Comprehensive Exam: Math 788F & 798

(1) Using Lemma 1 and Lemma 2 on the last page of the exam, prove Perron's Theorem that if $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $n \geq 1$ is such that $a_n = 1$, $a_0 \neq 0$, and $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$, then $f(x)$ is irreducible.

(2) Using Lemma 3 on the last page of the exam, explain how to settle the case $n = 10$ and $k = 3$ of Theorem 1 on the last page. (Hint: After using Lemma 3 to determine information about $a_n = a_{10}$, consider the Newton polygon of $f(x)$ with respect to the prime 3.)

(3) Show that if $g(x)$ is a polynomial as in Lemma 4 on the last page of this exam, then $g(x)$ cannot have a factor with degree in the interval $[\ell + 1, k]$. (In other words, prove the special case of this lemma when every a_j equals 1.)

(4) Explain how $\Phi_{124}(x)$ factors modulo p for each prime $p \in \{2, 5, 31, 997\}$. (You may use without proof that all four of these numbers are prime.)

(5) Using one of the theorems on the last page of this exam, prove that the Laguerre polynomials of the second kind given by

$$J_n(x) = \frac{1}{x} \int_0^x L_n(x)\, dx = -\frac{1}{n+1} \frac{dL_{n+1}(x)}{dx} = \sum_{j=0}^{n} \binom{n}{j} \frac{(-x)^j}{(j+1)!}$$

are irreducible for $n \geq 10$.

(6) Suppose that n is a sufficiently large integer and that k is an integer satisfying $2n/\log n \geq k \geq n^{2/3}$. Show that there is a prime $p > 3k$ that divides $n(n-1)\cdots(n-k+1)$. (This is part of an argument used in establishing that all but finitely many Bessel polynomials are irreducible.)

(7) Let $f(x) = a_{20}x^{20} + a_{19}x^{19} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, and suppose the "spots" associated with the Newton polygon of $f(x)$ with respect to 2 are $(0, 0)$, $(3, 2)$, $(19, 6)$, $(20, 4)$, and $(k, 1)$ for $k \in \{1, 2, 4, 5, \ldots, 18\}$.

(a) Give an example of an irreducible polynomial $f(x)$ with spots as above.

(b) If $f(x)$ is reducible with spots as above, then what are the degrees of its irreducible factors?

(c) Give an example of a reducible polynomial $f(x)$ with spots as above. You may (if you prefer) leave your answer in factored form.

(8) Let

$$f(x) = (2x - 3)(x - 1)(x - 2)\cdots(x - 100) - 1.$$

Thus, $f(x) \in \mathbb{Z}[x]$ and $f(x)$ has degree 101.

(a) Why is the content of $f(x)$ (the gcd of its coefficients) equal to 1?

(b) Assume $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$ with $\deg g \geq \deg h \geq 1$. Explain why $g(x) + h(x)$ has each element of $\{1, 2, \ldots, 100\}$ as a root.

(c) Given the set-up in part (b), consider $f(x) + h(x)^2$ and show that $h(1)^2 = h(2)^2 = \cdots = h(100)^2 = 1$.

(d) Given the set-up in part (b), why does part (c) imply that $\deg h \geq 50$?

(e) Given the set-up in part (b), deduce that $h(x) \equiv -g(x)$ so that $f(x) = -g(x)^2$, and use this to establish that $f(x)$ is irreducible.

(f) Using a similar argument, establish that

$$f(x) + 2 = (2x - 3)(x - 1)(x - 2) \cdots (x - 100) + 1$$

is irreducible.

Results Referred to on the Exam

Theorem 1. Let $a_0, a_1, \dots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let $f(x) = \sum_{j=0}^{n} a_j x^j / j!$. If $0 < |a_n| < n$, then $f(x)$ is irreducible unless (a_n, n) is $(\pm 5, 6)$ or $(\pm 7, 10)$.

Theorem 2. For $j \ge 0$, let $u_{2j} = 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2j-1)$. So $u_0 = 1, u_2 = 1, u_4 = 3, u_6 = 15, \dots$. For n an integer > 1, define $f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j}$ where the a_j's are arbitrary integers with $|a_0| = |a_n| = 1$. Then $f(x)$ is irreducible.

Theorem 3. For $j \ge 0$, let $u_{2j} = 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2j-1)$. For n an integer ≥ 1, define $f(x) = \sum_{j=0}^{n} a_j x^{2j} / u_{2j+2}$ where the a_j's are arbitrary integers with $|a_0| = |a_n| = 1$. Then $f(x)$ is irreducible unless $2n$ is of the form $3^u - 1$ where u is an integer > 1 in which case $f(x)$ can have the factor $x^2 + 3$ or $x^2 - 3$ and the remaining factor will be irreducible.

Theorem 4. For n an integer ≥ 1, define $f(x) = \sum_{j=0}^{n} a_j x^j / (j+1)!$ where the a_j's are arbitrary integers with $|a_0| = |a_n| = 1$. Then $f(x)$ is irreducible except in the following cases: (i) if $n = 2^u - 1 \ge 3$, then $f(x)$ can have the factor $x + 2$ or $x - 2$ and the remaining factor will be irreducible, and (ii) if $n = 8$, then $f(x)$ can be the product of two irreducible polynomials of degrees 2 and 6.

Lemma 1: Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \ne 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \ge 1$. Then $f(x)$ is irreducible.

Lemma 2: Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\}$. If the strict inequality $|f(z) + g(z)| < |f(z)| + |g(z)|$ holds for each $z \in \mathcal{C}$, then $f(x)$ and $g(x)$ have the same total number of zeroes (counting multiplicity) inside the circle $\mathcal{C}$ (i.e., in the interior of the region bounded by $\mathcal{C}$).

Lemma 3: Let $a_0, a_1, \dots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let $f(x) = \sum_{j=0}^{n} a_j x^j / j!$. Let k be a positive integer $\le n/2$. Suppose there exists a prime $p \ge k+1$ and a positive integer r for which $p^r | n(n-1) \cdots (n-k+1)$ and p^r does not divide a_n. Then $f(x)$ cannot have a factor of degree k.

Lemma 4: Let k and ℓ be integers with $k > \ell \ge 0$. Suppose $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ and p is a prime such that p does not divide b_n, $p | b_j$ for all $j \in \{0, 1, \dots, n - \ell - 1\}$, and the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Then for any integers $a_0, a_1, \dots, a_n$ with $|a_0| = |a_n| = 1$, the polynomial $f(x) = \sum_{j=0}^{n} a_j b_j x^j$ cannot have a factor with degree in the interval $[\ell + 1, k]$.