Homework 2 for 506, Spring 2009
due Friday, April 17

Problem 1. Describe Spec R for
(1) $R = \mathbb{Z}[x]$

Solution. Let $\mathfrak{p} \in \mathbb{Z}[x]$ be a prime ideal. Consider 2 cases:

I. $\mathbb{Z} \cap \mathfrak{p} = (0)$
II. $\mathbb{Z} \cap \mathfrak{p} \neq (0)$

Case I. Let $f \in \mathfrak{p}$ be a polynomial such that
(i) $\deg f$ is minimal among all polynomials in $\mathfrak{p}$,
(ii) the GCD of all coefficients of f is minimal among all polynomials in $\mathfrak{p}$ of degree $\deg f$.
I claim that f is irreducible in $\mathbb{Z}[x]$. Indeed, suppose $f(x) = g(x)h(x)$. Since $\mathfrak{p}$ is prime, we have that either $g \in \mathfrak{p}$ or $h \in \mathfrak{p}$. If $0 < \deg g, \deg g < \deg f$, then this contradicts the minimality of $\deg f$. Hence, one of g, h must be a constant. Therefore, $f(x) = mh(x)$, where $m \in \mathbb{Z}$. Since $\mathfrak{p} \cap \mathbb{Z} = (0)$, and $\mathfrak{p}$ is prime, we get $h(x) \in \mathfrak{p}$. This contradicts the assumption (ii) of minimality of GCD unless $m = 1$. Hence, $f(x)$ is irreducible.
Case II. Let $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Let $\mathfrak{p} \cap \mathbb{Z} = (p)$, where p is a prime number. By one of the isomorphism theorems, we have

$$\mathbb{Z}[x]/\mathfrak{p} \simeq \frac{\mathbb{Z}[x]/(p)}{\mathfrak{p}/(p)} \simeq \frac{\mathbb{F}_p[x]}{\mathfrak{p}/(p)}.$$

The ring $\mathbb{F}_p[x]$ is a PID (a polynomial ring over a field), hence, $\bar{\mathfrak{p}} = \mathfrak{p}/(p)$ is generated by some polynomial $\bar{f} \in \mathbb{F}_p[x]$. Moreover, $\bar{p}$ is a prime ideal (since $\mathbb{F}_p[x]/\bar{p} = \mathbb{Z}[x]/\mathfrak{p}$ is an integral domain), therefore, $\bar{f}$ is either zero or irreducible. If $\bar{f} = 0$, then $\mathfrak{p} = (p)$. So we assume that $\bar{f} \neq 0$. Let $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$ be a lifting of $\bar{f}$ to $\mathfrak{p}$ of minimal degree. We have $(a_n, p) = 1$, for otherwise we can subtract a multiple of px^n from $f(x)$ and get a lifting of $\bar{f}$ of lower degree. Moreover, we can assume that f is monic. Indeed, since $(p, a_n) = 1$, there exist $\alpha, \beta \in \mathbb{Z}$ such that $\alpha p + \beta a_n = 1$. Replacing f with $\alpha p x^n + \beta f(x)$ we get a monic polynomial satisfying the same properties as f. Moreover, since f is a lifting of minimal degree, we have $\deg f = \deg \bar{f}$.

I claim that $\mathfrak{p} = (p, f)$. We clearly have $p, f \in \mathfrak{p}$, so we just need to show they generate the entire ideal. Suppose not. Then there exists $g \in \mathfrak{p} \backslash (p, f)$. Choose such a g of minimal possible degree, and let $g(x) = b_m x^m + \ldots + b_0$. Arguing as above for f, we can assume that g is monic.

Consider 2 cases:
(i) $m \geq n$. Then take $g'(x) = g(x) - x^{m-n} f(x)$. We have $g'(x) \in \mathfrak{p}$ but $\deg g' < \deg g$. Hence, $g'(x) \in (p, f)$. But then $g = g' + x^{m-n} f \in (p, f)$. Contradiction.
(ii) $m < n$. Since $g \in \mathfrak{p}$, we have $\bar{g} \in \mathfrak{p}/(p) = (\bar{f})$. But since g is monic, we also have $\deg \bar{g} = \deg g = m < n = \deg f = \deg \bar{f}$. Hence, $\bar{g}$ is in the ideal generated by $\bar{f}$ only if $\bar{g} = 0$. But then g is zero modulo p, and, hence, $g \in (p) \subset (p, f)$. Contradiction again.

We conclude that there are 3 possibilities for prime ideals:

1. (0)-ideal,
2. principal ideals $(f(x))$ where $f(x)$ is an irreducible polynomial in $\mathbb{Z}[x]$ or (p) where $p \in \mathbb{Z}$ is a prime,
3. ideals generated by 2 elements $(p, f(x))$, where p is a prime integer, $f(x)$ is irreducible over $\mathbb{F}_p$.

The ideals of the form $(p, f(x))$ are maximal and correspond to closed points in $X = \operatorname{Spec} \mathbb{Z}[x]$. The space is irreducible and has dimension 2. The irreducible closed sets correspond to prime ideals, so they are of the form
$V((p, f(x)) =$ closed point in X,
$V((0)) = X$, or
$V((f(x)), V((p))$.
The latter sets are infinite since, for example, $(f(x)) \subset (p, f(x))$ for all p for which $f(x) \bmod p$ is still irreducible, and there are infinitely many of those. Hence, this is not a cofinite topology.