



**HAL**  
open science

# A generalization of a fourth irreducibility theorem of I. Schur

Michael Filaseta, Martha Allen

► **To cite this version:**

Michael Filaseta, Martha Allen. A generalization of a fourth irreducibility theorem of I. Schur. Hardy-Ramanujan Journal, In press, Volume 46 - 2023, 10.46298/hrj.2024.13075 . hal-04452699

**HAL Id: hal-04452699**

**<https://hal.science/hal-04452699>**

Submitted on 12 Feb 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial 4.0 International License

# A generalization of a fourth irreducibility theorem of I. Schur

Martha Allen and Michael Filaseta

**Abstract.** In a 1929 paper, Issai Schur investigated the irreducibility over the rationals of the polynomials  $\sum_{j=0}^n a_j x^{2j}/u_{2j+2}$  where the  $a_j$ 's are integers with  $|a_n| = |a_0| = 1$  and  $u_{2j+2}$  is the product of the odd numbers less than  $2j + 2$ . We establish a more general result holds with the condition  $|a_n| = 1$  relaxed but with finitely many exceptions. A proof is given showing that also, in some sense, the more general result is best possible.

**Keywords.** irreducible polynomial, Newton polygon.

**2010 Mathematics Subject Classification.** 11R09, 12E05, 11C08.

## 1. Introduction

In 1929, I. Schur [Sch29a] showed the following general theorem.

**Theorem 1.1. (Schur)** *Let  $n$  be a positive integer, and let  $a_0, a_1, \dots, a_n$  denote arbitrary integers with  $|a_n| = |a_0| = 1$ . Then*

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

*is irreducible.*

Here, and throughout this paper, irreducibility is over the field of rational numbers.

The second author [Fil96] showed that the condition that  $|a_n| = 1$  can be relaxed to  $0 < |a_n| < n$  provided  $(a_n, n) \notin \{(\pm 5, 6), (\pm 7, 10)\}$ , and that this result is in some sense best possible. More precisely, there are examples for each pair  $(a_n, n) \in \{(\pm 5, 6), (\pm 7, 10)\}$  where  $0 < |a_n| < n$ ,  $|a_0| = 1$  and the polynomial  $f(x)$  is reducible, and there are examples of reducible  $f(x)$  for each  $n > 1$  with  $a_n = \pm n$  and  $|a_0| = 1$ .

In a second paper by I. Schur [Sch29b], three other similar irreducibility results were obtained involving a condition  $|a_n| = 1$  on part of the leading coefficient as before. Two of these results were generalized by the authors in [AIFi03, AIFi04] as follows.

**Theorem 1.2.** *For  $n$  an integer  $\geq 1$ , define*

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

*where the  $a_j$ 's are arbitrary integers with  $|a_0| = 1$ . Let  $k'$  be the integer such that  $n+1 = k'2^u$  where  $k'$  is odd and  $u$  is an integer  $\geq 0$ . Let  $k''$  be the integer such that  $(n+1)n = k''2^u 3^v$  where  $(k'', 6) = 1$ ,  $u$  is an integer  $\geq 1$ , and  $v$  is an integer  $\geq 0$ . Let  $M = \min\{k', k''\}$ . If  $0 < |a_n| < M$ , then  $f(x)$  is irreducible.*

**Theorem 1.3.** For  $j \geq 0$ , let  $u_{2j} = 1 \times 3 \times 5 \times \cdots \times (2j - 1)$ . For  $n$  an integer  $> 1$ , define

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

where the  $a_j$ 's are arbitrary integers with  $|a_0| = 1$ . If  $0 < |a_n| < 2n - 1$ , then  $f(x)$  is irreducible for all but finitely many pairs  $(a_n, n)$ .

In this paper, we generalize the fourth irreducibility theorem of Schur [Sch29b] from 1929 in which again a condition  $|a_n| = 1$  on part of the leading coefficient is relaxed. Specifically, we prove the following.

**Theorem 1.4.** Let  $u_{2j} = 1 \times 3 \times 5 \times \cdots \times (2j - 1)$ . For  $n$  an integer  $\geq 1$ , define

$$f(x) = \sum_{j=0}^n a_j \frac{x^{2j}}{u_{2j+2}} \tag{1.1}$$

where the  $a_j$ 's are arbitrary integers with  $|a_0| = 1$ . Let  $k'$  be the integer such that  $2n + 1 = k'3^u$  where  $u$  is an integer  $\geq 0$  and  $(k', 3) = 1$ . Let  $k''$  be the integer such that  $(2n + 1)(2n - 1) = k''3^u5^v$  where  $u$  and  $v$  are integers  $\geq 0$  and  $(k'', 15) = 1$ . Let  $M = \min\{k', k''\}$ . If  $0 < |a_n| < M$ , then  $f(x)$  is irreducible for all but finitely many pairs  $(a_n, n)$ .

In the case of  $|a_n| = 1$ , I. Schur [Sch29b] showed that  $f(x)$  above is irreducible unless  $2n = 3^u - 1$  for some integer  $u \geq 2$ . Furthermore, he showed that if  $f(x)$  is reducible with  $|a_n| = 1$ , then  $f(x)$  is  $x^2 \pm 3$  times an irreducible polynomial. Observe that Theorem 1.4 gives no information in the case that  $2n = 3^u - 1$  as  $M = k' = 1$ . In the case that  $u = 1$  so that  $f(x)$  has degree 2, the quadratic will be irreducible. We will show that if  $f(x)$  is as in (1.1) with  $a_0 = 1$  and  $a_n = M = k'$  in general, then  $f(x)$  is either irreducible or divisible by a quadratic polynomial, and the latter can happen. The value of  $M$  is also 1 when  $k'' = 1$  which occurs only for  $n \in \{1, 2, 13\}$ . The case  $n = 1$  corresponds to  $f(x)$  being a quadratic as discussed above. For  $n = 13$ , we already know  $f(x)$  can have a quadratic factor since  $2 \cdot 13 = 3^3 - 1$ . For  $n \geq 2$  in general, we show that if  $f(x)$  is as in (1.1) with  $a_0 = 1$  and  $a_n = M = k'' < k'$ , then  $f(x)$  is either irreducible or divisible by a quartic polynomial, and the latter can happen. In the case  $n = 2$ , the polynomial  $f(x)$  is quartic and will be irreducible.

From henceforth, the polynomial  $f(x)$  will be as defined in (1.1). Theorem 1.4 goes back to work associated with the first author's dissertation [All01]. The result has the weakness over the prior results stated above in that there are finitely many, possibly zero, exceptional pairs  $(a_n, n)$  that are not determined. As determining these finitely many pairs seems particularly difficult due to an application of an ineffective result of Mahler [Mah61], we are left with this less than precise result. On the other hand, like with the prior results, as noted above, we will show that Theorem 1.4 is best possible in the sense that for each  $n > 2$ , if  $a_n = M$  and  $a_0 = 1$ , then there are integers  $a_{n-1}, a_{n-2}, \dots, a_1$  such that  $f(x)$  is reducible.

Before closing this introduction, we note that recent work related to the fourth irreducibility theorem of Schur [Sch29b] from 1929 has been done by A. Jakhar [Jak23].

## 2. The basic strategy

To establish that  $f(x)$  is irreducible for all but finitely many pairs  $(a_n, n)$  with  $0 < |a_n| < M$ , it suffices to show that  $f(x)$  is irreducible for sufficiently large  $n$ . We use the following two lemmas in proving the irreducibility of  $f(x)$  when  $0 < |a_n| < M$ . We explain the proof of Theorem 1.4 based on these lemmas after we state them. The proofs of the lemmas are in the next two sections.

**Lemma 2.1.** *Let  $a_0, a_1, \dots, a_n$  denote arbitrary integers with  $|a_0| = 1$ , and let*

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

*Let  $k$  be a positive odd integer  $\leq n$ . Suppose there exists a prime  $p > k + 2$  (so  $p \geq k + 4$ ) and a positive integer  $r$  for which*

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

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

*Comment.* Lemma 2.1 implies that if  $f(x)$  has a factor of degree  $k$  or  $k + 1$ , then

$$\prod_{\substack{p^r \mid ((2n+1)(2n-1)\cdots(2n-k+2)) \\ p \geq k+4}} p^r \quad \text{divides} \quad a_n,$$

where the notation  $p^r \parallel m$  denotes that  $p^r \mid m$  and  $p^{r+1} \nmid m$ .

**Lemma 2.2.** *Let  $n$  be a sufficiently large integer, and let  $k$  be an odd integer in  $[5, n]$ . Then*

$$\prod_{\substack{p^r \mid ((2n+1)(2n-1)\cdots(2n-k+2)) \\ p \geq k+4}} p^r > 2n + 1.$$

Observe that once the above lemmas are established, we can deduce the following consequences of these lemmas.

- If  $n$  is a sufficiently large integer and  $0 < |a_n| \leq 2n + 1$ , then  $f(x)$  cannot have a factor with degree  $\ell$  in  $[5, n]$ .
- If  $0 < |a_n| < k''$  where  $k''$  is the integer such that  $(2n+1)(2n-1) = k''3^u5^v$  with  $u \geq 0, v \geq 0$  and  $(k'', 15) = 1$ , then  $f(x)$  cannot have a cubic or quartic factor.
- If  $0 < |a_n| < k'$  where  $k'$  is the integer such that  $2n+1 = k'3^u$  with  $u \geq 0$  and  $(k', 3) = 1$ , then  $f(x)$  cannot have a linear or quadratic factor.

Taking  $M = \min\{k', k''\}$  as in Theorem 1.4 and noting  $k' \leq 2n + 1$ , we obtain that if  $n$  is sufficiently large and  $0 < |a_n| < M$ , then  $f(x)$  is irreducible, completing the proof of Theorem 1.4.

### 3. Proof of Lemma 2.1

In this section, we use Newton polygons to show that if there is a prime  $p \geq k + 4$  and a positive integer  $r$  such that  $p^r \mid ((2n+1)(2n-1)\cdots(2n-k+2))$  but  $p^r \nmid a_n$ , then  $f(x)$  cannot have a factor of degree  $k$  or  $k + 1$ . Here  $k$  is an odd positive integer  $\leq n$ . Before proceeding with the proof, we give some notation and background information on Newton polygons that will be useful.

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  $p^{\nu(m)+1} \nmid m$ . Let  $w(x) = \sum_{j=0}^n u_j x^j \in \mathbb{Z}[x]$  with  $u_n u_0 \neq 0$ , and let  $p$  be a prime. Set

$$S = \{(n-i, \nu(u_i)) : u_i \neq 0, 0 \leq i \leq n\}.$$

Consider the lower edges along the convex hull of these points. The left-most endpoint is  $(0, \nu(u_n))$  and the right-most endpoint is  $(n, \nu(u_0))$ . 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.

In investigating irreducibility with Newton polygons, we will make use of the following lemma.

**Lemma 3.1. (G. Dumas [Dum1906])** *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 non-negative integer such that  $p^k$  divides the leading coefficient 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.*

*Proof of Lemma 2.1.* Let

$$F(x) = u_{2n+2}f(x) = \sum_{j=0}^n a_j \frac{u_{2n+2}}{u_{2j+2}} x^{2j} = \sum_{j=0}^n b_j x^{2j},$$

where

$$b_j = a_j \frac{u_{2n+2}}{u_{2j+2}} = a_j (2n+1)(2n-1) \cdots (2j+3).$$

Note that the coefficients of the odd powers of  $x$  in  $F(x)$  are all zero. Writing these terms into  $F(x)$ , we set

$$F(x) = \sum_{j=0}^n b_j x^{2j} = \sum_{i=0}^{2n} c_i x^i.$$

If  $i$  is odd, then  $c_i = 0$ . On the other hand, if  $i$  is even, then  $i = 2j$  for some  $j \in \{0, 1, \dots, n\}$  and  $c_i = c_{2j} = b_j$ . We consider the Newton polygon of  $F(x)$  with respect to the prime  $p$ . The spots of the Newton polygon are

$$\{(2n - i, \nu(c_i)) : c_i \neq 0, 0 \leq i \leq 2n\}.$$

From the conditions that  $k$  is odd and  $p^r \mid ((2n+1)(2n-1) \cdots (2n-k+2))$ , we deduce that  $p^r \mid c_i$  for  $i \in \{0, 1, \dots, 2n - (k+1), 2n - k\}$ . Thus, the right-most spots in

$$\mathcal{R} = \{(2n - i, \nu(c_i)) : c_i \neq 0, 0 \leq i \leq 2n - k\},$$

associated with the Newton polygon of  $F(x)$  with respect to  $p$ , have  $y$ -coordinates  $\geq r$ . Since  $p^r \nmid a_n$  and  $c_{2n} = b_n = a_n$ , we have  $p^r \nmid c_{2n}$ . Thus, the left-most endpoint of the Newton polygon of  $F(x)$  with respect to  $p$ , which is  $(0, \nu(c_{2n})) = (0, \nu(a_n))$ , has  $y$ -coordinate  $< r$ . Since the slopes of the edges of a Newton polygon increase from left to right, the spots in  $\mathcal{R}$  all lie on or above edges of the Newton polygon of  $F(x)$  with respect to  $p$  which have a positive slope. We will show next that each of these positive slopes is  $< 1/(k+1)$  by showing that the right-most edge has slope  $< 1/(k+1)$ .

Observe that the slope of the right-most edge of the Newton polygon of  $F(x)$  with respect to  $p$  is given by

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(c_0) - \nu(c_{2j})}{2j} \right\} = \max_{1 \leq j \leq n} \left\{ \frac{\nu(a_0 u_{2n+2}) - \nu(a_j u_{2n+2}/u_{2j+2})}{2j} \right\}.$$

Since  $|a_0| = 1$ , we have  $\nu(a_0 u_{2n+2}) = \nu(u_{2n+2})$ . Also, for  $1 \leq j \leq n$ , we see that

$$\nu\left(a_j \frac{u_{2n+2}}{u_{2j+2}}\right) \geq \nu\left(\frac{u_{2n+2}}{u_{2j+2}}\right).$$

Thus,

$$\begin{aligned} \nu(a_0 u_{2n+2}) - \nu\left(a_j \frac{u_{2n+2}}{u_{2j+2}}\right) &\leq \nu(u_{2n+2}) - \nu\left(\frac{u_{2n+2}}{u_{2j+2}}\right) \\ &= \nu(u_{2j+2}) \leq \nu((2j+1)!). \end{aligned}$$

Thus, the right-most slope is

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(c_0) - \nu(c_{2j})}{2j} \right\} \leq \max_{1 \leq j \leq n} \left\{ \frac{\nu((2j+1)!)}{2j} \right\}. \quad (3.2)$$

To estimate the right-hand side of (3.2) further, we consider the two cases  $j < (p-1)/2$  and  $j \geq (p-1)/2$ . Suppose first  $j < (p-1)/2$ . Then  $2j+1 < p$ . Since  $p$  is a prime, we see that  $p \nmid (2j+1)!$ . Therefore,  $\nu((2j+1)!) = 0$ . Therefore,

$$\frac{\nu((2j+1)!)}{2j} = 0 \quad \text{for } j < (p-1)/2. \quad (3.3)$$

Now, suppose  $j \geq (p-1)/2$ . In this case, we have

$$\nu((2j+1)!) = \sum_{i=1}^{\infty} \left\lfloor \frac{2j+1}{p^i} \right\rfloor < \sum_{i=1}^{\infty} \frac{2j+1}{p^i} = \frac{2j+1}{p-1}.$$

Since  $j \geq (p-1)/2$  implies  $1/(2j) \leq 1/(p-1)$ , we obtain

$$\begin{aligned} \frac{\nu((2j+1)!)}{2j} &< \frac{2j+1}{2j} \cdot \frac{1}{p-1} = \left(1 + \frac{1}{2j}\right) \frac{1}{p-1} \\ &\leq \left(1 + \frac{1}{p-1}\right) \frac{1}{p-1} = \frac{p}{(p-1)^2} \quad \text{for } j \geq (p-1)/2. \end{aligned} \quad (3.4)$$

Combining (3.2), (3.3) and (3.4), we deduce the right-most slope is

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(c_0) - \nu(c_{2j})}{2j} \right\} < \frac{p}{(p-1)^2}.$$

Recalling that we have the condition  $p \geq k+4$  in the statement of Lemma 2.1, one can verify that  $p/(p-1)^2 < 1/(k+1)$ . Therefore, the slope of the right-most edge is  $< 1/(k+1)$ , and we deduce that each edge of the Newton polygon of  $F(x)$  with respect to  $p$  has slope  $< 1/(k+1)$ .

Now, assume  $F(x)$  has a factor  $g(x) \in \mathbb{Z}[x]$  with  $\deg g \in \{k, k+1\}$ . We will show that the translates of all the edges of the Newton polygon of  $g(x)$  with respect to  $p$  cannot be found among the edges of the Newton polygon of  $F(x)$  with respect to  $p$ . This will imply a contradiction to Lemma 3.1. Hence, it will follow that  $F(x)$  cannot have a factor of degree  $k$ .

First, we show that no translate of an edge for  $g(x)$  can be found among those edges in the Newton polygon of  $F(x)$  having positive slope. 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. We know the slope is  $< 1/(k+1)$ ; therefore,

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

Thus,  $c-a > k+1 \geq \deg g$  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.

Next, we show that not all the translates of the edges for  $g(x)$  can be found among the edges of the Newton polygon of  $F(x)$  having 0 or negative slope. Recall that the spots in  $\mathcal{R}$  all lie on or above

edges of the Newton polygon of  $F(x)$  with respect to  $p$  which have a positive slope. Thus, the spots forming the endpoints of the edges of the Newton polygon of  $F(x)$  having 0 or negative slope must be among the spots  $(2n - i, \nu(c_i))$  where  $2n - k + 1 \leq i \leq 2n$ . Since  $2n - (2n - k + 1) = k - 1 < \deg g$ , these edges by themselves cannot consist of a complete collection of translated edges of the Newton polygon of  $g(x)$  with respect to  $p$ , and we have a contradiction.

Therefore,  $F(x)$  cannot have a factor with degree  $k$  or  $k + 1$ .

#### 4. Proof of Lemma 2.2

Let  $n$  be sufficiently large, and let  $k$  be an odd integer in  $[5, n]$ . Write

$$(2n + 1)(2n - 1) \cdots (2n - k + 2) = uv,$$

where all the prime factors of  $u$  are  $\leq k + 2$  and all the prime factors of  $v$  are  $> k + 2$ . Then

$$v = \prod_{\substack{p^r \parallel ((2n+1)(2n-1)\cdots(2n-k+2)) \\ p \geq k+4}} p^r.$$

To establish Lemma 2.2, we want to show  $v > 2n + 1$ . We begin by establishing Lemma 2.2 when  $k \geq 13$ , and then handle other values of  $k \geq 5$ .

**Lemma 4.1.** *For  $n$  a sufficiently large integer and  $13 \leq k \leq n$ ,*

$$\prod_{\substack{p^r \parallel ((2n+1)(2n-1)\cdots(2n-k+2)) \\ p \geq k+4}} p^r > 2n + 1.$$

*Proof.* Let  $T = \{2n + 1, 2n - 1, \dots, 2n - k + 2\}$ . In establishing Lemma 4.1, we take  $n$  to be sufficiently large and break up the argument into 3 cases depending on the size of  $k$ .

*Case 1:*  $n^{\frac{2}{3}} < k \leq n$ .

We use the following lemma which follows from results on gaps between primes (for example, see [Hux72]).

**Lemma 4.2.** *For  $n$  sufficiently large and  $n^{\frac{2}{3}} < k \leq n$ , there is a prime in each of the intervals*

$$I_1 = \left( 2n - k + 2, 2n + 1 - \frac{k - 1}{2} \right] \quad \text{and} \quad I_2 = \left( 2n + 1 - \frac{k - 1}{2}, 2n + 1 \right].$$

By Lemma 4.2, there exist primes  $p_1 \in I_1$  and  $p_2 \in I_2$ . Since

$$2n + 1 \geq p_2 > p_1 > 2n - k + 2,$$

$p_1$  and  $p_2$  are in  $T$ . Since  $k$  is odd,  $p_1 \geq 2n - k + 4$ . Thus (since  $k \leq n$ ), both  $p_1$  and  $p_2$  are  $\geq n + 4 \geq k + 4$ . From the definition of  $v$ , we deduce

$$v \geq p_1 p_2 > n^2 > 2n + 1.$$

This establishes Lemma 4.1 for  $n^{\frac{2}{3}} < k \leq n$ .

*Case 2:*  $k_0 < k \leq n^{\frac{2}{3}}$  for some fixed but sufficiently large  $k_0$ .

For this case and indirectly later, we will make use of the following lemma which was established in [AIF04, Lemma 5].

**Lemma 4.3.** *Let  $m, \ell$  and  $k$  denote positive integers with  $k \geq 2$ , and let*

$$T = \{2m + 1, 2m + 3, \dots, 2m + 2\ell - 1\}.$$

*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*

$$\prod_{p > k} p^{N_p} = \frac{\prod_{t \in S} t}{\prod_{2 < p \leq k} p^{N_p}} \geq \frac{(2m + 1)^{\ell - \pi(k) + 1}}{(\ell - 1)!} \cdot 2^{\nu_2((\ell - 1)!)}$$

For the moment, we only consider  $1 \leq k \leq n^{\frac{2}{3}}$ . To apply Lemma 4.3, for each odd prime  $p \leq k + 2$ , consider a number in  $T = \{2n + 1, 2n - 1, \dots, 2n - k + 2\}$  which is divisible by  $p^e$  where  $e = e(p)$  is as large as possible. Let  $a_p$  denote such a number divisible by  $p^e$ . Note that some of these numbers may be the same. Dispose of all these numbers, and let  $S$  denote the set of numbers in  $T$  that are left.

Let  $N_p$  be the exponent of the largest power of  $p$  dividing  $\prod_{m \in S} m$ . Observe that

$$v \geq \prod_{p > k + 2} p^{N_p}.$$

By Lemma 4.3 (with  $2m + 1 = 2n - k + 2$ ,  $\ell = (k + 1)/2$ , and  $k$  replaced by  $k + 2$ ), we obtain

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

Let  $r = (k + 1)/2 - \pi(k + 2) + 1$ , and

$$\alpha_k = \frac{\left(\frac{k-1}{2}\right)!}{2^{\nu_2\left(\left(\frac{k-1}{2}\right)!\right)}}.$$

One can see that  $T$  consists of  $(k + 1)/2$  numbers, and that we have removed at most  $\pi(k + 2) - 1$  of them to obtain the set  $S$ . Thus,

$$|S| \geq r. \tag{4.5}$$

Note that  $v > 2n + 1$  if

$$(2n - k + 2)^r > \alpha_k(2n + 1). \tag{4.6}$$

Furthermore, (4.6) holds if

$$r \log(2n - k + 2) - (\log \alpha_k + \log(2n + 1)) > 0. \tag{4.7}$$

To reduce showing  $v > 2n + 1$  to establishing (4.6) or (4.7), we used  $1 \leq k \leq n^{2/3}$ .

We show now that (4.7) holds for  $k_0 \leq k \leq n^{2/3}$  to finish the proof of Lemma 4.1 in this case. Suppose then that  $k_0 \leq k \leq n^{2/3}$ . By the Prime Number Theorem, since  $k_0$  is sufficiently large and  $k > k_0$ , we have

$$\pi(k + 2) < \frac{1}{12}(k + 2).$$

Hence, we deduce

$$r = \frac{k + 1}{2} - \pi(k + 2) + 1 > \frac{k + 3}{2} - \frac{1}{12}(k + 2) > \frac{5}{12}(k + 2) > \frac{5}{6} \left( \frac{k - 1}{2} \right). \tag{4.8}$$



Since  $k \leq n^{\frac{2}{3}}$ , we obtain

$$2n - k + 2 > n. \quad (4.9)$$

Also, the definition of  $\alpha_k$  implies

$$\alpha_k \leq \left(\frac{k-1}{2}\right)! \leq k^{\frac{k-1}{2}} \leq n^{\frac{2}{3}\left(\frac{k-1}{2}\right)}. \quad (4.10)$$

By (4.8) and (4.9), we deduce

$$r \log(2n - k + 2) > \frac{5}{6} \left(\frac{k-1}{2}\right) \log n. \quad (4.11)$$

From (4.10), we obtain

$$\log \alpha_k \leq \frac{2}{3} \left(\frac{k-1}{2}\right) \log n. \quad (4.12)$$

Combining (4.11) and (4.12) with  $k \geq k_0$ , we see that

$$\begin{aligned} r \log(2n - k + 2) - (\log \alpha_k + \log(2n + 1)) &> \frac{1}{6} \left(\frac{k-1}{2}\right) \log n - \log(2n + 1) \\ &\geq \frac{1}{6} \left(\frac{k_0-1}{2}\right) \log n - \log(2n + 1). \end{aligned} \quad (4.13)$$

Since  $k_0$  is sufficiently large,

$$\frac{1}{6} \left(\frac{k_0-1}{2}\right) \log n - \log(2n + 1) > 0.$$

Hence, (4.7) holds, and  $v > 2n + 1$ .

*Case 3:*  $13 \leq k \leq k_0$ .

We show that (4.6) holds, which will establish Lemma 4.1 in this case. First, we obtain a lower bound for  $r$ . Since  $k \geq 13$ , the value of  $\pi(k+2)$  is less than or equal to the number of even primes plus the number of odd numbers less than or equal to  $k+2$  minus the number of odd numbers less than or equal to 15 that are not prime. Thus,

$$\pi(k+2) \leq 1 + \frac{k+3}{2} - 3 \leq \frac{k+3}{2} - 2.$$

Therefore,

$$r = \frac{k+1}{2} - \pi(k+2) + 1 \geq \frac{k+1}{2} - \frac{k+3}{2} + 3 = 2.$$

By (4.5), we deduce that there are at least two numbers in  $S$  when  $k \geq 13$ . Therefore, the left-hand side of (4.6) is  $\geq n^2$ . Observe that

$$\alpha_k \leq \left(\frac{k-1}{2}\right)! \leq \left(\frac{k_0-1}{2}\right)!.$$

Since  $\alpha_k$  is bounded by a fixed constant, depending only on  $k_0$ , the right-hand side of (4.6) has order  $n$ . Therefore, for sufficiently large  $n$ , we see that (4.6) holds and, hence,  $v > 2n + 1$ .

**Lemma 4.4.** *For  $k \in \{7, 9, 11\}$ , we have*

$$\prod_{\substack{p^r \parallel ((2n+1)(2n-1)\cdots(2n-k+2)) \\ p \geq k+4}} p^r > 2n + 1$$

for all but finitely many positive integers  $n$ .

*Proof.* The first part of our proof (Case 1 below) will only involve finitely many exceptional  $n$  which are  $\leq 13$ . A direct check verifies the inequality in Lemma 4.4 for  $14 \leq n \leq 42$ , and henceforth we only consider  $n \geq 43$  throughout the proof of Lemma 4.4. For the second part of the proof (Case 2 below), the exceptional  $n$  can also be made explicit, but we do not do so and allow for these exceptional  $n$  to be somewhat larger.

Following the proof of Lemma 4.1, Case 2, we set

$$T = \{2n + 1, 2n - 1, \dots, 2n - k + 2\},$$

and apply Lemma 4.3. Thus, for each odd prime  $p \leq k + 2$ , we remove from  $T$  a number  $a_p$  divisible by  $p^e$ , where  $e = e(p)$  is as large as possible, to obtain a subset  $S$  of  $T$  satisfying (4.5), where

$$r = (k + 1)/2 - \pi(k + 2) + 1.$$

A direct computation shows that  $r = 1$  for  $k \in \{7, 9, 11\}$ . Thus,  $|S| \geq 1$ . Fix a number  $a = a(n, k)$  in  $S$ .

*Case 1: There exists a prime  $p \geq k + 4$  such that  $p$  divides at least 1 of the numbers in  $T - \{a\}$ .*

Recall  $v$  is the product in Lemma 4.4. If  $k = 7$ , then  $T = \{2n + 1, 2n - 1, 2n - 3, 2n - 5\}$ . So  $a \geq 2n - 5$  and note that  $7 \nmid a$  and  $5 \nmid a$  since the numbers  $a_5$  and  $a_7$  were removed from  $T$  to form  $S$ . Also,  $3^2 \nmid a$ . Of the numbers in  $T - \{a\}$ , one of these is divisible by  $p \geq 11$ . Thus,

$$v \geq \frac{p(2n - 5)}{3} \geq \frac{11(2n - 5)}{3}.$$

A direct check shows that  $11(2n - 5)/3 > 2n + 1$  if and only if  $n > 29/8$ . Since  $n \geq 43$ , this last inequality holds, and  $v > 2n + 1$ .

If  $k = 9$ , then  $T = \{2n + 1, 2n - 1, 2n - 3, 2n - 5, 2n - 7\}$ . So  $a \geq 2n - 7$ . Note that  $11 \nmid a$ ,  $7 \nmid a$ , and  $5 \nmid a$ . Also  $3^2 \nmid a$ . One of the numbers in  $T - \{a\}$  is divisible by  $p \geq 13$ . Thus,

$$v \geq \frac{p(2n - 7)}{3} \geq \frac{13(2n - 7)}{3}.$$

As  $13(2n - 7)/3 > 2n + 1$  if and only if  $n > 47/10$ , we deduce again that  $v > 2n + 1$ .

If  $k = 11$ , then  $T = \{2n + 1, 2n - 1, 2n - 3, 2n - 5, 2n - 7, 2n - 9\}$ . So  $a \geq 2n - 9$ . Note that  $13 \nmid a$ ,  $11 \nmid a$ ,  $7 \nmid a$ ,  $5^2 \nmid a$ , and  $3^2 \nmid a$ . One of the numbers in  $T - \{a\}$  is divisible by  $p \geq 17$ . Thus,

$$v \geq \frac{p(2n - 9)}{3 \times 5} \geq \frac{17(2n - 9)}{15}.$$

As  $17(2n - 9)/15 > 2n + 1$  if and only if  $n > 42$ , we see again that  $v > 2n + 1$ .

*Case 2: There does not exist a prime  $p \geq k + 4$  such that  $p$  divides at least one of the numbers in  $T - \{a\}$ .*

To finish the proof of Lemma 4.4, we prove that this case occurs for at most finitely many  $n$ . We make use of the following lemma which is a special case of a more general theorem of Thue (see [Mor69]).

**Lemma 4.5.** *Let  $a$ ,  $b$ , and  $c$  be fixed integers with  $c \neq 0$ . Then there exist only finitely many integer pairs  $(x, y)$  for which  $ax^3 + by^3 = c$ .*

In this case, all the numbers in  $T - \{a\}$  are divisible only by primes  $p \leq k + 2$ . In particular, at least two of the numbers are powers of primes. More precisely, when  $k = 7$ , one of  $\{2n + 1, 2n - 1, 2n - 3, 2n - 5\}$  is a power of 3 and another a power of  $p$  for some  $p \in \{5, 7\}$ ; when  $k = 9$ , one of  $\{2n + 1, 2n - 1, 2n - 3, 2n - 5, 2n - 7\}$  is a power of 3 and another a power of  $p$  where

$p \in \{5, 7, 11\}$ ; and when  $k = 11$ , one of  $\{2n + 1, 2n - 1, 2n - 3, 2n - 5, 2n - 7, 2n - 9\}$  is a power of  $p_1$  and another a power of  $p_2$  where  $p_1 \neq p_2$  and  $p_1, p_2 \in \{3, 5, 7, 11, 13\}$ .

Let  $q$  be the greatest prime  $\leq k + 2$ , and let  $P = \{3, 5, 7, \dots, q\}$  be the set of odd primes  $\leq q$ . Let  $2n - i$  and  $2n - j$  where  $i \neq j$  and  $i, j \in \{-1, 1, 3, 5, 7, 9\}$  denote two numbers in  $T - \{a\}$  with each a power of a prime in  $P$ . So  $2n - i = p_1^u$  and  $2n - j = p_2^v$  where  $p_1, p_2 \in P$ . We consider the number of integer solutions  $u$  and  $v$  to

$$|p_1^u - p_2^v| = \ell \quad \text{where } \ell \in \{2, 4, 6, 8, 10\}. \quad (4.14)$$

Note that by letting  $u = 3q_1 + r_1$  and  $v = 3q_2 + r_2$  where  $q_1$  and  $q_2$  are integers and  $r_1, r_2 \in \{0, 1, 2\}$ , we can rewrite the above equation as

$$|c_1 x^3 - c_2 y^3| = \ell \quad (4.15)$$

where  $c_1$  and  $c_2$  are integers and  $x = p_1^{q_1}$  and  $y = p_2^{q_2}$ . By Lemma 4.5, there are only finitely many integer solutions  $x$  and  $y$  to (4.15), and thus finitely many integers  $q_1$  and  $q_2$ . This implies that there are only finitely many integers  $u$  and  $v$  that satisfy (4.14). Therefore, there are only finitely many integers  $n$  where no number in  $T - \{a\}$  is divisible by a prime  $p \geq k + 4$ , completing what we set out to show for this case.

Finally, we consider the case  $k = 5$ . In this case,

$$v = \prod_{\substack{p^r \parallel ((2n+1)(2n-1)(2n-3)) \\ p \geq 9}} p^r.$$

We establish the following lemma, which will finish the proof of Lemma 2.2. Furthermore, as noted after the statement of Lemma 2.2, we will have completed the proof of Theorem 1.4.

**Lemma 4.6.** *For  $n$  a sufficiently large integer, we have*

$$\prod_{\substack{p^r \parallel ((2n+1)(2n-1)(2n-3)) \\ p \geq 9}} p^r > 2n + 1.$$

*Proof.* We use the following consequence of a theorem of Mahler [Mah61] which is demonstrated in [Fil96].

**Lemma 4.7.** *Let  $a$  be a fixed non-zero integer, and let  $N$  be a fixed positive integer. Let  $\epsilon > 0$ . If  $n$  is sufficiently large (depending on  $a$ ,  $N$ , and  $\epsilon$ ), then the largest divisor of  $n(n + a)$  which is relatively prime to  $N$  is  $\geq n^{1-\epsilon}$ .*

Before proceeding, we note that Lemma 4.7 is ineffective, which in turn makes us unable to determine the finitely many exceptional pairs  $(a_n, n)$  mentioned in Theorem 1.4.

Since we are only interested in the primes  $p \geq 11$  that divide the product  $(2n + 1)(2n - 1)(2n - 3)$ , we take  $N = 3 \times 5 \times 7$  in Lemma 4.7. Let

$$A = \prod_{\substack{p^r \parallel (2n+1) \\ p \nmid N}} p^r, \quad B = \prod_{\substack{p^r \parallel (2n-1) \\ p \nmid N}} p^r, \quad \text{and} \quad C = \prod_{\substack{p^r \parallel (2n-3) \\ p \nmid N}} p^r.$$

Note that

$$\prod_{\substack{p^r \parallel ((2n+1)(2n-1)(2n-3)) \\ p \geq 11}} p^r = \prod_{\substack{p^r \parallel ((2n+1)(2n-1)(2n-3)) \\ p \nmid N}} p^r = ABC.$$

First consider the product  $(2n+1)(2n-1)$ . Take  $\epsilon = 1/4$ . Then by Lemma 4.7, the largest divisor of  $(2n+1)(2n-1)$  that is relatively prime to  $N$  is  $\geq (2n+1)^{3/4}$  for  $n$  sufficiently large. Thus,  $AB \geq (2n+1)^{3/4}$ . We deduce that either  $A \geq (2n+1)^{3/8}$  or  $B \geq (2n+1)^{3/8}$ .

We suppose  $A \geq (2n+1)^{3/8}$  (a similar argument can be done in the case that  $B \geq (2n+1)^{3/8}$ ). Next, we consider the product  $(2n-1)(2n-3)$ . Again, take  $\epsilon = 1/4$ . By Lemma 4.7, the largest divisor of  $(2n-1)(2n-3)$  which is relatively prime to  $N$  is  $\geq (2n-1)^{3/4}$  for  $n$  sufficiently large. Thus,  $BC \geq (2n-1)^{3/4}$ , and we deduce

$$\prod_{\substack{p^r \parallel ((2n+1)(2n-1)(2n-3)) \\ p \geq 11}} p^r = ABC \geq (2n+1)^{3/8}(2n-1)^{3/4} \\ > (2n-1)^{9/8} > (2n+1).$$

Therefore, for  $n$  sufficiently large, we see that the inequality in Lemma 4.6 (and hence in Lemma 2.2) holds.

## 5. Establishing sharpness of the results

We have shown that if  $0 < |a_n| < M$  (where  $M = \min\{k', k''\}$ ), then  $f(x)$  is irreducible. We show that this upper bound on  $|a_n|$  is sharp. More precisely, we show that for  $n > 2$ , when  $a_n = M$  and  $a_0 = 1$ , there exist integers  $a_{n-1}, a_{n-2}, \dots, a_1$  such that  $f(x)$  is reducible.

Either  $M = k' \leq k''$  or  $M = k'' < k'$ . We show the following results.

- If  $a_n = k'$  and  $a_0 = 1$ , then there are integers  $a_{n-1}, a_{n-2}, \dots, a_1$  for which  $f(x)$  has the irreducible quadratic factor  $x^2 - 3$  (or similarly  $x^2 + 3$ ).
- If  $a_n = k'' < k'$  and  $a_0 = 1$ , then there are integers  $a_{n-1}, a_{n-2}, \dots, a_1$  for which  $f(x)$  has the irreducible quartic factor  $x^4 - 5x^2 - 15$ .

We quickly address the situation where  $n \leq 2$  before restricting to  $n > 2$ . When  $n = 2$ , the polynomial  $f(x)$  is a quartic polynomial. Also,  $k' = 5$  and  $k'' = 1$ . From the comments after the statement of Lemma 2.2, we deduce that  $f(x)$  cannot have a linear or quadratic factor (and, thus,  $f(x)$  is irreducible) whenever  $n = 2$ ,  $0 < |a_n| < 5$  and  $|a_0| = 1$ . Furthermore, when  $n = 2$ ,  $|a_n| = 5$  and  $|a_0| = 1$ , by the lemma below, there exists an integer  $a_1$  such that  $x^2 - 3$  (or  $x^2 + 3$ ) is a factor of  $f(x)$ . When  $n = 1$ , we see that  $k' = k'' = 1$  and  $f(x) = a_1x^2/3 + a_0$ , which is a quadratic polynomial, and one can check that it is irreducible for  $0 < |a_1| < 3$  and  $|a_0| = 1$ . For  $|a_1| = 3$  and  $|a_0| = 1$ , with  $a_1$  and  $a_0$  of opposite signs, the quadratic  $f(x)$  has the linear factors of  $x + 1$  and  $x - 1$ .

For our goals above, we first show that, for  $n \geq 2$ , there exist integers  $a_{n-1}, a_{n-2}, \dots, a_1$  so that we can make  $x^2 - 3$  or  $x^2 + 3$  (whichever we choose) a factor of  $f(x)$  when  $a_n = k'$  and  $a_0 = 1$ .

**Lemma 5.1.** *Let  $n$  be an integer  $\geq 2$ , and let  $k'$  be the integer such that  $2n+1 = k'3^u$  where  $u$  is an integer  $\geq 0$  and  $(k', 3) = 1$ . If  $a_n = k'$  and  $a_0 = 1$ , then there exist integers  $a_{n-1}, a_{n-2}, \dots, a_1$  such that  $x^2 - 3$  (or  $x^2 + 3$ ) is a factor of  $f(x)$ .*

*Proof.* Examples showing that the lemma holds for  $n = 2$  are given by

$$u_6 f(x) = 5x^4 - 20x^2 + 15 = 5(x+1)(x-1)(x^2-3), \\ u_6 f(x) = 5x^4 + 20x^2 + 15 = 5(x^2+1)(x^2+3).$$

We now consider  $n \geq 3$ . Let  $a_n = k'$ ,  $a_0 = 1$ , and  $a_{n-2} = a_{n-3} = \dots = a_2 = 0$ . Then

$$u_{2n+2} f(x) = k'x^{2n} + a_{n-1}c_{n-1}x^{2n-2} + a_1c_1x^2 + c_0$$

where  $c_{n-1} = 2n + 1 = k'3^u$ ,  $c_0 = u_{2n+2} = 3 \times 5 \times \cdots \times (2n - 1) \times k'3^u$ , and  $c_1 = u_{2n+2}/3 = 5 \times \cdots \times (2n - 1) \times k'3^u$ . Let  $c = \nu_3(u_{2n+2})$ . Since  $n \geq 3$ , we have  $c > u = \nu_3(c_{n-1})$ . Then  $c - 1 = \nu_3(u_{2n+2}/3)$ . Let  $m$  be the integer for which  $c_0 = u_{2n+2} = k'3^c m$  where  $(3, m) = 1$ . Note that  $k'$  and  $m$  may not be coprime. Let  $t = x^2$  and consider the polynomial  $F(t)$  where

$$F(t) = k't^n + a_{n-1}c_{n-1}t^{n-1} + a_1c_1t + c_0.$$

We will obtain  $t - 3$  as a factor of  $F(t)$ , and thus  $x^2 - 3$  as a factor of  $f(x)$ , by choosing  $a_{n-1}$  and  $a_1$  so that  $F(3) = 0$ .

First, we show  $c = \nu_3(u_{2n+2}) \leq n - 1$ . Since  $n \geq 3$ , we have  $\nu_3(n!) \geq 1$ . Hence, we obtain

$$\begin{aligned} c &= \nu_3((2n + 1)!) - \nu_3(2 \times 4 \times \cdots \times (2n)) \\ &= \nu_3((2n + 1)!) - \nu_3(n!) \\ &= \sum_{j=1}^{\infty} \left\lfloor \frac{2n + 1}{3^j} \right\rfloor - \nu_3(n!) \\ &< \sum_{j=1}^{\infty} \frac{2n + 1}{3^j} - \nu_3(n!) \\ &= \frac{2n + 1}{2} - 1 = n - (1/2). \end{aligned}$$

Since  $c \in \mathbb{Z}$ , we deduce  $c \leq n - 1$ .

We are now ready to show that we can choose  $a_{n-1}$  and  $a_1$  so that  $F(3) = 0$ . Setting  $m' = 3^{n-c} + m \in \mathbb{Z}$  and using our notation above, we see that

$$\begin{aligned} F(3) &= k'3^n + a_{n-1}c_{n-1}3^{n-1} + a_1c_13 + c_0 \\ &= k'3^n + a_{n-1}k'3^{n+u-1} + a_1k'3^c m + k'3^c m \\ &= k'3^c(3^{n-c} + a_{n-1}3^{n+u-1-c} + a_1m + m) \\ &= k'3^c(m' + a_{n-1}3^{n+u-1-c} + a_1m). \end{aligned}$$

Since  $3^{n+u-1-c}$  and  $m$  are relatively prime integers, there exist integers  $s$  and  $t$  such that

$$3^{n+u-1-c}s + mt = 1.$$

By taking  $a_{n-1} = -sm'$  and  $a_1 = -tm'$ , we deduce that  $F(3) = 0$ , as we wanted.

By a very similar analysis, one can show  $x^2 + 3$  can be a factor of  $f(x)$  when  $a_n = k'$  and  $a_0 = 1$ , concluding the proof of Lemma 5.1.

We are left with considering the case that  $a_n = k'' < k'$  and  $a_0 = 1$ . We restrict to  $n \geq 3$ , and note that  $k'' < k'$  implies then that  $n \geq 12$ . The definitions of  $k'$  and  $k''$  further give that if  $k'' < k'$ , then  $5 \mid (2n + 1)$ . Also, we see that  $3 \nmid (2n + 1)$  since otherwise  $k' \leq (2n + 1)/3 < 2n - 1 \leq k''$ . Hence, we can write  $2n - 1 = 3^k m$  and  $2n + 1 = 5^\ell m'$  where  $k$  is a nonnegative integer and  $n$ ,  $\ell$ ,  $m$ , and  $m'$  are positive integers with  $n \geq 12$  and  $\gcd(mm', 15) = 1$ . Observe that  $k'' = mm'$ . With this notation, set  $a_n = mm'$ . We show that there exist integers  $a_{n-1}, a_{n-2}, \dots, a_1$  such that the polynomial

$$f(t) = a_n \frac{x^{2n}}{u_{2n+2}} + a_{n-1} \frac{x^{2n-2}}{u_{2n}} + \cdots + a_1 \frac{x^2}{3} + 1$$

has the quartic factor  $x^4 - 5x^2 - 15$ . Let  $t = x^2$ , and let

$$F(t) = a_n \frac{t^n}{u_{2n+2}} + a_{n-1} \frac{t^{n-1}}{u_{2n}} + \cdots + a_1 \frac{t}{3} + 1.$$

Note that  $F(x^2) = f(x)$ . Thus, it suffices to show that  $F(t)$  is divisible by the quadratic  $q(t) = t^2 - 5t - 15$ . To do this, we multiply  $F(t)$  by  $u_{2n+2}$  and divide through by  $a_n = mm'$  to obtain the polynomial

$$t^n + 5^\ell \frac{a_{n-1}}{m} t^{n-1} + 5^\ell 3^k a_{n-2} t^{n-2} + \cdots + 5^{\ell-1} 3^{k-1} u_{2n-2} a_2 t^2 + 5^\ell 3^{k-1} u_{2n-2} a_1 t + 5^\ell 3^k u_{2n-2}.$$

Let  $r, s, y$  and  $w$  be variables representing integers, and take  $a_{n-1} = mr$ ,  $a_{n-2} = s$ ,  $a_{n-3} = a_{n-4} = \cdots = a_3 = 0$ ,  $a_2 = -y$ , and  $a_1 = w + y$ . The polynomial above becomes

$$g(t) = t^n + 5^\ell r t^{n-1} + 5^\ell 3^k s t^{n-2} - 5^{\ell-1} 3^{k-1} u_{2n-2} y t^2 + 5^\ell 3^{k-1} u_{2n-2} (w + y) t + 5^\ell 3^k u_{2n-2}.$$

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

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

$$t^j \equiv b_j t + c_j \pmod{q(t)}.$$

Since

$$t^{j+1} \equiv 5t^j + 15t^{j-1} \pmod{q(t)}, \quad \text{for } j \geq 1, \quad (5.16)$$

we deduce

$$c_{j+1} = 5c_j + 15c_{j-1} \quad \text{and} \quad b_{j+1} = 5b_j + 15b_{j-1}, \quad \text{for } j \geq 1. \quad (5.17)$$

Letting

$$A = \begin{pmatrix} 0 & 1 \\ 15 & 5 \end{pmatrix},$$

we obtain from (5.17) and an induction argument that

$$A^j = \begin{pmatrix} c_j & b_j \\ c_{j+1} & b_{j+1} \end{pmatrix}, \quad \text{for } j \geq 0.$$

Next, we obtain some results for the values of  $\nu_3(c_j)$ ,  $\nu_3(b_j)$ ,  $\nu_5(c_j)$ , and  $\nu_5(b_j)$ . An induction argument gives that

$$A^{2j} \equiv \begin{pmatrix} 6 & 5 \\ 3 & 4 \end{pmatrix} \pmod{9} \quad \text{and} \quad A^{2j+1} \equiv \begin{pmatrix} 3 & 4 \\ 6 & 5 \end{pmatrix} \pmod{9}, \quad \text{for } j \geq 1.$$

Hence, we see that

$$\nu_3(c_j) = 1 \quad \text{and} \quad \nu_3(b_j) = 0, \quad \text{for } j \geq 2. \quad (5.18)$$

Next, we claim that

$$\nu_5(c_j) \geq \frac{j}{2} \quad \text{and} \quad \nu_5(b_j) \geq \frac{j-1}{2}, \quad \text{for } j \geq 2. \quad (5.19)$$

For  $j = 2$  and  $j = 3$ , one checks directly that (5.19) holds. From (5.17), we deduce

$$\nu_5(c_{j+1}) \geq \min\{\nu_5(c_j), \nu_5(c_{j-1})\} + 1$$

and

$$\nu_5(b_{j+1}) \geq \min\{\nu_5(b_j), \nu_5(b_{j-1})\} + 1.$$

By induction, we obtain that (5.19) holds.

Using that  $\det(A^j) = \det(A)^j$ , we obtain

$$c_j b_{j+1} - c_{j+1} b_j = \pm 15^j. \quad (5.20)$$

Given (5.19), we deduce that, for  $j \geq 2$ , at least one of  $\nu_5(c_j) = j/2$  and  $\nu_5(c_{j+1}) = (j+1)/2$  holds. Only one of  $j/2$  and  $(j+1)/2$  can be an integer. It follows that

$$\nu_5(c_j) = \frac{j}{2} \quad \text{for } j \geq 2 \text{ even.} \quad (5.21)$$

Note that parity considerations also imply from (5.19) that  $\nu_5(c_j) \geq (j+1)/2$  if  $j$  is odd and that  $\nu_5(b_j) \geq j/2$  if  $j$  is even.

Recall that  $t^2 \equiv 5t + 15 \pmod{q(t)}$ . We obtain from the definitions  $g(t)$ ,  $b_j$  and  $c_j$  that

$$g(t) \equiv (b_n + 5^\ell r b_{n-1} + 5^\ell 3^k s b_{n-2} + 5^\ell 3^{k-1} w u_{2n-2})t + c_n + 5^\ell r c_{n-1} + 5^\ell 3^k s c_{n-2} + 5^\ell 3^k u_{2n-2}(1-y)$$

modulo  $q(t)$ . We will show that for some integers  $r$ ,  $s$ ,  $y$ , and  $w$ , we have

$$b_n + 5^\ell r b_{n-1} + 5^\ell 3^k s b_{n-2} + 5^\ell 3^{k-1} w u_{2n-2} = 0$$

and

$$c_n + 5^\ell r c_{n-1} + 5^\ell 3^k s c_{n-2} + 5^\ell 3^k u_{2n-2}(1-y) = 0.$$

It will then follow that  $g(t) \equiv 0 \pmod{q(t)}$ .

We first show that there are integers  $r$ ,  $s$ , and  $y$  such that

$$5^\ell r c_{n-1} + 5^\ell 3^k s c_{n-2} = -(c_n + 5^\ell 3^k u_{2n-2}(1-y)).$$

Observe that  $n \geq 12$  and (5.17) imply  $c_{n-1} > 0$  and  $c_{n-2} > 0$ . Since in general, the Diophantine equation  $ax + by = c$  for fixed positive integers  $a$  and  $b$  and for an integer  $c$  has solutions in integers  $x$  and  $y$  if and only if  $\gcd(a, b) \mid c$ , the above equation in  $r$ ,  $s$ , and  $y$  will have integer solutions in  $r$  and  $s$  if we can choose  $y$  so that

$$\gcd(5^\ell c_{n-1}, 5^\ell 3^k c_{n-2}) \mid (c_n + 5^\ell 3^k u_{2n-2}(1-y)). \quad (5.22)$$

Since  $2n+1 = 5^\ell m'$  and

$$\nu_5((2n+1)!) < \frac{2n+1}{5} + \frac{2n+1}{5^2} + \frac{2n+1}{5^3} + \dots = \frac{2n+1}{4},$$

we obtain

$$\nu_5(5^\ell 3^k u_{2n-2}) \leq n/2. \quad (5.23)$$

Also, (5.19) implies  $\nu_5(c_n) \geq n/2$ . It follows that, by choosing  $1-y$  to satisfy a congruence modulo a sufficiently large power of 5, there is an integer  $y$  such that

$$\nu_5(c_n + 5^\ell 3^k u_{2n-2}(1-y)) \geq \ell + \min\{\nu_5(c_{n-1}), \nu_5(c_{n-2})\}.$$

We may also find such a  $y$  with  $1-y$  divisible by 3. Fix such a  $y$ . From (5.18), we obtain

$$\begin{aligned} \nu_3(c_n + 5^\ell 3^k u_{2n-2}(1-y)) &\geq 1 = \nu_3(5^\ell c_{n-1}) \\ &\geq \min\{\nu_3(5^\ell c_{n-1}), \nu_3(5^\ell 3^k c_{n-2})\}. \end{aligned}$$

Note that (5.20) implies that 3 and 5 are the only prime factors possibly in common with  $c_{n-1}$  and  $c_{n-2}$ . We deduce that (5.22) holds, and therefore there exist integers  $r_0$  and  $s_0$  such that

$$c_n + 5^\ell r_0 c_{n-1} + 5^\ell 3^k s_0 c_{n-2} + 5^\ell 3^k u_{2n-2}(1-y) = 0. \quad (5.24)$$

We fix  $r_0$  and  $s_0$  as above and observe that, for every integer  $t$ , we have

$$c_n + 5^\ell c_{n-1}(r_0 + 3^k c_{n-2}t) + 5^\ell 3^k c_{n-2}(s_0 - c_{n-1}t) + 5^\ell 3^k u_{2n-2}(1-y) = 0.$$

We set

$$r = r_0 + 3^k c_{n-2} t \quad \text{and} \quad s = s_0 - c_{n-1} t$$

and seek  $t$  and  $w$  so that

$$b_n + 5^\ell r b_{n-1} + 5^\ell 3^k s b_{n-2} + 5^\ell 3^{k-1} w u_{2n-2} = 0.$$

In other words, we want

$$5^\ell 3^{k-1} w u_{2n-2} + 5^\ell 3^k (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}) t + b_n + 5^\ell r_0 b_{n-1} + 5^\ell 3^k s_0 b_{n-2} = 0.$$

By (5.17), we can rewrite this equation as

$$5^\ell 3^{k-1} w u_{2n-2} + 5^\ell 3^k (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}) t + (5^\ell r_0 + 5) b_{n-1} + (5^\ell 3^k s_0 + 15) b_{n-2} = 0. \quad (5.25)$$

From (5.17) and (5.24), we obtain

$$(5^\ell r_0 + 5) c_{n-1} + (5^\ell 3^k s_0 + 15) c_{n-2} + 5^\ell 3^k u_{2n-2} (1 - y) = 0. \quad (5.26)$$

From  $n \geq 12$  and (5.17), we see that each of  $b_{n-2}$ ,  $b_{n-1}$ ,  $c_{n-2}$  and  $c_{n-1}$  is nonzero. Multiplying both sides of (5.25) by  $c_{n-1}$  and both sides of (5.26) by  $-b_{n-1}$  and then adding, we obtain

$$\begin{aligned} c_{n-1} 5^\ell 3^{k-1} u_{2n-2} w + c_{n-1} 5^\ell 3^k (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}) t \\ - (5^\ell 3^k s_0 + 15) (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}) \\ - 5^\ell 3^k u_{2n-2} (1 - y) b_{n-1} = 0. \end{aligned} \quad (5.27)$$

Multiplying both sides of (5.25) by  $c_{n-2}$  and both sides of (5.26) by  $-b_{n-2}$  and then adding, we obtain

$$\begin{aligned} c_{n-2} 5^\ell 3^{k-1} u_{2n-2} w + c_{n-2} 5^\ell 3^k (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}) t \\ + (5^\ell r_0 + 5) (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}) \\ - 5^\ell 3^k u_{2n-2} (1 - y) b_{n-2} = 0. \end{aligned} \quad (5.28)$$

Observe that (5.26) implies that if either (5.27) or (5.28) holds, then so does (5.25). Recall (5.21) and the comment after it. We work with (5.27) if  $n$  is odd and make use of  $\nu_5(c_{n-1}) = (n-1)/2$ ,  $\nu_5(c_{n-2}) \geq (n-1)/2$ , and  $\nu_5(b_{n-1}) \geq (n-1)/2$ . For  $n$  even, we work with (5.28) and make use of  $\nu_5(c_{n-1}) \geq n/2$ ,  $\nu_5(c_{n-2}) = (n-2)/2$ , and  $\nu_5(b_{n-2}) \geq (n-2)/2$ . We give the details of the argument in the case that  $n$  is odd, and simply note that a similar argument works in the case  $n$  is even.

Fix  $n \geq 12$  odd. Let

$$\begin{aligned} c &= c_{n-1} 5^\ell 3^{k-1} u_{2n-2}, \quad c' = c_{n-1} 5^\ell 3^k (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}), \\ c'' &= (5^\ell 3^k s_0 + 15) (c_{n-2} b_{n-1} - c_{n-1} b_{n-2}), \end{aligned}$$

and

$$c''' = 5^\ell 3^k u_{2n-2} (1 - y) b_{n-1}.$$

From (5.23), we deduce

$$\nu_5(c) \leq \frac{n}{2} + \frac{n-1}{2} = n - \frac{1}{2} \quad \implies \quad \nu_5(c) \leq n - 1.$$

Observe that

$$\nu_3((2n-1)!) < \frac{2n-1}{3} + \frac{2n-1}{3^2} + \frac{2n-1}{3^3} + \cdots = \frac{2n-1}{2} = n - \frac{1}{2}.$$



Since  $2n - 1 = 3^k m$ , we see that

$$\begin{aligned}\nu_3(3^{k-1}u_{2n-2}) &= \nu_3(u_{2n}) - 1 \\ &= \nu_3((2n-1)!) - \nu_3(2 \times 4 \times \cdots \times (2n-2)) - 1.\end{aligned}$$

Since  $n \geq 12$ , we have  $\nu_3(2 \times 4 \times \cdots \times (2n-2)) \geq \nu_3(2 \times 4 \times \cdots \times 22) = 4$ . Thus,  $\nu_3(3^{k-1}u_{2n-2}) \leq \nu_3((2n-1)!) - 5$ . From (5.18), we see that

$$\nu_3(c) \leq \nu_3(c_{n-1}) + \nu_3(3^{k-1}u_{2n-2}) \leq \nu_3((2n-1)!) - 4 < n - 4.$$

Since  $\nu_3(c)$  is an integer, we obtain

$$\nu_3(c) \leq n - 5.$$

Since  $\ell \geq 1$ , we have 5 divides  $5^\ell 3^k s_0 + 15$ . We obtain from (5.20) that

$$\nu_3(c'') \geq n - 2 \quad \text{and} \quad \nu_5(c'') \geq n - 1.$$

Observe that (5.18) implies  $\nu_3(c''') \geq \nu_3(c)$ . Since  $n$  is odd, we obtain from (5.21) and the comment after it that

$$\nu_5(b_{n-1}) \geq \frac{n-1}{2} = \nu_5(c_{n-1}).$$

Hence,  $\nu_5(c''') \geq \nu_5(c)$ . Combining the above, we deduce

$$\nu_3(c'' + c''') \geq \nu_3(c) \quad \text{and} \quad \nu_5(c'' + c''') \geq \nu_5(c).$$

We claim that  $\gcd(c, c')$  divides  $c'' + c'''$ . Let  $p$  be a prime and  $u$  a positive integer for which  $p^u \parallel \gcd(c, c')$ . The above analysis shows that if  $p = 3$  or  $p = 5$ , then  $p^u \mid (c'' + c''')$ . Now, consider the case that  $p$  is not 3 or 5. From (5.20) and the definition of  $c'$ , we obtain that  $p^u \mid c_{n-1}$ . From (5.26), we see that  $p^u$  must also divide

$$((5^\ell 3^k s_0 + 15)c_{n-2} + 5^\ell 3^k u_{2n-2}(1-y))b_{n-1} - (5^\ell 3^k s_0 + 15)b_{n-2}c_{n-1},$$

which is the same as  $c'' + c'''$ . 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 (5.25) and, hence, the existence of integers  $r, s, y$ , and  $w$  for which  $g(x)$  is divisible by  $x^2 - 5x - 15$ .

## References

- [All01] M. Allen, *Generalizations of the Irreducibility Theorems of I. Schur*, Dissertation from the University of South Carolina, 2001.
- [AlFi03] M. Allen and M. Filaseta, A generalization of a second irreducibility theorem of I. Schur, *Acta Arith.*, **109** (2003), 65–79.
- [AlFi04] M. Allen and M. Filaseta, A generalization of a third irreducibility theorem of I. Schur, *Acta Arith.*, **114** (2004), 183–197.
- [Dum1906] G. Dumas, Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels, *Journal de Math. Pures et Appl.*, **2** (1906), 191–258.
- [Fil96] M. Filaseta, A generalization of an irreducibility theorem of I. Schur, *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.
- [Hux72] M.N. Huxley, On the difference between consecutive primes, *Invent. Math.*, **15** (1972), 155–164.
- [Jak23] A. Jakhar, *On Schur's irreducibility results and generalised  $\varphi$ -Hermite polynomials*, arXiv:2306.01767.
- [Mah61] K. Mahler, *Lectures on Diophantine Approximations*, Cushing-Malloy, Ann Arbor, 1961.
- [Mor69] L.J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.
- [Sch29a] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I, *Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl.*, **14** (1929), 125–136.

[Sch29b] I. Schur, Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, II, *Sitzungsber. Preuss. Akad. Wiss. Berlin Phys.-Math. Kl.*, **14** (1929), 370–391.

**Martha Allen**

Department of Mathematics and Computer Science  
Georgia College and State University  
Milledgeville, GA 31061, U.S.A.  
*e-mail*: martha.allen@gcsu.edu

**Michael Filaseta**

Mathematics Department  
University of South Carolina  
Columbia, SC 29208, U.S.A.  
*e-mail*: filaseta@math.sc.edu