18.781, Fall 2007 Problem Set 8
Due: FRIDAY, November 2

These exercises continue to develop the theory of algebraic integers needed for cubic reciprocity.

In all the following problems, let $R = \mathbb{Z}[\omega]$, with $\omega = \frac{-1+i\sqrt{3}}{2}$.

1. Prove that the number of residue classes in $R/\pi R$ is $N(\pi)$. (That is, rewrite the portion of the proof done in class, and then finish the proof by showing the representatives we chose are indeed distinct mod π.)

2. Factor the following elements of R into primes (in R, of course): 7, 21, 45, 22, 143 (and prove that your factors are indeed prime).

3. As we'll discuss in lecture on Monday, it is often convenient to choose a particular representative from the set of elements defined up to a choice of units. For rational numbers, we chose n from the set $\{n, -n\}$. For an element $\eta \in R$, we must choose from among
$$\{\eta, -\eta, \omega\eta, -\omega\eta, \omega^2\eta, -\omega^2\eta\}.$$
Prove that for any prime π with $N(\pi) = p \equiv 1$ (3), exactly one of these six elements (i.e. π multiplied by some unit in R) is equivalent to 2 (mod 3).

4. A prime $\pi \in R$ is called primary if $\pi \equiv 2$ (3). Factor 19 in R, and find primary primes which are "associates" of each prime factor (that is, they differ from the prime factor by a multiple of a unit).

5. Prove that primitive roots exist for $R/\pi R$, where π is a prime in R. Conclude that
$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \text{ if and only if } \alpha \text{ is a cubic residue mod } \pi.$$
Recall that the symbol is defined by the congruence
$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{N(\pi)-1/3}\ (\pi).$$

6. Show that
$$\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2 = \left(\frac{\alpha^2}{\pi}\right)_3 = \left(\frac{\bar{\alpha}}{\bar{\pi}}\right)_3,$$
where $\bar{\alpha}$ denotes the complex conjugate ($a + bi \mapsto a - bi$).

7. The following questions concern $R/5R$.

(a) What is the factorization of $x^{24} - 1$ in $R/5R$?

(b) How many cubic residues are there in $R/5R$?

(c) Show that $\omega(1-\omega)$ has order 8 in $R/5R$ and that $\omega^2(1-\omega)$ has order 24 in $R/5R$.