Lecture 2: Some Properties of $0, 1$-Polynomials

Lemma 1: Suppose $F(x)$ is a $0, 1$-polynomial and $F(x) = u(x)v(x)$ where both $u(x)$ and $v(x)$ are non-reciprocal and have positive leading coefficients. Then the polynomial $w(x) = u(x)\tilde{v}(x)$ has the following properties:
(i) $w \neq \pm F$ and $w \neq \pm \widetilde{F}$.
(ii) $w\widetilde{w} = F\widetilde{F}$.
(iii) $w(1) = F(1)$.
(iv) $\|w\| = \|F\|$.
(v) w is a $0, 1$-polynomial with the same number of non-zero terms as F.

Lemma 2: Let $F(x)$ be a $0, 1$-polynomial with $F(0) = 1$. Then the "non-reciprocal part" of $F(x)$ is reducible if and only if $w(x)$ exists satisfying (i)-(v) of Lemma 1.

Proof: Assume the non-reciprocal part of $F(x)$ is reducible. Let $a(x)$ be an irreducible non-reciprocal factor. If $\tilde{a}(x)$ divides F, write $F(x) = u(x)v(x)$ where $\tilde{a}(x) \nmid u(x)$ and $a(x) \nmid v(x)$. If $\tilde{a}(x)$ does not divide F, consider an irreducible non-reciprocal $b(x)$ such that $a(x)b(x)$ divides F. If $\tilde{b}(x)$ divides F, write $F(x) = u(x)v(x)$ where $\tilde{b}(x) \nmid u(x)$ and $b(x) \nmid v(x)$. If $\tilde{a}(x)$ and $\tilde{b}(x)$ do not divide F, write $F(x) = u(x)v(x)$ where $a(x)|u(x)$ and $b(x)|v(x)$. In each case, u and v are non-reciprocal and we may take both u and v to have a positive leading coefficient. Lemma 1 now implies $w(x)$ exists.

Now, suppose $w(x)$ exists satisfying (i) and (ii) (note that this is all we need here), and we want to show the non-reciprocal part of $F(x)$ is reducible. Assume the non-reciprocal part of $F(x)$ is irreducible or ± 1. Write $F(x) = g(x)h(x)$ where each irreducible factor of $g(x)$ (at most one) is non-reciprocal and each irreducible factor of $h(x)$ is reciprocal. Note that

$$F\widetilde{F} = g\tilde{g}h\tilde{h} = \pm g\tilde{g}h^2.$$

Now, g being irreducible or ± 1 and (ii) imply $w = \pm gh = \pm F$ or $w = \pm \tilde{g}h = \pm \widetilde{F}$. In either case, we have a contradiction.

Theorem 1: Let $F(x)$ be a reciprocal $0, 1$-polynomial. Then $F(x)$ is not divisible by a non-reciprocal polynomial in $\mathbb{Z}[x]$.

Non-Example: $x^6 + x^5 + x^4 + 3x^3 + x^2 + x + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)$

Proof of Theorem 1 (Chris Smyth's version):

- Observe that $\widetilde{F}(x) = F(x)$.
- Assume $F(x)$ has a non-reciprocal factor $g(x)$.
- Then also $\tilde{g}(x)$ is a factor of $F(x)$.
- So $F(x)$ can be written in the form given in Lemma 1 (by Lemma 2).
- Let $w(x)$ be as in Lemma 1. Then $\big(F(x) - w(x)\big)\big(F(x) + \widetilde{w}(x)\big) = \big(\widetilde{w}(x) - w(x)\big)F(x)$.

- Compare the lowest degree non-zero terms on both sides.

Theorem 2: Let $f(x)$ be an irreducible non-reciprocal $0, 1$-polynomial with $f(0) = 1$. Then for each positive integer k, the polynomial $f(x^k)$ is irreducible.

Non-Examples: $x^2 + x + 1$ is irreducible but $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$
$x^2 + 4$ is irreducible but $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$

Open Problem: Maybe "non-reciprocal" can be replaced by "non-cyclotomic".

Proof of Theorem 2:

- Observe that β and $1/\beta$ cannot both be roots of $f(x)$ (since $f(x)$ is both irreducbile and non-reciprocal).
- $f(x^k)$ cannot have both α and $1/\alpha$ as roots (otherwise take $\beta = \alpha^k$).
- Therefore, $f(x)$ has no irreducible reciprocal factors.
- Assume $F(x) = f(x^k)$ is reducible.
- $F(x)$ can be written in the form given in Lemma 1 (by Lemma 2).
- Let $w(x)$ be as in Lemma 1. In particular, each coefficient of $w(x)$ is positive and (ii) holds.
- Observe that each term in $F\widetilde{F}$ has exponent a multiple of k.
- Therefore, $w(x) = h(x^k)$ for some $h(x) \in \mathbb{Z}[x]$.
- Deduce $h(x)\tilde{h}(x) = f(x)\tilde{f}(x)$ so that $h(x) = \pm f(x)$ or $h(x) = \pm \tilde{f}(x)$. Hence, $w(x) = \pm F(x)$ or $w(x) = \pm \widetilde{F}(x)$, a contradiction.

Capelli's Theorem: Discuss as time permits.

Theorem (Odlyzko & Poonen): Let $f(x)$ be a $0, 1$-polynomial with constant term 1. Then each root α of $f(x)$ satisfies:

(i) $\alpha \notin [0, \infty)$.

(ii) Re$(\alpha) < 1.22$.

(iii) $\dfrac{1}{\phi} < |\alpha| < \phi$ where $\phi = (1 + \sqrt{5})/2$.

(iv) If $|\alpha| < 0.7$, then $\alpha \in \mathbb{R}$.

Another Open Problem (Odlyzko and Poonen): If a $0, 1$-polynomial has a root with multiplicity ≥ 2, it is a root of unity.