Lecture 7: Testing Divisibility by Cyclotomic Polynomials

Theorem (F. & Schinzel): There is an algorithm that has the following property: given $f(x) = \sum_{j=1}^{N} a_j x^{d_j} \in \mathbb{Z}[x]$ with $N > 1$ and $\deg f = n > 1$, the algorithm determines whether $f(x)$ has a cyclotomic factor and with running time (as N tends to infinity)

$$\ll \exp\big((6+o(1))\sqrt{N/\log N}(\log N + \log\log n)\big)\log\big(\max_{1\le j\le N}\{|a_j|\}+1\big).$$

Lemma 1. Let $f(x) \in \mathbb{Z}[x]$ have N non-zero terms. If $f(x)$ is divisible by a cyclotomic polynomial, then there is a positive integer m such that every prime divisor of m is $\le N$ and $\Phi_m(x)|f(x)$.

Algorithm: Given $f(x)$ as above, determine whether there is at least one m such that $\Phi_m(x)$ divides $f(x)$.

Step 1. *Determine Relevant Primes.* Compute the set $P = \{p_1, p_2, \dots, p_r\}$ of all primes $\le N$, and let $\mathcal{Q}$ denote the set of all subsets of $\mathcal{P}$.

Step 2. *Obtain Exponent Bounds.* Compute $B_j = \left[\dfrac{\log\deg f}{\log p_j}\right] + 1$ for $1 \le j \le r$.

Step 3. *Compute Possible Cyclotomic Factors.* Construct a list of tuples $\big((q_1,e_1),(q_2,e_2),\dots,(q_s,e_s)\big)$ where $\{q_1,q_2,\dots,q_s\} \in \mathcal{Q}$ and if $q_i = p_j$ then $1 \le e_i \le B_j$.

Step 4. *Check Divisibility.* For each $\big((q_1,e_1),\dots,(q_s,e_s)\big)$ in Step 3, determine whether $\Phi_m(x)$ divides $f(x)$ where $m = q_1^{e_1}q_2^{e_2}\cdots q_s^{e_s}$. If one such m exists, indicate that $f(x)$ has a cyclotomic factor. Otherwise, indicate that $f(x)$ has no cyclotomic factor.

Notation: $f(x)$ mod $w(x)$ denotes the unique polynomial $g(x) \equiv f(x) \pmod{w(x)}$ with either $g(x) \equiv 0$ or $0 \le \deg g(x) < \deg w(x)$.

Lemma 2. Let $f(x) \in \mathbb{Z}[x]$. Let m, k, and ℓ be positive integers, with k and ℓ relatively prime and $m = k\ell$. Let

$$f(xy) \bmod \Phi_\ell(y) = \sum_{j=0}^{\phi(\ell)-1} a_j(x)y^j.$$

Then $\Phi_m(x)$ divides $f(x)$ if and only if $\Phi_k(x)$ divides each $a_j(x)$ for $0 \le j \le \phi(\ell)-1$.

Main Ideas of Proof of Lemma 2:

- Since $m = k\ell$ and k and ℓ being relatively prime, $\zeta_k\zeta_\ell$ is a primitive mth root of unity.
- Plug in $x = \zeta_k$ and $y = \zeta_\ell$ and use $\{1, \zeta_\ell, \zeta_\ell^2, \dots, \zeta_\ell^{\phi(\ell)-1}\}$ is a basis for $\mathbb{Q}(\zeta_m)$ over $\mathbb{Q}(\zeta_k)$ to deduce $\Phi_m(x)|f(x)$ implies $\Phi_k(x)$ divides each $a_j(x)$.
- The reverse implication is established by simply plugging in $x = \zeta_k$ and $y = \zeta_\ell$.

Main Ideas of Proof of Lemma 1:

- Suppose $\Phi_n(x)|f(x)$ and that p is a prime $> N$ for which $p^e||n$. Let $m = n/p^e$. It suffices to show $\Phi_m(x)|f(x)$.
- Write $f(x) = \sum_{j=0}^{r} b_j x^{d_j}$ where the b_j denote non-zero integers and the d_j denote distinct non-negative integers.
- Let $\overline{d}_j = d_j \bmod \ell$ where $\ell = p^e$. Then

$$f(xy) \equiv \sum_{j=0}^{r} b_j x^{d_j} y^{\overline{d}_j} \equiv \sum_{i=0}^{\ell-1} c_i(x) y^i \pmod{\Phi_\ell(y)},$$

  where the $c_i(x)$ are obtained by combining equal values of $\overline{d}_j$.
- Note that $f(x) = \sum_{i=0}^{\ell-1} c_i(x)$, so it suffices to show each $c_i(x)$ is divisible by $\Phi_m(x)$.
- If $\overline{d}_j < \phi(\ell) = p^{e-1}(p-1)$, then the value of $y^{\overline{d}_j}$ will remain unchanged when we consider it mod $\Phi_\ell(y)$. If $\overline{d}_j \geq p^{e-1}(p-1)$, then we use the reduction $y^{\overline{d}_j} = -\sum_{u=1}^{p-1} y^{\overline{d}_j - p^{e-1}u}$. Observe that the terms in this sum have different exponents for different $\overline{d}_j$ in $[p^{e-1}(p-1), p^e)$.
- Consider $i \geq p^{e-1}(p-1)$ (if it exists) for which there is an s with $\overline{d}_s = i$. Then there are $\leq N - 1 < p - 1$ values of $\overline{d}_j$ which are less than $p^{e-1}(p-1)$.
- Some exponent $w = \overline{d}_s - p^{e-1}u$ in the reduction of $y^{\overline{d}_s}$ to its mod $\Phi_\ell(y)$ expression is not a value of any $\overline{d}_j$.
- The value of $a_w(x)$ in Lemma 2 is precisely $-c_i(x)$, so $\Phi_m(x)|c_i(x)$.
- For $i < p^{e-1}(p-1)$, we must have $a_i(x)$ is either $c_i(x)$ or $-c_{i'}(x) + c_i(x)$ where $i' \geq p^{e-1}(p-1)$.
- Since $\Phi_m(x)$ divides $c_{i'}(x)$, again $\Phi_m(x)|c_i(x)$.

How do we determine whether $\Phi_m(x)$ divides $f(x)$ where $m = q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$?

- Compute the product $f(x) \prod_{j=1}^{s} \left(x^{m/q_j} - 1\right)$.
- Reduce exponents modulo m.
- Then $\Phi_m(x)$ divides $f(x)$ if and only if the resulting polynomial is identically 0.

Comments: The actual algorithm for obtaining the running time in the theorem is different in that instead of Lemma 1 the following result (whose proof is based on work of J. H. Conway and A. J. Jones) is used:

Lemma 1′: Let $f(x) \in \mathbb{Z}[x]$ have N non-zero terms. If $f(x)$ is divisible by a cyclotomic polynomial, then there is a positive integer m such that

$$2 + \sum_{p|m} (p-2) \leq N \quad \text{and} \quad \Phi_m(x)|f(x).$$