On a Problem of Turán

by

Michael Filaseta

University of South Carolina

Columbia, SC 29208

filaseta@math.sc.edu

http://www.math.sc.edu/~filaseta/

<u>Turán's Problem</u> (1960's)

Show that there is a C such that if

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

then there is an irreducible

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

such that

$$\sum_{j=0}^{r} |b_j - a_j| \le C.$$

Comment: The problem 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.

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 such congruence.

Example 1:

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

Example 2:

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

Open Problem:

Does there exist an "odd covering" of the integers, a finite 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.

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

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

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

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 Theorem 1: 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.

Equivalently, if there is an $f(x) \in \mathbb{Z}[x]$ such that $f(0) \neq 0$, $f(1) \neq -1$, and $x^n + f(x)$ is reducible for all non-negative integers n, then there is an odd covering of the integers.

First Attack on Turán's Problem

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 Turán's problem (modified so $\deg g > \deg f$ is allowed) is resolved with $C = 2$.

Comment: Schinzel's Theorem 1 implies that this is probably not easy. One would have to resolve the odd covering problem first.

Second Attack on Turán's Problem

Consider

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

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

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

Schinzel's Theorem 2: 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

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

One of these is such that

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

where

$$\|f\|^2 = \sum_{j=0}^{r} a_j^2.$$

Comment: Schinzel obtained a more general result concerning the irreducibility of polynomials of the form
$$Ax^m + Bx^n + f(x),$$
where A and B are non-zero integers. If $f(0) \neq 0$ and $f(1) \neq -A - B$, then he shows there are m and n for which this polynomial is irreducible and

$$n < m < \exp\big((5r+2\log|AB|+7)(\|f\|^2+A^2+B^2)\big).$$

Question: Can the upper bound on m be improved to a bound which is less than exponential in r, the degree of $f(x)$?

Notation:

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

$f(x)$ *reciprocal* means $\tilde{f}(x) = \pm f(x)$

the *non-reciprocal part of* $f(x)$ is $f(x)$ removed of its irreducible reciprocal factors (sort of)

Theorem (F., Ford, Konyagin). Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$ with

$$u(0) \neq 0, \; v(0) \neq 0, \; \text{and} \quad \gcd(u(x), v(x)) = 1.$$

Let r_1 and r_2 denote the number of non-zero terms in $u(x)$ and $v(x)$, respectively. If

$$m \geq \max \left\{ 2 \times 5^{2N-1}, 2 \max \{ \deg u, \deg v \} \left(5^{N-1} + \frac{1}{4} \right) \right\}$$

where

$$N = 2 \|u\|^2 + 2 \|v\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible unless one of the following holds:

(i) The polynomial $-u(x)v(x)$ is a pth power for some prime p dividing m.

(ii) One of $\pm u(x)$ or $\pm v(x)$ is a 4th power, the other is 4 times a 4th power, and $4|m$.

Theorem (F., Ford, Konyagin). The non-reciprocal part of $u(x)x^m + v(x)$ is irreducible unless ....

Comment: Schinzel had a similar result with a weaker lower bound on m. But simply improving this lower bound does not give us directly what we want.

Set-Up for Turán's Problem: Take

$$u(x) = A \quad \text{and} \quad v(x) = Bx^n + f(x)$$

to deduce something about the irreducibility of the non-reciprocal part of

$$Ax^m + Bx^n + f(x).$$

Main Difficulty: How does one show that such polynomials usually do not have reciprocal factors?

$$Ax^m + Bx^n + f(x)$$

$$M < m \le 2M \quad \text{and} \quad N < n \le 2N$$

Idea: Show that if M and N are large enough, then there are many polynomials of this form without irreducible reciprocal factors.

Case I: Reciprocal non-cyclotomic polynomials

Case II: Cyclotomic polynomials

$$G(x) = Ax^m + Bx^n + f(x)$$

$$M < m \le 2M \quad \text{and} \quad N < n \le 2N$$

Case I: Reciprocal non-cyclotomic polynomials

- For fixed $n \in (N, 2N]$ and a fixed reciprocal non-cyclotomic irreducible polynomial $g(x)$, there is at most 1 value of m for which $g(x)$ divides $G(x)$.
- For fixed $n \in (N, 2N]$, there are $\le 4N$ reciprocal non-cyclotomic irreducible polynomials $g(x)$ dividing a polynomial of the form $G(x)$.
- There are $\ll N^2$ pairs (m, n) for which $G(x)$ is divisible by a reciprocal non-cyclotomic irreducible polynomial.

$$G(x) = Ax^m + Bx^n + f(x) = Ax^m + v(x)$$

- For fixed $n \in (N, 2N]$, there are $\leq 2N$ reciprocal non-cyclotomic irreducible polynomials $g(x)$ dividing a polynomial of the form $G(x)$.

Any such $g(x)$ must divide

$$x^{\deg v} v(1/x) G(x) - A x^{m+\deg v} G(1/x)$$
$$= x^{\deg v} v(1/x) v(x) - A^2 x^{\deg v}$$

a polynomial of degree $2 \deg v \leq 4N$ that does not depend on m.

$$G(x) = Ax^m + Bx^n + f(x) = Ax^m + v(x)$$

$$M < m \le 2M \quad \text{and} \quad N < n \le 2N$$

Case II: Cyclotomic polynomials

- Similar to the previous case, each cyclotomic polynomial must divide

$$x^{\deg v} v(1/x) v(x) - A^2 x^{\deg v},$$

  a polynomial of degree $2 \deg v \le 4N$. Hence, if $\Phi_\ell(x) | G(x)$, then $\phi(\ell) \le 4N$.

- One can show that if $\Phi_\ell(x)$ divides a polynomial $G(x)$ for some ℓ, then there is such an ℓ all of whose prime divisors are no more than the number of non-zero terms of $G(x)$. Hence, we may suppose that if $p|\ell$, then $p \le N$.

$$G(x) = Ax^m + Bx^n + f(x)$$

$$M < m \le 2M \quad \text{and} \quad N < n \le 2N$$

Idea: Count pairs (m, n) such that $\Phi_\ell(x) | G(x)$ for some

$$\ell \in \mathcal{L} = \{\ell : \ell \ge 2, \phi(\ell) \le 4N, p|\ell \implies p \le N\}.$$

Want: There are $< MN$ such pairs.

Comment: Schinzel considers 4 cases:

(i) $B \ne \pm A, \pm 2A, \pm(1/2)A,$

(ii) $B = \pm 2A, \pm(1/2)A$

(iii) $B = -A$

(iv) $B = A$

$$G(x) = Ax^m + Bx^n + f(x)$$

$$M < m \leq 2M \quad \text{and} \quad N < n \leq 2N$$

$$\mathcal{L} = \{\ell : \ell \geq 2, \phi(\ell) \leq 4N, p|\ell \implies p \leq N\}$$

Case (i): $B \neq \pm A, \pm 2A, \pm(1/2)A$

- Schinzel showed that if one fixes $\ell \in \mathcal{L}$ and considers two intervals $I \subseteq (M, 2M]$ and $J \subseteq (N, 2N]$ with $|I| = |J| = \ell$, then the number of pairs $(m, n) \in I \times J$ for which $G(\zeta_\ell) = 0$ is bounded by 1.

$$G(x) = Ax^m + Bx^n + f(x)$$

$$M < m \leq 2M \quad \text{and} \quad N < n \leq 2N$$

$$\mathcal{L} = \{\ell : \ell \geq 2, \phi(\ell) \leq 4N, p|\ell \implies p \leq N\}$$

Case (i): $B \neq \pm A, \pm 2A, \pm(1/2)A$

Therefore, it follows that the number of "bad" pairs (m, n) is bounded by

$$\begin{aligned}
\sum_{\ell \in \mathcal{L}} \Big(\frac{M}{\ell} + 1\Big)\Big(\frac{N}{\ell} + 1\Big) \\
&\leq \sum_{\ell \in \mathcal{L}} \frac{MN}{\ell^2} + 3 \sum_{\ell \in \mathcal{L}} \frac{M}{\ell} \\
&\leq \Big(\frac{\pi^2}{6} - 1\Big) MN + 4M \log N \\
&\leq \frac{2}{3} MN.
\end{aligned}$$

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

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

Comment: The above is a consequence of Case (i). If one considers the other cases combined with a variation on sieves, then one can replace the bound "5" with "3" provided the bound on s is weakened but still made to depend polynomially on r.