ACTA ARITHMETICA
114.2 (2004)

A generalization of a third irreducibility theorem of I. Schur

by

Martha Allen (Milledgeville, GA) and
Michael Filaseta (Columbia, SC)

1. Introduction. For each nonnegative integer j, define u_j as the product of the odd numbers $\le j$. In particular, we have $u_0 = u_2 = 1$, $u_4 = 3$, $u_6 = 15, \ldots$ The purpose of this paper is to establish the following.

Theorem 1. *Let n be an integer > 1, and let $a_0, a_1, \ldots, a_n$ be arbitrary integers with $a_0 = \pm 1$ and $0 < |a_n| < 2n - 1$. Then*

$$f(x) = \sum_{j=0}^{n} a_j \frac{x^{2j}}{u_{2j}} \tag{1}$$

is irreducible over the rationals.

I. Schur (in [10]) obtained this result in the special case that $a_n = \pm 1$ and used it to establish the irreducibility of $H_{2n}(x)$ where $H_m(x)$ is the mth Hermite polynomial. The result stated above is best possible in the sense that, for any integer $n > 1$, if $|a_n| = 2n - 1$, then there are values of $a_0, a_1, \ldots, a_n$ with $a_0 = \pm 1$ such that the polynomial $f(x)$ in (1) is reducible. Indeed, if $|a_n| = 2n - 1$ and $a_0 = \pm 1$, then one can take $a_{n-2} = a_{n-3} = \cdots = a_1 = 0$ and a_{n-1} to be one of the four numbers $\pm u_{2n-2} \pm 1$ to deduce that $f(x)$ is divisible by $x^2 - 1$ (or, if desired, by $x^2 + 1$). There are other examples of reducibility that can occur when $|a_n| = 2n - 1$. The polynomial $f(x)$ defined by

$$\begin{aligned} u_{12} f(x) &= 11x^{12} + 1188x^8 + 6930x^4 + 10395 \\ &= 11(x^4 + 3)(x^8 + 105x^4 + 315) \end{aligned}$$

is such an example. On the other hand, as will be evident from the proof, if $|a_n| = 2n - 1$ and $f(x)$ is reducible, then $f(x)$ must have a factor of degree ≤ 4.

2000 *Mathematics Subject Classification*: 12E05, 11C08, 11R09.

The authors are grateful to the National Science Foundation and the National Security Agency for funding during research for this paper. Research by the first author was done in partial fulfillment of the requirement for a Ph.D. at the University of South Carolina.

This work is continuation of earlier work by the authors in [5] and [1] in which the role of x^{2j}/u_{2j} above is replaced by $x^j/j!$ and $x^j/(j+1)!$, respectively. The conditions on a_n were different for these results, but in a manner similar to that just described, the results there were best possible. The general techniques used for establishing Theorem 1 are similar to those used in [1], [5] and [6]. The authors were not, however, able to take advantage of work by E. F. Ecklund, Jr., R. B. Eggleton, P. Erdős, and J. L. Selfridge [3] that played a crucial role in the prior two papers [5] and [1] on the subject. We note that there were four irreducibility theorems of I. Schur contained in [9] and [10]; the authors plan to address the fourth of these in a subsequent paper.

The rest of the paper is organized as follows. In the next three sections, we give preliminary results that will be essential for our arguments. The second section focuses on those results which are already established in the literature, and the third section on a certain technical lemma that will play a role in the fourth section. The fourth section gives two crucial lemmas for our arguments; indeed, they imply immediately that $f(x)$ as in Theorem 1 cannot have a factor of degree $d \in [1, n]$ and $d \notin \{3, 4\}$ except possibly for seven pairs (n, d). Finally, the fifth section completes the proof of Theorem 1, handling these seven pairs (n, d) together with an analysis for $d \in \{3, 4\}$.

2. Preliminary material. In this section, we give some background results which already appear in the literature or are easily derived from it. As this is the case, the results in this section will be stated without proof.

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 leftmost endpoint is $(0, \nu(a_n))$ and the rightmost 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* in the construction of the Newton polygon.

In investigating irreducibility with Newton polygons, we will make use of the following result due to Dumas [2].

LEMMA 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 k be a nonnegative integer such that p^k divides the leading coef-*

ficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon for $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0,k)$ and using translates of the edges in the Newton 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.

We will make use of the following estimate, which can be found in [8], for $\pi(x)$, the number of primes $\leq x$.

LEMMA 2. *The inequality*

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

holds for all $x > 1$.

The next lemma deals with gaps between primes.

LEMMA 3. *For $x \geq 2479$, there is a prime in the interval $(x, 1.01x]$; and for $x \geq 213$, there is a prime in the interval $(x, 1.05x]$.*

The first result in Lemma 3 with intervals $(x, 1.01x]$ is obtained in [6] by making direct use of estimates like Lemma 2 above from [8]. A proof of the second result follows by noting $[1.05 \cdot 213] = 223$ is prime and by simply checking the lengths of the gaps between primes in the interval $[223, 2503]$ (the number 2503 is the smallest prime > 2479).

In addition, we will make use of the following consequence of work by D. H. Lehmer [7].

LEMMA 4. *Let m be an odd positive integer. If $m > 7$ and $m \notin \{25, 243\}$, then there is a prime $p \geq 11$ dividing $m(m+2)$. If $m > 5$ and $m \notin \{21, 45\}$, then there is a prime $p \geq 11$ dividing $m(m+4)$.*

In particular, we note that this lemma implies that the product of three consecutive odd numbers each ≥ 7 must be divisible by a prime ≥ 11. This particular use of the lemma is an easy consequence of prior work by Schur [10].

3. A technical lemma. Here, we establish the following:

LEMMA 5. *Let m, l, and k denote positive integers with $k \geq 2$, and let*

$$T = \{2m+1, 2m+3, \ldots, 2m+2l-1\}.$$

For each odd prime $p \leq k$ in turn, remove from T a number divisible by p^e where $e = e(p)$ is as large as possible. Let S denote the set of numbers that are left. Let N_p be the exponent in the largest power of p dividing $\prod_{t \in S} t$.

Then

$$\prod_{p>k} p^{N_p} = \frac{\prod_{t\in S} t}{\prod_{2<p\le k} p^{N_p}} \ge \frac{(2m+1)^{l-\pi(k)+1}}{(l-1)!} \cdot 2^{\nu_2((l-1)!)}.$$

Before turning to the proof, we remark that our intent above is for a different element of T to be selected for each odd prime $p \le k$. One constructs S by taking these primes one at a time in any order and removing from whatever elements of T still remain an element which is divisible by the largest power of the prime. If instead one considers each odd prime p and chooses a u_p in T divisible by as large a power of p as possible, allowing for repetition in the u_p, and defines S as the set T with the u_p removed, the estimate given in Lemma 5 is still valid. In fact, the only real reason in this paper to not allow for repetition in Lemma 5 is that it gives a stronger result which implies the analogous result with repetition.

Proof. The proof is based on an idea of Erdős [4]. Clearly, $|S| = l - \pi(k) + 1$ so that

$$\prod_{t\in S} t \ge (2m+1)^{l-\pi(k)+1}.$$

It remains to estimate $\prod_{2<p\le k} p^{N_p}$. First suppose that $l \le p \le k$. Note that since T is a set of l consecutive odd numbers, at most one element of T is divisible by p. However, any such number is not in S since it would have been one of the numbers removed from T to form S. Thus,

$$\prod_{2<p\le k} p^{N_p} = \prod_{2<p\le \min\{k,l-1\}} p^{N_p} \le \prod_{2<p\le l-1} p^{N_p}.$$

Denote by a_p an element of T that was removed with $\nu_p(a_p)$ maximal. For $1 \le j \le \nu_p(a_p)$, let $s+1$ denote the number of elements of T divisible by p^j. Since a_p was removed from T, we deduce that there are $\le s$ elements of S divisible by p^j. Observe that

$$2m+1+2sp^j \le 2m+2l-1 \quad \text{so that} \quad s \le \left[\frac{l-1}{p^j}\right].$$

We deduce that

$$N_p \le \sum_{j=1}^{\infty} \left[\frac{l-1}{p^j}\right] = \nu_p((l-1)!).$$

Thus,

$$(l-1)! = 2^{\nu_2((l-1)!)} \prod_{2<p\le l-1} p^{\nu_p((l-1)!)} \ge 2^{\nu_2((l-1)!)} \prod_{2<p\le l-1} p^{N_p},$$

and the result follows. ∎

4. Two further lemmas. In this section, we establish the following results concerning $f(x)$ as in (1).

LEMMA 6. *Let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = 1$, and let*

$$f(x) = \sum_{j=0}^{n} a_j \frac{x^{2j}}{u_{2j}}.$$

Let k be a positive odd integer $\le n$. Suppose there exists a prime $p \ge k+2$ and a positive integer r for which

$$p^r \mid (2n-1)(2n-3)\cdots(2n-k) \quad \text{and} \quad p^r \nmid a_n.$$

Then $f(x)$ cannot have a factor of degree k and cannot have a factor of degree $k+1$.

LEMMA 7. *Let n be an integer ≥ 3, and let k be an odd integer in $[3, n]$. Then*

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

unless one of the following conditions holds:

(1) $k = 3$ *and either* $2n-1$ *or* $2n-3$ *is a power of* 3,
(2) $k = 5$ *and* $n \in \{5, 14, 15\}$,
(3) $k = 7$ *and* $n = 14$.

Proof of Lemma 6. This argument is based on the proof of Lemma 1 in [5]. To prove that $f(x)$ cannot have a factor of degree k or $k+1$, it suffices to show that $F(x) = u_{2n} f(x)$ cannot have a factor of degree k or $k+1$. For l an odd positive integer, define $b_{2n-l} = 0$ and

$$b_{2n-(l+1)} = a_{(2n-(l+1))/2}(2n-1)(2n-3)\cdots(2n-l+2)(2n-l).$$

Then

$$F(x) = u_{2n} f(x) = \sum_{j=0}^{n} a_j \frac{u_{2n}}{u_{2j}} x^{2j} = \sum_{i=0}^{2n} b_i x^i.$$

Note that the condition $p^r \mid (2n-1)(2n-3)\cdots(2n-k)$ implies that $p^r \mid b_i$ for $i \in \{0, 1, 2, \ldots, 2n-k\}$. Thus, the $2n-k+1$ rightmost spots,

$$(k, \nu(b_{2n-k})), \ldots, (2n-1, \nu(b_1)), (2n, \nu(b_0)),$$

associated with the Newton polygon of $F(x)$ with respect to p have y-coordinates $\ge r$. Consider the leftmost endpoint $(0, \nu(a_n))$. By the given, $p^r \nmid a_n$; thus, the y-coordinate of the leftmost endpoint is $< r$.

Recall that the slopes of the edges of the Newton polygon of $F(x)$ increase from left to right. Thus, the spots $(i, \nu(b_{2n-i}))$ for $i \in \{k-1, k, k+1, \ldots, 2n\}$

all lie on or above edges of the Newton polygon which have positive slope. We will show that each of these positive slopes is $< 1/(k+1)$. Since the slopes of the edges of the Newton polygon increase from left to right, it suffices to show that the rightmost edge has slope $< 1/(k+1)$. Observe that the slope of the rightmost edge is given by

$$\max_{1\le j\le n}\left\{\frac{\nu(a_0u_{2n})-\nu(a_ju_{2n}/u_{2j})}{2j}\right\}.$$

Using the fact that $\nu((2j-1)!) < (2j-1)/(p-1)$, for $1 \le j \le n$ we obtain

$$\nu(a_0u_{2n})-\nu\left(a_j\,\frac{u_{2n}}{u_{2j}}\right) \le \nu(u_{2n})-\nu(u_{2n}/u_{2j}) = \nu(u_{2j})$$

$$\le \nu((2j-1)!) < \frac{2j-1}{p-1}.$$

As $p \ge k+2$, we deduce

$$\max_{1\le j\le n}\left\{\frac{\nu(a_0u_{2n})-\nu(a_ju_{2n}/u_{2j})}{2j}\right\} < \frac{1}{p-1} \le \frac{1}{k+1}.$$

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

Now suppose $F(x)$ has a factor $g(x) \in \mathbb{Z}[x]$ with $\deg g(x) \in \{k, k+1\}$. By Lemma 1, the Newton polygon of $F(x)$ with respect to p must include translations of the edges of the Newton polygon of $g(x)$ with respect to p. Suppose (a,b) and (c,d) with $a<c$ are two lattice points on an edge of the Newton polygon of $F(x)$ having positive slope. Since the slope is $< 1/(k+1)$, we obtain

$$\frac{1}{c-a} \le \frac{d-b}{c-a} < \frac{1}{k+1}.$$

Thus, $c-a > k+1 \ge \deg g(x)$ so that (a,b) and (c,d) cannot be the endpoints of a translated edge of the Newton polygon of $g(x)$. Therefore, the translates of the edges of the Newton polygon of $g(x)$ with respect to p must be among the edges of the Newton polygon of $F(x)$ having 0 or negative slope. On the other hand, the endpoints of the edges of the Newton polygon of $F(x)$ having 0 or negative slope must be among the spots $(i, \nu(b_{2n-i}))$ for $i \in \{0,1,\dots,k-1\}$. Since $k-1 < \deg g(x)$, these edges by themselves cannot consist of a complete collection of translated edges of the Newton polygon of $g(x)$, and so we have a contradiction. Thus, $F(x)$ cannot have a factor with degree k or $k+1$. ∎

The proof of Lemma 7 is a bit more involved. In the prior work of [1] and [5], we were able to take advantage of a result by Ecklund, Eggleton, Erdős, and Selfridge [3] in which a similar product is considered over p dividing instead a product of k consecutive integers. We are no longer able to

appeal to this result and instead establish Lemma 7 based on other estimates in the distribution of primes. Our approach here is nevertheless similar to that given in [3].

Proof of Lemma 7. Let k be as in the statement of the lemma (so k is odd), and set $c = n/k$. Define v to be the product appearing in the lemma, and let u be defined by

$$(2n-1)(2n-3)\cdots(2n-k) = uv.$$

Thus, u is a product of primes each $\leq k$. To establish Lemma 7, we will consider the following five cases: (i) $c \geq 25$ and $k \geq 1001$, (ii) $1 \leq c \leq 25$ and $k \geq 1001$, (iii) $n \geq 999$ with $9 \leq k \leq 999$, (iv) $k \in \{3, 5, 7\}$ and $k \leq n$, and (v) $n \leq 998$ with $9 \leq k \leq n$. In the first four cases, we establish Lemma 7 by showing $v > 2n$, and in the last case we will base our argument largely on computations.

Case (i). Consider $c \geq 25$ and $k \geq 1001$. To establish $v > 2n$, we show that $\log v > \log(2n)$. The definitions of u and v imply

$$\log v = \log((2n-1)\cdots(2n-k)) - \log u.$$

We combine a lower bound for $\log((2n-1)\cdots(2n-k))$ with an upper bound for $\log u$ to obtain a lower bound for $\log v$.

Observe that

$$(2n-1)(2n-3)\cdots(2n-k) \geq (2n-k)^{(k+1)/2} = ((2c-1)k)^{(k+1)/2}.$$

One checks that $\log(2c-1) > 0.99\log(2c)$ for $c \geq 25$. Hence,

$$\begin{aligned}\log((2n-1)(2n-3)\cdots(2n-k)) &\geq \frac{k+1}{2}\log(2c-1) + \frac{k+1}{2}\log k \\ &> 0.495k\log(2c) + \frac{k+1}{2}\log k,\end{aligned}$$

which gives us our lower bound on $\log((2n-1)\cdots(2n-k))$.

Since $(2n-2)(2n-4)\cdots(2n-k+1)$ is the product of $(k-1)/2$ consecutive even numbers, it is divisible by $((k-1)/2)! \cdot 2^{(k-1)/2}$. Using this in part, we see that

$$u \leq \frac{k!}{((k-1)/2)!} \prod_{\substack{p \leq k \\ p^r \| \binom{2n-1}{k}}} p^r.$$

It is not difficult to show based on well known identities for $\nu_p(m!)$ that if p^r exactly divides $\binom{2n-1}{k}$ then $p^r \leq 2n-1$ (cf. [3]). We deduce that

$$u \leq (2n-1)^{\pi(k)} k(k-1)\cdots\frac{k+1}{2} < (2n)^{\pi(k)} k^{(k+1)/2}.$$

Appealing to Lemma 2, we deduce

$$\begin{aligned}\log u &< \pi(k)\log(2n) + \frac{k+1}{2}\log k \\ &< \left(1+\frac{3}{2\log k}\right)\frac{k}{\log k}\log(2ck) + \frac{k+1}{2}\log k \\ &= k\left(1+\frac{3}{2\log k}\right) + \frac{k}{\log k}\left(1+\frac{3}{2\log k}\right)\log(2c) + \frac{k+1}{2}\log k \\ &= k\log(2c)\left(1+\frac{3}{2\log k}\right)\left(\frac{1}{\log(2c)}+\frac{1}{\log k}\right) + \frac{k+1}{2}\log k.\end{aligned}$$

Using $c \geq 25$ and $k \geq 1001$, we obtain

$$\log u < 0.49k\log(2c) + \frac{k+1}{2}\log k.$$

Combining our lower bound for $\log((2n-1)\cdots(2n-k))$ with our upper bound for $\log u$, we see that

$$\log v > 0.005k\log(2c).$$

For fixed $c \geq 25$, the function $0.005k\log(2c) - \log(2ck)$ is increasing for $k \geq 1001$ and positive. It follows, for $c \geq 25$ and $k \geq 1001$, that $\log v > \log(2ck) = \log(2n)$, completing the case under consideration.

Case (ii). Consider $1 \leq c \leq 25$ and $k \geq 1001$. Since $2ck-k+2 \geq k+2$, the primes in the interval

$$I = (2n-k+2, 2n-1] = (2ck-k+2, 2ck-1]$$

divide v. We consider the two possibilities $1.74 \leq c \leq 25$ and $1 \leq c \leq 1.74$ separately. For the first, we appeal to the first assertion in Lemma 3; for the second, we use the second assertion of Lemma 3. For $1.74 \leq c \leq 25$ and $k \geq 1001$, one checks that

$$2ck-k+2 \geq 2479 \quad \text{and} \quad 1.01^2(2ck-k+2) \leq 2ck-1.$$

For $1 \leq c \leq 1.74$ and $k \geq 1001$, one checks that

$$2ck-k+2 \geq 213 \quad \text{and} \quad 1.05^2(2ck-k+2) \leq 2ck-1.$$

Thus, in either case, there are two primes p_1 and p_2 in I. Furthermore, in both cases, we can find such primes satisfying

$$p_1 > (2c-1)k \quad \text{and} \quad p_2 > 1.01(2c-1)k.$$

It follows that

$$v \geq p_1p_2 > 1.01(2c-1)^2k^2 > 2ck = 2n.$$

Case (iii). Consider $n \geq 999$ and $9 \leq k \leq 999$. We apply Lemma 5 with $l = (k+1)/2$ to obtain

$$v \geq \frac{(2n-k)^{(k+1)/2-\pi(k)+1}}{((k-1)/2)!} \cdot 2^{\nu_2(((k-1)/2)!)}.$$

Let $s = (k+1)/2 - \pi(k)$. We deduce $v > 2n-1$ provided

$$\frac{(2n-k)(2n-k)^s}{2n-1} > \frac{((k-1)/2)!}{2^{\nu_2(((k-1)/2)!)}}.$$

Recall that $k \leq n$. It follows that $(2n-k)/(2n-1) > 1/2$. Thus, for this case, it suffices to show

$$(2n-k)^s \geq \frac{((k-1)/2)!}{2^{\nu_2(((k-1)/2)!)-1}}.$$

Fix

$$n_k = \max\left\{\left\lceil \frac{1}{2}\left(\left(\frac{((k-1)/2)!}{2^{\nu_2(((k-1)/2)!)-1}}\right)^{1/s} + k\right)\right\rceil, k\right\}.$$

We deduce that for each odd integer $k \in [9, 999]$, if $n \geq n_k$, then $v > 2n-1$. A computation shows that the maximum value of n_k over such k is in fact 999, establishing $v > 2n-1$ in this case.

Case (iv). Consider $k \in \{3,5,7\}$ and $k \leq n$. Our approach here is basically the same as in Case (iii), but we bypass using Lemma 5 by making use of a more direct analysis combined with Lemma 4. Fix $k \in \{3,5,7\}$; we consider the set $T = T_k = \{2n-1, 2n-3, \ldots, 2n-k\}$. For each odd prime $p \leq k$ beginning with $p = 3$, we choose an element a_p of T not yet chosen (so the a_p's are distinct) for which $\nu_p(a_p)$ is maximal. Regardless of k, there will be one element, say t, of T that is not equal to a_p for every $p \leq k$. For $k = 3$, we have $t \geq 2n-3$ and $\gcd(t,3) = 1$. If there is a prime ≥ 5 dividing a_3, then $v \geq 5t \geq 5(2n-3) > 2n-1$. If there are no primes ≥ 5 dividing a_3, then a_3 is a power of 3. Given the conditions of Lemma 7, the case $k = 3$ is complete. Now, consider $k \in \{5,7\}$. There are positive integers t_1 and t_2 satisfying

$$t = t_1 t_2, \quad \gcd\left(t_1, \prod_{p \leq k} p\right) = 1 \text{ and } t_2 \text{ minimal.} \tag{2}$$

For $k = 5$, we have $t_2 = 1$; for $k = 7$, we have $t_2 \in \{1,3\}$. The idea is to show that if $k \in \{5,7\}$, then there is a prime ≥ 11 that divides some a_p so that

$$v \geq 11t_1 \geq \frac{11t}{3} \geq \frac{11(2n-k)}{3} \geq \frac{11(2n-7)}{3} > 2n-1.$$

For each $k \in \{5,7\}$, we checked computationally whether the inequality asserted in Lemma 7 holds when $k \leq n \leq 125$. For $k = 5$ and $k \leq n \leq 125$, the inequality holds if and only if $n \notin \{5, 14, 15\}$. For $k = 7$ and $k \leq n \leq 125$, the inequality holds if and only if $n \neq 14$. For $n \geq 125$, one checks that

Lemma 4 implies that some a_p is divisible by a prime ≥ 11. Given the conditions of Lemma 7, the argument is complete now when $k \in \{5, 7\}$.

Case (v). Consider $n \leq 998$ with $9 \leq k \leq n$. There are a finite number of pairs (n, k) to consider, and we simply did a computation (using MAPLE 7) to determine whether the inequality in Lemma 7 holds. More explicitly, for a positive integer t, define $t_1 = t_1(t)$ and $t_2 = t_2(t)$ as in (2). Let $m_0 = 1$. For fixed (n, k), define recursively

$$m_j = m_{j-1} \cdot t_1(2n - (2j-1)) \quad \text{for } 1 \leq j \leq \frac{k+1}{2}.$$

For each (n, k), we computed values of m_j until we obtained one which exceeded $2n - 1$. With the conditions on n and k in this case, such a $j \leq (k+1)/2$ always existed, completing the case under consideration. ∎

5. A proof of Theorem 1. Let $f(x)$ be as in Theorem 1, and assume $f(x)$ is reducible. Then there is an odd integer k such that $f(x)$ has a factor (in $\mathbb{Q}[x]$) of degree k or $k+1$ in $[1, n]$. Lemmas 6 and 7 lead us far into the proof of Theorem 1 as they immediately imply that if $f(x)$ is reducible, then a_n must be divisible by a number $> 2n-1$ except possibly in the case that $k = 1$ or one of the three conditions stated in Lemma 7 occurs. We are left then with considering these cases.

Suppose $k = 1$. Noting that $2n-1$ is odd, we deduce from Lemma 6 that a_n must be divisible by $2n-1$. The condition $0 < |a_n| < 2n-1$ of Theorem 1 implies a contradiction. Recall also that it was noted in the introduction that a linear or quadratic factor can exist if $|a_n| = 2n-1$. So the strict inequality $|a_n| < 2n-1$, not required in the previous paragraph, is necessary here.

For the remainder of this section, we shall make use of several explicit Newton polygons. For this purpose, we define $\mathcal{N}_w(p)$ as the Newton polygon of a polynomial $w(x)$ with respect to a prime p. We refer to the horizontal distance between two points (x_1, y_1) and (x_2, y_2) as $|x_2 - x_1|$ and to the horizontal length of an edge of a Newton polygon as the horizontal distance between its endpoints. We work with $F(x) = u_{2n} f(x)$, noting that its factors have the same degree as the factors of $f(x)$. We fix $G(x)$ to be the polynomial $F(x)$ with $a_n = a_{n-1} = \cdots = a_1 = a_0 = 1$. Thus, if $G(x) = \sum_{j=0}^{n} b_j x^{2j}$, then $F(x) = \sum_{j=0}^{n} a_j b_j x^{2j}$. Throughout, we make use of Lemma 1 to derive information about the factors of $F(x)$ and, hence, $f(x)$. Specifically, we make use of the following (some of which have already been used and elaborated on in the proof of Lemma 6):

(A) If $F(x)$ has a factor of degree d, then for any prime p we find that d can be written as a sum of horizontal distances between consecutive lattice points along the edges of $\mathcal{N}_F(p)$. More explicitly, if $(x_0, y_0), (x_1, y_1), \ldots, (x_r, y_r)$ is a complete list of the lattice points

along the edges of $\mathcal{N}_F(p)$ with $0 = x_0 < x_1 < \cdots < x_{r-1} < x_r = \deg F$, then $d = \sum_{j=1}^{r} \varepsilon_j (x_j - x_{j-1})$ where each $\varepsilon_j \in \{0, 1\}$.

(B) If the slope of an edge of $\mathcal{N}_F(p)$ is positive and $< 1/d$, then the horizontal distance between any two lattice points on the edge is $> d$.

(C) If the slope of the rightmost edge of $\mathcal{N}_F(p)$ is $< 1/d$ and if the sum of the lengths of the edges of $\mathcal{N}_F(p)$ with a zero or negative slope is $< d$, then $F(x)$ cannot have a factor of degree d.

(D) The spots used to form $\mathcal{N}_F(p)$ lie on or above the spots used to form $\mathcal{N}_G(p)$.

(E) If the slope of the rightmost edge of $\mathcal{N}_G(p)$ is $< 1/d$, then the slope of the rightmost edge of $\mathcal{N}_F(p)$ is $< 1/d$.

The first item (A) above follows directly from Lemma 1; (B) is easily checked; (C) is a consequence of (A) and (B); (D) follows from the fact that $\nu_p(a_j b_j) \geq \nu_p(b_j)$; and (E) follows from (D) and $a_0 = \pm 1$ (so that the rightmost endpoint on $\mathcal{N}_F(p)$ is the same as the rightmost endpoint of $\mathcal{N}_G(p)$).

We turn now to the case that $n = 14$ and $k \in \{5, 7\}$ (arising in the conditions of Lemma 7). The Newton polygon $\mathcal{N}_G(23)$ consists of two edges, one adjoining the points $(0, 0)$ and $(4, 0)$ and one adjoining $(4, 0)$ to $(28, 1)$. From (C), (D) and (E), we deduce that a_{12}, a_{13}, and a_{14} are all divisible by 23. As $|a_{14}| < 27$, we have $p \nmid a_{14}$ for every prime $p \neq 23$. We consider $p = 3$. The Newton polygon $\mathcal{N}_G(3)$ consists of two edges, one adjoining the points $(0, 0)$ and $(18, 5)$ and one adjoining $(18, 5)$ to $(28, 8)$. Since $3 \nmid a_{14}$ and $a_0 = \pm 1$, the points $(0, 0)$ and $(28, 8)$ are on $\mathcal{N}_F(3)$. If $(18, 5)$ is as well, then by (D) the edges of $\mathcal{N}_F(3)$ are identical to those of $\mathcal{N}_G(3)$, and we deduce from (A) that $F(x)$ cannot have a factor of degree k. So it must be the case that $3 \mid a_5$ (so that the coefficient of x^{10} in $F(x)$ is divisible by a higher power of 3 than the coefficient of x^{10} in $G(x)$). In this case, $\mathcal{N}_F(3)$ consists of a single edge from $(0, 0)$ to $(28, 8)$ of slope $2/7$. It follows from (A) that $F(x)$ cannot have a factor of degree 5, 6, or 8. So $F(x)$ has a factor of degree 7. We consider now $p = 7$. The Newton polygon $\mathcal{N}_G(7)$ consists of three edges, one from $(0, 0)$ to $(6, 0)$, one from $(6, 0)$ to $(20, 1)$, and one from $(20, 1)$ to $(28, 2)$. From (C), (D) and (E), we deduce that $F(x)$ cannot have a factor of degree 7. This is a contradiction so that, in the case $n = 14$, the polynomial $f(x)$ cannot have a factor of degree in $[5, 8]$.

We turn next to the case that $k = 5$ and $n = 15$. The Newton polygon $\mathcal{N}_G(29)$ consists of a single edge from $(0, 0)$ to $(30, 1)$. From (C) and (E), we deduce that $29 \mid a_{15}$. This is sufficient to deal with this case as the condition $0 < |a_n| < 2n - 1$ in Theorem 1 cannot hold. To obtain the stronger result suggested in the introduction that $f(x)$ cannot have a factor of degree 5 or 6 when $|a_n| = 2n - 1$ and $k \leq n$, we note that an analysis of $\mathcal{N}_F(3)$ can be used. We omit the details.

We turn now to $k = 5$ and $n = 5$. The Newton polygon $\mathcal{N}_G(7)$ consists of two edges, one from $(0, 0)$ to $(2, 0)$ and one from $(2, 0)$ to $(10, 1)$. By (C), (D) and (E), we obtain $7 \mid a_5$. Since $|a_5| < 9$, we have $3 \nmid a_5$. The Newton polygon $\mathcal{N}_G(3)$ consists of a single edge from $(0, 0)$ to $(10, 3)$. As $3 \nmid a_0 a_5$, we deduce from (D) that the Newton polygon $\mathcal{N}_F(3)$ also consists of just this one edge. Hence, $f(x)$ cannot have a factor of degree 5 or 6.

Now, suppose $k = 3$ and $2n - 3$ is a power of 3. In Lemma 7, we obtained slightly more information than necessary to complete the proof of Theorem 1. Since $2n - 3$ is a power of 3 (and $n \geq k = 3$), it is clear that

$$\prod_{\substack{p^r \| (2n-1)(2n-3) \\ p \geq 5}} p^r = 2n - 1.$$

Hence, in this case, we obtain a contradiction from Lemma 6 and the condition $0 < |a_n| < 2n-1$. Thus, if $2n-3$ is a power of 3, then $f(x)$ cannot have a factor of degree 3 or 4. Note that an example was given in the introduction of a reducible quartic $f(x)$ arising when $|a_n| = 2n - 1$ with $n = 6$ and, in this example, $2n - 3$ is a power of 3.

It remains to consider $k = 3$ and $2n-1$ being a power of 3. Our analysis here is complicated by the fact that there are infinitely many cases under consideration. We proceed as follows. Observe that the product above is now $2n-3$ so that Lemma 6 implies $2n-3$ divides a_n. Since $2n-1$ is divisible by 3 and $0 < |a_n| < 2n - 1$, we deduce that $3 \nmid a_n$. Define u by $2n - 1 = 3^u$. As $n \geq k = 3$, we deduce $u \geq 2$. If $u = 2$, then $\mathcal{N}_G(3)$ and, hence, $\mathcal{N}_F(3)$ consist of a single edge with slope $3/10$, giving a contradiction (by (A)). Thus, $u \geq 3$ and, consequently, $n \geq 14$. Our approach will be to describe $\mathcal{N}_G(3)$ rather explicitly and, in particular, to show that the rightmost edge of $\mathcal{N}_G(3)$ has slope $3/10$ and the leftmost edge of $\mathcal{N}_G(3)$ has slope $(n+1)/(4n-2)$. Since $3 \nmid a_n a_0$, we deduce from (D) that the slopes of the edges of $\mathcal{N}_F(3)$ lie in the interval $[(n + 1)/(4n - 2), 3/10] \subset (1/4, 1/3)$. The slopes being positive and $< 1/3$ implies from (B) that $f(x)$ cannot have a factor of degree 3. The slopes also being $> 1/4$ implies that $f(x)$ cannot have a factor of degree 4 (otherwise, the horizontal distance between two lattice points would be ≤ 4, which is easily seen to be impossible). Thus, we will have a contradiction, and the proof of Theorem 1 will be complete.

We are left with showing that the rightmost edge of $\mathcal{N}_G(3)$ has slope $3/10$ and the leftmost edge of $\mathcal{N}_G(3)$ has slope $(n + 1)/(4n - 2)$. Here, $2n - 1 = 3^u$ with $u \geq 3$ (and $n \geq 14$). Let m be such that $2m - 1 = 3^{u-1}$. Then $m = (3^{u-1} + 1)/2 = (n + 1)/3$. Define

$$H(x) = \sum_{j=0}^{m} \frac{u_{2m}}{u_{2j}} x^{2j}.$$

Thus, H is the polynomial G with the role of u replaced by $u-1$. We will show that the Newton polygons $\mathcal{N}_G(3)$ and $\mathcal{N}_H(3)$ are closely connected; in fact, we will show that a translation of $\mathcal{N}_H(3)$ is embedded in the rightmost part of $\mathcal{N}_G(3)$. In the case that $u=2$, we already indicated that $\mathcal{N}_G(3)$ consists of a single edge with slope $3/10$. It will then follow that for every $u \geq 3$, the rightmost edge of $\mathcal{N}_G(3)$ has slope $3/10$, giving us partially what we want.

Fix $\nu = \nu_3$. We make use of the fact that

$$\nu(3^u - 2l) = \nu(l) \qquad \text{for } 1 \leq l < \frac{3^u}{2}. \tag{3}$$

From (3),

$$\begin{aligned}\nu\left(\frac{u_{2n}}{u_{2m}}\right) &= \nu((2n-1)(2n-3)\cdots(2m+1)) \\ &= \nu(3^u) + \nu(3^u-2) + \cdots + \nu(3^u-(2n-2m-2)) \\ &= u + \nu(1) + \nu(2) + \cdots + \nu(n-m-1) = u + \nu((n-m-1)!).\end{aligned}$$

One checks that $n-m-1 = 3^{u-1}-1$ so that

$$\begin{aligned}\nu((n-m-1)!) &= \sum_{j=1}^{u-1}\left[\frac{3^{u-1}-1}{3^j}\right] = \sum_{j=1}^{u-1}(3^{u-1-j}-1) \\ &= \frac{3^{u-1}-1}{2} - (u-1).\end{aligned}$$

We deduce that

$$\nu\left(\frac{u_{2n}}{u_{2m}}\right) = \frac{3^{u-1}-1}{2} + 1 = \frac{3^{u-1}+1}{2} = \frac{n+1}{3}. \tag{4}$$

Observe that

$$G(x) = \sum_{j=m+1}^{n} \frac{u_{2n}x^{2j}}{u_{2j}} + \frac{u_{2n}}{u_{2m}}H(x).$$

As $2n-2m = 3^u - 3^{u-1} = 2\cdot 3^{u-1} = (4n-2)/3$, we see that the lattice point $((4n-2)/3, (n+1)/3)$ is a spot in the construction of $\mathcal{N}_G(3)$. Furthermore, the spot $((4n-2)/3, (n+1)/3)$ and the spots to the right of it in the construction of $\mathcal{N}_G(3)$ are precisely the spots used to construct $\mathcal{N}_H(3)$ translated horizontally by $(4n-2)/3$ and vertically by $(n+1)/3$.

This does not completely establish what we want nor even that $\mathcal{N}_H(3)$ is embedded in $\mathcal{N}_G(3)$. To complete the proof, we establish two things: that the leftmost edge of $\mathcal{N}_G(3)$ has slope $(n+1)/(4n-2)$ and that this slope is less than the slopes of the edges appearing in $\mathcal{N}_H(3)$. Once the former is shown the latter will follow by induction as $(n+1)/(4n-2)$ is a decreasing function of n and $H(x)$ is simply $G(x)$ with u in $G(x)$ replaced by $u-1$. The slope of the line through $(0,0)$ and $((4n-2)/3, (n+1)/3)$ is $(n+1)/(4n-2)$.

To establish that the leftmost edge of $\mathcal{N}_G(3)$ has slope $(n+1)/(4n-2)$, it suffices to show that the slope of the line through $((4n-2)/3,(n+1)/3)$ and any spot (a,b) to the left of $((4n-2)/3,(n+1)/3)$ with $a>0$ is less than $(n+1)/(4n-2)$. For any such spot (a,b), we have an integer j for which

$$a=\frac{4n-2}{3}-2j,\qquad b=\nu(u_{2n})-\nu(u_{2n-a}),\qquad 0<j<3^{u-1}.$$

Recall that $2n-2m=(4n-2)/3$ so that

$$2n-a>2n-(4n-2)/3=2m.$$

Also, $a=2(2n-1)/3-2j=2(3^{u-1}-j)$. From (3) and (4), we have

$$\begin{aligned}\frac{n+1}{3}-b&=\nu\left(\frac{u_{2n}}{u_{2m}}\right)-\nu\left(\frac{u_{2n}}{u_{2n-a}}\right)=\nu(u_{2n-a})-\nu(u_{2m})\\&=\nu((2n-a-1)(2n-a-3)\cdots(2m+1))\\&=\nu\left(\frac{a}{2}\left(\frac{a}{2}+1\right)\cdots(n-m-1)\right)\\&=\nu((3^{u-1}-1)!)-\nu((3^{u-1}-j-1)!).\end{aligned}$$

One checks that this last difference is equal to $\nu(j!)<j/2$. Thus, the slope of the line through (a,b) and $((4n-2)/3,(n+1)/3)$ is

$$\frac{\nu(j!)}{2j}<\frac{1}{4}<\frac{n+1}{4n-2},$$

completing the proof of Theorem 1. ∎

References

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

[2] G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, J. Math. Pures Appl. (6) 2 (1906), 191–258.

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

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

[5] 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.

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

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

[8] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, ibid. 6 (1962), 64–94.

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

[10] —, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen. II*, ibid., 370–391.

Department of Mathematics and Computer Science
Georgia College and State University
Milledgeville, GA 31061, U.S.A.
E-mail: martha.allen@gcsu.edu
http://turing.gcsu.edu/~mallen/

Mathematics Department
University of South Carolina
Columbia, SC 29208, U.S.A.
E-mail: filaseta@math.sc.edu
http://www.math.sc.edu/~filaseta/

Received on 12.1.2004 (4693)