Some Other Past 788F Test Problems

1. On the back of this page, the first part of the proof of the theorem below is given. Finish the proof. (Do not repeat what is given on the back side of this page.)

   Theorem: *If $f(x) \in \mathbb{Z}[x]$ is monic, is irreducible, and has all its roots on $\{z : |z| = 1\}$, then $f(x)$ is a cyclotomic polynomial.*

2. Let $f(x) = x^3 + 22$. Determine with proof all primes p for which $f(x)$ is Eisenstein with respect to p. For each such p, find a value of a for which $f(x + a)$ is in Eisenstein form with respect to p.

3. Let k be a positive integer, and let $f(x) = 1 + x^2 + x^4 + \cdots + x^{2k}$.

   (a) Prove that $f(x)$ is a product of cyclotomic polynomials.

   (b) Determine all values of k for which $f(x)$ is irreducible.

4. Let
   $$f(x) = x^7 + 21x^6 - 30x^4 - 90x^3 + 1350x + 2700.$$
   Using Newton polygons, explain why $f(x)$ is irreducible. (Be careful, and indicate as clearly as possible what information you are obtaining from each Newton polygon you use in your argument.)

5. Prove that there is an infinite sequence of positive integer $a_0, a_1, a_2, \ldots$ such that
   $$a_0 < a_1 < a_2 < \cdots$$
   and such that
   $$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$
   is irreducible for every positive integer n.

6. Suppose that $f(x)$ is irreducible modulo p and that $f(x) \not\equiv x \pmod{p}$. Why is $f(x)$ a factor of some cylcotomic polynomial modulo p?

7. Let $p_1, p_2, \ldots, p_r$ be r distinct odd primes, and let $n = p_1 p_2 \cdots p_r$. Note that
   $$\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$
   Prove that for every prime q, $\Phi_n(x)$ is the product of at least 2^{r-1} irreducible (not necessarily distinct) polynomials modulo q.

Proof. Let α be such that $f(\alpha) = 0$. If we can establish that α is a root of some cyclotomic polynomial, then since both cyclotomic polynomials and $f(x)$ are irreducible, $f(x)$ will be cyclotomic. Thus, it suffices to show that there exists a positive integer m such that $\alpha^m = 1$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the complete list of roots of $f(x)$ with $\alpha_1 = \alpha$. Using elementary symmetric functions (cf. Uspensky [1]), it is easy to deduce that $(x-\alpha_1^k)(x-\alpha_2^k)\cdots(x-\alpha_n^k)$ is in $\mathbb{Z}[x]$ for every positive integer k. We can avoid the use of elementary symmetric functions, however, by restricting consideration to polynomials of the form

$$f_k(x) = (x - \alpha_1^{2^k})(x - \alpha_2^{2^k})\cdots(x - \alpha_n^{2^k}).$$

Then one easily deduces that

$$f_1(x^2) = (-1)^n f(x) f(-x) \in \mathbb{Z}[x].$$

Since $f_1(x^2)$ is a polynomial in x^2 with integer coefficients, $f_1(x)$ has integer coefficients. An easy induction argument now implies that $f_k(x) \in \mathbb{Z}[x]$ for every positive integer k.