Problem Set 4.

Let $\mathcal{O}$ be an order in a number field $K$ and define the conductor of the order $\mathcal{O}$ to be the $\mathcal{O}_K$ submodule of $\mathcal{O}$ given by $c(\mathcal{O}) = \{x \in K | x\mathcal{O}_K \subset \mathcal{O}\}$. Note that $c(\mathcal{O})$ is the largest $\mathcal{O}_K$ module contained in $\mathcal{O}$. We say a ideal $I$ of $\mathcal{O}$ is prime to an ideal $J$ of $\mathcal{O}$ if $I + J = \mathcal{O}$.

Problem 1 below establishes that:

1) Every ideal of $\mathcal{O}$ prime to $c(\mathcal{O})$ is invertible and factors uniquely into a product of invertible primes of $\mathcal{O}$.
2) A prime ideal $P$ in $\mathcal{O}$ is invertible if and only if $P$ is prime to $c(\mathcal{O})$.

1. i) Show that if $I \subset \mathcal{O}$ is an ideal with $I + c(\mathcal{O}) = \mathcal{O}$, then $I$ is an invertible $\mathcal{O}$ ideal which factors as a product of prime ideals. (Hint: Induct on the length of the $\mathcal{O}$-module $\mathcal{O}/I$, using that for any prime $P$ containing $I$ that $P^* = \{x \in K | xP \subset \mathcal{O}\}$ contains elements not in $\mathcal{O}$. Show that such a prime $P$ is invertible by examining $P^* = P^*(P + c(\mathcal{O}))$, noting that if $P^*P = P$ then $P^*$ is in $\mathcal{O}_K$.)

ii) For any prime $P$ of $\mathcal{O}$ let $\mathcal{O}_P$ be the subring of $K$ given by expressions $r/s$ for $r \in \mathcal{O}$ and $s \notin P$. Show that there is a unique maximal ideal $P\mathcal{O}_P$ in $\mathcal{O}_P$. Show that if $I$ is an invertible ideal in $\mathcal{O}$ then $I\mathcal{O}_P$ is a principal ideal in $\mathcal{O}_P$. Hint: Write $1 \in I I^{-1}$ as a sum of elements in $\mathcal{O}$ of the form $x_iy_i$, $x_i \in I$, $y_i \in I^{-1}$. Some summand is not in $P$, say $x_1y_1$. Show that $I\mathcal{O}_P = x_1\mathcal{O}_P$.

iii) Show that the prime ideals $P$ in $\mathcal{O}$ which contain $c(\mathcal{O})$ are not invertible $\mathcal{O}$-ideals. (Hint: Show that if $P$ is invertible in $\mathcal{O}$ then any ideal of $\mathcal{O}_P$ is of the form $(P\mathcal{O}_P)^k$ and is invertible. Use this to show that $\mathcal{O}_K \subset \mathcal{O}_P$ and consider the members of an integer basis for $\mathcal{O}_K$ to construct an element of $c(\mathcal{O})$ which is not in $P$ when $P$ is invertible).

2. Let $K$ be a number field and $p$ a prime number. Consider the order $\mathcal{O} = \mathbb{Z} + p\mathcal{O}_K$. Show that $P = p\mathcal{O}_K$ is a noninvertible prime ideal of $\mathcal{O}$. Show that the ideal $p\mathcal{O}$ of the order $\mathcal{O}$ does not factor as a product of prime ideals of $\mathcal{O}$.

3. (Chinese Remainder Theorem) Let $R$ be a commutative ring and let $A_1, \ldots, A_n$ be ideals of $R$ such that $A_i + A_j = R$ when $i \neq j$. Show that given $x_1, \ldots, x_n$ in $R$, there exists $x$ in $R$ such that $x - x_i \in A_i$.

4. a) Suppose that $R$ is an integral domain in which all prime ideals are maximal and every ideal is equal to a product of powers of prime ideals. If $R$ has finitely many
prime ideals, use (3.) to show that $R$ is a principal ideal domain. Give an example of such an $R$ which is not a field.

b) Use part a) to show that given an ideal $I$ of the maximal order $O_K$ of a number field and an nonzero element $a \in I$ there exists an element $b \in I$ such that $I = aO_K + bO_K$. 