T. N. Shorey's Influence in the Theory of Irreducible Polynomials

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

Carrie Finch
Mathematics Department
University of South Carolina
Columbia, SC 29208

J Russell Leidy
Mathematics Department
University of South Carolina
Columbia, SC 29208

Dedicated to Tarlok N. Shorey and his continuing contributions to Number Theory

1 Introduction

The idea of looking at the prime factorization of the coefficients of a polynomial in $\mathbb{Z}[x]$ in order to establish its irreducibility (over $\mathbb{Q}$) goes back to the classical Schönemann-Eisenstein criterion first derived in [29] and [6] in the middle of the 19th century. At the beginning of the 20th century, G. Dumas [5], again making use of primes that divide the coefficients of a polynomial, introduced the idea of using Newton polygons which allowed for variations and strengthening of the Schönemann-Eisenstein criterion. In a series of papers, I. Schur [30, 31, 32, 33] obtained irreducibility results for polynomials $f(x)$ associated with generalized Laguerre polynomials

$$L_m^{(\alpha)}(x) = \sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)}{(m-j)!j!}(-x)^j,$$

where m is a positive integer and α is an arbitrary real number. In particular, Schur established the explicit result that for $\alpha = 0$ or 1, the polynomial $L_m^{(\alpha)}(x)$ is irreducible for all positive integers m. Working in the ring of algebraic integers in $\mathbb{Q}(\gamma)$ where γ is a root of $f(x)$, Schur obtained his results by looking at the prime ideal factorizations of the principal ideals generated by each coefficient of $f(x)$. Later, work of Coleman [4] and the first author

2000 Mathematics Subject Classification: 11R09 (11C08, 33C45)

The authors express their appreciation to the National Security Agency for support during the research for this paper.

[9] showed that Schur's results could be established directly from the use of the main Newton polygon result of Dumas.

In the next section, we will give an expository account of how Newton polygons have been used to establish irreducibility results for the generalized Laguerre polynomials and discuss various results that have been obtained. We will see that this approach makes heavy use of knowledge about the largest prime factor of the product

$$\Delta(m,k) = m(m+1)\cdots(m+k-1),$$

where m and k denote positive integers. Observe that $\Delta(m,k)$ is simply the product of the k consecutive integers beginning with m. For a positive integer n, we let $P(n)$ denote the largest prime divisor of n. Thus, we will make a connection between the irreducibility of Laguerre polynomials and the value of $P\big(\Delta(m,k)\big)$. T. N. Shorey's contribution to this latter subject is extensive. Some of the first author's early work on irreducibility was in fact motivated by Shorey's paper [35]. We note also that Shorey's joint work with R. Tijdeman [36, 37, 38, 39] constitutes important research in this direction that still has not been completely utilized for irreducibility results obtainable by these methods.

As we will see, obtaining *explicit* results for the irreducibility of generalized Laguerre polynomials using the methods described here depend on having *explicit* estimates also for $P\big(\Delta(m,k)\big)$. In the third section of this paper, we illustrate this by an application of the following recent result due to S. Laishram and T. N. Shorey [22].

Theorem 1.1 *For m and k positive integers,*

$$P(\Delta(m,k)) > 1.8k \quad \text{for } m > k > 2$$

unless $(m,k) \in B$, where

$$\begin{aligned} B =& \{(8,3),(5,4),(6,4),(7,4),(14,13),(15,13),(16,13)\} \\ & \cup \big\{(j+1,j) : j \in \{3,5,8,11,14,18,63\}\big\}. \end{aligned}$$

In particular, we use Theorem 1.1 to show for the first time the following explicit result that generalizes the irreducibility theorems of Schur's mentioned above.

Theorem 1.2 *Let m and α be integers with $m \geq 1$ and $0 \leq \alpha \leq 10$. Then $L_m^{(\alpha)}(x)$ is irreducible unless (m,α) is one of the pairs $(2,2)$, $(4,5)$, and $(2,7)$.*

For each of the three pairs in the theorem, $x-6$ is a factor of the polynomial $L_m^{(\alpha)}(x)$. This does not continue to hold for larger values of α with $L_m^{(\alpha)}(x)$ reducible. In particular, it is easy to check that $L_2^{(\alpha)}(x)$ with $\alpha \in \mathbb{Q}$ is reducible if and only if $\alpha+2$ is a square in $\mathbb{Q}$. Indeed, the roots of $L_2^{(\alpha)}(x)$ are precisely $\alpha+2 \pm \sqrt{\alpha+2}$.

The choice to restrict to $\alpha \in \{0,1,\ldots,10\}$ in Theorem 1.2 is somewhat arbitrary. The goal here is mainly to illustrate how Theorem 1.1 and similar results can be used to obtain effective theorems on the irreducibility of classes of generalized Laguerre polynomials. It would not be difficult to extend these computations further to other values of α and even to consider rational values of α with these same methods.

Our application of Theorem 1.1 to obtain Theorem 1.2 will allow us to go further. For m a positive integer, set

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha) \qquad \text{for } 0 \le j \le m,$$

and let

$$f(x) = \sum_{j=0}^{m} a_j b_j x^j,$$

where the a_j's are arbitrary integers with $|a_0| = |a_m| = 1$. We consider as usual an empty product to be 1 so that the above definition implies $b_m = 1$. Observe that if $a_j = (-1)^j$, then $f(x) = m!L_m^{(\alpha)}(x)$ and, hence, the irreducibility of $f(x)$ for arbitrary a_j as above implies the irreducibility of $L_m^{(\alpha)}(x)$. Our approach will be able to address the irreducibility of these more general polynomials $f(x)$.

Theorem 1.3 *Let m and α be integers with $m \ge 1$ and $0 \le \alpha \le 10$. Let $f(x)$ be as above with arbitrary integers a_j satisfying $|a_0| = |a_m| = 1$. If $f(x)$ is reducible for some such choice of a_j, then (m, α) must be as listed in Table 1 below and $f(x)$ is the product*

m	α	Linear Factors
2	2	$x \pm 2,\ \ x \pm 6$
2	7	$x \pm 6,\ \ x \pm 12$
4	4	$x \pm 2,\ \ x \pm 10$
4	5	$x \pm 6$
8	8	$x \pm 2,\ \ x \pm 6,\ \ x \pm 18$
24	8	$x \pm 6$

Table 1

of a linear polynomial from the corresponding last column of the table and an irreducible polynomial of degree $m-1$. Furthermore, for each possibility for m and α as listed in Table 1 and each prescribed linear factor given in the corresponding last column of this table, there exist integers a_j with $|a_0| = |a_m| = 1$ such that $f(x)$ is reducible and has the prescribed factor.

To illustrate this result, consider $m = 8$ and $\alpha = 8$. The choice

$$a_8 = 1, \quad a_7 = -24634, \quad a_1 = 1, \quad a_0 = -1,$$

and $a_j = 0$ for $2 \le j \le 6$ shows that $f(x)$ can have the linear factor $x - 2$. The choice

$$a_8 = 1, \quad a_7 = -23852, \quad a_1 = 309, \quad a_0 = -1,$$

and $a_j = 0$ otherwise shows that $f(x)$ can have the linear factor $x - 6$. The choice

$$a_8 = 1, \quad a_7 = -21506, \quad a_1 = 202981, \quad a_0 = -1,$$

and $a_j = 0$ otherwise shows that $f(x)$ can have the linear factor $x - 18$. One can replace x with $-x$ in these examples to obtain the linear factors $x + 2$, $x + 6$ and $x + 18$, respectively.

The last column in our table will rely on constructing specific examples of this nature. Most of the argument for establishing Theorem 1.3 will be given in the third section as part of our argument for Theorem 1.2. We address the final details of the proof of Theorem 1.3 in the fourth and final section of the paper.

Note that Theorem 1.3 can be used to elaborate on the choices of a_j which lead to reducible $f(x)$. For example, in the case that $\alpha = 2$, arbitrary positive integers m and variable a_j as in the theorem, it is a simple matter to deduce that $f(x)$ is in fact irreducible unless $f(x) = \pm L_2^{(2)}(\pm x)$.

Our approach will suggest a further investigation that can be made. Most of the arguments will not make use of the factor $\binom{m}{j}$ in the definition of b_j. By removing this factor in b_j and rewriting $f(x)$, we can obtain information about the factorization of

$$a_m \frac{x^m}{(m+\alpha)!} + a_{m-1}\frac{x^{m-1}}{(m-1+\alpha)!} + \cdots + a_1 \frac{x}{(1+\alpha)!} + a_0 \frac{1}{\alpha!},$$

where $\alpha \in \{0, 1, \ldots, 10\}$ and the a_j's are arbitrary integers with $|a_0| = |a_m| = 1$. This in fact is emphasized by our demonstration of Theorem 2.2 in the next section. These polynomials are more general than the ones considered in Theorem 1.3, so a result similar to Theorem 1.3 for these polynomials would be of interest. On the other hand, linear factors (and not prescribed higher degree factors) can occur with m arbitrarily large; indeed, this has already been demonstrated for $\alpha = 1$ (see [31] and [1]).

2 The General Setting

If p is a prime and n is a nonzero integer, we define $\nu(n) = \nu_p(n)$ to be the nonnegative integer such that $p^{\nu(n)} \mid n$ and $p^{\nu(n)+1} \nmid n$. We define $\nu(0) = +\infty$. Consider $w(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{Z}[x]$ with $a_m a_0 \neq 0$ and let p be a prime. Let S be the following set of points in the extended plane:

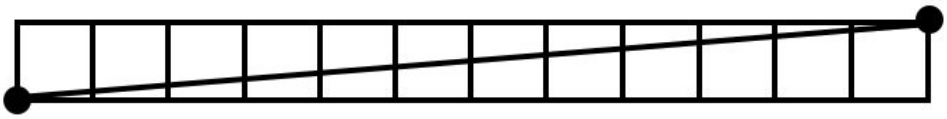
$$S = \{(0, \nu(a_m)), (1, \nu(a_{m-1})), (2, \nu(a_{m-2})), \ldots, (m-1, \nu(a_1)), (m, \nu(a_0))\}.$$

Consider the lower edges along the convex hull of these points. The left-most endpoint is $(0, \nu(a_m))$ and the right-most endpoint is $(m, \nu(a_0))$. The endpoints of each edge belong to S, and the slopes of the edges increase from left to right. When referring to the "edges" of a Newton polygon, we shall not allow two different edges to have the same slope. The polygonal path formed by these edges is called the Newton polygon of $w(x)$ with respect to the prime p.

The following result of G. Dumas [5] goes back to 1906.

Lemma 2.1 *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let t be a non-negative integer such that p^t divides the leading coefficient of $g(x)h(x)$ but p^{t+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 $(0, t)$ and using translates of the edges in the Newton polygon for $g(x)$ and $h(x)$ with respect to the prime p (using exactly one translate for each edge). Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.*

Observe that if $w(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{Z}[x]$ and p is a prime satisfying the three conditions $p \mid a_j$ for $0 \leq j \leq m-1$, $p^2 \nmid a_0$ and $p \nmid a_m$, then the Newton polygon of $w(x)$ with



Newton polygon of $w(x)$ with $m = 12$

respect to p consists of one edge with endpoints $(0,0)$ and $(m,1)$. Lemma 2.1 immediately implies that $w(x)$ is irreducible. Hence, Lemma 2.1 can be viewed as a generalization of the Schönemann-Eisenstein criterion. To see that Lemma 2.1 quite easily implies a result more general than the Schönemann-Eisenstein criterion, we leave the following as an exercise.

Example Let $w(x) = \sum_{j=0}^{m} a_j x^j \in \mathbb{Z}[x]$, and let p be a prime.

(a) Let k be an integer relatively prime to m. If $p \nmid a_m$, $p^k | a_j$ for $j \in \{0, 1, \ldots, m-1\}$, and $p^{k+1} \nmid a_0$, then $w(x)$ is irreducible.

(b) Let k be such that $p^k \| a_0$. Suppose that $p \nmid a_m$ and that for each $j \in \{1, 2, \ldots, m-1\}$ we have $p^{e(j)} | a_j$ for some positive integer $e(j)$ satisfying $me(j) + kj \geq km$. Then $w(x)$ factors in $\mathbb{Q}[x]$ as a product of irreducible polynomials each with degree a multiple of $m/\gcd(m,k)$.

Our main interest in this paper is to elaborate on the use of Theorem 1.1 and Lemma 2.1 for determining irreducibility results for the classical Laguerre polynomials defined in the introduction. There were also early applications of Lemma 2.1 to classical polynomials that were directed at the still open problem of establishing the irreducibility of the Legendre polynomials. Such work was done by J. H. Wahab [43, 44] and then R. F. McCoart [25].

We summarize in Table 2 below the known results concerning the irreducibility of all but finitely many or all Laguerre polynomials for various α. We note, though, in some cases, prior work was done establishing the irreducibility for a smaller class of polynomials. In particular, the case $\alpha = -2m - 1$ corresponds to the classical Bessel polynomials and several early irreducibility results for these polynomials can be found in E. Grosswald's work (cf. [17]). Though Dumas's work existed at the time, I. Schur [30, 33] did not make use of Lemma 2.1. His results, as well as many of the subsequent results in the table, involve more general polynomials. The result of R. F. Coleman [4] is indicated in the table in part as it is the first occurrence of a result for all m that involves the use of Lemma 2.1. Later, the first author [9] generalized the use of Lemma 2.1, showing for the first time that the full strength of I. Schur's results related to $\alpha = -m - 1$ can be obtained using Lemma 2.1; in fact a more general irreducibility result is given in [9]. The results in the table establishing irreducibility for all but finitely many m are effective; that is, in theory for a fixed α as in the first column, the specific m for which $L_m^{(\alpha)}(x)$ are reducible can be computed. Such a computation is typically not practical. No date is indicated in the latter results since, as of this writing, they have not appeared in print. Finally, we note that the main new result in this paper, that is the case where $\alpha \in \{2, 3, \ldots, 10\}$, is not tabulated in Table 2.

α	reducible $L_m^{(\alpha)}(x)$	Discoverer	Year
0	none	I. Schur [30]	1929
$-m-1$	none	I. Schur [30]	1929
1	none	I. Schur [33]	1931
$-m-1$	none	R. F. Coleman [4] (new proof)	1987
$-2m-1$	finitely many	M. Filaseta [10]	1995
$-m-2$	none	F. Hajir [18]	1995
$-2m-1$	none	M. Filaseta and O. Trifonov [12]	2002
fixed $\alpha \in \mathbb{Q}\backslash\mathbb{Z}^-$	finitely many	M. Filaseta and T. Y. Lam [11]	2002
$-m-3$	none	E. A. Sell [34]	2004
$-m-r$, $r=4,5,\ldots,9$	none	F. Hajir [20]	—
$-m-r$, fixed r	finitely many	F. Hajir [20]	—
m	$m=2$ only	M. Filaseta, T. Kidd, O. Trifonov	—

Table 2

To illustrate the approach and establish some preliminary results, we give here a proof of the following result of I. Schur [30].

Theorem 2.2 *Let m be a positive integer, and let $a_0, a_1, \ldots, a_m$ denote arbitrary integers with $|a_0| = |a_m| = 1$. Then*

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

is irreducible over the rationals.

The above result is the main result of I. Schur in [30]. If one takes $a_j = (-1)^j\binom{m}{j}$ in Theorem 2.2, then we deduce that $L_m^{(0)}(x)$, the classical Laguerre polynomials, are irreducible, which corresponds to the first entry in Table 2. If one takes $a_j = 1$ for each j in Theorem 2.2, then one gets a truncated Maclaurin series for e^x. This corresponds to the value of $(-1)^m L_m^{(-m-1)}(x)$ and, hence, the second entry in Table 2. The argument for Theorem 2.2 that we are about to give is based on a proof by the first author in [10]. It makes use of the following consequence of Lemma 2.1.

Lemma 2.3 *Let k be a positive integer. Suppose $v(x) = \sum_{j=0}^m c_j x^j \in \mathbb{Z}[x]$ and p is a prime such that $p \nmid c_m$, $p|c_j$ for all $j \in \{0,1,\ldots,m-k\}$, and the right-most edge of the Newton polygon for $v(x)$ 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 $u(x) = \sum_{j=0}^m a_j c_j x^j$ cannot have a factor in $\mathbb{Z}[x]$ of degree k.*

Proof We first consider the case that $a_j = 1$ for all $j \in \{0,1,\ldots,m\}$ so that $u(x) = v(x)$. Assume $u(x)$ in this case has a factor in $\mathbb{Z}[x]$ of degree k. Then there exist $w_1(x)$ and $w_2(x)$ in $\mathbb{Z}[x]$ with $u(x) = w_1(x)w_2(x)$ and $\deg w_1(x) = k$. We consider the Newton polygon for

$u(x) = v(x)$ with respect to p. Since the slopes of the edges of the Newton polygon for $u(x)$ increase from left to right, the conditions of the lemma imply that each edge has slope in $[0, 1/k)$. The left-most edge of the Newton polygon may have slope 0. For now, we consider an edge of the Newton polygon which does not have slope 0. Let (a, b) and (c, d) be two lattice points on such an edge. Then the slope of the line passing through these points is the slope of the edge so that

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

Hence, $|c - a| > k$. In other words, any two lattice points on an edge with non-zero slope of the Newton polygon for $u(x)$ with respect to p have their x-coordinates separated by a distance $> k$. Since $\deg w_1(x) = k$, translates of the edges of the Newton polygon for $w_1(x)$ with respect to p cannot be found within those edges of the Newton polygon for $u(x)$ with respect to p which have non-zero slope. Lemma 2.1 implies that the left-most edge of the Newton polygon for $u(x)$ must have slope 0 and length $\geq k$. The conditions of the lemma imply that $\nu(c_{m-j}) \geq 1$ for $j \in \{k, k+1, \ldots, m\}$ so that if the left-most edge of the Newton polygon for $u(x)$ with respect to p has slope 0, then it has length $< k$, giving a contradiction.

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

The above proof relies on the fact that the conditions imposed on $v(x)$ must be satisfied also by $u(x)$. Indeed, it would not weaken the lemma if we simply conclude that $v(x)$ does not have a factor in $\mathbb{Z}[x]$ of degree k. The wording, however, clarifies how a general theorem like Theorem 2.2, involving arbitrary integers a_j with $|a_0| = |a_m| = 1$, can be established by considering the special case that each $a_j = 1$.

For the purposes of dealing with Laguerre polynomials, we will want to take $c_j = b_j$, as defined in the introduction. Then $u(x) = f(x)$, and the lemma is asserting that $f(x)$ cannot have a factor in $\mathbb{Z}[x]$ of degree k if there is a prime p satisfying certain conditions. One of these conditions is that $p \nmid b_m$ which will hold trivially since $b_m = 1$. Another condition is that p must divide b_j for $0 \leq j \leq m - k$. We will obtain such a prime by taking p to be a divisor of $\Delta(n, k)$ with n chosen appropriately. Choosing a large prime divisor of this type will aid in establishing the final condition that the slope of the right-most edge of the

Newton polygon of say

$$g(x) = \sum_{j=0}^{m} b_j x^j$$

is $< 1/k$. It is in this way that we will connect the use of Theorem 1.1 to the irreducibility of Laguerre polynomials. This connection is clarified by our next lemma.

Lemma 2.4 *Let m, k and α be positive integers with $k \leq m/2$. Suppose that p is a prime divisor of $\Delta(m-k+1+\alpha, k)$ or of $\Delta(m-k+1, k)$ satisfying both of the following:*

(i) p does not divide $\Delta(\alpha+1, k)$.

(ii) $p \geq \dfrac{k\alpha}{k+1} + k + 1$.

Then $f(x)$ does not have a factor in $\mathbb{Z}[x]$ of degree k.

Proof Assume $f(x)$ has a factor in $\mathbb{Z}[x]$ of degree k. Suppose first that $p \mid \Delta(m-k+1+\alpha, k)$. In this case, as $\Delta(m-k+1+\alpha, k)$ divides b_j for $0 \leq j \leq m-k$, we deduce $p|b_j$ for $0 \leq j \leq m-k$. Now, suppose $p \mid \Delta(m-k+1, k)$. In this case, we justify also that $p|b_j$ for $0 \leq j \leq m-k$. Since $p \mid \Delta(m-k+1, k)$, we have p divides $m(m-1)\cdots(m-k+1)$. For $m-p+1 \leq j \leq m-k$, we use that $p > m-j$ to see that p divides the binomial

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

Hence, $p|b_j$ for $m-p+1 \leq j \leq m-k$. On the other hand, if $j \leq m-p$, then the expression $(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$ in the definition of b_j consists of a product of $\geq p$ consecutive integers and is therefore divisible by p. We deduce then that $p|b_j$ for all $j \leq m-k$ in this case as well.

The rest of our argument works for both choices of p as above. Since $b_m = 1$, clearly $p \nmid b_m$. By Lemma 2.3, it suffices to show that the right-most edge of the Newton polygon of $g(x)$ has slope $< 1/k$. Setting $\nu = \nu_p$, we have that the slope of this right-most edge is

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

Observe that

$$\frac{b_0}{b_j} = \frac{(j+\alpha)(j-1+\alpha)\cdots(1+\alpha)}{\binom{m}{j}}.$$

It follows that

$$\nu(b_0) - \nu(b_j) \leq \nu\big((j+\alpha)(j-1+\alpha)\cdots(1+\alpha)\big).$$

If $1 \leq j \leq k$, then (i) implies that the right side is 0. Hence,

$$\nu(b_0) - \nu(b_j) \leq 0 < \frac{j}{k} \quad \text{for } j \leq k. \tag{1}$$

For $j > k$, we note that the inequality $(j+\alpha)/(p-1) \le j/k$ holds provided $j(p-k-1) \ge k\alpha$. For $j > k$, we have $j \ge k+1$ so that $j(p-k-1) \ge (k+1)(p-k-1) \ge k\alpha$ by (ii). Therefore,

$$\nu(b_0) - \nu(b_j) \le \nu\big((j+\alpha)!\big) < \sum_{j=1}^{\infty} \frac{j+\alpha}{p^j} = \frac{j+\alpha}{p-1} \le \frac{j}{k} \quad \text{for } j > k. \tag{2}$$

Combining (1) and (2), we obtain

$$\frac{\nu(b_0) - \nu(b_j)}{j} < \frac{1}{k} \quad \text{for } 1 \le j \le m.$$

Lemma 2.3 now implies that $f(x)$ cannot have a factor in $\mathbb{Z}[x]$ of degree k. ■

We step back a moment and take another look at this proof. In particular, we note the role of the binomial $\binom{m}{j}$ in the proof. Or more precisely, we note when it was not used. In the case that $p \mid \Delta(m-k+1+\alpha, k)$, the binomial $\binom{m}{j}$ is insignificant. In other words, if the factor $\binom{m}{j}$ is omitted from our definition of b_j, then the above lemma would hold as it is provided we restrict p to being a divisor of $\Delta(m-k+1+\alpha, k)$. The importance of this remark lies in the fact that if we omit the factor $\binom{m}{j}$ in b_j and take $\alpha = 0$, then $f(x)$ becomes

$$m! \cdot \left(a_m \frac{x^m}{m!} + a_{m-1} \frac{x^{m-1}}{(m-1)!} + \cdots + a_1 x + a_0 \right).$$

Thus, $f(x)$ not having a factor (in $\mathbb{Z}[x]$) of degree k in this case corresponds to establishing that the polynomial in Theorem 2.2 does not have a factor of degree k. The above proof shows then that this polynomial cannot have a factor of degree k if there is a prime p dividing

$$\Delta(m-k+1, k) = m(m-1)\cdots(m-k+1)$$

satisfying (i) and (ii) with $\alpha = 0$. The latter simply means that we want a prime $p \ge k+1$ that divides the above product. Observe that $m-k+1 > k$ if $k \le m/2$. A classic result of J. J. Sylvester [40] implies that if $k \le m/2$, then such a prime p exists; that is, the product of k consecutive integers $> k$ must be divisible by a prime $> k$. We deduce then that the polynomial in Theorem 2.2 cannot have a factor in $\mathbb{Z}[x]$ of degree $k \in [1, m/2]$. It follows that the polynomial must be irreducible and the theorem follows.

We note that the use of Sylvester's theorem above could have been replaced by an application of Theorem 1.1 and Lemma 3.2 below. Indeed, an early motivation for results of the type given by Theorem 1.1 is an interest in improving Sylvester's theorem. Schur's paper [30] consists largely of giving a proof of Sylvester's theorem; apparently, Schur was unaware at the time that the result was known. Later P. Erdős [7], early in his career, gave an elementary argument of Sylvester's theorem. This clearly motivated later work of Erdős [8] where he obtained a stronger result and posed related problems. Some of the contributions along these lines include the work of K. Ramachandra [26], R. Tijdeman [41], and T. N. Shorey [35].

Before leaving this section, we note that the first author [9] generalized Theorem 2.2 by relaxing the condition that $a_m = \pm 1$. More precisely, he showed that one can take a_m to satisfy $0 < |a_m| < m$ unless $(a_m, m) \in \{(\pm 5, 6), (\pm 7, 10)\}$. Similar generalizations have been

obtained by M. Allen and the first author [1, 2] for other irreducibility results of Schur. The methods again involve both an application of Lemma 2.1 as well as information about large primes dividing products of consecutive integers. Besides results already cited in this paper, the works of J. B. Rosser and L. Schoenfeld [27] and L. Schoenfeld [28] should be noted for contributing to the needed prime number estimates. A similar approach can be found also in the work of the first author and R. L. Williams, Jr. [13] and, in the case of applying Lemma 2.1, the prior work of R. Gow [16].

3 The Proof of Theorem 1.2

In this section, we establish Theorem 1.2. Although the case $\alpha \in \{0, 1\}$ has already been handled by Schur [30, 33], we needn't take advantage of this history. The case $\alpha = 0$, as mentioned, follows from Theorem 2.2. In this section, we restrict ourselves therefore to $\alpha \in \{1, 2, \ldots, 10\}$. We begin with showing the important role that is played by Theorem 1.1.

Lemma 3.1 *Let m and α be positive integers with $m \leq 150$ and $\alpha \in \{1, 2, \ldots, 10\}$. Then $L_m^{(\alpha)}(x)$ is irreducible unless (m, α) is one of the pairs $(2, 2)$, $(4, 5)$, and $(2, 7)$. In these cases, $L_m^{(\alpha)}(x)$ is the product of a linear polynomial in $\mathbb{Q}[x]$ and an irreducible polynomial of degree $m - 1$. Furthermore, the more general polynomial $f(x)$ is irreducible for all choices of integers a_j with $|a_m| = |a_0| = 1$ except possibly for the pairs $(m, \alpha) \in \mathcal{T}$ where*

$$\mathcal{T} = \{(2, 2), (2, 7), (4, 4), (4, 5), (8, 8), (24, 8)\}.$$

If $(m, \alpha) \in \mathcal{T}$, then either $f(x)$ is irreducible or it is a product of a linear polynomial in $\mathbb{Z}[x]$ and an irreducible polynomial of degree $m - 1$.

The first part of this lemma involving $L_m^{(\alpha)}(x)$ is done with a direct computation, which we did using Maple, Version 9.5. The second part of the lemma involving the polynomials $f(x)$ is a more difficult computation and involves some analysis of the data. As this part of the lemma is only applied to establishing Theorem 1.3, which is the emphasis of the next section, we defer the proof to the next section. To establish Theorem 1.2, Lemma 3.1 implies that we may suppose $m > 150$, and we do so. Observe that the conditions of Theorem 1.2 and $m > 150$ imply that $(m - k + 1 + \alpha, k) \notin B$, where B is as defined in Theorem 1.1.

Assume $f(x)$, as formulated in the introduction, is reducible. Then $f(x)$ has a factor in $\mathbb{Z}[x]$ of degree say $k \leq m/2$. For the moment, we suppose that $k \geq \max\{3, 1.25\alpha\}$. Since $m - k + 1 + \alpha > m - k \geq k$, we deduce then from Theorem 1.1 that there is a prime $p > 1.8k$ that divides $\Delta(m - k + 1 + \alpha, k)$. We justify that the conditions in Lemma 2.4 hold so that that lemma provides us with a contradiction. Observe that it suffices to show $p > k + \alpha$ since this will imply both (i) and (ii). Since $k \geq 1.25\alpha$, we in fact have that $p > k + 0.8k \geq k + \alpha$ as desired. We have so far established then that $f(x)$ cannot have a factor of degree $\geq \max\{3, 1.25\alpha\}$. In other words, Theorem 1.1 has immediately narrowed down our consideration of factors to only those of small degree. More precisely, we are left with considering

$$k < \max\{3, 1.25\alpha\}.$$

In particular, with α as in Theorem 1.2, we are left only with considering factors of degree ≤ 12.

For the remaining small possibilities for k, we will need something stronger than Theorem 1.1 in regards to the largest prime factor dividing the product of k consecutive integers. In this regard, it is of some interest to note here that we may now appeal to Theorem 1 of S. Laishram and T. N. Shorey's paper [22]. By making use of the fact that $m > 150$ and $k \leq 12$, we can deduce that there is a prime $p > 2k$ dividing $\Delta(m-k+1+\alpha, k)$ and repeat the above argument. This would allow us to deduce $k < \max\{3, \alpha\}$. However, we will not make use of this additional reduction and appeal instead to a different approach to handle all $k < \max\{3, 1.25\alpha\}$. We combine the work of D. H. Lehmer [23] with some of our own computations.

Lemma 3.2 *If m is an integer ≥ 150 and $P(m(m+1)) \leq 11$, then m is one of the following:*

$$175,\ 224,\ 242,\ 384,\ 440,\ 539,\ 2400,\ 3024,\ 4374,\ 9800.$$

Lemma 3.3 *For p a prime, let $m(p)$ denote the largest integer m such that $m(m+1)(m+2)$ has all of its prime factors $\leq p$. Table 3 lists the values of $m(p)$ for all odd primes ≤ 41.*

p	$m(p)$
41	212380
37	17575
31	13454
29	13310
23	2430
19	2430

p	$m(p)$
17	440
13	350
11	98
7	48
5	8
3	2

Table 3: Values of $m(p)$

The above two lemmas follow from work of D. H. Lehmer [23]. The first of these lemmas is an immediate consequence of the tables there. For a proof of the second lemma, we used Table IB in [23] to obtain the value of $m(41)$ (looking for occurrences of two consecutive integers in this table) and then did a computation of $m(p)$ for $p \leq 37$ noting that $m(p) \leq m(41) \leq 212380$ for each such prime.

The next lemma we established by solving various Thue equations using KASH. The algorithm in KASH is based on an algorithm of Y. Bilu and G. Hanrot [3] which itself takes advantage of methods developed by N. Tzanakis and B. M. M. de Weger [42]. To handle the possibility of linear factors, we will consider $k = 1$ in Lemma 2.4. Accordingly, for each $\alpha \in \{1, 2, \ldots, 10\}$, we want one of $m+\alpha$ and m to have a prime factor p satisfying $p \nmid (\alpha+1)$ and $p \geq (\alpha/2) + 2$. We set

$$\mathcal{P} = \mathcal{P}_\alpha = \{p : p \text{ prime}, p = \alpha + 1 \text{ or } p < (\alpha/2) + 2\}.$$

Observe that $\mathcal{P}$ contains every prime divisor of $\alpha + 1$ since $(\alpha+1)/2 < (\alpha/2) + 2$. Suppose that each prime p dividing one of $m + \alpha$ and m is also in $\mathcal{P}$. This is precisely the case where Lemma 2.4 does not eliminate the possibility of $L_m^{(\alpha)}(x)$ having a linear factor in $\mathbb{Z}[x]$.

Therefore, in this case, each of $m+\alpha$ and m, having all of its prime factors in $\mathcal{P}$, can be written as a cube times a product of distinct primes in $\mathcal{P}$ appearing to the first or second power. In other words, the equation $(m+\alpha)-m=\alpha$ can be expressed as the Thue equation

$$AX^3 - BY^3 = \alpha,$$

where each of A and B divides

$$\prod_{p\in\mathcal{P}} p^2.$$

Therefore, if $m(m+\alpha)$ has all of its prime factors in $\mathcal{P}$, then m must be of the form BY^3 for some Thue equation as above. Thus, we can determine all such m by solving each of these Thue equations. Because of Lemma 3.1, we are interested in $m > 150$. The results of these computations are as follows.

Lemma 3.4 *For each $\alpha \in \{1, 2, \ldots, 10\}$, the integers $m > 150$ that satisfy $m(m+\alpha)$ has all of its prime factors in $\mathcal{P}$ are as indicated in Table 4.*

α	primes in $\mathcal{P}$	m's
1	2	none
2	2, 3	none
3	2, 3	none
4	2, 3, 5	320
5	2, 3	none
6	2, 3, 7	162, 288, 378
7	2, 3, 5	243
8	2, 3, 5	192, 640
9	2, 3, 5	216, 375, 720
10	2, 3, 5, 11	240, 320, 440, 540, 800, 990, 1200, 2420

Table 4

Lemma 3.4 implies that the only cases of $f(x)$ having a linear factor in $\mathbb{Z}[x]$ for $m > 150$ must occur in the final column of the row corresponding to α. These polynomials in general will have large coefficients, so we will want to address how one can verify that in fact no linear factors exist in these cases. We will return to that momentarily.

We consider next $\alpha \in \{1, 2, \ldots, 10\}$ and $3 \le k < 1.25\alpha$. Recall that our assumption is that $f(x)$ has a factor of degree k. We show that we can narrow down our consideration of pairs (α, k) to values in rows of Table 5. Observe that Lemma 3.3 and $m > 150$ imply that $\Delta(m-k+1+\alpha, 3)$ and, hence, $\Delta(m-k+1+\alpha, k)$ is divisible by a prime $p > 11$. Using this prime, one checks that Lemma 2.4 implies that if (α, k) does not correspond to a pair given by Table 5, then $f(x)$ does not have a factor of degree k and we obtain a contradiction. Thus, (α, k) is as in Table 5.

We illustrate the approach we used to eliminate the finite list of possibilities for (α, k) given in the table. We consider two cases that sufficiently demonstrate how to eliminate all the pairs given in the table and leave out the details for the remaining cases. For $\alpha = 10$ and

α	k
6	$k = 7$
7	$6 \le k \le 8$
8	$5 \le k \le 9$
9	$4 \le k \le 11$
10	$3 \le k \le 12$

Table 5

$k = 3$, Lemma 2.4 implies that we need only show that one of $\Delta(m-k+1+\alpha, k) = \Delta(m+8, 3)$ and $\Delta(m-k+1, k) = \Delta(m-2, 3)$ has a prime factor $p \ge 17$. Applying Lemma 3.3, we see that such a p dividing $\Delta(m+8, 3)$ exists in this case provided $m > 342$. Recall that $m > 150$. For $150 < m \le 342$, we check directly whether $\Delta(m+8, 3)$ has a prime factor ≥ 17. In fact, in this case, $m = 342$ is the only $m > 150$ for which $P\big(\Delta(m+8, 3)\big) < 17$. On the other hand, for $m = 342$, we have $\Delta(m-2, 3) = \Delta(340, 3)$ is divisible by 31 which exceeds 17. Thus, Lemma 2.4 implies that $f(x)$ cannot have a factor of degree $k = 3$, giving a contradiction in this case.

For our second example, we consider $\alpha = 10$ and $k = 12$. For the purposes of applying Lemma 2.4, we consider the largest prime dividing $\Delta(m-k+1+\alpha, k) = \Delta(m-1, 12)$ and the largest prime dividing $\Delta(m-k+1, k) = \Delta(m-11, 12)$. We want one of these to have a prime factor ≥ 23. By Lemma 3.3, we see that $(m-1)m(m+1)$ which is a factor of $\Delta(m-1, 12)$ is divisible by a prime ≥ 23 provided $m > 2431$. We first check directly for $m \in [151, 2431]$ to determine for which m the value of $\Delta(m-1, 12)$ has all of its prime factors < 23. In fact, this computation is enough in this case as even the smaller product $\Delta(m-1, 5)$ has a prime factor ≥ 23 for every $m \in [151, 2431]$. Since $m \ge 151$, Lemma 2.4 implies a contradiction.

We have now only to consider $k \le 2$. We begin with $k = 2$. Lemma 2.4 implies a contradiction in this case if there is a prime $p > 11$ dividing either $(m+\alpha)(m-1+\alpha)$ or $m(m-1)$. As $m > 150$ and $\alpha \ge 1$, Lemma 3.2 implies that each of $m-1$ and $m-1+\alpha$ must be among the positive integers listed in that lemma. As this list consists of integers any two of which differ by $\ge 18 > \alpha$, we deduce that this is impossible. Hence, $k \ne 2$.

We are left with the possibility that $k = 1$, in other words with establishing that $f(x)$ does not have a linear factor in $\mathbb{Z}[x]$. Observe that given $f(x)$ does not have a factor in $\mathbb{Z}[x]$ with degree in $[2, m/2]$, if $f(x)$ has a linear factor in $\mathbb{Z}[x]$, then $f(x)$ is a linear polynomial times an irreducible polynomial of degree $m-1$. As noted earlier, Lemma 2.4 and Lemma 3.4 imply (α, m) must come from one of the 18 pairs indicated in Table 4. For the remainder of this section, we restrict to considering the polynomials $L_m^{(\alpha)}(x)$ which will complete our proof of Theorem 1.2. The argument here can be skipped as the next section will include a more general argument that handles these 18 pairs for $f(x)$. On the other hand, the remainder of this section has some value as it provides a more direct and simpler argument and at the same time provides us with a chance to elaborate on some further literature and history regarding the Laguerre polynomials.

As $L_m^{(\alpha)}(x)$ is monic, linear factors in $\mathbb{Z}[x]$ correspond to integral roots. Such a root will necessarily be a divisor of the constant term of $L_m^{(\alpha)}(x)$. Due to the size of the coefficients

of $L_m^{(\alpha)}(x)$ as m increases and the large number of divisors that the constant term has, a direct check seems somewhat infeasible. This is particularly true given that a large amount of memory is necessary even to evaluate $L_m^{(\alpha)}(x)$ when m and x are large positive integers. We also had in mind a desire to give an approach to our investigations that would allow one to obtain similar results for $\alpha \notin \{0, 1, \ldots, 10\}$. So we sought to find an efficient method to determine whether $L_m^{(\alpha)}(x)$ has an integer root. It should perhaps be noted that, despite the remark made about numerous divisors of the constant term of $L_m^{(\alpha)}(x)$, one can narrow down the number of integer roots that need be examined considerably by using bounds on the roots of $L_m^{(\alpha)}(x)$. For example, for $\alpha \geq 1$, an easy consequence of work by M. E. H. Ismail and X. Li [21] is that each root of $L_m^{(\alpha)}(x)$ is real and lies in the interval

$$(0, 4m + 2\alpha - 4].$$

We describe next some motivation for our approach. Although the motivation is somewhat technical, as we will see momentarily, the method itself is quite simple. The motivation is nevertheless worth discussion as it gives us a chance to mention further historical investigations on the Laguerre polynomials. There has been considerable work done on obtaining the Galois groups associated with $L_m^{(\alpha)}(x)$ over $\mathbb{Q}$. This includes the work of Schur [32, 33], Coleman [4], Gow [16], Hajir [18, 19, 20] and Sell [34]. Classic work of B. L. van der Waerden [45] implies that almost all polynomials in $\mathbb{Z}[x]$ of degree m have Galois group the symmetric group S_m. The above work suggests that this is also the case for $L_m^{(\alpha)}(x)$. Indeed, the work by Schur [32, 33], Gow [16] and the recent work by Kidd, Trifonov and the first author noted in the last line of Table 2 are motivated in part to showing that for each positive integer m, there exists some α for which the Galois group of $L_m^{(\alpha)}(x)$ is different from S_m. In particular, these combined works have only now been able to accomplish this goal by showing that the alternating group A_m can be achieved as the Galois group for each positive integer m. Seeking polynomials with specified Galois groups has a long history and falls into the area of Inverse Galois Theory (cf. [24]). Assuming that a polynomial of degree > 1 in Theorem 1.2 is typical in that its associated Galois group is the symmetric group, then the classical Chebotarev Density Theorem (cf. [14] and [15]) implies that the density of primes p for which such a polynomial has no roots modulo p is at least $1/3$ and asymptotically, as m tends to infinity, $1/e$. We note that it is not the case that *all* of the polynomials in Theorem 1.2 have associated Galois group the symmetric group; the motivation is based simply on what one can expect of random polynomials under consideration without any computations of the actual Galois groups. Also, it is worth mentioning that even in the case that the Galois group is not the symmetric group, the density of primes p for which a polynomial has no roots modulo p can be estimated through use of the Chebotarev Density Theorem; in particular, for polynomials with degree > 1 and Galois group the alternating group, this density is at least $1/4$ and asymptotically, as m tends to infinity, also $1/e$.

Given that we can expect that $L_m^{(\alpha)}(x)$ will have no roots modulo p for at least $1/3$ of the primes, the idea is simple. We fix α and m under consideration. Next, we take a prime p and, to keep the size of the coefficients small, we compute the coefficients b_j modulo p recursively by using that $b_m = 1$ and

$$b_{m-j-1} \equiv b_{m-j} \cdot \frac{m-j}{j+1} \cdot (m - j + \alpha) \pmod{p} \qquad \text{for } 0 \leq j \leq m-1. \tag{3}$$

In this way, we obtain $\overline{b_j} \in \{0, 1, \ldots, p-1\}$ such that $\overline{b_j} \equiv b_j \pmod{p}$ for each $j \in \{0, 1, \ldots, m\}$. Next, we check whether $L_m^{(\alpha)}(x)$ has a root modulo p by considering the value of

$$\sum_{j=0}^{m} \overline{b_j} z^j \pmod{p} \tag{4}$$

for each $z \in \{0, 1, \ldots, p-1\}$. To avoid the trivial root 0 modulo p and concerns about the denominator in (3) being 0 modulo p, we consider only $p > m + \alpha$. Also, to avoid computing large values of z^j in (4) prior to the reduction modulo p, we compute exponentiation modulo p in a more efficient way. Making use of Maple, Version 9.5, as we did, efficiently computing z^j in this manner corresponds to using `&^` for exponentiation.

The above approach was used to determine, for a given α and m appearing in Table 4, a prime p for which $L_m^{(\alpha)}(x)$ has no roots modulo p. It follows then that each such $L_m^{(\alpha)}(x)$ cannot have an integer root and, hence, a factor of degree 1. This leads to a contradiction which completes our proof of Theorem 1.2. For the purposes of checking our work, we give in Table 6 below the list of primes we found for which $L_m^{(\alpha)}(x)$ has no root modulo p with α and m as in Table 4. In connection to the comments motivating this approach, we note that

α	m	prime
4	320	353
6	162	173
6	288	337
6	378	389
7	243	257
8	192	211

α	m	prime
8	640	673
9	216	251
9	375	389
9	720	743
10	240	257
10	320	331

α	m	prime
10	440	457
10	540	571
10	800	821
10	990	1019
10	1200	1213
10	2420	2437

Table 6: Primes establishing there are no linear factors in $\mathbb{Z}[x]$

the maximal number of primes that we needed to consider for any pair (α, m) in the table was 6 and that the average number of primes considered was exactly 2.5.

4 The Proof of Theorem 1.3

The previous sections have provided us with much of the ground work for establishing Theorem 1.3. We have in fact completed our argument for this theorem except for the following matters. First, we still need to justify the second part of Lemma 3.1 dealing with $f(x)$. Second, we need to explain why $f(x)$ cannot have a linear factor in $\mathbb{Z}[x]$ for the 18 values of (m, α) given in Table 4. Once these are completed, our proof of Theorem 1.3 will rest on justifying that if $f(x)$ is a reducible polynomial corresponding to $(m, \alpha) \in \mathcal{T}$, where $\mathcal{T}$ is as in Lemma 3.1, then $f(x)$ has a linear factor appearing in the corresponding last column of Table 1 and the remaining factor is irreducible. The approach of the previous section for handling these matters in the case that $f(x) = L_m^{(\alpha)}(x)$ took advantage of the fact that there are a finite number of (m, α) under consideration and, hence, a finite number of polynomials $L_m^{(\alpha)}(x)$ to consider. For general $f(x)$ with variable a_j, there are an infinite number of polynomials to consider for each pair (m, α) with $m > 1$. Nevertheless, we can give a single

computational approach that will handle these infinite classes of polynomials. We describe this next.

Lemma 2.4 played a crucial role in establishing Theorem 1.2, so it is reasonable to look back at this lemma for some further insight. In fact, a close look at the proof of this lemma suggests that some improvements may be possible, improvements that we will take advantage of now. We emphasize some main points in the proof. First, our choice of p as a prime dividing $\Delta(m-k+1+\alpha,k)$ or $\Delta(m-k+1,k)$ gives us the condition that $p|b_j$ for $0 \le j \le m-k$ needed to apply Lemma 2.3. Next, (i) and (ii) allowed us to obtain the estimates for (1) and (2), which establish that the right-most edge of the Newton polygon of $g(x)$ has slope $< 1/k$. Then we were able to apply Lemma 2.3 to finish the proof of Lemma 2.4. The key to improving here on what we did there is in noticing that (1) and (2)were based on some rather weak estimates. For both (1) and (2), we ignored the contribution of $\binom{m}{j}$ to the coefficients; for (2), we furthermore overestimated the size of $\nu\big((j+\alpha)(j+\alpha-1)\cdots(1+\alpha)\big)$ with $\nu\big((j+\alpha)!\big)$.

Faced with the possibility of improving Lemma 2.4 while at the same time realizing that the improvement is only needed for a finite number of choices of (m,α), we replace the argument given in (1) and (2) with an exact calculation for a given (m,α). In other words, for each choice of (m,α) with $m \le 150$ and $\alpha \in \{0,1,\dots,10\}$, we consider each positive integer $k \le m/2$ and then each prime dividing $\Delta(m-k+1+\alpha,k)$ or $\Delta(m-k+1,k)$. If the largest such prime exceeds $k+\alpha$, then the conditions in Lemma 2.4 are satisfied and we know $f(x)$ cannot have a factor of degree k. Otherwise, we compute the exact value of

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

If the value of this maximum is $< 1/k$ for any prime dividing $\Delta(m-k+1+\alpha,k)$ or $\Delta(m-k+1,k)$, then $f(x)$ cannot have a factor of degree k. Otherwise, we cannot determine if $f(x)$ has a factor of degree k. We do a similar argument with $k=1$ and the 18 pairs given by Table 4, computing the maximum above to see if it is less than 1. The computations, done with Maple, Version 9.5, established that $f(x)$ cannot have a factor of degree k except possibly for the following triples (m,α,k):

$$(2,2,1),\quad (2,6,1),\quad (2,7,1),\quad (4,4,1),\quad (4,5,1),$$
$$(4,5,2),\quad (6,4,2),\quad (6,4,3),\quad (8,8,1),\quad (24,8,1).$$

In particular, the 18 pairs (m,α) given in Table 4 do not lead to $f(x)$ having a linear factor in $\mathbb{Z}[x]$. As noted in the introduction, the triples $(2,2,1)$, $(2,7,1)$ and $(4,5,1)$ can be realized as leading to reducible polynomials by simply taking $f(x)=m!L_m^{(\alpha)}(x)$. In each of these cases, $x-6$ is a factor. In the case that $m=2$, the polynomial $m!L_m^{(\alpha)}(x)$ is quadratic and, hence, has a second linear factor. For $(m,\alpha)=(2,2)$, the second factor is $x-2$; for $(m,\alpha)=(2,7)$, the second factor is $x-12$. The remaining factors in Table 1, where (m,α) is one of $(2,2)$, $(2,7)$ and $(4,5)$, come from replacing x with $-x$. We also gave examples in the introduction showing that each of $x\pm 2$, $x\pm 6$ and $x\pm 18$ can be a factor if $(m,\alpha)=(8,8)$. We justify next that $f(x)$ can have the linear factors indicated in Table 1 if (m,α) is one of the pairs $(4,4)$ and $(24,8)$, that $f(x)$ cannot have a linear factor if $(m,\alpha)=(2,6)$, that $f(x)$ cannot have a quadratic factor if (m,α) equals $(4,5)$ or $(6,4)$, and that $f(x)$ cannot have a

cubic factor if $(m,\alpha)=(6,4)$. Then we will turn to showing that each reducible $f(x)$ with $(m,\alpha)\in\mathcal{T}$ has a linear factor appearing in the corresponding last column of Table 1.

Consider $(m,\alpha)=(4,4)$. Observe that if

$$a_4=1,\quad a_3=-4,\quad a_1=1,\quad a_0=-1,$$

and $a_2=0$, then $f(x)$ has a factor of $x-2$. On the other hand, if

$$a_4=1,\quad a_3=1,\quad a_1=-3,\quad a_0=-1,$$

and $a_2=0$, then $f(x)$ has a factor of $x-10$. In the case $(m,\alpha)=(24,8)$, we choose

$$a_{24}=1,\quad a_{23}=371688956836585083,\quad a_1=-2158979,\quad a_0=-1,$$

and $a_j=0$ for all other j to obtain the factor $x-6$ for $f(x)$. Replacing x with $-x$ in these examples establishes that each linear factor listed in Table 1 occurs as a linear factor of $f(x)$ if the a_j's are chosen appropriately.

In the case that $(m,\alpha)=(2,6)$, the Newton polygon of $f(x)$ with respect to the prime 2 is a single edge joining $(0,0)$ to $(2,3)$. Hence, $f(x)$ is irreducible in this case and, in particular, cannot have a linear factor.

We consider now the case $(m,\alpha)=(4,5)$. We want to justify in this case that $f(x)$ cannot have a quadratic factor in $\mathbb{Z}[x]$. The Newton polygon of $g(x)=\sum_{j=0}^{4}b_jx^j$ with respect to 3 consists of two edges, one joining the point $(0,0)$ to $(3,2)$ and one joining $(3,2)$ to $(4,3)$. As $f(x)=\sum_{j=0}^{4}a_jb_jx^j$ with $|a_4|=|a_0|=1$, the points $(0,0)$ and $(4,3)$ are endpoints of edges of the Newton polygon of $f(x)$ with respect to 3. We consider two possibilities depending on whether $3\mid a_1$ or not. If $3\mid a_1$, then the Newton polygon of $f(x)$ with respect to 3 is a single line segment joining $(0,0)$ and $(4,3)$, and we deduce from Lemma 2.1 that $f(x)$ is in fact irreducible. If $3\nmid a_1$, then the Newton polygon of $f(x)$ with respect to 3 is the same as the Newton polygon of $g(x)$ with respect to 3, and we deduce from Lemma 2.1 that $f(x)$ is either irreducible or it is a linear polynomial times an irreducible cubic. In either case, we see that $f(x)$ cannot have a quadratic factor in $\mathbb{Z}[x]$.

In the case that $(m,\alpha)=(6,4)$, the Newton polygon of $g(x)$ with respect to 5 consists of two edges, one joining $(0,0)$ to $(5,1)$ and one joining $(5,1)$ to $(6,2)$. If $5\mid a_1$, then the Newton polygon of $f(x)$ with respect to 5 is a single line segment joining $(0,0)$ and $(6,2)$, and we deduce from Lemma 2.1 that if $f(x)$ is reducible, then $f(x)$ is the product of two irreducible cubics. If $5\nmid a_1$, then the Newton polygon of $f(x)$ with respect to 5 is the same as the Newton polygon of $g(x)$ with respect to 5, and we deduce from Lemma 2.1 that if $f(x)$ is reducible, then it is a linear polynomial times an irreducible quintic. In either case here, we see that $f(x)$ cannot have a quadratic factor in $\mathbb{Z}[x]$.

Finally, we turn to establishing if $(m,\alpha)=(6,4)$, then $f(x)$ does not have a cubic factor in $\mathbb{Z}[x]$. The Newton polygon of $g(x)$ with respect to 3 consists of a single edge joining $(0,0)$ to $(6,3)$. The Newton polygon of $f(x)$ with respect to 3 in this case is the same as the Newton polygon of $g(x)$ with respect to 3. We deduce from Lemma 2.1 that each irreducible factor of $f(x)$ has an even degree. Hence, $f(x)$ cannot have a cubic factor in $\mathbb{Z}[x]$.

We turn now to establishing that if $f(x)$ has a linear factor in $\mathbb{Z}[x]$ for some (m,α) appearing in Table 1, then it must have one of the factors listed in the last column of that table. We give a simple lemma and a couple of examples which adequately explain the procedure we used in each case.

Lemma 4.1 *Let $w(x)$ be a monic polynomial in $\mathbb{Z}[x]$ divisible by $x-a$ with $a \in \mathbb{Z}$. Let p be a prime and e a nonnegative integer for which $p^e \| a$. Then the Newton polygon of $w(x)$ with respect to p has an edge that includes a translate of the line segment joining $(0,0)$ to $(1,e)$. Also, if the right-most edge has slope < 1, then necessarily $e = 0$.*

The first part of the lemma, involving the translated edge, is a straight-forward application of Lemma 2.1. Observe that if the right-most edge of the Newton polygon has slope < 1, then so do all of the edges so that the only possibility for the Newton polygon to contain a translation of the edge from $(0,0)$ to $(1,e)$ is for e to equal 0 as claimed. Before proceeding, we note also that Lemma 4.1 or a simple application of the classical Rational Root Test implies that if $p \mid a$, then p divides the constant term of $w(x)$. Observe that since $f(x)$ is monic, if $f(x)$ is reducible, then it has a factor of the form $x - a$ where $a \in \mathbb{Z}$. We are therefore able to take $w(x) = f(x)$ in Lemma 4.1 to obtain information about the factors $x - a$ that can divide $f(x)$.

Consider the case that $(m, \alpha) = (4, 5)$. The constant term of $f(x)$ is $3024 = 2^4 \cdot 3^3 \cdot 7$. Observe that the slope of the right-most edge of the Newton polygon for $f(x)$ with respect to some prime is no more than the slope of the right-most edge of the Newton polygon for $g(x)$ with respect to the same prime. As the latter slope is < 1 for $p = 7$, we deduce that a cannot be divisible by primes $p \geq 5$. The Newton polygon of $g(x)$ with respect to 2 is a single line segment from $(0,0)$ to $(4,4)$ and is also the Newton polygon of $f(x)$ with respect to 2. Hence, Lemma 4.1 implies that $2 \| a$. The Newton polygon of $g(x)$ with respect to 3 consists of two segments, one joining $(0,0)$ to $(3,2)$ and one joining $(3,2)$ to $(4,3)$. If $3 \nmid a_1$, then the Newton polygon of $f(x)$ with respect to 3 is the same as the Newton polygon of $g(x)$ with respect to 3 and, by Lemma 4.1, we deduce $3 \mid a$. If $3 \mid a_1$, then the Newton polygon of $f(x)$ with respect to 3 is a single line segment from $(0,0)$ to $(4,3)$ and Lemma 2.1 implies $f(x)$ is irreducible. Therefore, we obtain in this case that $a = \pm 6$, which justifies the row corresponding to $(m, \alpha) = (4, 5)$ in Table 1.

Consider next the case that $(m, \alpha) = (8, 8)$. The constant term of $f(x)$ is ± 518918400 which is divisible only by primes ≤ 13. As the slope of the right-most edge of the Newton polygon for $g(x)$ with respect to each prime $\in [5, 13]$ is < 1, we deduce the same is true of the slope of the right-most edge of the Newton polygon for $f(x)$. Therefore, Lemma 4.1 implies that the only primes dividing a are ≤ 3. The Newton polygon of $g(x)$ with respect to 2 is a single line segment from $(0,0)$ to $(8,8)$ and is also the Newton polygon of $f(x)$ with respect to 2. Hence, Lemma 4.1 implies that $2 \| a$. The Newton polygon of $g(x)$ with respect to 3 consists of three segments, one joining $(0,0)$ to $(1,0)$, one joining $(1,0)$ to $(7,2)$ and the final one joining $(7,2)$ to $(8,4)$. There are a few possibilities for the Newton polygon of $f(x)$ with respect to 3, but we do not need to analyze them as our interest now is simply in showing that $3^3 \nmid a$ as, once this is shown, we can deduce that $a \in \{\pm 2, \pm 6, \pm 18\}$ as indicated in Table 1. Assume $3^3 \mid a$. Then Lemma 4.1 implies that the Newton polygon of $f(x)$ with respect to 3 has an edge with slope ≥ 3. The slope of the right-most edge of the Newton polygon of $f(x)$ with respect to 3 has a slope that is no more than the slope of the right-most edge of the Newton polygon of $g(x)$ with respect to 3. As the latter slope is 2, the slope of each edge of the Newton polygon of $f(x)$ with respect to 3 is ≤ 2, giving a contradiction and completing the argument for $(m, \alpha) = (8, 8)$.

For each (m, α) listed in Table 1, a similar analysis was done. We omit the details.

The proof of Theorem 1.3 is essentially done. We should note, however, in establishing

that a polynomial $f(x) \in \mathbb{Z}[x]$ of degree m does not have a factor in $\mathbb{Z}[x]$ of degree $k \leq m/2$ unless $k = 1$, we have also shown that either $f(x)$ is irreducible or it is the product of a linear polynomial and an irreducible polynomial of degree $m-1$. This can be seen as follows. Suppose $f(x)$ has a factor $x - a$ as in Table 1, so $f(x) = (x - a)w(x)$ for some $w(x) \in \mathbb{Z}[x]$ of degree $m - 1$. We want to show $w(x)$ is irreducible. Clearly, this is the case if $m = 2$. If $m \neq 2$, then Table 1 implies $m \geq 4$. If $w(x)$ is reducible, then it has a factor $u(x) \in \mathbb{Z}[x]$ of degree $\leq (m-1)/2$. We deduce that one of $u(x)$ and $(x - a)u(x)$ is a factor of $f(x)$ of degree strictly > 1 and $\leq m/2$. This is a contradiction as $f(x)$ has been shown to have no nonlinear factors in $\mathbb{Z}[x]$ of degree $\leq m/2$. Hence, the proof of Theorem 1.3 is complete.

References

[1] M. Allen and M. Filaseta, *A generalization of a second irreducibility theorem of I. Schur*, Acta Arith., **109** (2003), 65–79.

[2] M. Allen and M. Filaseta, *A generalization of a third irreducibility theorem of I. Schur*, Acta Arith. **114** (2004), 183–197.

[3] Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory 60 (1996), no. 2, 373–392.

[4] R. F. Coleman, *On the Galois groups of the exponential Taylor polynomials*, L'Enseignement Math. 33 (1987), 183–189.

[5] G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, Journal de Math. Pure et Appl. 2 (1906), 191–258.

[6] G. Eisenstein, *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, Crelle J. 39 (1850), 160–182.

[7] P. Erdős, *A theorem of Sylvester and Schur*, J. London Math. Soc. 9 (1934), 282–288.

[8] P. Erdős, *On consecutive integers*, Nieuw Arch. Wisk. 3 (1955), 124–128.

[9] M. Filaseta, *A generalization of an irreducibility theorem of I. Schur*, in: Analytic Number Theory, Proc. Conf. in Honor of Heini Halberstam, vol. 1, B. C. Berndt, H. G. Diamond, and A. J. Hildebrand (eds.), Birkhäuser, Boston, 1996, 371–395.

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

[11] M. Filaseta and T.-Y. Lam, *On the irreducibility of the generalized Laguerre polynomials*, Acta Arth. **105** (2002), 177–182.

[12] M. Filaseta and O. Trifonov, *The Irreducibility of the Bessel polynomials*, J. Reine Angew. Math. 550 (2002), 125–140.

[13] M. Filaseta and R. L. Williams, Jr., *On the irreducibility of a certain class of Laguerre polynomials*, J. Number Theory 100 (2003), 229–250.

[14] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, 91–101.

[15] L. J. Goldstein, Analytic Number Theory, Prentice-Hall, Englewood Cliffs, New Jersey, 1971.

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

[17] E. Grosswald, Bessel Polynomials, Lecture Notes in Math. 698, Springer, Berlin, 1978.

[18] F. Hajir, *Some A_n-extensions obtained from generalized Laguerre polynomials*, J. Number Theory **50** (1995), 206–212.

[19] F. Hajir, *On the Galois group of generalized Laguerre polynomials*, preprint.

[20] F. Hajir, *Algebraic properties of a family of generalized Laguerre polynomials*, preprint.

[21] M. E. H. Ismail and X. Li, *Bounds on the extreme zeros of orthogonal polynomials*, Proc. Amer. Math. Soc. 115 (1992), 131–140.

[22] S. Laishram and T. N. Shorey, *The greatest prime divisor of a product of consecutive integers*, Acta Arith. 120 (2005), no. 3, 299–306.

[23] D. H. Lehmer, *On a problem of Störmer*, Illinois J. Math. 8 (1964), 57–79.

[24] B. H. Matzat, Konstruktive Galoistheorie, Lecture Notes in Math. 1284, Springer-Verlag, Berlin, 1987.

[25] R. F. McCoart, *Irreducibility of certain classes of Legendre polynomials*, Duke Math. J. 28 (1961), 239–246.

[26] K. Ramachandra, *A note on numbers with a large prime factor, III*, Acta Arith. 19 (1971), 49–62.

[27] J. B. Rosser and L. Schoenfeld, *Sharper bounds for Chebyshev functions $\theta(x)$ and $\psi(x)$*, Math. Comp., 29 (1975), 243–269.

[28] L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, II*, Math. Comp. **30** (1976), 337–360.

[29] T. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, Crelle J. 32 (1846), 3–105.

[30] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., 14 (1929), 125–136.

[31] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, II*, Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl., 14 (1929), 370–391.

[32] I. Schur, *Gleichungen ohne Affekt*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse (1930), 443–449.

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

[34] E. A. Sell, *On a certain family of generalized Laguerre polynomials*, Journal of Number Theory **107** (2004), 266–281.

[35] T. N. Shorey, *On gaps between numbers with a large prime factor, II* Acta Arith. 25 (1973/74), 365–373.

[36] T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression*, A tribute to Paul Erdős, 385–389, Cambridge Univ. Press, Cambridge, 1990.

[37] T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression. II*, Acta Arith. 53 (1990), 499–504.

[38] T. N. Shorey and R. Tijdeman, *On the greatest prime factors of an arithmetical progression. III*, Approximations diophantiennes et nombres transcendants (Luminy, 1990), 275–280, de Gruyter, Berlin, 1992.

[39] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, Cambridge Univ. Press, Cambridge, 1986.

[40] J. J. Sylvester, *On arithmetical series*, Messenger of Math. 21 (1892), 1–19, 87–120.

[41] R. Tijdeman, *On the maximal distance of numbers with a large prime factor*, J. London Math. Soc. 5 (1972), 313–320.

[42] N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory 31 (1989), 99–132.

[43] J. H. Wahab, *New cases of irreducibility of Legendre polynomials*, Duke Math J. 19 (1952), 165–176.

[44] J. H. Wahab, *New cases of irreducibility for Legendre polynomials II*, Duke Math. J. 27 (1960), 481–482.

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