ON THE IRREDUCIBILITY OF A CERTAIN CLASS OF LAGUERRE POLYNOMIALS

Michael Filaseta[1]
Mathematics Department
University of South Carolina
Columbia, SC 29208

Richard L. Williams, Jr.
Mathematics Department
University of South Carolina
Columbia, SC 29208

June 6, 2001

[1] The authors were supported by grants from the National Security Agency. Research by the second author associated with this paper was done in partial fulfillment of the requirement for a Ph.D. at the University of South Carolina.

1 Introduction

The generalized Laguerre polynomials are defined by

$$L_m^{(\alpha)}(x) = \sum_{j=0}^{m} \binom{m+\alpha}{m-j} \frac{(-x)^j}{j!}.$$

where m denotes a positive integer (the degree) and α a real number. In two papers, I. Schur [10, 11] investigated the irreducibility of $L_m^{(0)}(x)$ and $L_m^{(1)}(x)$ as well as their associated Galois groups. He established that these polynomials are irreducible for all positive integers m and that the Galois group of $L_m^{(0)}(x)$ is the symmetric group S_m for all m and the Galois group of $L_m^{(1)}(x)$ is the alternating group A_m if $m > 1$ is odd or if $m + 1$ is an odd square and, otherwise, the Galois group is S_m. That the Galois group of $L_m^{(1)}(x)$ is A_m whenever m is *odd* (and sometimes when m is a multiple of 4) is of particular interest as a classical result of Van der Waerden [12] is that almost all polynomials in a certain asymptotic sense have Galois group S_m. More recently, R. Gow [7] showed that the Laguerre polynomials $L_m^{(m)}(x)$ provide a possible complimentary list of polynomials to $L_m^{(1)}(x)$ in the sense that for each *even* m the polynomial $L_m^{(m)}(x)$ may well have Galois group A_m. More specifically, he established that if m is even, then the Galois group of $L_m^{(m)}(x)$ is A_m provided that the polynomial $L_m^{(m)}(x)$ is irreducible over the rationals. A computation shows that for $2 < m \leq 100$, $L_m^{(m)}(x)$ is irreducible. In addition, Gow established the irreducibility of $L_m^{(m)}(x)$ when m is of the form $2p^k$ where p is a prime greater than 3 or when m is of the form $4p^k$ where p is a prime greater than 7. The purpose of this paper is to give some further insight into the irreducibility of the polynomials $L_m^{(m)}(x)$. We establish

Theorem 1. *For almost all positive integers m the polynomial $L_m^{(m)}(x)$ is irreducible over the rationals (and, hence, has Galois group A_m for almost all even m). More precisely, the number of $m \leq t$ such that $L_m^{(m)}(x)$ is reducible is*

$$\ll \exp\left(\frac{9\log(2t)}{\log\log(2t)}\right).$$

Furthermore, for all but finitely many m, $L_m^{(m)}(x)$ is either irreducible or $L_m^{(m)}(x)$ is the product of a linear polynomial times an irreducible polynomial of degree $m-1$.

Our approach will be based on recent work of the first author [3, 4] and of his joint works with T.-Y. Lam [5] and O. Trifonov [6]. There several irreducibility results were established by combining the use of Newton polygons with information on the distribution of primes. Similar to the general form of these results and to the original work of Schur, we establish the following result from which Theorem 1 is an easy consequence.

Theorem 2. *For all but $O\big(\exp(9\log(2t)/\log\log(2t))\big)$ positive integers $m \leq t$, the polynomial*

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

is irreducible over the rationals for every choice of integers $a_0, a_1, \ldots, a_m$ with $|a_0| = |a_m| = 1$. Furthermore, there is an absolute constant m_0 such that the exceptional m for which some choice of integers $a_0, a_1, \ldots, a_m$ as above produces a reducible polynomial $f(x)$ are either $< m_0$ or are of the form $m = 2^i \times 3^j \times n$ where

$$n < \exp\left(\frac{8\log(2m)}{\log\log(2m)}\right).$$

In the case that $m \geq m_0$, either $f(x)$ is irreducible or $f(x)$ is the product of a linear polynomial times an irreducible polynomial of degree $m-1$.

We let A denote the set of exceptional m in Theorem 2, and let $A(t)$ denote the number of elements of A that are $\leq t$. Thus, Theorem 2 gives

$$A(t) \ll \exp\left(\frac{9\log(2t)}{\log\log(2t)}\right).$$

We note that the set A is nonempty. Indeed, 2 is an element of A since

$$2!L_2^{(2)}(x) = (x^2 - 8x + 12) = (x-6)(x-2).$$

The polynomial $L_2^{(2)}(x)$ may well be the only example of a reducible $L_m^{(m)}(x)$. However, we show in the final section of this paper that the set A is infinite. Our next theorem follows from the methods given there.

Theorem 3. $A(t) \gg \log t$.

Because of our approach for determining whether $f(x)$ has a quadratic factor, the value of m_0 in Theorem 2 is ineffective. We note here, however, that our approach can be modified to give an explicit constant x_0 such that if $m \geq x_0$, then either $f(x)$ is irreducible or it has a factor of degree ≤ 2.

Consider $f(x)$ as in the statement of Theorem 2. Define $c_m = a_m$, and

$$c_j = a_j\binom{m}{j}(2m)(2m-1)\cdots(m+j+1) \qquad \text{for } 0 \leq j \leq m-1.$$

Thus, we have

$$c_{m-1} = a_{m-1}\binom{m}{1}(2m), \;\; c_{m-2} = a_{m-2}\binom{m}{2}(2m)(2m-1), \ldots,$$

$$c_1 = a_1\binom{m}{1}(2m)(2m-1)\cdots(m+2), \;\text{ and }\; c_0 = a_0(2m)(2m-1)\cdots(m+1).$$

Thus, if $g(x) = m!f(x)$, then $g(x) = \sum_{j=0}^{m} c_j x^j$. Hence, it suffices to prove the analogous result in Theorem 2 for the polynomials $g(x) = \sum_{j=0}^{m} c_j x^j \in \mathbb{Z}[x]$.

We organize the remainder of this paper as follows. We begin by stating some general analytic results. Next, we provide a few technical lemmas crucial to the proof of Theorem 2. We prove Theorem 2 using a proof by contradiction. We assume that $g(x)$ has a factor of degree $k \in [1, m/2]$. We partition the interval $[1, m/2]$ into seven subintervals. In each such subinterval, we show that for m sufficiently large $g(x)$ cannot have a factor of degree k except in the case that $k = 1$ where $g(x)$ might have a linear factor if m takes on a specific form. We end the paper by giving a constructive proof that the set A is infinite.

2 Preliminaries

We begin with some analytic results which will aid in the proof of Theorem 2. We will make use of the following result of Rosser and Schoenfeld [9].

Lemma 1. *Let $\pi(x)$ denote the number of primes not exceeding x. Then*

$$\pi(x) < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) \qquad \text{for all } x > 1.$$

The next result can be found in [4].

Lemma 2. *Let a be a fixed non-zero integer, and let N be a fixed positive integer. Let $\epsilon > 0$. If m is sufficiently large (depending on a, N, and ϵ), then the largest divisor of $m(m+a)$ which is relatively prime to N is $\geq m^{1-\epsilon}$.*

Newton polygons will be an important tool utilized in determining the irreduciblility of the polynomials $g(x)$ discussed at the end of the previous section. We define the Newton polygon of a polynomial as follows. Let

$$f(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{Z}[x]$$

with $a_0 a_m \neq 0$. Let p be a prime, and let y be an integer. We use the p-adic notation

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

If $y = 0$, then we understand this to mean $\nu(y) = +\infty$. For $j \in \{0, 1, 2, \ldots, m\}$, we define the set of points

$$S = \{(0, \nu(a_m)), (1, \nu(a_{m-1})), \ldots, (m, \nu(a_0))\}$$

in the extended plane. We refer to the elements of S as the spots of $f(x)$. We consider the lower edges along the convex hull of these spots. The left-most edge has one endpoint being $(0, \nu(a_m))$ and the right-most edge has $(m, \nu(a_0))$ as an endpoint. The endpoints of every edge belong to the set S. 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 slopes of the edges are always increasing when calculated from the left-most edge to the right-most edge.

We will make use of the following result from [3] (which itself is based on work of M. G. Dumas [2]).

Lemma 3. *Let k and ℓ be integers with $k > \ell \geq 0$. Suppose $g(x) = \sum_{j=0}^{m} b_j x^j \in \mathbb{Z}[x]$ and p is a prime such that $p \nmid b_m$, $p | b_j$ for all $j \in \{0, 1, \ldots, m - \ell - 1\}$, and the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Then for any integers $a_0, a_1, \ldots, a_m$ with $|a_0| = |a_m| = 1$, the polynomial $G(x) = \sum_{j=0}^{m} a_j b_j x^j$ cannot have a factor with degree in the interval $[\ell + 1, k]$.*

3 Further Preliminaries

We now consider $f(x)$ as in Theorem 2 and $g(x) = m!f(x) = \sum_{j=0}^{m} c_j x^j$ as defined in the introduction. We establish some technical lemmas associated with the polynomial $g(x)$.

Lemma 4. *Let m be a positive integer. Suppose that p is a prime, that k and r are positive integers, and that ℓ is an integer in $[0, k)$ satisfying:*

(i) $p^r || (m - \ell)$ *or* $p^r || (2m - \ell)$

(ii) $p \geq 3k + 1$

(iii) $\Delta(r, p)\dfrac{\log(2m)}{p^r \log p} + \dfrac{1}{p-1} \leq \dfrac{1}{k}$ *where* $\Delta(r, p) = 2 \Big/ \left(1 - \dfrac{1}{3p^{r-1}}\right)$.

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

Proof. The conclusion of the lemma holds if $\ell \geq m$, so we suppose $\ell \leq m - 1$. The proof consists of verifying the hypotheses of Lemma 3. For this purpose, we only consider the case that $a_m = a_{m-1} = \cdots = a_0 = 1$. Then $c_m = 1$ so that $p \nmid c_m$. Also, we have

$$c_j = \binom{m}{j}(2m)(2m-1)\cdots(m+j+1) \qquad \text{for } 0 \leq j \leq m-1. \tag{1}$$

If $p^r || (2m - \ell)$, then it is clear from (1) that p divides c_j for $j \in \{0, 1, \ldots, m - \ell - 1\}$. If $p^r || (m - \ell)$, then writing (1) as

$$c_j = \binom{2m}{m-j} m(m-1)\cdots(j+1),$$

we see that p divides c_j for $j \in \{0, 1, \ldots, m - \ell - 1\}$.

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

$$\max_{1 \leq j \leq m} \left\{ \frac{\nu(c_0) - \nu(c_j)}{j} \right\}. \tag{2}$$

Let j be such that the quantity in (2) is maximal so that by (iii) it suffices to show that

$$\frac{\nu(c_0) - \nu(c_j)}{j} < \Delta(r, p)\frac{\log(2m)}{p^r \log p} + \frac{1}{p-1}.$$

Observe that by (1)

$$\frac{c_0}{c_j} = \frac{(2m)(2m-1)\cdots(m+1)}{\binom{m}{j}(2m)(2m-1)\cdots(m+j+1)} = \frac{j!(m+j)!(m-j)!}{m!^2}.$$

Since

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

we deduce

$$\begin{aligned}\nu(c_0) - \nu(c_j) &= \nu(j!) + \nu\left(\frac{(m+j)!}{m!}\right) - \nu\left(\frac{m!}{(m-j)!}\right) \qquad (3)\\ &< \frac{j}{p-1} + \sum_{s=1}^{\infty}\left(\left[\frac{m+j}{p^s}\right] - \left[\frac{m}{p^s}\right]\right) - \sum_{s=1}^{\infty}\left(\left[\frac{m}{p^s}\right] - \left[\frac{m-j}{p^s}\right]\right)\\ &= \frac{j}{p-1} + \sum_{s=1}^{N}\left(\left[\frac{m+j}{p^s}\right] - 2\left[\frac{m}{p^s}\right] + \left[\frac{m-j}{p^s}\right]\right)\end{aligned}$$

where $N = [\log(2m)/\log p]$. Note that

$$\left[\frac{m+j}{p^s}\right] - 2\left[\frac{m}{p^s}\right] + \left[\frac{m-j}{p^s}\right] < \frac{m+j}{p^s} - 2\left(\frac{m}{p^s} - 1\right) + \frac{m-j}{p^s} = 2$$

so that

$$\left[\frac{m+j}{p^s}\right] - 2\left[\frac{m}{p^s}\right] + \left[\frac{m-j}{p^s}\right] \le 1. \qquad (4)$$

If $j \ge p^r/\Delta(r,p)$, then using (3) and (4) we obtain

$$\frac{\nu(c_0) - \nu(c_j)}{j} < \frac{1}{p-1} + \frac{1}{j}\sum_{s=1}^{N} 1 = \frac{1}{p-1} + \frac{N}{j} \le \frac{1}{p-1} + \Delta(r,p)\frac{\log(2m)}{p^r \log p}$$

and our result follows.

Suppose that $j < p^r/\Delta(r,p)$ and choose e so that $p^e||(m+i)$ for some $1 \le i \le j$ with e maximal. We assume as we may that $e \ge 1$ for otherwise the quantity in (2) is equal to 0 and our result is trivial.

Claim. $e < r$.

To see that the claim is true, suppose $e \ge r$. If $p^r||(2m-\ell)$, then as $p^e||(m+i)$ we have $p^r|(2i+\ell)$. Thus,

$$p^r \le 2i + \ell < 2j + k \le 2j + \frac{p}{3} = 2j + \frac{p^r}{3p^{r-1}}.$$

Likewise, if $p^r||(m-\ell)$, then as $p^e||(m+i)$ we deduce $p^r|(i+\ell)$. Hence,

$$p^r \le i + \ell \le 2i + \ell < 2j + k \le 2j + \frac{p}{3} \le 2j + \frac{p^r}{3p^{r-1}}.$$

Both situations imply that

$$j \ge \frac{p^r}{2}\left(1 - \frac{1}{3p^{r-1}}\right) = p^r/\Delta(r,p),$$

which is a contradiction. The claim follows.

Using the claim, the fact that $p^r||(2m-\ell)$ or $p^r||(m-\ell)$, and the fact that $p^e||(m+i)$, we can replace r with e in the proof of the claim to obtain $j \ge p^e/\Delta(e,p)$. From the definition of e, we deduce for $s > e$ that

$$\left[\frac{m+j}{p^s}\right] - 2\left[\frac{m}{p^s}\right] + \left[\frac{m-j}{p^s}\right] = -\left[\frac{m}{p^s}\right] + \left[\frac{m-j}{p^s}\right] \le 0$$

so that

$$\sum_{s=1}^{N}\left(\left[\frac{m+j}{p^s}\right]-2\left[\frac{m}{p^s}\right]+\left[\frac{m-j}{p^s}\right]\right)\leq\sum_{s=1}^{e}\left(\left[\frac{m+j}{p^s}\right]-2\left[\frac{m}{p^s}\right]+\left[\frac{m-j}{p^s}\right]\right)\leq\sum_{s=1}^{e}1=e.$$

We now consider three possibilities: (1) $e \geq 2$, (2) $e = 1$ and $j < p$, and (3) $e = 1$ and $j \geq p$.

Suppose first that $e \geq 2$. Using $j \geq p^e/\Delta(e,p)$ we see that

$$\frac{\nu(c_0)-\nu(c_j)}{j}<\frac{1}{p-1}+\frac{e}{j}\leq\frac{1}{p-1}+\frac{e\Delta(e,p)}{p^e}. \tag{5}$$

Observe that $\Delta(e,p)$ decreases as e increases so that for $e \geq 2$ we have $\Delta(e,p) \leq \Delta(2,p)$. Also, $e/p^e \leq 2/p^2$. Hence, using (5) we have

$$\frac{\nu(c_0)-\nu(c_j)}{j}<\frac{1}{p-1}+\frac{2\Delta(2,p)}{p^2}=\frac{1}{p-1}+\frac{4}{p(p-\frac{1}{3})}.$$

Since $p \geq 3k+1$ we deduce $p \geq 5$. Further, we note that $p-1/3 > p-1 > 0$. From the inequality above we have

$$\frac{\nu(c_0)-\nu(c_j)}{j}<\frac{1}{p-1}+\frac{4}{p(p-1)}=\frac{p+4}{p(p-1)}\leq\frac{p+4}{p(3k)}\leq\frac{1}{k}\left(\frac{p+4}{p+10}\right)\leq\frac{1}{k}.$$

Applying Lemma 3 our result follows when $e \geq 2$.

Suppose that $e = 1$ and $j < p$. Since $j < p$ we deduce that $\nu(j!) = 0$. Note that previously in the argument we used the fact that $\nu(j!) < j/(p-1)$ leading to the expression $1/(p-1)$ in (5). Thus, we now obtain

$$\frac{\nu(c_0)-\nu(c_j)}{j}\leq\frac{e}{j}.$$

Also, as $e = 1$ and $j \geq p^e/\Delta(e,p) = p/\Delta(1,p) = p/3$ we have

$$\frac{\nu(c_0)-\nu(c_j)}{j}\leq\frac{1}{j}\leq\frac{3}{p}<\frac{3}{3k}=\frac{1}{k}.$$

Applying Lemma 3 our result follows when $e = 1$ and $j < p$.

Finally, suppose that $e = 1$ and $j \geq p$. We have

$$\frac{\nu(c_0)-\nu(c_j)}{j}<\frac{1}{p-1}+\frac{e}{j}\leq\frac{1}{p-1}+\frac{1}{p}<\frac{1}{2k}+\frac{1}{2k}=\frac{1}{k}.$$

Applying Lemma 3 our result follows when $e = 1$ and $j \geq p$. □

Lemma 5. *Let m be a positive integer. Suppose that p is a prime, that k and r are positive integers with $r \geq 2$, and that ℓ is an integer in $[0,k)$ satisfying:*

(i) $p^r || (m-\ell)$

(ii) $p \geq \max\{k+2, 2k-1\}$

(iii) $\dfrac{\log(2m)}{p^{r/2}\log p}+\dfrac{1}{p-1}\le\dfrac{1}{k}$.

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

Proof. For the proof of Lemma 5 we begin in a similar fashion as in the proof of Lemma 4. The proof consists of verifying the hypotheses of Lemma 3. We take $a_m=a_{m-1}=\cdots=a_0=1$. From the proof of Lemma 4, we see that $p\nmid c_m$ and if $p^r||(m-\ell)$ then p divides c_j for every $j\in\{0,1,\dots,m-\ell-1\}$.

Now, we need only show that the right-most edge of the Newton polygon of $g(x)$ with respect to p has slope $<1/k$. The right-most edge has slope given by (2). Let j be such that the quantity in (2) is maximal. We consider the following three possiblities: $j\le\ell$, $\ell+1\le j\le p^{r/2}$, and $j>p^{r/2}$.

Suppose $j\le\ell$. If $p|(m+i)$ for some $i\in\{1,2,\dots,j\}$, then since $p|(m-\ell)$ we deduce that p divides $i+\ell=(m+i)-(m-\ell)$ and

$$0<i+\ell\le j+\ell\le 2\ell\le 2(k-1)<p.$$

This is impossible, so $\nu((m+1)(m+2)\cdots(m+j))=0$. We obtain

$$\begin{aligned}\nu(c_0)-\nu(c_j)&\le\nu(j!)+\nu\left(\frac{(m+j)!}{m!}\right)-\nu\left(\frac{m!}{(m-j)!}\right)\\&=\nu(j!)-\nu\left(\frac{m!}{(m-j)!}\right)\le\nu(j!)<\frac{j}{p-1}<\frac{j}{k}.\end{aligned}$$

Dividing through by j and applying Lemma 3 our result follows when $j\le\ell$.

Suppose that $\ell+1\le j\le p^{r/2}$. Observe that condition (ii) in the lemma implies $p-1\ge 2k-2$ so that $k-1\le(p-1)/2$. Let $u=[r/2]+1$. By considering the parity of r we see that $u\ge(r+1)/2$. We now claim that the following inequality holds:

$$p^{r/2}+k-1<p^u. \tag{6}$$

To see that the inequality holds, we begin by noting that $g(r)=p^{r/2}$ is an increasing function of r for $r\ge1$. Furthermore,

$$g(1)=\sqrt{p}=\frac{2\sqrt{p}}{2}=\frac{\sqrt{p}+\sqrt{p}}{2}>\frac{\sqrt{p}+1}{2}.$$

Thus, it follows that $p^{r/2}>(\sqrt{p}+1)/2$ for all integers $r\ge1$. Multiplying both sides by $\sqrt{p}-1$ (which is positive as $p\ge2$) we have

$$\frac{p-1}{2}<(\sqrt{p}-1)p^{r/2}=p^{(r+1)/2}-p^{r/2}.$$

Hence,

$$p^{r/2}+k-1\le p^{r/2}+\frac{p-1}{2}<p^{r/2}+p^{(r+1)/2}-p^{r/2}\le p^u.$$

Thus, the inequality in (6) holds.

If $p^u|(m+i)$ for some $i \in \{1, 2, \dots, j\}$, then as in the case $j \le \ell$ we obtain $p^u|(i+\ell)$. Using $\ell + 1 \le j \le p^{r/2}$ and (6) we obtain

$$0 < i + \ell \le j + \ell \le p^{r/2} + k - 1 < p^u,$$

which is a contradiction. Therefore,

$$\sum_{s=1}^{\infty} \left(\left[\frac{m+j}{p^s} \right] - \left[\frac{m}{p^s} \right] \right) = \sum_{s=1}^{[r/2]} \left(\left[\frac{m+j}{p^s} \right] - \left[\frac{m}{p^s} \right] \right),$$

since the summand counts the number of multiples of p^s in $(m, m+j]$. Thus, we have

$$\begin{aligned} \nu(c_0) - \nu(c_j) &\le \frac{j}{p-1} + \sum_{s=1}^{[r/2]} \left(\left[\frac{m+j}{p^s} \right] - \left[\frac{m}{p^s} \right] \right) - \sum_{s=1}^{\infty} \left(\left[\frac{m}{p^s} \right] - \left[\frac{m-j}{p^s} \right] \right) \\ &\le \frac{j}{p-1} + \sum_{s=1}^{[r/2]} \left(\left[\frac{m+j}{p^s} \right] - 2\left[\frac{m}{p^s} \right] + \left[\frac{m-j}{p^s} \right] \right) - \sum_{s=[r/2]+1}^{\infty} \left(\left[\frac{m}{p^s} \right] - \left[\frac{m-j}{p^s} \right] \right). \end{aligned}$$

Recall (from the proof of Lemma 4) that the first summand on the right above is ≤ 1. On the other hand, there is a multiple of p^s for every $s \in ([r/2], r]$ in the interval $(m-j, m]$ (namely, the number $m - \ell$). Hence, the term

$$\left[\frac{m}{p^s} \right] - \left[\frac{m-j}{p^s} \right] \ge 1$$

for at least $r - [r/2] \ge r - (r/2) = r/2$ different s. Therefore, we obtain

$$\nu(c_0) - \nu(c_j) \le \frac{j}{p-1} + [r/2] - r/2 \le \frac{j}{p-1}.$$

Thus, in this case $(\nu(c_0) - \nu(c_j))/j < 1/k$ as well. Applying Lemma 3 we deduce that in the case $\ell + 1 \le j \le p^{r/2}$ our result follows.

Finally, suppose that $j > p^{r/2}$. Recall from the proof of Lemma 4 we have

$$\nu(c_0) - \nu(c_j) < \frac{j}{p-1} + \sum_{s=1}^{N} \left(\left[\frac{m+j}{p^s} \right] - 2\left[\frac{m}{p^s} \right] + \left[\frac{m-j}{p^s} \right] \right)$$

where $N = [\log(2m)/\log p]$. Also, in the proof of Lemma 4 we showed that

$$\left[\frac{m+j}{p^s} \right] - 2\left[\frac{m}{p^s} \right] + \left[\frac{m-j}{p^s} \right] \le 1.$$

Therefore, using these two facts combined with $j > p^{r/2}$ and (iii) we have

$$\frac{\nu(c_0) - \nu(c_j)}{j} < \frac{1}{p-1} + \frac{1}{j} \sum_{s=1}^{N} 1 \le \frac{1}{p-1} + \frac{N}{j} \le \frac{1}{p-1} + \frac{\log(2m)}{p^{r/2} \log p} \le \frac{1}{k}.$$

Applying Lemma 3 our result follows when $j > p^{r/2}$. □

We do not supply proofs for the next three results. The first is a consequence of gap results between primes (cf. M. N. Huxley [8]), the second can be found in G. Bachman [1], and the third is a straight forward exercise.

Lemma 6. *For m sufficiently large, there is a prime in the interval $(2m - m^{2/3}, 2m]$.*

Lemma 7. *Suppose p is a prime number and let n be a positive integer with*

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_s p^s,$$

as the base p representation of n (so that $0 \le a_i < p$ for each i). Then

$$\nu_p(n!) = \frac{n - s_n}{p - 1},$$

where $s_n = a_0 + a_1 + \cdots + a_s$.

Lemma 8. *Let k be a positive integer. If $k \equiv 3$ or $15 \pmod{18}$, then $3^2 || (2^k + 1)$.*

4 A Proof of Theorem 2

We consider m to be sufficiently large and assume that $g(x) = m!f(x)$ has a factor in $\mathbb{Z}[x]$ of degree $k \in [1, m/2]$. We divide the argument into cases depending on the size of k.

CASE 1. $m^{2/3} \le k \le m/2$.

Lemma 6 implies that for k in the interval above there exists a prime $p \in (2m - k, 2m]$. Thus, there exists a prime p of the form $2m - j$ where $j \in [0, k)$. In particular, we have $p > m$. Recall that

$$c_\ell = a_\ell \binom{m}{\ell} (2m)(2m-1)\cdots(m+\ell+1) \qquad \text{for } 0 \le \ell \le m-1.$$

Since $j \in \{0, 1, 2, \ldots, k-1\}$, the number $2m - j$ appears on the right-hand side above whenever $0 \le \ell \le m - k$. Therefore, we have

$$\nu_p(c_\ell) \ge 1 \qquad \text{for } \; 0 \le \ell \le m - k. \tag{7}$$

Also, $c_m = \pm 1$ implies $\nu_p(c_m) = 0$. To obtain a contradiction for the case under consideration, we show that $\nu_p(c_0) = 1$; the contradiction will be achieved since then it will follow that the right-most edge of the Newton polygon of $g(x)$ with respect to p has horizontal length $> m - k$ and the endpoints are this edge's only lattice points. In other words, $g(x)$ has an irreducible factor of degree $> m - k$ which is impossible. Alternatively, the slope of the right-most edge of the Newton polygon of $g(x)$ with respect to p is $< 1/(m-k) \le 1/k$ so that Lemma 3 applies with $\ell = k - 1$. For $j \in \{0, 1, 2, \ldots, m-1\}$ we deduce the inequality

$$2p > 2m \ge 2m - j > 0.$$

Hence, p itself is the only multiple of p among the numbers $2m - j$ with $0 \le j \le m - 1$. Since $c_0 = \pm(2m)(2m-1)\cdots(m+1)$ we obtain $\nu_p(c_0) = 1$.

CASE 2. $10^{30} \leq k < m^{2/3}$.

Let $z = (k/4)\log k$. We will show that there is a prime $p > z$ that divides $2m - j$ for some $j \in \{0, 1, 2, \ldots, k-1\}$. Then (7) follows as before. We consider $a_m = a_{m-1} = \cdots = a_0 = 1$ and obtain a contradiction to Lemma 3 by showing that the right-most edge of the Newton polygon of $g(x)$ with respect to p has slope $< 1/k$.

Let

$$T = \{2m - j \,:\, 0 \leq j \leq k-1\}.$$

Clearly, the elements of T are each $\geq m$. For each prime $p \leq z$, we consider an element $b_p = 2m - j \in T$ with $\nu_p(b_p)$ as large as possible. We let

$$S = T - \{b_p \,:\, p \leq z\}.$$

Note that for $k \geq 100$ we have $\log(1/4) + \log k + \log\log k \geq \log k$ from which it follows that

$$\frac{1.03}{\log(1/4) + \log k + \log\log k} \leq \frac{1.03}{\log k}$$

so that

$$\frac{1.03(k/4)\log k}{\log(1/4) + \log k + \log\log k} \leq \frac{(0.26k)\log k}{\log k} = 0.26k.$$

Since $k \geq 10^{30}$ and $z = (k/4)\log k$, we deduce from Lemma 1 that $\pi(z) < 1.03z/\log z$. It follows for $k \geq 10^{30}$ that

$$\pi(z) < \frac{1.03z}{\log z} \leq 0.26k < \frac{k}{3}. \tag{8}$$

We combine this estimate momentarily with $|S| \geq k - \pi(z)$. Since $k \leq m^{2/3}$, we deduce $m \geq k^{3/2}$. Consider a prime $p \leq z$ and let $r = \nu_p(b_p)$. By the definition of b_p, if $j > r$, then there are no multiples of p^j in T (and, hence, in S). For $1 \leq j \leq r$, there are $\leq [k/p^j] + 1$ multiples of p^j in T and, hence, at most $[k/p^j]$ multiples of p^j in S. Therefore,

$$\nu_p\biggl(\prod_{s\in S} s\biggr) \leq \sum_{j=1}^{r} \left[\frac{k}{p^j}\right] \leq \nu_p(k!),$$

and

$$\prod_{s\in S}\prod_{p\leq z} p^{\nu_p(s)} \leq k! \leq k^k.$$

On the other hand,

$$\prod_{s\in S} s \geq m^{|S|} \geq (k^{3/2})^{k-\pi(z)} = k^{1.5(k-\pi(z))}.$$

Claim. For $k \geq 10^{30}$ we have

$$k^{1.5(k-\pi(z))} > k^k.$$

To verfiy the claim it suffices to show that for $k \geq 10^{30}$ we have

$$1.5(k - \pi(z)) > k.$$

Observe that for $k \geq 10^{30}$ we have from (8)

$$\begin{aligned} 1.5\pi(z) < (1.5)(k/3) = k/2 &\implies k + 1.5\pi(z) < 1.5k \\ &\implies 1.5(k - \pi(z)) > k. \end{aligned}$$

The claim follows.

The above estimates now give

$$\prod_{s \in S} s > \prod_{s \in S} \prod_{p \leq z} p^{\nu_p(s)},$$

from which it follows that there is a prime $p > z$ that divides some element of S and, hence, divides some element of T. Fix a prime $p > z$ that divides an element $2m - \ell$ in T with $0 \leq \ell < k$, and let $\nu = \nu_p$. Since $k \geq 10^{30}$, we obtain $p > z > 5k$. The right-most edge of the Newton polygon of $g(x)$ with respect to p has slope as in (2). Fix $j \in \{1, 2, \ldots, m\}$ so that the quotient in (2) is maximal. To complete the case under consideration, we want to show that this quotient is $< 1/k$. Let L be an integer such that $p^{L+1} > m + j \geq p^L$. Then

$$\begin{aligned} \nu(c_0) - \nu(c_j) &= \nu(j!) + \nu\left(\frac{(m+j)!}{m!}\right) - \nu\left(\frac{m!}{(m-j)!}\right) \\ &= \nu\left(\frac{(m+j)!}{m!}\right) - \nu\left(\frac{m!}{j!(m-j)!}\right) \\ &= \nu\left(\frac{(m+j)!}{m!}\right) - \nu\left(\binom{m}{j}\right) \leq \nu\left(\frac{(m+j)!}{m!}\right) \\ &= \nu((m+1)(m+2)\cdots(m+j)) = \nu((m+j)!) - \nu(m!) \\ &= \sum_{\ell=1}^{\infty} \left(\left[\frac{m+j}{p^\ell}\right] - \left[\frac{m}{p^\ell}\right] \right) \leq \sum_{1 \leq \ell \leq L} \left(\frac{j}{p^\ell} + 1 \right) \\ &\leq \frac{j}{p-1} + L \leq \frac{j}{p-1} + \frac{\log(2m)}{\log p}. \end{aligned}$$

Thus, for each $j \in \{1, 2, \ldots, m\}$,

$$\nu(c_0) - \nu(c_j) \leq \nu((m+1)(m+2)\cdots(m+j)) \leq \frac{j}{p-1} + \frac{\log(2m)}{\log p}. \tag{9}$$

If p does not divide $(m+1)(m+2)\cdots(m+j)$, then $\nu((m+1)(m+2)\cdots(m+j)) = 0$ and our result follows. Thus, we suppose as we may that p divides $(m+i)$ for some $i \in \{1, 2, \ldots, j\}$. Further, since p divides $2m - \ell$, it follows that p divides $2i + \ell = 2(m+i) - (2m - \ell)$. This implies that $p \leq 2i + \ell \leq 2j + k - 1$. In other words, if $p > 2j + k - 1$, then

$$\nu((m+1)(m+2)\cdots(m+j)) = 0 \tag{10}$$

and our result follows. Thus, we assume that $p \leq 2j + k - 1$.

Initially, suppose that $j \leq 2k$. Then we deduce that

$$5k < p \leq 2j + k - 1 \leq 4k + k - 1 = 5k - 1$$

which is impossible.

Next, suppose that $j \geq \dfrac{2k\log(2m)}{\log k}$. Combining (9) with the fact that $p - 1 \geq 5k$ we obtain

$$\frac{\nu(c_0) - \nu(c_j)}{j} \leq \frac{1}{p-1} + \frac{\log(2m)}{j\log p} \leq \frac{1}{5k} + \frac{1}{2k} < \frac{1}{k},$$

which is what we desire.

Finally, it suffices for us to consider $2k + 1 \leq j < \dfrac{2k\log(2m)}{\log k}$. Recall that

$$\prod_{s\in S}\prod_{p\leq z} p^{\nu_p(s)} \leq k!.$$

Note that if $p > z \geq 5k$, then p divides at most one element of S. Therefore,

$$\prod_{s\in S}\prod_{\substack{p>z\\ p^{\nu_p(s)}\leq 2j+k-1}} p^{\nu_p(s)} \leq \prod_{z<p\leq 2j+k-1}(2j+k-1) \leq (2j+k-1)^{\pi(2j+k-1)}.$$

Combining these estimates and taking logarithms it follows that

$$\log\left(\prod_{s\in S}\prod_{p\leq z} p^{\nu_p(s)} \prod_{\substack{p>z\\ p^{\nu_p(s)}\leq 2j+k-1}} p^{\nu_p(s)}\right) \leq \log(k!) + \pi(2j+k-1)\log(2j+k-1). \tag{11}$$

Further, note that

$$\begin{aligned}\log(k!) &\leq (k+1)\log(k+1) - k \qquad (12)\\ &\leq (k+1)\log k + \frac{k+1}{k} - k = k\log k + \log k + 1 + \frac{1}{k} - k.\end{aligned}$$

Using Lemma 1, (11), (12), and $2k + 1 \leq j < \dfrac{2k\log(2m)}{\log k}$, we obtain

$$\begin{aligned}&\log\left(\prod_{s\in S}\prod_{p\leq z} p^{\nu_p(s)} \prod_{\substack{p>z\\ p^{\nu_p(s)}\leq 2j+k-1}} p^{\nu_p(s)}\right) \qquad (13)\\ &\leq (k+1)\log k + 1 + \frac{1}{k} - k + (2j+k-1) + \frac{3(2j+k-1)}{2\log k}\\ &\leq k\log k + 2j + \frac{3j}{\log k} + \frac{3k}{2\log k} + \log k\\ &\leq k\log k + \frac{4k\log(2m)}{\log k} + \frac{6k\log(2m)}{\log^2 k} + \frac{3k}{2\log k} + \log k\end{aligned}$$

$$\leq k\log k + \frac{4k\log m}{\log k} + \frac{6k\log m}{\log^2 k} + \frac{5k}{\log k} + \frac{5k}{\log^2 k} + \log k.$$

On the other hand, we have

$$\prod_{s\in S} s \geq m^{|S|} \geq m^{k-\pi(z)}.$$

Thus, taking logarithms and using (8) we obtain

$$\log\left(\prod_{s\in S} s\right) \geq (k-\pi(z))\log m \geq (k-0.26k)\log m = 0.74k\log m. \tag{14}$$

We claim that the estimate on the right-hand side of (14) is larger than the right-hand side of (13). Equivalently, we claim that

$$0.74\,k\log m > k\log k + \frac{4k\log m}{\log k} + \frac{6k\log m}{\log^2 k} + \frac{5k}{\log k} + \frac{5k}{\log^2 k} + \log k$$

is a true inequality. In other words, we claim

$$0.74\log m - \frac{4\log m}{\log k} - \log k - \frac{6\log m}{\log^2 k} > \frac{5}{\log k} + \frac{5}{\log^2 k} + \frac{\log k}{k}.$$

Using that $k \geq 10^{30}$, one easily deduces that the right-hand side above is < 0.1. Thus, it suffices to show that

$$0.74\log m - \frac{4\log m}{\log k} - \log k - \frac{6\log m}{\log^2 k} > 0.1. \tag{15}$$

To see this, note that as $k \leq m^{2/3}$ then

$$0.74\log m - \log k \geq 0.74\log m - (2/3)\log m > 0.07\log m.$$

Further, as $k \geq 10^{30}$, we have

$$\frac{4\log m}{\log k} + \frac{6\log m}{\log^2 k} \leq \frac{4\log m}{30\log 10} + \frac{6\log m}{900\log^2 10} \leq 0.06\log m.$$

Thus, since m is sufficiently large, it follows that

$$0.74\log m - \frac{4\log m}{\log k} - \log k - \frac{6\log m}{\log^2 k} > 0.01\log m > 0.1.$$

Hence,

$$\prod_{s\in S} s > \prod_{s\in S}\prod_{p\leq z} p^{\nu_p(s)} \prod_{\substack{p>z \\ p^{\nu_p(s)}\leq 2j+k-1}} p^{\nu_p(s)},$$

from which we deduce that there exists a prime $p > z$ which divides some $s \in S$ with $p^{\nu_p(s)} > 2j+k-1$. Fix such an s, and let ℓ now be such that $s = 2m-\ell$. Let r be an integer defined so that that $p^r > 2j+k-1 \geq p^{r-1}$ and such that p^r divides $2m-\ell$. Recall that $p \leq 2j+k-1$ so that $r \geq 2$. Note that $r - 1 \leq \log(2j + k - 1)/\log p$. Also, p^r does not divide $(m + i)$ for any $i \in \{1, 2, \ldots, j\}$ (for otherwise we deduce that $p^r \leq 2j + k - 1$). Hence, we have

$$\nu((m+1)(m+2)\cdots(m+j)) \leq \sum_{u=1}^{r-1} \left(\frac{j}{p^u} + 1\right) \leq \frac{j}{p-1} + r - 1. \tag{16}$$

We show next that

$$j > (5/4)k(r-1). \tag{17}$$

Since $r \geq 2$, we deduce

$$2(5k)^{r-1} \geq 2(5^{r-1})k \geq (5r-3)k$$

so that

$$4j + 2k - 2 \geq 2p^{r-1} \geq 2(5k)^{r-1} > 5kr - 3k - 2.$$

Hence, (17) easily follows. From (16) and (17), we obtain

$$\frac{\nu(c_0) - \nu(c_j)}{j} \leq \frac{1}{p-1} + \frac{r-1}{j} < \frac{1}{5k} + \frac{4}{5k} = \frac{1}{k},$$

which is what we desire.

CASE 3. $12 \leq k < 10^{30} = k_0$.

We will use Lemma 4 to prove the case under consideration. From Lemma 1,

$$\pi(3k) < \frac{3k}{\log(3k)}\left(1 + \frac{3}{2\log(3k)}\right) < k$$

for $k \geq 21$. Upon computation we see that $\pi(3k) < k$ for $12 \leq k \leq 20$. Using an argument as in Case 2, we briefly indicate why one of the numbers $2m, 2m-1, \ldots, 2m-k+1$, say $2m - \ell$, can be written as a product $s_1 s_2$ satisfying $s_1 \leq k! \leq k_0!$ and $\gcd(s_2, \prod_{p \leq 3k} p) = 1$. Take T as defined in Case 2 and S as well but with $z = 3k$. Then $\pi(3k) < k$ implies $|S| > 0$. Let ℓ be such that $2m - \ell \in S$ and note that

$$s_1 = \prod_{p \leq 3k} p^{\nu_p(2m-\ell)} \leq \prod_{s \in S} \prod_{p \leq 3k} p^{\nu_p(s)} \leq k!,$$

the last inequality following as in Case 2. Thus, we obtain $2m - \ell \in T$ as above. Note that $s_2 \geq c_1 2m$ for some constant c_1 (e.g., $c_1 = 1/(2 \times k_0!)$).

Since $g(x)$ has a factor of degree k, we obtain from Lemma 4 that for every prime power divisor p^r of s_2,

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

Since each such p is $\geq 3k + 1$, it follows that

$$\Delta(r,p)\frac{\log(2m)}{p^r \log p} > \frac{2}{3k} \geq \frac{1}{2k_0}.$$

Thus,

$$p^r < \frac{c_2 \log(2m)}{\log p}$$

where $c_2 = 6k_0$. From this we deduce that

$$p < \frac{2c_2 \log(2m)}{\log\log(2m)} \qquad \text{and} \qquad r < \frac{2\log\log(2m)}{\log p}.$$

These lead to a contradiction since m is sufficiently large,

$$\begin{aligned}\log s_2 = \sum_{p^r \| s_2} r \log p &\le \sum_{p < 2c_2 \log(2m)/\log\log(2m)} \frac{2\log\log(2m)}{\log p} \log p \\ &\le \frac{5c_2 \log(2m)}{\log\log(2m)} < \log(2c_1 m) \le \log s_2.\end{aligned}$$

Thus, $g(x)$ cannot have a factor of degree $k \in [12, k_0)$.

CASE 4. $4 \le k \le 11$.

Again we use Lemma 4 to settle the case under consideration. Observe that

$$c_{m-k} = a_{m-k} \frac{1}{k!} m(m-1)\cdots(m-k+1)(2m)(2m-1)\cdots(2m-k+1). \tag{18}$$

Define $d(k)$ to be the number of distinct irreducible linear factors in m in the coefficient c_{m-k} of $g(x)$. For example, if $k = 4$, then there are 6 distinct irreducible linear factors appearing in (18), namely m, $m-1$, $m-2$, $m-3$, $2m-1$, and $2m-3$. In general, $d(k) = k + [k/2]$. By a simple computation we obtain the following table.

k	3	4	5	6	7	8	9	10	11
$d(k)$	4	6	7	9	10	12	13	15	16
$\pi(3k)$	4	5	6	7	8	9	9	10	11

Using the table above we deduce that $\pi(3k) < d(k)$ for $4 \le k \le 11$. Using an argument as in Case 3, we get that one of the numbers $m, m-1, \ldots, m-k+1$, $2m, 2m-1, \ldots, 2m-k+1$ in the coefficient of c_{m-k} can be written as a product $s_1 s_2$ satisfying $s_1 \le k! \le 2^3 \times 3^2 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19$ and $\gcd(s_2, \prod_{p \le 3k} p) = 1$. We obtain that $s_2 \ge c_1 2m$ for some constant c_1. Assuming $g(x)$ has a factor of degree k, we obtain from Lemma 4 that for every prime power divisor p^r of s_2,

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

We are led to a contradiction by repeating the argument at the end of Case 4. Thus, $g(x)$ cannot have a factor of degree $k \in [4, 11]$.

CASE 5. $k = 3$.

Consider primes dividing $m, m-1$, and $m-2$. Take away at most two of these numbers which are divisible by the highest powers of 2 and 3 (one of these numbers could be divisible by the highest power of 2 and the highest power of 3) so that there is at least one number of the form $s_1 s_2$ where $s_1 \in \{1, 2\}$ and $\gcd(6, s_2) = 1$. Note that for $m \ge 6$ we have $s_2 \ge (m-2)/s_1 \ge (m-2)/2 \ge m/3$. Write $s_2 = 5^u \times 7^v \times s_3$ where $\gcd(35, s_3) = 1$. We claim that we may assume that $5^u < m^{1/3}$ and $7^v < m^{1/3}$ since m is sufficiently large. To see this, suppose that $5^u \geq m^{1/3}$. Then $u \geq 2$. Further, taking $k = 3$ and $p = 5$ we have $p \geq \max\{k+2, 2k-1\}$. Finally, since $5^u \geq m^{1/3}$ then $5^{u/2} \geq m^{1/6}$ and we have

$$\frac{\log(2m)}{5^{u/2}\log 5} + \frac{1}{5-1} \leq \frac{\log(2m)}{m^{1/6}\log 5} + \frac{1}{4} \leq \frac{1}{3}.$$

Thus, using $p = 5$, $r = u$, and $k = 3$ in Lemma 5 we deduce that $g(x)$ cannot have a factor of degree 3. Hence, we may assume that $5^u < m^{1/3}$.

A similar argument allows us to assume that $7^v < m^{1/3}$. Hence, we have $m/3 \leq s_2 = 5^u \times 7^v \times s_3 < m^{2/3}s_3$ so that $s_3 > m^{1/3}/3$.

We argue again in a manner similar to that given in Case 3. Assuming $g(x)$ has a factor of degree $k = 3$ we obtain from Lemma 4 that for every prime divisor p^r of s_3

$$\Delta(r,p)\frac{\log(2m)}{p^r \log p} + \frac{1}{p-1} > \frac{1}{3}.$$

Since each such p is at least $11 > 10 = 3k+1$, it follows that

$$\Delta(r,p)\frac{\log(2m)}{p^r \log p} > \frac{1}{3} - \frac{1}{p-1} > \frac{1}{3} - \frac{1}{9} = \frac{2}{9} > \frac{1}{6}.$$

Thus,

$$p^r < 6\Delta(r,p)\frac{\log(2m)}{\log p} < 18\frac{\log(2m)}{\log p}.$$

From this we deduce that

$$p < \frac{36\log(2m)}{\log\log(2m)} \qquad \text{and} \qquad r < \frac{2\log\log(2m)}{\log p}.$$

These lead to a contradiction since

$$\begin{aligned}\log s_3 = \sum_{p^r || s_3} r\log p &\leq \sum_{p < 36\log(2m)/\log\log(2m)} \frac{2\log\log(2m)}{\log p}\log p \\ &\leq \frac{80\log(2m)}{\log\log(2m)} < \log\left(\frac{m^{1/3}}{3}\right) < \log s_3.\end{aligned}$$

Thus, $g(x)$ cannot have a factor of degree $k = 3$.

CASE 6. $k = 2$.

In this case we use Lemma 2 to deduce that since m is sufficiently large $g(x)$ has no factor of degree 2. Taking $N = 30$ and $\epsilon = 1/2$ in Lemma 2 we deduce that there exists an integer M such that for $m \geq M$ the largest divisor of $m(m-1)$ which is relatively prime to 30 is $\geq m^{1/2}$. Hence, we can write $m(m-1) = s_1 s_2$ where $\gcd(30, s_2) = 1$ and $s_2 \geq m^{1/2}$ and such that if p^r divides s_2 then $p \geq 7$.

We argue again in a manner similar to that given in Case 3. Suppose $g(x)$ has a factor of degree $k = 2$. Note that every prime divisor p^r of s_2 is at least $7 = 3 \times 2 + 1 = 3k + 1$. Also, every prime divisor p^r of s_2 divides one of m and $m-1$. Thus, we obtain from Lemma 4 that for every prime divisor p^r of s_2,

$$\Delta(r,p)\frac{\log(2m)}{p^r\log p}+\frac{1}{p-1}>\frac{1}{2}.$$

The argument proceeds as before, obtaining a contradiction by considering the size of $\log s_2$. Thus, $g(x)$ cannot have a factor of degree $k=2$.

CASE 7. $k=1$.

We know now that there is an m_0' such that if $m\geq m_0'$ and $f(x)$ is as defined in Theorem 2, then $f(x)$ cannot have a factor of degree $k\in[2,m/2]$. We suppose in this section that m_0 is sufficiently large and, in particular, that $m_0\geq m_0'$. Write $m=2^i\times 3^j\times n$ where $\gcd(6,n)=1$ with $m\geq m_0$. Suppose that n satisfies

$$n\geq\exp\left(\frac{8\log(2m)}{\log\log(2m)}\right). \tag{19}$$

Since $g(x)$ has a factor of degree $k=1$ we obtain from Lemma 4 that, for every prime divisor p^r of n,

$$\Delta(r,p)\frac{\log(2m)}{p^r\log p}+\frac{1}{p-1}>1.$$

Since each such p is at least $5>4=3k+1$, it follows that

$$\Delta(r,p)\frac{\log(2m)}{p^r\log p}>1-\frac{1}{p-1}\geq 1-\frac{1}{3}=\frac{2}{3}\geq\frac{1}{2}.$$

Thus,

$$p^r<\frac{3}{2}\Delta(r,p)\frac{\log(2m)}{\log p}<\frac{9\log(2m)}{2\log p}.$$

From this we deduce that

$$p<\frac{5\log(2m)}{\log\log(2m)}\qquad\text{and}\qquad r<\frac{3\log\log(2m)}{2\log p}.$$

These lead to a contradiction since m sufficiently large implies

$$\begin{aligned}\log n=\sum_{p^r||n}r\log p&\leq\sum_{p<5\log(2m)/\log\log(2m)}\frac{3\log\log(2m)}{2\log p}\log p\\&<\frac{8\log(2m)}{\log\log(2m)}\leq\log n.\end{aligned}$$

Thus, $g(x)$ cannot have a factor of degree $k=1$.

On the other hand, if m is written as above with $m\geq m_0$ and n does not satisfy (19) and $g(x)$ has a linear factor, then we claim that $g(x)$ has an irreducible factor of degree $m-1$. Write $g(x)=u(x)v(x)$ where $u(x)\in\mathbb{Z}[x]$, $v(x)\in\mathbb{Z}[x]$, $\deg(u(x))=1$, and $\deg(v(x))=m-1$. Suppose that $v(x)$ is reducible. Then $v(x)$ has a factor $r(x)\in\mathbb{Z}[x]$ with $1\leq\deg(r(x))\leq(m-1)/2$. This implies that $r(x)u(x)$ is a factor of $g(x)$ with degree in $[2,(m+1)/2]$. Since

$m \geq m_0 \geq m_0'$, we know that $g(x)$ cannot have a factor of degree $k \in [2, m/2]$. Thus, $r(x)u(x)$ must have degree $(m+1)/2$ and $v(x)/r(x)$ is a factor of $g(x)$ of degree $(m-1)/2$. We are through unless $(m-1)/2 = 1$ (otherwise $g(x)$ has a factor of degree $k \in [2, m/2]$). In this case $m = 3$ and $g(x)$ has three linear factors. Since $m \geq m_0$ and m_0 is sufficiently large, this case need not be considered. Hence, the claim follows.

Finally, we estimate $A(t)$, the number of elements of A which are $\leq t$. Suppose that $m \in A$ and $m_0 \leq m \leq t$. Then $m = 2^i \times 3^j \times n$ where n satisfies the inequality in Theorem 2. Thus, $2^i \leq m \leq t$ so that $i \leq (\log t)/(\log 2)$. Similarly, we have $j \leq (\log t)/(\log 3)$. Hence,

$$A(t) \ll m_0 + (\log t)^2 \exp\left(\frac{8\log(2t)}{\log\log(2t)}\right) \ll \exp\left(\frac{9\log(2t)}{\log\log(2t)}\right).$$

This completes the proof of Theorem 2.

5 An Infinite Set of Reducible Examples

In this section, we establish that the set A of Theorem 2 is infinite. In fact, our argument is easily modified to give $A(t) \gg \log t$.

Recall the generalized Laguerre polynomial with $\alpha = m$ is of the form $h(x) = m! L_m^{(m)}(x) = \sum_{j=0}^m b_j x^j \in \mathbb{Z}[x]$ where

$$b_j = \binom{m}{j}(2m)(2m-1)\cdots(m+j+1) \qquad \text{for } 0 \leq j \leq m.$$

For each $0 \leq j \leq m$ note that

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

Furthermore, note that $g(x) = \sum_{j=0}^m c_j = \sum_{j=0}^m a_j b_j$ where the b_j's are defined as above.

Let $m = 3 \cdot 2^k = (2+1) \cdot 2^k = 2^{k+1} + 2^k$ where k is a positive integer with $k \equiv 3$ or $15 \pmod{18}$. Observe that the spots of the polynomial $h(x)$ are of the form $(m-j, \nu_p(b_j))$ where $j \in \{0, 1, \ldots, m\}$. Suppose $p = 2$ and consider the values of $\nu_2(b_{2^k})$ and $\nu_2(b_0)$. Taking $j = 2^k$ we have from above that

$$b_{2^k} = \binom{2^{k+1} + 2^k}{2^k}\binom{2^{k+2} + 2^{k+1}}{2^{k+1}} 2^{k+1}!.$$

Lemma 7 implies that $\nu_2((2^{k+2} + 2^{k+1})!) = 2^{k+2} + 2^{k+1} - 2$, $\nu_2((2^{k+1} + 2^k)!) = 2^{k+1} + 2^k - 2$, $\nu_2(2^{k+1}!) = 2^{k+1} - 1$, and $\nu_2(2^k!) = 2^k - 1$. Therefore, we have

$$\begin{aligned} \nu_2(b_{2^k}) = &\left[\nu_2((2^{k+1} + 2^k)!) - \nu_2(2^k!) - \nu(2^{k+1}!)\right] \\ &\quad + \left[\nu_2((2^{k+2} + 2^{k+1})!) - \nu_2(2^{k+1}!) - \nu(2^{k+2}!)\right] + \nu(2^{k+1}!) \\ \\ &= 0 + 0 + 2^{k+1} - 1 = 2^{k+1} - 1. \end{aligned}$$

Thus, if $j = 2^k$ we have the spot $(m - j, \nu_2(b_j)) = (2^{k+1}, 2^{k+1} - 1)$. Also,

$$b_0 = \binom{m}{0}\binom{2m}{m}m! = 1 \cdot \frac{(2m)!}{m!} = \frac{(2^{k+2} + 2^{k+1})!}{(2^{k+1} + 2^k)!}.$$

Hence, we have

$$\begin{aligned}
\nu_2(b_0) &= \nu_2((2^{k+2} + 2^{k+1})!) - \nu_2((2^{k+1} + 2^k)!) \\
&= (2^{k+2} + 2^{k+1} - 2) - (2^{k+1} + 2^k - 2) \\
&= 2^{k+2} - 2^k = 2^k \cdot 3 = m.
\end{aligned}$$

Thus, if $j = 0$ we have the spot $(m - j, \nu_2(b_j)) = (m, m)$.

Consider the integers

$$A = 6^3 \cdot b_3, \;\; B = 2 \cdot 6^{2^k} \cdot b_{2^k}, \;\; C = 2m^2 \cdot 6^{m-1}, \;\text{ and }\; D = 6^m + b_0.$$

Observe that 2^m exactly divides 6^m and b_0 so that $\nu_2(D) \geq m+1$. Also, $\nu_2(B) = \nu_2(2) + \nu_2(6^{2^k}) + \nu_2(b_{2^k}) = 1 + 2^k + 2^{k+1} - 1 = m$. Thus, $\nu_2(D) > \nu_2(B) = m$.

Next, let $s = \nu_3(b_0)$ and observe that

$$s = \nu_3\left(\frac{(2m)!}{m!}\right) < \nu_3((2m)!) = \sum_{j=1}^{\infty}\left[\frac{2m}{3^j}\right] \leq (2m)\sum_{j=1}^{\infty}\frac{1}{3^j} = (2m)(1/2) = m.$$

Thus, $\nu_3(D) = \min\{\nu_3(6^m), \nu_3(b_0)\} = \min\{m, s\} = s$. Further, $\nu_3(A) = \nu_3(6^3) + \nu_3(b_3) = 3 + \nu_3(b_3)$. We claim that as $k \equiv 3$ or $15 \pmod{18}$ then

$$\nu_3(b_3) = \nu_3(b_0) - 3.$$

To see this observe that

$$\begin{aligned}
b_3 &= \binom{m}{3}\binom{2m}{m-3}(m-3)! \\
&= \frac{m(m-1)(m-2)}{6} \cdot (2m)(2m-1)\cdots(m+4) \\
&= \frac{m(m-1)(m-2)}{6(m+1)(m+2)(m+3)}(2m)(2m-1)\cdots(m+1) \\
&= \frac{m(m-1)(m-2)}{6(m+1)(m+2)(m+3)}b_0.
\end{aligned}$$

Thus, in order to justify the claim it suffices to show that if $k \equiv 3$ or $15 \pmod{18}$ then

$$\nu_3\left(\frac{m(m-1)(m-2)}{6(m+1)(m+2)(m+3)}\right) = -3.$$

Observe that exactly one of m, $m-1$, and $m-2$ is divisible by 3. Moreover, as $m = 3 \cdot 2^k$ it follows that $\nu_3(m) = 1$, $\nu_3(m-1) = 0$, and $\nu_3(m-2) = 0$. Similarly, exactly one of $m+1$, $m+2$, and $m+3$ is divisible by 3. Further, as $k \equiv 3$ or $15 \pmod{18}$ Lemma 8 implies that

$3^2||2^k+1$. As $m+3 = 3\cdot 2^k + 3 = 3\cdot(2^k+1)$ we see that $\nu_3(m+3) = 1+2 = 3$, and $\nu_3(m+1) = \nu_3(m+2) = 0$. Therefore, we have

$$\begin{aligned}\nu_3(b_3) &= \nu_3(b_0) + \nu_3(m) + \nu_3(m-1) + \nu_3(m-2)\\ &\qquad - \nu_3(6) - \nu_3(m+1) - \nu_3(m+2) - \nu_3(m+3)\\ &= \nu_3(b_0) + 1 + 0 + 0 - 1 + 0 + 0 - 3 = \nu_3(b_0) - 3.\end{aligned}$$

The claim follows and we have $\nu_3(A) = 3 + \nu_3(b_3) = 3 + \nu_3(b_0) - 3 = \nu_3(b_0) = s$. Hence, we have $\nu_3(D) = \nu_3(A) = s$.

Also, $\nu_2(C) = \nu_2(2m^2 \cdot 6^{m-1}) = \nu_2(2\cdot 6^{m-1}) + \nu_2(m^2) = m + 2k > m$. Also, $\nu_3(C) = 0 + 2 + (m-1) = m+1 > m$. Therefore, $\gcd(A,B,C) = 2^i 3^j$ with $1 \leq i \leq m$ and $1 \leq j \leq s$. We deduce that $\gcd(A,B,C) > 1$ and $\gcd(A,B,C)|D$. It follows that there exists integers u, v, and t such that $Au + Bv + Ct = -D$.

Finally, we construct a reducible $g(x)$ by taking $a_m = a_0 = 1$, $a_3 = u$, $a_{2^k} = 2v$, $a_{m-1} = t$, and $a_j = 0$ for $j \notin \{0, 3, 2^k, m-1, m\}$. Thus, we have

$$g(x) = x^m + 2m^2 t x^{m-1} + 2v b_{2^k} x^{2^k} + u b_3 x^3 + b_0.$$

Observe that

$$\begin{aligned}g(6) &= 6^m + 2m^2 t \cdot 6^{m-1} + 2v b_{2^k} 6^{2^k} + u b_3 6^3 + b_0\\ &= 6^m + Ct + Bv + Au + b_0\\ &= D + Ct + Bv + Au = 0.\end{aligned}$$

Thus, $g(x)$ has a linear factor, namely, $x - 6$. The fact that A is infinite follows from the fact that there are infinitely many distinct degrees m which produce a reducible polynomial for some choice of the integers a_j.

References

[1] G. Bachman, *Introduction to p-adic numbers and valuation theory*, Academic Press, New York-London, 1964.

[2] M. G. Dumas, *Sur quelques cas d'irréducibilité des polynomes à coefficients rationnels*, J. Math. Pures Appl., **2** (1906), 191–258.

[3] M. Filaseta, *The irreduciblity of all but finitely many Bessel polynomials*, Acta Math. **174** (1995), 383–397.

[4] M. Filaseta, *A generalization of an irreduciblity theorem of I. Schur*, Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam, Vol. 1 (edited by B. Berndt, H. Diamond, and A. Hilderbrand), Birkhäuser, Boston (1996), 371–396.

[5] M. Filaseta and T.-Y. Lam, *On the irreducibility of the generalized Laguerre polynomials*, preprint.

[6] M. Filaseta and O. Trifinov, *The irreduciblity of the Bessel polynomials*, preprint.

[7] R. Gow, *Some generalized Laguerre polynomials whose Galois groups are the alternating groups*, Journal of Number Theory, **31** (1989), 201–207.

[8] M. N. Huxley, *On the difference between consecutive primes*, Invent. Math., **15** (1972), 164–170.

[9] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Math., **6** (1962), 64–89.

[10] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse **14** (1929), 125–136.

[11] I. Schur, *Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome*, Journal für die reine und angewandte Mathematik **165** (1931), 52–58.

[12] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. **43** (1936), 133–147.