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

by

M. Filaseta*, K. Ford, and S. Konyagin**

1. Introduction

A covering of the integers is a system of congruences $x \equiv a_j \pmod{m_j}$, where a_j and m_j denote integers with $m_j > 0$ for each j, such that every integer satisfies at least one of the congruences. An open problem (which surfaced over 40 years ago) is to determine whether a covering of the integers exists for which the indices j range over a finite set and the m_j are distinct odd integers > 1. The problem of whether an "odd covering" of the integers, as we will call it, exists led Erdős and Selfridge to offer money to entice its solution while essentially betting on the outcome of the answer. Erdős, convinced that an odd covering does exist, offered \$25 for a proof that no odd covering exists; Selfridge, convinced (at that point) that no odd covering exists, offered \$300 for the first explicit example of an odd covering. No award was promised to someone who gave a non-constructive proof that an odd covering of the integers exists. Over the years, the prize money has varied (cf. [1, p. 251]). Selfridge (private communication) has informed us that he is now increasing his award to \$2000.

This paper was motivated largely by related work of Schinzel [3] associated with irreducible polynomials. Throughout this paper, unless specified otherwise, reducibility and irreducibility shall be in the ring $\mathbb{Z}[x]$ (in particular, 1 and -1 are neither reducible nor irreducible). It is well known (based on an appropriate covering argument) that there are infinitely many (even a positive proportion) of positive integers k such that $k \times 2^n + 1$ is composite for all positive integers n (cf. [1, p. 77]). An analogous problem is to determine whether there exists an $f(x) \in \mathbb{Z}[x]$ such that $f(x)x^n + 1$ is reducible for all positive integers n. To make the problem non-trivial, one should add the condition that $f(1) \neq -1$. A consequence of Schinzel's result in [3] is that if there is a polynomial $f(x) \in \mathbb{Z}[x]$ for which $f(1) \neq -1$ and for which $f(x)x^n + 1$ is reducible over the integers for every positive integer n, then there must exist an odd covering of the integers. In fact, Schinzel established that the existence of such an $f(x)$ is equivalent to an explicitly described covering which is more restrictive than an odd covering. The argument he gives is based largely on obtaining specific knowledge about the factorization of $f(x)x^n + 1$ when n is sufficiently large. For the connection between the factorization of $f(x)x^n + 1$

*The first author was supported by NSA Grant MDA904-97-1-0035 and NSA Grant MDA904-99-1-0221.

**The research for this paper was done while the third author was a visitor at the University of South Carolina supported in part by ONR/DEPSCoR Grant N00014-96-1-1003.

and the odd covering problem, the reader should consult Schinzel's original argument [3].

In this paper, we concern ourselves with an alternative approach to establishing information about the factorization of $f(x)x^n + 1$ (information sufficient to carry out the connection with the odd covering problem as in [3]). Our approach is to associate the reducibility of the non-reciprocal part (defined below) of lacunary polynomials with an elementary problem of independent interest concerning the distribution of integers in residue classes. As a consequence, we are able to obtain new information about the factorization of lacunary polynomials. In particular, we address the factorization of $f(x)x^n + g(x)$ where $f(x)$ and $g(x)$ are relatively prime polynomials in $\mathbb{Z}[x]$ with $f(0) \neq 0$ and $g(0) \neq 0$.

To help with the statements of our main results, we discuss notation here. The expression $a \bmod k$ will denote the unique integer b in $[0, k)$ for which $a \equiv b \pmod{k}$. If u is a real number, $[u]$ will denote the greatest integer $\leq u$ and $\|u\|$ will represent the minimal distance from u to an integer. We will use $\{u\}$ to denote $u - [u]$ unless it is clear from the context that $\{u\}$ refers to a set consisting of the single element u. For a polynomial $F(x) = \sum_{j=0}^{r} a_j x^{d_j}$, we define $\|F\| = \sqrt{\sum_{j=0}^{r} a_j^2}$. Also, $\widetilde{F}(x) = x^{\deg F} F(1/x)$ and is called the reciprocal of $F(x)$. If $F(x) = \pm\widetilde{F}(x)$, then $F(x)$ is said to be reciprocal. The non-reciprocal part of $F(x)$ is the quotient of $F(x)$ with the product of all of its irreducible reciprocal factors in $\mathbb{Z}[x]$ that have positive leading coefficient to the multiplicity they occur as a factor of $F(x)$. To clarify, if $g(x)$ is such a factor, then the content of $g(x)$ (the gcd of its coefficients) is 1 (since it is irreducible in $\mathbb{Z}[x]$). Also, since $-g(x)$ will be a factor whenever $g(x)$ is, we have factored out only $g(x)$ with positive leading coefficients to make the *non-reciprocal part* well-defined.

Our first result is

Theorem 1. *Let $F(x) = \sum_{j=0}^{r} a_j x^{d_j} \in \mathbb{Z}[x]$, where $0 = d_0 < d_1 < \cdots < d_r$ and $a_0 a_1 \cdots a_r \neq 0$. Let k_0 be a real number ≥ 2, and suppose that*

$$\deg F \geq \max\left\{2^{N+9\times 2^{N-1}} + 2^{9\times 2^{N-2}}, k_0 \times 2^{9\times 2^{N-2}}\right\} \quad \text{where} \quad N = 2\|F\|^2 + 2r - 5.$$

If the non-reciprocal part of $F(x)$ is reducible in $\mathbb{Z}[x]$, then there is a positive integer $k \in [k_0, \deg F]$ such that the polynomial $G(x, y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j} y^{\ell_j}$ is reducible in $\mathbb{Z}[x, y]$, where $\overline{d}_j$ and ℓ_j are defined by

$$\overline{d}_j = d_j \bmod k \qquad \text{and} \qquad d_j = k\ell_j + \overline{d}_j.$$

Note that the converse of the above comes close to holding. If $G(x, y)$ is reducible, then one can obtain a factorization of $F(x)$ by simply taking $y = x^k$. But $F(x)$ having even a non-trivial factorization does not imply its *non-reciprocal part* is reducible.

Our second result is a modification of the above theorem. We introduce an extra power of x factor into the statement of the theorem which enables us to decrease the double exponential bound on the size of $\deg F$. The extra power of x is transparent in the statement of the result when one takes $y = x^k$.

Theorem 2. *Let $F(x) = \sum_{j=0}^{r} a_j x^{d_j} \in \mathbb{Z}[x]$, where $0 = d_0 < d_1 < \cdots < d_r$ and $a_0 a_1 \cdots a_r \neq 0$. Let k_0 be a real number ≥ 2, and suppose that*

$$\deg F \geq \max\left\{2 \times 5^{2N-1}, k_0\left(5^{N-1} + \frac{1}{4}\right)\right\} \quad \textit{where} \quad N = 2\,\|F\|^2 + 2r - 5.$$

If the non-reciprocal part of $F(x)$ is reducible in $\mathbb{Z}[x]$, then there is an integer $k \in [k_0, 4(\deg F)/3)$ satisfying:

(i) *For each $j \in \{0, 1, \dots, r\}$, the number $d_j \bmod k$ is in $[0, k/4) \cup (3k/4, k)$.*

(ii) *If $\overline{d}_j$ and ℓ_j are defined by*

$$\overline{d}_j = (d_j + [k/4]) \bmod k \quad \textit{and} \quad d_j + [k/4] = k\ell_j + \overline{d}_j$$

and $G(x, y) = \sum_{j=0}^{r} a_j x^{\overline{d}_j} y^{\ell_j}$, then $x^{-m}G(x, y)$ is reducible in $\mathbb{Z}[x, y]$, where m is a non-negative integer chosen as large as possible with the constraint that $x^{-m}G(x, y) \in \mathbb{Z}[x, y]$.

The condition $k \in [k_0, 4(\deg F)/3)$ in Theorem 2 is sufficient to imply that $\deg F + [k/4] \geq k$. It follows that at least one of the exponents ℓ_j on y in the polynomial $G(x, y)$ is positive. Thus, $x^{-m}G(x, y)$ being reducible does not follow immediately from $F(x)$ being reducible.

As a consequence of Theorem 2, we obtain the following

Corollary. *Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(0) \neq 0$, $g(0) \neq 0$, and $\gcd_{\mathbb{Z}}(f(x), g(x)) = 1$. Let r_1 and r_2 denote the number of non-zero terms in $f(x)$ and $g(x)$, respectively. If*

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

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 or identically 1 or -1 unless one of the following holds:

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

(ii) *For either $\varepsilon = 1$ or $\varepsilon = -1$, one of $\varepsilon f(x)$ and $\varepsilon g(x)$ is a 4th power, the other is 4 times a 4th power, and n is divisible by 4.*

In the case that $f(x) = 1$ (or, equivalently, $g(x) = 1$), the Corollary, without an explicitly stated bound on n, is due to Schinzel [2(Theorem 5), 3(Lemma 4)].

Observe that if (i) or (ii) of the Corollary holds, the polynomial $f(x)x^n + g(x)$ is reducible by an apparent factorization. This factorization shows that the *non-reciprocal part of* $f(x)x^n + g(x)$ is reducible as well except possibly in the case that $f(x) = \pm\tilde{g}(x)$. However, in this case, $f(x)x^n + g(x)$ is itself reciprocal. Since it is impossible for a reciprocal polynomial to have exactly one non-reciprocal irreducible factor, we deduce that, in this case, the non-reciprocal part of $f(x)x^n + g(x)$ cannot be irreducible. Thus, if (i) or (ii) holds, the non-reciprocal part of $f(x)x^n + g(x)$ is not irreducible.

2. A Preliminary Problem on the Distribution of Residues

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 $k \geq 2$ such that $a_j \bmod k < k/2$ 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 $k \geq 2$ is minimal are given by $\{3, 5\}$ and $\{50, 68, 125\}$. We begin this section by showing that for each r, there exists an $A(r)$ such that if $a_r \geq A(r)$, then there is a $k \in [2, a_r]$ satisfying $a_j \bmod k < k/2$ for every $j \in \{1, 2, \ldots, r\}$ (take $k_0 = 2$ in Lemma 2 below). At the same time we pursue finding an estimate for $A(r)$. This problem will play a crucial role in the proof of Theorem 1, the estimate for $A(r)$ producing the bound on $\deg F$ given there. For the proof of Theorem 2, we then consider the analogous problem in which the condition $a_j \bmod k < k/2$ is replaced by $a_j \equiv d_j \pmod{k}$ for some $d_j \in (-k/4, k/4)$. We note that the techniques in this section can easily be extended to deal with similar problems in which the a_j are restricted to a smaller selection of residues modulo k.

Lemma 1. *Let $\alpha \in (0, 1/2]$, and let r be an integer ≥ 2. Set*

$$B_r = B_r(\alpha) = \frac{\alpha^3}{4}\left(\frac{16}{\alpha^5}\right)^{2^{r-2}}.$$

If $x_1, x_2, \ldots, x_r$ are numbers in $[0, 1]$ with $1 = x_1 > x_2 > \cdots > x_r$, then there exists a real number $b \in [1, B_r]$ such that $\{bx_j\} < \alpha$ for each $j \in \{1, 2, \ldots, r\}$.

Proof. Define $X_1 = 1$, $X_2 = \alpha$, and

$$X_j = \frac{4}{\alpha^2}\left(\frac{\alpha^5}{16}\right)^{2^{j-3}} \quad \text{for } j \geq 3.$$

If $x_2 < X_2$, then the lemma holds with $b = 1$. Now, we consider the case that $x_2 \geq X_2$. Take the maximal t (necessarily ≥ 2) satisfying $x_j \geq X_j$ for $j \in \{1, 2, \ldots, t\}$. Thus, if $t + 1 \leq j \leq r$, then

$$x_j \leq x_{t+1} < X_{t+1}. \tag{1}$$

By Dirichlet's box principle, there exists a positive integer ℓ satisfying $||\ell x_j|| < x_j\alpha/2$ for each $j \in \{2, 3, \ldots, t\}$. Furthermore, we may take

$$\ell \leq \prod_{j=2}^{t} \frac{2}{X_j\alpha} = \frac{2}{\alpha^2}\left(\frac{\alpha}{2}\right)^{t-2}\left(\frac{16}{\alpha^5}\right)^{2^{t-2}-1} \leq \frac{\alpha^3}{8}\left(\frac{16}{\alpha^5}\right)^{2^{t-2}} = \frac{B_t}{2}.$$

The number $b = \ell + \alpha/2 < B_t$ satisfies the inequalities $\{bx_1\} = \alpha/2 < \alpha$, and $\{bx_j\} < x_j\alpha < \alpha$ for every $j \in \{2, 3, \ldots, t\}$. Finally, for $j > t$, we have by (1) that

$$bx_j < B_t x_j < B_t X_{t+1} = \alpha.$$

This completes the proof of the lemma. ∎

Lemma 2. *Let r be a positive integer, and let k_0 be a real number ≥ 2. Set*

$$A(r) = \max\left\{ 2^{9\times 2^{r-1}} 2^r + 2^{9\times 2^{r-2}}, k_0 2^{9\times 2^{r-2}} \right\}.$$

Let $a_1, a_2, \ldots, a_r$ be non-negative integers satisfying $a_1 < a_2 < \cdots < a_r$ and $a_r \geq A(r)$. Then there exists an integer $k \in [k_0, a_r]$ such that $a_j \bmod k < k/2$ for each $j \in \{1, 2, \ldots, r\}$.

Proof. If $r = 1$, the result holds trivially by considering $k = a_r$. If $r = 2$, the result can be established by considering the cases $k = a_2$ (if $a_1 < a_2/2$), $k = [a_2/2]$ (if $a_2/2 \leq a_1 \leq 3(a_2 - 2)/4$), and $k = a_1$ (if $3(a_2 - 2)/4 < a_1 < a_2$).

We deal now only with $r \geq 3$. For $\alpha \in (0, 1/2)$, we define

$$C_r(\alpha) = \max\left\{ \frac{B_r(\alpha)^2}{\frac{1}{2} - \alpha} + B_r(\alpha), k_0 B_r(\alpha) \right\},$$

where $B_r(\alpha)$ is as defined in Lemma 1. For an appropriate choice of α, we show that $C_r(\alpha) \leq A(r)$. We also show that, for any $\alpha \in (0, 1/2)$, the lemma holds even with the condition $a_r \geq A(r)$ replaced by $a_r \geq C_r(\alpha)$. The lemma will then follow.

Consider

$$\alpha = 2^{-1-2^{2-r}}.$$

Then

$$B_r = B_r(\alpha) \leq \frac{1}{32}\left(\frac{16}{\alpha^5}\right)^{2^{r-2}} = 2^{9\times 2^{r-2}}.$$

Note that

$$\left(1 - \frac{1}{n}\right)^n > \left(1 - \frac{1}{n}\right)\frac{1}{e} > \frac{1}{4} \qquad \text{for } n \geq 4.$$

Taking $n = 2^{r-1}$, we deduce $(1/2) - \alpha > 2^{-r}$ from the implications

$$\left(1 - \frac{1}{2^{r-1}}\right)^{2^{r-1}} > \frac{1}{4} \implies 1 - \frac{1}{2^{r-1}} > 2^{-2^{2-r}} \implies \frac{1}{2} - \frac{1}{2^r} > \alpha \implies \frac{1}{2} - \alpha > 2^{-r}.$$

The inequality

$$C_r(\alpha) \leq \max\left\{ 2^{9\times 2^{r-1}} 2^r + 2^{9\times 2^{r-2}}, k_0 2^{9\times 2^{r-2}} \right\} = A(r)$$

follows easily.

Now, suppose the conditions of the lemma hold with $a_r \geq C_r(\alpha)$ instead of $a_r \geq A(r)$ (and $\alpha \in (0, 1/2)$ arbitrary). Let $x_j = a_{r+1-j}/a_r$ for each $j \in \{1, 2, \ldots, r\}$, and consider $b \in [1, B_r]$ as in Lemma 1. Let $\kappa = a_r/b$ and $k = [\kappa]$. Observe that $a_r \geq C_r(\alpha)$ and $b \in [1, B_r]$ imply that $k_0 \leq \kappa \leq a_r$ so that $k \in [k_0, a_r]$. For each $j \in \{1, 2, \ldots, r\}$ we have $\{a_j/\kappa\} = \{b x_{r+1-j}\} < \alpha$ so that

$$\{a_j/k\} \leq \{a_j/\kappa\} + \left(\frac{a_j}{k} - \frac{a_j}{\kappa}\right) < \alpha + \left(\frac{a_r}{(a_r/B_r) - 1} - \frac{a_r}{a_r/B_r}\right) = \alpha + \frac{B_r^2}{a_r - B_r} \leq \frac{1}{2}.$$

It follows that $a_j \bmod k < k/2$ for each $j \in \{1, 2, \ldots, r\}$ as required. ■

Lemma 3. *Let r be a positive integer, and let k_0 be a real number ≥ 2. Set*

$$A'(r) = \max\left\{2 \times 5^{2r-1}, k_0\left(5^{r-1} + \frac{1}{4}\right)\right\}.$$

Let $a_1, a_2, \ldots, a_r$ be non-negative integers satisfying $a_1 < a_2 < \cdots < a_r$ and $a_r \geq A'(r)$. Then there exists an integer $k \in [k_0, 4a_r/3)$ such that $a_j \bmod k$ is in $[0, k/4) \cup (3k/4, k)$ for each $j \in \{1, 2, \ldots, r\}$.

Proof. We will establish that if D is a positive integer with $1 \leq D \leq \sqrt{a_r}/(5^{r-1}\sqrt{10})$, then one may take

$$k \in \left(\frac{a_r}{5^{r-1}D + (1/4)}, \frac{a_r}{D - (1/4)}\right). \tag{2}$$

In particular, taking $D = 1$ will give $k \in [k_0, 4a_r/3)$ as in the statement of the lemma.

Let $x_j = a_j/a_r$ for $j \in \{1, 2, \ldots, r\}$. We want to show that there is an integer k satisfying (2) and integers $c_1, c_2, \ldots, c_r$ such that

$$|a_j - c_j k| < \frac{k}{4} \qquad \text{for } 1 \leq j \leq r. \tag{3}$$

By the Dirichlet box principle, there is an integer d satisfying $D \leq d \leq 5^{r-1}D$, $D|d$, and

$$\|dx_j\| \leq \frac{1}{5} \qquad \text{for } 1 \leq j \leq r-1. \tag{4}$$

Clearly, (4) holds with $j = r$ as well. Observe that the upper bound on D above implies that $d \leq \sqrt{a_r/10}$. For $1 \leq j \leq r$, let c_j denote the nearest integer to dx_j.

For the moment, suppose $c_j \neq 0$ (so that $c_j \geq 1$) for each $j \in \{1, 2, \ldots, r\}$. Then (3) follows provided

$$\frac{k}{a_r} \in \bigcap_{1 \leq j \leq r} \left(\frac{x_j}{c_j + (1/4)}, \frac{x_j}{c_j - (1/4)}\right).$$

For each $j \in \{1, 2, \ldots, r\}$, since $c_j \leq d$, we deduce from (4) that

$$\frac{d + (1/5)}{d + (1/4)} \geq \frac{c_j + (1/5)}{c_j + (1/4)} \geq \frac{dx_j}{c_j + (1/4)} \quad \text{and} \quad \frac{d - (1/5)}{d - (1/4)} \leq \frac{c_j - (1/5)}{c_j - (1/4)} \leq \frac{dx_j}{c_j - (1/4)}.$$

Hence, (3) holds provided

$$\frac{k}{a_r} \in \left(\frac{d + (1/5)}{d(d + (1/4))}, \frac{d - (1/5)}{d(d - (1/4))}\right). \tag{5}$$

The length of the interval on the right is

$$\frac{1}{10(d^2 - \frac{1}{16})} > \frac{1}{10d^2} \geq \frac{1}{a_r}$$

so that k exists satisfying (5). Observe that (5) and the definition of d imply (2) holds.

Now, suppose some $c_j = 0$ with $j \in \{1, 2, \ldots, r\}$. We again choose k so that (5) holds. For each $c_j \neq 0$, the above argument gives $|a_j - c_j k| < k/4$ as in (3). On the other hand, if $c_j = 0$, then (4) and the definitions of c_j, x_j, and k imply

$$5da_j \leq a_r < k\frac{d\left(d + \frac{1}{4}\right)}{\left(d + \frac{1}{5}\right)} \leq \frac{5dk}{4}.$$

Hence, (3) holds for such c_j as well, completing the proof of the lemma. ■

It is of some interest to know whether the bounds given for $A(r)$ and $A'(r)$ are close to their actual values. In particular, does $A(r)$ have double exponential growth and does $A'(r)$ have exponential growth? We end this section with two examples which show that this is indeed the case.

Example 1: We describe a choice of $\{a_1, a_2, \ldots, a_r\}$ which shows that the growth of $A(r)$ is doubly exponential. Let s be a positive integer, and define $x_1 = 1$, $x_2 = 1/2$, and

$$x_{2j+2} = \frac{x_{2j}^2}{2} \quad \text{and} \quad x_{2j+1} = x_{2j} - x_{2j+2} \qquad \text{for } j \in \{1, 2, \ldots, s-1\}.$$

Equivalently, $x_1 = 1$ and

$$x_{2j} = \frac{1}{2^{2^j - 1}} \quad \text{for } j \in \{1, 2, \ldots, s\} \quad \text{and} \quad x_{2j+1} = \frac{2^{2^j} - 1}{2^{2^{j+1} - 1}} \quad \text{for } j \in \{1, 2, \ldots, s-1\}.$$

Let b be a real number in $\left[1, 2^{2^s - 1}\right)$. We will show that the inequalities

$$\{bx_j\} < \frac{1}{2} \qquad \text{for } j \in \{1, 2, \ldots, 2s\} \tag{6}$$

cannot all hold. Once this is established, one can take $r = 2s$ and $a_j = 2^{2^s - 1} x_{r+1-j} = x_{r+1-j}/x_r$ for $j \in \{1, 2, \ldots, r\}$ to obtain positive integers $a_1, a_2, \ldots, a_r$ with $a_r = 2^{2^{r/2} - 1}$ and $\max_{1 \leq j \leq r}\{a_j \bmod k\} \geq k/2$ for each integer $k \in [2, a_r]$ (for such k, consider $b = 1/(kx_r)$ in (6)).

Assume that (6) holds. We claim that $\{bx_{2j}\} < x_{2j}/2$ for $j \in \{1, 2, \ldots, s\}$. We prove this by induction on j. Since $\{bx_2\} < 1/2$, we have $\{2bx_2\} = 2\{bx_2\}$, or $\{bx_2\} = \{2bx_2\}/2$. But $\{2bx_2\}/2 = \{bx_1\}/2 < 1/4$. We obtain $\{bx_2\} < 1/4 = x_2/2$. We suppose now that $\{bx_{2j}\} < x_{2j}/2$ for some $j \leq s - 1$ and establish that $\{bx_{2j+2}\} < x_{2j+2}/2$. Set $n = 2^{2^j}$ so that

$$n = \frac{2}{x_{2j}} = \frac{x_{2j}}{x_{2j+2}}. \tag{7}$$

The induction hypothesis and (7) imply $\{bx_{2j}\} < x_{2j}/2 = 1/n$. The relationships $x_{2j+1} + x_{2j+2} = x_{2j}$, $\{bx_{2j+1}\} < 1/2$, and $\{bx_{2j+2}\} < 1/2$ imply $\{bx_{2j}\} = \{bx_{2j+1}\} + \{bx_{2j+2}\}$.

Therefore, $\{bx_{2j+2}\} \le \{bx_{2j}\} < 1/n$, and we have $\{nbx_{2j+2}\} = n\{bx_{2j+2}\}$ or, by (7), $\{bx_{2j}\} = n\{bx_{2j+2}\}$. We deduce that $\{bx_{2j+2}\} = \{bx_{2j}\}/n < 1/n^2 = x_{2j+2}/2$. Thus, by induction, $\{bx_{2j}\} < x_{2j}/2$ for $j \in \{1, 2, \ldots, s\}$. Now, we take $j = s$ to obtain $\{bx_{2s}\} < x_{2s}/2$. Since $b \ge 1$, we obtain $bx_{2s} \ge 1$. Hence, $b \ge 1/x_{2s} = 2^{2^s - 1}$, a contradiction. Thus, (6) does not hold.

Example 2: For r be a positive integer and $j \in \{1, 2, \ldots, r\}$, define $a_j = 3^{j-1}$. We show that for each $k \in [2, 4a_r]$, at least one of the r numbers a_j mod k is not in $[0, k/4) \cup (3k/4, k)$. Each $k \in [2, 4a_r]$ belongs to at least one interval $[4 \times 3^{j-2}, 4 \times 3^{j-1}]$ with $j \in \{1, 2, \ldots, r\}$. On the other hand, if $k \in [4 \times 3^{j-2}, 4 \times 3^{j-1}]$ for some j, then

$$\frac{k}{4} \le 3^{j-1} = a_j \le \frac{3k}{4}.$$

The desired conclusion follows.

3. Proofs of the Main Results

Proof of Theorem 1. We consider the non-reciprocal part of $F(x)$ to be reducible. We begin the proof by constructing non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $F(x) = u(x)v(x)$. Let $g(x)$ be an irreducible non-reciprocal factor of $F(x)$. Either $\tilde{g}(x)$ is also a factor of $F(x)$ or it is not. If it is, then take $u(x)$ and $v(x)$ so that $\tilde{g}(x) \nmid u(x)$ and $g(x) \nmid v(x)$. Observe that if α is a root of $g(x)$, then it will be a root of $u(x)$ but $1/\alpha$ will not; this implies $u(x)$ is not reciprocal. Similarly, $v(x)$ is not reciprocal. If $\tilde{g}(x)$ is not a factor of $F(x)$, then there is some irreducible non-reciprocal $h(x) \ne \tilde{g}(x)$ such that $g(x)h(x)$ divides $F(x)$. If $\tilde{h}(x)$ also divides $F(x)$, then we take $u(x)$ and $v(x)$ so that $\tilde{h}(x) \nmid u(x)$ and $h(x) \nmid v(x)$ and get (analogous to before) that $u(x)$ and $v(x)$ are non-reciprocal. So we are left with the possibility that both $\tilde{g}(x)$ and $\tilde{h}(x)$ do not divide $F(x)$. Take $u(x)$ and $v(x)$ so that $g(x)|u(x)$ and $h(x)|v(x)$. Since $g(\alpha) = 0$ implies $u(\alpha) = 0$ and $u(1/\alpha) \ne 0$ (which follows from the fact that the irreducible polynomial having $1/\alpha$ as a root, namely $\tilde{g}(x)$, is not a factor of $F(x)$), we deduce $u(x)$ is non-reciprocal. Similarly, $v(x)$ is non-reciprocal.

Define

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

Since $u(x)$ and $v(x)$ are non-reciprocal, we easily see that the polynomials $F(x)$, $\widetilde{F}(x)$, $W(x)$, and $\widetilde{W}(x)$ are distinct polynomials of degree d_r with any two having greatest common divisor of degree $< d_r$. Observe that

$$F(x)\widetilde{F}(x) = u(x)v(x)\tilde{u}(x)\tilde{v}(x) = W(x)\widetilde{W}(x). \tag{8}$$

Note that the coefficient of x^{d_r} on the left side of (8) is $\|F\|^2$ and the coefficient of x^{d_r} on the right side of (8) is $\|W\|^2$. Hence, $\|W\|^2 = \|F\|^2$. We write $W(x)$ in the form $W(x) = \sum_{j=0}^{s} b_j x^{e_j}$ where the b_j are non-zero and $0 = e_0 < e_1 < \cdots < e_s = d_r$. Then $\|W\|^2 = \|F\|^2$ implies $s \le \|F\|^2 - 1$. Consider the set

$$\begin{aligned} T = \{d_1, d_2, \ldots, d_r\} &\cup \{d_r - d_1, d_r - d_2, \ldots, d_r - d_{r-1}\} \\ &\cup \{e_1, e_2, \ldots, e_{s-1}\} \cup \{e_s - e_1, e_s - e_2, \ldots, e_s - e_{s-1}\}. \end{aligned}$$

Observe that $|T| \le 2\,\|F\|^2 + 2r - 5$. We use the lower bound on $d_r = \deg F$ in the statement of the theorem together with Lemma 2 to deduce that there is an integer $k \in [k_0, d_r]$ such that $t \bmod k < k/2$ for every $t \in T$. Fix such an integer k.

Define $\overline{d}_j$ and ℓ_j as in the theorem, and define $\overline{e}_j$ and m_j similarly by $\overline{e}_j = e_j \bmod k$ and $e_j = km_j + \overline{e}_j$ (for $0 \le j \le s$). Define $\overline{d}'_j$, ℓ'_j (for $0 \le j \le r$) and $\overline{e}'_j$, m'_j (for $0 \le j \le s$) by $\overline{d}'_j = d_r - d_j \bmod k$, $d_r - d_j = k\ell'_j + \overline{d}'_j$, $\overline{e}'_j = e_s - e_j \bmod k$, and $e_s - e_j = km'_j + \overline{e}'_j$. Define $G_1(x,y) = G(x,y)$ (as in the statement of the theorem),

$$G_2(x,y) = \sum_{j=0}^{r} a_j x^{\overline{d}'_j} y^{\ell'_j}, \quad H_1(x,y) = \sum_{j=0}^{s} b_j x^{\overline{e}_j} y^{m_j}, \quad \text{and} \quad H_2(x,y) = \sum_{j=0}^{s} b_j x^{\overline{e}'_j} y^{m'_j}.$$

Observe that the definition of k implies that the exponent in each power of x appearing in these expressions for $G_j(x,y)$ and $H_j(x,y)$ is $< k/2$. Also, $G_1(x,x^k) = F(x)$, $G_2(x,x^k) = \widetilde{F}(x)$, $H_1(x,x^k) = W(x)$, and $H_2(x,x^k) = \widetilde{W}(x)$. In particular, we deduce that $G_1(x,y)$, $G_2(x,y)$, $H_1(x,y)$, and $H_2(x,y)$ are distinct with each one not dividing the others.

Corresponding to (8), we establish next that

$$G_1(x,y)G_2(x,y) = H_1(x,y)H_2(x,y). \tag{9}$$

Expanding the product on the left-hand side of (9) we obtain an expression of the form $\sum_{j=0}^{J} g_j(x)y^j$ where possibly some $g_j(x)$ are 0 but, in any case, $\deg g_j < k$ for each j. Since

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

we deduce that the terms in $g_j(x)x^{kj}$ correspond precisely to the terms in the expansion of $F(x)\widetilde{F}(x)$ having degrees in the interval $[kj, k(j+1))$. Furthermore, J is determined by the degree of $F(x)\widetilde{F}(x)$ (namely, $J = [2d_r/k]$). Similarly, writing the right-hand side of (9) in the form $\sum_{j=0}^{J'} h_j(x)y^j$, we get $\deg h_j < k$ for each j and the terms in $h_j(x)x^{kj}$ correspond to the terms in the expansion of $W(x)\widetilde{W}(x)$ having degrees in the interval $[kj, k(j+1))$. Also, J' is determined by the degree of $W(x)\widetilde{W}(x)$ (so that $J' = [2d_r/k]$). We see now that (9) is a consequence of (8).

Since $G_1(x,y)$, $G_2(x,y)$, $H_1(x,y)$, and $H_2(x,y)$ are distinct (with no one dividing another), we deduce by unique factorization and (9) that each of the polynomials $G_1(x,y)$, $G_2(x,y)$, $H_1(x,y)$, and $H_2(x,y)$ is reducible. Since $G(x,y) = G_1(x,y)$, the theorem is established. ■

Proof of Theorem 2. We proceed as in the proof of Theorem 1. We choose the set T in precisely the same manner. The integer k is chosen using Lemma 3. Defining $G(x,y)$ as in the statement of Theorem 2, we obtain $G(x,x^k) = x^{[k/4]}F(x)$. We define $G_1(x,y) = G(x,y)$ and the polynomials $G_2(x,y)$, $H_1(x,y)$, and $H_2(x,y)$ in an analogous manner to the definition of $G(x,y)$ so that we have

$$G_2(x,x^k) = x^{[k/4]}\widetilde{F}(x), \; H_1(x,x^k) = x^{[k/4]}W(x), \; \text{ and } \; H_2(x,x^k) = x^{[k/4]}\widetilde{W}(x). \tag{10}$$

Writing $G_1(x,y)G_2(x,y) = \sum_{j=0}^{J} g_j(x)y^j$, we deduce here that the terms in $g_j(x)$ correspond precisely to the terms in the expansion of $x^{2[k/4]}F(x)\widetilde{F}(x)$ having degrees in the interval $[kj, k(j+1))$. A similar conclusion holds for the terms in $H_1(x,y)H_2(x,y)$, and we obtain (9) as before. From (10), given any two of $G_1(x,y)$, $G_2(x,y)$, $H_1(x,y)$, and $H_2(x,y)$, either one will have a factor different from x that does not divide the other. The theorem follows. ■

Proof of Corollary. We use Theorem 2 with $F(x) = \sum_{j=0}^{r} a_j x^{d_j} = f(x)x^n + g(x)$ and $k_0 = 2\max\{\deg f, \deg g\}$. For such $F(x)$, there is a non-negative integer ρ such that $g(x) = \sum_{j=0}^{\rho} a_j x^{d_j}$ and $f(x) = \sum_{j=\rho+1}^{r} a_j x^{d_j - n}$. Since $k \geq 2d_\rho$, we have $d_j + [k/4] < k$ for $j \in \{0, 1, \ldots, \rho\}$. Hence, each of $\ell_1, \ell_2, \ldots, \ell_\rho$ is 0. We claim that the numbers $\ell_{\rho+1}, \ell_{\rho+2}, \ldots, \ell_r$ are all equal. Assume $\ell_s \neq \ell_t$ with $\rho + 1 \leq s < t \leq r$. The ordering on the d_j and the definition of the ℓ_j in (ii) of Theorem 2 imply $\ell_t > \ell_s$. By (i) of Theorem 2 and the definition of $\overline{d}_j$, each $\overline{d}_j$ is in $[0, k/2)$. Hence, by the definition of the ℓ_j in (ii) of Theorem 2, we obtain

$$d_t - d_s = k(\ell_t - \ell_s) + (\overline{d}_t - \overline{d}_s) > k - \frac{k}{2} = \frac{k}{2} \geq \deg f.$$

This contradicts that $f(x) = \sum_{j=\rho+1}^{r} a_j x^{d_j - n}$. Hence, $\ell_{\rho+1}, \ell_{\rho+2}, \ldots, \ell_r$ are all equal. It follows that the polynomial $x^{-m}G(x,y)$ in Theorem 2 can be written as $x^{-m}G(x,y) = f(x)x^d y^\ell + g(x)x^{d'}$ for some positive integer ℓ (see the comment after the statement of Theorem 2) and some non-negative integers d and d' (with at least one being 0). Theorem 2 implies that the non-reciprocal part of $F(x)$ is reducible only if $x^{-m}G(x,y)$ is reducible. A straightforward application of Capelli's theorem (cf. [4, p. 91]) implies that if (i) and (ii) of the Corollary do not hold, then $x^{-m}G(x,y)$ is not reducible. It follows that if (i) and (ii) of the Corollary do not hold, then the non-reciprocal part of $F(x)$ is either irreducible or ± 1. This completes the proof. ■

References

1. R. K. Guy, *Unsolved Problems in Number Theory (Second Ed.)*, Springer-Verlag, New York, 1994.
2. A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. **11** (1965), 1–34.
3. A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967), 91–101.
4. A. Schinzel, *Selected Topics on Polynomials*, Univ. Mich. Press, Ann Arbor, 1982.

Michael Filaseta
Mathematics Department
University of South Carolina
Columbia, SC 29208
U.S.A.
filaseta@math.sc.edu

Kevin Ford
Mathematics Department
University of South Carolina
Columbia, SC 29208
U.S.A.
ford@math.sc.edu

Sergei Konyagin
Dept. of Mechanics & Mathematics
State University
Moscow 119899
Russia
kon@nw.math.msu.su