A generalization of a second irreducibility theorem of I. Schur

by

MARTHA ALLEN AND MICHAEL FILASETA

1 Introduction

In [8] and [9], I. Schur established four theorems concerning the irreducibility of certain classes of polynomials over the rationals. The second author [6] generalized one of these results to obtain the following.

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

$$f(x) = a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_2 \frac{x^2}{2} + a_1 x + a_0.$$

If $0 < |a_n| < n$, then $f(x)$ is irreducible unless

$$(a_n, n) \in \big\{ (\pm 5, 6), (\pm 7, 10) \big\}$$

in which cases either $f(x)$ is irreducible or $f(x)$ is the product of two irreducible polynomials of equal degree. If $|a_n| = n > 1$, then for some choice of $a_1, \dots, a_{n-1} \in \mathbb{Z}$ and $a_0 = \pm 1$, we have that $f(x)$ is reducible.

I. Schur (in [8]) obtained this result in the special case that $a_n = \pm 1$. Further results along the nature of Theorem 1 are also discussed in [6].

The purpose of this paper is to establish a generalization of a second theorem of I. Schur. Namely, we prove

Theorem 2. *For n an integer ≥ 1, define*

$$f(x) = a_n \frac{x^n}{(n+1)!} + a_{n-1} \frac{x^{n-1}}{n!} + \cdots + a_1 \frac{x}{2} + a_0$$

where the a_j's are arbitrary integers with $|a_0| = 1$. Let k', k'', u, v, and w be nonnegative integers satisfying

$$n + 1 = k' 2^u \quad \textit{with } k' \textit{ odd}$$

and

$$(n+1)n = k'' 2^v 3^w \quad \textit{with } \gcd(k'', 6) = 1.$$

Let $M = M(n) = \min\{k', k''\}$. If $0 < |a_n| < M$, then $f(x)$ is irreducible. Furthermore, the bound M on $|a_n|$ is best possible for every $n > 2$; that is, for each such n, there exist a_j as above but with $a_n = \pm M$ and with $f(x)$ reducible.

Both authors were supported by the National Security Agency and the second author was also supported by the National Science Foundation. Research by the first author was done in partial fulfillment of the requirement for a Ph.D. at the University of South Carolina.

I. Schur [9] dealt with the case again in which $a_n = \pm 1$. He also noted that with this restriction on a_n, the polynomial $f(x)$ can be reducible in the case that $n+1$ is a power of 2 or $n = 8$. This remark follows from our theorem upon recalling that 8 and 9 are the only prime powers (with exponents exceeding 1) that differ by 1 (see [2]).

In establishing Theorem 2, we will show the following results:

- If $0 < |a_n| \leq n+1$, then $f(x)$ cannot have a factor of degree k in $[3, n/2]$ except possibly for finitely many pairs (a_n, n).
- If $0 < |a_n| < k'$, then $f(x)$ cannot have a linear factor.
- If $0 < |a_n| < k''$, then $f(x)$ cannot have a quadratic factor.

The techniques used for these results will be similar to those used in [6] and [7]. The above three results show that for $0 < |a_n| < M$, $f(x)$ is irreducible except possibly for finitely many pairs (a_n, n). We also show for the exceptional finite list of pairs (a_n, n) that $f(x)$ is irreducible if $0 < |a_n| < M$. Finally, we will demonstrate that the bound on a_n in Theorem 2 is sharp if $n > 2$. As we will note in Section 5, the value of $M(2)$ can be replaced by 3 in Theorem 2 and this then is the best possible bound in this case.

2 The first preliminary result

In this section, we establish

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

$$f(x) = \sum_{j=0}^{n} a_j \frac{x^j}{(j+1)!}.$$

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

$$p^r | (n+1)n(n-1)\cdots(n-k+2) \text{ and } p^r \nmid a_n.$$

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

Lemma 1 implies that if $f(x)$ has a factor of degree k, then each prime power p^r that divides $(n+1)n\cdots(n-k+2)$ must also divide a_n. Thus,

$$\prod_{\substack{p^r \| (n+1)n(n-1)\cdots(n-k+2) \\ p \geq k+2}} p^r \mid a_n.$$

Our proof of Lemma 1 will be based on the use of Newton polygons and a theorem of Dumas [3]. If p is a prime and m is a nonzero integer, we define

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

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

Consider the lower edges along the convex hull of these points. The left-most endpoint is $(0, \nu(a_n))$ and the right-most endpoint is $(n, \nu(a_0))$. 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. We will refer to the points in S as spots of the Newton polygon.

Proof of Lemma 1. Let

$$F(x) = (n+1)! f(x) = \sum_{j=0}^{n} a_j \frac{(n+1)!}{(j+1)!} x^j = \sum_{j=0}^{n} b_j x^j,$$

where $b_j = a_j (n+1)!/(j+1)!$. Note that $F(x)$ has integer coefficients. To show that $f(x)$ cannot have a factor of degree k, it suffices to show that $F(x)$ cannot have a factor of degree k.

Consider the Newton polygon of $F(x)$ with respect to the prime p. Note that the condition

$$p^r | (n+1)n(n-1)\cdots(n-k+2)$$

implies that $p^r | b_j$ for $j \in \{0, 1, \ldots, n-k\}$. Thus, the $n-k+1$ right-most spots, $(k, \nu(b_{n-k})), \ldots, (n, \nu(b_0))$, have y-coordinates greater than or equal to r. Consider the coordinates of the left-most endpoint $(0, \nu(a_n))$. By the given, $p^r \nmid a_n$; thus, the y-coordinate of the left-most endpoint is less than r.

Since the slopes of the edges of the Newton polygon of $F(x)$ increase from left to right, the spots $(j, \nu(b_{n-j}))$ for $j \in \{k-1, k, k+1, \ldots, n\}$ all lie on or above edges of the Newton polygon which have positive slope.

The slope of the right-most edge is

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

For $1 \le j \le n$,

$$\begin{aligned}
\nu(b_0) - \nu(b_j) &= \nu(a_0 (n+1)!) - \nu\left(a_j \frac{(n+1)!}{(j+1)!} \right) \\
&\le \nu((n+1)!) - \nu\left(\frac{(n+1)!}{(j+1)!} \right) \\
&= \nu((j+1)!).
\end{aligned}$$

We consider two cases to estimate $\nu((j+1)!)/j$.

Case (i). Suppose $j < p-1$. Since p is prime and since $j+1 < p$, $p \nmid (j+1)!$. Therefore, $\nu((j+1)!) = 0$. So for $j < p-1$,

$$\frac{\nu((j+1)!)}{j} = 0.$$

Case (ii). Suppose $j \geq p-1$. Note that

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

Since $1/j \leq 1/(p-1)$, we deduce

$$\frac{\nu((j+1)!)}{j} < \frac{1}{p-1} + \frac{1}{j(p-1)} \leq \frac{1}{p-1} + \frac{1}{(p-1)^2} = \frac{p}{(p-1)^2}.$$

By the conditions in the lemma, $p \geq k+2$. One checks that this implies $p/(p-1)^2 < 1/k$. By combining Cases (i) and (ii), we obtain

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(b_0) - \nu(b_j)}{j} \right\} \leq \max_{1 \leq j \leq n} \left\{ \frac{\nu((j+1)!)}{j} \right\} < \frac{p}{(p-1)^2} < \frac{1}{k}.$$

In other words, the slope of the right-most edge is less than $1/k$. Since the slopes of the edges of the Newton polygon increase from left to right, the slope of each edge of the Newton polygon for $F(x)$ is less than $1/k$.

The remainder of the proof now follows in a manner similar to that given for Lemma 2 in [5] which relies on the classical use of a theorem of Dumas [3] that the edges of the Newton polygon of a factor of $F(x)$ with respect to p must be able to be translated into the edges of the Newton polygon of $F(x)$ with respect to p. The edges in the Newton polygon of $F(x)$ having slope $< 1/k$ implies that the lattice points along the edges with positive slope are separated by a horizontal distance $> k$. The remaining edges with 0 or negative slope have endpoints among the spots $(j, \nu(b_{n-j}))$ with $j \in \{0, 1, \ldots, k-1\}$. This implies that $F(x)$ cannot have a factor of degree k. $\square$

3 The second preliminary result

In this section, we establish

Lemma 2. *Let n be an integer ≥ 6, and let k be an integer in $[3, n/2]$. Then*

$$\prod_{\substack{p^r \| (n+1)n(n-1)\cdots(n-k+2) \\ p \geq k+2}} p^r > n+1$$

unless one of the following holds:

$$\begin{array}{lcl}
n = 11 & \textit{and} & k = 5 \\
n = 26 & \textit{and} & k = 4 \\
n = 17 & \textit{and} & k = 4 \\
n = 11 & \textit{and} & k = 4 \\
n = 10 & \textit{and} & k = 4 \\
n = 9 & \textit{and} & k = 4 \\
n = 8 & \textit{and} & k = 4 \\
n = 17 & \textit{and} & k = 3 \\
n = 9 & \textit{and} & k = 3 \\
n = 8 & \textit{and} & k = 3 \\
n = 7 & \textit{and} & k = 3.
\end{array}$$

For the proof of this lemma, we will make use of the following result of Ecklund, Eggleton, Erdős, and Selfridge[4].

Lemma 3. *Let n and k denote positive integers with $2 \le k \le n/2$. Set $\binom{n+1}{k} = UV$ where the prime factors of U are all $\le k$ and the prime factors of V are all $\ge k+1$. If $k \notin \{3,5,7\}$ and $U > V$, then $(n,k) \in S$ where*

$$S = \{(8,4),(20,8),(32,13),(32,14),(35,13),(35,17),(55,13)\}.$$

Proof of Lemma 2. Observe that

$$\prod_{\substack{p^r \| (n+1)n(n-1)\cdots(n-k+2) \\ p \ge k+2}} p^r = \prod_{\substack{p^r \| \binom{n+1}{k} \\ p \ge k+2}} p^r.$$

Initially, suppose $q = k+1$ is a prime. Then q divides at most 1 of the k consecutive numbers $n+1, n, n-1, \dots, n-k+2$. We let s be the integer such that $q^s \| \binom{n+1}{k}$. Since q divides at most 1 of the numbers $n+1, n, n-1, \dots, n-k+2$, we obtain $q^s \le n+1$. Thus,

$$(n+1) \prod_{\substack{p^r \| \binom{n+1}{k} \\ p \ge k+2}} p^r \ge q^s \prod_{\substack{p^r \| \binom{n+1}{k} \\ p \ge k+2}} p^r = \prod_{\substack{p^r \| \binom{n+1}{k} \\ p \ge k+1}} p^r. \tag{1}$$

Note that the left-hand side of (1) is still at least the right-hand side of (1) if $k+1$ is not a prime. We will make use of this inequality then independent of whether $k+1$ is prime.

We consider $k \in [3, n/2]$. We will show next that, for $k \ge 6$, $k \ne 7$, and $n \ge 33$,

$$\prod_{\substack{p^r \| \binom{n+1}{k} \\ p \ge k+1}} p^r > (n+1)^2. \tag{2}$$

Then, by combining (1) and (2),

$$\prod_{\substack{p^r \| \binom{n+1}{k} \\ p \geq k+2}} p^r > n+1 \tag{3}$$

which will establish Lemma 2 for $k \geq 6$, $k \neq 7$, and $n \geq 33$.

Claim 1: For $n \geq 33$ and $k \geq 6$, $\displaystyle\binom{n+1}{k} > (n+1)^4$.

Since $n/2 \geq k \geq 6$, $\binom{n+1}{k} \geq \binom{n+1}{6}$. It suffices therefore to show that

$$(n+1)n(n-1)(n-2)(n-3)(n-4) > 720(n+1)^4.$$

Dividing by $n+1$ and rearranging, the above inequality is equivalent to

$$\begin{aligned}(n+2)&(n^4 - 12n^3 - 661n^2 - 888n - 360) \\ &= n^5 - 10n^4 - 685n^3 - 2210n^2 - 2136n - 720 > 0.\end{aligned}$$

Descartes's Rule of Signs implies that $h(x) = x^4 - 12x^3 - 661x^2 - 888x - 360$ has only one positive real zero. Since $h(32) = -50280 < 0$ and $h(33) = 5184 > 0$, the claim is easily seen to follow.

Set $\binom{n+1}{k} = UV$ where the prime factors of U are all $\leq k$ and the prime factors of V are all $\geq k+1$. By Lemma 3 for $k \geq 6$, $k \neq 7$ and $(n,k) \notin S$, $U \leq V$. Thus,

$$\binom{n+1}{k} = UV \leq V^2 \implies V \geq \sqrt{\binom{n+1}{k}}.$$

By Claim 1, $\binom{n+1}{k} > (n+1)^4$ with k as above and $n \geq 33$. Therefore,

$$\prod_{\substack{p^r \| \binom{n+1}{k} \\ p \geq k+1}} p^r = V \geq \sqrt{\binom{n+1}{k}} > (n+1)^2.$$

Thus, (2) and, hence, (3) follow for $k \geq 6$, $k \neq 7$, $n \geq 33$, and $(n,k) \notin \{(35,13),(35,17),(55,13)\}$. We check directly that (3) also holds for $(n,k) \in \{(35,13),(35,17),(55,13)\}$.

Claim 2: For $n \geq 34$, $\displaystyle\prod_{\substack{p^r \| \binom{n+1}{7} \\ p \geq 9}} p^r > n+1$.

To establish this claim, we consider

$$T = \{n+1, n, n-1, n-2, n-3, n-4, n-5\}.$$

Remove from T an integer divisible by the largest possible power of 2, an integer divisible by the largest possible power of 3, an integer divisible by the largest possible power of 5, and an integer divisible by the largest possible power of 7. Some of these integers may be the same, but at least three integers remain. Let a, b, and c denote integers that are not removed. Only one of the seven numbers in T is divisible by 7, and this number was removed; thus, $7 \nmid abc$. At most two of the seven numbers are divisible by 5, and one divisible by the largest possible power of 5 was removed; thus, $25 \nmid abc$. Similarly, $3^3 \nmid abc$ and $2^5 \nmid abc$. So

$$\prod_{\substack{p^r \| \binom{n+1}{7} \\ p \geq 9}} p^r \geq \frac{abc}{5 \times 9 \times 16} \geq \frac{(n-3)(n-4)(n-5)}{5 \times 9 \times 16}.$$

One checks that

$$\frac{(n-3)(n-4)(n-5)}{5 \times 9 \times 16} > n+1 \iff n^3 - 12n^2 - 673n - 780 > 0.$$

Set $h(x) = x^3 - 12x^2 - 673x - 780$. By Descartes's Rule of Signs, $h(x)$ has only one positive real root. Since $h(33) < 0$ and $h(34) > 0$, $h(n) > 0$ for $n \geq 34$. Claim 2 follows.

Claim 3: For $n \geq 30$, $\displaystyle\prod_{\substack{p^r \| \binom{n+1}{5} \\ p \geq 7}} p^r > n+1$.

The argument is similar to the argument given for Claim 2. Let

$$T = \{n+1, n, n-1, n-2, n-3\}.$$

Remove from T an integer divisible by the largest possible power of 2, an integer divisible by the largest possible power of 3, and an integer divisible by the largest possible power of 5. Again, some of these numbers may be the same, but at least two numbers remain, say a and b. Thus, $ab \geq (n-2)(n-3)$. Also, $5 \nmid ab$, $3^2 \nmid ab$, and $2^4 \nmid ab$. We obtain that

$$\prod_{\substack{p^r \| \binom{n+1}{5} \\ p \geq 7}} p^r \geq \frac{ab}{3 \times 8} \geq \frac{(n-2)(n-3)}{24} > n+1$$

provided $n^2 - 29n - 18 > 0$. The latter inequality is easily deduced for $n \geq 30$, implying the claim.

Claim 4: For $n \geq 12$ with $n \notin \{17, 26\}$, $\displaystyle\prod_{\substack{p^r \| \binom{n+1}{4} \\ p \geq 6}} p^r > n+1$.

We begin in a similar manner to the previous arguments. Let T denote the set $\{n+1, n, n-1, n-2\}$, and remove an integer divisible by the largest possible power of 2, an integer divisible by the largest possible power of 3, and an integer divisible by the largest possible power of 5. At least one integer remains, say a. Let b, c, d denote the other three integers. An argument similar to Claim 2 and Claim 3 would give

$$\prod_{\substack{p^r \| \binom{n+1}{4} \\ p \geq 6}} p^r \geq \frac{a}{6} \geq \frac{n-2}{6}.$$

The above inequality is not strong enough. We modify the argument establishing the lemma, by considering two cases.

First, we suppose one of the numbers b, c, or d is divisible by a prime $q \geq 7$. In this case, one gets an extra factor of 7 above so that the product is at least $7(n-2)/6$. One checks that this is greater than $n+1$ for $n \geq 21$, establishing the claim in this case for $n \geq 21$.

Next, we suppose $p \nmid bcd$ for each prime $p \geq 7$; that is, b, c, and d are divisible only by the primes 2, 3, and 5. At most one of b, c, and d is divisible by 5. Let b and c denote two that are not. Thus, the only prime divisors of b and c are 2 and 3 and both b and c occur among $\{n+1, n, n-1, n-2\}$. It follows that one of $\{b, c\}$, $\{b/2, c/2\}$, and $\{b/3, c/3\}$ consists of two consecutive integers, one a power of two and one a power of three. We use that the only pairs of such consecutive positive integers are $(1, 2)$, $(2, 3)$, $(3, 4)$, and $(8, 9)$; this is a result due to G. C. Gerono in 1857 (see [2]). For $n \geq 12$ as in the claim, this leads to only three possibilities for n, namely $n = 17$, $n = 18$, and $n = 26$.

Given the two cases just considered, the full strength of the claim follows by a direct calculation of the product for $12 < n \leq 20$.

Claim 5: For $n \geq 6$, $\displaystyle\prod_{\substack{p^r \| \binom{n+1}{3} \\ p \geq 5}} p^r > n+1$ unless $n \in \{7, 8, 9, 17\}$.

This claim is established along lines similar to the previous claim. We omit the details.

We combine the information just obtained. The inequality in Lemma 2 follows with the indicated exceptions by a computation. More specifically, for $5 \leq k \leq n/2$ and $10 \leq n \leq 33$, the inequality was checked and the only case in these ranges where the inequality did not hold was for $k = 5$ and $n = 11$. The exceptions to the inequality given in Lemma 2, which arise when combining the claims above, are easily checked to in fact not satisfy the inequality of Lemma 2. This completes the proof of that lemma. □

4 The elimination of possible degrees of factors

We first show the following result.

Result 1. *For $0 < |a_n| < M(n)$, $f(x)$ cannot have a factor of degree k in $[3, n/2]$, where $M(n)$ is as given in Theorem 2. Furthermore, if $0 < |a_n| \leq n+1$, then $f(x)$ cannot have a factor of degree k in $[3, n/2]$ except possibly if*

$(n,k) \in \mathcal{S}$ *where*

$$\mathcal{S} = \{(11,5),(26,4),(17,4),(11,4),(10,4),\\ (9,4),(8,4),(17,3),(9,3),(8,3),(7,3)\}.$$

The set $\mathcal{S}$ corresponds to the list of exceptions given in Lemma 2. Assume that $f(x)$ has a factor of degree k in $[3, n/2]$. Lemma 1 implies that

$$\prod_{\substack{p^r \| (n+1)n(n-1)\cdots(n-k+2) \\ p \geq k+2}} p^r \leq |a_n|. \tag{4}$$

If $(n,k) \notin \mathcal{S}$, we deduce from Lemma 2 that $|a_n| > n+1$. Suppose now that $(n,k) \in \mathcal{S}$. Using direct computations, we checked that for $(n,k) \in \mathcal{S}$ the inequality

$$\prod_{\substack{p^r \| (n+1)n(n-1)\cdots(n-k+2) \\ p \geq k+2}} p^r \geq M$$

holds. We deduce then that $|a_n| \geq M$ and Result 1 follows.

Recall that $n+1 = k'2^u$ where u is an integer ≥ 0 and $(k',2) = 1$. Also, $(n+1)n = k''2^v3^w$ where v is an integer ≥ 1 and w is an integer ≥ 0 and $(k'',6) = 1$. Since $M = \min\{k', k''\}$, the following results imply $f(x)$ cannot have a quadratic or linear factor for $0 < |a_n| < M$.

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

Result 3. *If* $0 < |a_n| < k''$*, then* $f(x)$ *cannot have a quadratic factor.*

The proofs of these two results are straight forward. They follow as a consequence of (4) holding for $k = 1$ and 2 and since the product on the left of (4) is simply k' in the case $k = 1$ and k'' in the case $k = 2$.

5 Reducible examples

Finally, we show that for every $n > 2$, if $|a_n| = M(n) = \min\{k', k''\}$ and $|a_0| = 1$, then there exist integers $a_{n-1}, a_{n-2}, \ldots, a_1$ such that $f(x)$ is reducible. In particular, we will show the following:

- If $|a_n| = k'$ and $|a_0| = 1$, then $a_{n-1}, a_{n-2}, \ldots, a_1$ can be chosen such that $x+2$ (or $x-2$) is a factor of $f(x)$.
- If $|a_n| = k'' < k'$ and $|a_0| = 1$, then $a_{n-1}, a_{n-2}, \ldots, a_1$ can be chosen such that $x^2 - 3x - 6$ is a factor of $f(x)$.

Note that when $n = 2$, then $f(x)$ is a quadratic polynomial. It follows from Result 2 that $f(x)$ is irreducible for $0 < |a_n| < 3$ and $|a_0| = 1$. Furthermore, by our first construction below, when $|a_n| = 3$ and $|a_0| = 1$, a_1 can be chosen so the $x + 2$ (or $x - 2$) is a factor of $f(x)$. This justifies our final remarks in the introduction concerning $M(2)$.

For our arguments, we will make use of the following result which can be found in [1].

Lemma 4. *Let n be a positive integer, and let p be a prime. Then*

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

where $s_p(n)$ denotes the sum of the base p digits of n.

First we show that there exist integers $a_{n-1}, a_{n-2}, \dots, a_1$ such that $x + 2$ or $x - 2$ (whichever we choose) is a factor of $f(x)$ when $|a_n| = k'$ and $|a_0| = 1$. Let $a_n = k'$, $a_0 = 1$, and $a_{n-2} = a_{n-3} = \cdots = a_2 = 0$ (the cases $a_n = -k'$ or/and $a_0 = -1$ can be treated similarly). Then

$$(n+1)!f(x) = k'x^n + a_{n-1}c_{n-1}x^{n-1} + a_1c_1x + c_0,$$

where $c_{n-1} = n + 1 = k'2^u$, $c_0 = (n+1)!$, and $c_1 = c_0/2$. To establish that $f(\pm 2) = 0$ for some choice of integers a_{n-1} and a_1, it suffices to show that each of the equations

$$2^{n-1}c_{n-1}x + 2c_1y = 2^nk' \quad \text{and} \quad 2^{n-1}c_{n-1}x + 2c_1y = c_0$$

is solvable in integers x and y. The second of these is clearly solvable with $x = 0$ and $y = 1$. For the first, we use that the equation is solvable if and only if $\gcd(2^{n-1}c_{n-1}, 2c_1)$ divides $2^nk'$. As $c_{n-1} = 2^uk'$, it suffices to show $\nu_2(2c_1) \le n$. By Lemma 4,

$$\nu_2(2c_1) = \nu_2((n+1)!) = n + 1 - s_2(n+1) \le n,$$

so the existence of a_{n-1} and a_1 as above follows.

Now, we consider the case that $|a_n| = k'' < k'$ and $|a_0| = 1$ and show how to obtain $x^2 - 3x - 6$ as a factor of $f(x)$. One checks that the condition $k'' < k'$ implies $2|n$ and $3|(n+1)$. Therefore, we consider $n = 2^km \ge 8$ and $n + 1 = 3^\ell m'$ where k, ℓ, m, and m' are positive integers and $\gcd(mm', 6) = 1$ (there is no restriction here on the size of mm'). We show that if $a_n = mm'$, then there exist integers $a_{n-1}, a_{n-2}, \dots, a_1$ such that the polynomial

$$a_n\frac{x^n}{(n+1)!} + a_{n-1}\frac{x^{n-1}}{n!} + \cdots + a_1\frac{x}{2!} + 1$$

is divisible by the quadratic $q(x) = x^2 - 3x - 6$ (the cases $a_n = -mm'$ or/and $a_0 = -1$ can be treated similarly). To do this, we multiply the polynomial of degree n above by $(n+1)!$, replace a_n with mm', and divide through by mm' to obtain the polynomial

$$x^n + 3^\ell\frac{a_{n-1}}{m}x^{n-1} + 3^\ell 2^k a_{n-2}x^{n-2} + \cdots$$

$$+ 3^{\ell-1}2^{k-1}(n-1)!a_2x^2 + 3^{\ell}2^{k-1}(n-1)!a_1x + 3^{\ell}2^{k}(n-1)!.$$

Take $a_{n-1} = mr$, $a_{n-2} = s$, $a_{n-3} = a_{n-4} = \cdots = a_3 = 0$, $a_2 = -y$, and $a_1 = w + y$ and rewrite this polynomial as

$$g(x) = x^n + 3^{\ell}rx^{n-1} + 3^{\ell}2^{k}sx^{n-2} - 3^{\ell-1}2^{k-1}(n-1)!yx^2 + 3^{\ell}2^{k-1}(n-1)!(w+y)x + 3^{\ell}2^{k}(n-1)!.$$

It suffices now to show that there exist integers r, s, y, and w such that $g(x)$ is divisible by $q(x)$.

For $j \geq 0$, define integers c_j and b_j by

$$x^j \equiv c_j + b_jx \pmod{q(x)}.$$

Note that for $j \geq 1$ we have

(5) $$x^{j+1} \equiv 3x^j + 6x^{j-1} \pmod{q(x)}.$$

It follows that, for $j \geq 1$, we have

(6) $$c_{j+1} = 3c_j + 6c_{j-1} \qquad \text{and} \qquad b_{j+1} = 3b_j + 6b_{j-1}.$$

Letting

$$A = \begin{pmatrix} 0 & 1 \\ 6 & 3 \end{pmatrix},$$

we obtain from (6) and an induction argument that, for each $j \geq 0$, we have

$$A^j = \begin{pmatrix} c_j & b_j \\ c_{j+1} & b_{j+1} \end{pmatrix}.$$

Next, we obtain some results concerning the values of $\nu_2(c_j)$, $\nu_2(b_j)$, $\nu_3(c_j)$, and $\nu_3(b_j)$. An induction argument gives that, for $j > 1$, we have

$$A^j \equiv \begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix} \pmod{4}.$$

Hence, it follows that, for $j > 1$, we have

(7) $$\nu_2(c_j) = 1 \qquad \text{and} \qquad \nu_2(b_j) = 0.$$

We claim that for all $j \geq 0$ we have

(8) $$\nu_3(c_j) \geq \frac{j}{2} \qquad \text{and} \qquad \nu_3(b_j) \geq \frac{j-1}{2}.$$

For $j = 0$ and $j = 1$, one checks directly that (8) holds. From (6), we deduce

$$\nu_3(c_{j+1}) \geq \min\{\nu_3(c_j), \nu_3(c_{j-1})\} + 1$$

and

$$\nu_3(b_{j+1}) \geq \min\{\nu_3(b_j), \nu_3(b_{j-1})\} + 1.$$

An easy induction argument implies (8) holds. Using that $\det(A^j) = \det(A)^j$, we obtain

$$c_j b_{j+1} - c_{j+1} b_j = \pm 6^j. \tag{9}$$

Given (8), we deduce that, for $j \geq 0$, at least one of $\nu_3(c_j) = j/2$ and $\nu_3(c_{j+1}) = (j+1)/2$ holds. Only one of $j/2$ and $(j+1)/2$ can be an integer. It follows that

$$\nu_3(c_j) = \frac{j}{2} \quad \text{if } j \text{ is even}. \tag{10}$$

Note that parity considerations also imply from (8) that $\nu_3(c_j) \geq (j+1)/2$ if j is odd and that $\nu_3(b_j) \geq j/2$ if j is even.

Observe that $x^2 \equiv 3x + 6 \pmod{q(x)}$. We obtain from the definition of c_n and b_n that

$$\begin{aligned} g(x) \equiv \big(b_n + 3^\ell r b_{n-1} + 3^\ell 2^k s b_{n-2} + 3^\ell 2^{k-1} w (n-1)!\big) x \\ + c_n + 3^\ell r c_{n-1} + 3^\ell 2^k s c_{n-2} + 3^\ell 2^k (n-1)!(1-y) \end{aligned}$$

modulo $q(x)$. We will show that for some r, s, y, and w,

$$c_n + 3^\ell r c_{n-1} + 3^\ell 2^k s c_{n-2} + 3^\ell 2^k (n-1)!(1-y) = 0$$

and

$$b_n + 3^\ell r b_{n-1} + 3^\ell 2^k s b_{n-2} + 3^\ell 2^{k-1} w (n-1)! = 0.$$

It will follow then that, $g(x) \equiv 0 \pmod{q(x)}$. We first show that there are integers r, s, and y such that

$$3^\ell r c_{n-1} + 3^\ell 2^k s c_{n-2} = -(c_n + 3^\ell 2^k (n-1)!(1-y)).$$

The above equation has integer solutions r and s if

$$\gcd(3^\ell c_{n-1}, 3^\ell 2^k c_{n-2}) \mid (c_n + 3^\ell 2^k (n-1)!(1-y)).$$

Since $n+1 = 3^\ell m'$ and, from Lemma 4, $\nu_3((n+1)!) < (n+1)/2$, we obtain $\nu_3(3^\ell 2^k (n-1)!) \leq n/2$. Also since n is even, (10) implies $\nu_3(c_n) = n/2$. It follows that there is an integer y such that

$$\nu_3\big(c_n + 3^\ell 2^k (n-1)!(1-y)\big) \geq \min\{\nu_3(3^\ell c_{n-1}), \nu_3(3^\ell c_{n-2})\}.$$

Fix such a y. From (7) and $k \geq 1$, we obtain

$$\nu_2\big(c_n + 3^\ell 2^k (n-1)!(1-y)\big) \geq \min\{\nu_2(3^\ell c_{n-1}), \nu_2(3^\ell 2^k c_{n-2})\}.$$

Note that (9) implies that 2 and 3 are the only prime factors possibly in common with c_{n-1} and c_{n-2}. It follows that there are integers r_0 and s_0 such that

$$c_n + 3^\ell r_0 c_{n-1} + 3^\ell 2^k s_0 c_{n-2} + 3^\ell 2^k (n-1)!(1-y) = 0. \tag{11}$$

We will use later that r_0 is odd which follows from (7), the above equation, and the fact that $k \geq 1$ and $n \geq 3$. We fix r_0 and s_0 (and y) as above and note that for any integer t we have

$$c_n + 3^\ell c_{n-1}\big(r_0 + 2^k c_{n-2} t\big) + 3^\ell 2^k c_{n-2}\big(s_0 - c_{n-1} t\big) + 3^\ell 2^k (n-1)!(1-y) = 0.$$

We set

$$r = r_0 + 2^k c_{n-2} t \qquad \text{and} \qquad s = s_0 - c_{n-1} t$$

and seek t and w so that

$$b_n + 3^\ell r b_{n-1} + 3^\ell 2^k s b_{n-2} + 3^\ell 2^{k-1} w (n-1)! = 0.$$

In other words, we want

$$3^\ell 2^{k-1} w (n-1)! + 3^\ell 2^k \big(c_{n-2} b_{n-1} - c_{n-1} b_{n-2}\big) t \\ + b_n + 3^\ell r_0 b_{n-1} + 3^\ell 2^k s_0 b_{n-2} = 0.$$

By (6), we can rewrite this equation as

(12) $$3^\ell 2^{k-1} w (n-1)! + 3^\ell 2^k \big(c_{n-2} b_{n-1} - c_{n-1} b_{n-2}\big) t \\ + (3^\ell r_0 + 3) b_{n-1} + (3^\ell 2^k s_0 + 6) b_{n-2} = 0.$$

From (6) and (11), we obtain

(13) $$(3^\ell r_0 + 3) c_{n-1} + (3^\ell 2^k s_0 + 6) c_{n-2} + 3^\ell 2^k (n-1)!(1-y) = 0.$$

Multiplying both sides of (12) by c_{n-2} and both sides of (13) by $-b_{n-2}$ and then adding, we obtain

(14) $$c_{n-2} 3^\ell 2^{k-1} (n-1)! w + c_{n-2} 3^\ell 2^k \big(c_{n-2} b_{n-1} - c_{n-1} b_{n-2}\big) t \\ + (3^\ell r_0 + 3)\big(c_{n-2} b_{n-1} - c_{n-1} b_{n-2}\big) - 3^\ell 2^k (n-1)!(1-y) b_{n-2} = 0.$$

Observe that (13) implies that if (14) holds, then so does (12).

We show that (14) holds for some integers w and t. Since $n = 2^k m$, with k a positive integer, n is even so that $\nu_3(c_{n-1}) \geq n/2$, $\nu_3(c_{n-2}) = (n-2)/2$, and $\nu_3(b_{n-2}) \geq (n-2)/2$. Let

$$c = c_{n-2} 3^\ell 2^{k-1} (n-1)!, \quad c' = c_{n-2} 3^\ell 2^k \big(c_{n-2} b_{n-1} - c_{n-1} b_{n-2}\big),$$

$$c'' = (3^\ell r_0 + 3)\big(c_{n-2} b_{n-1} - c_{n-1} b_{n-2}\big), \ \text{ and } \ c''' = 3^\ell 2^k (n-1)!(1-y) b_{n-2}.$$

Recall that $\nu_3\big(3^\ell 2^k (n-1)!\big) \leq n/2$. We deduce

$$\nu_3(c) \leq \frac{n}{2} + \frac{n-2}{2} = n - 1.$$

Observe that $\nu_2(n!) < n$ (for example, from Lemma 4). Since $n = 2^k m$, we have $\nu_2(2^{k-1}(n-1)!) = \nu_2(n!) - 1$. From (7), we see that $\nu_2(c) \le \nu_2(n!) < n$. Since $\nu_2(c)$ is an integer,

$$\nu_2(c) \le n - 1.$$

Note that 3 divides $3^\ell r_0 + 3$. Since r_0 is odd, 2 divides $3^\ell r_0 + 3$. We obtain from (9) that

$$\nu_2(c'') \ge n - 1 \qquad \text{and} \qquad \nu_3(c'') \ge n - 1.$$

Observe that (7) implies $\nu_2(c''') \ge \nu_2(c)$. Next, we show that $\nu_3(c''') \ge \nu_3(c)$. Recall that since n is even,

$$\nu_3(b_{n-2}) \ge (n-2)/2 = \nu_3(c_{n-2}).$$

So,

$$\nu_3(c''') = \nu_3(3^\ell 2^k (n-1)!(1-y)b_{n-2}) \ge \nu_3(c_{n-2} 3^\ell 2^{k-1}(n-1)!) = \nu_3(c).$$

Combining the above, we deduce

$$\nu_2(c''' - c'') \ge \nu_2(c) \qquad \text{and} \qquad \nu_3(c''' - c'') \ge \nu_3(c).$$

We claim that $\gcd(c, c')$ divides $c''' - c''$. Let p be a prime and u a positive integer for which $p^u || \gcd(c, c')$. The above analysis shows that if $p = 2$ or $p = 3$, then $p^u | (c''' - c'')$. Now, consider the case that $p > 3$. From (9) and the definition of c', we obtain that $p^u | c_{n-2}$. From (13), we see that p^u must also divide

$$\big((3^\ell r_0 + 3)c_{n-1} + 3^\ell 2^k (n-1)!(1-y)\big)b_{n-2} - (3^\ell r_0 + 3)c_{n-2}b_{n-1} = c''' - c''.$$

Hence, $\gcd(c, c')$ divides $c''' - c''$.

It now follows that there exist integers w and t for which $cw + c't = c''' - c''$. This establishes the existence of integers w and t as in (12) and (14) and, hence, the existence of integers r, s, y, and w for which $g(x)$ is divisible by $x^2 - 3x - 6$.

Comment: The above argument for the case $k'' < k'$ is hampered somewhat by the presence of a non-zero coefficient of x in our choice of $g(x)$. It can be shown, however, that there are n (for example, $n = 32$) for which $k'' < k'$ and for which $f(x)$, with $|a_n| = k'$ and $|a_0| = 1$, has no factors $ax^2 + c \in \mathbb{Z}[x]$ regardless of the integral values chosen for $a_1, a_2, \ldots, a_{n-1}$.

References

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

[2] L. E. Dickson, *History of the Theory of Numbers, Vol. II*, Chelsea, New York, 1971, 744.

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

[4] E. F. Ecklund, JR., R. B. Eggleton, P. Erdős, and J. L. Selfridge, *On the prime factorization of binomial coefficients*, J. Austral. Math. Soc. (Series A) 26 (1978), 257–269.

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

[6] Michael Filaseta, *A generalization of an irreducibility theorem of I. Schur*, Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam, Volume 1, edited by B. C. Berndt, H. G. Diamond, and A. J. Hildebrand, Birkhäuser, Boston, 1996, 371–395.

[7] Michael Filaseta and Ognian Trifonov, *The Irreducibility of the Bessel polynomials*, Journal für die reine und angewandte Mathematik, to appear.

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

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

Dept. of Mathematics and Computer Science
Georgia College and State University
Milledgeville, GA 31061
allenm@mail.gcsu.edu
http://turing.gcsu.edu/˜mallen/

Mathematics Department
University of South Carolina
Columbia, SC 29208
filaseta@math.sc.edu
http://www.math.sc.edu/˜filaseta/