18.781, Fall 2007 Problem Set 10
Due: MONDAY, November 19

A few more problems on algebraic numbers and the general reciprocity program:

1. Show that $\sin(\pi/12)$ is algebraic.

2. In class, we determined that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain: We stated that unique factorization in a ring R implies R is a principal ideal domain. This means that every ideal in R is generated by a single element. Moreover, $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization since

$$6 = 2 \cdot 3 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5}).$$

   (a) Explain how, using the norm in $\mathbb{Z}[\sqrt{-5}]$, this factorization of 6 implies that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. (In particular, why can't the factorizations of 6 factor further?)

   (b) Investigate the ideal $(3, 1+\sqrt{-5})$, the ideal generated by 3 and $1+\sqrt{-5}$ (i.e. the smallest ideal containing these two elements in $\mathbb{Z}[\sqrt{-5}]$). Can you describe the set of elements in the ideal more concretely? Does the ideal consist of the entire ring $\mathbb{Z}[\sqrt{-5}]$? Is it a prime ideal? (Recall, an ideal P is "prime" if, for any $a, b \in P$, $a \in P$ or $b \in P$).

3. Define an nth power residue symbol. That is, choose a ring R in which to perform this calculation, and then describe how to define the nth power residue symbol using congruence conditions in R, and prove that your definition is well-defined (i.e. makes sense). (Hint: recall how we do this for cubic and quadratic reciprocity and do the same for nth order reciprocity using a congruence modulo a prime ideal: For a prime ideal P,

$$a \equiv b \ (P) \quad \text{means} \quad a - b \in P$$

   And now questions related to ANALYTIC NUMBER THEORY:

4. Prove that

$$\sum_{p:\ \text{prime}} \frac{1}{p(p-1)} < 1$$

5. Recall that we defined a character on $(\mathbb{Z}/q\mathbb{Z})^\times$ in class by choosing a complex number ζ such that $\zeta^{q-1} = 1$ and a primitive root g mod q. Let $\nu_g(n)$ denote the index of n for the primitive root g, i.e.

$$g^{\nu_g(n)} \equiv n \ (q)$$

Then we defined a character χ by

$$\chi(n) = \zeta^{\nu_g(n)}$$

Prove that given any other primitive root h, there exists a ζ' with $(\zeta')^{q-1} = 1$ such that

$$\zeta^{\nu_h(n)} = (\zeta')^{\nu_g(n)}$$