LAGUERRE POLYNOMIALS WITH GALOIS GROUP A_m FOR EACH m

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

Travis Kidd
Mathematics Department
University of South Carolina
Columbia, SC 29208

Ognian Trifonov
Mathematics Department
University of South Carolina
Columbia, SC 29208

Abstract

In 1892, D. Hilbert began what is now called Inverse Galois Theory by showing that for each positive integer m, there exists a polynomial of degree m with rational coefficients and associated Galois group S_m, the symmetric group on m letters, and there exists a polynomial of degree m with rational coefficients and associated Galois group A_m, the alternating group on m letters. In the late 1920's and early 1930's, I. Schur found concrete examples of such polynomials among the classical Laguerre polynomials except in the case of polynomials with Galois group A_m where $m \equiv 2 \pmod 4$. Following up on work of R. Gow from 1989, this paper complements the work of Schur by showing that for every positive integer $m \equiv 2 \pmod 4$, there is in fact a Laguerre polynomial of degree m with associated Galois group A_m.

1 Introduction

The generalized Laguerre polynomials are defined by

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

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

The first and third author express their appreciation to the National Science Foundation for support during the research for this paper. The first author also expresses his gratitude the National Security Agency for their support.

I. Schur [20, 21] showed that for every positive integer m, the polynomial $L_m^{(0)}(x)$ is irreducible (over $\mathbb{Q}$) and has associated Galois group the symmetric group S_m. He showed that $L_m^{(1)}(x)$ is irreducible for all positive integers m and has associated Galois group the alternating group A_m if $m > 1$ and m is odd; otherwise, the Galois group is S_m. Further, he showed that the polynomials $L_m^{(-m-1)}(x)$ (which correspond to a truncated McClaurin series for e^x) have associated Galois group A_m if $m \equiv 0 \pmod 4$ and, otherwise, have associated Galois group S_m. He notes in [20] that he has a specific class of polynomials where the associated Galois group is A_m only in the case $m \not\equiv 2 \pmod 4$. The problem of finding nice examples where the Galois group is A_m is further tantalizing as B. L. van der Waerden [24] showed that a random polynomial in $\mathbb{Z}[x]$ will have associated Galois group S_m with probability 1 so that, in particular, examples with Galois group A_m are rare.

There have been a variety of recent results concerning the irreducibility and Galois structure of $L_m^{(\alpha)}(x)$. M. Filaseta and T.-Y. Lam [6] showed that if α is a rational number that is not a negative integer, then $L_m^{(\alpha)}(x)$ is irreducible for m sufficiently large. F. Hajir [11, 12, 13] and E. A. Sell [23] have investigated the irreducibility and Galois groups associated with $L_m^{(\alpha)}(x)$ for $\alpha = -m - r$ where r is a positive integer. In particular, Hajir shows that for r large and m sufficiently large depending on r, the polynomial $L_m^{(-m-r)}(x)$ is irreducible and has associated Galois group S_m. There are cases that arise in their work where the Galois group is A_m, but not for $m \equiv 2 \pmod 4$. Hajir also notes that the Bessel polynomials, which were determined to be irreducible by M. Filaseta and O. Trifonov in [7], are actually the case $\alpha = -2m - 1$ of the Laguerre polynomials. As a consequence of work of Grosswald [10], $L_m^{(-2m-1)}(x)$ has associated Galois group S_m.

Interesting work of R. Gow [9] deals precisely with the original problem suggested by I. Schur of finding classical polynomials with Galois group A_m when $m \equiv 2 \pmod 4$. He considers the case $\alpha = m$ above, specifically the polynomials

$$L_m^{(m)}(x) = \sum_{j=0}^{m} (-1)^j \binom{2m}{m-j} \frac{x^j}{j!}.$$

Gow [9] shows that if m is an even integer > 2, then the Galois group associated with $L_m^{(m)}(x)$ is A_m (the alternating group) provided that the polynomial $L_m^{(m)}(x)$ is irreducible over the rationals. Gow deduced from his result that for infinitely many $m \equiv 2 \pmod 4$, the Galois group of $L_m^{(m)}(x)$ is A_m by showing that whenever $m = 2p^k$ where p is a prime > 3 and k is a positive integer, the polynomial $L_m^{(m)}(x)$ is irreducible. M. Filaseta and R. Williams [8] extended Gow's work by showing that asymptotically almost all $L_m^{(m)}(x)$ are irreducible (and, hence, almost all even m are such that $L_m^{(m)}(x)$ has associated Galois group A_m). But the question of Schur remained open as to whether there are classical polynomials, perhaps Laguerre polynomials $L_m^{(\alpha)}(x)$, which can be shown to have associated Galois group A_m for *every* positive integer $m \equiv 2 \pmod 4$.

Such problems have a long history. As far back as 1892, Hilbert [14] showed the existence of polynomials with Galois group S_m and with Galois group A_m for every m by making use of the now classical Hilbert's Irreducibility Theorem. Hilbert's work began what is now called the Inverse Galois Theory Problem, the problem of realizing transitive permutation groups as Galois

groups of polynomials. Schur's work can be viewed as an early initiative to construct specific examples where the groups S_m and A_m occur as Galois groups of polynomials. Explicit examples can be obtained from work since then (cf. [17]). Nevertheless, the examples constructed by Schur and suggested by Gow are of a different nature, involving classical polynomials.

In this paper, we complement the above work of Schur. Following the work of Gow [9], and working along the lines of Filaseta and Trifonov in [7] and of Filaseta and Williams in [8], we show that $L_m^{(m)}(x)$ is irreducible for every $m \equiv 2 \pmod 4$ with $m > 2$. In fact, $L_2^{(2)}(x)$ is reducible, and this is precisely what is needed to deduce that the Galois group associated with $L_m^{(m)}(x)$ is, for every positive integer $m \equiv 2 \pmod 4$, the alternating group A_m. More precisely, we show the following.

Theorem 1. *For every integer $m > 2$ with $m \equiv 2 \pmod 4$, the polynomial $L_m^{(m)}(x)$ is irreducible over $\mathbb{Q}$. Furthermore, for every positive integer m, either the polynomial $L_m^{(m)}(x)$ is irreducible or it is a linear polynomial times an irreducible polynomial of degree $m-1$.*

Corollary 1. *For each positive integer m, there is an integer α such that $L_m^{(\alpha)}(x)$ has Galois group the alternating group A_m.*

Theorem 1 will follow as a consequence of a more general result suggested by the prior work in [7] and [8]. We define integers $b_j = b_j^{(m)}$ by the equation

$$m!L_m^{(m)}(x) = \sum_{j=0}^{m} (-1)^j b_j x^j.$$

Thus,

$$b_j = \binom{m}{j}(2m)(2m-1)\cdots(m+j+1) \qquad \text{for } 0 \le j \le m.$$

Note that for $j = m$ the above is to be interpreted as asserting $b_m = 1$. Our main result is the following.

Theorem 2. *Let m be an integer > 2, and let $a_0, a_1, \ldots, a_m$ be arbitrary integers with $|a_0| = |a_m| = 1$. Set $G(x) = \sum_{j=0}^{m} a_j b_j x^j$, with b_j defined as above. If $G(x)$ is reducible, then $m \equiv 0 \pmod 4$ and $G(x)$ is a linear polynomial times an irreducible polynomial of degree $m-1$.*

It is clear that Theorem 2 implies Theorem 1. We note that Filaseta and Williams [8] have shown that there are infinitely many m such that for some $a_0, a_1, \ldots, a_m$ as in Theorem 2, the polynomial $G(x)$ has a linear factor. In particular, it is possible for $G(x)$ to be reducible. For reducible $G(x)$, our arguments give more. One can show, for example, that for every $\varepsilon > 0$, there is an effective $M = M(\varepsilon)$ such that if $G(x)$ is reducible and $m > M$, then $m = 2^k m'$ where m' is an odd integer satisfying

$$m' < \exp\left((1+\varepsilon)\frac{\log m}{\log\log m}\right).$$

In addition to previous methods employed in the subject, our approach makes use of new information obtained from the coefficients of the Laguerre polynomials, explicit estimates in the distribution of primes, and recent results from Diophantine approximation by S. Laishram and T. N. Shorey [15] and two of the authors and M. Bennett [1].

2 Preliminaries

In this section, we give some preliminary results which will allow us to establish Theorem 2 by considering separately several cases depending on the possible degree of a factor. In the next section, we will give some further preliminary results that required some new computations on our part.

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

The proof of Theorem 2 will make use of a variety of lemmas, which we present here. The first lemma is Lemma 2 of [5].

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

Our interest is in taking $c_j = b_j$ as defined in the introduction. Throughout, then, we use that

$$g(x) = \sum_{j=0}^{m} b_j x^j = \sum_{j=0}^{m} \binom{m}{j} (2m)(2m-1)\cdots(m+j+1)\, x^j.$$

In this case, $G(x)$ in Lemma 1 is equivalent to $G(x)$ as defined in Theorem 2.

Lemma 2. *Let k and r be positive integers with $r \geq 2$, let ℓ be a nonnegative integer less than k, and let p be a prime number. Then $G(x)$ does not have a factor of degree k if all of the following conditions hold:*

(i) $p^r || (m-\ell)$

(ii) $p \geq \max\{k+2, 2k-1\}$

(iii) $\dfrac{\log(2m)}{p^{r/2}\log p} + \dfrac{1}{p-1} \leq \dfrac{1}{k}$.

The above lemma is Lemma 5 in [8], and the proof given there is an application of Lemma 1 above. We will see a similar argument momentarily in our proof of Lemma 4 below. Next, we give a slight modification of Lemma 4 in [8].

Lemma 3. *Suppose that p is a prime, that k and r are positive integers, and that ℓ is an integer in $[0, k)$ satisfying:*

(i) $p^r || (m - \ell)$

(ii) $p \geq 3k$

(iii) $\Delta \dfrac{\log(2m)}{p^r \log p} + \dfrac{1}{p-1} \leq \dfrac{1}{k}$ *where* $\Delta = \Delta(r, p) = \dfrac{6p^{r-1}}{3p^{r-1} - 1}$.

Then $G(x)$ cannot have a factor with degree in $[\ell + 1, k]$.

The modification is in our statement of condition (ii). In [8], this condition was stated as $p \geq 3k + 1$. Since p is a prime, this change is only of significance when $k = 1$ and $p = 3$. We will want to take advantage of this change when $k = 1$, so we clarify how the argument in [8] can be adjusted accordingly. First, in the display after (5) of that paper, the expression

$$\frac{1}{p-1} + \frac{4}{p\left(p - \frac{1}{3}\right)}$$

occurs and an argument is given to show that this is $\leq 1/k$. In the case that $k = 1$ and $p = 3$, one can check this directly (indeed, the above expression equals $1/k$ in this case). The only other modification needed in the argument is in the case where $e = 1$ and $j < p$ given at the bottom of page 236 and top of page 237. One checks that the argument given establishes the desired result unless $j = 1$. Given that $\ell \in [0, k)$ and $k = 1$, we see that $\ell = 0$ so that $p = 3$ divides m by condition (i) of the lemma. In the argument in [8], the integer i satisfies $1 \leq i \leq j$ and, hence, $i = 1$. This leads to an impossibility as $p = 3$ must divide both m and $m + i = m + 1$. Thus, the situation $e = 1$ and $j < p$ cannot occur when $k = 1$ and $p = 3$ and the change in (ii) is justified.

Corollary 2. *Let k, r, ℓ, and p be as in Lemma 3 with condition (i) holding and such that $p \geq 3k+1$. Suppose that $r \geq 2$ and that $G(x)$ has a factor of degree k. Then*

$$m > \frac{1}{2}(3k + 1)^{3k+1}.$$

Also,

$$p^r < \frac{3k + 1}{\log(3k + 1)} \log(2m).$$

Proof. Since $G(x)$ has a factor of degree k, Lemma 3 (iii) cannot hold, so that

$$\Delta \frac{\log(2m)}{p^r \log p} + \frac{1}{p-1} > \frac{1}{k}.$$

Hence,

$$\log(2m) > \frac{p^r \log p}{\Delta} \left(\frac{1}{k} - \frac{1}{p-1}\right) = \frac{p^r}{2} \left(1 - \frac{1}{3p^{r-1}}\right) \left(\frac{1}{k} - \frac{1}{p-1}\right) \log p. \tag{1}$$

For the stated lower bound on m, we apply (1) to deduce

$$\begin{aligned}\log(2m) &> \frac{p}{2}\left(p^{r-1}-\frac{1}{3}\right)\left(\frac{1}{k}-\frac{1}{p-1}\right)\log p\\ &\geq \frac{3k+1}{2}\left(3k+\frac{2}{3}\right)\frac{2}{3k}\log(3k+1)\\ &> (3k+1)\log(3k+1).\end{aligned}$$

For the stated upper bound on p^r, we apply (1) to obtain

$$\begin{aligned}p^r &< 2\cdot\frac{\log(2m)}{\log p}\cdot\frac{3p^{r-1}}{3p^{r-1}-1}\cdot\frac{k(p-1)}{p-k-1}\\ &\leq 2\cdot\frac{\log(2m)}{\log(3k+1)}\cdot\frac{3p}{3p-1}\cdot\frac{k(p-1)}{p-k-1}\\ &\leq 2\cdot\frac{\log(2m)}{\log(3k+1)}\cdot\frac{9k+3}{9k+2}\cdot\frac{3k}{2}\\ &= 3k\left(1+\frac{1}{9k+2}\right)\frac{\log(2m)}{\log(3k+1)}\\ &< \frac{3k+1}{\log(3k+1)}\log(2m).\end{aligned}$$

This establishes the corollary. □

The next lemma is proved largely by following the argument for Lemma 3 in [8].

Lemma 4. *Let m be a positive integer. Suppose that p is a prime, that k is a positive integer $\leq m/2$, and that ℓ is an integer in $[0,k)$ such that $p|(m-\ell)$. If $G(x)$ has a factor with degree in $[\ell+1,k]$, then*

$$p \leq k + k\left\lfloor\frac{\log(2m)}{\log p}\right\rfloor. \tag{2}$$

Proof. Recall $g(x)=\sum_{j=0}^{m} b_j x^j$ where

$$\begin{aligned}b_j &= \binom{m}{j}(2m)(2m-1)\cdots(m+j+1) \qquad (3)\\ &= \binom{2m}{m-j}m(m-1)\cdots(j+1).\end{aligned}$$

Since $b_m = 1$, $p \nmid b_m$. Also, from the second formulation of b_j in (3), if $p|(m-\ell)$, then p divides b_j for $j \in \{0, 1, \ldots, m-\ell-1\}$. By Lemma 1, the right-most edge of the Newton polygon of $G(x)$ with respect to p has slope $\geq 1/k$. The right-most edge has slope

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

Let j be such that $(\nu(b_0)-\nu(b_j))/j$ is maximal. We deduce that

$$\frac{\nu(b_0)-\nu(b_j)}{j} \geq \frac{1}{k}. \tag{4}$$

Observe that by (3),

$$\frac{b_0}{b_j} = \frac{(2m)(2m-1)\cdots(m+1)}{\binom{m}{j}(2m)(2m-1)\cdots(m+j+1)} = \frac{j!(m+j)!(m-j)!}{m!^2}.$$

Since

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

we deduce

$$\begin{aligned}\nu(b_0)-\nu(b_j) &= \nu(j!)+\nu\left(\frac{(m+j)!}{m!}\right)-\nu\left(\frac{m!}{(m-j)!}\right)\\ &< \frac{j}{p-1}+\sum_{s=1}^{\infty}\left(\left\lfloor\frac{m+j}{p^s}\right\rfloor-\left\lfloor\frac{m}{p^s}\right\rfloor\right)-\sum_{s=1}^{\infty}\left(\left\lfloor\frac{m}{p^s}\right\rfloor-\left\lfloor\frac{m-j}{p^s}\right\rfloor\right)\\ &= \frac{j}{p-1}+\sum_{s=1}^{N}\left(\left\lfloor\frac{m+j}{p^s}\right\rfloor-2\left\lfloor\frac{m}{p^s}\right\rfloor+\left\lfloor\frac{m-j}{p^s}\right\rfloor\right)\end{aligned} \tag{5}$$

where $N = \lfloor \log(2m)/\log p \rfloor$. Note that

$$\left\lfloor\frac{m+j}{p^s}\right\rfloor-2\left\lfloor\frac{m}{p^s}\right\rfloor+\left\lfloor\frac{m-j}{p^s}\right\rfloor < \frac{m+j}{p^s}-2\left(\frac{m}{p^s}-1\right)+\frac{m-j}{p^s} = 2,$$

so

$$\left\lfloor\frac{m+j}{p^s}\right\rfloor-2\left\lfloor\frac{m}{p^s}\right\rfloor+\left\lfloor\frac{m-j}{p^s}\right\rfloor \leq 1. \tag{6}$$

We show that

$$j > p-k. \tag{7}$$

Assume otherwise and choose e so that $p^e||(m+i)$ for some $1 \leq i \leq j$ with e maximal. Apparently, $e \geq 1$; otherwise, from the first equation in (5),

$$\nu(b_0)-\nu(b_j) = \nu(j!)-\nu\left(\frac{m!}{(m-j)!}\right) = -\nu\left(\binom{m}{j}\right) \leq 0,$$

which contradicts (4). Since $p|(m-\ell)$, then as $p|(m+i)$ we deduce $p|(i+\ell)$. Hence,

$$p \le i+\ell < j+k \le (p-k)+k = p,$$

and we obtain a contradiction. Thus, (7) holds.

Now, we consider three cases: $p-k<j<p$, $p \le j < p^2$, and $j \ge p^2$. For $p-k<j<p$, we use that $\nu(j!)=0$ in (5); for $p \le j < p^2$, we use that $\nu(j!) \le j/p$ in (5). We combine these observations with (4), (5), and (6). For $p-k<j<p$, we obtain

$$\frac{1}{k} \le \frac{\nu(b_0)-\nu(b_j)}{j} \le \frac{1}{j}\sum_{s=1}^{N} 1 = \frac{N}{j} < \frac{1}{p-k}\left\lfloor \frac{\log(2m)}{\log p} \right\rfloor.$$

For $p \le j < p^2$, we have

$$\frac{1}{k} \le \frac{\nu(b_0)-\nu(b_j)}{j} \le \frac{1}{p}+\frac{1}{j}\sum_{s=1}^{N} 1 = \frac{1}{p}+\frac{N}{j} \le \frac{1}{p}+\frac{1}{p}\left\lfloor \frac{\log(2m)}{\log p} \right\rfloor.$$

For $j \ge p^2$, we obtain

$$\frac{1}{k} \le \frac{\nu(b_0)-\nu(b_j)}{j} < \frac{1}{p-1}+\frac{1}{j}\sum_{s=1}^{N} 1 = \frac{1}{p-1}+\frac{N}{j} \le \frac{1}{p-1}+\frac{N}{p^2}.$$

Observe that the conditions in the lemma imply (2) holds if $p=2$. Also, $N \ge 1$. For $p>2$, one checks that

$$\frac{1}{p-1}+\frac{N}{p^2} \le \frac{1}{p}+\frac{1}{p}\left\lfloor \frac{\log(2m)}{\log p} \right\rfloor.$$

In each of the three cases, (2) now follows. □

The next lemma allows us to get a bound for the largest prime p satisfying (2).

Lemma 5. *Let $a>0$, $b>e$, and $x>1$ be real numbers such that*

$$x < a + \frac{b}{\log x}.$$

Then,

$$x < a + \frac{b}{\log b - \log\log b}. \tag{8}$$

Proof. Consider the function $f(x) = x\log x$ defined on $[1,\infty)$. Since f is increasing and its range is $[0,\infty)$, for every nonnegative real number r, there exists a unique real number $x_r \ge 1$ such that $x_r \log x_r = r$. We claim that $x_r < r/(\log r - \log\log r)$ when $r>e$. Indeed, for $r>e$, $r\log r > r$, and $x_r < r$, implying $\log x_r < \log r$. Thus, $x_r > r/\log r$, and $\log x_r > \log r - \log\log r$, proving our claim.

Assume the bound (8) does not hold, that is $x \ge a + b/(\log b - \log\log b)$. Note that this implies $x-a>e$ since $b/\log b > e$ for $b>e$ (the function $x/\log x$ is increasing for $x>e$). We have $x-a < b/\log x < b/\log(x-a)$. Thus, $x-a < x_b < b/(\log b - \log\log b)$ contradicting our assumption. □

The next lemma is based on an argument of Erdős [4].

Lemma 6. *Let m and k be positive integers with $k \le m/2$. Set*

$$C = \{m, m-1, \dots, m-k+1\} \quad \textit{and} \quad A = \prod_{u \in C} u.$$

Let z be a positive real number. For each prime $p \le z$, let $d_p \in C$ with $\nu_p(d_p)$ maximal. Let e_p be the largest power of p dividing d_p (i.e., $e_p = p^{\nu_p(d_p)}$). Define

$$Q_z = Q_z(m,k) = \prod_{p>z} p^{\nu_p(A)}.$$

Then

$$Q_z \ge \frac{m(m-1)\cdots(m-k+1)}{(k-1)!\prod_{p\le z} e_p} \ge \frac{(m-k+1)^{k-\pi(z)}}{(k-1)!}.$$

Proof. Let $r(p)$ be such that $e_p = p^{r(p)}$. By the definition of e_p, if $n \in C$ and $p^j | n$, then $j \le r(p)$. Hence,

$$\prod_{\substack{p\le z\\ p^j || A}} p^j = \prod_{p\le z}\prod_{n\in C}\prod_{\substack{1\le j\le r(p)\\ p^j|n}} p \le \prod_{p\le z}\prod_{m-k+1\le n\le m}\prod_{\substack{1\le j\le r(p)\\ p^j|n}} p \le \prod_{p\le z}\prod_{j=1}^{r(p)} p^{\left\lfloor \frac{m}{p^j}\right\rfloor - \left\lfloor \frac{m-k}{p^j}\right\rfloor}.$$

Using that $\lfloor \frac{x}{w}\rfloor - \lfloor \frac{y}{w}\rfloor \le \lfloor \frac{x-y-1}{w}\rfloor + 1$ for integers x, y, and w, we deduce that this last double product is at most

$$\prod_{p\le z}\prod_{j=1}^{r(p)} p^{\left\lfloor \frac{k-1}{p^j}\right\rfloor + 1} = \left(\prod_{p\le z}\prod_{j=1}^{r(p)} p^{\left\lfloor \frac{k-1}{p^j}\right\rfloor}\right)\prod_{p\le z} p^{r(p)} \le (k-1)!\prod_{p\le z} e_p.$$

Setting $t = \min\{k, \pi(z)\}$, we deduce that

$$\begin{aligned}\prod_{p>z} p^{\nu_p(A)} &= \frac{A}{\prod_{p\le z} p^{\nu_p(A)}} \ge \frac{m(m-1)\cdots(m-k+1)}{(k-1)!\prod_{p\le z} e_p}\\ &\ge \frac{m(m-1)\cdots(m-k+1)}{(k-1)!\cdot m(m-1)\cdots(m-t+1)}\\ &\ge \frac{(m-k+1)^{k-\pi(z)}}{(k-1)!},\end{aligned}$$

completing the proof. □

Next, we turn to some estimates from the distribution of primes. The following lemma follows from Rosser and Schoenfeld [19] and Schoenfeld [22].

Lemma 7. *For x a real number, let $\pi(x)$ denote the number of primes $p \le x$, and let $\theta(x) = \sum_{p \le x} \log p$. Then*

$$\theta(x) > \begin{cases} x\left(1 - \dfrac{1}{2\log x}\right) & \text{for } x \ge 563 \\ x\left(1 - \dfrac{1}{3.5\log x}\right) & \text{for } x \ge 2657 \end{cases}$$

$$\theta(x) < x\left(1 + \frac{1}{2\log x}\right) \quad \text{for } x > 1$$

and

$$\theta(x) < 1.000081x \quad \text{for } x > 0.$$

Also,

$$\pi(x) < \min\left\{1.256\frac{x}{\log x}, \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right)\right\} \quad \text{for } x > 1.$$

Corollary 3. *For every integer $k \ge 378$, $\pi(3k) \le k/2$.*

Proof. For $k > 1000$, Lemma 7 implies

$$\pi(3k) < \frac{1.256 \cdot 3k}{\log(3k)} < \frac{1.256 \cdot 3k}{\log 3000} < \frac{k}{2}.$$

Direct calculation shows that $\pi(3k) < k/2$ for $k \in (378, 1000]$ and $\pi(3k) = k/2$ for $k = 378$. □

Let A be as in Lemma 6, and let $r = r(p)$ be the nonnegative integer such that $p^r || A$. We use the following notation:

- $P_0 = \prod_{p \le 3k} p^{r(p)}$
- $P_1 = \prod_{\substack{p \ge 3k+1 \\ p || A}} p$
- $P_2 = \prod_{\substack{p \ge 3k+1 \\ r(p) > 1}} p^{r(p)}$
- $p_{\max}$ denotes the largest prime p such that $r(p) > 0$
- $y = y(m,k) = (3k+1)\log(2m)/\log(3k+1)$.

As usual, we view empty products above as being 1.

Next, we note the following estimates for P_1 and P_2.

Corollary 4. *We have*

$$\log P_1 \leq 1.000081 \left(k + \frac{k \log(2m)}{\log(k \log(2m)) - \log\log(k \log(2m))} \right) - \theta(3k).$$

Proof. Observe that $P_1 \leq \exp\big(\theta(p_{\max}) - \theta(3k)\big)$. Furthermore, Lemma 4 and Lemma 5 imply

$$p_{\max} \leq k + \frac{k \log(2m)}{\log(k \log(2m)) - \log\log(k \log(2m))}.$$

Using Lemma 7, we obtain the result. □

Corollary 5. *If $P_2 > 1$, then $\log P_2 \leq 2.512\sqrt{y} - \pi(3k) \log y$.*

Proof. Corollary 2 implies that every prime p dividing P_2 satisfies $3k < p \leq \sqrt{y}$ and that

$$P_2 = \prod_{p | P_2} p^{r(p)} < y^{\pi(\sqrt{y}) - \pi(3k)}.$$

The result now follows from an application of Lemma 7. □

The next lemma appears in [7] and can be deduced from Lemma 7 and some computations.

Lemma 8. *If $x \geq 2479$, then there exists a prime in the interval $(x, 1.01x]$.*

The next lemma follows directly from Table IA in a paper by D. H. Lehmer [16].

Lemma 9. *If $m > 11859211$, then $m(m-1)$ has a prime factor > 23. If $m > 123201$, then $m(m-1)$ has a prime factor > 13.*

The next result is also a consequence of this same work.

Lemma 10. *Let m' and m'' be two distinct integers each > 466830 with the largest prime factor of $m'(m'-1)m''(m''-1)$ being ≤ 41. Then $|m' - m''| \geq 1519$.*

Note that $1154440 - 1152921 = 1519$ so the number 1519 cannot be replaced by a larger number. The lemma follows from examining Table IB in [16]. Our interest in the above result is the following.

Corollary 6. *Let k be an integer in the interval $[3, 43]$. If $m > 10^6$, then the product*

$$m(m-1)\cdots(m-k+1)$$

has at least $\lceil k/2 \rceil - 1$ distinct prime factors ≥ 43.

Proof. As $k \le 43$, each prime ≥ 43 can divide at most one of the numbers $m, m-1, \dots, m-k+1$. Lemma 10 implies that there is at most one number $(m-j)(m-j-1)$ with $j \in [0, k-2]$ that has all its prime factors ≤ 41. If there are no such numbers, then the corollary follows by considering the $\lfloor k/2 \rfloor \ge \lceil k/2 \rceil - 1$ numbers

$$m(m-1), (m-2)(m-3), \dots, (m-2\lfloor k/2 \rfloor + 2)(m-2\lfloor k/2 \rfloor + 1).$$

So suppose there is exactly one $j \in [0, k-2]$ with $(m-j)(m-j-1)$ having all its prime factors ≤ 41. By considering whether j is even or odd separately, one checks that

$$\{(m-2i)(m-2i-1) : 0 \le i < j/2\} \cup \{(m-2i-1)(m-2i-2) : j/2 \le i \le \lceil k/2 \rceil - 2\}$$

consists of $\lceil k/2 \rceil - 1$ numbers, each necessarily having a prime factor ≥ 43. □

For $k \in [3, 43]$ and $m > 10^6$, Corollary 6 implies that $m(m-1)\cdots(m-k+1)$ has a prime factor at least as large as the $(\lceil k/2 \rceil - 1)$th prime after 41. Using $\alpha(k)$ to denote this lower bound on the largest prime factor of $m(m-1)\cdots(m-k+1)$, we have the following table of values.

k	3	4	5	6	7	8	9	10	11
$\alpha(k)$	43	43	47	47	53	53	59	59	61

The next lemma is a variation of Stirling's formula noted by H. Robbins (cf. [18]).

Lemma 11. *For every positive integer k, we have*

$$k! = \sqrt{2\pi}\, k^{k+\frac{1}{2}} e^{-k+\delta(k)},$$

where $1/(12k+1) < \delta(k) < 1/(12k)$.

In a few places, it will be convenient to have an upper bound for $\log\big((k-1)!\big)$. Therefore, we indicate here the following consequence of Lemma 11.

Corollary 7. *If k is an integer ≥ 7, then*

$$\log\big((k-1)!\big) < k\log k - k.$$

Proof. For $k \ge 7$, Lemma 11 implies

$$\begin{aligned}\log\big((k-1)!\big) &< \frac{1}{2}\log(2\pi) + \left(k - \frac{1}{2}\right)\log(k-1) - (k-1) + \frac{1}{12(k-1)} \\ &< k\log k - k.\end{aligned}$$

The corollary follows. □

The next lemma is a result of S. Laishram and T. N. Shorey [15].

Lemma 12. *Let $k \ge 2$ and $n \ge 1$ be integers. Denote by $P(v)$ the greatest prime divisor of v. We have*

$$P(n(n+1)\cdots(n+k-1)) > 2k \quad \textit{for } n > \max\left(k+13, \frac{279}{262}k\right).$$

3 Computational Preliminaries and the Start of the Proof

In this section, we give some further results that we will use. We have separated these results as they involve some computations on our part that we used to obtain Theorem 2. We note here that our computations were done with Maple 9.5. We also include in this section some closely related estimates from [1].

The next result will be useful in making various estimates. It will allow us to restrict attention to m being large, that is $> 10^6$, in various places.

Lemma 13. *If m is a positive integer ≤ 100 but not a power of 2 or the number 24, then the polynomial $G(x)$ does not have a linear factor. For every positive integer $m \leq 10^6$, the polynomial $G(x)$ does not have a factor of degree $k \in [2, m/2]$.*

Proof. We verified the first part of the above lemma as follows. We considered each $m \in [2, 100]$ in turn and set p to be the maximum prime divisor of m. It follows that $p \nmid b_m$ and $p|b_j$ for $0 \leq j \leq m-1$. We then checked the slope of the right-most edge of the Newton polygon of $g(x)$ with respect to p. For every m not a power of 2 and not equal to 24, this slope is < 1. Hence, Lemma 1 (with $k = 1$ and $\ell = 0$) implies that $G(x)$ cannot have a linear factor. Although it is not required for the proof of the lemma, we note that if m is a power of 2 (see the final section of [8]) or $m = 24$, there exist integers $a_0, a_1, \ldots, a_m$ with $|a_0| = |a_m| = 1$ such that $G(x)$ is reducible. In other words, this condition on m in the lemma cannot be omitted.

We now explain the computations done to verify the second sentence in Lemma 13. Our computations are mainly based on an application of Lemma 4. We begin however with an initial calculation that bounds k. Since $k \in [2, m/2]$ implies $m \geq 4$, we suppose this is the case. Let $p = 2m - \ell$ be the largest prime $< 2m$. Recall that

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

where $b_m = 1$ and

$$b_j = \binom{m}{j}(2m)(2m-1)(2m-2)\cdots(m+j+1) \quad \text{for } 0 \leq j \leq m-1.$$

By Bertrand's postulate, we have $p > m$. It follows that $p||b_0$. Also, $p|b_j$ for $0 \leq j \leq m-\ell-1$ and $p \nmid b_{m-\ell}$. We deduce that the right-most edge of the Newton polygon of $g(x)$ with respect to p has slope $1/(m-\ell)$. If $\ell < m/2$, then this slope is $< 2/m$. In this case, it follows from Lemma 1 that $G(x)$ cannot have a factor with degree in $[\ell+1, m/2]$. In the case that $\ell \geq m/2$, it is vacuously true that $G(x)$ cannot have a factor with degree in $[\ell+1, m/2]$. Thus, in either case, if $G(x)$ has a factor with degree in $[2, m/2]$, then the factor must have degree $\leq \ell$. Note that also the degree would necessarily be $\leq m/2$. Setting

$$B = \min\{2m - p, \lfloor m/2 \rfloor\} = \min\{\ell, \lfloor m/2 \rfloor\},$$

we see that B serves as a bound on the largest $k \in [2, m/2]$ for which $G(x)$ has a factor of degree k. For clarification on the size of B, we note that for $m \leq 10^6$, the largest value of B is 131 (obtained for $m = 678666$).

Next, for a given $m \leq 10^6$, we verified as follows that $G(x)$ cannot have a factor of degree $k \in [2, B]$ (where B is defined above). We initially set $k = B$. Given k, we searched for the smallest value of ℓ such that $m - \ell$ has a prime factor p satisfying

$$p > k + k\left\lfloor \frac{\log(2m)}{\log p} \right\rfloor. \tag{9}$$

If such an ℓ and p are found, then Lemma 4 implies that $G(x)$ cannot have a factor with degree in $[\ell+1, k]$. The value of k is then replaced by ℓ and the process is repeated. We repeated the process of eliminating intervals $[\ell+1, k]$ for the degree of a factor of $G(x)$ until either $G(x)$ was determined not to have a factor for every degree in the interval $[2, B]$ or no prime p as in (9) was found for some given m and k. The latter did not happen for each $m \leq 10^6$, implying the lemma. □

The next lemma is from [1].

Lemma 14. *If k, l, x_1, and x_2 are nonnegative integers for which*

$$|2^u x_1 - 3^v x_2| \leq 100,$$

then either $\min(2^u x_1, 3^v x_2) \leq 65536$, *or*

$$\max(x_1, x_2) > \min(2^u x_1, 3^v x_2)^{0.285}.$$

Furthermore, if $10^6 < 2^u x_1 < \exp(10^6)$, *then*

$$\max(x_1, x_2) > \min(2^u x_1, 3^v x_2)^{1/3}.$$

Our next result is based on ideas from [1] centered around computations done there to obtain the result above in the case of bounded values for $2^k x_1$. The approach in [1] requires some revision though to apply to our next result and we give the details.

Lemma 15. *Let m' and m'' be two integers for which*

$$0 < |m' - m''| \leq 50 \quad \textit{and} \quad 10^6 < \max\{m', m''\} \leq 10^{200}.$$

Suppose

$$m' = 3^v M_1, \quad m'' = 2^u M_2, \quad \textit{and} \quad M_1 M_2 \leq \min\{m', m''\}^{0.55}.$$

Then

$$(v, u, M_1, M_2) \in S = \{(12, 11, 2, 519), (11, 13, 8, 173), (13, 10, 1, 1557), (9, 19, 293, 11)\}.$$

Furthermore, in the case of each element of S, we have

$$|m' - m''| \geq 30 \quad \textit{and} \quad M_1 M_2 > \min\{m', m''\}^{0.5}.$$

Proof. We describe the algorithm we used to establish Lemma 15 but in more generality. Fix p, q, a, τ, M and z. Here, the numbers p, q, a, M and z are intended to be positive integers and $\tau \in (0,1)$. We envision the numbers p and q being primes, but our algorithm does not require them to be primes. We do, however, restrict to $\gcd(p,q) = 1$. The algorithm we describe finds the solutions in nonnegative integers k and ℓ and positive integers M_1 and M_2 to

$$p^k M_1 - q^\ell M_2 = a \tag{10}$$

with the constraints

$$M < p^k M_1 \le z \quad \text{and} \quad M_1 M_2 \le \left(q^\ell M_2\right)^\tau < \left(p^k M_1\right)^\tau. \tag{11}$$

No assumption is made here on the primes dividing M_1, M_2 and a. For example, they may all be divisible by p. For Lemma 15, we want

$$a \in \{1,2,\dots,50\}, \quad (p,q) \in \{(2,3),(3,2)\}, \quad M = 10^6, \quad z = 10^{200} \quad \text{and} \quad \tau = 0.55.$$

Next, we find bounds on k. From the second condition in (11), we have

$$M_1 \le \left(p^k M_1\right)^\tau \implies M_1 \le p^{\tau k/(1-\tau)}. \tag{12}$$

Hence, from the first condition in (11),

$$p^{k/(1-\tau)} = p^k p^{\tau k/(1-\tau)} \ge p^k M_1 > M.$$

It follows that $p^k > M^{1-\tau}$. Combining this with a simple implication of the first condition in (11) gives

$$\left\lfloor \frac{(1-\tau)\log M}{\log p} \right\rfloor < k \le \left\lfloor \frac{\log z}{\log p} \right\rfloor.$$

We consider an interval of values of k simultaneously. Specifically, we take $k \in (K, K+K']$ where

$$\left\lfloor \frac{(1-\tau)\log M}{\log p} \right\rfloor \le K < K + K' \le \left\lfloor \frac{\log z}{\log p} \right\rfloor.$$

For a given K between the upper and lower limits above, we define a positive integer K' in such a way that we dispose of the cases with $k \in (K, K+K']$ all at once. Our main interest in considering an interval of k is to speed up computations for large k. With this in mind, we take

$$K' = \begin{cases} 1 & \text{if } K \le 100 \\ \min\{K/5, \lfloor \log z/\log p \rfloor - K\} & \text{if } K > 100. \end{cases}$$

Some motivation for choosing K' is given in [1]; however, in our case here, where τ is somewhat larger, the motivation is slightly different. Indeed, here, we can take K' even larger, but this choice of K' will suffice for our purposes.

In what follows, we will want $p^k > a$. Observe that the lower bound for k above together with the values values of τ and M and the two choices of $p \in \{2,3\}$ needed for Lemma 15 imply $p^k \ge 243$. Since $a \le 50$, the condition $p^k > a$ is satisfied. In general, one can increase the value

of M so that the lower bound on k implies $p^k > a$, and then a direct computation can be done to obtain solutions to (10) for values of $p^k M_1$ smaller than this new value of M.

Next, we find a lower bound ℓ' on ℓ. Analogous to (12), we deduce that $M_2 \le q^{\tau\ell/(1-\tau)}$. Hence,

$$q^{\ell/(1-\tau)} = q^{\ell} q^{\tau\ell/(1-\tau)} \ge q^{\ell} M_2 = p^k M_1 - a \ge \max\{M + 1 - a, p^k - a\}.$$

For $k \in (K, K + K']$, we deduce

$$\ell \ge \ell' = \max\{\lceil (1-\tau)\log(p^{K+1} - a)/\log q\rceil, \lceil (1-\tau)\log(M + 1 - a)/\log q\rceil\}. \tag{13}$$

We write $k \in (K, K + K']$ in the form $k = K + t$ so that $1 \le t \le K'$. The inequality $\ell \ge \ell'$ and (10) imply

$$p^{t-1} M_1 \equiv a p^{-K-1} \pmod{q^{\ell'}}.$$

Let M' denote the smallest positive integer $\equiv a p^{-K-1} \pmod{q^{\ell'}}$. Thus, $p^{t-1} M_1 \ge M'$. Set

$$M_1^{(u)} = p^{\tau(K+K')/(1-\tau)} \quad \text{and} \quad M_1^{(l)} = M/p^{K+K'}.$$

Then (12) implies $M_1^{(u)}$ is an upper bound on M_1 and (11) implies $M_1^{(l)} < M_1$. As M' is also a lower bound for $p^{t-1} M_1 < p^{K'} M_1$, we see that we must have

$$\max\{M'/p^{K'}, M_1^{(l)}\} < M_1^{(u)}. \tag{14}$$

If this inequality does not hold, then there are no solutions to (10) and (11) for $k \in (K, K + K']$.

The algorithm continues next by modifying the above idea to redefine ℓ' and M' so that a simple check of the inequality (14) typically shows that there are no solutions to (10) and (11) for $k \in (K, K + K']$. The atypical situation, where we cannot deduce that there are no solutions, will coincide with the case where solutions actually exist. Note that $p^{K'-1} M_1 \ge p^{t-1} M_1 \ge M'$ and that $p^k M_1 = p^K p^t M_1 \ge p^K M'$. The condition $M_1 M_2 < \big(p^k M_1\big)^{\tau}$ implies

$$q^{\ell} \cdot \frac{\big(p^k M_1\big)^{\tau}}{M'} \ge q^{\ell} \cdot \frac{\big(p^k M_1\big)^{\tau}}{p^{K'-1} M_1} > \frac{q^{\ell} M_2}{p^{K'-1}} = \frac{p^k M_1 - a}{p^{K'-1}}$$

so that

$$\begin{aligned}
q^{\ell} &> M' p^{-K'+1} \big(p^k M_1 - a\big) \big(p^k M_1\big)^{-\tau} \\
&= M' p^{-K'+1} \big(p^k M_1 - a\big)^{1-\tau} \left(\frac{p^k M_1 - a}{p^k M_1}\right)^{\tau} \\
&= M' p^{-K'+1} \big(p^k M_1 - a\big)^{1-\tau} \left(1 - \frac{a}{p^k M_1}\right)^{\tau} \\
&\ge M' p^{-K'+1} \big(p^K M' - a\big)^{1-\tau} \left(1 - \frac{a}{p^K M'}\right)^{\tau} \\
&= M' p^{-K'+1} \big(p^K M' - a\big) \big(p^K M'\big)^{-\tau}.
\end{aligned}$$

Defining

$$\ell'' = \left\lceil \frac{\log\left(M'\right) - (K'-1)\log p + \log\left(p^K M' - a\right) - \tau \log\left(p^K M'\right)}{\log q} \right\rceil, \tag{15}$$

we deduce now that $\ell \geq \ell''$ so that

$$p^k M_1 \equiv a \pmod{q^{\ell''}} \quad \Longrightarrow \quad p^{t-1} M_1 \equiv a p^{-K-1} \pmod{q^{\ell''}}.$$

Letting M'' denote the least positive integer $\equiv ap^{-K-1} \pmod{q^{\ell''}}$, it follows that the roles of ℓ' and M' can be replaced by ℓ'' and M'' above. With some abuse of notation, we reset ℓ' and M' to be ℓ'' and M'' and repeat the above procedure as needed to further change the values of ℓ' and M'. The significant conditions that ℓ' and M' satisfy each time they are revised are

$$\ell \geq \ell', \quad M_1 \geq M'/p^{K'-1} \quad \text{and} \quad p^{t-1} M_1 \equiv M' \pmod{q^{\ell'}}.$$

Observe that if $\max\{M'/p^{K'}, M_1^{(l)}\} \geq M_1^{(u)}$, then there are no solutions to (10) and (11) for $k \in (K, K+K']$.

We began with $K = \lfloor (1-\tau)\log M/\log p \rfloor$ and repeatedly defined ℓ' and M' as above. Each time we redefined ℓ' and M', we checked whether $\max\{M'/p^{K'}, M_1^{(l)}\} \geq M_1^{(u)}$. If the inequality held, then we replaced K with $K+K'$ and repeated the procedure until all $k \leq \log z/\log p$ were considered. We stopped redefining ℓ' and M' and checking $\max\{M'/p^{K'}, M_1^{(l)}\} \geq M_1^{(u)}$ after 10 iterations of the above procedure, that is after the 11th values of ℓ' and M' were obtained. This number of iterations is not significant; it is simply a number that worked. For the purposes of Lemma 15, this was sufficient to show that there were no solutions to (10) and (11) for $k \in (K, K+K']$ except when $K \leq 100$ and there was a solution for some $k \in (K, K+K']$. Since $K' = 1$ when $K \leq 100$, we were able to obtain the solution by taking $k = K+1$ and $M_1 = M'$, and rewriting $p^k M_1 - a$ in the form $q^\ell M_2$. Note that since we do not require $\gcd(q, M_2) = 1$, there may be more than one possibility for ℓ and M_2 for which $p^k M_1 - a = q^\ell M_2$. For each such choice of ℓ and M_2, we checked (10) and (11) directly.

In the cases where a solution was found for a particular $k = K+1$ and M' as above, it is still necessary to check that the same choice of k does not produce other solutions to (10) and (11). We know in this situation that $M_1 \equiv M' \pmod{q^{\ell'}}$, and we are interested in the possibility that $M_1 \geq M' + q^{\ell'}$. In this case, we can redefine M' to be $M' + q^{\ell'}$ and then ℓ' to be the value of ℓ'' given by (15). Again, we then iterated the above procedure, redefining M' and ℓ' up to 10 times and checking whether $\max\{M', M_1^{(l)}\} \geq M_1^{(u)}$ as we proceeded. In each case, this led to establishing that no further solutions to (10) and (11) held. Lemma 15 was thus verified. □

Lemma 16. *Let M_1 and M_2 be positive integers and u and v be nonnegative integers for which*

$$\left|3^v M_1 - 2^u M_2\right| = 1 \quad \textit{and} \quad 10^6 < \max\left\{3^v M_1, 2^u M_2\right\} \leq 10^{1000}.$$

Then

$$M_1 M_2 > \min\left\{3^v M_1, 2^u M_2\right\}^{0.7}.$$

Proof. The algorithm used to verify this lemma was essentially the same as described in the proof of Lemma 15. Here, we want

$$z = 10^{1000} \quad \text{and} \quad \tau = 0.7.$$

The only other difference is that we took

$$K' = \min\{K/9, \lfloor \log z / \log p \rfloor - K\} \quad \text{for } K > 100.$$

The computations, with these changes, verified the lemma. □

We proceed now to the proof of Theorem 2 which will be a proof by contradiction. Assume $G(x)$ is reducible. Then $G(x)$ has a factor of degree $k \in [1, m/2]$. We fix such a k and consider various cases depending on the sizes of k and m. We show that we are led to a contradiction if $k \geq 2$ or if $k = 1$ and $4 \nmid m$.

Observe that by Lemma 13, we have a contradiction already if $k \geq 2$ and $m \leq 10^6$. Hence, for such k, we need only consider the case that $m > 10^6$. In particular, for all but the final case (the case that $k = 1$) in what follows, we will feel free to take advantage of this lower bound on m.

We also make use of the following notation:

- p denotes a prime number
- C, A, Q_z, d_p, e_p are as in Lemma 6
- $\Delta = \Delta(p) = \dfrac{6p^{r-1}}{3p^{r-1} - 1} = 2\left(1 - \dfrac{1}{3p^{r-1}}\right)^{-1}$
- $d(m, k) = \log(k \log(2m)) - \log\log(k \log(2m))$

4 Case 1: $m/50 \leq k \leq m/2$

Since $m > 10^6$, we have $2m/1.01 \geq 2479$. By Lemma 8, there exists a prime p in the interval $(2m/1.01, 2m]$. In particular, $m < p \leq 2m$. From (3), we see that $p || b_0$, $p | b_j$ for all $j \leq p - m - 1$, and $p \nmid b_j$ for any $j \geq p - m$. Hence, the endpoints of the right-most edge of the Newton polygon of $g(x)$ are $(2m - p, 0)$ and $(m, 1)$. Thus, the slope of this edge is $1/(p - m)$. Lemma 1 then implies that $G(x)$ cannot have a factor in $\mathbb{Z}[x]$ with degree in the open interval $(2m - p, p - m)$. Now,

$$2m - p < 2m - \frac{2m}{1.01} < 0.02m = \frac{m}{50}$$

and

$$p - m > \frac{2m}{1.01} - m > 0.98m > \frac{m}{2}.$$

Hence, $G(x)$ cannot have a factor of degree k, and we obtain a contradiction in this case.

5 Case 2: $\sqrt{m} < k < m/50$

Note that since $m > 50k$, we deduce from Lemma 12 by taking $n = m - k + 1$ that there exists a prime $p \geq 2k + 1$ such that $p|(m - \ell)$ for some $\ell \in [0, k)$. Observe that $p \geq 2k + 1$ implies that $p > \sqrt{2m}$ so that $\log(2m)/\log p < 2$. This is a contradiction to Lemma 4, completing the case at hand.

6 Case 3: $\sqrt[3]{2m}/3 \leq k \leq \sqrt{m}$

We will show that there exists a prime $p \geq 3k + 1$ such that $p|(m - \ell)$ for some ℓ in $[0, k)$. The lower bound on k in this case will then imply

$$\log p > \log(3k) \geq \frac{\log(2m)}{3}$$

so that

$$\left\lfloor \frac{\log(2m)}{\log p} \right\rfloor \leq 2.$$

Lemma 4 will then imply a contradiction, finishing this case.

As $m > 10^6$, we have $k \geq \sqrt[3]{2 \cdot 10^6}/3 > 41$. Using Lemma 6 with $z = 3k$, it is sufficient to prove that $Q_{3k} > 1$ or

$$(m - k)^{k - \pi(3k)} > (k - 1)!.$$

Taking the logarithm of both sides, we see that it is sufficient to show

$$(k - \pi(3k)) \log(m - k) > \log\big((k - 1)!\big). \tag{16}$$

Using $m \geq 10^6$ and Corollary 7, we see that (16) will hold provided

$$(k - \pi(3k)) \log\left(10^6 - k\right) > k \log k - k.$$

We checked this inequality directly for $41 < k \leq 377$. For $k \geq 378$, Corollary 3 implies that $k - \pi(3k) \geq k/2$. Observe that

$$\frac{k}{2} \log(k^2 - k) = \log\left(k^{k/2}(k - 1)^{k/2}\right) > \log\left(k(k - 1)^{k-1}\right) > \log(k!). \tag{17}$$

Given that, in the case under consideration, we have $m \geq k^2$, (16) follows, completing the argument for this case.

7 Case 4: $k \geq 31$, $P_2 \neq 1$.

The condition $P_2 \neq 1$ is a strong condition given Corollary 2. With this condition, we will be able to eliminate the possibility that $k \geq 31$ even without the results of the previous cases. We take $z = 3k$ in Lemma 6. Since $P_2 \neq 1$, we deduce from Corollary 2 that

$$m > \eta_k \quad \text{where } \eta_k = \frac{1}{2}(3k + 1)^{3k+1}. \tag{18}$$

so that $k < m^{1/3k}$. Thus, we are interested in obtaining a contradiction with k satisfying $31 \leq k < m^{1/3k}$. Observe that $Q_{3k} = P_1 P_2$. Our contradiction will be obtained by showing

$$\log Q_{3k} > \log P_1 + \log P_2. \tag{19}$$

From Lemma 6 and Corollary 7, we have

$$\log Q_{3k} > (k - \pi(3k)) \log(m - k + 1) - k \log k + k.$$

Next, we estimate $\log Q_{3k}/\log(2m)$. For $k \geq 31$, the arithmetic function $(k-1)/\eta_k$ is decreasing so that

$$\frac{k-1}{\eta_k} \leq \frac{30}{\eta_{31}}.$$

Using (18) and $k \geq 31$, we get

$$\begin{aligned}\frac{\log(m-k+1)}{\log(2m)} &= 1 + \frac{\log\left(1 - \dfrac{k-1}{m}\right) - \log 2}{\log(2m)} \\ &> 1 + \frac{\log\left(1 - \dfrac{30}{\eta_{31}}\right) - \log 2}{\log(2 \cdot \eta_{31})} > 0.998.\end{aligned}$$

Also, (18) implies that $k \log k < \frac{1}{3}\log(2m)$. Thus,

$$\frac{\log Q_{3k}}{\log(2m)} > 0.998(k - \pi(3k)) - \frac{1}{3}.$$

Next, we estimate $\log P_1/\log(2m)$. Using (18) we have $k \log(2m) > 13239$. Since the function $\log x - \log\log x$ is increasing for $x > e$ we get

$$\log(k \log(2m)) - \log\log(k \log(2m)) > 7.24.$$

Now, Corollary 4 implies $\log P_1 < 1.000081k + 0.139k \log(2m)$. Note that (18) implies

$$\frac{k}{\log(2m)} < \frac{k}{(3k+1)\log(3k+1)} < \frac{1}{3\log(3k+1)} \leq \frac{1}{3\log 94} < 0.0734.$$

Using (18) once again we get

$$\frac{\log P_1}{\log(2m)} < 0.074 + 0.139k.$$

Now, we estimate $\log P_2/\log(2m)$. Recalling the definition of y, we note that

$$\frac{\sqrt{y}}{\log(2m)} = \sqrt{\frac{3k+1}{\log(2m)\log(3k+1)}} < \frac{1}{\log(3k+1)},$$

where the inequality follows from (18). Using Corollary 5 we get

$$\frac{\log P_2}{\log(2m)} < 2.512\frac{\sqrt{y}}{\log(2m)} < \frac{2.512}{\log(3k+1)} < 0.553.$$

Combining the estimates for Q_{3k}, P_1 and P_2, we see that equation (19) holds provided

$$0.86k - \pi(3k) > 0.963. \tag{20}$$

From Corollary 3, we have $\pi(3k) \leq k/2$ for $k \geq 378$. So, (20) holds for $k \geq 378$. Direct computation shows that (20) holds for $31 \leq k \leq 377$ as well. So, (19) holds. We have our contradiction and this case is complete.

8 Case 5: $48 \leq k < \sqrt[3]{2m}/3$, $P_2 = 1$

In this case $Q_{3k} = P_1$. Also, from Lemma 6, we deduce that

$$Q_{3k} \geq \frac{(m-k+1)^{k-\pi(3k)}}{(k-1)!}.$$

Note that

$$\log P_1 \leq \begin{cases} \theta(p_{\text{max}}) - \theta(3k) & \text{if } p_{\text{max}} \geq 3k \\ 0 & \text{if } p_{\text{max}} < 3k. \end{cases}$$

Thus, we are interested in establishing

$$(k-\pi(3k))\log(m-k+1) > \max\left\{\theta(p_{\text{max}}) - \theta(3k), 0\right\} + \log\left((k-1)!\right). \tag{21}$$

From Corollary 7, the above inequality holds provided

$$(k-\pi(3k))\log(m-k+1) > \max\left\{\theta(p_{\text{max}}) - \theta(3k), 0\right\} + k\log k - k. \tag{22}$$

We consider two cases depending on whether $p_{\text{max}} \leq 4k$ or not.

First, suppose $p_{\text{max}} \leq 4k$. For $48 \leq k \leq 1000$, one checks computationally that

$$(k-\pi(3k))\log(10^6 - k) > \theta(4k) - \theta(3k) + k\log k - k.$$

In other words, since $m \geq 10^6$, (22) holds for $48 \leq k \leq 1000$. Therefore, we may suppose now that $k > 1000$. Using $k > 1000$ and Lemma 7, we deduce that

$$\theta(4k) - \theta(3k) \leq 1.000081 \cdot 4k - 3k + \frac{3k}{3.5\log(3k)} < 1.11\,k.$$

It is therefore sufficient to show that

$$(k-\pi(3k))\log(m-k) > 1.11\,k + k\log k - k. \tag{23}$$

Since $k < \sqrt[3]{2m}/3$, we obtain

$$m - k > \frac{27}{2}k^3 - k > k^3.$$

From Corollary 3, we have $\pi(3k) \le k/2$ for $k > 1000$. Thus, it is sufficient to show

$$1.5k \log k > 0.11k + k \log k.$$

This is easily seen to hold for $k \ge 2$. Thus, we obtain a contradiction if $p_{\max} \le 4k$.

We suppose now that $p_{\max} > 4k$. As $p_{\max} > 4k$, we deduce from Lemma 4 that

$$\log(2m)/\log p_{\max} \ge 4$$

which implies

$$m \ge \frac{1}{2}p_{\max}^4 \ge \frac{1}{2}(4k+1)^4 > 128k^4.$$

Since $128k^3 \ge 128 \cdot 48^3 > 10^7$, we deduce

$$m - k > m\left(1 - \frac{1}{128 \cdot k^3}\right) > 0.9999999\, m.$$

Observe further that Lemma 4 implies

$$p_{\max} \le k + k\frac{\log(2m)}{\log p_{\max}} \le k + k\frac{\log(2m)}{\log(4k)}.$$

Now, from Lemma 7, we have

$$\theta(p_{\max}) < 1.000081 \cdot p_{\max} \le 1.000081 \cdot \left(k + k\frac{\log(2m)}{\log(4k)}\right).$$

We see now that (22) holds if

$$\begin{aligned}(k - \pi(3k))\big(\log(0.9999999) + \log m\big) \\ > 1.000081 \cdot \left(k + k\frac{\log 2 + \log m}{\log(4k)}\right) - \theta(3k) + k\log k - k.\end{aligned}$$

We rewrite this in the form

$$A(k)\log m > B(k), \tag{24}$$

where

$$A(k) = k - \pi(3k) - \frac{1.000081k}{\log(4k)}$$

and

$$\begin{aligned}B(k) = 1.000081 \cdot \left(k + k\frac{\log 2}{\log(4k)}\right) - \theta(3k) \\ + k\log k - k - (k - \pi(3k))\log(0.9999999)\end{aligned}$$

$$< k\log k - 0.0000001\pi(3k) + 0.0000812k - \theta(3k) + \frac{0.69321k}{\log(4k)}.$$

Using that $m \geq 10^6$, one can check by a direct computation that (24) holds for $48 \leq k \leq 1000$. We therefore consider $k \geq 1001$.

From Lemma 7, we obtain for $k \geq 1001$ that

$$A(k) \geq k - \frac{3k}{\log 3003}\left(1 + \frac{3}{2\log 3003}\right) - \frac{k}{\log 4004} > 0.43\,k.$$

Recalling that $m > 128k^4$, we see that

$$A(k)\log m > 0.43k\big(4(\log k) + \log 128\big) > 1.7k\log k + 2k.$$

On the other hand, for $k \geq 1001$, we have

$$B(k) < k\log k + 0.0000812k + \frac{0.69321k}{\log 4004} < k\log k + 0.1\,k.$$

Combining the above, we deduce (24) holds. Thus, we obtain a contradiction for the case that $p_{\max} > 4k$.

9 Case 6: $3 \leq k \leq 47$, $m \geq e^{1000}/2$

For this case, we set $m_0 = e^{1000}$. We also write $P_0 = P_0' P_0'' P_0'''$ where the prime factors of P_0' are all at most $2k-2$, the prime factors of P_0'' are all at least $2k-1$ and exactly divide A, and the prime factors of P_0''' are all at least $2k-1$ with their squares each dividing A. We have $Q_{2k-2} = P_0'' P_0''' P_1 P_2$. We obtain a contradiction by showing $\log Q_{2k-2}/\log(2m) > \log\left(P_0'' P_0''' P_1 P_2\right)/\log(2m)$.

First, we estimate $\log Q_{2k-2}/\log(2m)$. We now apply Lemma 6 with $z = 2k-2$. We deduce that

$$(k-1)!\,Q_{2k-2} \geq (m-k+1)^{k-\pi(2k-2)}. \tag{25}$$

Observe that $m \geq e^{1000}/2$ and $3 \leq k \leq 47$ imply

$$\log\left(1 - \frac{k-1}{m}\right) \geq \log\left(1 - \frac{46}{e^{1000}/2}\right) > -10^{-10}$$

so that

$$\log(m-k+1) = \log\left(1 - \frac{k-1}{m}\right) + \log(2m) - \log 2 > \log(2m) - 0.7.$$

From (25) and $2m \geq m_0$, we deduce

$$\frac{\log Q_{2k-2}}{\log(2m)} \geq \left(1 - \frac{0.7}{\log(2m)}\right)(k - \pi(2k-2)) - \frac{\log(k-1)!}{\log(2m)} \geq a(k),$$

where

$$a(k) = 0.9993\,(k - \pi(2k-2)) - \frac{\log(k-1)!}{1000}.$$

Next, we estimate $\log(P_1 P_0'')/\log(2m)$. We have

$$P_0'' \le \prod_{2k-2<p\le 3k} p.$$

Thus,

$$\log P_0'' \le \theta(3k) - \theta(2k-2).$$

Moreover, since $\log(2m) \ge 1000$ and $\log t - \log\log t$ is increasing for $t > e$, Corollary 4 implies

$$\log P_1 \le 1.000081\left(k + \frac{k\log(2m)}{\log(1000k) - \log\log(1000k)}\right) - \theta(3k).$$

We get

$$\frac{\log(P_0'' P_1)}{\log(2m)} \le 1.000081\left(\frac{k}{1000} + \frac{k}{\log(1000k) - \log\log(1000k)}\right). \tag{26}$$

We make our first use of Lemma 2 in estimating $\log P_0'''/\log(2m)$. Observe that if p divides P_0''' and $p^r \| A$, then $r \ge 2$ and there is a nonnegative integer $\ell < k$ such that $p^r \| (m-\ell)$. By Lemma 2 (and our assumption that $G(x)$ has a factor of degree k), we have that each prime p dividing P_0''' satisfies

$$p^{r/2} < \frac{(p-1)k}{p-k-1}\frac{\log(2m)}{\log p}.$$

Thus, we have that

$$P_0''' \le \Pi_0^2 \cdot \big(\log(2m)\big)^{2(\pi(3k)-\pi(2k-2))},$$

where

$$\Pi_0 = \prod_{2k-2<p\le 3k} \frac{(p-1)k}{(p-k-1)\log p}.$$

We obtain

$$\frac{\log P_0'''}{\log(2m)} \le \frac{\log \Pi_0}{500} + \frac{2\big(\pi(3k) - \pi(2k-2)\big)\log\log(2m)}{\log(2m)}. \tag{27}$$

Finally, we estimate $\log P_2/\log(2m)$. If $P_2 > 1$, then Corollary 5 implies

$$\log P_2 \le 2.512\sqrt{y} - \pi(3k)\log y, \tag{28}$$

where $y = (3k+1)\,\log(2m)/\log(3k+1)$. Note that

$$y \ge 1000\,(3k+1)/\log(3k+1) > (3k)^2 \quad \text{for } 3 \le k \le 47.$$

By Lemma 7,

$$2.512\sqrt{y} > \pi(\sqrt{y})\log y > \pi(3k)\log y.$$

Thus, (28) holds when $P_2 = 1$ as well. Also, since $3k+1 > \log(3k+1)$, we have $y > \log(2m)$. We deduce that

$$\frac{\log P_2}{\log(2m)} < 2.512\sqrt{\frac{3k+1}{1000\log(3k+1)}} - \frac{\pi(3k)\log\log(2m)}{\log(2m)}. \tag{29}$$

Combining (26), (27), (29), and noting that $\pi(3k) \le 2\,\pi(2k-2)$ for $3 \le k \le 47$, we obtain

$$\frac{\log\left(P_0'' P_0''' P_1 P_2\right)}{\log(2m)} < b(k),$$

where

$$b(k) = 1.000081\left(\frac{k}{1000} + \frac{k}{\log(1000k) - \log\log(1000k)}\right) + \frac{\log\Pi_0}{500} + 0.08\sqrt{\frac{3k+1}{\log(3k+1)}}.$$

Direct calculation shows that $a(k) > b(k)$ for all $3 \le k \le 47$. Case 6 is complete.

10 Case 7: $3 \le k \le 47$, $m < e^{1000}/2$

For this case, we fix $k \in [3, 47]$ and let M denote a number for which a contradiction to $G(x)$ having a factor of degree k has been established for all $m > M$. Initially, based on Case 6, we take $M = \lfloor e^{1000}/2 \rfloor \le e^{1000}/2$. We consider $m \le M$. We explicitly find $\tilde{p} = \tilde{p}(k, M)$ defined as

$$\tilde{p} = \max\left\{p : p \text{ prime}, p \le k + k\left\lfloor \frac{\log(2M)}{\log p}\right\rfloor\right\}. \tag{30}$$

Note that the left-hand side of the inequality inside the display increases with p and the right-hand side decreases. Hence, if the inequality does not hold for a certain p, then it will not hold for any larger value of p. From a computational point of view, this means that the value of $\tilde{p}$ can be obtained quickly for each fixed k in this case simply by stepping through the primes until the inequality stops holding.

By Lemma 4 and the definition of $\tilde{p}$, we have $p_{\max} \le \tilde{p}$. Next, we use Lemma 2 and Lemma 3 to obtain an explicit upper bound $R(p) = R(p, k, M)$ on $r(p)$ for each p in the interval $[2k-1, \tilde{p}]$. Since by assumption $G(x)$ has a factor of degree k, we see that the inequality in Lemma 2 (iii) does not hold if $r \ge 2$. Thus, if $r \ge 2$, then also

$$r \le \left\lfloor 2\log\left(\frac{k(p-1)\log(2m)}{(p-k-1)\log p}\right)\Big/\log p\right\rfloor \le \left\lfloor 2\log\left(\frac{k(p-1)\log(2M)}{(p-k-1)\log p}\right)\Big/\log p\right\rfloor.$$

To use Lemma 3, we observe that

$$\frac{\Delta}{p^r} = \frac{1}{p^r}\cdot\frac{6p^{r-1}}{3p^{r-1}-1} = \frac{6}{3p^r - p}. \tag{31}$$

For $p \ge 3k$, the inequality in Lemma 3 (iii) does not hold, and we deduce

$$\frac{6k(p-1)\log(2m)}{(p-k-1)\log p} > 3p^r - p. \tag{32}$$

Thus, for $p \geq 3k$, we have

$$r \leq \left\lfloor \log\left(\frac{2k(p-1)\log(2m)}{(p-k-1)\log p} + \frac{p}{3}\right) \Big/ \log p \right\rfloor$$

In particular, we deduce that $r(p) \leq R(p)$, where

$$R(p) = \begin{cases} \max\left\{1, \left\lfloor 2\log\left(\frac{k(p-1)\log(2M)}{(p-k-1)\log p}\right) \Big/ \log p \right\rfloor\right\} & \text{if } 2k-1 \leq p \leq 3k-1 \\ \left\lfloor \log\left(\frac{2k(p-1)\log(2M)}{(p-k-1)\log p} + \frac{p}{3}\right) \Big/ \log p \right\rfloor & \text{if } 3k \leq p \leq \tilde{p}. \end{cases} \tag{33}$$

Observe in the case that $2k-1 \leq p \leq 3k-1$, we established a bound on the condition that $r(p) \geq 1$. It is for this reason that a maximum is taken above. However, it is not difficult, though not really helpful either, to show that the bound we obtained for $2k-1 \leq p \leq 3k-1$ when $r(p) \geq 2$ is at least 1. Hence, with a little more effort, the maximum can be dropped and the value of $R(p)$ in the case that $2k-1 \leq p \leq 3k-1$ replaced by simply the bound achieved under the condition $r(p) \geq 2$.

For the purposes of our next two cases, we note that the above holds for $k = 1$ and $k = 2$ with minor adjustments. The bound $\tilde{p}$ for $p_{\max}$ given by (30) is valid as is. For $k \in \{1, 2\}$, Lemma 2 (ii) requires that $p \geq k+2$ rather than $p \geq 2k-1$. So the upper bound $R(p)$ is valid but only with the lower bound $2k-1$ on p replaced by $k+2$. Note that for $k = 1$, we have $k+2 > 3k-1$ so that the value of $R(p)$ is valid only in the case $3k \leq p \leq \tilde{p}$. In other words, Lemma 2 does not help in obtaining the bound $R(p)$ in the case $k = 1$.

Returning to the present case and using the notation of Lemma 6, we have

$$Q_{2k-2} \leq \prod_{2k-1 \leq p \leq \tilde{p}} p^{R(p)}.$$

Observe that Lemma 6 implies

$$Q_{2k-2} \geq \frac{m(m-1)\cdots(m-k+1)}{(k-1)!\ \prod_{p \leq 2k-2} e_p},$$

where e_p is as defined there. Set

$$\varepsilon_0(m) = \varepsilon_0(k, m) = \begin{cases} 0.55 & \text{if } 10^6 < m \leq 10^{200} \text{ and } 3 \leq k \leq 29 \\ 0.285 & \text{otherwise.} \end{cases}$$

Then Lemma 14 and Lemma 15 imply

$$e_2 e_3 \leq \frac{d_2 d_3}{\min\{d_2, d_3\}^{\varepsilon_0(m)}}$$

if $d_2 \neq d_3$. In this case, we deduce that

$$\prod_{p \leq 2k-2} e_p \leq \frac{m(m-1)\cdots(m-\pi(2k-2)+1)}{\min\{d_2, d_3\}^{\varepsilon_0(m)}} \leq \frac{m(m-1)\cdots(m-\pi(2k-2)+1)}{(m-k+1)^{\varepsilon_0(m)}}.$$

In the case that $d_2 = d_3$, we even have the stronger inequality

$$\prod_{p \le 2k-2} e_p \le m(m-1)\cdots(m-\pi(2k-2)+2).$$

Note that $k > \pi(2k-2)$ for $3 \le k \le 47$. From our lower bound on Q_{2k-2} above, we obtain

$$Q_{2k-2} \ge \frac{(m-k+1)^{k+\varepsilon_0(M)-\pi(2k-2)}}{(k-1)!}.$$

Hence, if

$$m \ge \left\lfloor \left((k-1)! \prod_{2k-1 \le p \le \tilde{p}} p^{R(p)} \right)^{\frac{1}{k+\varepsilon_0(M)-\pi(2k-2)}} \right\rfloor + k, \tag{34}$$

then

$$m-k+1 > \left((k-1)! \prod_{2k-1 \le p \le \tilde{p}} p^{R(p)} \right)^{\frac{1}{k+\varepsilon_0(M)-\pi(2k-2)}}$$

and we obtain a contradiction.

More generally, suppose that we have proved that $G(x)$ has no irreducible factor of degree k for all $m > M_j$ (where k is a fixed integer in $[3, 47]$). Then, $G(x)$ has no irreducible factor of degree k for all $m > M_{j+1}$, where

$$M_{j+1} = M_{j+1}(k) = \left\lfloor \left((k-1)! \prod_{2k-1 \le p \le \tilde{p}(k, M_j)} p^{R(p,k,M_j)} \right)^{\frac{1}{k+\varepsilon_0(k,M_j)-\pi(2k-2)}} \right\rfloor + k.$$

To complete this case, we proceed as follows. Fix $k \in [3, 47]$. As indicated earlier, we begin with $M_1 = e^{1000}/2$, an upper bound on the size of m that we still need to consider. Next, we compute $M_2, M_3, \ldots, M_{12}$. For all $k \in [19, 47]$, we have $M_7 < 10^6$, so we are done when k is in that range. Similarly, $M_{12} < 10^6$ for all $k \in [12, 18]$. For the remaining cases $k \in \{3, 4, \ldots, 11\}$, Corollary 6 can be used to obtain a contradiction. We recall the table of values of $\alpha(k)$ after Corollary 6 and list the value of $\tilde{p}(k, M_{12})$ for each k in the table.

k	3	4	5	6	7	8	9	10	11
$\alpha(k)$	43	43	47	47	53	53	59	59	61
$\tilde{p}(k, M_{12})$	19	31	43	29	41	47	43	47	53

Since $m > 10^6$, Corollary 6 implies that $m(m-1)\cdots(m-k+1)$ must have a prime factor larger than $\alpha(k)$. On the other hand, the largest prime divisor of $m(m-1)\cdots(m-k+1)$ is bounded by $\tilde{p}(k, M_{12})$. Since $\alpha(k) > \tilde{p}(k, M_{12})$ for each $k \in \{3, 4, \ldots, 11\}$, we obtain a contradiction for these k, completing the case under consideration.

11 Case 8: $k = 2$

Here, $A = m(m-1)$. We write $A = 2^{r(2)} \cdot 3^{r(3)} \cdot 5^{r(5)} \cdot P_1 P_2$. By Lemma 14,

$$5^{r(5)} \cdot P_1 P_2 \geq (m-1)^{0.285}.$$

First, we suppose that $m \geq m_0 = e^{18000}/2$. We show the above inequality does not hold. In other words, we show

$$0.285 \log(m-1) > r(5) \log 5 + \log P_1 + \log P_2. \tag{35}$$

We have

$$\begin{aligned} 0.285 \log(m-1) &= 0.285\big(\log(2m) - \log 2 + \log(1-1/m)\big) \\ &\geq 0.285\big(\log(2m) - \log 2 + \log(1-1/m_0)\big) \\ &> 0.285 \log(2m) - 0.198. \end{aligned} \tag{36}$$

Lemma 2 implies

$$5^{r(5)} < \left(\frac{4 \log(2m)}{\log 5}\right)^2.$$

Thus,

$$r(5) \log 5 < 2 \log\log(2m) + 1.821. \tag{37}$$

Note that the above inequality is true even if $r(5) = 1$ and Lemma 2 does not apply.

Recall the definition of $d(m,k)$ given at the end of Section 3. Corollary 4 implies

$$\log P_1 \leq 1.000081(2 + 2\log(2m)/d(m,2)) - \theta(6),$$

where

$$d(m,2) \geq \log 36000 - \log\log 36000 > 8.14 \quad \text{and} \quad \theta(6) = \log 30.$$

We deduce that

$$\log P_1 < 0.246 \log(2m) - 1.401. \tag{38}$$

From Corollary 5, if $P_2 > 1$, then we have

$$\log P_2 \leq 2.512\sqrt{y} - 3\log y, \quad \text{where } y = 7\log(2m)/\log 7.$$

The function $2.512\sqrt{y} - 3\log y$ is increasing and positive for $y > 6$. Since

$$y \geq 7 \cdot 18000/\log 7 > 64000,$$

we obtain $2.512\sqrt{y} - 3\log y > 0$ and the above estimate for P_2 holds in the case $P_2 = 1$ too. Since $\sqrt{\log(2m)} \geq \sqrt{18000}$, we obtain

$$\log P_2 \leq 2.512 \frac{y}{\sqrt{y}} - 3\log y \tag{39}$$

$$\leq 2.512\sqrt{\frac{7}{\log 7}} \cdot \frac{\log(2m)}{\sqrt{\log(2m)}} - 3\log\left(\frac{7\log(2m)}{\log 7}\right)$$
$$\leq 2.512\sqrt{\frac{7}{\log 7}} \cdot \frac{\log(2m)}{\sqrt{18000}} - 3\log\log(2m) - 3\log\left(\frac{7}{\log 7}\right)$$
$$< 0.036\log(2m) - 3\log\log(2m) - 3.84.$$

Combining (37), (38), and (39) we have

$$r(5)\log 5 + \log P_1 + \log P_2 < 0.282\log(2m) - \log\log(2m) - 3.42.$$

This inequality together with (36) imply that (35) holds. Hence, we obtain a contradiction for $m \geq e^{18000}/2$.

We are left now with establishing a contradiction for $m < e^{18000}/2$. We view $M_1 = e^{18000}/2$ as a first lower bound on m for which the current case of $k = 2$ has been established, and we obtain new lower bounds M_j successively with $j \geq 2$ as follows. Suppose M_j is known. Recall the discussion after (33). We use (30) with $M = M_j$ to obtain an upper bound $\tilde{p} = \tilde{p}(2, M_j)$ on $p_{\max}$. Then we apply (33) with the lower bound $2k-1$ replaced by $k+2 = 4$ on p. This provides us with an upper bound on $r(p)$ for $5 \leq p \leq \tilde{p}$. Specifically, we have

$$R(p, M_j) = \begin{cases} \max\left\{1, \left\lfloor 2\log\left(\dfrac{2(p-1)\log(2M)}{(p-3)\log p}\right)\Big/\log p\right\rfloor\right\} & \text{if } p = 5 \\ \left\lfloor \log\left(\dfrac{4(p-1)\log(2M)}{(p-3)\log p} + \dfrac{p}{3}\right)\Big/\log p\right\rfloor & \text{if } 6 \leq p \leq \tilde{p}(2, M_j). \end{cases}$$

For this section, we set

$$\varepsilon_0(m) = \begin{cases} 0.7 & \text{if } 10^6 < m \leq 10^{1000} \\ 1/3 & \text{if } 10^{1000} < m < e^{18000}/2. \end{cases}$$

Lemma 6 with $k = 2$ and $z = 4$ implies

$$Q_4 \geq \frac{m(m-1)}{e_2 e_3}.$$

From Lemma 14 and Lemma 16, for $m < e^{18000}/2$, we have that

$$e_2 e_3 \leq \frac{m(m-1)}{(m-1)^{\varepsilon_0(m)}}.$$

Hence, $Q_4 \geq (m-1)^{\varepsilon_0(m)}$. By the definition of Q_4, we obtain a contradiction if

$$(m-1)^{\varepsilon_0(m)} > \prod_{5 \leq p \leq \tilde{p}(2, M_j)} p^{R(p, M_j)}.$$

We deduce that if $m > M_{j+1}$, where

$$M_{j+1} = \left\lfloor \left(\prod_{5 \le p \le \tilde{p}(2, M_j)} p^{R(p, M_j)} \right)^{1/\varepsilon_0(M_j)} \right\rfloor + 2,$$

then $G(x)$ cannot have a quadratic factor. Thus, this serves as our new lower bound on m.

Solving for M_j recursively, we find that $M_{25} < 1.3 \cdot 10^{18}$. One checks that $\tilde{p}\big(2, 1.3 \cdot 10^{18}\big) = 23$. Since this is an upper bound on the largest prime factor of $m(m-1)$, we deduce from Lemma 9 that $m \le 11859211$. Since $\tilde{p}\big(2, 11859211\big) = 13$, we get from another application of Lemma 9 that $m \le 123201 < 10^6$. Thus, we are done in this case.

12 Case 9: $k = 1$, $4 \nmid m$

We will handle this case in a manner that is similar to the previous one. One difference, however, from this case and all the previous ones is that we do not restrict ourselves to $m > 10^6$. On the other hand, given Lemma 13, we do consider only $m > 100$. Note that $A = m$ so that $m = 2^{r(2)} \cdot 3^{r(3)} \cdot P_1 P_2$. The conditions in this case imply $r(2) \le 1$, so $2m \le 4 \cdot 3^{r(3)} \cdot P_1 P_2$. First, we obtain a contradiction for $m \ge m_0 = e^{50}/2$ by showing

$$\log(2m) > \log 4 + r(3) \log 3 + \log P_1 + \log P_2. \tag{40}$$

To bound $r(3) \log 3$, we use Lemma 3 with $k = 1$ and $\ell = 0$. From (31), we obtain

$$3^{r(3)} < \frac{4 \log(2m)}{\log 3} + 1 < 3.661 \log(2m).$$

Thus,

$$r(3) \log 3 < 1.3 + \log \log(2m). \tag{41}$$

The function $d(m, 1) = \log \log m - \log \log \log m$ is increasing for $m \ge 16$. Hence, for $m \ge m_0$, we have $d(m, 1) \ge \log 50 - \log \log 50$. Corollary 4 implies

$$\log P_1 < 1.000081 + 0.393 \log(2m) - \log 6. \tag{42}$$

For $k = 1$, we have $y = 4 \log(2m)/\log 4$. Corollary 5 and $m \ge m_0$ imply

$$\begin{aligned} \log P_2 &\le 2.512 \frac{y}{\sqrt{y}} - 2 \log y \\ &\le 2.512 \sqrt{\frac{4}{\log 4}} \cdot \frac{\log(2m)}{\sqrt{\log(2m)}} - 2 \log \left(\frac{4 \log(2m)}{\log 4} \right) \\ &\le 2.512 \sqrt{\frac{4}{\log 4}} \cdot \frac{\log(2m)}{\sqrt{50}} - 2 \log \log(2m) - 2 \log \left(\frac{4}{\log 4} \right) \\ &< 0.604 \log(2m) - 2 \log \log(2m) - 2.119. \end{aligned} \tag{43}$$

Combining (41), (42), (43), and since $\log\log(2m) > 3.91$ for $m \geq m_0$, we obtain

$$\log 4 + r(3)\log 3 + \log P_1 + \log P_2 < 0.997\log(2m).$$

Thus, (40) holds and we get a contradiction for $m \geq e^{50}/2$.

For $m < e^{50}/2$, we recursively construct, analogous to the previous case, a sequence of lower bounds M_j on m for which the case $k = 1$ has been settled. We begin with $M_1 = e^{50}/2$. Suppose M_j is known with $j \geq 1$. Applying (30) with $M = M_j$, we obtain an upper bound $\tilde{p} = \tilde{p}(1, M_j)$ on $p_{\max}$. As noted in the discussion after (33), we have in this case that

$$R(p) = \left\lfloor \log\left(\frac{2(p-1)\log(2M)}{(p-2)\log p} + \frac{p}{3}\right) \Big/ \log p \right\rfloor$$

is an upper bound on $r(p)$ for $3 \leq p \leq \tilde{p}$. By the definition of $r(p)$, we deduce that $G(x)$ cannot have a linear factor if $m > M_{j+1}$, where

$$M_{j+1} = 2\prod_{3 \leq p \leq \tilde{p}} p^{R(p)}.$$

Recursively constructing M_j as above leads to $M_5 = 18$. As we are considering $m > 100$, we derive at a contradiction.

References

[1] M. Bennett, M. Filaseta, and O. Trifonov, *On the factorization of consecutive integers*, preprint.

[2] G. Dumas, *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, J. Math. Pures Appl. 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. (Series A) 26 (1978), 257–269.

[4] P. Erdős, *On consecutive integers*, Nieuw Archief voor Wiskunde III 3 (1955), 124–128.

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

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

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

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

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

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

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

[12] F. Hajir, *On the Galois group of generalized Laguerre polynomials*, J. Théor. Nombres Bordeaux 17 (2005), 517–525.

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

[14] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. reine angew. Math. **110** (1892), 104–129.

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

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

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

[18] H. Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly 62 (1955), 26-29.

[19] J. B. Rosser and L. Schoenfeld *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–89.

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

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

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

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

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