§ 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.

Remark: If the polynomial is reducible, then it is possible to determine a non-trivial factor in the same time but ...
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 $f$ has a non-trivial factor in $\mathbb{Z}[x]$ which contains $c(r, H)$ terms.

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

Example: For almost any $a_j \in \mathbb{Z}$ with $|a_j| \leq 1000$ and any positive integers $\epsilon_1, \ldots, \epsilon_{100}$, if the polynomial
\[ a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_{100} x^{100} \]
is reducible over $\mathbb{Q}$, then it has a non-trivial factor with $\leq c$ terms.

Theorem (A. Schinzel and M.F. 2004): There is an algorithm which determines if a given $f(x) \in \mathbb{Z}[x]$ of degree $n > 1$, which has height $H$ and $r > 1$ non-zero terms, has a cyclotomic factor and that runs in time big-of $c_1(H, r)(\log n)^{c_2(r)}$ as $r$ tends to infinity.

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

The division algorithm for polynomials takes time that is polynomial in the degrees of the input polynomials.

\[ x^{100} - x^{18} + 1 = (x^3 + x + 1)q(x) + r(x) \]
\[ q(x) \text{ has } 96 \text{ terms} \]
\[ r(x) = 101010478x^2 - 19122919x - 60075671 \]

To check whether a fixed $\Phi_m(x)$ divides $f(x)$, check instead whether $(x^{m-1}) | f(x)$.

We’ll come back to this.
\[ f(x) = \sum_{j=1}^{r} a_j x^j, \quad F(x_1, \ldots, x_t) = a_0 + \sum_{j=1}^{r} a_j x^j \]

(1) \[ d_i = m_{i1} v_1 + \cdots + m_{it} v_t, \quad 1 \leq i \leq r \]

\[ F(y_1^{m_{i1}} \cdots y_t^{m_{it}}, \ldots, y_1^{m_{i1}} \cdots y_t^{m_{it}}) = \prod_{i=1}^{r} F_i(y_1, \ldots, y_t) \]

\[ y_j = x^{v_j}, \quad 1 \leq j \leq t \]

\[ F(x_1^{d_1}, x_2^{d_2}, \ldots, x_t^{d_t}) = f(x) \]

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

Counter-Thought: We want \( m_{ij} \) and \( v_j \) in \( \mathbb{Z} \), but not necessarily positive.

\[ f(x) = \sum_{j=1}^{t} a_j v^j, \quad F(x_1, \ldots, x_t) = a_0 + \sum_{j=1}^{t} a_j v^j \]

(1) \[ d_i = m_{i1} v_1 + \cdots + m_{it} v_t, \quad 1 \leq i \leq r \]

\[ F(y_1^{m_{i1}} \cdots y_t^{m_{it}}, \ldots, y_1^{m_{i1}} \cdots y_t^{m_{it}}) \]

\[ y_j = x^{v_j}, \quad 1 \leq j \leq t \]

\[ F(x_1^{d_1}, x_2^{d_2}, \ldots, x_t^{d_t}) = f(x) \]

Recall: Factor and substitute \( y_j = x^{v_j} \).

**Theorem (A. Schinzel, 1969):** Fix

\[ F = a_0 x_1 + \cdots + a_t x_t + a_0, \]

with \( a_j \) 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

\[ \overrightarrow{a} = (d_1, d_2, \ldots, d_t) \in \mathbb{Z}^t \]

with \( d_0 > \cdots > d_t > 0 \), is such that

\[ f(x) = F(x_1, x_2, \ldots, x_t) \]

has no non-constant reciprocal factor.

This Part of Algorithm:

- Compute set of matrices \( S \).
- The set of matrices depends on

\[ F = a_0 x_1 + \cdots + a_t x_t + a_0, \]

not on \( d_1, d_2, \ldots, d_t \).

(3) \[ f(x) = \sum_{i=1}^{s} x^{v_i} F_i(x_1, \ldots, x_t) \]

Conclusion: (1) and (2) imply (3)

This Part of Algorithm:

- Compute set of matrices \( S \).
- Determine all solutions to (1).

(1) \[ d_i = m_{i1} v_1 + \cdots + m_{it} v_t, \quad 1 \leq i \leq r \]

Easy Lemma: There’s an algorithm that determines for a given integral matrix \( (m_{ij}) \in S \) whether (1) holds for some \( v_j \in \mathbb{Z} \). If it does, the solution is unique and the algorithm outputs the solution. The algorithm runs in time \( O(r \log n) \).

Each \( x^{v_i} F_i(x_1, \ldots, x_t) \) is a constant or irreducible for some solution to (1).

This Part of Algorithm:

- Compute set of matrices \( S \).
- Determine all solutions to (1).

(1) \[ d_i = m_{i1} v_1 + \cdots + m_{it} v_t, \quad 1 \leq i \leq r \]

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

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

We’ve checked:

\[ f \] does have a cyclotomic factor.

We want to know:

Does \( f \) have a reciprocal factor?

Does \( f \) have a reciprocal factor?

Suppose \( w(x) \) is a reciprocal factor.

\[ w(\alpha) = 0 \implies \alpha \neq 0 \quad \text{and} \quad w(1/\alpha) = 0 \implies f(\alpha) = 0 \quad \text{and} \quad g(\alpha) = 0, \]

where \( g(x) = x^{\deg f(1/x)} \neq f(x) \)

We want to compute \( \gcd(f, g) \).
In general, if $f$ and $g$ are sparse polynomials around degree $n$ in $\mathbb{Z}[x]$, how does one compute $\gcd(f, g)$? Some items to keep in mind:

→ The Euclidean algorithm will run in time that is polynomial in $n$, not $\log n$.

→ Plaisted (1977) has shown that this problem is at least as hard as any problem in NP.

Plaisted's takes $f$ and $g$ to be divisors of $x^N - 1$ where $N$ is a product of small primes.

We are interested in the case that both $f$ and $g$ do not have a cyclotomic factor.

**Theorem (A. Schinzel and M.F.):** 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 $r + 1$ nonzero terms, with at least one of $f(x)$ and $g(x)$ free of any cyclotomic factors, and outputs the value of $\gcd(f(x), g(x))$ and runs in time $O_H(\log n)$.

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

which have arbitrarily many terms.

**Corollary:** If $f(x), g(x) \in \mathbb{Z}[x]$ with $f(x)$ or $g(x)$ not divisible by a cyclotomic polynomial, then $\gcd(f(x), g(x))$ has $O_H(1)$ terms.

Note that if $a$ and $b$ are relatively prime positive integers, then

$$\gcd(x^a - 1, (x^a - 1)(x^b - 1)) = (x^a - 1)(x^b - 1) = x - 1$$

Theorem (A. Schinzel and M.F.): 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 $r + 1$ nonzero terms, with at least one of $f(x)$ and $g(x)$ free of any cyclotomic factors, and outputs the value of $\gcd(f(x), g(x))$ and runs in time $O_H(\log n)$.

**Lemma (Bomberi 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 $\mathfrak{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$, $\xi \neq 0$ is algebraic and $F_1(\xi^{a_1}, \ldots, \xi^{a_k}) = F_2(\xi^{a_1}, \ldots, \xi^{a_k}) = 0$, then either $\xi$ is a root of unity or there exists a non-zero vector $\mathfrak{v} \in \mathbb{Z}^k$ having length at most $c_1$ and orthogonal to $\mathfrak{a}$.

**Issues to Deal With:**

- Bomberi & Zannier’s work requires relatively prime multivariate polynomials.

- Divide by $\gcd(F_1^{(2)}, F_2^{(2)})$.

  Keep track of the $c_1$'s. They are part of $\gcd(f(x), g(x))$.

- **Issues to Deal With:**
  - Bomberi & Zannier’s work requires relatively prime multivariate polynomials.
  - Keep track of the $c_1$'s. They are part of $\gcd(f(x), g(x))$.

- **Issues to Deal With:**
  - Bomberi & Zannier’s work requires relatively prime multivariate polynomials.
  - Some variables may be missing.

- **Issues to Deal With:**
  - Bomberi & Zannier’s work requires relatively prime multivariate polynomials.
  - Some variables may be missing.

- **Issues to Deal With:**
  - Bomberi & Zannier’s work requires relatively prime multivariate polynomials.
  - Some variables may be missing.

- **Issues to Deal With:**
  - Bomberi & Zannier’s work requires relatively prime multivariate polynomials.
  - Some variables may be missing.