A GENERALIZATION OF AN IRREDUCIBILITY THEOREM OF I. SCHUR

Michael Filaseta*

Dedicated to my Ph.D. advisor, Heini Halberstam, on the occasion of his retirement

1. Introduction

In 1929, I. Schur [19] established the following result:

Theorem 1 (I. Schur). *Let n be a positive integer, and let $a_0, a_1, \cdots, a_n$ 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.

Irreducibility here and throughout this paper refers to irreducibility over the rationals. Some condition, such as $|a_0| = |a_n| = 1$, on the integers a_j is necessary; otherwise, the irreducibility of all polynomials of the form above would imply every polynomial in $\mathbb{Z}[x]$ is irreducible (which is clearly not the case). In this paper, we will mainly be interested in relaxing the condition $|a_n| = 1$. Specifically, we will show:

Theorem 2. *Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let $f(x) = \sum_{j=0}^{n} a_j x^j / j!$. If $0 < |a_n| < n$, then $f(x)$ is irreducible unless*

$$a_n = \pm 5 \quad \text{and} \quad n = 6$$

or

$$a_n = \pm 7 \quad \text{and} \quad n = 10$$

in which cases either $f(x)$ is irreducible or $f(x)$ is the product of two irreducible polynomials of equal degree. If $|a_n| = n$, then either $f(x)$ is irreducible or $f(x)$ is $x \pm 1$ times an irreducible polynomial of degree $n - 1$.

*Research was supported by NSF Grant DMS-9400937.

In the cases that the pair (a_n, n) is $(\pm 5, 6)$ or $(\pm 7, 10)$, one can obtain reducible $f(x)$. In the way of examples, we note

$$5 \times \frac{x^6}{6!} - 1 = \left(\frac{x^3}{12} + 1\right)\left(\frac{x^3}{12} - 1\right)$$

and

$$7 \times \frac{x^{10}}{10!} - 1 = \left(\frac{x^5}{720} + 1\right)\left(\frac{x^5}{720} - 1\right).$$

These particular examples arise partially because $6!/5$ and $10!/7$ are squares. It is possible to show that if n is a positive integer and p is a prime for which $n!/p$ is a square, then $(n, p) \in \{(2, 2), (6, 5), (10, 7)\}$.

If one chooses $a_0 = \pm 1$, the integers $a_1, a_2, \ldots, a_{n-2}$ arbitrarily, and $a_n = \pm n$ (or any multiple of n will do), it is easy to see that there is an integer a_{n-1} for which $f(-1) = 0$ and there is an integer a_{n-1} for which $f(1) = 0$. Thus, $x \pm 1$ may be a factor of $f(x)$ when $|a_n| = n$. The last statement of the theorem implies that the remaining factor of degree $n - 1$ will necessarily be irreducible.

In the next three sections, we establish Theorem 2. It is of some interest to know to what extent one can further extend the range on a_n in Theorem 2. In Section 5, we will establish

Theorem 3. *Let C be a positive number $< 1/\sqrt{2}$. Let n be a positive integer, and let $a_0, a_1, \ldots, a_n$ be arbitrary integers with $|a_0| = 1$ and $0 < |a_n| \le Cn^{3/2}$. Let $f(x) = \sum_{j=0}^{n} a_j x^j / j!$. Then for all but finitely many pairs of integers (a_n, n), either $f(x)$ is irreducible or $f(x)$ factors in $\mathbb{Q}[x]$ as the product of a linear polynomial and an irreducible polynomial of degree $n - 1$. In the case that $f(x)$ has a linear factor, one necessarily has $n | a_n$.*

The proof we will give of Theorem 3 is non-effective; the exceptional pairs (a_n, n) cannot be determined. A weaker inequality such as

$$0 < |a_n| \le n \exp\left(\sqrt{\frac{\log n}{(\log\log n)^3}}\right)$$

would make Theorem 3 effective, and we describe how this can be done in Section 6.

From Theorem 3, it follows that if $|a_n|$ is not too large, then either $f(x)$ is irreducible or it has a linear factor. Suppose instead we wish to conclude that either $f(x)$ is irreducible or it has a factor of degree ≤ 2. Then a stronger result, with a larger upper bound on $|a_n|$, can be obtained directly from our methods. In fact, an even stronger result can be obtained if for some $k \ge 3$ one allows for $f(x)$ to have a factor of degree $\le k$. We will not elaborate further on this, but these remarks are easily deduced from the proof we give of Theorem 3.

The proof of Theorem 3 will be based on finding an upper bound on n for the exceptional pairs (a_n, n) in the statement of the theorem. The condition $0 < |a_n| \le Cn^{3/2}$ then implies that this list of exceptional pairs is finite. The author has considered specifically the case that $0 < |a_n| \leq 2n$. In particular, if $f(x)$ is as above with $n < |a_n| < 2n$, then either $f(x)$ is irreducible or $(a_n, n) = (\pm 6, 4)$. If $|a_n| = 2n$ and $f(x)$ is reducible, then $f(x)$ is the product of two irreducible polynomials. One of these two polynomials will be linear, and in fact will be $x \pm 1$ or $2x \pm 1$, unless $(a_n, n) = (\pm 10, 5)$ and $f(x)$ factors as the product of an irreducible quadratic and an irreducible cubic. In this regard, the examples

$$6 \times \frac{x^4}{4!} - 1 = \left(\frac{x^2}{2} + 1\right)\left(\frac{x^2}{2} - 1\right) \quad \text{and} \quad 10 \times \frac{x^5}{5!} + \frac{x^3}{3!} + \frac{x^2}{2!} + 1 = \frac{1}{12}\left(x^2 + 2\right)\left(x^3 + 6\right)$$

are worth noting. This result with $0 < |a_n| \leq 2n$ can be obtained in a very similar manner to the proof of Theorem 2, and we do not elaborate on the details.

In the sixth section of this paper, we will discuss other results related to the irreducibility of $f(x)$. In particular, we will give a proof of the following nice generalization of Schur's theorem due to T.Y. Lam (private communication):

Theorem 4 (T.Y. Lam). *Let n be an integer ≥ 2, and let $a_0, a_1, \ldots, a_n$ be arbitrary integers with $\gcd(a_0 a_n, n!) = 1$. Then $\sum_{j=0}^{n} a_j x^j / j!$ is irreducible.*

We observe that, as a consequence of Lam's theorem, if p is a prime, $|a_0| = 1$, and $|a_n| = p$, then $f(x)$ is irreducible for $n < p$. Together with Theorem 2, this implies that if $|a_n| = p$, then the condition $|a_n| < n$ in Theorem 2 may be replaced by $|a_n| \neq n$. In other words, if $|a_n| = p$, then $f(x)$ irreducible unless $(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$ or $n = p$.

2. Background and Sketch of the Proof of Theorem 2

Recently, the author [9] established that all but finitely many Bessel polynomials are irreducible. The proof of Theorem 2 will be based on the same techniques. However, there are really two basic elements of the proof and these both have a long history. The first is the use of Newton polygons to deduce the irreducibility of the polynomials in Theorem 2. In 1906, G. Dumas [6] obtained an important result, discussed below, which has been the basis of many irreducibility theorems since then (cf. [9,11,13,24]), so it is not surprising that Newton polygons should play a role in the proof of Theorem 2. In fact, R.F. Coleman [4] has already observed that Newton polygons can be used to establish the irreducibility of the polynomials in Theorem 1 in the case that $a_n = a_{n-1} = \cdots = a_1 = a_0 = 1$; and the author [9] recently gave a proof of Theorem 1 in its full generality using Newton polygons. The second basic element of our proof of Theorem 2 is the use of information on the distribution of primes. In particular, a result of E.F. Ecklund, Jr., R.B. Eggleton, P. Erdős, and J.L. Selfridge [7] on prime divisors of binomial coefficients will play an important role.

Newton polygons can be described as follows. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$. Let p be a prime, and let m be an integer. We use the p-adic notation

$$\nu(m) = \nu_p(m) = r \quad \text{if } p^r | m \text{ and } p^{r+1} \nmid m.$$

If $m = 0$, then we will understand this to mean $\nu(m) = +\infty$. For $j \in \{0, \ldots, n\}$, we define a set of points $S = \{(0, \nu(a_n)), (1, \nu(a_{n-1})), \ldots, (n, \nu(a_0))\}$ in the extended plane.

The elements of S we refer to 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 edge belong to the set S. We emphasize that, for our purposes, when referring to the "edges" of a Newton polygon, we shall not allow 2 different edges to have the same slope. The polygonal path formed by these edges is called the Newton polygon of $f(x)$ with respect to the prime p. Observe that the slope of the edges are always increasing when calculated from the left-most edge to the right-most edge. The following theorem is due to Dumas [6].

Theorem 5. *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 of the Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing from left to right.*

Although we will stick here to the use of Newton polygons as just described, we note that there are other contexts in which Newton polygons occur. In particular, one may describe Newton polygons, or more appropriately Newton polytopes, in several variables as follows. Associate with a polynomial $f(x_1, \ldots, x_m)$ a set T of points $(e_1, e_2, \ldots, e_m)$ in $\mathbb{R}^m$ corresponding to the terms $a x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m}$ of f with $a \neq 0$. Denote by C_f the convex hull of the set T in $\mathbb{R}^m$. Then C_f is called the Newton polytope of f. We mention two results associated with Newton polytopes. D.N. Bernstein [3] has shown that the number of intersection points (counted with multiplicity) of m algebraic curves in m variables can be determined from the use of Newton polytopes. If f factors as the product of polynomials g and h in $\mathbb{Z}[x_1, \ldots, x_m]$, A.M. Ostrowski [16] has established that $C_f = C_g + C_h$. If one replaces the prime p in our definition of Newton polygons above with a variable, then Ostrowski's theorem comes close to directly implying Theorem 5 (but note the example $f(x) = g(x)h(x)$ with $g(x) = h(x) = x + 1$ and $p = 2$ in this context).

Our main use of Theorem 5 is summarized in our first lemma. We note that the proof is similar to the proof of Lemma 2 in [9].

Lemma 1. *Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let*

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

Let k be a positive integer $\leq n/2$. Suppose there exists a prime $p \geq k + 1$ and a positive integer r for which

$$p^r | n(n-1) \cdots (n-k+1) \quad \text{and} \quad p^r \nmid a_n.$$

Then $f(x)$ cannot have a factor of degree k.

Proof. It suffices to show that

$$F(x) = n! f(x) = \sum_{j=0}^{n} a_j \, (n!/j!) \, x^j$$

cannot have a factor of degree k. We set $b_j = a_j n!/j!$ for $0 \le j \le n$. The condition $p^r | n(n-1)\cdots(n-k+1)$ implies that $p^r | b_j$ for $j \in \{0, 1, \ldots, n-k\}$. Thus, the $n-k+1$ right-most spots, $(k, \nu(a_{n-k} n!/(n-k)!)), \ldots, (n, \nu(a_0 n!))$, associated with the Newton polygon of $F(x)$ with respect to p have y-coordinates $\ge r$. Since $p^r \nmid a_n$ and $b_n = a_n$, we have $p^r \nmid b_n$, and the left-most spot $(0, \nu(a_n))$ has y-coordinate $< r$. Recall that the slopes of the edges of the Newton of $F(x)$ with respect to p increase from left to right. This is sufficient to imply that the spots $(j, \nu(b_{n-j}))$ for $j \in \{k-1, k, k+1, \ldots, n\}$ all lie on or above edges of the Newton polygon of $F(x)$ which have positive slope.

Next, we show that each of these positive slopes is $< 1/k$. Since the slopes of the edges of the Newton polygon increase from left to right, it suffices to show that the right-most edge has slope $< 1/k$. The slope of that edge is

$$\max_{1 \le j \le n} \left\{ \frac{\nu(b_0) - \nu(b_j)}{j} \right\}.$$

For $1 \le j \le n$, we have

$$\begin{aligned} \nu(b_0) - \nu(b_j) &= \nu(a_0 n!) - \nu(a_j n!/j!) \\ &\le \nu(n!) - \nu(n!/j!) \\ &= \nu(j!) = \left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + \left[\frac{j}{p^3}\right] + \cdots \\ &< j\left(\frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \frac{j}{p-1}. \end{aligned}$$

Since $p \ge k+1$, we obtain

$$\max_{1 \le j \le n} \left\{ \frac{\nu(b_0) - \nu(b_j)}{j} \right\} < \frac{1}{p-1} \le \frac{1}{k}.$$

Thus, each edge of the Newton polygon of $F(x)$ has slope $< 1/k$.

Now, assume $F(x)$ has a factor $g(x) \in \mathbb{Z}[x]$ of degree k. We obtain a contradiction to Theorem 5 by showing that translates of all the edges of the Newton polygon of $g(x)$ with respect to p cannot be found among the edges of the Newton polygon of $F(x)$ with respect to p. First, we show that no translate of an edge of the Newton polygon of $g(x)$ can be found among those edges in the Newton polygon of $F(x)$ having positive slope. Suppose (a, b) and (c, d), with $a < c$, are two lattices points on an edge of the Newton polygon of $F(x)$ having positive slope. Since we have already shown such a slope is $< 1/k$, we deduce

$$\frac{1}{k} > \frac{d-b}{c-a} \ge \frac{1}{c-a}.$$

Therefore, $c - a > k = \deg g(x)$. It follows that (a, b) and (c, d) cannot be endpoints of a translated edge of the Newton polygon of $g(x)$. Therefore, the translates of the edges of the Newton polygon of $g(x)$ with respect to p must be among the edges of the Newton polygon of $F(x)$ having zero or negative slope. We have already observed that all the spots $(j, \nu(b_{n-j}))$ for $j \in \{k-1, k, \cdots, n\}$ lie on or above the edges of the Newton polygon of $F(x)$ having positive slope. Therefore, the spots forming the endpoints of the edges of the Newton polygon of $F(x)$ having zero or negative slope must be among the spots $(j, \nu(b_{n-j}))$ where $j \in \{0, 1, \ldots, k-1\}$. Since $k - 1 < \deg g(x)$, these edges by themselves cannot consist of a complete collection of translated edges of the Newton polygon of $g(x)$. Therefore, we obtain a contradiction, completing the proof. ■

As a consequence, we deduce

Lemma 2. *If $0 < |a_n| < n$, then $f(x)$ cannot have a linear factor.*

Proof. If $0 < |a_n| < n$, then there must be a prime power p^r such that $p^r | n$ and $p^r \nmid a_n$. The lemma follows by taking $k = 1$ in Lemma 1. ■

In the next two sections, we will show that if $0 < |a_n| \leq n$ and $f(x)$ has a factor of degree $k \in [2, n/2]$, then either $a_n = \pm 5$, $n = 6$, and $k = 3$ or $a_n = \pm 7$, $n = 10$, and $k = 5$. We explain here why Theorem 2 will then follow. Suppose $f(x)$ is reducible. Then $f(x)$ and likewise $F(x)$ has a factor of degree $k \in [1, n/2]$. If $0 < |a_n| < n$, then Lemma 2 and the results just mentioned that we will be establishing in the next two sections easily imply this case of Theorem 2. Now, consider the possibility that $|a_n| = n$. In this case, we still know that $F(x)$ cannot have a factor of degree $k \in [2, n/2]$. For $n > 3$, it follows that $F(x)$ has a linear factor and the remaining factor is irreducible; for $n = 3$, considering the Newton polygon of $F(x)$ with respect to 2 allows us to make the same conclusion (i.e., in this case, $F(x)$ factors as a linear polynomial times an irreducible quadratic in $\mathbb{Z}[x]$). We want to show that either $F(x) = (x+1)g(x)$ or $F(x) = (x-1)g(x)$ where $g(x) \in \mathbb{Z}[x]$. Since $|a_n| = n$, we deduce that n divides each coefficient of $F(x)$. We write $F(x) = nh(x)$ where $h(x)$ is a monic polynomial in $\mathbb{Z}[x]$ having constant term $\pm(n-1)!$. We deduce from the rational root test applied to $h(x)$ that $F(x)$ has an integer root m which divides $(n-1)!$. We now only need to show that no prime p divides m. Assume some prime p divides m, and let $r = \nu_p((n-1)!)$. As in the proof of Lemma 1, we have $\nu_p(j!) < j$ for $j \geq 1$. Thus,

$$\nu_p\left(a_j \frac{(n-1)!}{j!} m^j\right) \geq \nu_p((n-1)!) - \nu_p(j!) + j \geq r + 1 \quad \text{for } 1 \leq j \leq n.$$

Hence,

$$h(m) = \sum_{j=0}^{n} a_j \frac{(n-1)!}{j!} m^j \equiv \pm(n-1)! \not\equiv 0 \pmod{p^{r+1}}.$$

This contradicts that $F(m)$, and hence $h(m)$, is zero.

The above discussion explains the main role of Newton polygons in the proof of Theorem 2. We now turn to the role of results from the distribution of primes. In proving Theorem 1, Schur used the following:

Theorem 6 (J.J. Sylvester [22]). *Let k be a positive integer. Then at least one of any k consecutive integers $> k$ is divisible by a prime $> k$.*

Theorem 6 was rediscovered by Schur in [19]. The theorem implies immediately that for any positive integer k, one of $k+1, k+2, \ldots, 2k$ is a prime (since one of these integers must be divisible by a prime $\geq k+1$). Thus, Bertrand's Postulate is a consequence of Theorem 6.

As mentioned earlier, if $f(x)$ is as in Theorem 2 (so its degree is n) and $f(x)$ is reducible, then $f(x)$ has a factor of degree $k \in [1, n/2]$. This implies $n-k+1 > k$, so Theorem 6 implies that one of the k numbers $n, n-1, \dots, n-k+1$ is divisible by a prime $p \geq k+1$. Observe that if $0 < |a_n| \leq k$, then $p \nmid a_n$. Hence, from Lemma 1, we obtain

Lemma 3. *If $0 < |a_n| \leq k$, then $f(x)$ cannot have a factor of degree k.*

Observe that if $a_n = \pm 1$, then we deduce immediately that $f(x)$ is irreducible. In other words, we have just established Theorem 1.

To prove Theorem 2, we will make use of a generalization of Theorem 6 obtained by Ecklund, Eggleton, Erdős, and Selfridge [7]. We note the important related work by P. Erdős [8], K. Ramachandra [17], R. Tijdeman [23], M. Jutila [14], K. Ramachandra and T.N. Shorey [18], and T.N. Shorey [20] involving estimates for the largest prime factor of the product of k consecutive positive integers, say $n(n-1)\cdots(n-k+1)$. Also, see A. Granville [10] for a result concerning $p \geq k+1$ for which $p || n(n-1)\cdots(n-k+1)$.

With $F(x)$ as before and $0 < |a_n| \leq n$, we want to show for $(a_n, n) \notin \{(\pm 5, 6), (\pm 7, 10)\}$ that $F(x)$ cannot have a factor of degree $k \in [2, n/2]$. Assume otherwise. Then Lemma 1 implies

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \geq k+1}} p^r$$

divides a_n. Since $0 < |a_n| \leq n$, we will obtain a contradiction if the above product is $> n$. In other words, we would like to know not just that $n(n-1)\cdots(n-k+1)$ is divisible by a prime $> k$ (as in Theorem 6) but further that the contribution of all the prime factors of this product which are $> k$ is $> n$. This is not in fact always the case, but it usually is. We will obtain the following lemma as a consequence of the work in [7], but we note here that the work in [7] contains considerably stronger estimates (see the next section).

Lemma 4. *Let k be an integer $\in [2, n/2]$. Then*

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \geq k+1}} p^r > n \tag{1}$$

unless one of the following holds:

$$\begin{aligned}
n &= 12 \quad \textit{and} \quad k = 5 \\
n &= 10 \quad \textit{and} \quad k = 5 \\
n &= 9 \quad \textit{and} \quad k = 4 \\
n &= 18 \quad \textit{and} \quad k = 3 \\
n &= 10 \quad \textit{and} \quad k = 3 \\
n &= 9 \quad \textit{and} \quad k = 3 \\
n &= 8 \quad \textit{and} \quad k = 3
\end{aligned}$$

$$n = 6 \quad \textit{and} \quad k = 3$$
$$n = 2^\ell + 1 \quad \textit{and} \quad k = 2$$
$$n = 2^\ell \quad \textit{and} \quad k = 2,$$

where ℓ represents an arbitrary positive integer.

Although the proof of Theorem 2 does not require an inequality stronger than (1), we note that Lemma 4 holds if the right-hand side of (1) is replaced by $2n$. One easily checks that each value for the pair (n,k) in the list above gives rise to a choice of n and k for which (1) does not hold. After establishing Lemma 4, the proof of the irreducibility of the polynomials $f(x)$ in Theorem 2 will almost be complete. To handle the remaining cases of n and k given above, we will appeal once again to the use of Newton polygons. This will be done in Section 4.

3. The Proof of Lemma 4

Throughout this section, we let n and k denote positive integers with $2 \le k \le n/2$. Our goal in this section is to establish Lemma 4. As mentioned in the previous section, Lemma 4 will be a fairly direct consequence of the work in [7]. There we find the following result:

Lemma 5. *Set $\binom{n}{k} = UV$ where the prime factors of U are all $\le k$ and the prime factors of V are all $\ge k+1$. If $k \notin \{3,5,7\}$ and $U > V$, then $(n,k) \in S$ where*

$$S = \{(9,4), (21,8), (33,13), (33,14), (36,13), (36,17), (56,13)\}.$$

Now, consider $k \ge 4$. Observe that since $n \ge 2k$, $\binom{n}{k} \ge \binom{n}{4} > n^2$ provided

$$n(n-1)(n-2)(n-3) - 24n^2 > 0.$$

The left-hand side above can be written as

$$n(n+1)\big(n(n-7) - 6\big)$$

which is clearly positive since $n \ge 2k \ge 8$. Hence, we obtain

Lemma 6. *For $k \ge 4$, $\binom{n}{k} > n^2$.*

For $k \ge 4$ and $k \notin \{5,7\}$, we deduce from the above two lemmas that if $(n,k) \notin S$, then

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r = \prod_{\substack{p^r || \binom{n}{k} \\ p \ge k+1}} p^r \ge \sqrt{\binom{n}{k}} > n.$$

In other words, for such (n,k), (1) holds. One checks directly that each pair $(n,k) \in S$ also satisfies (1) with the exception of the pair $(9,4)$. Thus, we have

Lemma 7. *If $k \geq 4$ and $k \neq 5$ and $k \neq 7$, then (1) holds unless $(n,k) = (9,4)$.*

We are left now with determining when (1) holds with $k \in \{2,3,5,7\}$. One can deal with $k = 5$ and $k = 7$ in a fairly simple manner. We explain the argument for $k = 5$ and leave the analogous argument for $k = 7$ to the reader. We remove from the set $T = \{n, n-1, n-2, n-3, n-4\}$ the integer divisible by the largest power of 2, the integer divisible by the largest power of 3, and the integer divisible by 5. Two of these may be the same; but in any case, at least two, say a and b, of the five integers will remain in T. Since the integer divisible by the largest power of 2 was removed from T, we deduce that $16 \nmid ab$. Similarly, $9 \nmid ab$ and $5 \nmid ab$. Hence,

$$\prod_{\substack{p^r || n(n-1)\cdots(n-4) \\ p \geq 6}} p^r \geq \frac{ab}{24} \geq \frac{(n-3)(n-4)}{24}.$$

It is easy to verify that this last expression is $> n$ for $n \geq 32$. It follows that (1) holds for $k = 5$ and $n \geq 32$. One checks directly that (1) holds for $k = 5$ and $n \in \{11\} \cup \{13, 14, \ldots, 31\}$.

Next, we consider $k = 3$. We will use the following result which was established by G.C. Gerono in 1857 (cf. [5, p. 744]).

Lemma 8. *The only solutions to the equation $|p^r - q^s| = 1$, where p and q are primes and r and s are integers greater than one, are $(p,r,q,s) = (3,2,2,3)$ and $(2,3,3,2)$.*

The next lemma is well-known and follows immediately from Lemma 8.

Lemma 9. *If $n > 9$, then there exists a prime $p > 3$ such that $p | n(n-1)$.*

Lemma 10. *If $k = 3 \leq n/2$, then (1) holds unless $n \in \{6, 8, 9, 10, 18\}$.*

Proof. One checks (1) directly for $k = 3$ and $6 \leq n \leq 18$. We therefore only consider $n \geq 19$. Let u be the greatest positive integer such that 2^u divides one of n, $n-1$, and $n-2$. Let v be the greatest positive integer such that 3^v divides one of n, $n-1$, and $n-2$. Note that exactly one member of $\{n, n-1, n-2\}$, say m_1, is divisible by 2^u, and one of these quantities, say m_2, is divisible by 3^v. The numbers m_1 and m_2 may not be distinct, but there must be at least one number, say m_3, among n, $n-1$, and $n-2$ which is different from m_1 and m_2. Observe that either $m_3 = m$ or $m_3 = 2m$ where m is a positive integer having each of its prime divisors > 3.

Next, we show that $n(n-1)(n-2)/m_3$ is divisible by a prime > 3. If $m_3 = n-2$, then we deduce from Lemma 9 that $n(n-1)$ is divisible by a prime > 3. Similarly, if $m_3 = n$, we deduce such a prime exists dividing $(n-1)(n-2)$. If $m_3 = n-1$ and m_3 is odd, then n and $n-2$ are even and Lemma 9 implies that $(n/2)(n-2)/2$ is divisible by some prime > 3. If $m_3 = n-1$ and m_3 is even, then n and $n-2$ are odd and only one is divisible by 3; hence, there exists a prime > 3 dividing one of n and $n-2$. Thus, we have shown that $n(n-1)(n-2)/m_3$ is divisible by a prime > 3. It now follows that

$$\prod_{p > 3} p^{\nu_p(n(n-1)(n-2))} \geq 5m_3/2 \geq 5(n-2)/2 = (5n-10)/2 > n.$$

Thus, (1) holds. ■

The proof of Lemma 4 now follows from

Lemma 11. *If $k = 2 \leq n/2$, then (1) holds unless $n = 2^\ell$ or $2^\ell + 1$ for some positive integer ℓ.*

Proof. For $k = 2$, the inequality (1) is simply

$$\prod_{\substack{p^r || n(n-1) \\ p \geq 3}} p^r > n.$$

One of n or $n-1$ is odd and, hence, divides the product on the left. If n is not of the form 2^ℓ or $2^\ell + 1$, then neither n nor $n-1$ is a power of 2. Therefore,

$$\prod_{\substack{p^r || n(n-1) \\ p \geq 3}} p^r \geq 3(n-1) > n,$$

completing the proof. ∎

4. The Remaining Cases for Theorem 2

We set

$$F(x) = n!f(x) = \sum_{j=0}^{n} b_j x^j \qquad \text{where } b_j = a_j\,(n!/j!)\,.$$

From Section 2, Theorem 2 holds provided we can show that if $0 < |a_n| \leq n$ and $F(x)$ has a factor of degree $k \in [2, n/2]$, then either $a_n = \pm 5$, $n = 6$, and $k = 3$ or $a_n = \pm 7$, $n = 10$, and $k = 5$. We therefore assume $F(x)$ has a factor of degree $k \in [2, n/2]$. Since $0 < |a_n| \leq n$, Lemma 1 implies that (1) does not hold. Hence, Lemma 4 implies that the pair (n, k) belongs to a short list of possible values. In this section, we complete the proof of Theorem 2 by examining each of these possibilities for (n, k).

For $n = 12$ and $k = 5$, we observe that Lemma 1 implies that $11|a_n$. Since $|a_n| \leq n = 12$, we deduce $a_n = \pm 11$. We consider the Newton polygon of $F(x)$ with respect to 3. Since we do not know what the values of a_j are, we cannot determine precisely what this Newton polygon looks like. Since $a_n = \pm 11$ and $a_0 = \pm 1$, $\nu_3(b_n) = 0$ and $\nu_3(b_0) = 5$. This means that the left-most spot of the Newton polygon is $(0, 0)$ and the right-most spot is $(12, 5)$. If we first consider the case where $a_j = 1$ for $1 \leq j \leq 11$, we see that the Newton polygon consists of the line segment joining $(0, 0)$ to $(3, 1)$ together with the line segment joining $(3, 1)$ to $(12, 5)$. Since $\nu_3(b_j)$ can only increase by choosing the numbers a_j in a different way, in general if we let the values of a_j vary over the integers, the Newton polygon of $F(x)$ with respect to 3 will consist of precisely these 2 line segments unless $3|a_{n-3}$. If $3|a_{n-3}$, then the Newton polygon is simply the segment joining $(0, 0)$ to $(12, 5)$. In either case, Theorem 5 implies that $F(x)$ cannot have a factor of degree 5 in $\mathbb{Z}[x]$, and we obtain a contradiction.

Now, suppose $n = 10$ and $k = 5$. Here, Lemma 1 implies $7|a_n$. Since $|a_n| \leq n = 10$, we obtain $a_n = \pm 7$. One checks that the Newton polygon of $F(x)$ with respect to 5 is the segment joining $(0, 0)$ to $(10, 2)$. The lattice points along this Newton polygon are

$(0,0)$, $(5,1)$, and $(10,2)$. Hence, Theorem 5 implies that if $F(x)$ is reducible, then it is the product of two irreducible polynomials of degree 5. Recall that in Theorem 2, we allow the possibility that $a_n = \pm 7$, $n = 10$, and $f(x)$ (or equivalently $F(x)$) factors as a product of two irreducible quintics. Thus, we are done in this case.

If $n = 9$ and $k = 4$, then Lemma 1 implies $7|a_n$ so that $a_n = \pm 7$. The Newton polygon of $F(x)$ with respect to 3 is simply the line segment joining $(0,0)$ to $(9,4)$. We deduce from Theorem 5 that $F(x)$ cannot have a factor of degree 4 in $\mathbb{Z}[x]$, obtaining a contradiction.

If $n = 18$ and $k = 3$, then Lemma 1 implies $17|a_n$ so that $a_n = \pm 17$. The Newton polygon of $F(x)$ with respect to 3 is the line segment joining $(0,0)$ to $(18,8)$. There are only three lattice points on the Newton polygon, namely $(0,0)$, $(9,4)$, and $(18,8)$. Hence, $F(x)$ cannot have a factor of degree 3 in $\mathbb{Z}[x]$.

If $n = 10$ and $k = 3$, we use Lemma 1 to deduce that $5|a_n$. Since $0 < |a_n| \leq 10$, we deduce here that $a_n = \pm 5$ or $a_n = \pm 10$. In either case, we consider the Newton polygon of $F(x)$ with respect to 3. If $3 \nmid a_{n-1}$, then the Newton polygon consists of 2 edges, one joining $(0,0)$ to $(1,0)$ and the other joining $(1,0)$ to $(10,4)$. If $3|a_{n-1}$, then the Newton polygon consists of exactly 1 edge joining $(0,0)$ to $(10,4)$. In either case, we again deduce that $F(x)$ cannot have a cubic factor in $\mathbb{Z}[x]$.

If $n = 9$ and $k = 3$, Lemma 1 implies that $a_n = \pm 7$. As before, one can show that $F(x)$ cannot have a cubic factor in $\mathbb{Z}[x]$ by considering the Newton polygon of $F(x)$ with respect to 3.

If $n = 8$ and $k = 3$, Lemma 1 implies that $a_n = \pm 7$, and one shows that $F(x)$ cannot have a cubic factor in $\mathbb{Z}[x]$ by considering the Newton polygon of $F(x)$ with respect to 2.

For $n = 6$ and $k = 3$, Lemma 1 implies that $a_n = \pm 5$. Theorem 2 allows for the possibility that $a_n = \pm 5$, $n = 6$, and $k = 3$, so we are done in this case.

Now, suppose that $n = 2^\ell + 1$ for some positive integer ℓ and that $k = 2$. Lemma 1 implies that n divides a_n. Since $0 < |a_n| \leq n$, we deduce that $a_n = \pm n$. We consider

$$g(x) = a_n x^n + \sum_{j=0}^{n-1} (n!/j!)\, x^j,$$

so that $g(x)$ is the polynomial $F(x)$ with $a_j = 1$ for $0 \leq j \leq n-1$. As we have already seen in the cases above, the Newton polygon of $g(x)$ with respect to a prime is related to the Newton polygon of $F(x)$ with respect to that prime. We consider the Newton polygon of $g(x)$ with respect to 2. We now justify that this Newton polygon consists of two line segments, one joining $(0,0)$ to $(1,0)$ and one joining $(1,0)$ to $(n, n-2)$. Clearly $(0,0)$ and $(1,0)$ are spots obtained in the construction of the Newton polygon of $g(x)$ with respect to 2. The right-most spot is $(n, \nu_2(n!))$, and

$$\nu_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \cdots = 2^{l-1} + 2^{l-2} + \cdots + 2 + 1 = 2^l - 1 = n - 2.$$

Since $(1,0)$ and $(n, n-2)$ are spots, the slope of the right-most edge of the Newton polygon of $g(x)$ with respect to 2 is $\geq (n-2)/(n-1)$. To show that the line segment joining $(1,0)$ and $(n, n-2)$ is an edge of this Newton polygon, it suffices to show that the slope of the right-most edge is $\leq (n-2)/(n-1)$. Since $(0,0)$ and $(1,0)$ are spots, the right-most edge has slope

$$\max_{1\leq j\leq n-1}\left\{\frac{\nu_2(n!)-\nu_2(n!/j!)}{j}\right\}=\max_{1\leq j\leq n-1}\left\{\frac{\nu_2(j!)}{j}\right\}.$$

For any positive integer j, $\nu_2(j!)=[j/2]+[j/4]+\cdots<j$. Thus, $\nu_2(j!)\leq j-1$, and

$$\max_{1\leq j\leq n-1}\left\{\frac{\nu_2(j!)}{j}\right\}\leq\max_{1\leq j\leq n-1}\left\{\frac{j-1}{j}\right\}=\frac{n-2}{n-1}.$$

This completes the justification that the Newton polygon of $g(x)$ with respect to 2 consists of a line segment joining $(0,0)$ to $(1,0)$ together with a line segment joining $(1,0)$ to $(n,n-2)$.

We now concern ourselves with the Newton polygon of $F(x)$ with respect to 2. Note that the spots associated with the Newton polygon of $F(x)$ with respect to 2 lie on or above the edges of the Newton polygon of $g(x)$ with respect to 2. The interior of the triangle T with vertices $(0,0)$, $(1,0)$, and $(n,n-2)$ will in general contain many lattice points. We will show that none of these lattice points can be a spot associated with the Newton polygon of $F(x)$ with respect to 2. It will then follow that if $(1,0)$ is not a spot associated with the Newton polygon of $F(x)$ with respect to 2, then this Newton polygon is simply the line segment joining $(0,0)$ to $(n,n-2)$. On the other hand, if $(1,0)$ is a spot associated with the Newton polygon of $F(x)$ with respect to 2, then the Newton polygon of $F(x)$ with respect to 2 is the same as the Newton polygon of $g(x)$ with respect to 2. Since n is odd, $\gcd(n,n-2)$ and $\gcd(n-2,n-1)$ are both 1 so that in any case the only lattice points on the edges of the Newton polygon of $F(x)$ with respect to 2 are the endpoints of its edges. This will easily imply that $F(x)$ cannot have a quadratic factor.

Now, we show that the lattice points strictly inside the triangle T are not spots associated with the Newton polygon of $F(x)$ with respect to 2. The point $(n,n-2)$ is the right endpoint of the right-most edge of this Newton polygon. The line passing through $(n,n-2)$ and a point interior to T has slope $>(n-2)/n$. In particular, this implies $(1,1)$ is not inside T. Since the spots associated with the Newton polygon of $F(x)$ with respect to 2 are the points of the form $(n-j,\nu_2(b_j))$, it suffices to show

$$\max_{1\leq j\leq n-2}\left\{\frac{\nu_2(b_0)-\nu_2(b_j)}{j}\right\}\leq\frac{n-2}{n}.$$

Since $\nu_2(a_0)=\nu_2(\pm1)=0$ and $\nu_2(a_j)\geq 0$, we need only show

$$\max_{1\leq j\leq n-2}\left\{\frac{\nu_2(n!)-\nu_2(n!/j!)}{j}\right\}\leq\frac{n-2}{n}. \tag{2}$$

Observe that this is stronger than the earlier inequality we obtained with $(n-2)/n$ replaced by $(n-2)/(n-1)$. Since $n-2=2^\ell-1$, we obtain for $1\leq j\leq n-2$ that

$$\nu_2(j!)=\left[\frac{j}{2}\right]+\left[\frac{j}{4}\right]+\cdots+\left[\frac{j}{2^{\ell-1}}\right]\leq j\left(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^{\ell-1}}\right)=\frac{j\left(2^{\ell-1}-1\right)}{2^{\ell-1}}=\frac{j(n-3)}{n-1}.$$

Thus,

$$\frac{\nu_2(n!) - \nu_2(n!/j!)}{j} = \frac{\nu_2(j!)}{j} \le \frac{n-3}{n-1} < \frac{n-2}{n} \quad \text{for } 1 \le j \le n-2.$$

Hence, (2) follows.

Now, suppose that $n = 2^\ell$ for some positive integer ℓ and that $k = 2$. Here, Lemma 1 implies $a_n = \pm(n-1)$. We define $g(x)$ as above. Since a_n is odd, the left-most endpoint of the Newton polygon of $g(x)$ with respect to 2 is $(0,0)$. Since

$$\nu_2(n!) = [n/2] + [n/4] + \cdots = 2^{\ell-1} + 2^{\ell-2} + \cdots + 2 + 1 = 2^\ell - 1,$$

the right-most endpoint of the Newton polygon of $g(x)$ with respect to 2 is $(n, 2^\ell - 1) = (n, n-1)$. Analogous to the previous case, the slope of the right-most edge of the Newton polygon of $g(x)$ with respect to 2 is

$$\max_{1\le j\le n} \left\{ \frac{\nu_2(n!) - \nu_2(n!/j!)}{j} \right\} = \max_{1\le j\le n} \left\{ \frac{\nu_2(j!)}{j} \right\} \le \max_{1\le j\le n} \left\{ \frac{j-1}{j} \right\} = \frac{n-1}{n}.$$

We deduce that the Newton polygon of $g(x)$, and hence of $F(x)$, with respect to 2 consists of the line segment joining $(0,0)$ to $(n, n-1)$. Since $\gcd(n, n-1) = 1$, we conclude $F(x)$ cannot have a quadratic factor.

This completes the proof of Theorem 2.

5. The Proof of Theorem 3

The proof of Theorem 3 will mainly be based on the ideas already presented in the proof of Theorem 2. The possibility that $f(x)$ has a linear factor or has a factor of degree $k \ge 8$ will not involve any new ideas, and we shall not elaborate much on these details. There are however two aspects of the arguments here that will be different, one which deals with the possibility that $f(x)$ has a factor of degree $k \in [3,7]$ and one which deals with the possibility that $f(x)$ has a quadratic factor.

As before we set $F(x) = \sum_{j=0}^n b_j x^j$ with $b_j = n!a_j/j!$, and assume that $F(x)$ has a factor of degree $k \in [1, n/2]$. Lemma 2 was an immediate consequence of Lemma 1. A stronger result than Lemma 2 that also follows immediately from Lemma 1 is the following.

Lemma 12. *If $F(x)$ has a linear factor in $\mathbb{Z}[x]$, then $n | a_n$.*

The above lemma clarifies the situation when $k = 1$. To establish Theorem 3, we only need to show now that if n is sufficiently large, then any $f(x)$ as in the statement of the theorem cannot have a factor of degree $k \in [2, n/2]$. To deal with large values of k, we use a variant of (1). Specifically, Lemma 1 implies that if $F(x)$ is as in the statement of Theorem 3, then $F(x)$ cannot have a factor of degree k if

$$(3) \qquad \prod_{\substack{p^r \| n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r > C n^{3/2}.$$

We consider $k \in [8, n/2]$. Lemma 5 (with n sufficiently large) implies

$$\prod_{\substack{p^r || n(n-1)\cdots(n-k+1) \\ p \ge k+1}} p^r \ge \sqrt{\binom{n}{k}} \ge \sqrt{\binom{n}{8}},$$

and it easily follows that (3) holds in this case.

Next, we consider $k \in [3, 7]$. We will make use of a result of K. Mahler which we state in the form given in [15].

Lemma 13. *Let c and v be two positive constants, and let*

$$p_1, \dots, p_r, p_{r+1}, \dots, p_{r+r'}, p_{r+r'+1}, \dots, p_{r+r'+r''}$$

be finitely many distinct primes. Denote by Σ an infinite sequence of distinct triples

$$\{P^{(k)}, Q^{(k)}, R^{(k)}\} \qquad (k = 1, 2, 3, \dots)$$

where $P^{(k)}$, $Q^{(k)}$, and $R^{(k)}$ are integers as follows,

$$P^{(k)} \ne 0, \quad Q^{(k)} \ne 0, \quad R^{(k)} \ne 0, \quad P^{(k)} + Q^{(k)} + R^{(k)} = 0,$$

$$\left(P^{(k)}, Q^{(k)}\right) = \left(P^{(k)}, R^{(k)}\right) = \left(Q^{(k)}, R^{(k)}\right) = 1.$$

Put

$$H^{(k)} = \max\left(\left|P^{(k)}\right|, \left|Q^{(k)}\right|, \left|R^{(k)}\right|\right),$$

and write $P^{(k)}$, $Q^{(k)}$, and $R^{(k)}$ as products of integers,

$$P^{(k)} = P_1^{(k)} P_2^{(k)}, \quad Q^{(k)} = Q_1^{(k)} Q_2^{(k)}, \quad R^{(k)} = R_1^{(k)} R_2^{(k)},$$

where $P_1^{(k)}$ has no prime factors distinct from $p_{r+1}, \dots, p_{r+r'}$, $Q_1^{(k)}$ has no prime factors distinct from $p_{r+r'+1}, \dots, p_{r+r'+r''}$, and $R_1^{(k)}$ has no prime factors distinct from $p_1, \dots, p_r$. If

$$\left|P_2^{(k)} Q_2^{(k)} R_2^{(k)}\right| \le c H^{(k)v} \qquad (k = 1, 2, 3, \dots),$$

then $v \ge 1$.

We make use of the above lemma to establish the following.

Lemma 14. *Let a be a fixed non-zero integer, and let N be a fixed positive integer. Let $\varepsilon > 0$. If n is sufficiently large (depending on a, N, and ε), then the largest divisor of $n(n+a)$ which is relatively prime to N is $\ge n^{1-\varepsilon}$.*

Proof. We show that there are only finitely many positive integers n satisfying $\mathcal{P}$ where $\mathcal{P} = \mathcal{P}(n)$ denotes the property that the largest divisor of $n(n+a)$ relatively prime to N

is $< n^{1-\varepsilon}$. For each positive integer n satisfying $\mathcal{P}$, we consider $d = \gcd(a, n)$. Thus, n is associated with a pairwise relatively prime triple $\{P, Q, R\}$ as in Lemma 13 with

$$P = (n+a)/d, \quad Q = -a/d, \quad \text{and} \quad R = -n/d.$$

Observe that d is uniquely determined by Q and hence n is uniquely determined by Q and R. In other words, there is a one-to-one correspondence between n satisfying $\mathcal{P}$ and the triples $\{P, Q, R\}$ arising from such n. For each triple $\{P, Q, R\}$, we consider $H = \max\{|P|, |Q|, |R|\}$. Let $p_1, \ldots, p_s$ be the complete list of distinct prime divisors of N. We momentarily fix an ordering of these primes and integers r and r' with $0 \le r \le r + r' \le s$. With the ordering and r and r' fixed, we consider triples $\{P, Q, R\}$ arising from n as above and write

$$P = P_1 P_2, \quad Q = Q_1 Q_2, \quad \text{and} \quad R = R_1 R_2$$

where P_1 has no prime factors distinct from $p_{r+1}, \ldots, p_{r+r'}$, Q_1 has no prime factors distinct from $p_{r+r'+1}, \ldots, p_s$, and R_1 has no prime factors distinct from $p_1, \ldots, p_r$. Setting $r'' = s - r - r'$, $c = |a|^2$, and $v = 1 - \varepsilon$, we obtain from Lemma 13 that there can be only finitely many triples $\{P, Q, R\}$ satisfying

$$|P_2 Q_2 R_2| \le |a|^2 H^{1-\varepsilon}.$$

Since $d \le |a|$, we deduce

$$|a|^2 H^{1-\varepsilon} \ge |a|^2 \left(\frac{n}{d}\right)^{1-\varepsilon} \ge |a|\, n^{1-\varepsilon}.$$

Thus, there are only finitely many n for which $|P_2 Q_2 R_2| \le |a|\, n^{1-\varepsilon}$. We now let the ordering on the primes $p_1, \ldots, p_s$ vary as well as the values of r and r' noting that there are only a finite number (depending on a and N) of possible orderings and values of r and r' to consider. Observe that if n satisfies property $\mathcal{P}$, then the largest divisor of PQR relatively prime to N is $< |a| n^{1-\varepsilon}$. In particular, there is an ordering of the primes $p_1, \ldots, p_s$ and values of r and r' for which $|P_2 Q_2 R_2| \le |a| n^{1-\varepsilon}$. As we have just seen, there can be only finitely many such n. ■

Now, we make an argument similar to that used by Erdős in [8]. For each prime $p \le k$, consider s_p equal to an element from $\{n, n-1, \ldots, n-k+1\}$ with $\nu_p(s_p)$ as large as possible. Let

$$S = \{n, n-1, \ldots, n-k+1\} - \{s_p : p \le k\}.$$

Since $k \ge 3$, the set S contains at least one element, say s, and there are at least two additional integers, say m and $m + a$, among the numbers $n, n-1, \ldots, n-k+1$. For each $p \le k$, we have removed a multiple of p, namely s_p, from $\{n, n-1, \ldots, n-k+1\}$ in obtaining S so that there are at most $[k/p]$ multiples of p that can be in S. The definition of s_p in fact implies that there are at most $[k/p^j]$ multiples of p^j in S for each $j \ge 1$. Thus,

$$\nu_p\left(\prod_{u \in S} u\right) \le \sum_{j=1}^{\infty} \left[\frac{k}{p^j}\right] = \nu_p(k!) \quad \text{for } p \le k.$$

In particular, for such p, $\nu_p(s) \le \nu_p(k!)$. We deduce

$$\prod_{\substack{p^r || s \\ p \ge k+1}} p^r \ge \frac{s}{k!}.$$

Let $N = \prod_{p \le k} p$ and recall $k \le 7$. By Lemma 14, provided n (and hence $n-k+1$) is sufficiently large,

$$\prod_{\substack{p^r || m(m+a) \\ p \ge k+1}} p^r \ge n^{3/4} \ge 2(7!)n^{1/2}.$$

Since $s \ge n-k+1 > n/2$, it follows that (3) holds. Hence, (3) holds for n sufficiently large and for all $k \in [3, n/2]$.

In the above arguments, it is clear that we could in fact establish a considerably stronger inequality than (3). The more delicate case which we now consider is when $k = 2 \le n/2$. To clarify how the bound in (3) arises and hence our bound on $|a_n|$ in Theorem 3, we define $\psi = \psi(n) = Cn^{1/2}$, the ratio of the right-hand side of (3) to n. We write $g(x) = a_n x^n + \sum_{j=0}^{n-1} (n!/j!)x^j$. As before (in dealing with the possibility that $f(x)$ has a quadratic factor in Theorem 2), we want to relate the Newton polygon of $g(x)$ with respect to 2 with the Newton polygon of $F(x)$ with respect to 2. In this case, the Newton polygon of $g(x)$ with respect to 2 cannot be described as precisely. Observe that Lemma 1 implies that the largest odd factor of $n(n-1)$ divides a_n. Define non-negative integers r, s, m, and m' by

$$n(n-1) = 2^r m \quad \text{and} \quad |a_n| = 2^s m' m \quad \text{where } 2 \nmid m'm.$$

From

$$n(n-1) = 2^r m = 2^{r-s}(2^s m) \le 2^{r-s}|a_n| \le 2^{r-s} n\psi(n),$$

we deduce

$$r - s > \log_2\left(\frac{n-1}{\psi}\right) = \log_2\left(\frac{n}{\psi}\right) + O(1/n).$$

In particular, $r > s$ and r is greater than the right-hand side above.

We consider two cases depending on whether n is odd or even. First, suppose n is odd and sufficiently large. The definition of s implies that $(0, s)$ is the left-most spot of the Newton polygon of $g(x)$ with respect to 2. Since n is odd, $(1, 0)$ is also a spot obtained in the construction of this Newton polygon. The definition of r implies we can write $n-1 = 2^r w$ for some positive odd integer w. Observe that $m = wn$ so that $2^s m \le |a_n| \le n\psi$ implies

$$w \le \psi \quad \text{and} \quad s \le \log_2\left(\frac{\psi}{w}\right).$$

Let D denote the number of times the digit 1 occurs in the binary expansion of w. It is an easy exercise to show that

$$D = w - \left[\frac{w}{2}\right] - \left[\frac{w}{4}\right] - \cdots .$$

Let γ denote the greatest integer $\leq \log_2 w$. If $D = \gamma + 1$, then necessarily $w = 2^{\gamma+1} - 1$ and we deduce $D = \log_2(w+1)$. On the other hand, if $D \neq \gamma + 1$, then $D \leq \gamma \leq \log_2 w$. Thus, in any case, we deduce

$$w - \left[\frac{w}{2}\right] - \left[\frac{w}{4}\right] - \cdots \leq \log_2(w+1).$$

Thus,

$$\begin{aligned}
\nu_2(n!) = \nu_2((n-1)!) &= \left[\frac{2^r w}{2}\right] + \left[\frac{2^r w}{4}\right] + \cdots + \left[\frac{2^r w}{2^r}\right] + \left[\frac{2^r w}{2^{r+1}}\right] + \cdots \\
&= 2^{r-1} w + 2^{r-2} w + \cdots + 2w + w + \left[\frac{w}{2}\right] + \left[\frac{w}{4}\right] + \cdots \\
&= 2^r w - w + \left[\frac{w}{2}\right] + \left[\frac{w}{4}\right] + \cdots \\
&= n - 1 - w + \left[\frac{w}{2}\right] + \left[\frac{w}{4}\right] + \cdots \\
&= n - E,
\end{aligned}$$

where

$$2 \leq E = 1 + w - \left[\frac{w}{2}\right] - \left[\frac{w}{4}\right] - \cdots \leq 1 + \log_2(w+1).$$

Note that the bound on s given above implies

$$s + E \leq 1 + \log_2 \psi + \log_2 \left(1 + \frac{1}{w}\right) \leq 2 + \log_2 \psi.$$

From this we obtain from the previous bound on $r - s$ that

$$r - 2s - E = (r - s) - (s + E) \geq \log_2 n - 2\log_2 \psi - 2 + O(1/n).$$

The definition of ψ now implies

$$(4) \qquad r - 2s - E \geq -2 - 2\log_2 C + O(1/n).$$

We will make use of this inequality momentarily but note here that the condition $C < 1/\sqrt{2}$ in Theorem 3 implies that the right-hand side of (4) is > -1.

The right-most spot of the Newton polygon of $g(x)$ with respect to 2 is $(n, n-E)$. In dealing with the analogous situation in the proof of Theorem 2, we had $n = 2^\ell + 1$, $s = 0$, and $E = 2$. We were able to describe precisely the Newton polygon of $g(x)$ with respect to 2. In particular, we showed that the right-most edge had slope $\leq (n-2)/(n-1)$. That same argument works here. Let ℓ be the line passing through the spot $(n, n-E)$ and having slope $(n-2)/(n-1)$. Then every spot obtained in the construction of the Newton polygon of $g(x)$ with respect to 2 is on or to the left of ℓ. Since $n - 1 = 2^r w$ and $n!/(n-j)!$ has $n-1$ as a factor for $j \in \{2, 3, \ldots, n\}$, each spot $(j, \nu_2(n!/(n-j)!))$ for such j is on or above the line $y = r$. Since n is sufficiently large, $r > s$. Thus, each spot other than the two left-most spots $(0, s)$ and $(1, 0)$ is in the closed region R in the plane bounded above

$y = r$ and to the left of ℓ. Observe that $E \geq 2$ and the definition of ℓ imply that both $(0, s)$ and $(1, 0)$ are on or above ℓ. The points $(0, s)$ and $(n, n - E)$ are also spots obtained in constructing the Newton polygon of $F(x)$ with respect to 2, and the remaining spots in obtaining this Newton polygon, other than possibly the second spot from the left, must also lie in the region R. Let $(1, u)$ denote the second spot from the left. The left-most edge of this Newton polygon will have a negative slope if $u < s$, but since $r > s$, the remaining edges will have positive slopes. In particular, the assumption that $F(x)$ has a factor of degree $k = 2$ implies that there are two lattice points, say (a, b) and (c, d), along an edge of the Newton polygon of $F(x)$ with respect to 2 such that $d - b \geq 1$ and either $c - a = 1$ or $c - a = 2$. The right-most edge of the Newton polygon of $g(x)$ with respect to 2, and hence the right-most edge of the Newton polygon of $F(x)$ with respect to 2, has slope $\leq (n - 2)/(n - 1) < 1$. Since the slopes of the edges increase from left to right, we obtain $(d - b)/(c - a) < 1$. Since $d - b \geq 1$, we deduce $c - a \neq 1$. Thus, $c - a = 2$. Now, $(d - b)/(c - a) < 1$ and $d - b \geq 1$ imply $d - b = 1$. Therefore, there must be an edge of the Newton polygon of $F(x)$ with respect to 2 that has slope $1/2$.

We show that the above is impossible by showing that each edge with a positive slope has slope $> 1/2$. Let P be the point of intersection of the lines $y = r$ and ℓ. Let ℓ' denote the line passing through $(0, s)$ and P, and let t denote its slope. We claim that if an edge of the Newton polygon of $F(x)$ with respect to 2 has positive slope, then that slope must be $\geq \min\{t, 1\}$. To see this, suppose first that $(1, u)$ is on or above ℓ'. Then all the spots in obtaining the Newton polygon of $F(x)$ with respect to 2 lie on or above ℓ', and we can deduce that the left-most edge must have slope at least t. Since the slopes of the edges increase from left to right, we get in this case all the edges have slope $\geq t$. Now, suppose $(1, u)$ is below ℓ'. Then the left-most edge has slope $u - s$ which is either ≤ 0 or ≥ 1. Every spot lies on or above the line passing through $(1, u)$ and P, and it follows that the slope of the second left-most edge is at least as large as the slope of the line through $(1, u)$ and P. But the slope of that line is $\geq t$. Hence, every edge with a positive slope has slope $\geq \min\{t, 1\}$.

It now suffices to show that $t > 1/2$. The coordinates of P and, hence, the slope of ℓ' can be computed directly. We obtain

$$t = \frac{(r - s)(n - 2)}{(r + E)(n - 1) - n}.$$

The inequality $t > 1/2$ is equivalent to

$$(r - 2s - E)(n - 1) > r - s - n.$$

Recall that n is sufficiently large and $C < 1/\sqrt{2}$. We deduce from (4) that $r - 2s - E$ is greater than -1 plus a positive constant (depending on C). On the other hand, it is easy to see that both r and s must be $\ll \log n$. Hence, $t > 1/2$.

We have still to consider the possibility that n is even and sufficiently large. Here, $n = 2^r w$ for some odd integer w. The left-most spot on the Newton polygon of $g(x)$ with respect to 2 is $(s, 0)$ and the right-most spot is $(n, n - E)$ for some $E \in [1, \log_2(w + 1)]$. Here, the right-most edge of the Newton polygon has slope $\leq (n - 1)/n$. Letting ℓ now denote the line passing through $(n, n-E)$ with slope $(n-1)/n$ and considering R to be the set of points on or above $y=r$ and on or to the left of ℓ, we continue as in the case that n is odd. Here, the situation is somewhat easier since every edge will have a positive slope. We omit further details.

6. Miscellaneous Remarks

We begin with a proof of Theorem 4. We consider $r=1$ in Lemma 1 and observe that Lemma 1 holds with the condition $p \nmid a_n$ replaced by $p \nmid a_n a_0$; in fact, no change (other than taking $r=1$) is required in the proof of Lemma 1 as given. By Theorem 6, for any integer $k \in [1, n/2]$, there is a prime $p \geq k+1$ dividing $n(n-1)\cdots(n-k+1)$. The condition $\gcd(a_n a_0, n!) = 1$ implies that such a p does not divide $a_n a_0$. Hence, by Lemma 1 so revised, $f(x)$ cannot have a factor of degree k for any $k \in [1, n/2]$. It follows that $f(x)$ must be irreducible, and hence Theorem 4 is established.

Since Theorem 2 is a generalization of Theorem 1 with the condition $|a_n| = 1$ being relaxed, it is reasonable to ask whether an analogous result to Theorem 2 holds with instead the condition $|a_0| = 1$ in Theorem 1 relaxed. There is certainly irreducibility results that can be obtained along this line, but nothing as strong as the analog to Theorem 2 can hold in this case. For example, in Theorem 2, if $a_n = \pm 2$ and $a_0 = 1$, we can deduce that $f(x)$ is irreducible unless $f(x)$ is one of the following:

$$\pm(x+1)^2, \quad \pm(x-1)^2, \quad \text{or} \quad \pm\,(x+1)(x-1).$$

On the other hand, if $a_0 = 2$ and a_n is fixed, then there are arbitrarily large n for which $f(x)$ can be reducible. Specifically, we consider $n = 2^\ell$ with ℓ a positive integer, and we take $a_2 = a_3 = \cdots = a_{n-2} = 0$. Observe that $\nu_2(n!) = n-1$, and write $n! = 2^{n-1}m$ where m is an odd integer. We deduce that

$$\frac{n!f(2)}{2^n} = a_n + 2^{\ell-1}a_{n-1} + ma_1 + m.$$

Since m is odd, there exist integers a_{n-1} and a_1 for which this last expression above is 0. Hence, for some $a_1, a_2, \ldots, a_{n-1}$, $f(x)$ has $x-2$ as a factor.

As mentioned in the introduction, an effective version of Theorem 3 can be obtained if we require

$$0 < |a_n| \leq n \exp\left(\sqrt{\frac{\log n}{(\log\log n)^3}}\right).$$

We sketch how this can be done. It will be clear from the argument that a slight improvement on this bound is possible, but we do not bother with such details here.

The more difficult case in Section 5 with $k=2$ does not need to be modified (the estimates there are already effective). In fact, the only change that needs to be made is in the case that $k \in [3, 7]$ (and now the worse estimate comes from $k=3$). To obtain the above version of Theorem 3, we replace the role of Lemmas 13 and 14 with the following (the remaining arguments are essentially the same).

Lemma 13′. *Let ℓ be a positive integer. Let $a_1, \dots, a_\ell$ be positive integers with $a_j \le A_1$ for $1 \le j \le \ell - 2$ and with each of $a_{\ell-1}$ and $a_\ell \le A_2$ where A_1 and A_2 are both ≥ 3. Let $b_1, \dots, b_\ell$ be integers with each b_j having absolute value $\le B$ where $B \ge 2$. Set*

$$\Lambda = b_1 \log a_1 + \cdots + b_\ell \log a_\ell.$$

There is a positive constant c depending only on ℓ and A_1 such that either $\Lambda = 0$ or

$$|\Lambda| > \exp\left(-c \log^2 A_2 \log B \log\log A_2\right).$$

Lemma 13′ is due to A. Baker [1]. Baker actually proved substantially more, but the above will suffice for our purposes. In particular, c can be made explicit. For a discussion of some other related work, see the section on "New Developments" in [2] and the notes on page 31 of [21].

Lemma 14′. *Let a be a non-zero integer, and let N be a fixed positive integer. There is an effectively computable constant $n_0 = n_0(a, N)$ such that if $n \ge n_0$, then the largest divisor of $n(n+a)$ which is relatively prime to N is*

$$\ge 2(7!) \exp\left(\sqrt{\frac{\log n}{(\log\log n)^3}}\right).$$

Proof. Let a be as in the lemma, and let $p_1, \dots, p_r$ be the complete list of prime divisors of N. Let n be large, and let m_1 and m_2 be the largest divisors of n and $n + a$, respectively, which are relatively prime to N. Thus, we can find non-negative integers $e_1, \dots, e_r$ and $f_1, \dots, f_r$ such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} m_1 \quad \text{and} \quad n + a = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} m_2.$$

Set

$$\Lambda = (f_1 - e_1) \log p_1 + (f_2 - e_2) \log p_2 + \cdots + (f_r - e_r) \log p_r + \log m_2 - \log m_1.$$

Thus, $\Lambda = \log((n+a)/n) \asymp |a|/n \ll 1/n$. In particular, $\Lambda \ne 0$. Since N is fixed, each p_j is $\ll 1$. Also, each e_j and f_j (and, hence, $f_j - e_j$) is $\ll \log n$. Letting $A = \max\{3, m_1, m_2\}$, we deduce from Lemma 13 that for some constant c depending only on N,

$$\frac{1}{n} \gg \exp\left(-c \log^2 A \log\log A \log\log n\right).$$

This inequality implies that

$$A \ge 2(7!) \exp\left(\sqrt{\frac{\log n}{(\log\log n)^3}}\right),$$

and the lemma follows. ∎

Finally, we comment that in [12], Patrick Harley obtained a complete list of the reducible polynomials that exist when $2 \le a_n \le 10$. The case that a_n is prime has already been addressed at the end of the introduction. We summarize some of Harley's findings by noting that when $a_n = 4$, there are reducible $f(x)$ only of degrees $n = 2$ and 4; when $a_n = 6$, there are reducible $f(x)$ only of degrees $n = 2$, 3, 4, and 6; when $a_n = 8$, there are reducible $f(x)$ only of degrees $n = 2$, 4, and 8; when $a_n = 9$, there are reducible $f(x)$ only of degrees $n = 3$ and 9; and when $a_n = 10$, there are reducible $f(x)$ only of degrees $n = 2$, 5, and 10.

Acknowledgments: The author thanks P. Moree, A. Schinzel, and the referee for several of the references below. In particular, the referee pointed out reference [7] and Schinzel reference [15], and each of these played a crucial role in the final version of this paper.

References

1. A. Baker, *The theory of linear forms in logarithms*, *Transcendence Theory: Advances and Applications*, Academic Press, London, 1977, pp. 1–27.
2. A. Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1979.
3. D.N. Bernstein, *The number of integral points in integral polyhedra*, Funct. Anal. Appl. **10** (1976), 223-224.
4. R.F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, L'Enseignement Math. **33** (1987), 183–189.
5. L.E. Dickson, *History of the Theory of Numbers, Vol. II*, Chelsea, N.Y., 1971.
6. G. Dumas, *Sur quelques cas d'irréducibilité des polynomes à coeffcients rationnels*, Journal de Math. Pures et Appl. **2** (1906), 191–258.
7. E.F. Ecklund, Jr., R.B. Eggleton, P. Erdős, and J.L. Selfridge, *On the prime factorization of binomial coefficients*, J. Austral. Math. Soc. (Series A) **26** (1978), 257–269.
8. P. Erdős, *On consecutive integers*, Nieuw Archief voor Wiskunde III **3** (1955), 124–128.
9. M. Filaseta, *The irreducibility of all but finitely many Bessel polynomials*, Acta Math. **174** (1995), 383–397.
10. A. Granville, *On the scarcity of powerful binomial coefficients*, preprint.
11. E. Grosswald, *Bessel Polynomials*, Lecture Notes in Mathematics, Vol. 698, Springer-Verlag, Berlin, 1978.
12. P. Harley, *A generalization of an irreducibility theorem of I. Schur*, Masters' Thesis, University of South Carolina (1995).
13. H. Ille, *Zur Irreduzibilität der Kugelfunktionen*, Jahrbuch der Dissertationen der Universität Berlin (1924).
14. M. Jutila, *On numbers with a large prime factor II*, J. Indian Math. Soc. (N.S.) **38** (1974/75), 124–130.
15. K. Mahler, *Lectures on Diophantine Approximations*, Cushing-Malloy, Ann Arbor, 1961.
16. A.M. Ostrowski, *On multiplication and factorization of polynomials, I. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. **13** (1975), 201–228.

17. K. Ramachandra, *A note on numbers with a large prime factor III*, Acta Arith. **19** (1971), 77–90.
18. K. Ramachandra and T.N. Shorey, *On gaps between numbers with a large prime factor*, Acta Arith. **24** (1973), 99–111.
19. I. Schur, *Einege Sätze über Primzahlen mit Anwendugen auf Irreduzibilitätsfragen, I*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse. **14** (1929), 125–136.
20. T.N. Shorey, *On gaps between numbers with a large prime factor II*, Acta Arith. **25** (1973/74), 365–373.
21. T.N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Univ. Press, Cambridge, 1986.
22. J.J. Sylvester, *On arithmetical series*, Messenger of Math. **21** (1892), 1–19.
23. R. Tijdeman, *On the maximal distance of numbers with a large prime factor*, J. London Math. Soc. (2) **5** (1972), 313–320.
24. J.H. Wahab, *New cases of irreducibility of Legendre polynomials*, Duke Math J. **19** (1952), 165–176.

Mathematics Department
University of South Carolina
Columbia, SC 29208

filaseta@math.sc.edu