From Covering Problems to a Conjecture of Turán

by

Michael Filaseta
University of South Carolina
Columbia, SC 29208

filaseta@math.sc.edu

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

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:

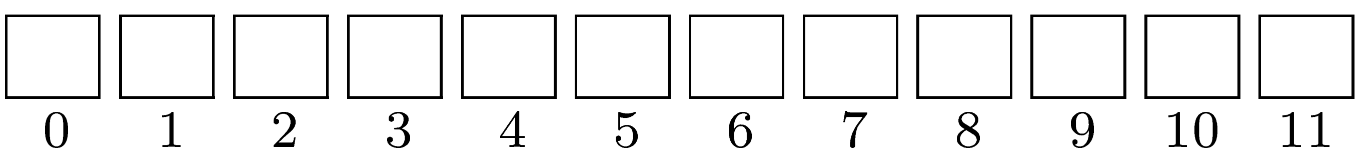
$$x \equiv 0 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 1 \pmod{4}$$

$$x \equiv 1 \pmod{6}$$

$$x \equiv 3 \pmod{12}$$



Open Problem:

In a finite covering with distinct moduli, can the minimum modulus be arbitrarily large?

Choi: minimum modulus can be 20

Erdős: $500 for solution

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)

Applications of Coverings

Sierpinski: 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)
(but 19 to go)

Polignac's Problem: Is it true that if k is an odd integer > 1, then there is an integer n and a prime p such that $k = 2^n + p$? What if k is sufficiently large?

Examples: 127 and 905

Erdős: No, arbitrarily large odd k without this property exist.

Schinzel: These applications of Sierpinski and Erdős are in some sense equivalent.

Related Polynomial Problems

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: $f(1) \neq -1$

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

Question 2: Does there exist a polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(0) \neq 0$, $f(1) \neq -1$, and $x^n + f(x)$ is reducible for all non-negative integers n?

Comment: These questions remain open.

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 (Schinzel): 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.

Comment 1: An analogous result holds for the second polynomial question.

Comment 2: The result holds with any odd constant term.

Comment 3: Examples of reducibility exist with constant term any multiple of 4.

Basic Ideas

- The polynomial $f(x)x^n + 1$ can have trivial factorizations. For example,

$$(x+1)^3 x^6 + 1 \quad \text{factors}$$

  and

$$4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1).$$

- For n large, we shouldn't expect much else.

- The previous remark becomes stupid if we consider cyclotomic factors. For example,

$$(x+1)x^7 + 1 \quad \text{factors.}$$

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 one of

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

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

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

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

Comment: Schinzel essentially proved this with a different understanding of what "m is large" means.

Theorem (Schinzel): 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.

Idea of Proof: Take $u(x) = f(x)$ and $v(x) = 1$ and do some more things.

(see `http://www.math.sc.edu/~filaseta/seminars/`)

(first four seminars this year)

Turán's Problem (1960's)

Problem: 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 a

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

irreducible (over $\mathbb{Q}$) such that

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

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.

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

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

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

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

One of these is such that

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

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 $f(x)$?

Ideas Behind Improvement

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

- Apply FFK result with $u(x) = A$ and $v(x) = Bx^n + f(x)$ to reduce problem to consideration of cyclotomic factors.

- Let

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

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

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

Conclusion

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: One can replace the bound "5" with "3" provided the bound on s is weakened but still made to depend polynomially on r.