i, 2 + i, 2 - i$$

(b) Show that any Gaussian integer has only finitely many divisors.

Solution: First note that there are only finitely many numbers with a given norm. In other words, given $n \in \mathbb{N}$, there are only finitely many solutions to $a^2 + b^2 = n$.

Thus, if $z \in \mathbb{Z}[i]$ has norm $N(z)$ then the list of divisors of z must have norms which divide $N(z)$. There are finitely many integer divisors of $N(z)$, each of which has finite many possibilities for Gaussian integers with that norm.

5. Let $p \in \mathbb{Z}$ be a prime integer. Prove that either p is a Gaussian prime or else it is the product of two complex conjugate Guassian primes: $p = \alpha\overline{\alpha}$.

Solution: Here is an important result that you should be able to prove that I'll use:

Lemma. *If $\alpha, \beta \in \mathbb{C}$ such that the imaginary part of α is not zero then there exists $r \in \mathbb{R}$ such that $\beta = r\overline{\alpha}$.*

Suppose $p = xy$ where $x, y \in \mathbb{Z}[i]$ are not units. $N(p) = p^2$ and therefore if $xy = p$ we must have $N(x)N(y) = p^2$. Since x, y are not units, we must have $N(x) = N(y) = p$. Now, applying the lemma, you should be able to see that $x = \overline{y}$, and we're done.

6. Let $\alpha \in \mathbb{Z}[i]$ be a prime Gaussian integer. Prove that either $\alpha\overline{\alpha}$ is a prime integer or else $\alpha\overline{\alpha}$ is the square of a prime integer.