Lecture 5: Classifying Reducible Polynomials with Small Norm

Theorem (Schinzel): Fix $a_0, \dots, a_r \in \mathbb{Z} - \{0\}$. Then there is an algorithm for obtaining a finite classification of the polynomials of the form $a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0$ that have reducible non-reciprocal part.

Lemma: Let s and t be positive integers. Suppose a system of linear equations in the variables $x_0, \dots, x_s$ is of the form

$$\alpha_{i0}x_0 + \alpha_{i1}x_1 + \cdots + \alpha_{is}x_s = \beta_i \qquad \text{for } 1 \le i \le t,$$

where the α_{ij} and β_i are all in $\mathbb{Z}$. Suppose further that the system of equations has infinitely many solutions $(x_0, \dots, x_s) \in \mathbb{R}^{s+1}$. If the system has at least one solution $(x_0, \dots, x_s) \in \mathbb{Z}^{s+1}$ with $x_0, x_1, \dots, x_s$ *distinct*, then the system has infinitely many such solutions.

Main Ideas for Proof of Lemma:

- Set $A = (\alpha_{i,j-1})$, a $t \times (s+1)$ matrix, and let ρ be its rank.
- Rearrange so the the first ρ rows and first ρ columns are linearly independent.
- Let B be the $\rho \times \rho$ matrix from the upper left part of A, and note that $D = |\det B| \ge 1$.
- Solve to obtain $x_i = \dfrac{1}{D}\Big(c_i + \sum_{j=\rho}^{s} b_{ij}x_j\Big)$ for $0 \le i \le \rho - 1$ with c_i and b_{ij} in $\mathbb{Z}$.
- Fix a solution $(k_0, k_1, \dots, k_s)$ consisting of distinct integers.
- Define $k_i' = k_i + \ell_i D$ for $\rho \le i \le s$, and $k_i' = \dfrac{1}{D}\Big(c_i + \sum_{j=\rho}^{s} b_{ij}k_j'\Big) = k_i + \sum_{j=\rho}^{s} b_{ij}\ell_j$ for $0 \le i \le \rho - 1$. Note that $(k_0', k_1', \dots, k_s')$ is a solution and each $k_j \in \mathbb{Z}$.
- Prove the k_j''s are distinct by taking $\ell_j \equiv 0 \pmod{d}$, for all j, where d is large (so that the k_j''s are distinct modulo d).

Proof of Theorem:

- First, consider the case that the d_j (and a_j) are fixed.
- Recall the non-reciprocal part of $f(x)$ is reducible if and only if there exists $w(x)$ different from $\pm f(x)$ and $\pm\tilde{f}(x)$ such that $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.
- Write $f(x) = \sum_{j=0}^{r} a_j x^{d_j}$ and $w(x) = \sum_{j=0}^{s} b_j x^{k_j}$. Here, the a_j and d_j are given integers with $0 = d_0 < d_1 < \cdots < d_{r-1} < d_r = n$; the b_j and k_j as unknown integers with $0 = k_0 < k_1 < \cdots < k_{s-1} < k_s = n$.

- Since $\|w\| = \|f\|$, we deduce $\sum_{j=0}^{s} |b_j| \leq \|f\|^2$. Thus, there are finitely many possibilities for the b_j's. Fix the b_j's.

- Define $E = \{n - k_j + k_i : 0 \leq i, j \leq s\}$, the set of exponents appearing in $w(x)\widetilde{w}(x)$. Consider a system of equations with each equation consisting of an element from E equal to either another element of E (possible cancellation) or an element of E equal to an expression of the form $n - d_j + d_i$ (from the right-hand side of $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$). Consider only a system satisfying: (i) each element of E occurs in such an equation at least once, (ii) every exponent of an uncancelled term in $f(x)\tilde{f}(x)$ is used exactly once, and (iii) the equations $n - k_s + k_0 = 0$ and $n - k_0 + k_s = 2n$ are used. We only allow equations of the form $n - k_j + k_i = n - k_v + k_u$ if $(i, j) \neq (u, v)$. Replace the equations in (iii) with $k_0 = 0$ and $k_s = n$. We want to know if the system has a solution (for each such system).

- One of the following three possibilities for a system may occur: (i′) the system may have a unique solution (in $\mathbb{R}^{s+1}$), (ii′) the system may have no solutions, or (iii′) the system may have infinitely many solutions. The cases (i′) and (ii′) are good.

- Justify (iii′) is impossible in distinct integers k_j. By the lemma, there is a solution in distinct integers k'_j with either $k'_u = \min_{0 \leq j \leq s}\{k'_j\} \leq -1$ or $k'_v = \max_{0 \leq j \leq s}\{k'_j\} \geq n + 1$. Note both $k'_u \leq 0$ and $k'_v \geq n$ hold. Hence, $n - k'_v + k'_u \leq -1$. Either $n - k'_v + k'_u = n - k'_j + k'_i$ with $(i, j) \neq (u, v)$ or $n - k'_v + k'_u = m$ for some exponent m appearing in $f(x)\tilde{f}(x)$. Both are impossibilities.

- For variable d_j, consider each possibility of cancelled terms in $f(x)\tilde{f}(x)$ and proceed as above.

- After obtaining a solution for $w(x)$, plug the result into $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$ and solve for the d_j. Here, the possibility of infinitely many solutions in the d_j is fine (and occurs).

- Plug in the resulting d_j to see if now $w(x) = \pm f(x)$ or $w(x) = \pm\tilde{f}(x)$. This requires solving another system of equations. Discuss what the final classification looks like.