Office Hours This Week:	**M**	**3:00-4:00 p.m.**
	W	**2:15-3:15 p.m.**
	R	**12:00-1:00 p.m.**

Lemma 9.1.1. *Let $f(x)$ be an arbitrary polynomial in $\mathbb{Z}[x]$. If the non-reciprocal part of $f(x)$ is reducible, then there exist polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying $u(x)$ and $v(x)$ are both non-reciprocal and $f(x) = u(x)v(x)$.*

Lemma 9.1.3. *Suppose $f(x)$ is a $0,1$-polynomial with $f(0) \neq 0$ and $f(x) = u(x)v(x)$ where each of $u(x)$ and $v(x)$ is non-reciprocal and each of $u(x)$ and $v(x)$ has a positive leading coefficient. Then the polynomial $w(x) = u(x)\tilde{v}(x)$ also has the following properties:*

(i) $w(x) \neq \pm f(x)$ *and* $w(x) \neq \pm \tilde{f}(x)$*.*

(ii) $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$*.*

(iii) $w(1)^2 = f(1)^2$*.*

(iv) $\|w\| = \|f\|$*.*

(v) $w(x)$ *is a $0,1$-polynomial with the same number of non-zero terms as* $f(x)$*.*

(vi) $w(1) = f(1)$*.*

Examples of questions we would like to answer:

1. How does

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

factor in $\mathbb{Z}[x]$?

2. Let $f_0(x) = 1$. For $k \geq 1$, define $f_k(x)$ to be the reducible polynomial of the form $f_{k-1}(x)+x^n$ with n as small as possible and $n > \deg f_{k-1}$.

$$F(x) = x^n + x^{35} + x^{34} + x^{33} + x^{32} + x^{16} + x^{15} + x^3 + 1$$

1. How does

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

factor in $\mathbb{Z}[\boldsymbol{x}]$?

1. How does

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

factor in $\mathbb{Z}[x]$?

Lemma 9.1.3. *Suppose $f(x)$ is a $0,1$-polynomial with $f(0) \neq 0$ and $f(x) = u(x)v(x)$ where each of $u(x)$ and $v(x)$ is non-reciprocal and each of $u(x)$ and $v(x)$ has a positive leading coefficient. Then the polynomial $w(x) = u(x)\tilde{v}(x)$ also has the following properties:*

(i) $w(x) \neq \pm f(x)$ *and* $w(x) \neq \pm \tilde{f}(x)$.

(ii) $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.

(iii) $w(1)^2 = f(1)^2$.

(iv) $\|w\| = \|f\|$.

(v) $w(x)$ *is a $0,1$-polynomial with the same number of non-zero terms as* $f(x)$.

1. How does

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

factor in $\mathbb{Z}[x]$?

Lemma 9.1.3. *Suppose $f(x)$ is a $0,1$-polynomial with $f(0) \neq 0$ and $f(x) = u(x)v(x)$ where each of $u(x)$ and $v(x)$ is non-reciprocal and each of $u(x)$ and $v(x)$ has a positive leading coefficient. Then the polynomial $w(x) = u(x)\tilde{v}(x)$ also has the following properties:*

(i) $w(x) \neq \pm f(x)$ *and* $w(x) \neq \pm \tilde{f}(x)$.

(ii) $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.

(v) $w(x)$ *is a $0,1$-polynomial with the same number of non-zero terms as* $f(x)$.

1. How does

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

factor in $\mathbb{Z}[x]$?

Lemma 9.1.3. *Suppose $f(x)$ is a $0,1$-polynomial with $f(0) \neq 0$ and $f(x) = u(x)v(x)$ where each of $u(x)$ and $v(x)$ is non-reciprocal and each of $u(x)$ and $v(x)$ has a positive leading coefficient. Then the polynomial $w(x) = u(x)\tilde{v}(x)$ also has the following properties:*

(i) $w(x) \neq \pm f(x)$ *and* $w(x) \neq \pm \tilde{f}(x)$.

(ii) $w(x)\widetilde{w}(x) = f(x)\tilde{f}(x)$.

(v) $w(x)$ *is a $0,1$-polynomial with the same number of non-zero terms as* $f(x)$.

What if such a $w(x)$ exists?

(Maple Time)

Irreducibility and GCD Algorithms for Sparse Polynomials

joint work with

Andrew Granville

Andrzej Schinzel

§ Introduction

Suppose we want to check the primality of

$$N = 2^{30402457} - 1.$$

How fast can we do this computation?

How fast can we expect to do it?

If the number of binary operations for a computation is bounded by a polynomial in the length of the input, then we say it can be done in polynomial time.

§ Introduction

Suppose we want to check the primality of

$$N = 2^{30402457} - 1.$$

How fast can we do this computation?

How fast can we expect to do it?

What is the length of the input?

The number N contains 30402457 bits.

Determining if N is prime in 30402457^2 steps would be good.

§ Introduction

Suppose we want to check the primality of

$$N = 2^{30402457} - 1.$$

How fast can we do this computation?

How fast can we expect to do it?

What is the length of the input?

To clarify, typing

```
2^30402457-1
```

takes 12 keystrokes.

But this is a talk about polynomials

$$f(x) \in \mathbb{Z}[x].$$

Suppose f has degree n, height $\leq H$ and $\leq r$ ~~non-zero~~ terms.

all terms are non-zero

maximum coefficient in absolute value

But this is a talk about polynomials

$$f(x) \in \mathbb{Z}[x].$$

Suppose f has degree n, height $\le H$ and $\le r$ non-zero terms.

Traditionally, $f(x)$ has $n+1$ coefficients and each coefficient can have "length" on the order of $\log H$ so that the total length of the input is of order $n \log H$. Actually, I should say $n\big(\log H + \log n\big)$.

But this is a talk about polynomials

$$f(x) \in \mathbb{Z}[x].$$

Suppose f has degree n, height $\leq H$ and $\leq r$ non-zero terms.

Lenstra, Lenstra and Lovasz showed that one can factor f in time that is polynomial in n and $\log H$.

But this is a talk about polynomials

$$f(x) \in \mathbb{Z}[x].$$

Suppose f has degree n, height $\leq H$ and $\leq r$ non-zero terms.

We might expect an algorithm exists that runs in time that is polynomial in $\log n$, r and $\log H$

Example:

$$
\begin{aligned}
&+ x^{66} + x^{65} + x^{64} + x^{63} + x^{62} \\
&+ x^{61} + x^{60} + x^{59} + x^{58} + x^{57} \\
&+ x^{56} + x^{55} + x^{54} + x^{53} + x^{52} \\
&+ x^{51} + x^{50} + x^{49} + x^{48} + x^{47} \\
&+ x^{46} + x^{45} + x^{44} + x^{43} + x^{42} \\
&+ x^{41} + x^{40} + x^{39} + x^{38} + x^{37} \\
&+ x^{36} + x^{35} + x^{34} + x^{33} + x^{32} \\
&+ x^{31} + x^{30} + x^{29} + x^{28} + x^{27} \\
&+ x^{26} + x^{25} + x^{24} + x^{23} + x^{22} \\
&+ x^{21} + x^{20} + x^{19} + x^{18} + x^{17}
\end{aligned}
$$

$$+x^{16}+x^{15}+x^{14}+x^{13}+x^{11}$$
$$+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}$$
$$+x^{4}+x^{3}+x^{2}+x+1)$$

But this is a talk about *irreducibility testing* of polynomials

$$f(x) \in \mathbb{Z}[x].$$

Here, it is more reasonable to expect an algorithm to run in time that is polynomial in $\log n$, r and $\log H$.

But we won't do that.

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*

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

$f(x)$ is reciprocal means that if $f(\alpha) = 0$, then $\alpha \neq 0$ and $f(1/\alpha) = 0$

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*

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

$f(x)$ is reciprocal means that

$$f(x) = \pm\, x^{\deg f} f(1/x)$$

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*

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

$$\boxed{f(x) \neq \pm\, x^{\deg f} f(1/x)}$$

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*

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

Remark: If the polynomial is reducible, then it is possible to determine a non-trivial factor in the same time but ...

- **If f has a cyclotomic factor, then the algorithm will detect this and output an $m \in \mathbb{Z}^+$ with $\Phi_m(x)$ a factor.**
- **If f has no cyclotomic factor but has a reciprocal factor, then the algorithm will give an explicit reciprocal factor.**
- **Otherwise, the algorithm outputs the complete factorization of $f(x)$ into irreducible polynomials over $\mathbb{Q}$.**

Comment: It is not even obvious that such output can be given in time that is less than polynomial in $\deg f$.

- If f has a cyclotomic factor, then the algorithm will detect this and output an $m \in \mathbb{Z}^+$ with $\Phi_m(x)$ a factor.
- If f has no cyclotomic factor but has a reciprocal factor, then the algorithm will give an explicit reciprocal factor.
- Otherwise, the algorithm outputs the complete factorization of $f(x)$ into irreducible polynomials over $\mathbb{Q}$.

The algorithm does these in the order listed.

Corollary: ***If $f(x) \in \mathbb{Z}[x]$ is nonreciprocal and reducible, then $f(x)$ has a nontrivial factor in $\mathbb{Z}[x]$ which contains $\le c(r, H)$ terms.***

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*

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

Open Vague Problem: Is there a sparse nonreciprocal polynomial that behaves like

$$1 + x + x^2 + \cdots + x^{n-1}\,?$$

- **If f has a cyclotomic factor, then the algorithm will detect this and output an $m \in \mathbb{Z}^+$ with $\Phi_m(x)$ a factor.**

Theorem (Granville, Schinzel, F.): *There is an algorithm that has the following property: given $f(x) = \sum_{j=0}^{r} a_j x^{d_j} \in \mathbb{Z}[x]$ of degree $n > 1$ and with $r+1$ terms, the algorithm determines if $f(x)$ has a cyclotomic factor in running time*

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

- **If f has a cyclotomic factor, then the algorithm will detect this and output an $m \in \mathbb{Z}^+$ with $\Phi_m(x)$ a factor.**

Rough Thought: Find an approach for determing if $f(x)$ has a cyclotomic factor that only makes use of basic arithmetic operations on the exponents of $f(x)$.

And that approach is

- **If f has a cyclotomic factor, then the algorithm will detect this and output an $m \in \mathbb{Z}^+$ with $\Phi_m(x)$ a factor.**

Rough Thought: Find an approach for determing if $f(x)$ has a cyclotomic factor that only makes use of basic arithmetic operations on the exponents of $f(x)$.

And that approach is (... drum roll ...)

There is a cyclotomic factor of $f(x) = \sum_{j=0}^{r} a_j x^{d_j}$ **if and only if** $\exists$ **a partition**

$$\{0, 1, \ldots, r\} = J_1 \dot\cup J_2 \dot\cup \cdots \dot\cup J_s$$

such that if, for $1 \le i \le s$,

$$\sum_{j \in J_i} a_j x^{d_j} = x^{b_i} g_i(x^{e_i}), \quad M_i = \cdots$$

then there are $m_i \in M_i$ **for which**

$$m_0 = \prod_{p \mid m_1 \cdots m_s} \max_{1 \le i \le s} \{p^k : p^k \| m_i e_i\}$$

satisfies

$$m_0 = m_i \gcd(m_0, e_i), \quad i \in \{1, 2, \ldots, s\}.$$

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

We'll come back to this.

- **Otherwise, the algorithm outputs the complete factorization of $f(x)$ into irreducible polynomials over $\mathbb{Q}$.**

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j}$$

f has no reciprocal factors

(other than constants)

- **Otherwise, the algorithm outputs the complete factorization of $f(x)$ into irreducible polynomials over $\mathbb{Q}$.**

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j}$$

$$\begin{aligned} F &= F(x_1, x_2, \ldots, x_r) \\ &= a_r x_r + \cdots + a_1 x_1 + a_0, \end{aligned}$$

$$f(x) = F\left(x^{d_1}, x^{d_2}, \ldots, x^{d_r}\right)$$

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j}, \qquad F(x_1, \ldots, x_r) = a_0 + \sum_{j=1}^{r} a_j x_j$$

$$(1) \qquad \begin{pmatrix} d_1 \\ \vdots \\ d_r \end{pmatrix} = (m_{ij})_{r\times t} \begin{pmatrix} v_1 \\ \vdots \\ v_t \end{pmatrix}$$

$$d_i = m_{i1}v_1 + \cdots + m_{it}v_t, \ 1 \leq i \leq r$$

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j}, \qquad F(x_1, \ldots, x_r) = a_0 + \sum_{j=1}^{r} a_j x_j$$

$$(1) \qquad d_i = m_{i1} v_1 + \cdots + m_{it} v_t, \; 1 \le i \le r$$

(m_{ij}) will come from a finite set depending only on F

$v_j \in \mathbb{Z}$ show exist for some (m_{ij})

$$f(x) = \sum_{j=0}^{r} a_j x^{d_j}, \quad F(x_1, \ldots, x_r) = a_0 + \sum_{j=1}^{r} a_j x_j$$

$$(1) \quad d_i = m_{i1}v_1 + \cdots + m_{it}v_t, \; 1 \le i \le r$$

$$F(y_1^{m_{11}} \cdots y_t^{m_{1t}}, \ldots, y_1^{m_{r1}} \cdots y_t^{m_{rt}})$$

$$y_j = x^{v_j}, \quad 1 \le j \le t$$

$$F\left(x^{d_1}, x^{d_2}, \ldots, x^{d_r}\right) = f(x)$$

Thought: A factorization in $\mathbb{Z}[y_1, \ldots, y_t]$ implies a factorization of $f(x)$ in $\mathbb{Z}[x]$.