Group Assignment 3 (Just Problem 2)

Lucas Bouck

November 3, 2015

Problem:

Prove the rational roots theorem. Let $p(x) = a_0 + a_1x + ... + a_nx^n$ be a polynomial such that each a_j is an integer. If $t = r/s$ (where r and s are integers and t is written in lowest terms, so that $gcd(r, s) = 1$) satisfies $p(t) = 0$, then $r|a_0$ and $s|a_n$.

Proof:

Let $p(x) = a_0 + a_1x + ... + a_nx^n$ be a polynomial such that each a_j is an integer. Assume there exists a $t = r/s$ where r and s are integers and t is written in lowest terms, so that $gcd(r, s) = 1$ such that $p(t) = 0$. We want to show that $r|a_0$ and $s|a_n$. Since $p(t) = 0$, we get $a_0 + a_1t + ... + a_nt^n = a_0 + a_1\frac{r}{s} + ... + a_n\frac{r^n}{s^n}$. By subtracting a_0 from both sides, we get:

$$\begin{aligned}
-a_0 &= a_1\frac{r}{s} + ... + a_n\frac{r^n}{s^n} \\
-a_0s^n &= a_1rs^{n-1} + a_2r^2s^{n-2} + ... + a_nr^n \\
-a_0s^n &= r\left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_nr^{n-1}\right) \\
\left(-a_0s^{n-1}\right)s &= r\left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_nr^{n-1}\right)
\end{aligned}$$

Since $a_0, s \in \mathbb{Z}$, $-a_0s^{n-1} \in \mathbb{Z}$. Since $-a_0s^{n-1} \in \mathbb{Z}$, $s|r\left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_nr^{n-1}\right)$. Since $gcd(r, s) = 1$, $s|\left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_nr^{n-1}\right)$. Therefore, there exists an integer z such that $sz = \left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_nr^{n-1}\right)$. We can then break the left term into $\left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_nr^{n-1}\right) = \left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_{n-1}r^{n-2}s^1\right) + a_nr^{n-1}$. Let $\left(a_1s^{n-1} + a_2rs^{n-2} + ... + a_{n-1}r^{n-2}s^1\right) = d$. Since all of $a_j \in \mathbb{Z}$ and $r, s \in \mathbb{Z}$, then $d \in \mathbb{Z}$. Since $s|s$ and each term of d is some integer multiplied by s, then s divides each term of d. Thus, $s|d$. Therefore, there exists an integer l such that $sl = d$. Then, $sz = d + a_nr^{n-1} = sl + a_nr^{n-1}$. Then, $sz - sl = s(z - l) = a_nr^{n-1}$. By multiplying r to both sides, we get $s(z - l)r = s(zr - lr) = a_nr^n$.Let $zr - lr = k$. Since $z, l, r \in \mathbb{Z}$, then $k \in \mathbb{Z}$. Thus, there exists an integer k such that $sk = a_nr^n$. Thus, $s|a_nr^n$. Since $gcd(r, s) = 1$ and n is a natural number, by a previous result proven in previous written assignment, $gcd(r^n, s) = 1$. Since $s|a_nr^n$ and $gcd(r^n, s) = 1$, $s|a_n$.

We still need to show that $r|a_0$. Using an earlier equation, we know $-a_0 = a_1\frac{r}{s} + ... + a_n\frac{r^n}{s^n}$. By multiplying s^n to both sides, we get $-a_0s^n = a_1rs^n + ... + a_nr^n$. By factoring out r we get $-a_0s^n = r(a_1s^n + ... + a_nr^{n-1})$. Then, $a_0s^n = r(-(a_1s^n + ... + a_nr^{n-1}))$. Let $-(a_1s^n + ... + a_nr^{n-1}) = m$. Since all $a_j \in \mathbb{Z}$ and $r, s \in \mathbb{Z}$, then $m \in \mathbb{Z}$. Thus, there exists an integer m such that $rm = a_0s^n$. Therefore, $r|a_0s^n$. Since $gcd(r, s) = 1$ and n is a natural number, then $gcd(r, s^n) = 1$. Since $gcd(r, s^n) = 1$, then $r|a_0$.

We have now proven $s|a_n$ and $r|a_0$. We are done.