On an Irreducibility Theorem of A. Schinzel Associated with Coverings of the Integers

by

Michael Filaseta
University of South Carolina

Kevin Ford
University of South Carolina

Sergei Konyagin
Moscow State University
(visiting University of South Carolina)

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: 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.

Key Idea: Investigate non-cyclotomic factors of $f(x)x^n + 1$, and show that typically the non-cyclotomic part of $f(x)x^n + 1$ is irreducible.

Key Idea: Investigate non-cyclotomic factors of $f(x)x^n + 1$, and show that typically the non-cyclotomic part of $f(x)x^n + 1$ is irreducible.

Observation: One gets a non-trivial factorization of $f(x)x^n + 1$ when one of the following holds:

(i) $f(x)$ is minus a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$.

Note: $4x^4+1 = (2x^2+2x+1)(2x^2-2x+1)$

Schinzel: For fixed $f(x) \in \mathbb{Z}[x]$ and n sufficiently large, the non-cyclotomic part of $f(x)x^n + 1$ is irreducible unless (i) or (ii) holds.

Schinzel: For fixed $f(x) \in \mathbb{Z}[x]$ and n sufficiently large, the non-cyclotomic part of $f(x)x^n + 1$ is irreducible unless one of the following holds:

(i) $f(x)$ is minus a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$.

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

In fact, for each n, the above polynomial is divisible by one of

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

Notation:

irreducibility will be over the integers

if $f(x) = \sum_{j=0}^{n} a_j x^j$, then $\|f\| = \sqrt{\sum_{j=0}^{n} a_j^2}$

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

$\tilde{f}(x)$ will be called the *reciprocal of* $f(x)$

$f(x)$ *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)

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

$\tilde{f}(x)$ will be called the *reciprocal of* $f(x)$

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

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

Comment: Given $f(x) \in \mathbb{Z}[x]$, if n is sufficiently large and $f(x)x^n + 1$ is divisible by an irreducible reciprocal polynomial $g(x)$, then $g(x)$ is cyclotomic.

Therefore, for n large, the non-cyclotomic part of $f(x)x^n + 1$ and non-reciprocal part of $f(x)x^n + 1$ are the same.

Schinzel: For fixed $f(x) \in \mathbb{Z}[x]$ and n sufficiently large, the non-reciprocal part of $f(x)x^n + 1$ is irreducible unless one of the following holds:

(i) $f(x)$ is minus a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$.

Forget Everything Said Except Note:

We want to say something about when the non-reciprocal part of $f(x)x^n + 1$ is irreducible.

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

$$f(0) \neq 0, \ g(0) \neq 0, \ \text{and} \ \ \gcd(f(x), g(x)) = 1.$$

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

$$n \geq \max\left\{2 \times 5^{2N-1}, 2\max\left\{\deg f, \deg g\right\}\left(5^{N-1} + \frac{1}{4}\right)\right\}$$

where

$$N = 2\,\|f\|^2 + 2\,\|g\|^2 + 2r_1 + 2r_2 - 7,$$

then the non-reciprocal part of $f(x)x^n + g(x)$ is irreducible unless one of the following holds:

(i) The polynomial $-f(x)g(x)$ is a pth power for some prime p dividing n.

(ii) One of $\pm f(x)$ or $\pm g(x)$ is a 4th power, the other is 4 times a 4th power, and $4|n$.

Capelli's Theorem: Let F be a field. The polynomial $x^n + a \in F[x]$ is reducible if and only if either (i) a is minus a pth power in F for a prime p dividing n or (ii) a is 4 times a 4th power in F and 4 divides n.

Idea: Take $F = \mathbb{Q}(x)$. Instead of $f(x)x^n + g(x)$, consider $f(x)y^n + g(x)$ which is reducible in $Q(x)$ if and only if $y^n + f(x)/g(x)$ is. Apply Capelli's Theorem.

Problem: If $f(x)x^n + g(x)$ is reducible, then $f(x)y^n + g(x)$ may be irreducible

Want:

If the non-reciprocal part of $f(x)x^n + g(x)$ is reducible, then $f(x)y^n + g(x)$ is reducible.

Another Related Problem:

Suppose that $a_1, a_2, \ldots, a_r$ are distinct non-negative integers written in increasing order and that we wish to determine an integer $k \ge 2$ such that

$$a_j \bmod k < k/2 \quad \text{for each } j \in \{1, 2, \ldots, r\}.$$

The value $k = 2a_r + 1$ satisfies this property.

Examples of sets $S = \{a_1, \ldots, a_r\}$ for which this choice of $k \ge 2$ is minimal are given by

$$\{3, 5\} \quad \text{and} \quad \{50, 68, 125\}.$$

Fix r. Is it true that if a_r is sufficiently large, then one can always find a smaller k with this property?

Want:

If the non-reciprocal part of $f(x)x^n + g(x)$ is reducible, then $f(x)y^n+g(x)$ is reducible.

Let $F(x) = f(x)x^n + g(x)$. If the non-reciprocal part of $F(x)$ is reducible, then there are non-reciprocal $u(x)$ and $v(x)$ with

$$F(x) = u(x)v(x).$$

Consider

$$W(x) = u(x)\tilde{v}(x).$$

Then

$$F(x)\widetilde{F}(x) = u(x)v(x)\tilde{u}(x)\tilde{v}(x) = W(x)\widetilde{W}(x).$$

Compare the coefficients of $x^{\deg F}$ on the left and right. On the left it is $\|F\|^2$, and on the right it is $\|W\|^2$. Hence,

$$\|W\| = \|F\|.$$

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

$$F(x) = u(x)v(x) \quad \text{and} \quad W(x) = u(x)\tilde{v}(x)$$

$$\|W\| = \|F\|$$

Hence, the number of non-zero terms among both $F(x)$ and $W(x)$ is bounded by

$$\|f\|^2 + \|g\|^2 + r_1 + r_2,$$

which is independent of n.

Take a positive integer k (not too small and not too large) such that each exponent in F, W, $\widetilde{F}$, and $\widetilde{W}$ is $< k/2$ when reduced modulo k.

Exponents in F, W, $\widetilde{F}$, $\widetilde{W}$ mod k are $< k/2$.

$$F(x) = \sum_{j=0}^{r} a_j x^{d_j} \to G_1(x,y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j} y^{\ell_j}$$

$$\widetilde{F}(x) = \sum_{j=0}^{r} a_j x^{d_r - d_j} \to G_2(x,y) = \sum_{j=0}^{r} a_j x^{\overline{d'_j}} y^{\ell'_j}$$

$$G_1(x, x^k) = F(x) \quad \text{and} \quad G_2(x, x^k) = \widetilde{F}(x)$$

$$G_1(x,y)G_2(x,y) = \sum_{j=0}^{t} g_j(x) y^j$$

$$\deg g_j(x) < k \quad \text{for all } j$$

$$\sum_{j=0}^{t} g_j(x) x^{kj} = G_1(x,x^k)G_2(x,x^k) = F(x)\widetilde{F}(x)$$

$$W(x) = \sum_{j=0}^{s} b_j x^{e_j} \rightarrow H_1(x,y) = \sum_{j=0}^{r} a_j x^{\overline{e}_j} y^{m_j}$$

$$\widetilde{W}(x) = \sum_{j=0}^{s} b_j x^{e_r - e_j} \rightarrow H_2(x,y) = \sum_{j=0}^{s} b_j x^{\overline{e'_j}} y^{m'_j}$$

$$H_1(x, x^k) = W(x) \quad \text{and} \quad H_2(x, x^k) = \widetilde{W}(x)$$

$$H_1(x,y)H_2(x,y) = \sum_{j=0}^{t'} h_j(x) y^j$$

$$\deg h_j(x) < k \quad \text{for all } j$$

$$\sum_{j=0}^{t'} h_j(x) x^{kj} = H_1(x, x^k) H_2(x, x^k) = W(x)\widetilde{W}(x)$$

$$\sum_{j=0}^{t} g_j(x)x^{kj} = G_1(x,x^k)G_2(x,x^k) = F(x)\widetilde{F}(x)$$

$$\sum_{j=0}^{t'} h_j(x)x^{kj} = H_1(x,x^k)H_2(x,x^k) = W(x)\widetilde{W}(x)$$

$$\sum_{j=0}^{t} g_j(x)x^{kj} = \sum_{j=0}^{t'} h_j(x)x^{kj}$$

$$g_j(x) = h_j(x) \quad \text{for all } j$$

$$G_1(x,y)G_2(x,y) = \sum_{j=0}^{t} g_j(x)y^j$$

$$H_1(x,y)H_2(x,y) = \sum_{j=0}^{t'} h_j(x)y^j$$

$$G_1(x,y)G_2(x,y) = H_1(x,y)H_2(x,y)$$

$$G_1(x,y)G_2(x,y) = H_1(x,y)H_2(x,y)$$

$$G_1(x,x^k) = F(x) \quad \& \quad G_2(x,x^k) = \widetilde{F}(x)$$
$$H_1(x,x^k) = W(x) \quad \& \quad H_2(x,x^k) = \widetilde{W}(x)$$

G_1, G_2, H_1, & H_2 are pairwise distinct.

Each is reducible.

$$F(x) = \sum_{j=0}^{r} a_j x^{d_j}, \; G_1(x,y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j} y^{\ell_j}$$

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

$$G_1(x,y) = f(x)x^d y^\ell + g(x)$$

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

$$G_1(x, y) = f(x)x^d y^\ell + g(x)$$

Conclusion: If the non-reciprocal part of $f(x)x^n + g(x)$ is reducible, then

$$f(x)x^d y^\ell + g(x)$$

is reducible.

Apply Capelli's Theorem.