18.786 Problem Set 1 - Spring 2008

Due Thursday, Feb. 14 at 1:00

1. Using the notation $\tilde{\zeta}_n := e^{2\pi i/n} + e^{-2\pi i/n}$, find $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$ for:
   (a) $\alpha = \sqrt{2} + \sqrt{7}$,
   (b) $\alpha = i\sqrt[3]{4}$,
   (c) $\alpha = \tilde{\zeta}_5$.

2. Find the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ for any $d \in \mathbb{Z}_{\geq 0}$.

3. As mentioned on the first day of class, there is the following ideal factorization in $R = \mathbb{Z}[\sqrt{-5}]$:

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

   Find the index of each of these ideals in R. Use the complex norm $|a + bi| = \sqrt{a^2 + b^2}$ to show that none of these ideals are principal.

4. In this problem, you will use symmetric polynomials to prove that the set of algebraic integers of R with respect to $R' \supset R$ forms a subring in R'.

   A function $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is *symmetric* if $f(x_{\pi(1)}, \ldots, x_{\pi(n)}) = f(x_1, \ldots, x_n)$ for any permutation π. The elementary symmetric functions are defined by

$$S_k(x_1, \ldots, x_n) := \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k} \qquad (0 \leq k \leq n).$$

   (a) Prove that any symmetric function can be written as a polynomial in the S_k (*hint: Define a canonical ordering of monomials and argue inductively*).
   (b) If α is an algebraic integer with minimal polynomial $f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in R[x]$ (roots $\alpha_1 = \alpha, \ldots, \alpha_n$), then show that $S_k(\alpha_1, \ldots, \alpha_n) \in R$ for all k.
   (c) Suppose that α, β are algebraic integers with minimal polynomials $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ and $g(x) = (x - \beta_1) \cdots (x - \beta_m)$, respectively. Consider the function

$$F(x) := \prod_{j=1}^{m} f(x - \beta_j),$$

   which has as roots all sums $x = \alpha_i + \alpha_j$, including $\alpha + \beta$. Using symmetric functions, conclude that $F(x) \in R[x]$. Define a similar polynomial $F_2(x) \in R[x]$ that has $\alpha\beta$ as a root, concluding the proof that the algebraic integers are closed under addition and multiplication.

5. Use the complex norm to prove the division algorithm for $\mathbb{Z}[i]$: If $a, b \in \mathbb{Z}[i]$ and $b \neq 0$, then there are $q, r \in \mathbb{Z}[i]$ such that $a = bq + r$ and $|r| < |b|$.

   Remark. This implies that $\mathbb{Z}[i]$ is a Euclidean domain, and hence a principal ideal domain and unique factorization domain as well!

6. Install a recent version of SAGE or PARI/GP and learn some of the basic commands. Use the following approach to write $p = 44560482149$ as a sum of two integer squares:

- Recall Wilson's Theorem, which states that $(p-1)! \equiv -1 \pmod{p}$ for any prime. If $p = 4k+1$, this implies that $(2k)!$ is a solution to $x^2 \equiv -1 \pmod{p}$.
- A solution to this equivalence means that $(x+i)(x-i) = np$ for some $n \in \mathbb{Z}$. Wilson's Theorem was historically used to verify the existence of such a solution, but it's computationally more efficient to use $x = a^{(p-1)/4}$ for a primitive multiplicative root mod p. Clearly p does not divide either term of the product, so p is not a prime in $\mathbb{Z}[i]$. Therefore, $p = (a+bi)(a-bi)$ for some Gaussian integer (we'll see why it has exactly these two factors later).
- To find one of the factors, calculate the GCD of p and $x+i$ using the Euclidean algorithm. Then $p = a^2 + b^2$!

Turn in a printout of your calculations along with the rest of the assignment.