Lecture 3: Factoring Lacunary Polynomials

Notation:

- *irreducibility* will be over the integers
- if $f(x) = \sum_{j=0}^{n} a_j x^j$, then $\|f\|^2 = \sum_{j=0}^{n} a_j^2$
- $\tilde{f}(x) = x^{\deg f} f(1/x)$
- $\tilde{f}(x)$ will be called the *reciprocal of* $f(x)$
- $f(x)$ *reciprocal* means $\tilde{f}(x) = \pm f(x)$
- the *non-reciprocal part of* $f(x)$ is $f(x)$ removed of its irreducible reciprocal factors (sort of)

Lemma: 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) $w \neq \pm F$ and $w \neq \pm \widetilde{F}$
(ii) $w\widetilde{w} = F\widetilde{F}$
(iii) $\|w\| = \|F\|$
(iv) w is a $0,1$-polynomial with the same number of non-zero terms as F

Example: Demonstrate how the above can be used to factor

$$f(x) = 1 + x^{211} + x^{517} + x^{575} + x^{1245} + x^{1398}.$$

Question 1: Are lacunary polynomials easier to factor than non-lacunary polynomials?

MAPLE Demonstration: Discuss comparisons of running times with MAPLE's `irreduc` command. Mention the next theorem, and use MAPLE to demonstrate a general algorithm for factoring $0,1$-polynomials.

Theorem (F. & Schinzel): There is an algorithm with the following property: Given a non-reciprocal $f(x) \in \mathbb{Z}[x]$ with N non-zero terms and height H, the algorithm determines whether $f(x)$ is irreducible in time $c(N,H)(\log \deg f)^{c'(N)}$ where $c(N,H)$ depends only on N and H and $c'(N)$ depends only on N.

Question 2: Can we categorize the polynomials having small Euclidean norm that are reducible?

Theorem (Mills): Suppose $f(x) = x^a \pm x^b \pm 1$ with $a > b > 0$ or $f(x) = x^a \pm x^b \pm x^c \pm 1$ with $a > b > c > 0$. Then the non-cyclotomic part of $f(x)$ is irreducible unless $f(x)$ is a variation of $x^{8k} + x^{7k} + x^k - 1 = (x^{2k}+1)(x^{3k} + x^{2k} - 1)(x^{3k} - x^k + 1)$.

Theorem (Schinzel): Fix $a_0, \ldots, a_r \in \mathbb{Z} - \{0\}$. Then it is possible to classify the polynomials of the form $a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0$ that have reducible non-reciprocal part.

Theorem (F. & Solan): If $a > b > c > d > 0$, then the non-reciprocal part of $x^a + x^b + x^c + x^d + 1$ is irreducible.

Theorem: If $a > b > c > d > e > 0$, then the non-reciprocal part of $f(x) = x^a + x^b + x^c + x^d + x^e + 1$ is irreducible unless $f(x)$ is a variation of $f(x) = x^{5s+3t} + x^{4s+2t} + x^{2s+2t} + x^t + x^s + 1 = (x^{3s+2t} - x^{s+t} + x^t + 1)(x^{2s+t} + x^s + 1)$.

Theorem (F. & Murphy): If $n > c > b > a > 0$, then the non-reciprocal part of $f(x) = x^n \pm x^c \pm x^b \pm x^a \pm 1$ is irreducible unless $f(x)$ is a variation of ....

Comment: Give some background concerning the proofs. More details of the proofs will be given in subsequent notes.