



ON THE IRREDUCIBILITY OF THE NON-CYCLOTOMIC PART OF MOST 0, 1-POLYNOMIALS WITH FEW TERMS

Michael Filaseta

*Department of Mathematics, University of South Carolina, Columbia, South
Carolina*

`filaseta@math.sc.edu`

Alexandros Kalogirou

*Department of Mathematics, University of South Carolina, Columbia, South
Carolina*

`kalogira@email.sc.edu`

Received: 8/17/25, Accepted: 5/5/26, Published: 9/28/26

Abstract

We provide a proof that, for a fixed integer $k \geq 2$, almost all 0, 1-polynomials, with $k + 1$ terms and constant term 1, are irreducible after their cyclotomic factors are removed. This is a special case of a more general theorem due to Andrzej Schinzel, but our proof provides some new ideas and a more elementary presentation.

– *To Mel Nathanson and Carl Pomerance in celebration of their 80th birthdays*

1. Introduction

In [21], A. Schinzel established the following interesting result.

Theorem 1 (Schinzel, 1986). *Let $k \geq 2$ be an integer. Let $a_0, a_1, \dots, a_k$ be fixed non-zero integers. Then for almost all choices of positive integers $n_1 < \dots < n_k$, the polynomial $F(x) = a_0 + a_1x^{n_1} + \dots + a_kx^{n_k}$, removed of its cyclotomic factors, is irreducible over $\mathbb{Q}$.*

In other words, for a fixed integer $k \geq 2$, the number of choices for $n_1, \dots, n_k$ in the interval $[1, N]$ for which $F(x)$, removed of its cyclotomic factors, is irreducible divided by $\binom{N}{k}$ tends to 1 as the positive integer $N \geq k$ tends to infinity. Notably, Schinzel's result is much stronger, allowing the coefficients to come from an arbitrary algebraic number field and giving an explicit upper bound on the number of exceptional choices of $n_1, \dots, n_k$ in the interval $[1, N]$ for which $F(x)$, removed of its cyclotomic factors, is reducible. This upper bound was improved upon in

Schinzel's work [22] to $O(N^{\lfloor (k+1)/2 \rfloor})$, where the implied constant depends only on the coefficients $a_0, a_1, \dots, a_k$.

Recently, the second author [14] made use of Theorem 1 to establish, in an analogous lacunary setting, a conjecture of A. Odlyzko and B. Poonen [18]. Odlyzko and Poonen conjectured that almost all polynomials with coefficients coming from $\{0, 1\}$ and constant term 1 are irreducible. To help explain the second author's result, we note that one can show that a positive proportion, depending on k , of the polynomials of the form

$$F(x) = 1 + x^{n_1} + \dots + x^{n_k}, \quad \text{where } n_j \in \mathbb{Z}^+ \text{ and } n_1 < \dots < n_k, \quad (1)$$

are reducible; for example, a positive proportion of the $F(x)$ in (1) will be divisible by $(x^{k+1} - 1)/(x - 1)$. In [14], the second author was able to show that this proportion must go to 0 as k goes to infinity. More precisely, he establishes

$$\lim_{k \rightarrow \infty} \limsup_{N \rightarrow \infty} \frac{|\{(n_1, \dots, n_k) \in [1, N]^k : n_1 < \dots < n_k, F(x) \text{ in (1) is reducible}\}|}{\binom{N}{k}} = 0.$$

The Odlyzko–Poonen conjecture was resolved under the extended Riemann hypothesis by E. F. Breuillard and P. P. Varjú [7]. The conjecture has, since it was proposed, sparked an interest in the study of polynomials with random coefficients and high degree, with the first breakthrough coming from S. V. Konyagin [15], whose work was highly influential both in the work of Breuillard and Varjú [7], as well as in the broader and related work of L. Bary-Soroker, D. Hokken, G. Kozma, and B. Poonen [1], L. Bary-Soroker and G. Kozma [3] and L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma [2]. The conjecture remains open unconditionally, and while the question addressed in [14] has some external similarity with the Odlyzko–Poonen conjecture, the two are associated with very different random polynomial models and the two are independent.

In the next three sections, we provide a more elementary, largely self-contained, account of what is needed from Theorem 1 for the second author's work in [14], with the hope of making Schinzel's important work in [21, 22], at least in the case of 0, 1-polynomials (polynomials whose coefficients are each 0 or 1), more easily accessible to a wider audience. Specifically, we prove the following.

Theorem 2. *Fix an integer $k \geq 2$. For almost all choices of positive integers $n_1 < \dots < n_k$, the polynomial $F(x) = 1 + x^{n_1} + \dots + x^{n_k}$, removed of its cyclotomic factors, is irreducible. More precisely, for N a positive integer, the number of choices for $(n_1, \dots, n_k) \in [1, N]^k$ with $n_1 < \dots < n_k$ and with $F(x)$, removed of its cyclotomic factors, reducible is $O_k(N^{k - (1/(2k+1))})$ as $N \rightarrow \infty$.*

In the last section of the paper, we also connect some of the ideas that permeate Schinzel's work and their presentation here with the conjecture posed by Odlyzko

and Poonen. We provide there an additive number theoretic conjecture whose resolution would mark significant progress towards the Odlyzko–Poonen conjecture and is at the same time interesting in its own right.

To prove Theorem 2, we will take advantage of the fact that the coefficients of $F(x)$ are 0 and 1 in a way that will simplify what was done in [21, 22]. This is the purpose in Lemma 2 in the next section, which comes from [10]. To handle the more general case of Theorem 1, Schinzel takes advantage of his work in [20] (also, see Theorem 1 due to Schinzel in [10]). Restricting the coefficients to 0 and 1, as we do here, allows us to showcase more easily the themes around non-reciprocal factors, that is, factors $w(x)$ where $w(x) \neq \pm x^{\deg w} w(1/x)$. Generally speaking, a lacunary polynomial will have more than one non-reciprocal irreducible factor if and only if its exponents have extra additive structure that one can exploit to reduce their count.

To address possible irreducible reciprocal factors of $F(x)$ that are not cyclotomic, that is non-cyclotomic irreducible polynomials $w(x) \in \mathbb{Z}[x]$ of degree at least 1 for which $w(x) = \pm x^{\deg w} w(1/x)$, our argument will borrow ideas from [21] while providing some simplifications and different approaches to aspects of Schinzel’s arguments there.

Before leaving this introduction, we address the important achievement of E. Bombieri and U. Zannier as given in the appendix by Zannier in [23] (see also [5, Theorem 1.6] and [22, Theorem BZ]). We restrict the result to the context of Theorem 1 and Theorem 2.

Theorem 3 (Bombieri and Zannier, 1998). *Fix an integer $k \geq 2$. Let $n_1 < \dots < n_k$ be positive integers, and let $G(x_1, \dots, x_k)$ and $H(x_1, \dots, x_k)$ in $\mathbb{Z}[x_1, \dots, x_k]$ be relatively prime polynomials in $\mathbb{Q}[x_1, \dots, x_k]$. Suppose that $G(x^{n_1}, \dots, x^{n_k})$ and $H(x^{n_1}, \dots, x^{n_k})$ have a non-cyclotomic irreducible factor in common. Then there are $\gamma_j \in \mathbb{Z}$, not all 0, and a computable constant $C(G, H)$ only depending on G and H such that*

$$\gamma_1 n_1 + \dots + \gamma_k n_k = 0 \quad \text{and} \quad \sum_{j=1}^k |\gamma_j| \leq C(G, H).$$

A proof of Theorem 3 is outside the scope of this paper, but it is worth noting that Theorem 3 allows us to quickly give an appropriate bound on the number of polynomials of the form given in Theorem 1 which have an irreducible reciprocal non-cyclotomic factor. Here, the terminology *reciprocal*, as indicated above, has the following meaning. If $f(x) \in \mathbb{R}[x]$, then the reciprocal of $f(x)$ is $\tilde{f}(x) = x^{\deg f} f(1/x)$. A polynomial $f(x) \in \mathbb{R}[x]$ is said to be reciprocal if $f(x) = \pm \tilde{f}(x)$. This definition is motivated by the fact that if $f(x)$ is reciprocal and $\alpha \in \mathbb{C}$ is a root of $f(x)$, then $\alpha \neq 0$ and $1/\alpha$ is also a root of $f(x)$. The roots α and $1/\alpha$ will also occur in the factorization of $f(x)$ over $\mathbb{C}$ to the same multiplicity. The cyclotomic polynomials are examples of reciprocal polynomials.

Fix non-zero integers $a_0, a_1, \dots, a_k$. Take

$$G(x_1, \dots, x_k) = a_0 + a_1 x_1 + \dots + a_k x_k$$

and

$$H(x_1, \dots, x_k) = x_1 \cdots x_k G(x_1^{-1}, \dots, x_k^{-1}).$$

One can check that these polynomials are relatively prime in $\mathbb{Q}[x_1, \dots, x_k]$ since they are distinct linear polynomials in x_1 (or in any other variable) and neither has a factor in $\mathbb{Q}[x_2, \dots, x_k]$. Now, suppose $F(x) = a_0 + a_1 x^{n_1} + \dots + a_k x^{n_k}$, as in the statement of Theorem 1, has an irreducible non-cyclotomic reciprocal factor $w(x) \in \mathbb{Z}[x]$, and let α be a root of $w(x)$. Then α and $1/\alpha$ are roots of $w(x)$ and, hence, of $F(x)$. We deduce that α is a root of both $G(x^{n_1}, \dots, x^{n_k}) = F(x)$ and

$$H(x^{n_1}, \dots, x^{n_k}) = x^{n_1 + \dots + n_k} G(x^{-n_1}, \dots, x^{-n_k}) = x^{n_1 + \dots + n_{k-1}} F(1/x).$$

Thus, $G(x^{n_1}, \dots, x^{n_k})$ and $H(x^{n_1}, \dots, x^{n_k})$ are both divisible by $w(x)$. We obtain from Theorem 3 that $n_1, \dots, n_k$ must satisfy one of finitely many linear equations in $n_1, \dots, n_k$ over $\mathbb{Q}$, where the linear equations depend only on $a_0, a_1, \dots, a_k$ and in particular not on $n_1, \dots, n_k$. For each such equation, one of the variables n_j can be expressed in terms of the others leading to $O(N^{k-1})$ choices for $n_1 < \dots < n_k \leq N$ satisfying the equation. We deduce then that the number of choices of positive integers $n_1, \dots, n_k$, with $n_1 < \dots < n_k \leq N$, for which $F(x)$ has an irreducible non-cyclotomic reciprocal factor is $O_k(N^{k-1})$ which is small compared to $\binom{N}{k}$ and thus negligible in comparison to all $F(x)$ considered in Theorem 1. To clarify, as in Schinzel's initial work on this topic in [21], we will not make use of this application of Theorem 3 as we proceed.

2. Non-reciprocal Factors

The *non-reciprocal part* of a polynomial $f(x) \in \mathbb{Z}[x]$ is $f(x)$ removed of every irreducible reciprocal factor in $\mathbb{Z}[x]$ having positive leading coefficient. Thus, for example, the non-reciprocal part of $f(x) = 2x(x+1)^2(3x^2-3x-1)(-2x^2+3x-2)$ is $-x(3x^2-3x-1)$, which corresponds to the irreducible factors 2, $x+1$ twice, and $2x^2-3x+2$ in $\mathbb{Z}[x]$ being removed from $f(x)$. In this section, we show that for almost all polynomials $F(x)$ as in Theorem 2, the non-reciprocal part of $F(x)$ is irreducible.

Lemma 1. *Fix an integer $k \geq 2$. For all but $O_k(N^{k-1})$ choices of positive integers $n_1 < n_2 < \dots < n_k \leq N$, the 0, 1-polynomial $F(x)$ in (1) has exactly one irreducible non-reciprocal factor.*

Faithful to the themes throughout our treatment on 0, 1-polynomials, we will arrive at the above conclusion by finding linear equations satisfied by the components of the vector $\vec{n} = \langle n_1, \dots, n_k \rangle$, consisting of the non-zero exponents of $F(x)$, in the case where $F(x)$ does not have exactly one irreducible non-reciprocal factor. The idea that will produce these linear constraints is contained in the following lemma from [10]. We give a proof to emphasize the simplicity of this result.

Lemma 2. *Let $f(x) \in \mathbb{Z}[x]$ be a 0, 1-polynomial, with $f(0) = 1$ and such that $f(x)$ is divisible by the product of two non-reciprocal irreducible polynomials in $\mathbb{Z}[x]$, not necessarily distinct. Then there is a 0, 1-polynomial $g(x)$ with the same number of terms as $f(x)$ and with $g(x) \notin \{f(x), \tilde{f}(x)\}$ satisfying*

$$f(x)\tilde{f}(x) = g(x)\tilde{g}(x). \quad (2)$$

Proof. We begin by showing that there are monic non-reciprocal polynomials $w_1(x)$ and $w_2(x)$ in $\mathbb{Z}[x]$ such that $f(x) = w_1(x)w_2(x)$. Since the non-zero coefficients of $f(x)$ are positive and $f(0) = 1$, every monic factor of $f(x)$ in $\mathbb{Z}[x]$ cannot have positive real roots and therefore must have constant term 1. Therefore, for some positive integers λ_i, λ'_i and λ''_j , we can write

$$f(x) = \prod_{i=1}^{t_1} p_i^{\lambda_i}(x) \tilde{p}_i^{\lambda'_i}(x) \prod_{j=1}^{t_2} q_j^{\lambda''_j}(x) \prod_{e=1}^{t_3} r_e(x),$$

where in the first product $p_i(x)$ and $\tilde{p}_i(x)$ are pairs of monic irreducible non-reciprocal factors of $f(x)$ in $\mathbb{Z}[x]$, in the second product $q_j(x)$ are monic irreducible non-reciprocal factors of $f(x)$ in $\mathbb{Z}[x]$ for which $\tilde{q}_j(x)$ is not a factor of $f(x)$, and in the third product the $r_e(x)$ are monic irreducible reciprocal factors of $f(x)$ in $\mathbb{Z}[x]$ which are not necessarily distinct. Furthermore, we take, as we can, the $2t_1 + t_2$ polynomials $p_i(x)$, $\tilde{p}_i(x)$ and $q_j(x)$ to be distinct. If the first product is empty, then we can take $w_1(x)$ to be any irreducible factor of the second product, which will have at least two factors by assumption. If the first product is not empty, then we can take $w_1(x)$ to be $\prod_{i=1}^{t_1} p_i^{\lambda_i}(x)$.

Set $g(x) = w_1(x)\tilde{w}_2(x)$, where $f(x) = w_1(x)w_2(x)$ and where $w_1(x)$ and $w_2(x)$ are monic and non-reciprocal. Then $g(x) \notin \{f(x), \tilde{f}(x)\}$, and $g(x)$ satisfies (2). As noted above, since $w_1(x)$ and $w_2(x)$ are monic factors of $f(x)$, we have $w_1(0) = w_2(0) = 1$. It follows that $g(x)$ is monic. It remains to show that $g(x)$ is a 0, 1-polynomial with the same number of terms as $f(x)$.

Write $g(x) = \sum_{i=1}^l a_i x^{m_i}$ with integers $0 \leq m_0 < m_1 < \dots < m_l$, $a_i \neq 0$, and $a_l = 1$. Since $f(0) = 1$, so that x is not a factor of $f(x)$, we see that

$$n = \deg f = \deg \tilde{f} = \deg g = \deg \tilde{g}.$$

Let k be the number of terms of $f(x)$. By comparing the coefficients of x^n on both sides of (2), we find that $\sum_{i=1}^l a_i^2 = k$, which implies that $l \leq k$. Using (2) again, we

find that $k^2 = f(1)\tilde{f}(1) = g(1)\tilde{g}(1)$. Together with the Cauchy–Schwarz inequality, we obtain

$$k^2 = f(1)\tilde{f}(1) = g(1)\tilde{g}(1) = \left(\sum_{i=1}^l a_i\right)^2 \leq l \left(\sum_{i=1}^l a_i^2\right) = lk \leq k^2.$$

This proves that $l = k$, and the equality in the Cauchy–Schwarz inequality implies that $g(x)$ has all its coefficients equal to 1. $\square$

Let $F(x)$ be as in (1) with $k \geq 2$, and let $G(x)$ be a 0, 1-polynomial with the same number of terms as $F(x)$ satisfying

$$F(x)\tilde{F}(x) = G(x)\tilde{G}(x). \quad (3)$$

Since $G(x) = F(x)$ satisfies (3), we know such a $G(x)$ exists. We show that for the majority of the exponent vectors $\vec{n}$, the equation (3) implies that $G(x) \in \{F(x), \tilde{F}(x)\}$. Lemma 2 will then imply that the majority of the vectors $\vec{n}$ are such that either the non-reciprocal part of $F(x)$ is irreducible or the non-reciprocal part of $F(x)$ is 1. It will then remain to bound the number of vectors $\vec{n}$ such that the non-reciprocal part of $F(x)$ is 1.

From (1) and (3), we have $F(0) = G(0) = 1$. Write $F(x) = \sum_{i=0}^k x^{n_i}$ and $G(x) = \sum_{i=0}^k x^{m_i}$, where $0 = n_0 < n_1 < \dots < n_k \leq N$ and $0 = m_0 < m_1 < \dots < m_k$. Set $d = n_k$. From (3), we deduce that

$$m_k = n_k = d. \quad (4)$$

We then see that

$$\tilde{F}(x) = \sum_{i=0}^k x^{d-n_i} \quad \text{and} \quad \tilde{G}(x) = \sum_{i=0}^k x^{d-m_i},$$

where here the monomials show up in descending degree order.

With the above notation, we have that the second largest degree of a monomial on the left-hand side of (3) is either $2d - n_1$ or $n_{k-1} + d$. Observe that if these two values are equal, then $n_1 + n_{k-1} = d = n_k$, and the total number of vectors $\vec{n} = \langle n_1, \dots, n_k \rangle$ satisfying this equation is at most N^{k-1} . The quantity N^{k-1} is small compared to the total number of possibilities for $F(x)$ as in (1), which is $\binom{N}{k}$ with k fixed. So we restrict now to the case that $2d - n_1 \neq n_{k-1} + d$. We will use this idea again, that if we have a linear combination of the $n_1, \dots, n_k$, with coefficients not all 0, with the linear combination equal to 0, then the vectors $\vec{n}$ satisfying this equation account for $O(N^{k-1})$ of the $\binom{N}{k}$ different $F(x)$ in (1).

Next, we note that we can suppose that the second largest degree of a monomial on the left-hand side of (3) is $2d - n_1$. Otherwise, we can redefine the n_i by

interchanging the roles of $F(x)$ and $\tilde{F}(x)$ so that equation (1) still holds and the second largest degree of a monomial on the left-hand side of (3) is $2d - n_1$, as desired. Similarly, by interchanging the roles of $G(x)$ and $\tilde{G}(x)$ if need be, we can suppose that the second largest degree of a monomial on the right-hand side of (3) is $2d - m_1$. Doing so, we deduce then that $n_1 = m_1$ or, equivalently, that

$$n_k - n_1 = m_k - m_1. \quad (5)$$

The goal is to show that for all but $O_k(N^{k-1})$ vectors $\vec{n}$, the remaining $m_k - m_i$, with $2 \leq i \leq k-1$, satisfy

$$m_k - m_i = n_k - n_i.$$

This will then demonstrate, since (4) holds, that $G(x) = F(x)$.

Suppose there is some $i \in \{2, \dots, k-1\}$ such that $m_k - m_i \neq n_k - n_i$. Since the product on the right-hand side of (3) will include a term of degree $m_k - m_i$ which also must appear on the left-hand side of (3), we deduce that there exist $(g, h) \neq (k, i)$ such that $g > h$ and

$$m_k - m_i = n_g - n_h. \quad (6)$$

Here, it is possible that $n_h = n_0 = 0$. We consider the possibility that $g \neq k$ in (6). Either $n_h \neq n_1$ or $n_h \neq n_0 = 0$. If $n_h \neq n_1$, then taking the difference of (5) and (6), we find that

$$m_i - m_1 = n_k + n_h - n_g - n_1. \quad (7)$$

Here, we have $k > g > h$ and $n_1 \notin \{n_h, n_k\}$, so the right-hand side of (7) is a linear combination of at least 3 distinct n_i . There is some term on the right-hand side of (3) of degree $d + m_i - m_1$ which must equal a term on the left-hand side of (3) of degree $d + n_u - n_v$ for some u and v , so that the left-hand side of (7) can be replaced by a difference in two components of $\vec{n}$. As noted earlier, the resulting equation in the n_i implies there are $O_k(N^{k-1})$ vectors $\vec{n}$ for which $n_h \neq n_1$ in (6).

With still $g \neq k$, we suppose now $n_h \neq n_0$ or, equivalently, $h \neq 0$. In this case, we take the difference of (4) and (6), leading to (7) but with m_1 and n_1 replaced by m_0 and n_0 , respectively. Proceeding as we did for $n_h \neq n_1$, we deduce again that there are $O_k(N^{k-1})$ vectors $\vec{n}$ for which $n_h \neq n_0$ in (6).

We can deduce now that for all but $O_k(N^{k-1})$ vectors $\vec{n}$, if (6) holds for some $i \in \{2, \dots, k-1\}$ and some g and h , then we must have $g = k$. Recalling (4) and (5), we deduce then that, except for $O_k(N^{k-1})$ exceptions of the $\vec{n}$, for each $m_k - m_i$ with $i \in \{0, 1, \dots, k-1\}$, there is an $h \in \{0, 1, \dots, k-1\}$ such that $m_k - m_i = n_k - n_h$. The inequalities

$$m_k - m_0 > \dots > m_k - m_{k-1} \quad \text{and} \quad n_k - n_0 > \dots > n_k - n_{k-1}$$

now imply that, outside $O_k(N^{k-1})$ exceptions, we have $m_i = n_i$ for every $i \in \{0, 1, \dots, k-1\}$, implying $G(x) = F(x)$.

Lemma 2 implies now that for all but $O_k(N^{k-1})$ of the vectors $\vec{n}$, either the non-reciprocal part of $F(x)$ is irreducible or the non-reciprocal part of $F(x)$ is 1. It remains to bound the number of vectors $\vec{n}$ such that the non-reciprocal part of $F(x)$ is 1. However, if the non-reciprocal part of $F(x)$ is 1, then $F(x)$ is necessarily reciprocal so that $n_k - n_{k-1} = n_1$. Thus, the non-reciprocal part of $F(x)$ is 1 for at most $O(N^{k-1})$ vectors $\vec{n}$. Lemma 1 follows.

3. Preliminary Information for Analyzing Reciprocal Factors

For an integer n and a positive integer d , we use the notation $n \bmod d$ to refer to the unique integer $a \in \{0, 1, \dots, d-1\}$ such that $n \equiv a \pmod{d}$. The following lemma is a variation of a lemma in [12] (see also [11]).

Lemma 3. *Let k and N be positive integers. Let $\varepsilon = \varepsilon(k, N) \in (0, 1/2]$. Set $\kappa = \lfloor 1/\varepsilon \rfloor + 1$ and*

$$V(k) = \max \left\{ \frac{\kappa^{2k-2}}{2} \left(\varepsilon - \frac{1}{\kappa} \right)^{-1}, \kappa^{k-1} + \varepsilon \right\}.$$

If $n_1, n_2, \dots, n_k$ are nonnegative integers satisfying $n_1 < n_2 < \dots < n_k \leq N$ and $n_k \geq V(k)$, then there exists an integer

$$d \in \left(\frac{n_k}{\kappa^{k-1} + \varepsilon}, \frac{n_k}{1 - \varepsilon} \right) \quad (8)$$

such that $n_j \bmod d$ is in $[0, \varepsilon d) \cup ((1 - \varepsilon)d, d)$ for every $j \in \{1, 2, \dots, k\}$.

Proof. For $k = 1$, we have $n_k \geq V(k) \geq \kappa^{k-1} + \varepsilon > 1$, so we can take $d = n_k$. We consider now the case that $k > 1$. Since $\varepsilon \leq 1/2$, we have $\kappa = \lfloor 1/\varepsilon \rfloor + 1 \geq 3$. By the definition of κ , we have $\kappa > 1/\varepsilon$ or, equivalently, $\varepsilon > 1/\kappa$. The condition $n_k \geq V(k)$ implies that

$$\frac{n_k}{\kappa^{k-1} + \varepsilon} \geq 1 \quad \text{and} \quad \sqrt{2n_k} \left(\varepsilon - \frac{1}{\kappa} \right)^{1/2} \geq \kappa^{k-1}. \quad (9)$$

Note that the conditions in the lemma and $k > 1$ imply that d exists as in (8) since, by the first inequality in (9), the interval in (8) has length

$$\frac{n_k(\kappa^{k-1} + 2\varepsilon - 1)}{(\kappa^{k-1} + \varepsilon)(1 - \varepsilon)} \geq \frac{\kappa + 2\varepsilon - 1}{1 - \varepsilon} \geq 2 \cdot \frac{1 + \varepsilon}{1 - \varepsilon} > 1.$$

To establish the lemma, it suffices to show that there is an integer d satisfying (8) and integers $w_1, w_2, \dots, w_k$ such that

$$|n_j - w_j d| < \varepsilon d \quad \text{for } 1 \leq j \leq k. \quad (10)$$

Let $x_j = n_j/n_k$ for $j \in \{1, 2, \dots, k\}$. We explain next how the Dirichlet box principle implies that there is a positive integer $t \leq \kappa^{k-1}$ satisfying

$$\|tx_j\| < \frac{1}{\kappa} \quad \text{for } 1 \leq j \leq k-1, \quad (11)$$

where $\|x\|$ denotes the distance from x to the nearest integer. For each $t' \in \{1, 2, \dots, \kappa^{k-1} + 1\}$, we define the point

$$P(t') = (\{t'x_1\}, \{t'x_2\}, \dots, \{t'x_{k-1}\}),$$

with coordinates in the interval $[0, 1)$, where $\{t'x_j\}$ denotes the fractional part of $t'x_j$. For each of the κ^{k-1} choices of $u_j \in \{0, 1, \dots, \kappa-1\}$, where $1 \leq j \leq k-1$, we consider the cube

$$\mathcal{C}(u_1, \dots, u_{k-1}) = \{(s_1, s_2, \dots, s_{k-1}) : u_j/\kappa \leq s_j < (u_j + 1)/\kappa \text{ for } 1 \leq j \leq k-1\}.$$

By the Dirichlet box principle, there are t'_1 and t'_2 in $\{1, 2, \dots, \kappa^{k-1} + 1\}$ with $t'_1 > t'_2$ such that the points $P(t'_1)$ and $P(t'_2)$ are both in the same cube $\mathcal{C}(u_1, \dots, u_{k-1})$. Set $t = t'_1 - t'_2 \in \{1, 2, \dots, \kappa^{k-1}\}$. For every $j \in \{1, 2, \dots, k-1\}$, we obtain

$$tx_j = t'_1x_j - t'_2x_j = \lfloor t'_1x_j \rfloor - \lfloor t'_2x_j \rfloor + \{t'_1x_j\} - \{t'_2x_j\}.$$

It follows that each such tx_j is within $|\{t'_1x_j\} - \{t'_2x_j\}| < 1/\kappa$ of the integer $\lfloor t'_1x_j \rfloor - \lfloor t'_2x_j \rfloor$. This establishes (11). Since $x_k = 1$, we see that (11) holds with $j = k$ as well. Observe that (9) implies that

$$t \leq \sqrt{2n_k} \left(\varepsilon - \frac{1}{\kappa} \right)^{1/2}. \quad (12)$$

For $1 \leq j \leq k$, take w_j to be the nearest integer to tx_j .

For the moment, suppose $w_j \neq 0$ (so that $w_j \geq 1$) for each $j \in \{1, 2, \dots, k\}$. Then (10) follows provided

$$\frac{d}{n_k} \in \bigcap_{1 \leq j \leq k} \left(\frac{x_j}{w_j + \varepsilon}, \frac{x_j}{w_j - \varepsilon} \right).$$

Recall that $\varepsilon > 1/\kappa$. For each $j \in \{1, 2, \dots, k\}$, since $tx_j \leq t$ so that $w_j \leq t$, we deduce from (11) that

$$\frac{t + (1/\kappa)}{t + \varepsilon} \geq \frac{w_j + (1/\kappa)}{w_j + \varepsilon} > \frac{tx_j}{w_j + \varepsilon}$$

and

$$\frac{t - (1/\kappa)}{t - \varepsilon} \leq \frac{w_j - (1/\kappa)}{w_j - \varepsilon} < \frac{tx_j}{w_j - \varepsilon}.$$

Hence, (10) holds provided

$$\frac{d}{n_k} \in \left(\frac{t + (1/\kappa)}{t(t + \varepsilon)}, \frac{t - (1/\kappa)}{t(t - \varepsilon)} \right). \quad (13)$$

Using (12), we see that the length of the interval on the right is

$$\frac{2}{t^2 - \varepsilon^2} \left(\varepsilon - \frac{1}{\kappa} \right) > \frac{2}{t^2} \left(\varepsilon - \frac{1}{\kappa} \right) \geq \frac{1}{n_k}$$

so that d exists satisfying (13). From (13) and $t \in \{1, 2, \dots, \kappa^{k-1}\}$, we see that

$$\frac{d}{n_k} > \frac{t + (1/\kappa)}{t(t + \varepsilon)} > \frac{1}{t + \varepsilon} \geq \frac{1}{\kappa^{k-1} + \varepsilon}$$

and

$$\frac{d}{n_k} < \frac{t - (1/\kappa)}{t(t - \varepsilon)} < \frac{1}{t - \varepsilon} \leq \frac{1}{1 - \varepsilon}.$$

Thus, we also see that (8) holds.

Now, suppose some $w_j = 0$ with $j \in \{1, 2, \dots, k\}$. We again choose d so that (13) holds and, hence, (8) as well. For each $w_j \neq 0$, the above argument gives $|n_j - w_j d| < \varepsilon d$ as in (10). On the other hand, if $w_j = 0$, then (11) and the definitions of w_j , x_j , and d imply

$$\kappa t n_j < n_k < d \frac{t(t + \varepsilon)}{t + (1/\kappa)} \leq \kappa \varepsilon t d.$$

Hence, (10) holds for such w_j as well, completing the proof. $\square$

The above lemma serves the same purpose as Lemma 1 in [21], where instead Schinzel makes use of work of E. Bombieri and J. D. Vaaler [6] and of E. Hlawka [13].

We will want to make use of the *Newton polytope* (or *Newton polyhedron*) associated with a multivariate polynomial, so we briefly discuss this topic next. Let $x_1, \dots, x_r$ be indeterminates, and let $P(x_1, \dots, x_r) \in K[x_1, \dots, x_r]$ be a polynomial in r variables over a field K . We write

$$P(x_1, \dots, x_r) = \sum_{i=1}^s \alpha_i \prod_{j=1}^r x_j^{c_{ij}},$$

where $\alpha_i \in K \setminus \{0\}$ and $c_{i,j} \in \mathbb{Z}^+ \cup \{0\}$. Define the points $p_i = (c_{i1}, \dots, c_{ir})$, for $1 \leq i \leq s$. The *Newton polytope associated with* $P(x_1, \dots, x_r)$ is the convex hull of the points p_i , which can be written as

$$\mathcal{N}(P) = \left\{ \sum_{i=1}^s t_i p_i : t_i \in [0, 1], \sum_{i=1}^s t_i = 1 \right\},$$

where scalar multiplication and addition of points is performed coordinate-wise in the same way as vectors. In the case of two variables where $r = 2$, the boundary of the convex hull $\mathcal{N}(P)$ is referred to as the *Newton polygon* associated with $P(x_1, \dots, x_r)$.

A classical result for Newton polytopes due to A. M. Ostrowski [19] is the following (cf. Theorem 18, p. 89, of [23]).

Lemma 4 (Ostrowski, 1975). *If $P(x_1, \dots, x_r)$ and $Q(x_1, \dots, x_r)$ are two non-zero polynomials in $K[x_1, \dots, x_r]$, then*

$$\mathcal{N}(PQ) = \mathcal{N}(P) + \mathcal{N}(Q),$$

where the sum on the right is the Minkowski sum defined by

$$\mathcal{N}(P) + \mathcal{N}(Q) = \{p + q : p \in \mathcal{N}(P), q \in \mathcal{N}(Q)\}.$$

Next, we provide another well-known result pertaining to the Minkowski sum of two convex polytopes in $\mathbb{R}^2$ (see for example Theorem 13.5 and its proof in [4]). To describe the result, it is helpful to give some terminology for the edges (sides) of a polytope in $\mathbb{R}^2$. We say an edge of a polytope is a lower (an upper) edge if the polytope lies on or above (on or below) the line formed by extending that edge. It is also possible that an edge is a vertical line segment, and we say an edge is a left vertical (a right vertical) edge if the polytope lies on or to the right of (on or to the left of) the line formed by extending that edge. Finally, in the context of Newton polytopes in $\mathbb{R}^2$, it is possible that a polytope is a line segment. In this case, we view the polytope as having two edges, a lower edge and an upper edge (or a left vertical edge and a right vertical edge). Note that some types of edges may not exist for a given polytope. For example, if a polytope is just a vertical line segment, then it has a left vertical edge and a right vertical edge but does not have lower or upper edges. The following result describes the Minkowski sum of two polytopes in $\mathbb{R}^2$ in terms of translates of the edges of the two polytopes.

Lemma 5. *If $P(x_1, x_2)$ and $Q(x_1, x_2)$ are two non-zero polynomials in $K[x_1, x_2]$, then the boundary of the Minkowski sum $\mathcal{N}(P) + \mathcal{N}(Q)$ can be formed by translating the edges of $\mathcal{N}(P)$ and $\mathcal{N}(Q)$ in such a way that the lower (upper, left vertical, right vertical) edges along $\mathcal{N}(P)$ and $\mathcal{N}(Q)$ are translated to form the lower (upper, left vertical, right vertical, respectively) edges along $\mathcal{N}(P) + \mathcal{N}(Q)$ without overlapping and with the slopes of the edges of $\mathcal{N}(P) + \mathcal{N}(Q)$ increasing (decreasing, undefined, undefined, respectively) going from left to right.*

To clarify, if a lower (upper, left vertical, right vertical) edge of length ℓ_1 on $\mathcal{N}(P)$ is parallel to a lower (upper, left vertical, right vertical) edge of length ℓ_2 on $\mathcal{N}(Q)$, then they are translated to form a lower (upper, left vertical, right vertical) edge of length $\ell_1 + \ell_2$ on $\mathcal{N}(P) + \mathcal{N}(Q)$. In Figure 1, we illustrate Lemmas 4 and 5 with an example of two Newton polytopes and their Minkowski sum.

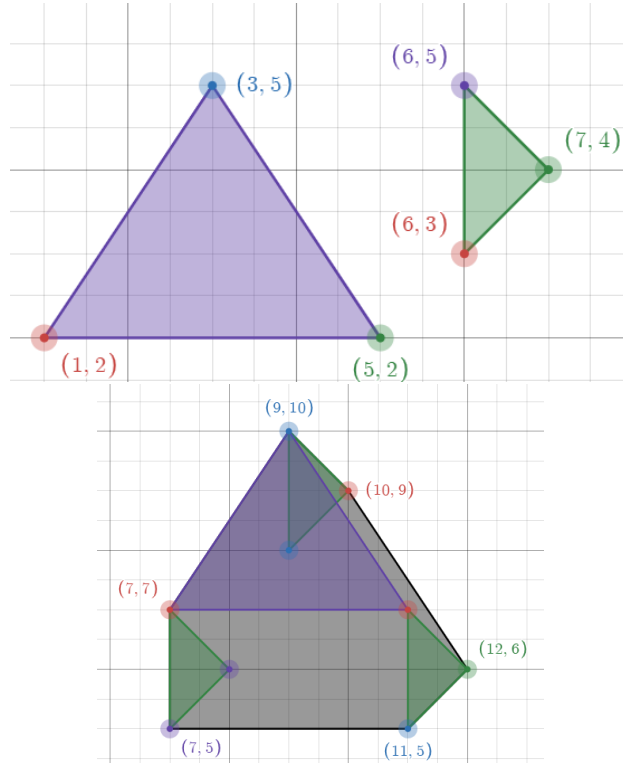


Figure 1: Figure: The Newton Polytopes for $P(x, y) = xy^2 + x^5y^2 + x^3y^5$, $Q(x, y) = x^6y^3 + x^7y^4 + x^6y^5$ and $P(x, y) \cdot Q(x, y)$

4. Finishing the Proof of Theorem 2

As a result of Lemma 1, to complete the proof of Theorem 2, we show there are $O_k(N^{k-(1/(2k+1))})$ polynomials $F(x)$ as in (1) with $n_k \leq N$ for which $F(x)$ has an irreducible non-cyclotomic reciprocal factor. We take $k \geq 2$ to be fixed and view N as sufficiently large compared to k . The conditions in Lemma 3 require $V(k) \leq n_k \leq N$ so that, in particular, to use the lemma, we will want

$$N \geq V(k) = \max \left\{ \frac{\kappa^{2k-2}}{2} \left(\varepsilon - \frac{1}{\kappa} \right)^{-1}, \kappa^{k-1} + \varepsilon \right\}. \quad (14)$$

A hurdle to overcome is how small the difference of ε and $1/\kappa$ is as this difference appears on the right-hand side of (14). We take $\varepsilon = 1/(\lfloor N^{1/(2k+1)} \rfloor - 1)$. Then

$$\kappa = \lfloor 1/\varepsilon \rfloor + 1 = \lfloor N^{1/(2k+1)} \rfloor \sim N^{1/(2k+1)}, \quad (15)$$

as $N \rightarrow \infty$, and we obtain

$$\varepsilon - \frac{1}{\kappa} = \frac{1}{(\lfloor N^{1/(2k+1)} \rfloor - 1) \lfloor N^{1/(2k+1)} \rfloor} \geq \frac{1}{(N^{1/(2k+1)} - 1) N^{1/(2k+1)}} > \frac{1}{N^{2/(2k+1)}}.$$

It follows that

$$\frac{\kappa^{2k-2}}{2} \left(\varepsilon - \frac{1}{\kappa} \right)^{-1} < \frac{\lfloor N^{1/(2k+1)} \rfloor^{2k-2}}{2} N^{2/(2k+1)} \leq \frac{N^{2k/(2k+1)}}{2} < N^{2k/(2k+1)}.$$

Since $k \geq 2$ is fixed and N is sufficiently large, we see that

$$\kappa^{k-1} + \varepsilon \leq \lfloor N^{1/(2k+1)} \rfloor^{k-1} + \frac{1}{(\lfloor N^{1/(2k+1)} \rfloor - 1)} \leq \sqrt{N} < N^{2k/(2k+1)}.$$

Thus, with $\varepsilon = 1/(\lfloor N^{1/(2k+1)} \rfloor - 1)$, we obtain that $V(k) < N^{2k/(2k+1)}$ and (14) follows. With ε as above, we discard from consideration the at most $V(k)^k < N^{2k^2/(2k+1)} = N^k N^{-k/(2k+1)}$ vectors $\vec{n}$ for which $n_k < V(k)$, noting that there are $O_k(N^{k-k/(2k+1)})$, as $N \rightarrow \infty$, such vectors $\vec{n}$.

We consider now vectors $\vec{n}$ with $1 \leq n_1 < \dots < n_k \leq N$ and $n_k \geq V(k)$. By Lemma 3, with k fixed and N large, there is a positive integer d and integers m_j and t_j such that

$$n_j = m_j d + t_j \quad \text{and} \quad |t_j| < \varepsilon d < \frac{1.01d}{N^{1/(2k+1)}}, \quad (16)$$

for all $j \in \{1, \dots, k\}$. Also, from (8) and our choice of ε , we choose, as we may, d so that

$$\frac{n_k}{N^{(k-1)/(2k+1)}} \ll \frac{n_k}{\kappa^{k-1} + \varepsilon} < d < 1.01n_k. \quad (17)$$

Define

$$m' = \max_{1 \leq j \leq k} \{m_j\} = m_k, \quad t' = \max\{0, t_1, \dots, t_k\} \quad \text{and} \quad t'' = -\min\{0, t_1, \dots, t_k\}.$$

Since k is fixed and N is large, we deduce from (15), (16) and (17) that

$$m' < \frac{n_k}{d} + 1 < \kappa^{k-1} + 1 + \varepsilon \ll \sqrt{N},$$

$$\max\{t', t''\} < \frac{1.01d}{N^{1/(2k+1)}} < \frac{1.03N}{N^{1/(2k+1)}} = 1.03 N^{2k/(2k+1)},$$

and

$$m' \cdot \max\{t', t''\} < \left(\frac{N}{d} + 1 \right) \frac{1.01d}{N^{1/(2k+1)}} < 2.04 N^{2k/(2k+1)}.$$

Following a key idea of Schinzel's in [21], we define

$$\begin{aligned} G(y, z) &= y^{t''} + \sum_{j=1}^k y^{t_j+t''} z^{m_j} \in \mathbb{Z}[y, z], \\ H(y, z) &= y^{t'} z^{m'} + \sum_{j=1}^k y^{t'-t_j} z^{m'-m_j} \in \mathbb{Z}[y, z]. \end{aligned} \tag{18}$$

A significant motivation here is that $G(x, x^d) = x^{t''} F(x)$ and $H(x, x^d) = x^a \tilde{F}(x)$, where a is a nonnegative integer and $\tilde{F}(x) = x^{\deg F} F(1/x) = x^{n_k} F(1/x)$. In particular, if $g(x) \in \mathbb{Z}[x]$ is a monic reciprocal factor of $F(x)$, then $g(x)$ is a factor of both $G(x, x^d)$ and $H(x, x^d)$.

For a polynomial $P(y, z) \in \mathbb{Z}[y, z]$, let $\deg_y P$ and $\deg_z P$ denote the degree of $P(y, z)$ in y and the degree of $P(y, z)$ in z , respectively. Momentarily, we will make use of the inequality

$$(\deg_y G)(\deg_z H) + (\deg_z G)(\deg_y H) \leq 2(t' + t'')m' < 9N^{2k/(2k+1)}. \tag{19}$$

We are now in a position to prove the following lemma, which is a simplified version of Lemma 2 from [21].

Lemma 6. *Let $F(x)$ be as in (1) with $k \geq 3$ and $V(k) \leq n_k \leq N$. If $g(x)$ is an irreducible reciprocal factor of $F(x)$ in $\mathbb{Z}[x]$, then either*

$$\deg g < 9N^{2k/(2k+1)} \tag{20}$$

or there exist four distinct nonnegative indices $i, j, u, v \leq k$ such that

$$\begin{vmatrix} n_i - n_j & m_i - m_j \\ n_u - n_v & m_u - m_v \end{vmatrix} = 0. \tag{21}$$

Proof. Note that we can take $g(x)$ to be monic since $F(x)$ is monic. Let

$$D(y, z) = \gcd(G(y, z), H(y, z)),$$

where the greatest common divisor is taken over $\mathbb{Z}[y, z]$. One can justify that this is the same as the greatest common divisor taken over $\mathbb{Q}[y, z]$, but this is not needed. We consider two cases, depending on whether $D(y, z)$ is a constant or not. Since $g(x)$ is a monic reciprocal factor of $F(x)$, we have $g(x)$ is a factor of both $G(x, x^d)$ and $H(x, x^d)$. Thus, either $g(x) \mid D(x, x^d)$ or $g(x)$ divides both $G(x, x^d)/D(x, x^d)$ and $H(x, x^d)/D(x, x^d)$.

We consider first the case that $D(y, z)$ is a constant. For a root ξ of $g(x)$, we see that

$$G(\xi, \xi^d) = 0 = H(\xi, \xi^d).$$

Since $D(y, z)$ is a constant, the resultant of $G(y, z)$ and $H(y, z)$, with respect to z , say, is a non-zero polynomial $R(y)$. Furthermore, there exist two non-zero polynomials $A(y, z)$ and $B(y, z)$ in $\mathbb{Z}[y, z]$ such that

$$A(y, z)G(y, z) + B(y, z)H(y, z) = R(y).$$

The substitution $y = \xi$ and $z = \xi^d$ shows that ξ is a root of $R(y)$ so that $\deg_y R$ is a bound on $\deg g$. The definition of the resultant (or its equivalent form as the determinant of a Sylvester matrix) together with (19) implies

$$\deg_y R \leq (\deg_y G)(\deg_z H) + (\deg_z G)(\deg_y H) < 9N^{2k/(2k+1)}.$$

We deduce that (20) holds.

Now, we consider the case that $D(y, z)$ is not a constant. We appeal to Lemmas 4 and 5. Since $D(y, z)$ is a factor of $G(y, z)$ and $H(y, z)$, these lemmas imply that either a left vertical edge or a lower edge (whichever exists, possibly both), say $\mathcal{E}$, of $\mathcal{N}(D)$ can be translated to form part (or all) of an edge of a left vertical or a lower edge of $\mathcal{N}(G)$ and of $\mathcal{N}(H)$. On the other hand, the definition of $G(y, z)$ and $H(y, z)$ in (18) implies that $\mathcal{N}(G)$ is a translation of the reflection of $\mathcal{N}(H)$ about the origin. This reflection takes a left vertical edge or a lower edge of $\mathcal{N}(H)$ to a parallel right vertical or parallel upper edge on the reflection of $\mathcal{N}(H)$. We deduce then that $\mathcal{N}(G)$ consists of two edges parallel to $\mathcal{E}$, either a left and right vertical edge or a lower and upper edge. The idea is to deduce then that we can find 4 distinct points along the edges of $\mathcal{N}(G)$, which we call $(t_i, m_i), (t_j, m_j), (t_u, m_u)$ and (t_v, m_v) , such that the edge through (t_i, m_i) and (t_j, m_j) is parallel to the edge through (t_u, m_u) and (t_v, m_v) . What needs a little bit of care for this deduction is the case that $\mathcal{N}(G)$ is a line segment. However, as a condition in the lemma, we have $k \geq 3$ which in turn implies from (18) that $\mathcal{N}(G)$ is the convex hull of at least 4 distinct points arising from the degrees of y and z in the monomials in $G(y, z)$. If $\mathcal{N}(G)$ is a line segment, then we can deduce that there are at least 4 points on this line segment, and labeling them as $(t_i, m_i), (t_j, m_j), (t_u, m_u)$ and (t_v, m_v) , we arrive at the same conclusion as above, that the edge through (t_i, m_i) and (t_j, m_j) is parallel to the edge through (t_u, m_u) and (t_v, m_v) . We deduce

$$\begin{vmatrix} t_i - t_j & m_i - m_j \\ t_u - t_v & m_u - m_v \end{vmatrix} = 0.$$

For each $e \in \{i, j, u, v\}$, from (16), we have $t_e = n_e - m_e d$, and now (21) follows. $\square$

The above lemma will be used to restrict the possibilities for the vector $\vec{n}$ when $k \geq 3$. For the purposes of establishing the main result in [14], there is no harm in restricting to $k \geq 3$. However, we can refer to the literature to resolve the remaining case where $k = 2$ in Theorem 2. In this case, the polynomial $F(x)$ is a 0, 1-polynomial having 3 terms, and independent work of W. Ljunggren [16] and

H. A. Tverberg [24] implies that $F(x)$ removed of its cyclotomic factors is irreducible or 1. In the latter case, the non-reciprocal part of $F(x)$ is 1, and we already showed at the end of Section 2 that there are at most $O(N^{k-1})$ such $F(x)$. This then is sufficient for addressing the case that $k = 2$ in Theorem 2.

We begin taking advantage of Lemma 6 by making use of a recent result of V. Dimitrov [8] (see also J. F. McKee and C. J. Smyth [17] and W. Zudilin [25]) resolving the Schinzel–Zassenhaus conjecture. This will allow us to address the possibility that an irreducible non-cyclotomic reciprocal factor $g(x)$ of $F(x)$ satisfies (20). Before doing so, however, we point out that one could obtain sufficient information for handling the case of (20) by instead using a result of E. Dobrowolski [9], which is how Schinzel addressed $g(x)$ having a similar degree bound in [21]. The use of [9] would cost an extra factor of a power of $\log N$ in our count of polynomials having an irreducible non-cyclotomic reciprocal factor. The choice of using Dimitrov’s result is for convenience (the argument is a little shorter) and to emphasize the utility of this excellent work.

Dimitrov’s result in [8] implies that if $g(x)$ is an irreducible non-cyclotomic polynomial satisfying (20), then there is a root ξ of $g(x)$ satisfying

$$|\xi| \geq 2^{1/(4b)}, \quad \text{where } b = 9N^{2k/(2k+1)} \geq \deg g. \quad (22)$$

This leads to the following.

Lemma 7. *If $F(x)$ has an irreducible non-cyclotomic factor $g(x)$ satisfying (20), then*

$$n_k - n_{k-1} \leq \frac{36 \log k}{\log 2} N^{2k/(2k+1)}. \quad (23)$$

Proof. Since $g(x)$ is a factor of $F(x)$, there is a root ξ of $g(x)$ and, hence, $F(x)$ satisfying

$$\xi^{n_k} = -\xi^{n_{k-1}} - \dots - 1,$$

where ξ is as in (22). By the triangle inequality, we obtain

$$|\xi|^{n_k} \leq k|\xi|^{n_{k-1}}.$$

Taking logarithms of both sides, we see that

$$n_k - n_{k-1} \leq \frac{\log k}{\log |\xi|} \leq \frac{4b \log k}{\log 2} = \frac{36 \log k}{\log 2} N^{2k/(2k+1)},$$

completing the proof. $\square$

The conditions on $g(x)$ in Lemma 6 and Lemma 7 are different, but we are interested in their commonality, where $g(x)$ is an irreducible non-cyclotomic reciprocal factor of $F(x)$. We note that Lemma 7 is the crucial place where we are taking into

account that $g(x)$ is not cyclotomic. Other aspects of the arguments in this section apply even if $g(x)$ is cyclotomic.

We immediately see that (23) happens for a vanishing proportion of vectors $\vec{n}$; there are at most N^{k-1} choices for the first $n_1, n_2, \dots, n_{k-1}$ coordinates and then $O_k(N^{2k/(2k+1)})$ for n_k . In particular, there are at most $O_k(N^{k-(1/(2k+1))})$ different $F(x)$ for which an irreducible non-cyclotomic reciprocal factor $g(x)$ can satisfy (20). Furthermore, an analogous argument allows us to say that for all but $O_k(N^{k-(1/(2k+1))})$ different $F(x)$ we have that no two of $n_1, \dots, n_k$ differ in absolute value by $O_k(N^{2k/(2k+1)})$ as N goes to infinity. Here, we have used that there are at most $\binom{k}{2}$ choices for two different n_j and the implied constant in the big- O symbol can be an arbitrarily large constant depending only on k . We will make more use of this bound on the number of $n_1, \dots, n_k$ with no two differing in absolute value by $O_k(N^{2k/(2k+1)})$ momentarily, but for now we deduce from (16) and (17) that for all but $O_k(N^{k-(1/(2k+1))})$ polynomials $F(x)$ as in (1) with $n_k \leq N$, the values of $m_1, \dots, m_k$ are distinct. More specifically, if some $m_i = m_j$ with $1 \leq i < j \leq k$, then (16) and (17) imply

$$0 < n_j - n_i \leq |t_j| + |t_i| < \frac{2.02d}{N^{1/(2k+1)}} \leq \frac{3N}{N^{1/(2k+1)}} \ll N^{2k/(2k+1)},$$

which occurs for $O_k(N^{k-(1/(2k+1))})$ of the $F(x)$.

We restrict now to the case that $m_1, \dots, m_k$ are distinct and (21) holds. As we also know that $n_1, \dots, n_k$ are distinct, we obtain that the 4 entries on the left in (21) are all non-zero. From (21), we see that

$$(n_i - n_j)(m_u - m_v) = (n_u - n_v)(m_i - m_j). \quad (24)$$

We deduce now from (16) and (17) that

$$0 < |m_i - m_j| \leq \max\{|m_i|, |m_j|\} < \frac{n_k}{d} + 1 < \frac{3n_k}{d} \ll N^{(k-1)/(2k+1)}.$$

The same lower and upper bounds hold on $|m_u - m_v|$. On the other hand, we see from (24) that $(n_i - n_j)/\gcd(n_i - n_j, n_u - n_v)$ divides $m_i - m_j$ and that also $(n_u - n_v)/\gcd(n_i - n_j, n_u - n_v)$ divides $m_u - m_v$. Given the bounds on $|m_i - m_j|$ and $|m_u - m_v|$, we deduce that

$$\frac{\max\{|n_i - n_j|, |n_u - n_v|\}}{\gcd(|n_i - n_j|, |n_u - n_v|)} \ll N^{(k-1)/(2k+1)}. \quad (25)$$

From (25), we see that either

$$\gcd(|n_i - n_j|, |n_u - n_v|) \geq N^{(k+1)/(2k+1)} \quad (26)$$

or

$$\max\{|n_i - n_j|, |n_u - n_v|\} \ll N^{2k/(2k+1)}. \quad (27)$$

In the case of (27), we have $|n_i - n_j| \ll N^{2k/(2k+1)}$ so that, by our earlier comments, we deduce there are at most $O_k(N^{k-(1/(2k+1))})$ polynomials $F(x)$ as in (1) with $n_k \leq N$ and (27) holding for some i, j, u and v as above. In the case of (26), we see that there are at most N^{k-2} choices for

$$\{n_1, \dots, n_k\} \setminus \{n_j, n_v\},$$

and, given $n_k \leq N$, there are at most N choices for $\gcd(|n_i - n_j|, |n_u - n_v|)$. Given these, we deduce from (26) that there are $O_k(N/N^{(k+1)/(2k+1)}) = O_k(N^{k/(2k+1)})$ choices for n_j and $O(N^{k/(2k+1)})$ choices for n_v . Hence, at most $O_k(N^{k-(1/(2k+1))})$ polynomials $F(x)$ are as in (1) with $n_k \leq N$ and (26) holding for some i, j, u and v as above.

In conclusion, there are $O_k(N^{k-(1/(2k+1))})$ polynomials as in Lemma 6 with $g(x)$ an irreducible non-cyclotomic reciprocal polynomial. This completes the proof of Theorem 2.

5. A Conjecture Associated with Lemma 2

It would be of some interest to establish, in the direction of the conjecture of Odlyzko and Poonen [18], that almost all of the 2^N polynomials of the form (1), with $0 \leq k \leq N$ and $n_k \leq N$, have an irreducible non-reciprocal part. This would easily follow from Lemma 2 if one can show the following.

Conjecture 1. Let $A \subseteq \{0, 1, 2, \dots, n\}$ with $0 \in A$. Consider the function ϕ defined for all such A , sending A into the multiset with $|A|^2$ elements given by

$$A - A = \{x - y : x, y \in A\}.$$

Then the image of ϕ contains $2^{n-1} + o(2^n)$ distinct elements as $n \rightarrow \infty$.

Observe that if A is as in the conjecture and a' is the maximum element of A , then the set

$$A' = \{a' - a : a \in A\}$$

is such that the multisets $A - A$ and $A' - A'$ are identical. Furthermore, $A' \subseteq \{0, 1, 2, \dots, n\}$ with $0 \in A'$. The conjecture is claiming that an element in the image of ϕ almost always determines the pair A and A' . If we view A as the set of exponents of x in $F(x)$ (including 0) in (1), then A' corresponds to the set of exponents of x in the reciprocal $\tilde{F}(x)$.

Lemma 2 implies that Conjecture 1 follows from the Odlyzko–Poonen conjecture. Conjecture 1 is also true under the extended Riemann hypothesis, through the roundabout argument of linking it to the conditional resolution of the Odlyzko–Poonen conjecture by Breuillard and Varjú [7]. The objective then would be to give an unconditional proof of Conjecture 1 and hopefully one that is elementary and more intrinsic to the conjecture.

References

- [1] L. Bary-Soroker, D. Hokken, G. Kozma, and B. Poonen, Irreducibility of Littlewood polynomials of special degrees, *Int. Math. Res. Not. IMRN* **21** (2025), Paper No. rnaf326, 5 pp.
- [2] L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma, Irreducibility of random polynomials: general measures, *Invent. Math.* **233** (2023), 1041–1120.
- [3] L. Bary-Soroker and G. Kozma, Irreducible polynomials of bounded height, *Duke Math. J.* **169** (2020), 579–598.
- [4] M. de Berg, O. Cheong, M. van Kreveld, and M. Overmars, *Computational Geometry, Algorithms and Applications*, third edition, Springer-Verlag, Berlin, 2008.
- [5] E. Bombieri, D. Masser, and U. Zannier, Anomalous subvarieties—structure theorems and applications, *Int. Math. Res. Not. IMRN* **19** (2007), Paper No. rnm057, 33 pp.
- [6] E. Bombieri and J. D. Vaaler, On Siegel’s lemma, *Invent. Math.* **73** (1983), 11–32; Addendum to: “On Siegel’s lemma”, *Invent. Math.* **75** (1984), p. 377.
- [7] E. F. Breuillard and P. P. Varjú, Irreducibility of random polynomials of large degree, *Acta Math.* **223** (2019), 195–249.
- [8] V. Dimitrov, A proof of the Schinzel–Zassenhaus conjecture on polynomials, preprint, [arXiv: 1912.12545](https://arxiv.org/abs/1912.12545).
- [9] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34** (1979), 391–401.
- [10] M. Filaseta, On the factorization of polynomials with small Euclidean norm, In *Number Theory in Progress, Vol. 1 (Zakopane–Kościelisko, 1997)*, de Gruyter, Berlin, 1999, 143–163.
- [11] M. Filaseta, On the factorization of lacunary polynomials, *Acta Arith.* **210** (2023), 23–52.
- [12] M. Filaseta, K. Ford, and S. Konyagin, On an irreducibility theorem of A. Schinzel associated with coverings of the integers, *Illinois J. Math.* **44** (2000), 633–643.
- [13] E. Hlawka, Über Gitterpunkte in Zylindern, *Österreich. Akad. Wiss. Math.-Nat. Kl. S.-B. IIa* **156** (1948), 203–217.
- [14] A. Kalogirou, Irreducibility of lacunary polynomials with 0,1 coefficients, preprint, [arXiv: 2410.10035](https://arxiv.org/abs/2410.10035).
- [15] S. V. Konyagin, On the number of irreducible polynomials with 0, 1 coefficients, *Acta Arith.* **88** (1999), 333–350.
- [16] W. Ljunggren, On the irreducibility of certain trinomials and quadrimomials, *Math. Scand.* **8** (1960), 65–70.
- [17] J. F. McKee and C. J. Smyth, *Around the Unit Circle – Mahler Measure, Integer Matrices and Roots of Unity*, Universitext, Springer, Cham, 2021.
- [18] A. M. Odlyzko and B. Poonen, Zeros of polynomials with 0, 1 coefficients, *Enseign. Math.* **39** (1993), 317–348.
- [19] A. M. Ostrowski, On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms, *Aequationes Math.* **13** (1975), 201–228.
- [20] A. Schinzel, Reducibility of lacunary polynomials I, *Acta Arith.* **16** (1969), 123–159.

- [21] A. Schinzel, Reducibility of lacunary polynomials VII, *Monatsh. Math.* **102** (1986), 309–337.
- [22] A. Schinzel, Reducibility of lacunary polynomials XII, *Acta Arith.* **90** (1999), 273–289.
- [23] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, 77, Cambridge Univ. Press, Cambridge, 2000.
- [24] H. A. Tverberg, On the irreducibility of the trinomials $x^n \pm x^m \pm 1$, *Math. Scand.* **8** (1960), 121–126.
- [25] W. Zudilin, *Analytic Methods in Number Theory – When Complex Numbers Count*, Monographs in Number Theory, 11, World Sci. Publ., Hackensack, NJ, 2024.