Factoring Sparse Polynomials

Theorem 1 (Schinzel): Let r be a positive integer, and fix non-zero integers $a_0, \ldots, a_r$. Let

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

Then there exist finite sets S and T of matrices satisfying:

Theorem 1 (Schinzel): Let r be a positive integer, and fix non-zero integers $a_0, \dots, a_r$. Let

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

Then there exist finite sets S and T of matrices satisfying:

(i) Each matrix in S or T is an $r \times \rho$ matrix with integer entries and of rank ρ for some $\rho \leq r$.

Theorem 1 (Schinzel): Let r be a positive integer, and fix non-zero integers $a_0, \ldots, a_r$. Let

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

Then there exist finite sets S and T of matrices satisfying:

(i) Each matrix in S or T is an $r \times \rho$ matrix with integer entries and of rank ρ for some $\rho \leq r$.

(ii) The matrices in S and T are computable.

(iii) For every set of positive integers $\boldsymbol{d_1, \ldots, d_r}$ with $\boldsymbol{d_1 < d_2 < \cdots < d_r}$, the non-reciprocal part of $\boldsymbol{F(x^{d_1}, \ldots, x^{d_r})}$ is reducible if and only if there is an $\boldsymbol{r \times \rho}$ matrix $\boldsymbol{N}$ in $\boldsymbol{S}$ and integers $\boldsymbol{v_1, \ldots, v_\rho}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

but there is no $\boldsymbol{r \times \rho'}$ matrix $\boldsymbol{M}$ in $\boldsymbol{T}$ with $\boldsymbol{\rho' < \rho}$ and no integers $\boldsymbol{v'_1, \ldots, v'_{\rho'}}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}.$$

the non-reciprocal part of $\boldsymbol{F}(\boldsymbol{x}^{\boldsymbol{d}_1}, \ldots, \boldsymbol{x}^{\boldsymbol{d}_r})$ is reducible the non-reciprocal part of $F(x^{d_1}, \ldots, x^{d_r})$ is reducible

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

the non-reciprocal part of $F(x^{d_1}, \dots, x^{d_r})$ is reducible

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

$$F(x^{d_1}, \dots, x^{d_r}) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0$$

Theorem 2 (Schinzel): Let r be a positive integer, and fix non-zero integers $a_0, \ldots, a_r$. Let

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

Then there exist finite sets S and T of matrices satisfying:

Theorem 2 (Schinzel): Let r be a positive integer, and fix non-zero integers $a_0, \ldots, a_r$. Let

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

Then there exist finite sets S and T of matrices satisfying:

(i) Each matrix in S or T is an $r \times \rho$ matrix with integer entries and of rank ρ for some $\rho \leq r$.

Theorem 2 (Schinzel): Let r be a positive integer, and fix non-zero integers $a_0, \ldots, a_r$. Let

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

Then there exist finite sets S and T of matrices satisfying:

(i) Each matrix in S or T is an $r \times \rho$ matrix with integer entries and of rank ρ for some $\rho \leq r$.

(ii) The matrices in S and T are computable.

(iii) For every set of positive integers $d_1, \ldots, d_r$ with $F(x^{d_1}, \ldots, x^{d_r})$ not reciprocal and $d_1 < d_2 < \cdots < d_r$, the *non-cyclotomic* part of $F(x^{d_1}, \ldots, x^{d_r})$ is reducible if and only if there is an $r \times \rho$ matrix N in S and integers $v_1, \ldots, v_\rho$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

but there is no $r \times \rho'$ matrix M in T with $\rho' < \rho$ and no integers $v'_1, \ldots, v'_{\rho'}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}.$$

(iii) For every set of positive integers $d_1, \dots, d_r$ with $F(x^{d_1}, \dots, x^{d_r})$ not reciprocal and $d_1 < d_2 < \cdots < d_r$, the *non-cyclotomic* part of $F(x^{d_1}, \dots, x^{d_r})$ is reducible if and only if there is an $r \times \rho$ matrix N in S and integers $v_1, \dots, v_\rho$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

but there is no $r \times \rho'$ matrix M in T with $\rho' < \rho$ and no integers $v'_1, \dots, v'_{\rho'}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}.$$

(iii) For every set of positive integers $d_1, \ldots, d_r$ with $F(x^{d_1}, \ldots, x^{d_r})$ not reciprocal and $d_1 < d_2 < \cdots < d_r$, the *non-cyclotomic* part of $F(x^{d_1}, \ldots, x^{d_r})$ is reducible if and only if there is an $r \times \rho$ matrix N in S and integers $v_1, \ldots, v_\rho$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

but there is no $r \times \rho'$ matrix M in T with $\rho' < \rho$ and no integers $v'_1, \ldots, v'_{\rho'}$ satisfying

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}.$$

Theorem: There is an algorithm with the following property: Given a non-reciprocal $f(x) \in \mathbb{Z}[x]$ with N non-zero terms, degree n and height H, the algorithm determines whether $f(x)$ is irreducible in time

$$c(N,H)(\log n)^{c'(N)}$$

where $c(N,H)$ depends only on N and H and $c'(N)$ depends only on N.

Theorem: There is an algorithm with the following property: Given a *non-reciprocal* $f(x) \in \mathbb{Z}[x]$ with N non-zero terms, degree n and height H, the algorithm determines whether $f(x)$ is irreducible in time

$$c(N, H)(\log n)^{c'(N)}$$

where $c(N, H)$ depends only on N and H and $c'(N)$ depends only on N.

Proof. Let

$$f(x) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Proof. Let

$$f(x) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Consider

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

so that

$$F(x^{d_1}, \ldots, x^{d_r}) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Proof. Let

$$f(x) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Consider

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

so that

$$F(x^{d_1}, \ldots, x^{d_r}) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Begin the algorithm by constructing the finite sets S and T of matrices in Schinzel's Theorem 2.

Proof. Let

$$f(x) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Consider

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

so that

$$F(x^{d_1}, \ldots, x^{d_r}) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Begin the algorithm by constructing the finite sets S and T of matrices in Schinzel's Theorem 2. Observe that S and T depend on F and not on the $d_1, \ldots, d_r$.

Proof. Let

$$f(x) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Consider

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

so that

$$F(x^{d_1}, \ldots, x^{d_r}) = a_r x^{d_r} + \cdots + a_1 x^{d_1} + a_0.$$

Begin the algorithm by constructing the finite sets S and T of matrices in Schinzel's Theorem 2. Observe that S and T depend on F and not on the $d_1, \ldots, d_r$, so this takes running time $\leq c_1(N, H)$.

Next, the algorithm checks each matrix $\boldsymbol{N}$ in $\boldsymbol{S}$ to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

for some integers $v_1, \ldots, v_\rho$.

Next, the algorithm checks each matrix N in S to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

for some integers $v_1, \ldots, v_\rho$. In other words, $v_1, \ldots, v_\rho$ are unknowns and elementary row operations are done to solve the above system of equations.

Next, the algorithm checks each matrix $\boldsymbol{N}$ in $\boldsymbol{S}$ to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

for some integers $v_1, \ldots, v_\rho$. In other words, $v_1, \ldots, v_\rho$ are unknowns and elementary row operations are done to solve the above system of equations. The rank of $\boldsymbol{N}$ is $\boldsymbol{\rho}$, so if a solution exists, then it is unique.

Next, the algorithm checks each matrix $\boldsymbol{N}$ in $\boldsymbol{S}$ to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

for some integers $v_1, \ldots, v_\rho$. In other words, $v_1, \ldots, v_\rho$ are unknowns and elementary row operations are done to solve the above system of equations. The rank of N is ρ, so if a solution exists, then it is unique. This involves performing elementary operations ($+$, $-$, $\times$, and $\div$) with entries in N and the d_j (which are $\leq n$).

Next, the algorithm checks each matrix N in S to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = N \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_\rho \end{pmatrix}$$

for some integers $v_1, \ldots, v_\rho$. In other words, $v_1, \ldots, v_\rho$ are unknowns and elementary row operations are done to solve the above system of equations. The rank of N is ρ, so if a solution exists, then it is unique. This involves performing elementary operations ($+$, $-$, $\times$, and $\div$) with entries in N and the d_j (which are $\leq n$). The running time here is $\leq c_2(N, H) \log^2 n$.

Next, the algorithm checks each matrix $\boldsymbol{M}$ in $\boldsymbol{T}$ to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}$$

for some integers $v'_1, \ldots, v'_{\rho'}$ by using elementary row operations to solve the system of equations for the v'_j.

Next, the algorithm checks each matrix $\boldsymbol{M}$ in $\boldsymbol{T}$ to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}$$

for some integers $v'_1, \ldots, v'_{\rho'}$ by using elementary row operations to solve the system of equations for the v'_j. The rank of M is ρ', so if a solution exists, then it is unique.

Next, the algorithm checks each matrix M in T to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}$$

for some integers $v'_1, \ldots, v'_{\rho'}$ by using elementary row operations to solve the system of equations for the v'_j. The rank of M is ρ', so if a solution exists, then it is unique. This involves performing elementary operations ($+$, $-$, $\times$, and $\div$) with entries in M and the d_j (which are $\leq n$).

Next, the algorithm checks each matrix M in T to see if

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_r \end{pmatrix} = M \begin{pmatrix} v'_1 \\ v'_2 \\ \vdots \\ v'_{\rho'} \end{pmatrix}$$

for some integers $v'_1, \ldots, v'_{\rho'}$ by using elementary row operations to solve the system of equations for the v'_j. The rank of M is ρ', so if a solution exists, then it is unique. This involves performing elementary operations ($+$, $-$, $\times$, and $\div$) with entries in M and the d_j (which are $\leq n$). The running time is again $\leq c_2(N, H) \log^2 n$.

Schinzel's Theorem 2 now indicates to us whether $f(x)$ has a reducible non-cyclotomic part.

Schinzel's Theorem 2 now indicates to us whether $f(x)$ has a reducible non-cyclotomic part. If so, then we output that $f(x)$ is reducible. If not, we have more work to do.

Recall, we had the following theorem.

Theorem: 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 $\deg f = n$, the algorithm determines whether $f(x)$ has a cyclotomic factor and with running time

$$\ll \exp\left((2 + o(1))\sqrt{N/\log N}(\log N + \log\log n)\right) \times \log(H + 1)$$

as N tends to infinity, where $H = \max_{1 \le j \le N}\{|a_j|\}$.

Recall, we had the following theorem.

Theorem: 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 $\deg f = n$, the algorithm determines whether $f(x)$ has a cyclotomic factor and with running time

$$\ll \exp\Big((2+o(1))\sqrt{N/\log N}(\log N + \log\log n)\Big) \times \log(H+1)$$

as N tends to infinity, where $H = \max_{1 \le j \le N}\{|a_j|\}$.

We'll come back to this.

$$\exp\left((2+o(1))\sqrt{N/\log N}(\log N+\log\log n)\right)\\ \times\log(H+1)$$

$$\exp\left((2+o(1))\sqrt{N/\log N}(\log N+\log\log n)\right)$$
$$\times\log(H+1)$$

split into two parts

$$\exp\left((2+o(1))\sqrt{N/\log N}(\log N)\right)\times\log(H+1)$$
$$\exp\left((2+o(1))\sqrt{N/\log N}\,(\log\log n)\right)$$

$$\exp\left((2+o(1))\sqrt{N/\log N}(\log N+\log\log n)\right)$$
$$\times\log(H+1)$$

split into two parts

$$c_3(N,H)$$
$$\exp\left((2+o(1))\sqrt{N/\log N}\,(\log\log n)\right)$$

$$\exp\left((2+o(1))\sqrt{N/\log N}(\log N + \log\log n)\right) \times \log(H+1)$$

split into two parts

$$c_3(N, H)$$

$$(\log n)^{c_4(N)}$$

Theorem: 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 $\deg f = n$, the algorithm determines whether $f(x)$ has a cyclotomic factor and with running time

$$\le c_3(N, H)(\log n)^{c_4(N)}$$

as N tends to infinity, where $H = \max_{1 \le j \le N}\{|a_j|\}$.

Theorem: 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 $\deg f = n$, the algorithm determines whether $f(x)$ has a cyclotomic factor and with running time

$$\le c_3(N, H)(\log n)^{c_4(N)}$$

as N tends to infinity, where $H = \max_{1 \le j \le N}\{|a_j|\}$.

Algorithm Continued: If the non-cyclotomic part of $f(x)$ is irreducible, then use the algorithm in the above theorem.

Theorem: 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 $\deg f = n$, the algorithm determines whether $f(x)$ has a cyclotomic factor and with running time

$$\le c_3(N, H)(\log n)^{c_4(N)}$$

as N tends to infinity, where $H = \max_{1 \le j \le N}\{|a_j|\}$.

Algorithm Continued: If the non-cyclotomic part of $f(x)$ is irreducible, then use the algorithm in the above theorem. This completes the proof of the theorem. ■

A Curious Connection with the Odd Covering Problem

Coverings of the Integers:

A *covering of the integers* is a system of congruences

$$x \equiv a_j \pmod{m_j}$$

having the property that every integer satisfies at least one of the congruences.

Coverings of the Integers:

A *covering of the integers* is a system of congruences

$$x \equiv a_j \pmod{m_j}$$

having the property that every integer satisfies at least one of the congruences.

Example 1:

$$x \equiv 0 \pmod{2}$$
$$x \equiv 1 \pmod{2}$$

Example 2:

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 1 \pmod{4} \\ x &\equiv 1 \pmod{6} \\ x &\equiv 3 \pmod{12} \end{aligned}$$

Example 2:

$$
\begin{aligned}
x &\equiv 0 \pmod{2}\\
x &\equiv 2 \pmod{3}\\
x &\equiv 1 \pmod{4}\\
x &\equiv 1 \pmod{6}\\
x &\equiv 3 \pmod{12}
\end{aligned}
$$

0	1	2	3	4	5	6	7	8	9	10	11

Open Problem:

Does there exist an "odd covering" of the integers, a covering consisting of distinct odd moduli > 1?

Open Problem:

Does there exist an "odd covering" of the integers, a covering consisting of distinct odd moduli > 1?

Erdős: \$25 (for proof none exists)

Open Problem:

Does there exist an "odd covering" of the integers, a covering consisting of distinct odd moduli > 1?

Erdős: \$25 (for proof none exists)

Selfridge: \$2000 (for explicit example)

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers $\boldsymbol{k}$ such that $\boldsymbol{k \times 2^n + 1}$ is composite for all non-negative integers $\boldsymbol{n}$.

Selfridge's Example: $\boldsymbol{k = 78557}$

(smallest odd known)

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$

(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(x)x^n + 1$ is reducible for all non-negative integers n?

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$
(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(x)x^n + 1$ is reducible for all non-negative integers n?

Require: $f(1) \neq -1$

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$
(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -1$ and $f(x)x^n + 1$ is reducible for all non-negative integers n?

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers $\boldsymbol{k}$ such that $\boldsymbol{k \times 2^n + 1}$ is composite for all non-negative integers $\boldsymbol{n}$.

Selfridge's Example: $\boldsymbol{k = 78557}$
(smallest odd known)

Polynomial Question: Does there exist $\boldsymbol{f(x) \in \mathbb{Z}[x]}$ such that $\boldsymbol{f(1) \neq -1}$ and $\boldsymbol{f(x)x^n + 1}$ is reducible for all non-negative integers $\boldsymbol{n}$?

Answer: Nobody knows.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

$$n \equiv 0 \pmod 2 \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

$$n \equiv 0 \pmod{2} \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$
$$n \equiv 2 \pmod{3} \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2, 3, 4, 6, 12\}.$$

$$n \equiv 0 \pmod{2} \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$
$$n \equiv 2 \pmod{3} \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$$
$$n \equiv 1 \pmod{4} \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

$$n \equiv 0 \pmod{2} \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$
$$n \equiv 2 \pmod{3} \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$$
$$n \equiv 1 \pmod{4} \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1}$$
$$n \equiv 1 \pmod{6} \implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

$$\begin{aligned}
n \equiv 0 \pmod 2 &\implies f(x)x^n + 12 \equiv 0 \pmod{x+1} \\
n \equiv 2 \pmod 3 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1} \\
n \equiv 1 \pmod 4 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1} \\
n \equiv 1 \pmod 6 &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1} \\
n \equiv 3 \pmod{12} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^4-x^2+1}
\end{aligned}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n+4$ is reducible for all non-negative integers n.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Comment: For each n, the first polynomial is divisible by at least one $\Phi_k(x)$ where k divides 12.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Comment: For each n, the second polynomial is divisible by at least one $\Phi_k(x)$ where k divides some integer N having more than 10^{17} digits.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n+4$ is reducible for all non-negative integers n.

Comment: For each n, the second polynomial is divisible by at least one $\Phi_k(x)$ where k divides

$$2^{436750334086348800}3^{41}5^{31}7^{37}11^{29}13^{23}17^{16}19^{18}23^{23}29^{29}31^{31}37^{37}41^{41}.$$

Schinzel's Theorem: If there is an $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -1$ and $f(x)x^n + 1$ is reducible for all non-negative integers n, then there is an odd covering of the integers.

Turán's Conjecture

Conjecture: There is an absolute constant C such that if

$$f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x],$$

then there is a

$$g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{Z}[x]$$

irreducible (over $\mathbb{Q}$) such that $\sum_{j=0}^{r} |b_j - a_j| \le C$.

Conjecture: There is an absolute constant C such that if

$$f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x],$$

then there is a

$$g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{Z}[x]$$

irreducible (over $\mathbb{Q}$) such that $\displaystyle\sum_{j=0}^{r} |b_j - a_j| \le C.$

Comment: The conjecture remains open. If we take $g(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$ where possibly $s > r$, then the problem has been resolved by Schinzel.

First Attack on Turán's Problem:

Old Theorem: When m is large, either $u(x)x^m + v(x)$ has an obvious factorization or the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible.

First Attack on Turán's Problem:

Old Theorem: When m is large, either $u(x)x^m + v(x)$ has an obvious factorization or the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible.

Idea: Consider

$$g(x) = x^n + f(x).$$

If one can show $g(x)$ is irreducible for some n, then the conjecture of Turán (modified so $\deg g > \deg f$ is allowed) is resolved with $C = 1$.

First Attack on Turán's Problem:

Old Theorem: When m is large, either $u(x)x^m + v(x)$ has an obvious factorization or the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible.

Idea: Consider

$$g(x) = x^n + f(x).$$

If $f(0) = 0$ or $f(1) = -1$, then consider instead

$$g(x) = x^n + f(x) \pm 1.$$

If one can show $g(x)$ is irreducible for some n, then the conjecture of Turán (modified so $\deg g > \deg f$ is allowed) is resolved with $C = 2$.

First Attack on Turán's Problem:

Idea: Consider

$$g(x) = x^n + f(x).$$

If $f(0) = 0$ or $f(1) = -1$, then consider instead

$$g(x) = x^n + f(x) \pm 1.$$

If one can show $g(x)$ is irreducible for some n, then the conjecture of Turán (modified so $\deg g > \deg f$ is allowed) is resolved with $C = 2$.

First Attack on Turán's Problem:

Idea: Consider

$$g(x) = x^n + f(x).$$

If $f(0) = 0$ or $f(1) = -1$, then consider instead

$$g(x) = x^n + f(x) \pm 1.$$

If one can show $g(x)$ is irreducible for some n, then the conjecture of Turán (modified so $\deg g > \deg f$ is allowed) is resolved with $C = 2$.

Problem: Dealing with $g(x) = x^n + f(x)$ is essentially equivalent to the odd covering problem. So this is hard.

Second Attack on Turán's Problem:

Idea: Consider

$$g(x) = x^m \pm x^n + f(x).$$

If $f(0) = 0$, then consider instead

$$g(x) = x^m \pm x^n + f(x) \pm 1.$$

Theorem (Schinzel): For every

$$f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x],$$

there exist infinitely many irreducible

$$g(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$$

such that

$$\sum_{j=0}^{\max\{r,s\}} |a_j - b_j| \le \begin{cases} 2 & \text{if } f(0) \ne 0 \\ 3 & \text{always.} \end{cases}$$

Theorem (Schinzel): For every

$$f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x],$$

there exist infinitely many irreducible

$$g(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$$

such that

$$\sum_{j=0}^{\max\{r,s\}} |a_j - b_j| \le \begin{cases} 2 & \text{if } f(0) \neq 0 \\ 3 & \text{always.} \end{cases}$$

One of these is such that

$$s < \exp\big((5r+7)(\|f\|^2+3)\big).$$

Ideas Behind Proof:

Ideas Behind Proof:

- Consider $F(x) = x^m + x^n + f(x)$ with $m \in (M, 2M]$ and $n \in (N, 2N]$ where M and N are large and $M > N$.

Ideas Behind Proof:

- Consider $F(x) = x^m + x^n + f(x)$ with $m \in (M, 2M]$ and $n \in (N, 2N]$ where M and N are large and $M > N$.
- Apply result on $u(x)x^m + v(x)$ with $u(x) = 1$ and $v(x) = x^n + f(x)$ to reduce problem to consideration of reciprocal factors.

Ideas Behind Proof:

- Consider $F(x) = x^m + x^n + f(x)$ with $m \in (M, 2M]$ and $n \in (N, 2N]$ where M and N are large and $M > N$.
- Apply result on $u(x)x^m + v(x)$ with $u(x) = 1$ and $v(x) = x^n + f(x)$ to reduce problem to consideration of reciprocal factors.
- Find a bound on the number of $x^m + x^n + f(x)$ with reciprocal non-cyclotomic factors.

Ideas Behind Proof:

- To bound the $x^m + x^n + f(x)$ with cyclotomic factors, set

  $$\mathcal{A} = \{(m,n) : M < m \le 2M, N < n \le 2N\},$$

  and let $\mathcal{A}_p \subset A$ (arising from when $F(\zeta_{p^k}) = 0$). Use a "sieve" argument to estimate the size of

  $$\mathcal{A} - \bigcup \mathcal{A}_p.$$

Ideas Behind Proof:

- To bound the $x^m + x^n + f(x)$ with cyclotomic factors, set

  $$\mathcal{A} = \{(m,n) : M < m \le 2M, N < n \le 2N\},$$

  and let $\mathcal{A}_p \subset \mathcal{A}$ (arising from when $F(\zeta_{p^k}) = 0$). Use a "sieve" argument to estimate the size of

  $$\mathcal{A} - \bigcup \mathcal{A}_p.$$

- Deduce that some $F(x) = x^m + x^n + f(x)$ with $m \in (M, 2M]$ and $n \in (N, 2N]$ is irreducible (where M and N are large and $M > N$).

Current Knowledge:

Theorem: Given $f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x]$, there are infinitely many irreducible $g(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$ such that

$$\sum_{j=0}^{\max\{r,s\}} |a_j - b_j| \le 5.$$

One of these is such that

$$s \le 4r \exp\left(4\|f\|^2 + 12\right).$$

Current Knowledge:

Theorem: Given $f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x]$, there are infinitely many irreducible $g(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$ such that

$$\sum_{j=0}^{\max\{r,s\}} |a_j - b_j| \le 5.$$

One of these is such that

$$s \le 4r \exp\left(4\|f\|^2 + 12\right).$$

Current Knowledge:

Theorem: Given $f(x) = \sum_{j=0}^{r} a_j x^j \in \mathbb{Z}[x]$, there are infinitely many irreducible $g(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$ such that

$$\sum_{j=0}^{\max\{r,s\}} |a_j - b_j| \le 3.$$

One of these is such that

$$s \le \text{some polynomial in } r.$$