Lecture 9: The Polynomial $f(x)x^n + g(x)$

Theorem (Schinzel; F., Ford, Konyagin): Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(0) \neq 0$, $g(0) \neq 0$, and $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$. Let r_1 and r_2 denote the number of non-zero terms in $f(x)$ and $g(x)$, respectively. If

$$n \geq 2 \max\left\{5^{2N-1}, \max\{\deg f, \deg g\}\left(5^{N-1} + \frac{1}{4}\right)\right\} \quad \text{with} \quad N = 2\big(\|f\|^2 + \|g\|^2 + r_1 + r_2\big) - 7,$$

then the non-reciprocal part of $f(x)x^n + g(x)$ is irreducible or identically ± 1 unless one of the following holds:

(i) The polynomial $-f(x)g(x)$ is a pth power for some prime p dividing n.

(ii) For either $\varepsilon = 1$ or $\varepsilon = -1$, one of $\varepsilon f(x)$ and $\varepsilon g(x)$ is a 4th power, the other is 4 times a 4th power, and n is divisible by 4.

Notation: For n a positive integer, a mod n is the unique integer b in $\{0, 1, \ldots, n-1\}$ such that $a \equiv b \pmod{n}$. Also, $\|x\|$ is the distance from x to its nearest integer.

Congruence Problem: Let $a_1, a_2, \ldots, a_r$ denote distinct non-negative integers written in increasing order. Determine an integer $k \geq 2$ such that a_j mod $k \in [0, k/4) \cup (3k/4, k)$ for each $j \in \{1, 2, \ldots, r\}$.

Comment: Clearly, $\exists k \leq 4a_r + 1$. For $\{5, 8\}$ and $\{20, 75, 138\}$, this is the minimum such k.

Actual Problem: Show that if a_r is large as a function of r, then the minimum such k is "small" (smaller than $4a_r + 1$).

Lemma: Let r be a positive integer, and let k_0 be a real number ≥ 2. Set

$$A(r) = \max\left\{2 \times 5^{2r-1}, k_0\left(5^{r-1} + \frac{1}{4}\right)\right\}.$$

Let $a_1, a_2, \ldots, a_r$ be non-negative integers satisfying $a_1 < a_2 < \cdots < a_r$ and $a_r \geq A(r)$. Then there exists an integer $k \in [k_0, 4a_r/3)$ such that a_j mod k is in $[0, k/4) \cup (3k/4, k)$ for each j.

Main Ideas for Proof of Lemma:

- Define $x_j = a_j/a_r$ for $j \in \{1, 2, \ldots, r\}$.
- By the Dirichlet box principle, there is an integer d satisfying $1 \leq d \leq 5^{r-1}$ and $\|dx_j\| \leq 1/5$ for $1 \leq j \leq r-1$. Note that the same inequality holds for $j = r$.
- Since $a_r \geq 2 \times 5^{2r-1}$, we have $d \leq \sqrt{a_r/10}$.
- For $1 \leq j \leq r$, let c_j denote the nearest integer to dx_j.
- First, suppose $c_j \neq 0$ (so that $c_j \geq 1$) for each $j \in \{1, 2, \ldots, r\}$.

- For each $j \in \{1, 2, \dots, r\}$, $c_j \le d$ implies

$$\frac{d+(1/5)}{d+(1/4)} \ge \frac{c_j+(1/5)}{c_j+(1/4)} \ge \frac{dx_j}{c_j+(1/4)} \quad \text{and} \quad \frac{d-(1/5)}{d-(1/4)} \le \frac{c_j-(1/5)}{c_j-(1/4)} \le \frac{dx_j}{c_j-(1/4)}.$$

- If $\dfrac{k}{a_r} \in \left(\dfrac{d+(1/5)}{d(d+(1/4))}, \dfrac{d-(1/5)}{d(d-(1/4))}\right) \subseteq \bigcap_{1\le j\le r} \left(\dfrac{x_j}{c_j+(1/4)}, \dfrac{x_j}{c_j-(1/4)}\right)$, then $|a_j - c_j k|$ $< k/4$ for $1 \le j \le r$.

- The first interval above has length $> 1/(10d^2) \ge 1/a_r$, so k exists. Justify $k_0 \le k < 4a_r/3$.

- If some $c_j = 0$, again choose k in the interval above. Now, $c_j = 0$ implies $|a_j| < k/4$ since $5da_j \le a_r < kd\big(d+\frac{1}{4}\big)/\big(d+\frac{1}{5}\big) \le 5dk/4$.

Main Ideas for Proof of Theorem:

- Assume the non-reciprocal part of $F(x) = f(x)x^n + g(x) = \sum_{j=0}^{r} a_j x^{d_j}$ is reducible. Then there are non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $F(x) = u(x)v(x)$.

- Define $W(x) = u(x)\tilde{v}(x) = \sum_{j=0}^{s} b_j x^{e_j}$ and note that $F(x)\widetilde{F}(x) = W(x)\widetilde{W}(x)$ and $\|W\|^2 = \|F\|^2$ (so $s \le \|F\|^2 - 1$).

- Define $T = \{d_1, d_2, \dots, d_r\} \cup \{d_r - d_1, d_r - d_2, \dots, d_r - d_{r-1}\} \cup \{e_1, e_2, \dots, e_{s-1}\} \cup \{e_s - e_1, e_s - e_2, \dots, e_s - e_{s-1}\}$. Thus, $|T| \le 2\,\|F\|^2 + 2r - 5$.

- Let $k_0 = 2\max\{\deg f, \deg g\}$. By the lemma, there is a $k \in [k_0, 4d_r/3]$ such that $t \bmod k$ is in $[0, k/4) \cup (3k/4, k)$ for each $t \in T$.

- Define $\overline{d}_j$ and ℓ_j by $\overline{d}_j = (d_j + [k/4]) \bmod k$ and $d_j + [k/4] = k\ell_j + \overline{d}_j$.

- Set $G_1(x,y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j} y^{\ell_j}$ so that $G_1(x, x^k) = x^{[k/4]}F(x)$. Similarly, define $G_2(x,y)$, $H_1(x,y)$, and $H_2(x,y)$ so that $G_2(x,x^k) = x^{[k/4]}\widetilde{F}(x)$, $H_1(x,x^k) = x^{[k/4]}W(x)$, and $H_2(x,x^k) = x^{[k/4]}\widetilde{W}(x)$.

- Writing $G_1(x,y)G_2(x,y) = \sum_{j=0}^{J} g_j(x) y^j$, we deduce here that the terms in $g_j(x)$ correspond precisely to the terms in the expansion of $x^{2[k/4]}F(x)\widetilde{F}(x)$ having degrees in the interval $[kj, k(j+1))$. A similar conclusion holds for the terms in $H_1(x,y)H_2(x,y)$.

- Deduce $G_1(x,y)G_2(x,y) = H_1(x,y)H_2(x,y)$ and, consequently, $G_1(x,y)$ has a non-trivial irreducible factor other than x.

- Define ρ by $g(x) = \sum_{j=0}^{\rho} a_j x^{d_j}$ and $f(x) = \sum_{j=\rho+1}^{r} a_j x^{d_j - n}$.

- Observe that $\ell_0 = \ell_1 = \dots = \ell_\rho = 0$ (since $d_j + [k/4] < k$ for $j \in \{0, 1, \dots, \rho\}$) and, for some ℓ, $\ell_{\rho+1} = \ell_{\rho+2} = \dots = \ell_r = \ell$ (otherwise, $d_r - d_{\rho+1} \ge \deg f$).

- Deduce $G_1(x,y) = f(x)x^d y^\ell + g(x)x^{d'}$ for some positive integer ℓ and some non-negative integers d and d'.

- Apply Capelli's theorem.