ON THE IRREDUCIBILITY OF THE GENERALIZED LAGUERRE POLYNOMIALS

M. Filaseta\(^1\) and T.-Y. Lam

June 10, 2001

\(^1\)The author gratefully acknowledges support from the National Security Agency.
1 Introduction

The generalized Laguerre polynomials are defined by

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

where \( m \) is a positive integer and \( \alpha \) is an arbitrary complex number. In 1929, I. Schur [4] established the irreducibility over the rationals of \( L_m^{(0)}(x) \), the classical Laguerre polynomials, for every \( m \). In 1931, I. Schur [5] considered \( L_m^{(\alpha)}(x) \) in general and showed that \( L_m^{(1)}(x) \) is irreducible over the rationals for every \( m \). The case \( \alpha \notin \{0, 1\} \) remained open. The purpose of this paper is to establish the following:

**Theorem 1.** Let \( \alpha \) be a rational number which is not a negative integer. Then for all but finitely many positive integers \( m \), the polynomial \( L_m^{(\alpha)}(x) \) is irreducible over the rationals.

Before going to the proof, it is worth noting that reducible \( L_m^{(\alpha)}(x) \) do exist even with \( \alpha = 2 \). In particular, we give the following examples:

\[
\begin{align*}
L_2^{(2)}(x) &= \frac{1}{2}(x - 2)(x - 6) \\
L_2^{(23)}(x) &= \frac{1}{2}(x - 20)(x - 30) \\
L_4^{(23)}(x) &= \frac{1}{24}(x - 30)(x^3 - 78x^2 + 1872x - 14040) \\
L_4^{(12/5)}(x) &= \frac{1}{15000}(25x^2 - 420x + 1224)(25x^2 - 220x + 264) \\
L_5^{(39/5)}(x) &= -\frac{1}{375000}(5x - 84)(625x^4 - 29500x^3 + 448400x^2 - 2662080x + 5233536).
\end{align*}
\]

It is not difficult to show that in fact there are infinitely many positive integers \( \alpha \) for which \( L_2^{(\alpha)}(x) \) is reducible (a product of two linear polynomials).

**Theorem** is a direct consequence of the following more general result:
Theorem 2. Let $\alpha$ be a rational number which is not a negative integer. Then for all but finitely many positive integers $m$, the polynomial
\[
\sum_{j=0}^{m} a_j \frac{(m + \alpha)(m - 1 + \alpha) \cdots (j + 1 + \alpha)x^j}{(m - j)!j!}
\]
is irreducible over the rationals provided only that $a_j \in \mathbb{Z}$ for $0 \leq j \leq m$ and $|a_0| = |a_m| = 1$.

I. Schur obtained his irreducibility results for $L_m^{(0)}(x)$ and $L_m^{(1)}(x)$ through general results similar to the above (except also for all $m \geq 1$). Recent work of a similar nature has been done by Filaseta [1, 2] and by Filaseta and Trifonov [3]. We note also that the above results can be made effective so that for any fixed $\alpha \in \mathbb{Q}$ it is possible to determine a finite set $S = S(\alpha)$ of $m$ such that the polynomial in Theorem 2 is irreducible (for $a_j$ as stated there) provided $m \not\in S$.

2 A Proof of Theorem 2

For a prime $p$ and a non-zero integer $a$, we define $\nu(a) = \nu_p(a) = e$ where $p^e || a$. We set $\nu(0) = +\infty$. We define the Newton polygon of a polynomial $f(x) = \sum_{j=0}^{n} a_j x^j$ with respect to a prime $p$, where $a_n a_0 \neq 0$ as the lower convex hull of the points $(j, \nu(a_n - j))$. Thus, the slopes of the edges of the Newton polygon of $f(x)$ with respect to $p$ are increasing from left to right. We begin with the following preliminary results.

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

Lemma 2. Let $a, b, c$ and $d$ be integers with $bc - ad \neq 0$. Then the largest prime factor of $(am + b)(cm + d)$ tends to infinity as the integer $m$ tends to infinity.

Lemma 1 is given as Lemma 2 in [1]. Lemma 2 above is a fairly easy consequence of the fact that the Thue equation $ux^3 - vy^3 = w$ has finitely many solutions in integers $x$ and $y$ where $u, v$, and $w$ are fixed integers with $w \neq 0$. It also immediately follows from Corollary 1.2 of [6]. We omit the proofs.
Fix $\alpha$ now as in Theorem 2. Throughout the argument we suppose as we may that $m$ is large. Define

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

for $0 \leq j \leq m$.

We want to show that for all but finitely many positive integers $m$, the polynomial $f(x) = \sum_{j=0}^{m} a_j c_j x^j$ is irreducible over the rationals, where $a_j$ are arbitrary integers with $|a_0| = |a_n| = 1$. Motivated by Lemma 1, we consider instead $g(x) = \sum_{j=0}^{m} c_j x^j$. Let $u$ and $v$ be relatively prime integers with $v > 0$ such that $\alpha = u/v$. The condition that $\alpha$ is not a negative integer implies that for each $j \in \{0, 1, \ldots, m-1\}$, $m - j + \alpha$ and, hence, $v(m - j) + u$ cannot be zero. We assume that $g(x)$ has a factor in $\mathbb{Z}[x]$ of degree $k \in [1, m/2]$ and establish the theorem by obtaining a contradiction to Lemma 1. We divide the argument into cases depending on the size of $k$.

Case 1. $k > m/\log^2 m$.

For $a$ and $b$ integers with $b > 0$, let $\pi(x; b, a)$ denote the number of primes $\leq x$ which are $\equiv a \pmod{b}$. Then the Prime Number Theorem for Arithmetic Progressions implies that if $\gcd(a, b) = 1$, then

$$\pi(x; b, a) = \frac{1}{\phi(b)} \int_{2}^{x} \frac{dt}{\log t} + O\left(\frac{x}{\log^4 x}\right)$$

$$= \frac{1}{\phi(b)} \left( \frac{x}{\log x} + \frac{x}{\log^2 x} + \frac{2x}{\log^3 x} + O\left(\frac{x}{\log^4 x}\right) \right).$$

By considering $\pi(x; b, a) - \pi(x; b, a)$, it follows that for $a$ and $b$ fixed, the interval $(x - h, x]$ contains a prime $\equiv a \pmod{b}$ if $h = x/(2\log^2 x)$ and if $x$ is sufficiently large. Taking $a = u, b = v$, and $x = vm + u$, we deduce that for some integer $j \in [0, k)$, the number $v(m - j) + u$ is prime. Call such a prime $p$, and observe that $p \geq 2vm/3$ (since $v$ is a positive integer and $m$ is large). We deduce that $p$ does not divide $v$. Observe that

$$c_\ell = \binom{m}{\ell} (vm + u)(v(m - 1) + u) \cdots (v(\ell + 1) + u)$$

for $0 \leq \ell \leq m$.

For $j \in \{0, 1, \ldots, k-1\}$, the numbers $v(m - j) + u$ appear in the numerator of the fraction on the right-hand side above whenever $0 \leq \ell \leq m - k$. Therefore,

$$\nu_p(c_\ell) \geq 1 \quad \text{for} \quad 0 \leq \ell \leq m - k. \quad (1)$$
Since \( c_m = \pm 1, \nu_p(c_m) = 0 \). To obtain a contradiction from Lemma 1 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 slope \(< \frac{1}{m - k} < \frac{1}{k} \). Recall that \( p \nmid v \) and that \( p \geq 2v m/3 \). For \( j \in \{0, 1, \ldots, m - 1\} \), we deduce the inequality

\[
2p > vm + u \geq v(m - j) + u \geq v + u > -p.
\]

The condition that \( \alpha \) is not a negative integer implies that none of \( v(m - j) + u \) can be zero. Hence, \( p \) itself is the only multiple of \( p \) among the numbers \( v(m - j) + u \) with \( 0 \leq j \leq m - 1 \). Since \( c_0 = (vm + u)(v(m - 1) + u) \cdots (v + u)/v^m \), we obtain \( \nu_p(c_0) = 1 \).

**Case 2.** \( k_0 \leq k \leq m/\log^2 m \) with \( k_0 = k_0(u, v) \) a sufficiently large integer.

Let \( z = k(\log \log k)^{1/2} \). We first show that there is a prime \( p > z \) that divides \( v(m - j) + u \) for some \( j \in \{0, 1, \ldots, k - 1\} \). Then (1) follows as before, and we will obtain a contradiction to Lemma 1 by showing that the right-most edge of the Newton polygon of \( g(x) \) with respect to \( p \) has slope \(< \frac{1}{k} \).

Let

\[
T = \{v(m - j) + u : 0 \leq j \leq k - 1\}.
\]

Since \( m \) is large, we deduce that the elements of \( T \) are each \( \geq m/2 \). Also, observe that \( \gcd(u, v) = 1 \) implies that each element of \( T \) is relatively prime to \( v \). For each prime \( p \leq z \), we consider an element \( a_p = v(m - j) + u \in T \) with \( \nu_p(a_p) \) as large as possible. We let

\[
S = T - \{a_p : p \nmid v, p \leq z\}.
\]

By the Prime Number Theorem,

\[
\pi(z) \leq \frac{2k(\log \log k)^{1/2}}{\log k}.
\]

We combine this estimate momentarily with \( |S| \geq k - \pi(z) \). Since \( k \leq m/\log^2 m \), we obtain \( m \geq k \log^2 k \). Consider a prime \( p \leq z \) with \( p \) not dividing \( v \), and let \( r = \nu_p(a_p) \). By the definition of \( a_p \), 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 \( \leq \lceil k/p^j \rceil + 1 \) multiples of \( p^j \) in \( T \) and, hence, at most \( \lceil k/p^j \rceil \) multiples of \( p^j \) in \( S \). Therefore,

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

4
and
\[ \prod_{s \in S} \prod_{p \leq z} p^{\nu_p(s)} \leq k! \leq k^k. \]

On the other hand,
\[ \prod_{s \in S} s \geq \left( \frac{m}{2} \right)^{|S|} \geq \left( \frac{k \log^2 k}{2} \right)^{k - \pi(z)}. \]

Recalling our bound on \( \pi(z) \), we obtain
\[
\log \left( \prod_{s \in S} s \right) \geq (k - \pi(z))( \log k + 2 \log \log k - \log 2) \\
\geq \left( k - \frac{2k \sqrt{\log k}}{\log k} \right)( \log k + 2 \log \log k - \log 2) \\
\geq k \log k + 2k \log \log k + O(k \sqrt{\log \log k}).
\]

Since \( k \geq k_0 \) where \( k_0 \) is sufficiently large,
\[
\log \left( \prod_{s \in S} s \right) > k \log k \geq \log \left( \prod_{s \in S} \prod_{p \leq z} p^{\nu_p(s)} \right).
\]

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 in \( T \), and let \( \nu = \nu_p \). The right-most edge of the Newton polygon of \( g(x) \) with respect to \( p \) is
\[
\max_{1 \leq j \leq m} \left\{ \frac{\nu(c_0) - \nu(c_j)}{j} \right\}.
\]

Fix \( j \in \{1, 2, \ldots, m\} \). To complete the case under consideration, we want to show that the fraction above is \( < 1/k \). Observe that
\[
\nu(c_0) - \nu(c_j) \leq \nu \left( (v_j + u)(v(j - 1) + u) \cdots (v + u) \right) \\
\leq \nu((v_j + |u|)!) = \sum_{j=1}^{\infty} \left[ \frac{v_j + |u|}{p^j} \right] \\
< \sum_{j=1}^{\infty} \frac{v_j + |u|}{p^j} = \frac{v_j + |u|}{p-1}.
\]
Since $p > z = k(\log \log k)^{1/2}$ and $k \geq k_0$, we easily deduce that the right-most edge of the Newton polygon of $g(x)$ with respect to $p$ has slope $< 1/k$ as desired. Hence, as indicated at the beginning of this case, we obtain a contradiction to Lemma [1].

**Case 3.** $2 \leq k < k_0$.

By Lemma [2] (with $a = v$, $b = u$, $c = v$, and $d = u - v$), the largest prime factor of the product $(vm + u)(v(m-1) + u)$ tends to infinity. Since $m$ is large, we deduce that there is a prime $p > (v + |u|)k_0$ that divides $(vm + u)(v(m-1) + u)$. The argument now follows as in the previous case. In particular,

$$\frac{\nu(c_0) - \nu(c_j)}{j} < \frac{vj + |u|}{j(p-1)} \leq \frac{v + |u|}{p-1} \leq \frac{1}{k_0} < \frac{1}{k}$$

for $1 \leq j \leq m$,

and the right-most edge of the Newton polygon of $g(x)$ with respect to $p$ has slope $< 1/k$. Hence, in this case, we also obtain a contradiction.

**Case 4.** $k = 1$.

From Lemma [2] the largest prime factor of $m(vm + u)$ tends to infinity with $m$. We consider a large prime factor $p$ of this product. In particular, we suppose that $p > v + |u|$. Note this implies $p \nmid v$. As in the previous case, we are through if $p | (vm + u)$. So suppose $p | m$. The binomial coefficient $\binom{m}{j}$ appears in the definition of $c_j$, and this is sufficient to guarantee that $\nu(c_j) \geq 1$ and $\nu(c_{m-j}) \geq 1$ for $1 \leq j \leq p - 1$. On the other hand,

$$c_j = \binom{m}{j} \frac{(vm + u)(v(m-1) + u) \cdots (v(j+1) + u)}{v^{m-j}}.$$

For $j \leq m - p$, the numerator of the fraction on the right is a product of $\geq p$ consecutive terms in the arithmetic progression $vt + u$ with $\gcd(p, v) = 1$; thus, $\nu(c_{m-j}) \geq 1$ for $j \geq p$. This implies that (1) holds with $k = 1$. It follows in the same manner as before that the slope of the right-most edge is $< 1$. A contradiction to Lemma [1] is again obtained (and the proof of the theorem is complete).

**References**


