CLASSES OF POLYNOMIALS HAVING ONLY ONE NON–CYCLOTOMIC IRREDUCIBLE FACTOR

A. Borisov, M. Filaseta*, T. Y. Lam**, and O. Trifonov

1. Introduction

In 1986, during the problem session at the West Coast Number Theory Conference, the second author stated the following:

Conjecture 1. *Let n be an integer ≥ 2, and let $f(x) = 1 + x + x^2 + \cdots + x^n$. Then $f'(x)$ is irreducible over the rationals.*

He noted then that the conjecture is true if $n = p - 1 \geq 2$ or if $n = p^r$ where p is a prime and r a positive integer. Calculations showed the conjecture also held for $n \leq 100$. Recently, in a study of more general polynomials, the first author [2] obtained further irreducibility results for $f(x)$; in particular, he established irreducibility in the case that $n + 1$ is a squarefree number ≥ 3 and in the case that $n = 2p - 1$ where p is prime.

The third author independently observed that $f^{(k)}(x)$ is Eisenstein if $n = p - 1$ for every integer $k \in [1, n-1]$ and, based on some further computations, conjectured:

Conjecture 2. *Let n and k be integers with $n \geq 2$ and $1 \leq k \leq n - 1$, and let $f(x) = 1 + x + x^2 + \cdots + x^n$. Then $f^{(k)}(x)$ is irreducible over the rationals.*

In 1991, again during the problem session at the West Coast Number Theory Conference, Jeff Lagarias mentioned a class of polynomials associated with some work of Eugene Gutkin [5] concerning billiards. Eugene Gutkin was interested in showing that the polynomials had no roots in common other than from obvious cyclotomic factors. As a consequence, Jeff Lagarias made the following conjecture attributed to Eugene Gutkin:

Conjecture 3. *Let n be an integer ≥ 4, and let*

$$p(x) = (n-1)(x^{n+1} - 1) - (n+1)(x^n - x).$$

Then $p(x)$ is $(x-1)^3$ times an irreducible polynomial if n is even and $p(x)$ is $(x-1)^3(x+1)$ times an irreducible polynomial if n is odd.

In this paper, we explain some approaches to these three conjectures. The connection between Conjectures 3 and the two previous conjectures is more transparent if one observes

*The second author was supported by NSF Grant DMS-9400937 and NSA Grant MDA904-97-1-0035.
**The third author was supported by NSA Grant MDA904-97-1-0054.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

that in Conjecture 1 we have $f(x) = (x^{n+1} - 1)/(x - 1)$ so that

$$f'(x) = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}.$$

Higher derivatives of $f(x)$ as in Conjecture 2 take a similar form. We are able to show that Conjectures 1 and 3 hold for almost all n and that Conjecture 2 holds for most choices of n and k. More precisely, we establish each of the following theorems.

Theorem 1. *Let $\varepsilon > 0$. For all but $O(t^{(1/3)+\varepsilon})$ positive integers $n \le t$, the derivative of the polynomial $f(x) = 1 + x + x^2 + \cdots + x^n$ is irreducible.*

Theorem 2. *Fix a positive integer k. For all but $o(t)$ positive integers $n \le t$, the kth derivative of the polynomial $f(x) = 1 + x + x^2 + \cdots + x^n$ is irreducible.*

Theorem 3. *Fix a positive integer m. There is an N such that if n is a positive integer $\ge N$ and $f(x) = 1 + x + x^2 + \cdots + x^n$, then the polynomial $f^{(n-m)}(x)$ is irreducible.*

Theorem 4. *Let $\varepsilon > 0$. For all but $O(t^{(4/5)+\varepsilon})$ positive integers $n \le t$, the polynomial*

$$p(x) = (n-1)(x^{n+1} - 1) - (n+1)(x^n - x),$$

is such that $p(x)$ is $(x-1)^3$ times an irreducible polynomial if n is even and $p(x)$ is $(x-1)^3(x+1)$ times an irreducible polynomial if n is odd.

In Theorem 2, our arguments give $O(t \log\log t / \log t)$ in place of $o(t)$. We would be interested in an upper bound of the type $O(t^\theta)$ for some $\theta \in (0,1)$ that is independent of k. Our arguments suggest that such a θ exists, but we have been unable to establish this.

The rest of the paper is organized as follows. In the next section, we give a proof of Theorem 3. The proofs of the remaining theorems above that we will present here rely on the location of the p-adic zeroes of the polynomials. Section 3 establishes some preliminary results based on these zeroes. As noted at the end of that section, these preliminary results can be extended to handle certain other classes of polynomials where almost all polynomials in the class have one non-cyclotomic irreducible factor. In the remaining sections of the paper, we give proofs of each of the remaining theorems based on these preliminary results.

Acknowledgment: The authors express their gratitude to Andrzej Schinzel who encouraged the first three authors to correspond with one another in matters related to this research. They also express their gratitude to Charles Nicol for early remarks concerning this work.

2. A Proof of Theorem 3 and Further Remarks

Consider $f(x)$ as in Theorem 3. If $m = 1$, then $f^{(n-m)}(x)$ is linear and, hence, irreducible for every integer $n \ge 1$. If $m = 2$, then $f^{(n-m)}(x)$ is quadratic and it is a simple matter to show that this quadratic has imaginary roots. Thus, in this case, $f^{(n-m)}(x)$ is irreducible for every integer $n \ge 2$. It is of some interest to continue by considering the cubics one obtains in Theorem 3 by setting $m = 3$. The proof we will present for Theorem

3 is effective so that in theory it is possible to determine for a fixed m what polynomials of the form $f^{(n-m)}(x)$ are reducible. We will demonstrate this at the end of the section by showing that for $m = 3$ the cubic $f^{(n-m)}(x)$ is irreducible for every integer $n \geq 4$.

We turn now to the proof of Theorem 3. Observe that

$$f^{(n-m)}(x) = \sum_{j=n-m}^{n} j(j-1)\cdots(j-n+m+1)x^{j-n+m} = \sum_{j=0}^{m}(n-j)(n-j-1)\cdots(m-j+1)x^{m-j}.$$

We set $k = n - m$ and consider the polynomial

$$\begin{aligned} F_k(x) = \frac{x^m f^{(k)}(1/x)}{k!} &= \sum_{j=0}^{m} \frac{(k+m-j)(k+m-j-1)\cdots(m-j+1)}{k!} x^j \\ &= \sum_{j=0}^{m} \binom{k+m-j}{m-j} x^j = \sum_{j=0}^{m} \binom{k+j}{j} x^{m-j}. \end{aligned}$$

It suffices now to show that if k is sufficiently large, then the polynomial $F_k(x)$ is irreducible.

For a prime p and an integer a, we define $\nu(a) = \nu_p(a) = e$ where $p^e || a$. We define the Newton polygon of a polynomial $F(x) = \sum_{j=0}^{n} a_j x^j$ as the lower convex hull of the points $(j, \nu(a_j))$ (cf. [3], [6], [15]). We consider the Newton polygon of a polynomial $F(x)$. Let the lattice points along the edges be $(x_0, y_0), (x_1, y_1), \ldots, (x_s, y_s)$ with $0 = x_0 < x_1 < \cdots < x_s = \deg F(x)$. Then the degree of any irreducible factor of $F(x)$ (over $\mathbb{Z}[x]$) must be some sum of the differences $x_1 - x_0, x_2 - x_1, \ldots, x_s - x_{s-1}$. In other words, if r is the degree of an irreducible factor of $F(x)$, then there are integers $j_1, \ldots, j_t$ with $1 \leq j_1 < j_2 < \cdots < j_t \leq s$ such that $r = \sum_{i=1}^{t}(x_{j_i} - x_{j_i - 1})$.

The next result is due to Sylvester [13] and was first used to obtain irreducibility results by I. Schur [12]. It is a generalization of Bertrand's postulate that for every integer $m \geq 1$, there is a prime in the interval $(m, 2m]$ (take $k = m$).

Lemma 1. *Let m and k be positive integers with $m \geq k$. Then there is a prime $p \geq k+1$ which divides one of the numbers $m+1, m+2, \ldots, m+k$.*

We will also use an effective version of Thue's theorem (it follows with a little modification from Theorem 4.1 in [1]; also see [11]).

Lemma 2. *Let a, b, and d be integers with $d \neq 0$. Let q be a positive integer ≥ 3. Then there are finitely many integer pairs (x, y) for which $ax^q - by^q = d$. Furthermore, these pairs can effectively be determined.*

The following is a combinatorial lemma and follows directly from (5.26) of [4].

Lemma 3. *Let m and k be positive integers. Let $F_k(x)$ be as in the theorem. Then*

$$F_k(x+1) = \sum_{j=0}^{m} \binom{k+m+1}{j} x^{m-j}.$$

Fix a positive integer m. By the comments at the beginning of this section, we may suppose that $m \geq 3$ (and do so). If $F_k(x)$ is reducible, then it has a factor with degree in the interval $[1, m/2]$. It suffices therefore to show that for each $\ell \in [1, m/2]$, there are only finitely many k for which $F_k(x)$ has a factor of degree ℓ. Fix an integer $\ell \in [1, m/2]$, and suppose $F_k(x)$ has a factor $g(x)$ in $\mathbb{Z}[x]$ of degree ℓ. Define $q = m$ in the case that $\ell = 1$. Otherwise, define q as the largest prime divisor of $m(m-1)\cdots(m-\ell+1)$. Since $m-\ell \geq \ell$, we deduce from Lemma 1 that $q \geq \ell + 1$. Observe that our choice of q guarantees that $q \geq 3$. Let $t \in \{0, 1, \ldots, \ell - 1\}$ such that q divides $m - t$.

Suppose now that $p > m$ is a prime dividing $k + t + 1$ (if no such p exists, we can skip this part). Let r be the positive integer such that $p^r || (k + t + 1)$. We claim that q divides r. For $t + 1 \leq j \leq m$, we deduce from

$$\binom{k+j}{j} = \frac{(k+j)(k+j-1)\cdots(k+1)}{j!}$$

that p, which is $> m$, divides the numerator of this last expression but not its denominator. In fact, p^r must exactly divide the numerator. On the other hand, one easily deduces from $p > m > t$ and $p | (k + t + 1)$ that p does not divide $\binom{k+t}{t}$. Hence, the Newton polygon of $F_k(x)$ with respect to the prime p has as its left-most edge the line segment with endpoints $(0, r)$ and $(m - t, 0)$. Recall that $\ell \geq t + 1$. Since $F_k(x)$ has the factor $g(x)$ of degree ℓ, it follows that there must be two lattice points, say (a, b) and (c, d) with $c > a$, on the left-most edge of the Newton polygon of $F_k(x)$ with $c - a \leq \ell$. On the other hand, by considering the slope of the left-most edge, we see that

$$\frac{|d-b|}{c-a} = \frac{r}{m-t} \qquad \Longrightarrow \qquad (m-t)|d-b| = (c-a)r.$$

The definition of q implies $c - a \leq \ell < q$. Thus, q and $c - a$ are relatively prime (in the case that q is a prime, this is clear; in the case that $\ell = 1$ where we have defined $q = m$, this follows since $c - a \leq \ell = 1$ implies $c - a = 1$). On the other hand, $q | (m - t)$, so the above equation gives that q divides r as claimed.

We now make use of Lemma 3. We consider any prime $p > m$ dividing $k + m - t + 1$, and let r be the positive integer such that p^r exactly divides $k + m - t + 1$. Observe that since $t \leq \ell - 1 \leq (m/2) - 1$, we have $k + m - t + 1 \neq k + t + 1$, so we are in a different situation than the above. We use an argument similar to the above to show that q divides r in this situation as well. Here, we have

$$\binom{k+m+1}{j} = \frac{(k+m+1)(k+m)\cdots(k+m-j+2)}{j!}.$$

The conditions $p > m$ and p^r exactly divides $k + m - t + 1$ with $r \geq 1$ imply that for every j with $t + 1 \leq j \leq m$, p^r exactly divides $\binom{k+m+1}{j}$. Also, p does not divide $\binom{k+m+1}{t}$. We deduce that the Newton polygon of $F_k(x + 1)$ with respect to p contains the line segment with endpoints $(0, r)$ and $(m - t, 0)$. The same argument as above gives as before that since $F_k(x)$ (and hence $F_k(x + 1)$) has a factor of degree ℓ, q must divide r.

Let $p_1, \dots, p_s$ denote the distinct primes $\le m$. Let

$$T = \{p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} : 0 \le e_j \le q-1 \text{ for each } j\}.$$

By the above, $k+m-t+1 = au^q$ and $k+t+1 = bv^q$ for some integers a and b in T and some integers u and v. We deduce that (u,v) is a solution to the diophantine equation $ax^q - by^q = m-2t$. Note that $m-2t > 0$ and that q and t only depend on m and ℓ. For each choice of a and b in T, we deduce from Lemma 2 that there are only finitely many k with $k+m-t+1 = au^q$ and $k+t+1 = bv^q$ as above. Since T is a finite set, there are only finitely many $F_k(x)$ with a factor in $\mathbb{Z}[x]$ of degree ℓ. This completes the proof of Theorem 3.

We end this section by establishing that the cubics obtained by taking derivatives of $f(x)$ as in Theorem 3 are all irreducible.

Theorem 5. *Let $f(x) = 1 + x + x^2 + \cdots + x^n$. For every integer $n \ge 4$, the polynomial $f^{(n-3)}(x)$ is irreducible.*

As in our arguments above (with $m = 3$), we consider

$$F_k(x) = x^3 + \binom{k+1}{1} x^2 + \binom{k+2}{2} x + \binom{k+3}{3}.$$

We want to show that $F_k(x)$ is irreducible for all $k \ge 1$. In the argument for Theorem 3, we have $m = q = 3$, $\ell = 1$, and $t = 0$. We deduce that $k+4 = au^3$ and $k+1 = bv^3$ for some positive integers a, b, u, and v with a and b divisors of 36. Such k are determined from the diophantine equation $au^3 - bv^3 = 3$.

A simple restriction on a and b that follows directly from $au^3 - bv^3 = 3$ is that either both a and b are divisible by 3 or neither is. Also, since one of $k+4 = au^3$ and $k+1 = bv^3$ is odd, at least one of a and b is odd. We show further that only the cases where a and b are both not divisible by 9 are of interest to us (in other words, we need only consider a and b divisors of 12). If 3^{3e+2} exactly divides $k+1$ for some non-negative integer e, then the Newton polygon of $F_k(x)$ with respect to 3 consists of a line segment with endpoints $(0, 3e+1)$ and $(3, 0)$. This segment contains no lattice points other than the endpoints. Hence, $F_k(x)$ is irreducible. An analogous argument works when 3^{3e+2} exactly divides $k+4$ by considering $F_k(x+1)$ rather than $F_k(x)$. It follows then that a and b must be divisors of 12.

Our next two lemmas appear in [7], Theorem 5 on page 220 and Theorem 6 on page 225.

Lemma 4. *If $d > 1$, the equation $u^3 + dv^3 = 1$ has at most one integer solution with $uv \ne 0$. If such a solution exists, then necessarily $u + v\sqrt[3]{d}$ is the fundamental unit in the ring $\mathbb{Z}[\sqrt[3]{d}]$.*

Lemma 5. *The complete set of solutions to the diophantine equation $2u^3 - v^3 = 3$ is given by $(u,v) = (1,-1)$ and $(u,v) = (4,5)$, and the complete set of solutions to the diophantinve equation $4u^3 - v^3 = 3$ is given by $(u,v) = (1,1)$.*

Lemma 4 will be used to examine solutions to

$$u^3 - 2v^3 = 1 \quad \text{and} \quad u^3 - 4v^3 = 1.$$

We will want $uv \neq 0$. Integer solutions to these correspond to integer solutions to $u^3 + 2(-v)^3 = 1$ and $u^3 + 4(-v)^3 = 1$. Lemma 4 asserts that there is at most one solution to $u^3 + 2(-v)^3 = 1$ with $uv \neq 0$. Apparently, this is given by $(u, v) = (-1, -1)$. Now, we apply Lemma 4 to the second equation. Observe that $5 + 3\sqrt[3]{4} + 2\sqrt[3]{4}^2$ is a unit in $\mathbb{Z}[\sqrt[3]{4}]$. If the fundamental unit in $\mathbb{Z}[\sqrt[3]{4}]$ were of the form $u + v\sqrt[3]{4}$ with u and v integers satisfying $u^3 + 4v^3 = 1$, then there would be some positive integer t for which

$$\left(u + v\sqrt[3]{4}\right)^t = 5 + 3\sqrt[3]{4} + 2\sqrt[3]{4}^2.$$

Expanding the right side and expressing it in terms of the basis $\{1, \sqrt[3]{4}, \sqrt[3]{4}^2\}$, it is easy to see that v will be a divisor of the coefficient of $\sqrt[3]{4}$ and a divisor of the coefficient of $\sqrt[3]{4}^2$. We deduce that v divides both 3 and 2 and, hence, is ± 1. Since $u^3 + 4v^3 = 1$, we easily obtain a contradiction. Therefore, the fundamental in $\mathbb{Z}[\sqrt[3]{4}]$ cannot be of the form stated in Lemma 4, and we deduce that there are no solutions to $u^3 + 4(-v)^3 = 1$ with $uv \neq 0$.

Lemma 5 is only part of Theorem 6 in [7, p. 225]. The first sentence of Lemma 5 is stated explicitly. The second sentence follows by considering $4u^3 + (-v)^3 = 3$ in Theorem 6. Theorem 6 in [7] implies that there is at most one solution to this diophantine equation. Apparently, it is given by $(u, v) = (1, 1)$.

Given the restrictions on a and b above, we show next that the only solutions to $au^3 - bv^3 = 3$ with u and v positive arise from one of the following:

(i) $(a, b) = (4, 1)$ and $(u, v) = (1, 1)$.

(ii) $(a, b) = (6, 3)$ and $(u, v) = (1, 1)$.

(iii) $(a, b) = (2, 1)$ and $(u, v) = (4, 5)$.

To simplify matters, we restrict ourselves to $a \geq b$. If $a < b$ and $au^3 - bv^3 = 3$ with u and v positive, then also $b(-v)^3 - a(-u)^3 = 3$. Thus, we can make the restriction $a \geq b$ provided we also consider solutions with both u and v negative. Given our restrictions on a and b, we get that there are only six cases to consider.

Case 1. $(a, b) = (1, 1)$.

Here, we want solutions to $u^3 - v^3 = 3$. Since we are considering u and v to have the same sign, we have $uv > 0$. Then the factor $u^2 + uv + v^2$ of $u^3 - v^3$ is ≥ 3 with equality if and only if $uv = 1$. We easily deduce that $u^3 - v^3 = 3$ has no solutions in integers u and v with $uv > 0$.

Case 2. $(a, b) = (2, 1)$.

Here, we are interested in solutions of $2u^3 - v^3 = 3$ with $uv > 0$. We apply Lemma 5 above to obtain the unique solution $(u, v) = (4, 5)$.

Case 3. $(a, b) = (4, 1)$.

From Lemma 5, the only solution to $4u^3 - v^3 = 3$ is $(u, v) = (1, 1)$.

Case 4. $(a, b) = (3, 3)$.

If $3u^3 - 3v^3 = 3$, then $u^3 - v^3 = 1$. Since we require $uv > 0$, the factor $u^2 + uv + v^2$ of $u^3 - v^3$ is ≥ 3 so that $u^3 - v^3 = 1$ has no solutions in integers u and v with $uv > 0$.

Case 5. $(a,b) = (6,3)$.

If $6u^3 - 3v^3 = 3$, then $2u^3 - v^3 = 1$. As noted above, Lemma 4 implies $u^3 - 2v^3 = 1$ has only the solution $(u,v) = (-1,-1)$. Interchanging the roles of u and v and changing the signs of u and v, we deduce that $2u^3 - v^3 = 1$ has only the solution $(u,v) = (1,1)$ (assuming $uv > 0$).

Case 6. $(a,b) = (12,3)$.

If $12u^3 - 3v^3 = 3$, then $4u^3 - v^3 = 1$. From the comments after Lemma 4 above, it follows that there are no integer solutions to $4u^3 - v^3 = 1$ with $uv \neq 0$.

We deduce from (i), (ii), and (iii) that we only need consider the three possibilities $k+1 = 1$, $k+1 = 3$, and $k+1 = 125$. One checks the latter two directly to see that $F_k(x)$ is irreducible. We are not allowing $k = 0$ so the first possibility does not really arise. This completes the proof of Theorem 5.

3. Preliminary Results

For p a prime, we let $|\ |_p$ represent the p-adic norm on $\mathbb{Q}$ and let $\mathbb{Q}_p$ denote the completion of the rationals with respect to this norm. We denote by $\nu_p(a)$ the value of $-\log|a|_p/\log p$ where we interpret $\nu_p(0)$ as ∞. Both $|\ |_p$ and ν_p extend in a natural way to the algebraic closure of $\mathbb{Q}_p$. We drop the subscripts when using ν_p when it is clear what the prime p under consideration is. We make use of the Newton polygon of a polynomial $f(x) = \sum_{j=0}^{n} a_j x^j$ with coefficients in some extension of $\mathbb{Q}_p$; as in the previous section, this Newton polygon is defined as the lower convex hull of the points $(j, \nu(a_j))$. Throughout the remainder of this paper, we work in an algebraic closure of $\mathbb{Q}_p$ unless noted otherwise or unless it is clear from the context that we are working in $\mathbb{C}$. As references, we mention the books of Gouvea [3], Koblitz [6], and Weis [15].

A lemma we will make use of throughout the remainder of the paper is the following.

Lemma 6. *Let ζ be an m^{th} p-adic root of unity and ζ' and m'^{th} p-adic root of unity. Suppose $p \nmid mm'$. Then $\nu(\zeta - \zeta') = 0$.*

The lemma follows from Lemma 2.12 of [14]. It is also easily established by observing that $\zeta(\zeta')^{-1} - 1$ is a root of $\sum_{j=0}^{mm'-1}(x+1)^j$, a monic polynomial with constant term relatively prime to p. We will make particular use of the lemma with $\zeta' = \pm 1$.

The next result, an essential ingredient to our arguments for Theorems 1 and 2, is based on the work of the first author in [2].

Proposition 1. *Let $w(x) = \sum_{j=0}^{n+1} a_j x^j \in \mathbb{Z}[x]$ with $a_{n+1} \neq 0$, and let m and r be integers with $m > 0$, $r \geq 0$, $n+1 = m+r$. Let p be a prime such that $p|m$, $p > r$, and $p \nmid a_{n+1}$. Write $m = p^\ell m'$ where $\nu_p(m') = 0$. Suppose that $w(x) \equiv a_{n+1}(x^m - 1)x^r \pmod{p^\ell}$ and that, for each $\zeta \neq 1$ such that $\zeta^{m'} = 1$, we have $\nu_p(w(\zeta)) = \ell$. Let $w(x) = g(x)h(x)$ be a factorization of $w(x)$ in $\mathbb{Z}[x]$. Let*

$$A = \sum_{g(\beta)=0} \left(\beta - \frac{1}{\beta}\right), \ B = \sum_{h(\gamma)=0} \left(\gamma - \frac{1}{\gamma}\right), \ C = \sum_{g(\beta)=0} (1-\beta) \ \text{ and } \ D = \sum_{h(\gamma)=0} (1-\gamma),$$

where the sums are over the distinct roots of $g(x)$ and $h(x)$ and where we consider A and B only in the case that $a_0 \neq 0$. Then A, B, C, and D are rational numbers satisfying:

(i) if $r = 0$, then each of $\nu(A)$, $\nu(B)$, $\nu(C)$, and $\nu(D)$ is positive,

(ii) if $r > 0$, $p^\ell || a_0$, and $\gcd(\ell, r) = 1$, then either $\nu(A) > 0$, $\nu(C) > 0$, $p|h(0)$, and $D \neq 0$ or $\nu(B) > 0$, $\nu(D) > 0$, $p|g(0)$, and $C \neq 0$.

Comment: We have defined A, B, C, and D as sums over distinct roots of $g(x)$ or $h(x)$. The conclusions of the proposition, however, hold even if any of these sums is taken over the roots counted to their multiplicities. The same proof below, word for word, can be used to establish this.

Proof. First, we observe that each of A, B, C, and D is rational; this follows as each is a symmetric function of the roots of either $g(x)$ or $h(x)$ both of which contain rational coefficients. Note that the rational values of A, B, C, and D depend only on the coefficients of $g(x)$ and $h(x)$. It follows that these values are independent of whether we view the roots β of $g(x)$ and the roots γ of $h(x)$ as complex numbers or as lying in an algebraic closure of $\mathbb{Q}_p$.

We begin by determining information about the p-adic location of the zeroes of $w(x)$. Let ζ be an m'th root of unity different from 1. We determine next the Newton polygon of $f(x) = w(x+\zeta)$. Write $f(x) = \sum_{j=0}^{n+1} b_j x^j$ and observe that $b_0 = f(0) = w(\zeta)$. We deduce that the left-most endpoint of the Newton polygon of $f(x)$ is $(0, \nu(w(\zeta))) = (0, \ell)$. Also, the conditions in the lemma imply that there is a $v(x) \in \mathbb{Z}[x]$ for which $w(x) = a(x^{m+r} - x^r) + p^\ell v(x)$ where $a = a_{n+1}$. Note that $p \nmid a$. It follows that

$$\begin{aligned} f(x) &= a\big((x+\zeta)^{m+r} - (x+\zeta)^r\big) + p^\ell v(x+\zeta) \\ &= a \sum_{j=0}^{m+r} \left(\binom{m+r}{j} \zeta^{m+r-j} - \binom{r}{j} \zeta^{r-j} \right) x^j + p^\ell v(x+\zeta) \\ &= a \sum_{j=0}^{m+r} \left(\binom{m+r}{j} - \binom{r}{j} \right) x^j \zeta^{r-j} + p^\ell v(x+\zeta) \end{aligned}$$

where we interpret $\binom{r}{j}$ as zero if $j > r$. We use that $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$ with equality when $\nu(x) \neq \nu(y)$. We deduce

$$\nu(b_j) \geq \min\left\{ \ell, \nu\left(\binom{m+r}{j} - \binom{r}{j} \right) \right\},$$

and equality holds if the minimum is not ℓ. For $1 \leq j \leq r$, the conditions $p^\ell | m$ and $p > r$ imply that $\binom{m+r}{j} \equiv \binom{r}{j} \pmod{p^\ell}$, and we obtain $\nu(b_j) \geq \ell$. For $j > r$, we have $\binom{r}{j} = 0$. One easily checks that

$$\nu\left(\binom{m+r}{p^u} \right) = \ell - u \quad \text{for } 1 \leq u \leq \ell$$

and

$$\nu\left(\binom{m+r}{j} \right) \geq \ell - u \quad \text{if } p^u \leq j < p^{u+1} \quad \text{and} \quad 1 \leq u \leq \ell - 1.$$

Furthermore, this last inequality holds also for $u = 0$ provided j is restricted to $r < j < p$. We deduce that $\nu(b_{p^u}) = \ell - u$ for $1 \le u \le \ell$ and that $\nu(b_j) \ge \ell - u$ for $p^u \le j < p^{u+1}$ and $0 \le u \le \ell - 1$. Also, $\nu(b_j) \ge 0$ for $p^\ell < j \le n + 1$. It follows that the Newton polygon of $f(x)$ has left-most edges joining the points $(0, \ell)$ and $(p^u, \ell - u)$ for $1 \le u \le \ell$. (It is easy to see that the right-most edge is the segment with endpoints $(p^\ell, 0)$ and $(n+1, 0)$, but we will not need this fact.)

We use the classical connection between Newton polygons of a polynomial and the p-adic roots of the polynomial. We deduce that $f(x)$ has exactly p roots α with $\nu(\alpha) = 1/p$ and, for each $u \in \{1, , 2, \dots, \ell - 1\}$, exactly $p^{u+1} - p^u$ roots α with $\nu(\alpha) = 1/(p^{u+1} - p^u)$. We view these roots as forming ℓ sets, each set containing roots with equal ν-values. Note that since $p \nmid m'$, p does not ramify in $\mathbb{Q}_p(\zeta)$. We deduce that the roots in any one set are distinct roots of the same irreducible factor of $f(x)$ over $\mathbb{Q}_p(\zeta)$.

Observe that α is a root of $w(x)$ if and only if $\alpha - \zeta$ is a root of $f(x)$. If we view the roots of $f(x)$ in the form $\alpha - \zeta$ and consider the ℓ sets of roots formed as above, we see that $w(x)$ has ℓ "clusters" around ζ of roots with the property that if α and α' belong to the same cluster, then $\nu(\alpha - \zeta) = \nu(\alpha' - \zeta) > 0$. Furthermore, the roots in any one of these clusters are distinct roots of the same irreducible factor of $w(x)$ over $\mathbb{Q}_p(\zeta)$ and, hence, of the same irreducible factor of $w(x)$ over $\mathbb{Q}$. In other words, if one root from a cluster is a root of $g(x)$ (or $h(x)$), then all the roots from that cluster are roots of $g(x)$ (or $h(x)$, respectively).

The above holds for each $\zeta \ne 1$ satisfying $\zeta^{m'} = 1$. There are $m' - 1$ such ζ forming $(m' - 1) \times \ell$ clusters of roots of $w(x)$. We show next that these are disjoint clusters. This is clearly true of clusters formed from the same ζ; in other words, if α and α' are roots with $\nu(\alpha - \zeta) \ne \nu(\alpha' - \zeta)$, then clearly $\alpha \ne \alpha'$. Now, suppose α is in a cluster around ζ and in a cluster around ζ' where $\zeta \ne \zeta'$, $\zeta \ne 1$, $\zeta' \ne 1$, $\zeta^{m'} = 1$, and $(\zeta')^{m'} = 1$. Then it follows that

$$\nu\big((\zeta' - \zeta)\alpha\big) = \nu\big(\zeta'(\alpha - \zeta) - \zeta(\alpha - \zeta')\big) \ge \min\{\nu\big(\zeta'(\alpha - \zeta)\big), \nu\big(\zeta(\alpha - \zeta')\big)\} > 0.$$

Lemma 6 implies that $\nu(\zeta' - \zeta) = 0$. Since $\nu(\alpha - \zeta) > 0$ and $\nu(\zeta) = 0$, we also deduce $\nu(\alpha) = 0$. We therefore obtain a contradiction, and we can conclude that the $(m' - 1) \times \ell$ clusters consist of distinct roots.

The total number of roots in these $(m' - 1) \times \ell$ clusters is $(m' - 1) \times p^\ell$. Since $w(x)$ has $m + r = m'p^\ell + r$ roots, we have yet to account for $p^\ell + r$ roots of $w(x)$. By considering the Newton polygon of $w(x)$ and using the condition $w(x) \equiv a(x^m - 1)x^r \pmod{p^\ell}$, we deduce that $w(x)$ has exactly r roots α with the property that $\nu(\alpha) > 0$. Note that the other roots α of $w(x)$ necessarily satisfy $\nu(\alpha) = 0$. In a manner similar to the above (but easier), we deduce that each of the r roots around 0 does not belong to any of the above clusters of roots. These r roots around 0 form a cluster as before except that we cannot in general deduce that these roots necessarily are roots of the same irreducible factor of $w(x)$ over $\mathbb{Q}_p(\zeta)$ (or over $\mathbb{Q}$). The condition $\gcd(\ell, r) = 1$ in (ii) implies that the left-most edge of the Newton polygon of $w(x)$ contains only the lattice points at its endpoints, namely $(0, \ell)$ and $(r, 0)$. Since p does not ramify in $\mathbb{Q}_p(\zeta)$, we deduce that in this case the cluster of r roots around 0 are distinct roots of a single irreducible factor of $w(x)$ over $\mathbb{Q}_p(\zeta)$.

We show now that the remaining p^ℓ roots of $w(x)$ form a cluster of roots around 1. The argument for roots around 1 is analogous to the case for ζ above (just set $\zeta = 1$) except that we cannot obtain here that $\nu(b_0) = \nu(w(1)) = \ell$. On the other hand, the condition $w(x) \equiv a(x^m - 1)x^r \pmod{p^\ell}$ implies $\nu(b_0) = \nu(w(1)) \geq \ell$. The argument proceeds as before, and we deduce that there are p^ℓ roots α of $w(x)$ with the property that $\nu(\alpha - 1) > 0$ (we could say more, but this is all we will need). As before, it is easy to argue that these p^ℓ roots around 1 are distinct from the roots of $w(x)$ belonging to other clusters. We cannot, however, deduce that these roots are distinct or that they are roots of the same irreducible factor of $w(x)$ over $\mathbb{Q}_p(\zeta)$ (or over $\mathbb{Q}$).

We now apply the information we have established about the location of the zeroes of $w(x)$. We consider the case that $r = 0$. Then there are no roots in the cluster described above around 0. It follows that the roots of $g(x)$ consist of complete clusters around ζ for some choices of $\zeta \neq 1$ together with possibly some of the p^ℓ roots around 1; likewise for $h(x)$. If $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_s$ denote the clusters around $\zeta \neq 1$ which contain roots of $g(x)$ and $\mathcal{C}_0$ denotes the roots in the cluster around 1 that are roots of $g(x)$, then we deduce that

$$\nu(C) \geq \min_{0 \leq j \leq s} \left\{ \nu\left(\sum_{\beta \in \mathcal{C}_j} (1 - \beta) \right) \right\}.$$

Observe that

$$\nu\left(\sum_{\beta \in \mathcal{C}_0} (1 - \beta) \right) \geq \min_{\beta \in \mathcal{C}_0} \left\{ \nu(1 - \beta) \right\} > 0.$$

For each $j \in \{1, 2, \ldots, s\}$, we define ζ_j as the m'th root of unity such that the roots of $\mathcal{C}_j$ are those around ζ_j, and we write

$$\sum_{\beta \in \mathcal{C}_j} (1 - \beta) = \sum_{\beta \in \mathcal{C}_j} \big((1 - \zeta_j) - (\beta - \zeta_j) \big) = |\mathcal{C}_j|(1 - \zeta_j) - \sum_{\beta \in \mathcal{C}_j} (\beta - \zeta_j).$$

Since $|\mathcal{C}_j|$ by construction is a multiple of p, we deduce that each of the terms in this last expression has ν-value > 0. It follows now that $\nu(C) > 0$. The same argument gives $\nu(D) > 0$. Since $r = 0$ and $w(x) \equiv a(x^m - 1)x^r \pmod{p^\ell}$, we deduce that $a_0 \neq 0$ so that A and B are defined. Also, in this case, $\nu(\beta) = 0$ for each root β of $g(x)$ and $\nu(\gamma) = 0$ for each root γ of $h(x)$. Define $\zeta_1, \ldots, \zeta_s$ as before, and let $\zeta_0 = 1$. We use that

$$\begin{aligned} \nu(A) &\geq \min_{0 \leq j \leq s} \left\{ \nu\left(\sum_{\beta \in \mathcal{C}_j} \left(\beta - \frac{1}{\beta} \right) \right) \right\} \\ &\geq \min_{0 \leq j \leq s} \left\{ \nu\left(\sum_{\beta \in \mathcal{C}_j} \left((\beta - \zeta_j) + \frac{\beta - \zeta_j}{\beta \zeta_j} + \left(\zeta_j - \frac{1}{\zeta_j} \right) \right) \right) \right\}. \end{aligned}$$

Following along lines similar to our argument that $\nu(C) > 0$, we deduce that $\nu(A) > 0$. An analogous argument gives $\nu(B) > 0$.

For (ii), we have shown that the cluster of r roots around 0 are roots of a single irreducible factor of $w(x)$ over $\mathbb{Q}_p(\zeta)$. Hence, these r roots are either roots of $g(x)$ or roots of

$h(x)$. Suppose the cluster of roots around 0 are roots of $h(x)$. Then each root α of $g(x)$ belongs to a cluster around a root of unity so that the arguments above give $\nu(A) > 0$ and $\nu(C) > 0$. Since $p \nmid a_{n+1}$, the leading coefficient of $h(x)$ is not divisible by p and we deduce that $\nu(h(0)) = \sum_{h(\gamma)=0} \nu(\gamma)$. Since $h(x)$ has roots from the cluster of roots around 0, we obtain $\nu(h(0)) > 0$ so that $p|h(0)$. If S is the set of r roots clustered around 0, then we consider

$$\sum_{\gamma \in S} (1-\gamma) = r - \sum_{\gamma \in S} \gamma.$$

Since $\nu(\gamma) > 0$ for each $\gamma \in S$, the sum on the right has a positive ν-value. Since $p > r > 0$, $\nu(r) = 0$. It follows that $\nu\big(\sum_{\gamma \in S}(1-\gamma)\big) = 0$. Hence, the arguments in the previous paragraph now imply $\nu(D) = 0$. In particular, we must have $D \neq 0$. A similar argument can be used in the case that the cluster of roots around 0 are roots of $g(x)$. The proposition follows. ■

For the proof of Theorem 4, we will make use of three results similar to Proposition 1. They are as follows:

Proposition 2. *Let $w(x) = \sum_{j=0}^{n+1} a_j x^j \in \mathbb{Z}[x]$ with $a_{n+1} \neq 0$. Let p be an odd prime such that $p|(n+1)$ and $p \nmid a_{n+1}$. Write $n+1 = p^\ell m'$ where $\nu_p(m') = 0$. Suppose that $w(x) \equiv a_{n+1}(x^{n+1} - 1) \pmod{p^\ell}$ and that, for each $\zeta \neq \pm 1$ such that $\zeta^{m'} = 1$, we have $\nu_p(w(\zeta)) = \ell$. Let $w(x) = g(x)h(x)$ be a factorization of $w(x)$ in $\mathbb{Z}[x]$. Let*

$$A = \sum_{g(\beta)=0} \left(\beta - \frac{1}{\beta}\right), \ B = \sum_{h(\gamma)=0} \left(\gamma - \frac{1}{\gamma}\right), \ C' = \sum_{g(\beta)=0} (1-\beta^2) \ \text{and} \ D' = \sum_{h(\gamma)=0} (1-\gamma^2),$$

where the sums are over the distinct roots of $g(x)$ and $h(x)$ and where we consider A and B only in the case that $a_0 \neq 0$. Then A, B, C', and D' are rational numbers satisfying $\nu(A) > 0$, $\nu(B) > 0$, $\nu(C') > 0$, and $\nu(D') > 0$.

Proposition 3. *Let $w(x) = \sum_{j=0}^{n+1} a_j x^j \in \mathbb{Z}[x]$ with $a_{n+1} \neq 0$. Let p be an odd prime such that $p|n$ and $p \nmid a_{n+1}$. Write $n = p^\ell m'$ where $\nu_p(m') = 0$. Suppose that $w(x) \equiv a_{n+1}(x^n - 1)(x+1) \pmod{p^\ell}$ and that, for each $\zeta \neq 1$ such that $\zeta^{m'} = 1$, we have $\nu_p(w(\zeta)) = \ell$. Let $w(x) = g(x)h(x)$ be a factorization of $w(x)$ in $\mathbb{Z}[x]$. Define A, B, C', and D' as in Proposition 2. Then A, B, C', and D' are rational numbers satisfying $\nu(A) > 0$, $\nu(B) > 0$, $\nu(C') > 0$, and $\nu(D') > 0$.*

Proposition 4. *Let $w(x) = \sum_{j=0}^{n+1} a_j x^j \in \mathbb{Z}[x]$ with $a_{n+1} \neq 0$. Suppose $w(x)$ is a reciprocal polynomial so that $w(x) = \pm x^{n+1} w(1/x)$. Let p be an odd prime such that $p|(n-1)$, $p|a_{n+1}$, and $p \nmid a_n$. Write $n-1 = p^\ell m'$ where $\nu_p(m') = 0$. Suppose that $w(x) \equiv a_n(x^{n-1} - 1)x \pmod{p^\ell}$ and that, for each $\zeta \neq \pm 1$ such that $\zeta^{m'} = 1$, we have $\nu_p(w(\zeta)) = \ell$. Let $w(x) = g(x)h(x)$ be a factorization of $w(x)$ in $\mathbb{Z}[x]$. Define A, B, C', and D' as above. Then A, B, C', and D' are rational numbers such that if $AB = 0$, then at least one of $\nu(C') > 0$ and $\nu(D') > 0$ holds.*

Proofs of Propositions 2, 3, and 4 can be given along the lines of the argument presented here for Proposition 1. To aid the reader, we briefly describe certain aspects of these proofs. As in the proof of Proposition 1, the roots of $w(x)$ in each of the above results can be grouped in clusters. In each of Propositions 2, 3, and 4, around each of the $m'-2$ (if m' is even) or $m'-1$ (if m' is odd) different ζ satisfying $\zeta \neq \pm 1$ and $\zeta^{m'} = 1$, there are p^ℓ roots which form various clusters, with each cluster of roots belonging to the same irreducible factor of $w(x)$ and each cluster containing a multiple of p different roots. In the case of Proposition 2, there are p^ℓ other roots of $w(x)$ forming a cluster around 1 and, if m' is even, p^ℓ other roots forming a cluster around -1; each of these clusters contains roots that are not necessarily roots of the same irreducible factor of $w(x)$. This is sufficient to establish Proposition 2. There are similar clusters of size p^ℓ around each of 1 (for all m') and -1 (if m' is even) in the case of Proposition 4. However, in this case there are two additional roots to account for; one of these two roots α satisfies $\nu(\alpha) > 0$ and the other root α' satisfies $\nu(\alpha') < 0$. If $AB = 0$, one can show that the roots α and α' are either both roots of $g(x)$ or are both roots of $h(x)$. If the former holds then $\nu(D') > 0$, and if the latter holds then $\nu(C') > 0$. In Proposition 3, there is one cluster with p^ℓ roots around 1 containing roots that are not necessarily roots of the same irreducible factor of $w(x)$. There are also $p^\ell + 1$ roots around -1 (if m' is even) or one such root (if m' is odd) forming clusters with the roots in each cluster being roots of the same irreducible factor of $w(x)$; one cluster contains $p+1$ roots (if m' is even) or 1 root (if m' is odd) and the remaining clusters contain a multiple of p different roots of $w(x)$. It follows easily that $\nu(A) > 0$, $\nu(B) > 0$, $\nu(C') > 0$, and $\nu(D') > 0$.

There is a variety of results analogous to the propositions in this section that can be established by similar means. Note that in Proposition 1 we dealt with a sum C of terms of the form $1-\beta$ whereas the remaining propositions dealt with a sum C' involving terms of the form $1-\beta^2$. As will be evident later, C is of value in establishing Theorem 1 as the term $1-\beta$ is 0 when β is one of the cyclotomic roots of $nx^{n+1} - (n+1)x^n + 1$ (i.e., when $\beta = 1$), the numerator of $f'(x)$. Similarly, C' is helpful in establishing Theorem 4 since $1-\beta^2$ is 0 when β is one of the cyclotomic roots of $p(x)$ (i.e., when $\beta = \pm 1$). More generally, one can make use of

$$C_k = \sum_{g(\beta)=0} (1-\beta^k) \quad \text{and} \quad D_k = \sum_{h(\gamma)=0} (1-\gamma^k)$$

in dealing with certain classes of polynomials for which the cyclotomic roots are known to be roots of $x^k - 1$. The proofs presented in the following sections will help illustrate applications of such propositions to the irreducibility of the non-cyclotomic parts of polynomials of a given form.

4. A Proof of Theorem 1

Let $n \geq 2$. We wish to show that $nx^{n+1} - (n+1)x^n + 1$ is $(x-1)^2$ times an irreducible polynomial in $\mathbb{Z}[x]$. It suffices to show the same for the reciprocal of $nx^{n+1} - (n+1)x^n + 1$, and for this purpose we define $w(x) = x^{n+1} - (n+1)x + n$. We consider $n \geq 2$ and $w(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $\deg g(x) \geq 1$, $\deg h(x) \geq 1$, and $g(1) \neq 0$. Note that $\deg g(x) \geq 1$ is possible since the product of the roots of $w(x)$ is $\pm n$ so that $w(x)$ has a root different from 1. Since $w(x)$ is monic, we may suppose that each of $g(x)$ and $h(x)$ are monic and do so. Our goal is to show $h(x) = (x-1)^2$.

We make use of A and B of Proposition 1 but not of C and D. If β is a root of $g(x)$, then β and $g(0)/\beta$ are algebraic integers. Also, if γ is a root of $h(x)$, then γ and $h(0)/\gamma$ are algebraic integers. Since $g(0)h(0) = n$, we deduce that nAB is a rational integer. We will see momentarily that if $B = 0$, then $h(x) = (x-1)^2$. In addition, we show that if $B \neq 0$, then upper and lower bounds on the value of $n|AB|$ can be obtained which are inconsistent for all but $O(t^{(1/3)+\varepsilon})$ positive integers $n \le t$. The proof of Theorem 1 will then be complete.

Since $(x^{n+1}-1)/(x-1)$ has distinct roots on the unit circle and since the derivative of a polynomial has roots inside the convex hull of the roots of the polynomial (cf. [9, Problem 31 on page 108]), the roots of $(nx^{n+1}-(n+1)x^n+1)/(x-1)^2$ have absolute value < 1. It is clear that 1 is a root of $w(x)$ with multiplicity 2. It follows that the remaining roots of $w(x)$ have absolute value > 1. Observe that $w'(x)$ only has cyclotomic roots. It follows that the $n-1$ roots of $w(x)$ with absolute value > 1 are distinct.

Now, we establish that if $B = 0$, then $h(x) = (x-1)^2$. We show instead the contrapositive. Suppose $h(x) \neq (x-1)^2$. Since $g(1) \neq 0$, $(x-1)^2$ is a factor of $h(x)$. The comments above imply that each of $g(x)$ and $h(x)$ must have a root with absolute value > 1. Furthermore, the absolute value of the product of the roots of either of these polynomials exceeds 1. Thus, $g(0)$ and $h(0)$ each has absolute value > 1. Note that $g(0)$ and $h(0)$ must be relatively prime since a common divisor p would divide both $g(0)h(0) = n$ and the coefficient of x in the product $g(x)h(x)$, namely $n+1$, which is clearly impossible.

We apply Proposition 1 with $m = n$ and $r = 1$. We consider first a prime divisor p of $h(0)$. Note then that $p|m$ and $p \nmid g(0)$. We let ℓ and m' be defined as in the proposition. Since $n \equiv 0 \pmod{p^\ell}$, we obtain $w(x) \equiv (x^n - 1)x \pmod{p^\ell}$. Suppose $\zeta^{m'} = 1$ and $\zeta \neq 1$. Then $\zeta^n = 1$ so that $w(\zeta) = n(1-\zeta)$. Since $\nu(1-\zeta) = 0$, we obtain $\nu(w(\zeta)) = \nu(n) = \ell$. Observe that the conclusions of Proposition 1 (ii) now follow as $w(0) = n \neq 0$ and $r = 1$ imply the hypotheses in Proposition 1 (ii) hold. Since $p \nmid g(0)$, we deduce that $\nu(A) > 0$. On the other hand,

$$A + B = \sum_{w(\alpha)=0} \left(\alpha - \frac{1}{\alpha} \right) = \frac{n+1}{n},$$

where we have used here that the roots of $w(x)$ other than 1 are distinct and that the summand above is 0 when $\alpha = 1$ (so that we can consider the sum above as a sum over roots of $w(x)$ with each root appearing to its multiplicity). Since $p|n$, we have $\nu((n+1)/n) < 0$. Since $\nu(A) > 0$, we obtain $B \neq 0$. Thus, we can deduce that if $B = 0$, then $h(x) = (x-1)^2$.

Now, suppose $B \neq 0$. Since $g(1) \neq 0$, we still have that $g(0)$ has absolute value > 1. If we repeat the argument in the previous paragraph but this time considering a prime p dividing $g(0)$ (so that the roles of $g(x)$ and $h(x)$ and the roles of A and B are switched), we obtain $A \neq 0$. In addition, we see that for each prime divisor p of n (so p divides $h(0)$ or $g(0)$), these arguments give from Proposition 1 (ii) that either $\nu(A) > 0$ or $\nu(B) > 0$. We deduce that at least one of the rational integers $g(0)A$ and $h(0)B$ is a multiple of p. Thus, if $p|n$, then $p|nAB$.

Next, we show that if $p|(n+1)$, then $p^2|nAB$. Since we now have that $AB \neq 0$, we will get the lower bound

$$n|AB| \geq \Big(\prod_{p|(n+1)} p\Big)^2 \Big(\prod_{p|n} p\Big). \tag{1}$$

We apply Proposition 1 with $m = n+1$ and $r = 0$. Thus, p is a prime divisor of m. Again, we let ℓ and m' be defined as in the proposition. Since $n \equiv -1 \pmod{p^\ell}$, we obtain $w(x) \equiv x^{n+1} - 1 \pmod{p^\ell}$. If $\zeta^{m'} = 1$, then $\zeta^{n+1} = 1$ so that $w(\zeta) = (n+1)(1-\zeta)$. If also $\zeta \neq 1$, then $\nu(1-\zeta) = 0$ and we obtain $\nu(w(\zeta)) = \nu(n+1) = \ell$. Thus, we can apply Proposition 1 (i). We obtain $\nu(A) > 0$ and $\nu(B) > 0$. Therefore, each of the rational integers $g(0)A$ and $h(0)B$ is a multiple of p. It easily follows that the integer nAB is divisible by p^2, and we obtain (1).

To obtain an upper bound for $n|AB|$, we use the following result about the complex zeroes of $w(x)$.

Lemma 7. *If $n \geq 2$ and $re^{i\theta}$ (with $r, \theta \in \mathbb{R}$) is a root of $w(x) = x^{n+1} - (n+1)x + n$, then $|r-1| < (5/n)\log n$.*

The result is essentially contained in [2] and [8]. It can be established by observing $w(\alpha) = 0$ implies $|\alpha^{n+1}| \leq |(n+1)\alpha - n| \leq (2n+1)|\alpha|$ so that

$$|\alpha| \leq (2n+1)^{1/n} = \exp\left(\frac{\log(2n+1)}{n}\right) \leq 1 + \frac{2\log(2n+1)}{n} \leq 1 + \frac{5\log n}{n}.$$

Observe that since the roots of $w(x)$ other than 1 have absolute value > 1, Lemma 7 implies that for all integers $n \geq 2$, if $re^{i\theta} \neq 1$ is a root of $w(x)$, then $0 < r - 1 < (5/n)\log n$.

Next, we show that

$$|A| \leq 10\log n \quad \text{and} \quad |B| \leq 10\log n. \tag{2}$$

Using $\overline{\beta}$ to denote the conjugate of β, we can rearrange the terms in the definition of A to obtain

$$A = \sum_{g(\beta)=0} \left(\beta - \frac{1}{\overline{\beta}}\right).$$

Since $g(\beta) = 0$ implies β is a root of $w(x)$, we deduce that if $\beta = re^{i\theta}$, then

$$\left|\beta - \frac{1}{\overline{\beta}}\right| = r - \frac{1}{r} \leq \frac{10\log n}{n}.$$

The first inequality in (2) now follows. The second inequality is deduced in an analogous manner. From (2), we obtain the estimate

$$n|AB| \leq 100n(\log n)^2. \tag{3}$$

Since $AB \neq 0$, we deduce from (1) and (3) that

$$\Big(\prod_{p|(n+1)} p\Big)^2 \Big(\prod_{p|n} p\Big) \leq 100n(\log n)^2.$$

Since $n \leq t$, it follows that

$$\prod_{p|(n+1)} p \ll t^{1/3}(\log t)^{2/3} \quad \text{or} \quad \prod_{p|n} p \ll t^{1/3}(\log t)^{2/3}.$$

Theorem 1 is now a consequence of the following

Lemma 8. *Let $\theta > 0$. For n a positive integer, define $Q(n) = \prod_{p|n} p$. Then for every $\varepsilon > 0$, the number of $n \leq t$ for which $Q(n) \leq t^\theta$ is $O(t^{\theta+\varepsilon})$*

Proof. Observe that $Q(n)$ is always squarefree. For each squarefree number $m = p_1 p_2 \cdots p_s \leq t^\theta$ where each p_j denotes a prime with $p_1 < p_2 < \cdots < p_s$, the number of $n \leq t$ for which $Q(n) = m$ is is equal to the number of solutions in positive integers $x_1, x_2, \ldots, x_s$ to

$$x_1 \log p_1 + x_2 \log p_2 + \cdots + x_s \log p_s \leq \log t.$$

We consider the p_j which are $\leq \sqrt{\log t}$ first. Suppose p_k is the largest of these. Clearly $k \leq \sqrt{\log t}$ and each x_j is bounded by $2 \log t$. Thus, the number of choices for $x_1, x_2, \ldots, x_k$ is $\leq (2 \log t)^{\sqrt{\log t}} \ll \exp\big(2\sqrt{\log t}\log\log t\big)$. Now, each remaining p_j satisfies $p_j > \sqrt{\log t}$ so that $\log p_j > (1/2)\log\log t$. Hence,

$$\big(x_{k+1} + x_{k+2} + \cdots + x_s\big)\frac{\log\log t}{2} \leq x_{k+1}\log p_{k+1} + x_{k+2}\log p_{k+2} + \cdots + x_s \log p_s \leq \log t.$$

Let N denote the greatest integer $\leq 2\log t/(\log\log t)$. Then the number of choices for $x_{k+1}, x_{k+2}, \ldots, x_s$ is bounded by the number of solutions to $x_{k+1} + x_{k+2} + \cdots + x_s \leq N$ in positive integers $x_{k+1}, x_{k+2}, \ldots, x_s$. Equivalently, we seek a bound on the number of solutions to

$$y_{k+1} + y_{k+2} + \cdots + y_s \leq N - s - k$$

in non-negative integers $y_{k+1}, y_{k+2}, \ldots, y_s$. Each such solution corresponds to a unique non-negative binary number consisting of $\leq N - 1$ digits given by y_{k+1} ones, followed by 1 zero, followed by y_{k+2} ones, followed by 1 zero, and so on (ending with y_s ones). It follows that there are $\leq 2^N$ choices for $x_{k+1}, x_{k+2}, \ldots, x_s$ as above. Thus, the number of possibilities for the s positive integers $x_1, x_2, \ldots, x_s$ is

$$\ll \exp\big(2\sqrt{\log t}\log\log t\big) \times 2^{2\log t/(\log\log t)} \ll \exp\left(\frac{2\log t}{\log\log t}\right) \ll t^\varepsilon.$$

This is a bound on the number of $n \leq t$ for which $Q(n) = m$ for some given squarefree $m \leq t^\theta$. Letting m vary, the lemma follows. ■

5. A Proof of Theorem 2

Let n denote a positive integer, and set

$$f(x) = 1 + x + x^2 + \cdots + x^n.$$

Our goal is to show that for each positive integer k and for most $n \le t$, the polynomial $f^{(k)}(x)$ is irreducible. As in the previous section, we will make use of Proposition 1. The main difficulty we will encounter is in showing that the condition $\nu(w(\zeta)) = \ell$ is satisfied in Proposition 1. Indeed, already for $k = 2$, it is the case that in many instances $\nu(w(\zeta)) \ne \ell$ when the other conditions of Proposition 1 hold. Thus, it will become necessary to bound the number of times $\nu(w(\zeta)) \ne \ell$. For this purpose, we will introduce an auxiliary polynomial $u(x)$ (see the discussion after Lemma 14) that depends on k and r but not on n and which has the property that $\nu(w(\zeta)) \ne \ell$ if and only if $\nu(u(\zeta)) > 0$. This allows us to obtain the bound we need on the number of times $\nu(w(\zeta)) \ne \ell$, and we proceed by applying Proposition 1 as in the previous section.

We begin with a lemma which is easily established by induction. The details of the proof are left to the reader.

Lemma 9. *Let k be a positive integer $\le n-1$. Then*

$$f^{(k)}(x) = \frac{1}{(x-1)^{k+1}} \left(\sum_{j=n-k+1}^{n+1} (-1)^{n+1-j} \binom{k}{n+1-j} \left(\prod_{\substack{i=n-k+1 \\ i \ne j}}^{n+1} i \right) x^j + (-1)^{k+1} k! \right).$$

We also make use of

Lemma 10. *Let n and k be positive integers with $k \le n-1$. Then each root of $f^{(k)}(x)$ has absolute value < 1.*

Proof. Observe that the roots of $f(x)$ are on the unit circle $\{z : |z| = 1\}$ and that $f(x)$ has no repeated roots. As in Section 4, we use that the roots of the derivative of a polynomial in $\mathbb{R}[x]$ lie in the convex hull of the roots of the polynomial. It follows that all the derivatives of $f(x)$ have only roots with absolute value < 1. ■

Lemma 11. *Let n and k be positive integers with $k \le n-1$. Let j be an integer satisfying $n-k+1 \le j \le n+1$. Then*

$$\binom{k}{n+1-j} \left(\prod_{\substack{i=n-k+1 \\ i \ne j}}^{n+1} i \right)$$

is divisible by $k!$.

Proof. Observe that

$$\prod_{\substack{i=n-k+1 \\ i \ne j}}^{n+1} i = \left(\prod_{i=j+1}^{n+1} i \right) \left(\prod_{i=n-k+1}^{j-1} i \right),$$

a product of $n+1-j$ consecutive integers times a product of $k-(n+1-j)$ positive integers. The first of these products on the right is therefore divisible by $(n+1-j)!$ and the second is divisible by $(k-(n+1-j))!$. It follows that

$$\binom{k}{n+1-j}\Bigg(\prod_{\substack{i=n-k+1\\ i\neq j}}^{n+1} i\Bigg) = \frac{k!}{(n+1-j)!(k-(n+1-j))!}\Bigg(\prod_{i=j+1}^{n+1} i\Bigg)\Bigg(\prod_{i=n-k+1}^{j-1} i\Bigg)$$

is an integer multiple of $k!$. The lemma follows. ■

Lemma 11 is not really necessary for what follows. But it makes matters slightly easier. Note that it follows from Lemma 11 that if α is a root of $f^{(k)}(x)$, then $1/\alpha$ is an algebraic integer.

Lemma 12. *Let n and k be positive integers with $k \le n-1$. Let m be an integer satisfying $n-k+1 \le m \le n+1$. Set $r = n+1-m$. Then*

$$(-1)^{n+k-m}\binom{k}{n+1-m}\Bigg(\prod_{\substack{i=n-k+1\\ i\neq m}}^{n+1} i\Bigg) \equiv -k! \pmod{m},$$

and there is a constant $\alpha(k,r)$ depending only on r and k and independent of n such that

$$\frac{1}{m}\Bigg((-1)^{n+k-m}\binom{k}{n+1-m}\Bigg(\prod_{\substack{i=n-k+1\\ i\neq m}}^{n+1} i\Bigg) + k!\Bigg) \equiv \alpha(k,r) \pmod{m}.$$

Proof. Consider the function

$$F(x) = (x+r)(x+r-1)\cdots(x+1)\times(x-1)(x-2)\cdots(x-(k-r)).$$

Observe that

$$F(m) = \prod_{\substack{i=n-k+1\\ i\neq m}}^{n+1} i.$$

The constant term of $F(x)$ is $(-1)^{k-r}r!(k-r)! = (-1)^{k+m-n-1}(n+1-m)!(k+m-n-1)!$. Thus, $F(m) \equiv (-1)^{k+m-n-1}(n+1-m)!(k+m-n-1)! \pmod{m}$. Writing $\binom{k}{n+1-m}$ as $k!/((n+1-m)!(k+m-n-1)!)$, the first congruence in the lemma follows.

Observe that $(-1)^{n+k-m}\binom{k}{n+1-m} = (-1)^{r+k-1}\binom{k}{r}$. The above shows that $F(x) = f_0 + f_1x + G(x)x^2$ where $(-1)^{r+k-1}\binom{k}{r}f_0 = -(k!)$, f_1 is the coefficient of x in $F(x)$ (which depends only on r and k), and $G(x) \in \mathbb{Z}[x]$. Since

$$(-1)^{n+k-m}\binom{k}{n+1-m}\Bigg(\prod_{\substack{i=n-k+1\\ i\neq m}}^{n+1} i\Bigg) + k!$$

is the same as $(-1)^{r+k-1}\binom{k}{r}F(m)+k!$, we deduce that the expression on the left-hand side of the second congruence is congruent modulo m to $(-1)^{r+k-1}\binom{k}{r}$ times f_1. The lemma follows. ∎

We fix a positive integer k and consider $n \geq k+1$. Let $w(x)$ be $(-1)^{k-1}/k!$ times the reciprocal polynomial of the numerator of $f^{(k)}(x)$ in Lemma 9 where k is a positive integer. In other words, we set

$$w(x) = x^{n+1} + \frac{1}{k!}\sum_{j=n-k+1}^{n+1}(-1)^{n+k-j}\binom{k}{n+1-j}\Bigg(\prod_{\substack{i=n-k+1\\ i\neq j}}^{n+1} i\Bigg)x^{n+1-j}.$$

This can be rewritten as

$$w(x) = x^{n+1} + \frac{1}{k!}\sum_{j=0}^{k}(-1)^{k+j-1}\binom{k}{j}\Bigg(\prod_{\substack{0\leq i\leq k\\ i\neq j}}(n+1-i)\Bigg)x^{j}.$$

Note that Lemma 11 implies $w(x) \in \mathbb{Z}[x]$.

Let m be an integer with $n-k+1 \leq m \leq n+1$, and let p be a prime divisor of m with $p > k$ (if it exists). Define r, ℓ and m' as in Proposition 1. It follows from the first congruence in Lemma 12 that $w(x) \equiv (x^m - 1)x^r \pmod{p^\ell}$. The definition of m implies that $0 \leq n+1-m = r \leq k < p$. Except for the condition that $\nu(w(\zeta)) = \ell$, the conditions of Proposition 1 are clearly satisfied. In addition to the condition $\nu(w(\zeta)) = \ell$, we will want that either both A and B are non-zero or both C and D are non-zero. We address these matters next.

Since $w(x) \equiv (x^m-1)x^r \pmod{p^\ell}$, there is a polynomial $v(x)$ in $\mathbb{Z}[x]$ such that $w(x) = (x^m-1)x^r + p^\ell v(x)$. Setting $x = \zeta$ where $\zeta^{m'} = 1$, we deduce $\nu(w(\zeta)) \geq \ell$. We will not be able to prove in general that $\nu(w(\zeta)) = \ell$, but instead we will show that typically this is the case.

Lemma 13. *Let $u(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$. Let p be a prime not dividing b_s. Then there exist $\leq s$ different numbers ζ such that for some positive integer m' relatively prime to p, we have $\zeta^{m'} = 1$ and $\nu(u(\zeta)) > 0$.*

Proof. Let $x_1, x_2, \ldots, x_s$ be the s not necessarily distinct p-adic roots of $u(x)$. If ζ is as in the lemma, then $\nu(\zeta - x_i) > 0$ for some $i \in \{1, 2, \ldots, s\}$. If ζ and ζ' are distinct roots of unity as in the lemma and i is such that both $\nu(\zeta - x_i) > 0$ and $\nu(\zeta' - x_i) > 0$, then we would have $\nu(\zeta - \zeta') > 0$, contradicting Lemma 6. Hence, for each $i \in \{1, 2, \ldots, s\}$, there is at most one ζ as in the lemma for which $\nu(\zeta - x_i) > 0$. The lemma follows. ∎

Lemma 14. *Let $u(x) = \sum_{j=0}^{s} b_j x^j \in \mathbb{Z}[x]$ with $u(1) \neq 0$, let $z \geq \max\{|u(1)|, |b_s|, 2\}$, and let m' be a positive integer. Then there is a constant c (depending only on $u(x)$) such that there are $\leq cm'/(\log z)$ different primes p satisfying $\gcd(p, m') = 1$, $p > z$, and there is a ζ for which $\zeta^{m'} = 1$, $u(\zeta) \neq 0$, and $\nu(u(\zeta)) > 0$.*

Proof. Let $H(x)$ be the part of $x^{m'} - 1$ which is coprime to $u(x)$; in other words, $H(x) = (x^{m'} - 1)/\gcd(u(x), x^{m'} - 1)$. Let R denote the resultant of $H(x)$ and $u(x)$. Then R is a non-zero integer which can be expressed as a product of numbers of the form $u(\zeta)$ where $\zeta^{m'}=1$ and $u(\zeta)\neq 0$. It follows that R is divisible by the product of the primes p in the lemma. If we consider the $\leq m'$ complex roots of $H(x)$ (all with absolute value 1), we see that R is bounded by $\left(\sum_{j=0}^{s}|b_j|\right)^{m'}$. Thus, if P denotes the number of primes p in the lemma, then

$$z^P \leq \left(\sum_{j=0}^{s}|b_j|\right)^{m'}.$$

It follows that $P \ll m'/\log z$, implying the lemma. ■

We describe next the polynomials $u(x)$ that we will use in Lemma 14. We return to our discussion of $w(x)$ and consider $\zeta\neq 1$ for which $\zeta^{m'}=1$. Since $\zeta^{n+1}=\zeta^{n+1-m}=\zeta^r$ and $r\leq k$, we can view $w(\zeta)$ as a polynomial in ζ of degree $\leq k$ which has, by Lemma 12, each coefficient divisible by m. We multiply this polynomial by $k!/m$ and use the second congruence in Lemma 12 to deal with the coefficient of ζ^r modulo m. For the remaining coefficients, observe that

$$\prod_{\substack{0\leq i\leq k\\ i\neq j, i\neq r}}(n+1-i)\equiv \frac{(-1)^{k-r}(k-r)!r!}{r-j} \pmod{m}.$$

Note that $-(k-r)\leq r-j\leq r$ so that this last expression is a rational integer. We deduce now that if

$$y_1(x)=\alpha(k,r)x^r+(-1)^{r-1}\sum_{\substack{0\leq j\leq k\\ j\neq r}}\binom{k}{j}\left(\frac{(-1)^j(k-r)!r!}{r-j}\right)x^j,$$

then $(k!/m)w(\zeta)-y_1(\zeta)=my_2(\zeta)$ for some polynomial $y_2(x)\in\mathbb{Z}[x]$. The coefficients of $y_1(x)$ only depend on r and k, and the coefficient of x^j for $j\neq r$ and $0\leq j\leq k$ in $y_1(x)$ is clearly non-zero. Recall that $w(1)=0$. Under the conditions of Proposition 1, $\nu(\zeta-1)=0$, so the factor of $x-1$ in $w(x)$ does not affect the value of $\nu(w(\zeta))$. We divide $y_1(x)$ by the highest power of $x-1$ that divides it and call the quotient $u(x)$. Observe that $\nu(w(\zeta))>\ell$ if and only if $\nu(y_1(\zeta))>0$ if and only if $\nu(u(\zeta))>0$. The advantage of dealing with $u(x)$ over $w(x)$ is that $u(x)$ depends only on k and r and not on n. With k still fixed, we let $r=n+1-m$ vary from 0 to k to obtain $k+1$ different polynomials $u(x)$. The idea now is to show that in many instances $\nu(u(\zeta))=0$.

With k and r fixed, we define a pair (m',p), with m' a positive integer and p a prime not dividing m', as a *bad* pair (rather than a bad apple) if there is a $\zeta\neq 1$ for which $\zeta^{m'}=1$ and $\nu(u(\zeta))>0$. For $t>0$, we determine an upper bound for the number of bad pairs (m',p) with $p^\ell m'\leq t$ for some positive integer ℓ. The number $p^\ell m'$ will correspond to m in Proposition 1. Observe that we do not require that ζ be a primitive m'th root of unity. This introduces some complications in bounding the number of bad (m',p).

For a given m', we can use Lemma 14 to bound the number of primes p for which $\nu(u(\zeta))>0$, but we must deal with the possibility not covered by Lemma 14 that $u(\zeta)=0$. We show next that there are at least three choices of $r\in\{0,1,\dots,k\}$, in the case $k\neq 2$, for which $u(x)$ has no cyclotomic factors. We will use the following preliminary result.

Lemma 15. *For each positive integer $k \geq 15$, there exist at least two distinct primes in the interval $(k/2, k-2]$.*

Proof. The result was verified directly for $15 \leq k < 200$. Now, suppose $k \geq 200$. Note that $1.96k/2 < k-2$. We show that for each $x \geq 100$ there is a prime in the interval $(x, 1.4x]$; the lemma then follows since then there is a prime in the interval $(k/2, 1.4k/2]$ and a prime in the interval $(1.4k/2, 1.96k/2] \subseteq (1.4k/2, k-2]$. Define $\vartheta(x) = \sum_{p \leq x} \log p$. We make use of the estimate from Rosser and Schoenfeld [10] that

$$x\left(1 - \frac{1}{\log x}\right) < \vartheta(x) < x\left(1 + \frac{1}{2\log x}\right) \qquad \text{for all } x \geq 41.$$

To establish there is a prime in $(x, 1.4x]$ for $x \geq 100$, it suffices therefore to show

$$1.4x\left(1 - \frac{1}{\log(1.4x)}\right) \geq x\left(1 + \frac{1}{2\log x}\right).$$

This is a simple matter to verify; indeed, the inequality above holds for all $x \geq 100$ follows from the fact that it holds for $x = 100$. ■

Lemma 16. *Let k be an integer with $k = 3$ or $k \geq 5$. For each $r \in \{k-2, k-1, k\}$, the polynomial $u(x)$ defined above has no cyclotomic divisors.*

Proof. We work in the field of complex numbers. Fix k and r as in the lemma. By the definition of $u(x)$, we know that 1 is not a root of $u(x)$. We assume now that $u(x)$ has a root which is a root of unity. Then $u(\zeta) = 0$ for some $\zeta \neq 1$ satisfying $\zeta^d = 1$ for some positive integer d. We take d minimal and note that $d \geq 2$. We justify first that $d \neq 2$.

If $d = 2$, then -1 is a root of $u(x)$ and, hence, also of $y_1(x)$. One checks directly that $y_1(-1) \neq 0$ in the case that $k = 3$ and $r = 1$. For the remaining choices of k and r, we use the definition of $y_1(x)$ together with the a formula for $\alpha(k, r)$. In particular, the definition of $y_1(x)$ and the choice of r imply that, for $k \geq 5$, if $y_1(-1) = 0$, then $\alpha(k, r) > 0$. From the proof of Lemma 12, we see that $\alpha(k, r)$ is $(-1)^{r+k-1}\binom{k}{r}$ times the coefficient f_1 of x in

$$F(x) = (x+r)(x+r-1)\cdots(x+1) \times (x-1)(x-2)\cdots(x-(k-r)).$$

When $r = k$, every coefficient of $F(x)$ is positive and we easily deduce that $\alpha(k, r) < 0$. Now, suppose $r = k-2$ and $k \geq 5$ (we have already dealt with $k = 3$). Since the coefficient of x in the expanded product $(x+2)(x+1)(x-1)(x-2)$ is zero and its constant term is 4, we see that f_1 is simply 4 times the coefficient of x in $(x+r)(x+r-1)\cdots(x+3)$. Thus, $f_1 > 0$, and we conclude that $\alpha(k, r) < 0$. It remains to consider the case that $r = k-1$. One checks directly that in this case

$$f_1 = (k-1)! - \sum_{j=1}^{k-1} \frac{(k-1)!}{j} = -\sum_{j=2}^{k-1} \frac{(k-1)!}{j}.$$

Since $k \geq 3$, we obtain $\alpha(k, r) = \alpha(k, k-1) < 0$. We deduce that $u(-1) \neq 0$ so that $d > 2$.

The definition of $u(x)$ implies that we must also have $y_1(\zeta)=0$. Using the definition of $y_1(x)$, we consider the expression $y_1(\zeta)/((k-r)!r!\zeta^r)$ as a sum of $k+1$ terms and observe that it is an element of $\mathbb{Q}(\zeta)$ which is an extension of degree $\phi(d)$ over $\mathbb{Q}$. Thus, we can rewrite the expression as a polynomial in $\{1,\zeta,\dots,\zeta^{\phi(d)-1}\}$ with rational coefficients. Call this polynomial $\rho(\zeta)$.

We consider first the case that $k\geq 15$. By Lemma 15, there are two primes in the interval $(k/2,k-2]$. Call these primes p_1 and p_2. We show that at least one of these two primes does not divide d. Since ζ is a root of $y_1(x)$, a non-zero polynomial of degree k, we deduce that the degree of the minimal polynomial for ζ (in $\mathbb{Q}[x]$) is $\leq k$. Hence, $\phi(d)\leq k$. On the other hand, each of p_1 and p_2 is $>k/2$. If p_1 and p_2 are both factors of d, then we would have

$$k\geq\phi(d)\geq\phi(p_1p_2)=(p_1-1)(p_2-1)>\left(\frac{k}{2}-1\right)^2,$$

which is easily seen to be impossible for the k under consideration. Thus, either p_1 or p_2 does not divide d. Now, fix p to be a prime in $(k/2,k-2]$ which does not divide d. Consider $j'=r-p\in\{0,1,\dots,k\}$. Observe that for each $j\in\{0,1,\dots,k\}$ we have

$$-p<r-k\leq r-j\leq r<2p.$$

It follows that in the sum defining $y_1(x)$, the expression $r-j$ in the summand is divisible by p if and only if $j=j'$. Since $p\in(k/2,k]$, we get that $p||k!$. Since $r\leq k$, we clearly have that $p|(k-r+p)!$. We obtain

$$\binom{k}{j'}=\frac{k!}{(r-p)!(k-r+p)!}\in\mathbb{Z}\qquad\Longrightarrow\qquad p\text{ does not divide }\binom{k}{j'}.$$

If we consider the $k+1$ non-zero terms in $y_1(x)/((k-r)!r!x^r)$, we see that the constant term $\alpha(k,r)/((k-r)!r!)$ may have denominator divisible by p (and, in fact, does though this is not needed) and the denominator of the coefficient of $x^{j'-r}=x^{-p}$ is divisible by p. No other denominators will be divisible by p.

We justify momentarily that ζ^{-p} when expressed as a polynomial in ζ of degree $\leq\phi(d)$ includes a term ζ^i with $i>0$ and with coefficient not divisible by p. More precisely, we show that $\zeta^{-p}-b=pG(\zeta)$ is impossible if $b\in\mathbb{Z}$ and $G(x)\in\mathbb{Z}[x]$. It will then follow that $\rho(\zeta)$ has at least one coefficient which can be expressed as a rational number (possibly 0) with denominator not divisible by p plus a non-zero rational number with denominator divisible by p. This coefficient is clearly non-zero. It follows that $\rho(\zeta)\neq 0$, and we deduce that $y_1(\zeta)\neq 0$. This is a contradiction. Hence, $u(x)$ does not have a cyclotomic factor for $k\geq 15$.

Assume that there exist $b\in\mathbb{Z}$ and $G(x)\in\mathbb{Z}[x]$ such that $\zeta^{-p}-b=pG(\zeta)$. By applying the automorphisms of $\mathbb{Q}(\zeta)$ fixing $\mathbb{Q}$, we may replace ζ in this equation with any primitive root of $x^d-1=0$. Since $d>2$, we deduce that there are ζ_1 and ζ_2 primitive roots of $x^d-1=0$ with $\zeta_1\neq\zeta_2$ satisfying $\zeta_1^{-p}-b=pG(\zeta_1)$ and $\zeta_2^{-p}-b=pG(\zeta_2)$. Subtracting, we obtain $\zeta_2^{-p}-\zeta_1^{-p}=p\big(G(\zeta_2)-G(\zeta_1)\big)$. Setting $\zeta_3=\zeta_1^p\zeta_2^{-p}\in\mathbb{Q}(\zeta)$, we easily deduce that $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta_3-1)$ is a multiple of p. Since ζ_3-1 is a root of $1+(x+1)+(x+1)^2+\cdots+(x+1)^{d-1}$, a monic polynomial with constant term d, we obtain a contradiction. Thus, the lemma is established in the case that $k \geq 15$.

For $k \leq 14$, the polynomials $u(x)$ were computed explicitly using Maple V (Release 4) and it was determined that if $k = 3$ or $5 \leq k \leq 14$, then each $u(x)$ has no cyclotomic factors. The lemma follows. ■

For each $k \geq 2$, we ideally will want three of the polynomials $u(x)$, as r varies, to be free of cyclotomic divisors. Lemma 16 shows that such polynomials exist unless $k = 2$ or $k = 4$. In the case $k = 4$, a simple computation verifies that $u(x)$ has no cyclotomic divisors if $r \in \{1, 3, 4\}$. For $k = 2$, we will not have three such $u(x)$. In this case, $u(x)$ has no cyclotomic divisors if $r = 0$ or if $r = 2$. In the case $r = 1$, we have $u(x) = -x - 1$ which has the cyclotomic factor $x + 1$. As a consequence, we will make a slightly different argument in the case $k = 2$.

Suppose now that $u(x)$ is a polynomial as above having no cyclotomic factors. We consider $n \leq t$ with t sufficiently large. We also suppose that $p > z \geq k$ with z sufficiently large (as in Lemma 14). For a positive integer $d > 1$, we define $S(d)$ to be the set of primes p not dividing d for which there is a *primitive* dth root of unity ζ such that $\nu(u(\zeta)) > 0$. Observe that if (m', p) is a bad pair, then $p \in S(d)$ for some d dividing m'. Furthermore, if $p \in S(d)$ and ζ is a primitive dth root of unity for which $\nu(u(\zeta)) > 0$, then for every positive integer m'', we have $\zeta^{dm''} = 1$ so that (dm'', p) is a bad pair. It is not difficult to see that every bad pair can be obtained in this manner; in other words, every bad pair is of the form (dm'', p) where $p \in S(d)$ and m'' is a positive integer. Since we are only interested in bad pairs (m', p) with $p^\ell m' \leq t$ for some positive integer ℓ, we only need to consider bad pairs (dm'', p) that satisfy $pdm'' \leq t$. In other words, for a given $d > 1$ and a given $p \in S(d)$, there are $\leq m'' \leq t/(dp)$ bad pairs (dm'', p) for us to consider.

The fact that we are only interested in $p > z$ produces another restriction on the m' we are considering. This is apparent in the statement of Lemma 14. If we set ε to be a positive number $< 1/c$, then Lemma 14 implies there are no primes p in $S(d)$ whenever $d \leq \varepsilon \log z$. This gives us

Lemma 17. *Given the notation above, the number of bad pairs (m', p) for which $p > z$ and $pm' \leq t$ is bounded by*

$$\sum_{d > \varepsilon \log z} \sum_{\substack{p \in S(d) \\ p > z}} \frac{t}{dp}.$$

We now prove

Lemma 18. *Given the notation above, the number of bad pairs (m', p) for which $p > z$ and $pm' \leq t$ is $\ll t \log\log t / \sqrt{z \log z}$.*

Proof. We rewrite the sum in Lemma 17 as $S_1 + S_2$ where

$$S_1 = \sum_{\varepsilon \log z < d \leq \sqrt{z \log z}} \sum_{\substack{p \in S(d) \\ p > z}} \frac{t}{dp} \quad \text{and} \quad S_2 = \sum_{d > \sqrt{z \log z}} \sum_{\substack{p \in S(d) \\ z < p \leq t}} \frac{t}{dp}.$$

We use Lemma 14 to estimate the number of $p \in S(d)$ which are $> z$ to deduce that

$$S_1 \leq \sum_{\varepsilon \log z < d \leq \sqrt{z \log z}} \sum_{\substack{p \in S(d) \\ p > z}} \frac{t}{dz} \ll \sum_{d \leq \sqrt{z \log z}} \frac{t}{z \log z} \ll \frac{t}{\sqrt{z \log z}}.$$

To estimate S_2, we observe that Lemma 13 implies that each prime p can appear in at most k different sets $S(d)$. Since each d in the summand for S_2 is $> \sqrt{z \log z}$, we deduce

$$S_2 = \sum_{d > \sqrt{z \log z}} \sum_{\substack{p \in S(d) \\ z < p \leq t}} \frac{t}{dp} \leq \sum_{z < p \leq t} \frac{kt}{p\sqrt{z \log z}} \ll \frac{t \log \log t}{\sqrt{z \log z}}.$$

The lemma follows. ■

Consider a pair (m', p) which is not bad. Suppose $w(x) = g(x)h(x)$ with A, B, C, and D defined as in Proposition 1 except with each root in the sums appearing to their multiplicities. Note the comment after Proposition 1. Suppose that $p||m$. Observe that the condition $p > z \geq k$ implies p divides only one of the k numbers between $n-k+1$ and $n+1$, so $p|| \prod_{0 \leq i < k}(n+1-i)$. Suppose now that $m \neq n+1$ so $r > 0$. We can apply Proposition 1 (ii) as $p|| \prod_{1 \leq i \leq k}(n+1-i)$ implies $\ell = 1$. We are now ready to show

Lemma 19. *Suppose that $w(x) = g(x)h(x)$ with A, B, C, and D defined as in Proposition 1. Suppose further that each of $g(x)$ and $h(x)$ has a root different from 1 and that there is a prime $p > k$ such that $p|| \prod_{1 \leq i \leq k}(n+1-i)$. Then either $AB \neq 0$ or $CD \neq 0$.*

Proof. We begin by showing that either A or C is non-zero and either B or D is non-zero. Observe that

$$A + C = \sum_{g(\beta)=0} \left(1 - \frac{1}{\beta}\right).$$

The roots β of $w(x)$ other than 1 have absolute value > 1 (by Lemma 10) so that the numbers $1/\beta$ are strictly inside the unit circle centered at the origin in the complex plane. This implies that the real part of each summand above is non-negative and at least one summand is positive. We deduce that the right-hand side above is non-zero and, hence, either A or C is non-zero. Similarly, one obtains that either B or D is non-zero.

If $A = 0$, then we have $C \neq 0$ and we assume $D = 0$. Proposition 1 (ii) implies $\nu(B) > 0$. On the other hand, the definition of A and B together with the coefficients of $w(x)$ give

$$A + B = \sum_{w(\alpha)=0} \left(\alpha - \frac{1}{\alpha}\right) = \frac{k(n+1)}{n}. \tag{4}$$

Since $p \nmid k(n+1)$ and $A = 0$, we deduce that $\nu(A+B) = \nu(B) \leq 0$. This apparent contradiction implies that $D \neq 0$ so that $CD \neq 0$. A similar argument can be done to show that if $C = 0$, then $AB \neq 0$. The lemma follows. ■

We now give the proof of Theorem 2. We fix $k \geq 2$ (the case $k = 1$ is covered by Theorem 1). We begin by presenting the argument for $k = 3$ and $k \geq 5$ and then explain the necessary changes in the argument for $k=2$ and $k=4$. We consider z sufficiently large and, in particular, $\geq k$. Let $t>0$. For m an integer with $n-k+1 \leq m \leq n-k+3$, we consider p such that $p|m$ and $p>z$ (if it exists). For each choice of $r=n-m+1 \in \{k-2, k-1, k\}$, we construct $u(x)$ as above and count the number of bad pairs corresponding to $u(x)$. We let T denote the set of $n \leq t$ for which $\nu(u(\zeta))>0$ for some such m and p. By Lemma 18, there are $\ll t \log\log t/\sqrt{z \log z}$ bad pairs (m', p). With ℓ and m' as in Proposition 1, we see that since $p>z$ and $p^\ell m' \leq t$, we have $\ell \leq (\log t)/(\log p) \leq (\log t)/(\log z)$. The number of $n \in T$ is bounded by the number of triples (m', p, ℓ) with (m', p) a bad pair for some $u(x)$ (with $r \in \{k-2, k-1, k\}$) and $\ell \leq (\log t)/(\log z)$. Therefore, we deduce that

$$|T| \ll \frac{t \log\log t}{\sqrt{z \log z}} \times \frac{\log t}{\log z} = \frac{t (\log t) \log\log t}{\sqrt{z \log^3 z}}.$$

We will consider those p for which $p||m$ (in other words, the case when $\ell=1$). If $n \leq t$ and $n \notin T$, then the equation $\nu(w(\zeta))=\ell=1$ holds whenever $n-k+1 \leq m \leq n-k+3$, $m=p^\ell m'=pm'$, $p \nmid m'$, $\zeta \neq 1$, and $\zeta^{m'}=1$. Therefore, we can apply Proposition 1 for these n, m, and p. However, before doing so, it will be convenient for us to restrict our attention to n for which $n(n-1)\cdots(n-k+1)$ is not divisible by a large powerful number (a positive integer d such that if p is a prime divisor of d, then $p^2|d$). More precisely, we set

$$T' = \{n \leq t : \exists \text{ a powerful number } d > k!^k t^{1/2} \text{ dividing } n(n-1)\cdots(n-k+1)\}.$$

We wish to ignore the elements of T'; however, first we obtain an upper bound for $|T'|$.

Let $n \in T'$, and let p be a prime divisor of d where d is the largest powerful number dividing n. Consider those p that occur as a factor of more than one of $n+1-i$ with $i \in \{1, 2, \ldots, k\}$. Clearly $p \leq k$. For each such p, there are trivially no more than $k-1$ different $i \in \{1, 2, \ldots, k\}$ such that $p||(n+1-i)$. Set $d(i)=\gcd(n+1-i, d)$, and let $d'(i)$ denote the largest powerful number dividing $d(i)$. Then $\prod_{i=1}^k (d(i)/d'(i))$ divides $\prod_{p \leq k} p^{k-1}$. Note that $d=\prod_{i=1}^k d(i)$. We deduce that

$$t^{1/2} < \frac{d}{k!^k} \leq \frac{\prod_{i=1}^k d(i)}{\prod_{p \leq k} p^{k-1}} \leq \prod_{i=1}^k d'(i) = \prod_{1 \leq i \leq k} \prod_{\substack{p^e || (n+1-i) \\ e \geq 2}} p^e \leq \prod_{1 \leq i \leq k} \Bigg(\prod_{\substack{p^e || (n+1-i) \\ e \geq 2}} p^{[e/2]} \Bigg)^3.$$

Thus, one of the numbers $n+1-i$ with $i \in \{1, 2, \ldots, k\}$ is divisible by the square of an integer $> t^{1/(6k)}$. Hence,

$$|T'| \leq k + k \sum_{\ell > t^{1/(6k)}} \frac{t}{\ell^2} \ll t^{(6k-1)/(6k)}.$$

Now, we consider $n \leq t$ with $n \notin T \cup T'$ and assume that $f^{(k)}(x)$ is reducible. Lemma 10 implies that $f^{(k)}(x)$ can be expressed as a product of two polynomials with roots different from 1. It follows that $w(x)=g(x)h(x)$ where each of $g(x)$ and $h(x)$ are monic polynomials with integer coefficients each having a root different from 1. We fix $m \in \{n-k+1, n-k+2, n-k+3\}$, and consider the notation of Proposition 1 (so, in particular, $p|m$) with the sums involving A, B, C, and D being taken over all roots to their multiplicities. Again, we suppose $p||m$ and $p > z \geq k$. We use Lemma 19 to obtain that either both A and B are non-zero or both C and D are non-zero.

Suppose that $AB \neq 0$. Since $p||m$ where $m \in \{n-k+1, n-k+2, n-k+3\}$ and since $p > z \geq k$, we deduce that

$$p|| \prod_{1 \leq i \leq k} (n+1-i).$$

Since $k \geq 3$, we have $r = n - m + 1 \geq k - 2 > 0$. We apply Proposition 1 (ii), noting that $\ell = 1$. We deduce that either $\nu(A) > 0$ or $\nu(B) > 0$.

Analogous to the proof of Theorem 1, we consider a multiple of AB that lies in $\mathbb{Z}$. Since $n \notin T'$, we can express $n(n-1)\cdots(n-k+1)$ as the product of two positive integers n_1 and n_2 where n_1 is a powerful number, $n_1 \leq k!^k t^{1/2}$, n_2 is squarefree, and $\gcd(n_1, n_2) = 1$. Note that $g(0)A \in \mathbb{Z}$, $h(0)B \in \mathbb{Z}$, and

$$g(0)h(0) = \frac{(-1)^{k-1}}{k!} \prod_{1 \leq i \leq k} (n+1-i) = \frac{(-1)^{k-1} n_1 n_2}{k!}. \tag{5}$$

It follows that each prime p dividing the denominator of A or B (as reduced fractions) must divide $n_1 n_2$. Suppose p divides the denominator of A or B and $p|n_2$. Since n_2 is squarefree, (5) implies that p divides at most one of $g(0)$ and $h(0)$. Since $g(0)A$ and $h(0)B$ are integers, we deduce that p divides at most one of the denominators of A and B. On the other hand, if p divides exactly one of these denominators, then (4) implies that p divides n. It follows now that $n_1 n AB \in \mathbb{Z}$.

We bound $|A|$ and $|B|$ using an argument similar to that used to obtain (2). The proof of Lemma 7 is easily modified to give that each root α of $w(x)$ satisfies

$$1 \leq |\alpha| < 1 + O_k\left(\frac{\log n}{n}\right).$$

Now, the argument for (2) gives that each of A and B is $\ll \log n$. We obtain

$$n_1 n AB \ll \big(t^{1/2}\big) t (\log t)^2 \ll t^2.$$

In the case that $AB \neq 0$ we deduce that

$$\prod_{m=n-k+1}^{n-k+3} \Bigg(\prod_{p||m, p>z} p \Bigg) \ll t^2. \tag{6}$$

We show next that this same inequality holds in the case that $CD \neq 0$.

Suppose that $CD \neq 0$. We follow the above argument for the case $AB \neq 0$ with the following changes. Both C and D are rational numbers by Proposition 1 and furthermore algebraic integers since $g(x)$ and $h(x)$ are monic. Hence, C and D and, hence, CD are in $\mathbb{Z}$. Instead of the bound on $|\alpha|$ for roots α of $w(x)$ obtained above, we use the weaker bound $|\alpha| \ll 1$. We deduce that each of C and D is $\ll t$. Now, (6) follows as before.

We have shown that if $n \notin T \cup T'$ and $f^{(k)}(x)$ is reducible, then (6) holds (where so far we are only considering $k = 3$ and $k \geq 5$). We show now that (6) does not hold for very many $n \leq t$. To get the result stated in the theorem, it is in fact sufficient to show that for almost all $m \leq t$, one has

$$\prod_{p || m,\, p > z} p \geq m^{1-(1/(k+2))}.$$

Let T'' denote the set of $m \leq t$ for which this inequality does not hold. Observe that if $m \in T''$, then either (i) m is divisible by the square of a prime $> z$, or (ii) m divided by the product above is divisible only by primes $\leq z$. The number of $m \leq t$ for which (i) holds is

$$\leq \sum_{m \leq t} \sum_{\substack{p > z \\ p^2 | m}} 1 \leq \sum_{p > z} \sum_{\substack{m \leq t \\ p^2 | m}} 1 \leq \sum_{p > z} \frac{t}{p^2} \ll \frac{t}{z \log z}.$$

For the number of $m \leq t$ satisfying (ii), we define S to be the set of such m which exceed $\sqrt{t}$. The number of remaining m is clearly $\leq \sqrt{t}$. For each $m \in S$, we have

$$\prod_{p \leq z} \prod_{\substack{1 \leq j < \infty \\ p^j | m}} p \geq m^{1/(k+2)} > t^{1/(2k+4)}.$$

Therefore,

$$\sum_{m \in S} \sum_{p \leq z} \sum_{\substack{1 \leq j < \infty \\ p^j | m}} \log p > \frac{|S| \log t}{2k+4}.$$

On the other hand, for z sufficiently large,

$$\sum_{m \in S} \sum_{p \leq z} \sum_{\substack{1 \leq j < \infty \\ p^j | m}} \log p \leq \sum_{1 \leq m \leq t} \sum_{p \leq z} \sum_{\substack{1 \leq j < \infty \\ p^j | m}} \log p$$

$$\leq \sum_{p \leq z} (\log p) \sum_{j=1}^{\infty} \sum_{\substack{1 \leq m \leq t \\ p^j | m}} 1 \leq \sum_{p \leq z} (\log p) \sum_{j=1}^{\infty} \frac{t}{p^j} = \sum_{p \leq z} \frac{t(\log p)}{p-1} \leq 2t \log z.$$

It follows that

$$|S| \ll \frac{t \log z}{\log t}.$$

We take $z = (\log t)^{10}$. Combining all the estimates above (including the ones for T and T'), we deduce that the number of $n \leq t$ for which $f^{(k)}(x)$ is reducible is $O(t \log\log t / \log t)$.

Next, we consider the cases $k = 4$ and $k = 2$. The case $k = 4$ is identical to the above except that we replace $m \in \{n-k+1, n-k+2, n-k+3\}$ with $m \in \{n-3, n-2, n\}$. Thus,

$r = n - m + 1 \in \{1, 3, 4\}$ and, as noted after the proof of Lemma 16, each corresponding $u(x)$ has no cyclotomic divisors. For $k = 2$, we consider only $m \in \{n-1, n+1\}$ so that $r \in \{0, 2\}$. The argument is slightly different here as each prime divisor p of $n+1$ satisfying $p > k$ does not divide the constant term of $w(x)$. In other words, with $r = 0$, we are led to applying Proposition 1 (i) rather than (ii). In this case, we deduce that each of $\nu(A)$, $\nu(B)$, $\nu(C)$, and $\nu(D)$ is positive. For $r = 2$, one makes use of Proposition 1 (ii) as before. We deduce that

$$\Bigg(\prod_{p || (n+1), p > z} p \Bigg)^2 \Bigg(\prod_{p || (n-1), p > z} p \Bigg) \ll t^2$$

instead of (6). The remainder of the argument for $k = 2$ is the same as before. Theorem 2 follows.

6. Proof of Theorem 4

We set

$$w(x) = p(x) = (n-1)(x^{n+1} - 1) - (n+1)(x^n - x).$$

We begin by describing the location of the complex zeroes of $w(x)$.

Lemma 20. *Let $n \geq 2$. Then 1 is a root of $w(x)$ with multiplicity 3. Furthermore, if n is odd, then -1 is a root of $w(x)$ with multiplicity 1.*

A proof of Lemma 20 can be given directly by considering the values of $w(x)$ and its derivatives at 1 and -1. We omit the details.

Lemma 21. *Let $n \geq 2$. If $w(\alpha) = 0$, then $|\alpha| = 1$.*

Proof. Observe that if θ is not an integer multiple of $2\pi/(n-1)$, then

$$\frac{\sin(\frac{n+1}{2}\theta)}{\sin(\frac{n-1}{2}\theta)} = \frac{e^{i(n+1)\theta/2} - e^{-i(n+1)\theta/2}}{e^{i(n-1)\theta/2} - e^{-i(n-1)\theta/2}} = \frac{e^{i(n+1)\theta} - 1}{e^{in\theta} - e^{i\theta}} = \frac{e^{-i(n+1)\theta} - 1}{e^{-in\theta} - e^{-i\theta}}.$$

Denote the left-hand side above by $F(\theta)$. It follows that if $F(\theta) = (n+1)/(n-1)$, then $e^{\pm i\theta}$ is a root of $w(x)$. For each positive integer $k < (n-1)/2$,

$$\frac{2k}{n+1} < \frac{2k}{n-1} < \frac{2(k+1)}{n+1}.$$

Define

$$I_k = \left[\frac{2\pi k}{n+1}, \frac{2\pi k}{n-1} \right) \bigcup \left(\frac{2\pi k}{n-1}, \frac{2\pi(k+1)}{n+1} \right).$$

Then it is easily checked that $F(\theta)$ takes on every real value for $\theta \in I_k$. In particular, for each positive integer $k < (n-1)/2$, there is a $\theta \in I_k$ such that $F(\theta) = (n+1)/(n-1)$ and, consequently, $w(e^{\pm i\theta}) = 0$. If n is even, then we obtain $n-2$ distinct roots of $w(x)$ different from ± 1 of the form $e^{i\theta}$. If n is odd, then we obtain $n-3$ distinct roots of $w(x)$ different from ± 1 of the form $e^{i\theta}$. Combining this information with Lemma 20 implies the desired result. ■

We consider $w(x) = g(x)h(x)$ as in the propositions. We take $g(x)$ so that $g(1) \neq 0$ and $g(-1) \neq 0$. If $p(x)$ does not factor as in the theorem, then we can find such $g(x)$ and $h(x)$ with each containing at least one root other than 1 and -1. We assume we have such a factorization of $w(x)$, and define A, B, C', and D' as in the propositions. Observe that if we obtain a contradiction for all but $O(t^{(4/5)+\varepsilon})$ different $n \leq t$, then Lemma 20 implies the theorem.

Let p be an odd prime divisor of $n+1$, and define ℓ and m' as in Proposition 2. Observe that $w(x) \equiv (n-1)(x^{n+1}-1) \pmod{p^\ell}$. If $\zeta \neq \pm 1$ and $\zeta^{m'} = 1$, then $w(\zeta)\zeta = (n+1)(\zeta-1)(\zeta+1)$. Clearly, $\nu(\zeta) = 0$. Also, Lemma 6 implies that $\nu(\zeta-1) = \nu(\zeta+1) = 0$. It follows that $\nu(w(\zeta)) = \ell$. From Proposition 2, we obtain $\nu(C')$ and $\nu(D')$ are positive.

Let p be an odd prime divisor of n, and define ℓ and m' as in Proposition 3. Then $w(x) \equiv -(x^n-1)(x+1) \pmod{p^\ell}$. If $\zeta \neq 1$ and $\zeta^{m'} = 1$, then $w(\zeta) = 2n(\zeta-1)$. We deduce that $\nu(w(\zeta)) = \ell$. From Proposition 3, we obtain $\nu(C')$ and $\nu(D')$ are positive.

By Lemma 21, the roots of $w(x)$ have absolute value 1. We easily deduce that $A = B = 0$. Let p be an odd prime divisor of $n-1$, and define ℓ and m' as in Proposition 4. Then $w(x) \equiv -(n+1)(x^{n-1}-1)x \pmod{p^\ell}$. If $\zeta \neq \pm 1$ and $\zeta^{m'} = 1$, then $w(\zeta) = (n-1)(\zeta-1)(\zeta+1)$. As in the case $p|(n+1)$ above, we obtain $\nu(w(\zeta)) = \ell$. From Proposition 4, we obtain that at least one of $\nu(C') > 0$ and $\nu(D') > 0$ holds.

Lemma 21 implies that for each root α of $w(x)$, the real part of $1-\alpha^2$ is positive unless $\alpha = \pm 1$. Since we are considering $g(x)$ and $h(x)$ to each have a root other than ± 1, the real parts of C' and D' are positive. Also, Lemma 21 implies that C' and D' are each $\ll n$. Since the leading coefficient of $w(x)$ is $n-1$, we deduce that $(n-1)^2 C'D'$ is a non-zero integer with absolute value $\leq (n-1)^2 n^2$.

Combining the above information, we see that if $n \leq t$, then

$$\Big(\prod_{p|(n+1), p>2} p \Big)^2 \Big(\prod_{p|n, p>2} p \Big)^2 \Big(\prod_{p|(n-1), p>2} p \Big) \ll (n-1)^2 |C'D'| \ll (n-1)^2 n^2 \ll t^4.$$

Theorem 4 now follows as a consequence of Lemma 8.

References

1. A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge, 1979.
2. A. Borisov, *On some polynomials allegedly related to the abc conjecture*, Acta Arith. **84** (1998), 109–128.
3. F. Q. Gouvêa, *p-adic Numbers, An Introduction*, Springer-Verlag, Berlin, 1997.
4. R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics, A Foundation for Computer Science*, Addison-Wesley, Reading, Massachusetts, 1989.
5. E. Gutkin, *Billiard Tables of Constant Width and Dynamical Characterizations of the Circle*, Abstract, Penn State Workshop, October, 1993.
6. N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, New York, 1977.
7. L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.
8. J.-L. Nicolas and A. Schinzel, *Localisation des zeros de polynomes intervenant en theorie du signal*, Cinquante ans de polynômes (Paris, 1988), Lecture Notes in Math., 1415, Springer-Verlag, Berlin (1990), 167–179.

9. G. Pólya and G. Szegö, *Problems and Theorems in Analysis I*, Springer-Verlag, New York, 1972.
10. J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–89.
11. T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations, Cambridge Tracts 87*, Cambridge Univ. Press, Cambridge, 1986.
12. I. Schur, *Einege Sätze über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, I*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse. **14** (1929), 125–136.
13. J. J. Sylvester, *On arithmetical series*, Messenger of Math. **21** (1892), 1–19.
14. L. Washington, *Cyclotomic Fields*, Springer-Verlag, New York, 1997.
15. E. Weiss, *Algebraic Number Theory*, Chelsea, New York, 1963.