THE IRREDUCIBILITY OF ALL BUT FINITELY MANY BESSEL POLYNOMIALS

Michael Filaseta*

1. Introduction

Grosswald conjectured that the Bessel Polynomials

$$y_n(x) = \sum_{j=0}^{n} \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

are all irreducible over the rationals and obtained several results concerning their irreducibility. The statement of this conjecture and his results are described in his book *Bessel Polynomials* [7]. The author in [4] established that almost all Bessel Polynomials are irreducible. More precisely, if $k(t)$ denotes the number of $n \le t$ for which $y_n(x)$ is *reducible*, then $k(t) = o(t)$. He later [5] observed that the argument could be strengthened to obtain $k(t) \ll t/\log\log\log t$. More recently, it was shown by Sid Graham and the author [6] that a simplification of these methods with some additional elementary arguments lead to $k(t) \ll t^{2/3}$. In this paper, we prove that $y_n(x)$ is irreducible for all but finitely many (possibly 0) positive integers n. Although the current methods lead to an effective bound on the number of reducible $y_n(x)$, such a bound would be quite large and we do not concern ourselves with it.

The coefficient of x^j in $y_n(x)$ is $\binom{n+j}{2j} \prod_{k=1}^{j}(2k-1)$ and, hence, integral. The constant term is 1. Thus, the irreducibility of $y_n(x)$ over the rationals is equivalent to the irreducibility of $y_n(x)$ over the integers. It is slightly more convenient to consider

$$z_n(x) = x^n y_n(2/x) = \sum_{j=0}^{n} \frac{(2n-j)!}{j!(n-j)!} x^j$$

*Research was supported in part by the NSA under grant number MDA904-92-H-3011.

rather than $y_n(x)$. The polynomials $z_n(x)$ are monic polynomials with integer coefficients, and $y_n(x)$ is irreducible if and only if $z_n(x)$ is irreducible. The methods we discuss here will enable us to obtain the following general result from which the irreducibility of all but finitely many $y_n(x)$ is an immediate consequence.

Theorem 1. *There exists an absolute constant n_0 such that for any $n \geq n_0$ and any integers $a_0, a_1, \dots, a_n$ with $|a_0| = |a_n| = 1$,*

$$\sum_{j=0}^{n} a_j \frac{(2n-j)!}{j!(n-j)!} x^j$$

is irreducible.

There is an equivalent formulation of Theorem 1 with the coefficients of $z_n(x)$ replaced by the coefficients of $y_n(x)$. Specifically, for n sufficiently large and for arbitrary integers $a_0, a_1, a_2, \dots, a_n$ with $|a_0| = |a_n| = 1$, the polynomial

$$\sum_{j=0}^{n} a_j \frac{(n+j)!}{2^j (n-j)! j!} x^j$$

is irreducible. For computational reasons, which will not be elaborated on, the author suspects that Theorem 1 holds with $n_0 = 1$ and conjectures so here.

The remainder of the paper is divided up as follows. In Section 2, we discuss some preliminary material related to Newton polygons. We also mention some errors that appear in the literature. In Section 3, we illustrate the techniques in this paper by giving a new proof of a related theorem of I. Schur [8]. Section 4 contains a proof of Theorem 1.

2. Newton Polygons

For a prime p and integers a and b with $ab \neq 0$, we make use of the p-adic notation

$$\nu(a/b) = \nu_p(a/b) = e_1 - e_2 \quad \text{where } \; p^{e_1} || a \; \text{ and } \; p^{e_2} || b.$$

We define $\nu(0) = +\infty$. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$. Let $S = \{(0, \nu(a_n)), (1, \nu(a_{n-1})), \dots, (n-1, \nu(a_1)), (n, \nu(a_0))\}$, a set of points in the extended plane. Following Grosswald [7], we refer to the elements of S as spots. We consider the lower edges along the convex hull of these spots. The left-most edge has one endpoint being $(0, \nu(a_n))$ and the right-most edge has $(n, \nu(a_0))$ as an endpoint. The endpoints of every such edge belong to the set S. The slopes of the edges are increasing when calculated from left to right. The polygonal path formed by these edges is called the Newton polygon for $f(x)$ with respect to p. Dumas [2] established the following:

Lemma 1. *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let k be a non-negative integer such that p^k divides the leading coefficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon for $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p (using exactly one translate for each edge). Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.*

A proof of Lemma 1 can be found in [11] and further discussions and examples related to them can be found in [1]. We emphasize that, for our purposes, when referring to the "edges" of a Newton polygon, we shall not allow 2 different edges of the same Newton polygon to have the same slope.

Many of the irreducibility results of Grosswald [7] concerning Bessel Polynomials are based on making use of Newton polygons. The author was unable to verify one of these results, Theorem 1 (f) on page 99 of [7]. The result asserts that if p is the largest prime factor of n or of $n+1$, then $z_n(x)$ cannot have any factors of degree $< p-1$. Later (cf. [4]), Grosswald used this result to help establish that $z_n(x)$ is irreducible for all $n \leq 10^6$. This consequence of Theorem 1 (f) would now be in question, but Sid Graham has meanwhile verified that $z_n(x)$ is irreducible for $n \leq 10^7$ using methods from [6]. Much of the work in this paper began as an effort to correct Theorem 1 (f).

Before ending this discussion, we mention that the statement of Theorem A′ in [7] is not correct. The reference to this theorem in [7], however, has a correct statement of a similar result. The error in Theorem A′ is that spots are considered along the edges of the Newton polygon rather than arbitrary lattice points. The polynomial $f(x) = (x+2)^2$ with the prime $p = 2$ provides a simple counterexample.

Our use of Newton polygons is summarized in the following lemma.

Lemma 2. *Let k and ℓ be integers with $k > \ell \ge 0$. Suppose $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ and p is a prime such that $p \nmid b_n$, $p | b_j$ for all $j \in \{0, 1, \dots, n-\ell-1\}$, and the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Then for any integers $a_0, a_1, \dots, a_n$ with $|a_0| = |a_n| = 1$, the polynomial $f(x) = \sum_{j=0}^{n} a_j b_j x^j$ cannot have a factor with degree in the interval $[\ell+1, k]$.*

Proof. We first consider the case that $a_j = 1$ for all $j \in \{0, 1, \dots, n\}$ so that $f(x) = g(x)$. Assume $f(x)$ in this case has a factor with degree in $[\ell+1, k]$. Then there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $f(x) = u(x)v(x)$ and $\ell + 1 \le \deg u(x) \le k$. We consider the Newton polygon for $f(x) = g(x)$ with respect to p. Since the slopes of the edges of the Newton polygon for $f(x)$ increase from left to right, the conditions of the lemma imply that each edge has slope in $[0, 1/k)$. The left-most edge of the Newton polygon may have slope 0. For now, we consider an edge of the Newton polygon which does not have slope 0. Let (a, b) and (c, d) be 2 lattice points on such an edge. Then the slope of the line passing through these points is the slope of the edge so that

$$\frac{1}{|c-a|} \le \frac{|d-b|}{|c-a|} < \frac{1}{k}.$$

Hence, $|c - a| > k$. In other words, any 2 lattice points on an edge with non-zero slope of the Newton polygon for $f(x)$ with respect to p have their $x-$coordinates separated by a distance $> k$. Since $\deg u(x) \le k$, we get that translates of the edges of the Newton polygon for $u(x)$ with respect to p cannot be found within those edges of the Newton polygon for $f(x)$ with respect to p which have non-zero slope. From Lemma 1 (with $k = 0$), the left-most edge of the Newton polygon for $f(x)$ must have slope 0 and length $\ge \deg u(x)$. The conditions of the present lemma imply that $\nu(b_{n-j}) \ge 1$ for $j \in \{\ell+1, \ell+2, \dots, n\}$ so that if the left-most edge of the Newton polygon for $f(x)$ with respect to p has slope 0, then it has length $\le \ell < \deg u(x)$, giving a contradiction.

Next, we consider the general case of arbitrary integers $a_0, a_1, \dots, a_n$ with $a_0 = \pm 1$ and $a_n = \pm 1$. The conditions on a_0 and a_n imply that the left and right-most endpoints of the Newton polygon for $f(x)$ with respect to p are the same as the left and right-most endpoints of the Newton polygon for $g(x)$ with respect to p, respectively. Also, $p|a_j b_j$ for all $j \in \{0, 1, \dots, n-\ell-1\}$. All the edges of the Newton polygon for $g(x)$ with respect to p lie above or on the line containing the right-most edge. The same statement holds for $f(x)$ in place of $g(x)$. Note that $\nu(a_j b_j) \geq \nu(b_j)$ for all $j \in \{0, 1, \dots, n\}$. Hence, we also get that all the edges of the Newton polygon for $f(x)$ lie above or on the line containing the right-most edge of the Newton polygon for $g(x)$. Since the right-most endpoint for each of these 2 Newton polygons is the same, we deduce that the slope of the right-most edge of the Newton polygon for $f(x)$ is less than or equal to the slope of the right-most edge of the Newton polygon for $g(x)$. Therefore, the right-most edge of the Newton polygon for $f(x)$ must have slope $< 1/k$. Thus, $f(x)$ satisfies the same conditions imposed on $g(x)$ in the statement of the lemma so that by appealing to the first part of the proof, the lemma follows. ■

Observe that one may strengthen Lemma 2 by requiring only $p \nmid a_0 a_n$ rather than $|a_0| = |a_n| = 1$. We will not, however, make use of this stronger version of Lemma 2 in the proof of Theorem 1.

3. A Theorem of I. Schur

As mentioned in the previous section, this paper began partially as an effort to correct Theorem 1 (f) in [7]. A second motivation for the author's approach to establishing Theorem 1 is based on an interest of the author to find a proof of a result of I. Schur [8] that makes use of Newton polygons. This result of Schur is the following.

Theorem 2. *Let n be a positive integer, and let $a_0, a_1, \dots, a_n$ denote arbitrary integers with $|a_0| = |a_n| = 1$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_1 x + a_0$$

is irreducible over the rationals.

Schur's approach made use of prime ideals in algebraic number fields rather than Newton polygons. We note that other than the use of Newton polygons, the approach used here makes considerable use of the techniques in Schur's paper. In particular, Schur's argument made use of a very nice lemma given next, the proof of which was the largest portion of his paper [8]. As it turned out, the lemma had already been established by Sylvester [9]. 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 3. *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 $m+1, m+2, \dots, m+k$.*

Proof of Theorem 2. To make use of Lemma 2, we consider

$$g(x) = \sum_{j=0}^{n} \frac{n!}{j!} x^j \qquad \text{and} \qquad f(x) = \sum_{j=0}^{n} a_j \frac{n!}{j!} x^j.$$

It suffices to show that $f(x)$ is irreducible over the integers. Assume $f(x)$ is reducible. Let k be the smallest degree of an irreducible factor of $f(x)$. Necessarily, $k \leq n/2$. Thus, $n - k \geq k$ so that Lemma 3 implies there is a prime $p \geq k+1$ dividing $n - \ell$ for some $\ell \in \{0, 1, \dots, k-1\}$. We consider the Newton polygon for $g(x)$ with respect to such a prime p. For $j \in \{0, 1, \dots, n-\ell-1\}$, we get that $n!/j!$ is divisible by $n - \ell$ and, hence, p. To obtain a contradiction and thereby prove the theorem, Lemma 2 implies that it suffices to show that the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Observe that the slope of the right-most edge can be determined by

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(n!) - \nu(n!/j!)}{j} \right\}.$$

Fix $j \in \{1, \dots, n\}$. Note that $p^{\nu(n!) - \nu(n!/j!)}$ is the largest power of p which divides $j!$. Let r be the non-negative integer for which $p^r \leq n < p^{r+1}$. Then for $j \in \{1, \dots, n\}$,

$$\nu(n!) - \nu(n!/j!) = \left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + \cdots + \left[\frac{j}{p^r}\right] \leq j \left(\frac{1}{p} + \cdots + \frac{1}{p^r} \right) = j \frac{p^r - 1}{p^r(p-1)}.$$

Therefore,

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(n!) - \nu(n!/j!)}{j} \right\} \leq \frac{p^r - 1}{p^r(p-1)} < \frac{1}{p-1}.$$

Recall that $p \geq k+1$. Hence, the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$, and the proof is complete. ■

4. The Proof of Theorem 1

Throughout this section, we set

$$f(x) = \sum_{j=0}^{n} a_j \frac{(2n-j)!}{j!(n-j)!} x^j,$$

where the a_j's are as in the statement of Theorem 1. Our goal is to show that if n is sufficiently large, then $f(x)$ is irreducible. Lemma 2 implies that we can obtain information about the degrees of the factors of $f(x)$ by considering the Newton polygon for $z_n(x)$.

Lemma 4. *Let n be a positive integer. Suppose that p is a prime, that k and r are positive integers, and that ℓ is a non-negative integer for which*

(i) $$p^r || (n-\ell),$$

(ii) $$p \geq 2\ell + 1,$$

and

(iii) $$\frac{\log(2n)}{p^r \log p} + \frac{1}{p-1} \leq \frac{1}{k}.$$

Then $f(x)$ cannot have a factor with degree $\in [\ell+1, k]$.

Proof. The result is trivial unless $\ell \leq n-1$, so we suppose this to be the case. Using the notation in Grosswald [7], we define for $m \in \{0, 1, \ldots, n\}$,

$$c_m = \frac{(n+m)!}{m!(n-m)!}, \tag{1}$$

so that $z_n(x) = \sum_{m=0}^{n} c_m x^{n-m}$. The proof consists of verifying the hypotheses of Lemma 2. Observe that $c_0 = 1$ so that $p \nmid c_0$. From (1), we see that

$$c_m = \binom{n+m}{n} n(n-1)\cdots(n-m+1) \quad \text{ for } m \geq 1;$$

therefore $p | c_m$ for $m = \ell+1, \ldots, n$.

Now we need to show that the right–most edge of the Newton polygon of $z_n(x)$ with respect to p has slope $< 1/k$. The right-most edge has slope

$$= \max_{1\le u\le n}\left\{\frac{\nu(c_n)-\nu(c_{n-u})}{u}\right\}$$

so that, by (iii), it suffices to establish that

$$\frac{\nu(c_n)-\nu(c_{n-u})}{u} < \frac{\log(2n)}{p^r\log p} + \frac{1}{p-1}$$

for $1 \le u \le n$.

From (1), we see that

$$\nu(c_n)-\nu(c_{n-u}) = \nu(u!) + \nu\left(\frac{(2n)!}{(2n-u)!}\right) - \nu\left(\frac{n!}{(n-u)!}\right). \tag{2}$$

Note that

$$\nu(u!) = \sum_{j=1}^{\infty}\left[\frac{u}{p^j}\right] < \sum_{j=1}^{\infty}\frac{u}{p^j} = \frac{u}{p-1}.$$

To handle the remaining terms in (2), we introduce the notation

$$a(n,j) = \left[\frac{n}{p^j}\right] - \left[\frac{n-u}{p^j}\right],$$

so that

$$\nu\left(\frac{(2n)!}{(2n-u)!}\right) - \nu\left(\frac{n!}{(n-u)!}\right) = \sum_{j=1}^{\infty}\left(a(2n,j)-a(n,j)\right).$$

We note that $a(n,j)$ is the number of multiples of p^j in the interval $(n-u,n]$. Moreover, the sum above may be truncated at $j = [\log(2n)/\log p]$ since $a(2n,j) = a(n,j) = 0$ when $p^j > 2n$. To complete the proof it therefore suffices to show that

$$a(2n,j) - a(n,j) \le u/p^r \tag{3}$$

for $j \ge 1$. We distinguish three cases: $j \le r$; $u \le 2\ell$; $j > r$ and $u > 2\ell$.

Suppose $j \le r$. By condition (i), there is some m such that $n = p^r m + \ell$. From (ii), $2\ell < p \le p^j$. Thus,

$$\begin{aligned} a(2n,j) &= \left[\frac{2n}{p^j}\right] - \left[\frac{2n-u}{p^j}\right] \\ &= \left[2mp^{r-j} + \frac{2\ell}{p^j}\right] - \left[2mp^{r-j} + \frac{2\ell-u}{p^j}\right] \\ &= \left[\frac{2\ell}{p^j}\right] - \left[\frac{2\ell-u}{p^j}\right] = -\left[\frac{2\ell-u}{p^j}\right]. \end{aligned}$$

Similarly,

$$a(n,j) = -\left[\frac{\ell-u}{p^j}\right].$$

Since $[w]$ is an increasing function, we see that

$$a(2n,j) - a(n,j) = \left[\frac{\ell-u}{p^j}\right] - \left[\frac{2\ell-u}{p^j}\right] \le 0 \quad \text{if } 1 \le j \le r.$$

Since $u > 0$, (3) follows in this case.

Now suppose that $u \le 2\ell$. Since $2\ell < p$, $2n-2\ell$ is the only multiple of p in $[2n-2\ell, 2n]$. Therefore, $(2n-u, 2n]$ has no multiples of p, and so $a(2n,j) = 0$. Thus, (3) holds in this case.

Finally, suppose that $j > r$ and $u > 2\ell$. The number of multiples of p^r in $(2n-u, 2n]$ is $\le [u/p^r] + 1$. Moreover, one of these multiples, $2n-2\ell$, is not divisible by p^j since $j > r$. Therefore,

$$a(2n,j) \le a(2n,r) - 1 \le \left[\frac{u}{p^r}\right].$$

Since $a(n,j) \ge 0$, inequality (3) holds in this case, completing the proof. ■

The next lemma is a version of Lemma 4 for negative values of ℓ. For the purposes of establishing Theorem 1, we will only require a weakened form of the next lemma corresponding to the case $\ell = -1$.

Lemma 5. *Let n be a positive integer. Suppose that p is a prime, that k and r are positive integers, and that ℓ is a negative integer for which*

(i′)
$$p^r \| (n-\ell),$$

(ii′)
$$p \ge 2|\ell| + 1,$$

and

(iii′)
$$\max\left\{\frac{1}{p-2|\ell|+1}, \frac{\log(2n)}{(p^r-2|\ell|+1)\log p}\right\} + \frac{1}{p-1} \le \frac{1}{k}.$$

Then $f(x)$ cannot have a factor with degree $\in [|\ell|, k]$.

Proof. We only sketch the first part of the proof as it is essentially the same as the first part of the proof of Lemma 4. We suppose that $|\ell| \le n$ since otherwise the conclusion of the lemma is trivial. By considering Lemma 2 and

$$c_m = \binom{n}{m}(n+m)(n+m-1)\cdots(n+1) \quad \text{for } m \ge 1,$$

it suffices to show that the right-most edge of the Newton polygon of $z_n(x)$ with respect to p has slope $< 1/k$. We continue as in the proof of Lemma 4 modifying the way we deal with the last two terms on the right-hand side of (2). To get our desired result, it follows from (iii$'$) that we need only establish the inequality

$$\begin{aligned} \nu\left(\frac{(2n)!}{(2n-u)!}\right) - \nu\left(\frac{n!}{(n-u)!}\right) &= \sum_{j=1}^{\infty} (a(2n,j) - a(n,j)) \\ &\le u \max\left\{\frac{1}{p-2|\ell|+1}, \frac{\log(2n)}{(p^r-2|\ell|+1)\log p}\right\} \end{aligned} \tag{4}$$

for $1 \le u \le n$.

Next, we observe that the argument in the proof of Lemma 4 gives here that if $j \le r$, then

$$a(2n,j) = \left[\frac{2\ell}{p^j}\right] - \left[\frac{2\ell-u}{p^j}\right] = -1 - \left[\frac{2\ell-u}{p^j}\right].$$

and

$$a(n,j) = -1 - \left[\frac{\ell-u}{p^j}\right].$$

Hence,

$$a(2n,j) - a(n,j) = \left[\frac{\ell-u}{p^j}\right] - \left[\frac{2\ell-u}{p^j}\right].$$

This last expression on the right is simply the number of multiples of p^j in the interval $I = (2\ell-u, \ell-u]$, and condition (ii$'$) assures that there is at most one such multiple.

We consider now three cases depending on the size of u and establish that (4) holds in each case. First, we consider $1 \le u \le p + 2\ell$. For such u, one checks that

$$n - \ell - p < n - u + 1 \le n \quad \text{and} \quad 2n - 2\ell - p < 2n - u + 1 \le 2n.$$

Hence, each of the expressions $(2n)!/(2n-u)!$ and $n!/(n-u)!$ occuring at the beginning of (4) is not divisible by p, and the inequality in (4) easily follows.

Next, we consider the case that $p+2\ell < u \le p^r + 2\ell$. For such u,

$$n-\ell-p^r < n-u+1 \le n \quad \text{and} \quad 2n-2\ell-p^r < 2n-u+1 \le 2n,$$

and we deduce that none of $n, n-1, \dots, n-u+1$ are divisible by p^r and none of $2n, 2n-1, \dots, 2n-u+1$ are divisible by p^r. In other words, we can restrict the sum in (4) to $j < r$. As mentioned above, for each $j < r$, we have that $a(2n,j) - a(n,j) = 0$ or 1. Furthermore, $a(2n,j) - a(n,j) = 1$ precisely when there is a multiple of p^j in the interval $I = (2\ell - u, \ell - u]$. The latter can only happen if there is an integer ℓ' such that

$$2\ell - u + 1 \le \ell' p^j \le \ell - u.$$

Since $\ell - u < 0$, we deduce that $\ell' < 0$ and

$$p^j \le -\ell' p^j \le -2\ell + u - 1 = 2|\ell| + u - 1.$$

It follows that we can now restrict the sum in (4) to

$$j \le \left[\frac{\log(u + 2|\ell| - 1)}{\log p} \right] \le \frac{\log(u + 2|\ell| - 1)}{\log p}.$$

Since $a(2n,j) - a(n,j) \le 1$ for each such j, it suffices to show in this case that

$$\frac{\log(u + 2|\ell| - 1)}{u \log p} \le \frac{1}{p - 2|\ell| + 1}.$$

This inequality holds since $u \ge p + 2\ell + 1 = p - 2|\ell| + 1$ and since the left-hand side is a decreasing function of u.

Finally, we consider the case that $p^r + 2\ell < u \le n$. As in the proof of Lemma 4, we restrict the sum in (4) to $j \le [\log(2n)/\log p]$. As above, for each $j < r$, we obtain $a(2n,j) - a(n,j) \le 1$. Among the numbers $2n, 2n-1, \dots, 2n-u+1$, the multiples of p^r are precisely the numbers of the form $2n - 2\ell - tp^r$ where $t \in \{1, 2, \dots, [(u + 2|\ell| - 1)/p^r]\}$. It follows that for $j \ge r$,

$$a(2n,j) \le a(2n,r) \le \left[\frac{u + 2|\ell| - 1}{p^r} \right].$$

Therefore,

$$a(2n,j) - a(n,j) \le \frac{u+2|\ell|-1}{p^r}$$

for $j \ge r$. Since $u \ge p^r + 2\ell + 1$, one checks that the right-hand side above is ≥ 1 and, hence, the above inequality also holds for $j < r$. We obtain that

$$\nu\left(\frac{(2n)!}{(2n-u)!}\right) - \nu\left(\frac{n!}{(n-u)!}\right) = \sum_{j=1}^{\infty} \left(a(2n,j) - a(n,j)\right) \le \frac{(u+2|\ell|-1)\log(2n)}{p^r \log p}.$$

It suffices therefore to show that

$$\frac{(u+2|\ell|-1)\log(2n)}{up^r \log p} \le \frac{\log(2n)}{(p^r - 2|\ell| + 1)\log p},$$

and this inequality holds since $(u+2|\ell|-1)/u$ is a decreasing function and since in this case $u \ge p^r - 2|\ell| + 1$. ∎

To prove Theorem 1, let n be sufficiently large and assume $f(x)$ is reducible. Let $k = k(n)$ denote the smallest degree of an irreducible factor of $f(x)$. Necessarily, $k \le n/2$. We consider different arguments depending on the size of k.

Case 1. $n^{2/3} \le k \le n/2$.

We begin by making use of the prime number theorem and a result of Grosswald [7]. We consider a non-negative integer ℓ as small as possible such that $p = n+\ell+1$ is prime. Since n is sufficiently large, we may take $\ell \le 2n/\log n$. Then Theorem 4 on page 111 of Grosswald [7] implies that $z_n(x)$ cannot have an irreducible factor with degree in the interval $(\ell, n-\ell)$; more specifically, the endpoints of the right-most edge of the Newton polygon for $z_n(x)$ with respect to p are $(\ell, 0)$ and $(n, 1)$ so that $z_n(x)$ has an irreducible factor of degree $\ge n - \ell$ and any remaining factor must have degree $\le \ell \le 2n/\log n$. From the point of view of Lemma 2, taking $g(x) = z_n(x)$, we get that $p|b_j$ for all $j \in \{0, 1, \dots, n-\ell-1\}$ and the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $1/(n-\ell)$. Thus, we get that $f(x)$ cannot have a factor with degree in the interval $[\ell+1, n-\ell-1]$. Hence, since $\ell \le 2n/\log n$, $f(x)$ cannot have a factor of degree $k \in (2n/\log n, n/2]$. Thus, we deduce that $k \le 2n/\log n$.

Recall in this case that $k \geq n^{2/3}$ and n is large. We show that there is some prime $p > 3k > n^{2/3}$ that divides $n(n-1)\dots(n-k+1)$ so that

$$\frac{\log(2n)}{p^r \log p} + \frac{1}{p-1} < \frac{\log(2n)}{3k\log(n^{2/3})} + \frac{1}{3k} < \frac{2}{3k} + \frac{1}{3k} = \frac{1}{k}.$$

By Lemma 4, it will then follow that $f(x)$ cannot have a factor of degree k, giving the desired contradiction (for this case). To see that such a prime exists, we observe that since n and, hence, k are large,

$$\pi(3k) < \frac{4k}{\log k}.$$

We follow an argument of Erdős [3] (also described by Tijdeman [10]). For each prime $p \leq 3k$, we consider a number among $n, n-1, \dots, n-k+1$ which is divisible by p^e where $e = e(p)$ is as large as possible. We dispose of all of these numbers, and let S denote the set of numbers that are left. Since $\pi(3k) \leq 4k/\log k$, we are left with at least $k - (4k/\log k)$ numbers each of size $\geq n-k+1 > n/2$. Thus,

$$\prod_{m \in S} m \geq \left(\frac{n}{2}\right)^{k-(4k/\log k)}.$$

For each prime p, let N_p denote the exponent in the largest power of p dividing $\prod_{m\in S} m$. Then for $p \leq 3k$,

$$N_p \leq \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots$$

so that

$$\prod_{p \leq 3k} p^{N_p} \leq k! \leq k^k \leq \left(\frac{2n}{\log n}\right)^k.$$

Therefore,

$$\prod_{p > 3k} p^{N_p} \geq (n/2)^{k-(4k/\log k)} 2^{-k} n^{-k} (\log n)^k \geq n^{-(4k/\log k)} \left(\frac{\log n}{4}\right)^k.$$

An easy calculation shows that this last expression is > 1. Thus,

$$\prod_{p > 3k} p^{N_p} > 1,$$

from which the existence of a prime $p > 3k$ that divides $n(n-1)\dots(n-k+1)$ follows.

Case 2. $k_0 \leq k < n^{2/3}$ with k_0 a sufficiently large positive integer.

For k_0 so chosen and $k \geq k_0$, it easily follows that

$$\pi(3k) \leq \frac{k}{10}.$$

We follow the argument in Case 1 replacing $4k/\log k$ by $k/10$. Thus, we obtain here that

$$\prod_{m \in S} m \geq \left(\frac{n}{2}\right)^{9k/10}$$

and

$$\prod_{p \leq 3k} p^{N_p} \leq k! \leq k^k \leq n^{2k/3}.$$

Hence,

$$\prod_{p > 3k} p^{N_p} \geq \left(\frac{n}{2}\right)^{9k/10} n^{-2k/3} = \left(\frac{n}{2^{27}}\right)^{k/30} n^{k/5} \geq n^{k/5}. \tag{5}$$

Note that since $p > 3k$ in the product above, if p divides the product $n(n-1)\cdots(n-k+1)$, then p divides exactly one of $n, n-1, \ldots, n-k+1$. For $p > 3k$ and $p|n(n-1)\cdots(n-k+1)$, we take $r = r(p) > 0$ and $\ell = \ell(p) \in \{0, 1, \ldots, k-1\}$ such that conditions (i) and (ii) of Lemma 4 are satisfied. Observe that $r \geq N_p$ (with equality holding if $N_p \neq 0$). Hence, since we are assuming $f(x)$ has a factor of degree k, Lemma 4 implies that for every prime $p > 3k$ such that $p|n(n-1)\cdots(n-k+1)$, we have

$$\frac{\log(2n)}{p^{N_p}\log p} + \frac{1}{p-1} \geq \frac{\log(2n)}{p^{r(p)}\log p} + \frac{1}{p-1} > \frac{1}{k}. \tag{6}$$

For each prime $p > 3k$, we have $1/(p-1) \leq 1/(3k)$. Therefore, we deduce from (6) that

$$\frac{\log(2n)}{p^{N_p}\log p} > \frac{2}{3k},$$

or, in other words,

$$p^{N_p} < \frac{3k\log(2n)}{2\log p}. \tag{7}$$

Since $p > 3k \geq 3k_0$ and $n \geq 2k \geq 2k_0$, we get that for k_0 sufficiently large, if $N_p \neq 0$, then

$$p < \frac{k\log n}{7} \quad \text{and} \quad N_p < \frac{\log k + \log\log n - \log 7}{\log p}.$$

Therefore,

$$\sum_{p>3k} N_p \log p \leq \sum_{3k<p\leq k\log n/7} (\log k + \log\log n - \log 7) \leq \frac{k\log n}{6},$$

where in the last inequality we have used that $\pi(x) \leq (7/6)x/\log x$ for x sufficiently large. On the other hand, from (5),

$$\sum_{p>3k} N_p \log p \geq \frac{k\log n}{5}.$$

This gives a contradiction, so $f(x)$ has no factor of degree $k \in [k_0, n^{2/3})$.

Case 3. $5 \leq k < k_0$.

The number of primes $\leq 2k$ is less than or equal to the number of even primes (i.e., 1) plus the number of odd numbers $\leq 2k$ minus 2 (for the odd numbers 1 and 9 which are not prime). Hence, $\pi(2k) \leq k-1$. Using an argument as in Case 1, we get that one of the numbers $n, n-1, \ldots, n-k+1$, say $n-\ell$, can be written as a product $m_1 m_2$ satisfying $m_1 \leq k! \leq k_0!$ and $\gcd(m_2, \prod_{p\leq 2k} p) = 1$. We get that $m_2 \geq c_1 n$ for some constant c_1 (for example, $c_1 = 1/(2\times k_0!)$). Assuming $f(x)$ has a factor of degree k, we get from Lemma 4 that for every prime power divisor p^r of m_2,

$$\frac{\log(2n)}{p^r \log p} + \frac{1}{p-1} > \frac{1}{k}.$$

Since each such p is $\geq 2k+1$, we get that

$$\frac{\log(2n)}{p^r \log p} > \frac{1}{2k} \geq \frac{1}{2k_0}.$$

Thus,

$$p^r < \frac{c_2 \log n}{\log p}$$

for some constant c_2. Then one gets that

$$p < \frac{2c_2 \log n}{\log\log n} \quad \text{and} \quad r < \frac{2\log\log n}{\log p}.$$

These lead to a contradiction since for n sufficiently large,

$$\log m_2 = \sum_{p^r || m_2} r \log p \le \sum_{p < 2c_2 \log n / \log\log n} \frac{2 \log\log n}{\log p} \log p$$
$$\le \frac{5c_2 \log n}{\log\log n} < \log(c_1 n) \le \log m_2.$$

Thus, $f(x)$ cannot have a factor of degree $k \in [5, k_0)$.

Case 4. $1 \le k \le 4$.

For these values of k, we get that $\pi(2k) = k$. We repeat the argument in Case 3 except now we consider the $k+1$ numbers $n+1, n, n-1, \dots, n-k+1$. Among these there is an $n - \ell = m_1 m_2$ with $m_1 \le 12$, $m_2 \ge (n-\ell)/12 \ge n/15$ and $\gcd(m_2, \prod_{p \le 2k} p) = 1$. Observe that if p^r is a prime power divisor of m_2, then $p \ge 2k+1$ so that either (i) and (ii) (if $\ell \ge 0$) or (i$'$) and (ii$'$) (if $\ell = -1$) hold. Furthermore, if $\ell = -1$ and the maximum appearing on the left-hand side of (iii$'$) is $1/(p - 2|\ell| + 1) = 1/(p-1)$, then (iii$'$) also holds, implying $f(x)$ does not have an irreducible factor of degree $k \in \{1, 2, 3, 4\}$ and giving a contradiction. Hence, using Lemma 4 if $\ell \ge 0$ and Lemma 5 if $\ell = -1$, we get that

$$\frac{\log(2n)}{(p^r - 1)\log p} + \frac{1}{p-1} > \frac{1}{k}.$$

Since $p \ge 2k+1$ and $k \le 4$, we deduce

$$\frac{\log(2n)}{(p^r - 1)\log p} > \frac{1}{2k} \ge \frac{1}{8}.$$

We then obtain

$$p^r \le 2\,(p^r - 1) < \frac{16 \log(2n)}{\log p} \le \frac{20 \log n}{\log p}.$$

The argument in Case 3 now easily follows through with c_1 replaced by $1/15$ and c_2 replaced by 20.

Combining the cases, we get that for n sufficiently large, $f(x)$ cannot have a factor of degree $k \in [1, n/2]$, from which Theorem 1 follows.

Acknowledgments: The author thanks Sid Graham for looking over an early draft of the manuscript and providing some helpful suggestions. In particular, Graham helped in the presentation of the proof of Lemma 4. The author is also grateful to the referee for his or her suggestions in improving the paper.

References

1. H. L. Dorwart, *Irreducibility of polynomials*, Amer. Math. Monthly **42** (1935), 369–381.
2. M. G. Dumas, *Sur quelques cas d'irréducibilité des polynomes à coefficients rationnels*, Journal de Math. Pures et Appl. **2** (1906), 191–258.
3. P. Erdős, *On consecutive integers*, Nieuw Archief voor Wiskunde III **3** (1955), 124–128.
4. M. Filaseta, *The irreducibility of almost all Bessel Polynomials*, J. of Number Theory **27** (1987), 22–32.
5. M. Filaseta, *On an irreducibility theorem of I. Schur*, Acta Arith. **58** (1991), 251–272.
6. M. Filaseta and S. W. Graham, *An estimate for the number of reducible Bessel Polynomials of bounded degree*, Colloquium Mathematicum **65** (1993), 65–68.
7. E. Grosswald, *Bessel Polynomials*, Lecture Notes in Math. Vol. 698, Springer-Verlag, Berlin, 1978.
8. I. Schur, *Einege Sätze über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, I*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse. **14** (1929), 125–136.
9. J. J. Sylvester, *On arithmetical series*, Messenger of Math. **21** (1892), 1–19.
10. R. Tijdeman, *On the maximal distance of numbers with a large prime factor*, J. London Math. Soc. (2) **5** (1972), 313–320.
11. B.L. van der Waerden, *Algebra, Vol. 1*, (translated by F. Blum and J. Schulenberger from the 7th edition), Frederick Ungar Publ. Co., New York, 1970.

Mathematics Department
University of South Carolina
Columbia, SC 29208