Theorem (Granville, Schinzel, F.): *An algorithm exists for determining if a given nonreciprocal polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible and that runs in time*

$$O_{r,H}\big(\log n\,(\log\log n)^2 |\log\log\log n|\big).$$

- **If f has no cyclotomic factor but has a reciprocal factor, then the algorithm will give an explicit reciprocal factor.**

---

f does not have a cyclotomic factor

We want to compute $\gcd(f, g)$ where $g(x) = x^{\deg f} f(1/x) \neq f(x)$.

Theorem (Granville, Schinzel, F.): *There is an algorithm which takes as input two polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, each of degree $\le n$ and height $\le H$ and having $\le r+1$ nonzero terms, with at least one of $f(x)$ and $g(x)$ free of any cyclotomic factors, and outputs the value of $\gcd_{\mathbb{Z}}(f(x), g(x))$ and runs in time $O_{r,H}\big(\log n\big)$.*

$$f(x) = \sum_{j=1}^{k} a_j x^{d_j} \longrightarrow F_1(\vec{x}) = \sum_{j=1}^{k} a_j x_j$$

$$g(x) = \sum_{j=1}^{k} b_j x^{d_j} \longrightarrow F_2(\vec{x}) = \sum_{j=1}^{k} b_j x_j$$

Theorem (Granville, Schinzel, F.): *There is an algorithm which takes as input two polynomials* $f(x)$ *and* $g(x)$ *in* $\mathbb{Z}[x]$, *each of degree* $\le n$ *and height* $\le H$ *and having* $\le r+1$ *nonzero terms, with at least one of* $f(x)$ *and* $g(x)$ *free of any cyclotomic factors, and outputs the value of* $\gcd_{\mathbb{Z}}(f(x), g(x))$ *and runs in time* $O_{r,H}\big(\log n\big)$.

$$F_1\big(x^{d_1}, \dots, x^{d_k}\big) = f(x)$$

$$F_2\big(x^{d_1}, \dots, x^{d_k}\big) = g(x)$$

Lemma (Bombieri and Zannier): *Let*

$$F_1, F_2 \in \mathbb{Q}[x_1, \ldots, x_k]$$

be coprime polynomials. There exists a number $c_1(F_1, F_2)$ *with the following property. If* $\overrightarrow{u} = \langle u_1, \ldots, u_k \rangle \in \mathbb{Z}^k$, $\xi \neq 0$ *is algebraic and*

$$F_1(\xi^{u_1}, \ldots, \xi^{u_k}) = F_2(\xi^{u_1}, \ldots, \xi^{u_k}) = 0,$$

then either ξ *is a root of unity or there exists a non-zero vector* $\overrightarrow{v} \in \mathbb{Z}^k$ *having length at most* c_1 *and orthogonal to* $\overrightarrow{u}$.

$$f(x) = \sum_{j=1}^{k} a_j x^{d_j} \quad \rightarrow \quad F_1(\vec{x}) = \sum_{j=1}^{k} a_j x_j$$

$$g(x) = \sum_{j=1}^{k} b_j x^{d_j} \quad \rightarrow \quad F_2(\vec{x}) = \sum_{j=1}^{k} b_j x_j$$

There exists a number $c_1(\overrightarrow{a}, \overrightarrow{b}, k)$ *with the following property. If* $f(\xi) = g(\xi) = 0$, *then there exists a non-zero vector* $\overrightarrow{v} \in \mathbb{Z}^k$ *having length at most* c_1 *and orthogonal to* $\overrightarrow{u}$.

$$\overrightarrow{u} = \langle d_1, \ldots, d_k \rangle$$

Note: It is important that c_1 is computable.

Idea: The lattice of vectors orthogonal to $\overrightarrow{v}$ is $(k-1)$-dimensional so that there exists a vector $\langle e_1, \ldots, e_{k-1}\rangle$ and a matrix $\mathcal{M}$ in $\mathbb{Z}^{k-1}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_k \end{pmatrix} = \mathcal{M} \cdot \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_{k-1} \end{pmatrix}.$$

So

$$d_i = \sum_{j=1}^{k-1} m_{ij} e_j,$$

with the $m_{ij} \in \mathbb{Z}$ bounded.

$$d_i = \sum_{j=1}^{k-1} m_{ij} e_j \qquad x^{d_i} = \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$f(x) = \sum_{i=1}^{k} a_i x^{d_i} = \sum_{i=1}^{k} a_i \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$F_1^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} a_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$g(x) = \sum_{i=1}^{k} b_i x^{d_i} = \sum_{i=1}^{k} b_i \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$d_i = \sum_{j=1}^{k-1} m_{ij} e_j \qquad x^{d_i} = \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$F_1^{(2)}\left(x^{e_1}, \ldots, x^{e_{k-1}}\right) = f(x)$$

$$F_1^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} a_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$g(x) = \sum_{i=1}^{k} b_i x^{d_i} = \sum_{i=1}^{k} b_i \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$d_i = \sum_{j=1}^{k-1} m_{ij} e_j \qquad x^{d_i} = \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$F_1^{(2)}\left(x^{e_1}, \ldots, x^{e_{k-1}}\right) = f(x)$$

$$F_1^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} a_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$g(x) = \sum_{i=1}^{k} b_i x^{d_i} = \sum_{i=1}^{k} b_i \prod_{j=1}^{k-1} \left(x^{e_j}\right)^{m_{ij}}$$

$$F_2^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} b_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$d_i = \sum_{j=1}^{k-1} m_{ij} e_j \qquad x^{d_i} = \prod_{j=1}^{k-1} (x^{e_j})^{m_{ij}}$$

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_1^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} a_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$F_2^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} b_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$F_1^{(2)}\left(x^{e_1}, \ldots, x^{e_{k-1}}\right) = f(x)$$

$$F_1^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} a_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$F_2^{(2)}\left(x^{e_1}, \ldots, x^{e_{k-1}}\right) = g(x)$$

$$F_2^{(2)}(y_1, \ldots, y_{k-1}) = \sum_{i=1}^{k} b_i \prod_{j=1}^{k-1} y_j^{m_{ij}}$$

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$f(x) = \sum_{j=1}^{k} a_j x^{d_j} \quad \longrightarrow \quad F_1(\vec{x}) = \sum_{j=1}^{k} a_j x_j$$

$$g(x) = \sum_{j=1}^{k} b_j x^{d_j} \quad \longrightarrow \quad F_2(\vec{x}) = \sum_{j=1}^{k} b_j x_j$$

$$F_1(x^{d_1}, \ldots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \ldots, x^{d_k}) = g(x)$$

Lemma (Bombieri and Zannier): *Let*

$$F_1, F_2 \in \mathbb{Q}[x_1, \ldots, x_k]$$

be coprime polynomials. There exists a number $c_1(F_1, F_2)$ *with the following property. If* $\overrightarrow{u} = \langle u_1, \ldots, u_k \rangle \in \mathbb{Z}^k$, $\xi \neq 0$ *is algebraic and*

$$F_1(\xi^{u_1}, \ldots, \xi^{u_k}) = F_2(\xi^{u_1}, \ldots, \xi^{u_k}) = 0,$$

then either ξ *is a root of unity or there exists a non-zero vector* $\overrightarrow{v} \in \mathbb{Z}^k$ *having length at most* c_1 *and orthogonal to* $\overrightarrow{u}$.

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$f(x) = \sum_{j=1}^{k} a_j x^{d_j} \quad \longrightarrow \quad F_1(\vec{x}) = \sum_{j=1}^{k} a_j x_j$$

$$g(x) = \sum_{j=1}^{k} b_j x^{d_j} \quad \longrightarrow \quad F_2(\vec{x}) = \sum_{j=1}^{k} b_j x_j$$

$$F_1(x^{d_1}, \ldots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \ldots, x^{d_k}) = g(x)$$

$$F_1(x^{d_1}, \ldots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \ldots, x^{d_k}) = g(x)$$

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$F_1(x^{d_1}, \dots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \dots, x^{d_k}) = g(x)$$

$$F_1^{(2)}(x^{e_1}, \dots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \dots, x^{e_{k-1}}) = g(x)$$

$$\Longrightarrow \quad \begin{aligned} F_1^{(k)}(x^{\text{some exponent}}) &= f(x) \\ F_2^{(k)}(x^{\text{same exponent}}) &= g(x) \end{aligned}$$

$$F_1(x^{d_1}, \ldots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \ldots, x^{d_k}) = g(x)$$

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$\Longrightarrow \quad \begin{aligned} F_1^{(k)}(x^{\text{some exponent}}) &= f(x) \\ F_2^{(k)}(x^{\text{same exponent}}) &= g(x) \end{aligned}$$

The exponents and coefficients in $F_1^{(j)}$ and $F_2^{(j)}$ remain bounded.

$$F_1(x^{d_1}, \ldots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \ldots, x^{d_k}) = g(x)$$

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$\Longrightarrow \begin{array}{l} F_1^{(k)}(x^{\text{some exponent}}) = f(x) \\ F_2^{(k)}(x^{\text{same exponent}}) = g(x) \end{array}$$

Compute $\gcd\left(F_1^{(k)}(x), F_2^{(k)}(x)\right)$.

$$F_1(x^{d_1}, \ldots, x^{d_k}) = f(x)$$

$$F_2(x^{d_1}, \ldots, x^{d_k}) = g(x)$$

$$F_1^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = f(x)$$

$$F_2^{(2)}(x^{e_1}, \ldots, x^{e_{k-1}}) = g(x)$$

$$\Longrightarrow \quad \begin{array}{l} F_1^{(k)}(x^{\text{some exponent}}) = f(x) \\ F_2^{(k)}(x^{\text{same exponent}}) = g(x) \end{array}$$

Note we are not saying such $F_1^{(k)}(x)$ and $F_2^{(k)}(x)$ exist.

Lemma (Bombieri and Zannier): *Let*

$$F_1, F_2 \in \mathbb{Q}[x_1, \ldots, x_k]$$

be coprime polynomials. There exists a number $c_1(F_1, F_2)$ *with the following property. If* $\overrightarrow{u} = \langle u_1, \ldots, u_k \rangle \in \mathbb{Z}^k$, $\xi \neq 0$ *is algebraic and*

$$F_1(\xi^{u_1}, \ldots, \xi^{u_k}) = F_2(\xi^{u_1}, \ldots, \xi^{u_k}) = 0,$$

then either ξ *is a root of unity or there exists a non-zero vector* $\overrightarrow{v} \in \mathbb{Z}^k$ *having length at most* c_1 *and orthogonal to* $\overrightarrow{u}$.

One additional item for the Final Exam

(and future Comps)

Let $f(x) \in \mathbb{R}[x]$ with $f(0) \neq 0$. Write

$$f(x) = \sum_{j=0}^{n} a_j x^j = a_n \prod_{j=1}^{n} (x - \alpha_j)$$

and

$$w(x) = a_n \prod_{\substack{1 \le j \le n \\ |\alpha_j| > 1}} (x - \alpha_j) \prod_{\substack{1 \le j \le n \\ |\alpha_j| \le 1}} (\alpha_j x - 1).$$

Recall that

$$M(f) = |a_n| \prod_{1 \le j \le n} \max\{|\alpha_j|, 1\} \quad \text{and} \quad \|f\| = \sqrt{\sum_{j=0}^{n} a_j^2}\,.$$

Prove the following:

(a) Explain why $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.

(b) Prove $M(f) \le \|f\|$.

(c) For $f(x) \in \mathbb{R}[x]$, prove $\|f\| \le 2^{\deg f} M(f)$.

(d) Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}[x]$ such that $g(x) | f(x)$. Prove $\|g\| \le 2^{\deg g} \|f\|$.