Harvard Math 129: Algebraic Number Theory
Homework Assignment 4

William Stein

Due: Thursday, March 10, 2005

The problems have equal point value, and multi-part problems are of the same value. In any problem where you use a computer, include in your solution the exact commands you type and their output. You may use any software, including (but not limited to) MAGMA and PARI.

1. Let p be a prime. Let $\mathcal{O}_K$ be the ring of integers of a number field K, and suppose $a \in \mathcal{O}_K$ is such that $[\mathcal{O}_K : \mathbb{Z}[a]]$ is finite and coprime to p. Let $f(x)$ be the minimal polynomial of a. We proved in class that if the reduction $\overline{f} \in \mathbb{F}_p[x]$ of f factors as
$$\overline{f} = \prod g_i^{e_i},$$
where the g_i are distinct irreducible polynomials in $\mathbb{F}_p[x]$, then the primes appearing in the factorization of $p\mathcal{O}_K$ are the ideals $(p, g_i(a))$. In class, we did not prove that the exponents of these primes in the factorization of $p\mathcal{O}_K$ are the e_i. Prove this.

2. Let $a_1 = 1 + i$, $a_2 = 3 + 2i$, and $a_3 = 3 + 4i$ as elements of $\mathbb{Z}[i]$.
   (a) Prove that the ideals $I_1 = (a_1)$, $I_2 = (a_2)$, and $I_3 = (a_3)$ are coprime in pairs.
   (b) Compute $\#\mathbb{Z}[i]/(I_1 I_2 I_3)$.
   (c) Find a single element in $\mathbb{Z}[i]$ that is congruent to n modulo I_n, for each $n \leq 3$.

3. Find an example of a field K of degree at least 4 such that the ring $\mathcal{O}_K$ of integers of K is not of the form $\mathbb{Z}[a]$ for any $a \in \mathcal{O}_K$.

4. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and suppose that $\mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic $p \in \mathbb{Z}$. Prove that there is an element $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (p, \alpha)$. This justifies why PARI can represent prime ideals of $\mathcal{O}_K$ as pairs (p, α). (More generally, if I is an ideal of $\mathcal{O}_K$, we can choose one of the elements of I to be *any* nonzero element of I.)

5. (*) Give an example of an order $\mathcal{O}$ in the ring of integers of a number field and an ideal I such that I cannot be generated by 2 elements as an ideal. Does the Chinese Remainder Theorem hold in $\mathcal{O}$? [The (*) means that this problem is more difficult than usual.]