18.781, Fall 2007 Problem Set 7
Due: FRIDAY, October 26

We are beginning a new section on algebraic number theory. Supporting discussion for this material can be found in Chapter 9 of NZM (though it is somewhat less focused than our in-class discussions). The text "A Classical Introduction to Modern Number Theory" by Ireland and Rosen is a good source for many of the results we'll discuss, though there are many additional books on algebraic number theory in the library that may be of use.

Throughout the following problems, ω will denote a complex cubic root of unity $\frac{1+i\sqrt{3}}{2}$. Moreover, R will be used to denote the ring $\mathbb{Z}[\omega]$.

1. Show that 13 is not a prime in R by giving an explicit factorization into non-unit elements.

2. Prove that $\mathbb{Z}[i]$ is a Euclidean domain (a ring with Euclidean algorithm) by exhibiting a function λ from $\mathbb{Z}[i]$ to the non-negative integers, and then mimicking the proof as done in class for R.

3. What are the units of $\mathbb{Z}[i]$? (Prove your answer is correct).

4. Factor 2 into irreducible elements in $\mathbb{Z}[i]$ (or prove that it is, itself, irreducible – i.e. not able to be non-trivially factored).

5. If $\alpha \in R$, show that α must be congruent to one of 0,1, or -1 mod $(1-\omega)$.

6. Show that if, in R, $N(\wp) \neq 3$ for a prime $\wp$, then $1, \omega$, and ω^2 are distinct in $R/\wp R$. Conclude that $3|N(\wp)-1$.