PURDUE UNIVERSITY MATH DEPARTMENT
PROBLEM OF THE WEEK
SPRING 2010, PROBLEM 9

WILLIAM WU

Problem Let f be a nonconstant polynomial with integer coefficients. Show that for infinitely many primes p_i there is at least one corresponding integer x_i with p_i a factor of $f(x_i)$.

Solution Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. For brevity of notation, call p a *divisor* of f if there exists an integer x_i such that $p \mid f(x_i)$.

If $a_0 = 0$, then for every prime p,

$$f(p) = a_1 p + \ldots + a_n p^n = p(a_1 + \ldots + a_n p^{n-1})$$

is divisible by p, which verifies the proposition. So henceforth, assume $a_0 \neq 0$. Suppose by way of contradiction that the proposition is false. Then f only has a finite number of prime divisors $p_1, p_2, \ldots, p_m$. Construct a new polynomial $g(x)$ as follows:

(1)
$$f\left(a_0 \prod_{i=1}^m p_i x\right) := a_0 + a_1 \left(a_0 \prod_{i=1}^m p_i x\right) + \ldots + a_n \left(a_0 \prod_{i=1}^m p_i x\right)^n$$

(2)
$$= a_0 \underbrace{\left(1 + a_1 \cdot \prod_{i=1}^m p_i x + a_2 \cdot a_0 \left(\prod_{i=1}^m p_i\right)^2 x^2 + \ldots a_n \cdot a_0^{n-1} \left(\prod_{i=1}^m p_i\right)^n x^n\right)}_{g(x)}.$$

We now make two observations about $g(x)$. Firstly, every coefficient of $g(x)$ except the constant term has $\prod_{i=1}^m p_i$ as a factor. Thus, for all integers x, and all i from 1 to m,

$$1 \equiv g(x) \bmod p_i.$$

Consequently, no prime divisor of f is also a prime divisor of g; or put differently, f and g share no prime divisors.

On the other hand, if p is a prime divisor of g, then it is also a prime divisor of f. To see this, note that if $p \mid g(x_p)$ for some integer x_p, then

$$p \mid g(x_p) \quad \Longrightarrow \quad p \mid a_0 g(x_p) \quad \Longleftrightarrow \quad p \mid f\left(a_0 \prod_{i=1}^m p_i x_p\right).$$

Combining these two observations, it follows for all integers x, $g(x)$ cannot have any prime factors, so either $g(x) = 1$ or $g(x) = -1$. However, g is an nth degree polynomial, so it cannot take on either 1 or -1 more than n times each, unless g is either identically 1 or identically

Date: March 12, 2010.

-1. Since $g(0) = 1$, it follows that g is identically 1. Thus, every coefficient of g aside from the constant term must be zero:

$$0 = a_1 \prod_{i=1}^{n} p_i, \qquad 0 = a_2 \cdot a_0 \prod_{i=1}^{n} p_i, \qquad \ldots \qquad 0 = a_n \cdot a_0^{n-1} \prod_{i=1}^{n} p_i.$$

Since $\prod_{i=1}^{n} p_i \neq 0$ and $a_0 \neq 0$ by assumption, we can divide out these terms to get

$$0 = a_1, \qquad 0 = a_2, \qquad \ldots \qquad 0 = a_n.$$

Then $f(x) = a_0$, a constant polynomial, which contradicts the premise. □

E-mail address: william.wu@themathpath.com

The Math Path LLC