MATH 380A/500A, PROBLEM SET 5

The following problems are due at the beginning of class on Monday, Oct. 7, 2013.

(1) Let R be the integral closure of the ring of integers $\mathbb{Z}$ in the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ (or equivalently in the complex numbers $\mathbb{C}$). Show that for any prime number p, there exist infinitely many maximal ideals $\mathfrak{m}$ in R such that $\mathfrak{m} \cap \mathbb{Z} = \langle p \rangle$.

Hint: First, show that for any positive integer n, there exists a monic polynomial f in $\mathbb{F}_p[x]$ with n distinct irreducible factors ($\mathbb{F}_p$ is the field $\mathbb{Z}/p$). Then, use the Hilbert irreducibility theorem (see below) to show that this polynomial can be lifted to a monic and irreducible polynomial $\widetilde{f} \in \mathbb{Z}[x]$, i.e. $\widetilde{f}$ is such that f is the reduction of $\widetilde{f}$ modulo p. Show that the quotient ring $\mathbb{Z}[x]/\langle f \rangle$ contains n distinct maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ such that $\mathfrak{m}_i \cap \mathbb{Z} = \langle p \rangle$. Finally, use the lying over and incomparability theorems to prove the desired statement about R.

Theorem 1 (Hilbert irreducibility)**.** Suppose that $f(x, y)$ is an irreducible polynomial in $\mathbb{Z}[x, y]$. Then there exists an integer a such that the specialization $f(x, a)$ is irreducible in $\mathbb{Z}[x]$.

(I also see a somewhat more complicated way of solving this problem using Dirichlet's theorem on arithmetic progressions instead of Hilbert's irreducibility theorem. However, I would be very interested to know if there was a proof that didn't use any hard number-theoretic results.)

(2) Eisenbud, exercise 4.27.

(3) Eisenbud, exercise 5.1, except that the statement about addition is incorrect. Instead, prove the following: If $\mathrm{in}(f) + \mathrm{in}(g) \neq 0$, then $\mathrm{in}(f + g)$ is equal to either $\mathrm{in}(f) + \mathrm{in}(g)$, $\mathrm{in}(f)$, or $\mathrm{in}(g)$. Also, prove the second paragraph, which seems to be correct.

(4) Eisenbud, exercise 5.2. An explanation of terminology: if I is an ideal of R, $\mathrm{in}(I)$ is the ideal in $\mathrm{gr}_I(R)$ generated by the elements $\mathrm{in}(f)$ as f ranges over all elements of I.