Seminar Notes: *Irreducibility and greatest common divisor algorithms for sparse polynomials* (11/29/06)

Joint work with Andrzej Schinzel

Theorem A. *There are constants $c_1 = c_1(r, H)$ and $c_2 = c_2(r)$ such that an algorithm exists for determining whether a given nonreciprocal polynomial $f(x) \in \mathbb{Z}[x]$ as above is irreducible and that runs in time $O\big(c_1 \cdot (\log n)^{c_2}\big)$.*

Definition 1. *For a polynomial $F\big(x_1, \dots, x_r, x_1^{-1}, \dots, x_r^{-1}\big)$, in the variables $x_1, \dots, x_r$ and their reciprocals $x_1^{-1}, \dots, x_r^{-1}$, define*

$$J\,F = x_1^{u_1} \cdots x_r^{u_r} F\big(x_1, \dots, x_r, x_1^{-1}, \dots, x_r^{-1}\big),$$

where each u_j is an integer chosen as small as possible so that $J\,F$ is a polynomial in $x_1, \dots, x_r$. Then $F(x_1, \dots, x_r) \in \mathbb{Q}[x_1, \dots, x_r]$ is reciprocal if

$$J\,F\big(x_1^{-1}, \dots, x_r^{-1}\big) = \pm F(x_1, \dots, x_r).$$

Some Numbered Equations:

$$\begin{pmatrix} d_1 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v_1 \\ \vdots \\ v_t \end{pmatrix} \tag{1}$$

$$y_1^{u_1} \cdots y_t^{u_t} F(y_1^{m_{11}} \cdots y_t^{m_{1t}}, \dots, y_1^{m_{r1}} \cdots y_t^{m_{rt}}) = F_1(y_1, \dots, y_t) \cdots F_s(y_1, \dots, y_t) \tag{2}$$

$$f(x) = \prod_{i=1}^{s} x^{w_i} F_i(x^{v_1}, \dots, x^{v_t}) = \prod_{i=1}^{s} J\,F_i(x^{v_1}, \dots, x^{v_t}) \tag{3}$$

Easy but Important Point: (1) and (2) imply (3)

Theorem 1 (Schinzel, 1969)**.** *Fix*

$$F = F(x_1, \dots, x_r) = a_r x_r + \cdots + a_1 x_1 + a_0,$$

where the a_j are nonzero integers. There exists a finite computable set of matrices S with integer entries, depending only on F, with the following property: Suppose the vector $\overrightarrow{d} = \langle d_1, d_2, \dots, d_r \rangle$ is in $\mathbb{Z}^r$ with $d_r > d_{r-1} > \cdots > d_1 > 0$ and such that $f(x) = F(x^{d_1}, x^{d_2}, \dots, x^{d_r})$ has no non-constant reciprocal factor. Then there is an $r \times t$ matrix $M = (m_{ij}) \in S$ of rank $t \le r$ and a vector $\overrightarrow{v} = \langle v_1, v_2, \dots, v_t \rangle$ in $\mathbb{Z}^t$ such that (1) holds and the factorization given by (2) in $\mathbb{Z}[y_1, \dots, y_t]$ of a polynomial in t variables $y_1, y_2, \dots, y_t$ as a product of s irreducible polynomials over $\mathbb{Q}$ implies the factorization of $f(x)$ given by (3) as a product of polynomials in $\mathbb{Z}[x]$ each of which is either irreducible over $\mathbb{Q}$ or a constant.

Main Points:
- (1) happens for some M from a finite set not depending on $d_1, d_2, \dots, d_r$
- (1) and (2) with irreducibles imply (3) with irreducibles

Theorem B. *There is an algorithm which takes as input two polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, each of degree $\leq n$ and height $\leq H$ and having $\leq r+1$ nonzero terms, with at least one of $f(x)$ and $g(x)$ free of cyclotomic factors, and outputs the value of $\gcd_{\mathbb{Z}}(f(x), g(x))$ and runs in time $O\big(c_5 \log n\big)$ for some constant $c_5 = c_5(r, H)$.*

Theorem 2 (Bombieri & Zannier, 2000)**.** *Let*

$$F(x_1, \ldots, x_k), G(x_1, \ldots, x_k) \in \mathbb{Q}[x_1, \ldots, x_k]$$

be coprime polynomials. There exists an effectively computable number $B(F, G)$ with the following property. If $\overrightarrow{u} = \langle u_1, \ldots, u_k \rangle \in \mathbb{Z}^k$, $\xi \neq 0$ is algebraic and

$$F(\xi^{u_1}, \ldots, \xi^{u_k}) = G(\xi^{u_1}, \ldots, \xi^{u_k}) = 0,$$

then either ξ is a root of unity or there exists a nonzero vector $\overrightarrow{v} \in \mathbb{Z}^k$ having components bounded in absolute value by $B(F, G)$ and orthogonal to $\overrightarrow{u}$.