IRREDUCIBILITY OF GENERALIZED HERMITE-LAGUERRE POLYNOMIALS

SHANTA LAISHRAM AND T. N. SHOREY

1. Introduction

Let \( n \) and \( 1 \leq \alpha < d \) be positive integers with \( \gcd(\alpha, d) = 1 \). Any positive rational \( q \) is of the form \( q = u + \frac{\alpha}{d} \) where \( u \) is a non-negative integer. For integers \( a_0, a_1, \ldots, a_n, \)

\[ G(x) := G_q(x) = a_n x^n + a_{n-1} (\alpha + (n-1+u)d)x^{n-1} + \cdots + \]

\[ a_1 \left( \prod_{i=1}^{n-1} (\alpha + (i+u)d) \right) x + a_0 \left( \prod_{i=0}^{n-1} (\alpha + (i+u)d) \right) .\]

This is an extension of Hermite polynomials and generalized Laguerre polynomials. Therefore we call \( G(x) \) the generalized Hermite-Laguerre polynomial. For an integer \( \nu > 1 \), we denote by \( P(\nu) \) the the greatest prime factor of \( \nu \) and we put \( P(1) = 1 \).

We prove

**Theorem 1.** Let \( P(a_0a_n) \leq 3 \) and suppose \( 2 \nmid a_0a_n \) if degree of \( G_{\frac{3}{2}}(x) \) is 43. Then \( G_{\frac{3}{2}} \) and \( G_{\frac{3}{3}} \) are irreducible except possibly when \( 1 + 3(n-1) \) and \( 2 + 3(n-1) \) is a power of 2, respectively where it can be a product of a linear factor times a polynomial of degree \( n-1 \).

**Theorem 2.** Let \( 1 \leq k < n, \ 0 \leq u \leq k \) and \( a_0a_n \in \{ \pm 2^t : t \geq 0, t \in \mathbb{Z} \} \). Then \( G_{u+\frac{1}{2}} \) does not have a factor of degree \( k \) except possibly when \( k \in \{1, n-1\}, u \geq 1 \).

Schur [Sch29] proved that \( G_{\frac{3}{2}}(x^2) \) with \( a_n = \pm 1 \) and \( a_0 = \pm 1 \) are irreducible and this implies the irreducibility of \( H_{2n} \) where \( H_m \) is the \( m \)-th Hermite polynomial. Schur [Sch73] also established that Hermite polynomials \( H_{2n+1} \) are \( x \) times an irreducible polynomial by showing that \( G_{\frac{3}{2}}(x^2) \) with \( a_n = \pm 1 \) and \( a_0 = \pm 1 \) is irreducible expect for some explicitly given finitely many values of \( n \) where it can have a quadratic factor. Further Allen and Filaseta [AlFi04] showed that \( G_{\frac{3}{2}}(x^2) \) with \( a_1 = \pm 1 \) and \( 0 < |a_n| < 2n-1 \) is irreducible. Finch and Saradha [FiSa10] showed that \( G_{u+\frac{1}{2}} \) with \( 0 \leq u \leq 13 \) have no factor of degree \( k \in [2, n-2] \) except for an explicitly given finite set of values of \( u \) where it may have a factor of degree 2.

From now onwards, we always assume \( d \in \{2, 3\} \). A new ingredient in the proofs of Theorems 1 and 2 is the following result which we shall prove in Section 3.
Theorem 3. Let $k \geq 2$ and $d = 2, 3$. Let $m$ be a positive integer such that $d \nmid m$ and $m > dk$. Then

\[
P(m(m + d) \cdots (m + d(k - 1))) > \begin{cases} 
3.5k & \text{if } d = 2 \text{ and } m \leq 2.5k \\
4k & \text{if } d = 2 \text{ and } m > 2.5k \\
3k & \text{if } d = 3
\end{cases}
\]

unless $(m, k) \in \{(5, 2), (7, 2), (25, 2), (243, 2), (9, 4), (13, 5), (17, 6), (15, 7), (21, 8), (19, 9)\}$ when $d = 2$ and $(m, k) = (125, 2)$ when $d = 3$.

If $d = 2, 3$ and $m > dk$, this is an improvement of [LaSh06a].

In Section 4, we shall combine Theorem 3 with the irreducibility criterion from [ShTi10] (see Lemma 4.1) to derive Theorems 1 and 2. This criterion come from Newton polygons. 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 $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$ and let $p$ be a prime. Let $S$ be the following set of points in the extended plane:

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

Consider the lower edges along the convex hull of these points. The left-most endpoint is $(0, \nu(a_n))$ and the right-most endpoint is $(n, \nu(a_0))$. The endpoints of each edge belong to $S$ and the slopes of the edges increase from left to right. When referring to the edges of a Newton polygon, we shall not allow two different edges to have the same slope. The polygonal path formed by these edges is called the Newton polygon of $f(x)$ with respect to the prime $p$. For the proof of Theorems 1 and 2, we use [ShTi10, Lemma 10.1] whose proof depends on Newton polygons.

A part of this work was done when the authors were visiting Max-Planck Institute for Mathematics in Bonn during August-October, 2008 and February-April, 2009, respectively. We would like to thank the MPIM for the invitation and the hospitality. We also thank Pieter Moree for his comments on a draft of this paper. The authors are indebted to the referee for his suggestions and remarks which improved the exposition of the paper.

2. Preliminaries for Theorem 3

Let $m$ and $k$ be positive integers with $m > kd$ and $\gcd(m, d) = 1$. We write

\[\Delta(m, d, k) = m(m + d) \cdots (m + (k - 1)d)\]

For positive integers $\nu, \mu$ and $1 \leq l < \mu$ with $\gcd(l, \mu) = 1$, we write

\[\pi(\nu, \mu, l) = \sum_{p \leq \nu} 1, \quad \pi(\nu) = \pi(\nu, 1, 1)\]

\[\theta(\nu, \mu, l) = \sum_{p \leq \nu, p \equiv l (\text{mod } \mu)} \log p.\]
Let \( p_{i,\mu,l} \) denote the \( i \)th prime congruent to \( l \) modulo \( \mu \). Let \( \delta_{\mu}(i, l) = p_{i+1, \mu,l} - p_{i,\mu,l} \) and \( W_{\mu}(i, l) = (p_{i,\mu,l}, p_{i+1, \mu,l}) \). Let \( M_0 = 1.92367 \times 10^{10} \).

We recall some well-known estimates on prime number theory.

**Lemma 2.1.** We have

\[
\begin{align*}
(i) & \quad \pi(\nu) \leq \frac{\nu}{\log \nu} \left( 1 + \frac{1.2762}{\log \nu} \right) \text{ for } \nu > 1 \\
(ii) & \quad \nu(1 - \frac{3.965}{\log^2 \nu}) \leq \theta(\nu) < 1.00008\nu \text{ for } \nu > 1 \\
(iii) & \quad \sqrt{2\pi k} e^{-k} k^k e^{\frac{1}{12k+1}} < k! < \sqrt{2\pi k} e^{-k} k^k e^{\frac{1}{12}} \text{ for } k > 1 \\
(iv) & \quad \text{ord}_p(k!) \geq \frac{k-p}{\log\left(\frac{k-1}{\log p}\right)} \text{ for } k > 1 \text{ and } p < k.
\end{align*}
\]

The estimates (i), (ii) are due to Dusart [Dus98, p.14], [Dus99]. The estimate (iii) is [Rob55, Theorem 6]. For a proof of (iv), see [LaSh04b, Lemma 2(i)].

The following lemma is due to Ramaré and Rumely [RaRu96, Theorems 1, 2].

**Lemma 2.2.** Let \( l \in \{1, 2\} \). For \( \nu_0 \leq 10^{10} \), we have

\[
\theta(\nu, 3, l) \geq \left\{ \begin{array}{ll}
\frac{\nu}{2} (1 - 0.002238) & \text{for } \nu \geq 10^{10} \\
\frac{\nu}{2} (1 - \frac{2 \times 1.798158}{\sqrt{36}}) & \text{for } 10^{10} > \nu \geq \nu_0
\end{array} \right.
\]

and

\[
\theta(\nu, 3, l) \leq \left\{ \begin{array}{ll}
\frac{\nu}{2} (1 + 0.002238) & \text{for } \nu \geq 10^{10} \\
\frac{\nu}{2} (1 + \frac{2 \times 1.798158}{\sqrt{36}}) & \text{for } 10^{10} > \nu \geq \nu_0
\end{array} \right.
\]

We derive from Lemmas 2.1 and 2.2 the following result.

**Corollary 2.3.** Let \( M_0 < m \leq 131 \times 2k \) if \( d = 2 \) and \( 6450 \leq m \leq 10.6 \times 3k \) if \( d = 3 \). Then \( \rho(\Delta(m, d, k)) \geq m \).

**Proof.** Let \( M_0 < m \leq 131 \times 2k \) if \( d = 2 \) and \( 6450 \leq m \leq 10.6 \times 3k \) if \( d = 3 \). Then \( k \geq k_1 \) where \( k_1 = 7.34 \times 10^7, 203 \) when \( d = 2, 3 \), respectively. Let \( 1 \leq l < d \) and assume \( m \equiv l \pmod{d} \). We observe that \( \rho(\Delta(m, d, k)) \geq m \) holds if

\[
\theta(m + d(k-1), d, l) - \theta(m - 1, d, l) = \sum_{m \leq p \leq m+(k-1)d \atop p \equiv l(d)} \log p > 0.
\]

Now from Lemmas 2.1 and 2.2, we have

\[
\frac{\theta(m-1, d, l)}{\phi(d)} < \theta_1 := \left\{ \begin{array}{ll}
1.00008 & \text{if } d = 2 \\
1 + \frac{2 \times 1.798158}{\sqrt{6450}} & \text{if } d = 3
\end{array} \right.
\]

and

\[
\frac{\theta(m + (k-1)d, d, l)}{\phi(d)} > \theta_2 := \left\{ \begin{array}{ll}
1 - \frac{3.965}{\log^2(10^{10})} & \text{if } d = 2 \\
1 - \frac{2 \times 1.798158}{\sqrt{6450}} & \text{if } d = 3
\end{array} \right.
\]
Thus \( P(\Delta(m, d, k) \geq m) \) holds if

\[
\theta_2(m + d(k - 1)) > \theta_1 m
\]

i.e., if

\[
\frac{d(k - 1)}{m} > \frac{\theta_1}{\theta_2} - 1.
\]

This is true since for \( k \geq k_1 \), we have

\[
\frac{dk(1 - \frac{1}{k})}{\theta_1}\frac{\theta_2 - 1}{\theta_1} \geq \frac{dk(1 - \frac{1}{k_1})}{\theta_1}\frac{\theta_2 - 1}{\theta_1} > (dk) \begin{cases} 
131.3 & \text{if } d = 2 \\
10.6 & \text{if } d = 3
\end{cases}
\]

and \( m \) is less than the last expression. Hence the assertion. \( \square \)

Now we give some results for \( d = 2 \). The next result follows from Lemma 2.1 (ii).

**Corollary 2.4.** Let \( d = 2, k > 1 \) and \( 2k < m < 4k \). Then

\[
P(\Delta(m, d, k)) > \begin{cases} 
3.5k & \text{if } m \leq 2.5k \\
4k & \text{if } m > 2.5k
\end{cases}
\]

unless \((m, k) \in \{(5, 2), (7, 2), (9, 4), (13, 5), (17, 6), (15, 7), (21, 8), (19, 9)\} \}

**Proof.** We observe that the set \( \{m, m+2, \ldots, m+2(k-1)\} \) contains all primes between \( 3.5k \) and \( 4k \) if \( m \leq 2.5k \) and all primes between \( 4k \) and \( 4.5k \) if \( 2.5k < m < 4k \).

Therefore (4) holds if

\[
\theta(4k) > \theta(3.5k) \quad \text{and} \quad \theta(4.5k) > \theta(4k).
\]

Let \((r, s) = (3.5, 4) \) or \((4, 4.5)\). Then from Lemma 2.1, we see that \( \theta(sk) > \theta(rk) \) if

\[
sk(1 - \frac{3.965}{\log^2(sk)}) > 1.00008 \times rk
\]

or

\[
s - 1.00008r > \frac{s}{1.00008r} \frac{3.965}{\log^2(sk)}
\]

or

\[
k > \frac{1}{s} \exp \left( \frac{3.965s}{s - 1.00008r} \right).
\]

This is true for \( k \geq 88 \). Thus \( k \leq 87 \). For \( 10 \leq k \leq 87 \), we check that there is always a prime in the intervals \((3.5k, 4k)\) and \((4k, 4.5k)\) and hence (4) follows in this case. For \( 2 \leq k \leq 9 \), the assertion follows by computing \( P(\Delta(m, 2, k)) \) for each \( 2k < m < 4k \). \( \square \)

The following result concerns Grimm’s Conjecture, [LaSh06b, Theorem 1].

**Lemma 2.5.** Let \( m \leq M_0 \) and \( l \) be such that \( m+1, m+2, \ldots, m+l \) are all composite numbers. Then there are distinct primes \( P_i \) such that \( P_i | (m+i) \) for each \( 1 \leq i \leq l \).

As a consequence, we have
Corollary 2.6. Let $4k < m \leq M_0$. Then either $P(\Delta(m, 2, k)) > 4k$ or $P(\Delta(m, 2, k)) \geq p_{k+1}$.

Proof. If $m + 2i$ is prime for some $i$ with $0 \leq i < k$, then the assertion holds clearly since $P(\Delta(m, 2, k)) \geq m + 2i > 4k$. Thus we suppose that $m + 2i$ is composite for all $0 \leq i < k$. Since $m$ is odd, we obtain that $m + 2i + 1$ with $0 \leq i < k$ are all even and hence composite. Therefore $m, m + 1, m + 2, \ldots, m + 2k - 1$ are all composite and hence, by Lemma 2.5, there are distinct primes $P_j$ with $P_j|(m - 1 + j)$ for each $1 \leq j \leq 2k$. Therefore $\omega(\Delta(m, 2, k)) \geq k$ implying $P(\Delta(m, 2, k)) \geq p_{k+1}$. \hfill \Box

Corollary 2.7. Let $d = 2$ and $4k < m \leq M_0$. Then $P(\Delta(m, 2, k)) > 4k$ for $k \geq 30$.

Proof. By Corollary 2.6, we may assume that $P(\Delta(m, 2, k)) \geq p_{k+1}$. By Lemma 2.1, we get $p_{k+1} \geq k \log k$ which is $> 4k$ for $k \geq 60$. For $30 \leq k < 60$, we check that $p_{k+1} > 4k$. Hence the assertion follows. \hfill \Box

The following result follows from [Leh64, Tables IIA, IIIA].

Lemma 2.8. Let $d = 2$, $m > 4k$ and $2 \leq k \leq 37, k \neq 35$. Then $P(\Delta(m, 2, k)) > 4k$.

Proof. The case $k = 2$ is immediate from [Leh64, Table IIA]. Let $k \geq 3$ and $m \geq 4k$. For $m$ and $1 \leq i < k$ such that $m + 2i = N$ with $N$ given in [Leh64, Tables IIA, IIIA], we check that $P(\Delta(m, 2, k)) > 4k$. Hence assume that $m + 2i$ with $1 \leq i < k$ is different from those $N$ given in [Leh64, Tables IIA, IIIA].

For every prime $31 < p \leq 4k$, we delete a term in \{m, m + 2, \ldots, m + 2(k - 1)\} divisible by $p$. Let $i_1 < i_2 < \ldots < i_l$ be such that $m + 2i_j$ is in the remaining set where $l \geq k - (\pi(4k) - \pi(31))$. From [Leh64, Tables IIA, IIIA], we observe that $i_{j+1} - i_j \geq 3$ implying $k - 1 \geq i_l - i_1 \geq 3(l - 1) \geq 3(k - \pi(4k) + 10)$. However we find that the inequality $k - 1 \geq 3(k - \pi(4k) + 10)$ is not valid except when $k = 28, 29$. Hence the assertion of the Lemma is valid except possibly for $k = 28, 29$.

Therefore we may assume that $k = 28, 29$. Further we suppose that $l = k - (\pi(4k) - \pi(31)) = 10$ otherwise $3(l - 1) \geq 30 > k - 1$, a contradiction. Thus we have either $i_{t+1} - i_t = 27$ implying $i_1 = 0, i_{j+1} = i_j + 3 = 3j$ for $1 \leq j \leq 9$ or $i_1 = 1, i_{j+1} = i_j + 3 = 3j + 1$ for $1 \leq j \leq 9$ or $i_{t+1} - i_t = 28$ implying $i_1 = 0, i_{j+1} = 3j + 1$ if $1 \leq j \leq r$ and $i_{j+1} = 3j + 1$ if $r < j \leq 9$ for some $r \geq 1$. Let $X = m + 2i_1 - 6$. Note that $X$ is odd since $m$ is odd. Also $X \geq 4k + 1 - 6 \geq 107$. We have either

$$P((X + 6) \cdots (X + 54)(X + 60)) \leq 31$$

or there is some $r \geq 1$ for which

$$P((X + 6) \cdots (X + 6r)(X + 6(r + 1) + 2) \cdots (X + 60 + 2)) \leq 31.$$ 

Note that (5) is the only possibility when $k = 28$. Now we consider (5). Suppose $3|X$. Then putting $Y = \frac{X}{3}$, we get $P((Y + 2) \cdots (Y + 18)(Y + 20)) \leq 31$ which implies $Y + 2 < 20$ by Corollary 2.4 and Lemma 2.8 with $k = 10$. Since $X + 6 \geq m \geq 113$, we get a
contradiction. Hence we may assume that \(3 \nmid X\). Then \(3 \nmid (X+6) \cdots (X+54)(X+60)\).
After deleting terms \(X+6i\) divisible by primes \(11 \leq p \leq 31\), we are left with three terms divisible by primes 5 and 7 and hence \(m \leq X + 6 \leq 35\) which is again a contradiction. Therefore (5) is not possible.

Now we consider (6) which is possible only when \(k = 29\). Since \(X + 6 = m > 4k = 116\), we have \(X > 110\). Suppose \(r = 1, 9\). Then we have \(P((X + 12) \cdots (X + 54) + 2)(X + 60 + 2)) \leq 31\) if \(r = 1\) and \(P((X + 6) \cdots (X + 54)) \leq 31\) if \(r = 9\). Putting \(Y = X+8\) in the first case and \(Y = X\) in the latter, we get \(P((Y+6) \cdots (Y+54)) \leq 31\) if \(r = 3\) or \(X \equiv Y \mod 3\). Hence we may assume that \(3 \nmid Y\). Then \(3 \nmid (Y + 6) \cdots (Y + 54)\). After deleting terms \(Y + 6i\) divisible by primes \(11 \leq p \leq 31\), we are left with two terms divisible by primes 5 and 7 only. Let \(Y + 6i = 5^{a_1}7^{b_1}\) and \(Y + 6j = 5^{a_2}7^{b_2}\) where \(b_1 \leq 1 < b_2\) and \(a_2 \leq 1 < a_1\). Since \(|i - j| \leq 8\), the equality \(6(i - j) = 5^{a_1}7^{b_1} - 5^{a_2}7^{b_2}\) implies \(5^a - 7^b = \pm 6, \pm 12, \pm 18, \pm 24, \pm 36, \pm 48\). By taking modulo 6, we get \((-1)^a \equiv 1\) modulo 6 implying \(a\) is even. Taking modulo 8 again, we get either

\[b\text{ is even, } 5^a - 7^b = (5^{\frac{a}{2}} - 7^{\frac{b}{2}})(5^{\frac{a}{2}} + 7^{\frac{b}{2}}) = \pm 24, \pm 48\]
giving

\[(7) \quad 5^a = 25, 7^b = 49\]
or

\[b\text{ is odd, } 5^a - 7^b = -6, 18.\]

Let \(5^a - 7^b = -6\). Considering modulo 5, we get \(2^b \equiv 1\) implying \(4|b\), a contradiction. Let \(5^a - 7^b = 18\). By considering modulo 7 and modulo 9 and since \(a\) is even, we get \(3|(a - 2)\) and \(3|(b - 1)\) implying \((5^{\frac{a+2}{3}} + 35(-7^{\frac{b+1}{3}}))^3 = 90\). Solving the Thue equation \(x^3 + 35y^3 = 90\) gives \(x = 5, y = -1\) or \(25 - 7 = 18\) is the only solution. Hence \(6 \cdot 3 = 25 - 7 = X + 6i - (X + 6j)\). Also the solution (7) implies \(-6 \cdot 4 = 25 - 49 = X + 6i - (X + 6j)\). Thus \(X \leq 25\) which is not possible.

Assume now that \(2 \leq r \leq 8\). Then \(P((X + 6)(X + 12)(X + 56)(X + 62)) \leq 31\). Suppose \(3 \nmid X(X + 2)\). Putting \(Y = \frac{x+6}{3}\) if \(3\nmid X\) and \(Y = \frac{x+56}{3}\) if \(3\nmid (X + 2)\), we get either \(P(Y(Y + 2)(3Y + 50)(6Y + 56)) \leq 31\) or \(P(Y(Y + 2)(3Y + 50)(3Y - 44)) \leq 31\). In particular \(P(Y(Y + 2)) \leq 31\). For \(Y = N - 2\) given by [Leh64, Table IIA] such that \(P(Y(Y + 2)) \leq 31\), we check that \(P((3Y + 50)(3Y + 56)) \geq 31\) and \(P((3Y + 50)(3Y - 44)) \geq 31\) except when \(Y \in \{55, 145, 297, 1573\}\). This gives \(m = X + 6 = 3Y - 50\) and then we further check that \(P(\Delta(m, 2, k)) > 116\). Hence we suppose \(3 \nmid X(X + 2)\). Then \(3 \nmid (X + 6) \cdots (X + 6r)\) for \(r = 1, 2, \cdots, 5\). If a prime power \(p^a\) divides two terms of the product, then \(p^a|(X + 6j), p^a|(X + 6i)\) or \(p^a|(X + 6j + 2), p^a|(X + 6i + 2)\) or \(p^a|(X + 6j), p^a|(X + 6i + 2)\) for some \(i, j\). Hence \(p^a|6(i - j)\) or \(p^a|6(i - j) + 2\). Since \(1 \leq j < i \leq 10\), we get \(p^a \in \{5, 7, 11, 13, 19, 25\}\). After deleting terms divisible by primes \(5 \leq p \leq 31\) to their highest powers, we are left with two terms such that their product divides \(25 \cdot 7 \cdot 11 \cdot 13 \cdot 19\) and hence \(X + 6 \leq \sqrt{25 \cdot 7 \cdot 11 \cdot 13 \cdot 19} = 869\). We check that \(P((X + 6)(X + 12)(X + 56)(X + 62)) > 31\) for \(110 \leq X \leq 683\) except
when $X \in \{113, 379\}$. Further we check that $P(\Delta(m, 2, k)) > 116$ for $m = X + 6$. Hence the result.

The remaining results in this section deal with the case $d = 3$. The first one is a computational result.

**Lemma 2.9.** Let $l \in \{1, 2\}$. If $p_{1,3,l} \leq 6450$, then $\delta_3(i, l) \leq 60$.

As a consequence, we obtain

**Corollary 2.10.** Let $d = 3$ and $3k < m \leq 6450$ with $\gcd(m, 3) = 1$. Then (1) holds unless $(m,k) = (125, 2)$.

**Proof.** For $k \leq 20$, it follows by direct computation. For $k > 20$, (1) follows as $3(k - 1) \geq 60$ and, by Lemma 2.9, the set $\{m + 3i : 0 \leq i < k\}$ contains a prime. □

We shall also need the following result of Nagell [Nag58] (see [Cao99]) on diophantine equations.

**Lemma 2.11.** Let $a, b, c \in \{2, 3, 5\}$ and $a < b$. Then the solutions of

$$a^x + b^y = c^z$$

in integers $x > 0, y > 0, z > 0$ are given by

$$(a^x, b^y, c^z) \in \{(2, 3, 5), (2^4, 3^2, 5^2), (2, 5^2, 3^3), (2^2, 5, 3^2), (3, 5, 2^3), (3^3, 5, 2^5), (3, 5^3, 2^7)\}.$$

As a corollary, we have

**Corollary 2.12.** Let $X > 80, 3 \nmid X$ and $1 \leq i \leq 7$. Then the solutions of

$$P(X(X + 3i)) = 5 \quad \text{and} \quad 2|X(X + 3i)$$

are given by

$$(i, X) \in \{(1, 125), (2, 250), (4, 500), (5, 625)\}.$$

**Proof.** Let $1 \leq i \leq 7$. We observe that $2|X, 2|(X + 3i)$ only if $X$ and $i$ are both even and $5|X, 5|(X + 3i)$ only if $i = 5$. Let the positive integers $r, s$ and $\delta = \ord_2(i) \in \{0, 1, 2\}$ be given by

$$(8) \quad X = 2^{r+\delta}, \ X + 3i = 2^{\delta}5^s \quad \text{or} \quad X = 2^\delta 5^s, \ X + 3i = 2^{r+\delta} \quad \text{if} \ i \neq 5$$

and

$$(9) \quad X = 5^{s+1}, \ X + 3i = 5 \times 2^r \quad \text{or} \quad X = 5 \times 2^r, \ X + 3i = 5^{s+1} \quad \text{if} \ i = 5,$$

where $r + 2 \geq r + \delta \geq 7$ and $s \geq 2$ since $X > 80$. Hence we have

$$(10) \quad 2^r - 5^s = \pm \left(\frac{X + 3i}{2^{\ord_2(i)} \cdot 5^{\ord_5(i)}} - \frac{X}{2^{\ord_2(i)} \cdot 5^{\ord_5(i)}}\right) = \pm 3 \times \left(\frac{i}{2^{\ord_2(i)} \cdot 5^{\ord_5(i)}}\right).$$
Let $i \in \{1, 2, 4, 5\}$. Then $2^r - 5^s = \pm 3$. By Lemma 2.11, we have $2^r = 2^7, 5^s = 5^3$ and $2^7 - 5^3 = 3$ implying $X = 2^{\text{ord}_2(i)} \cdot 5^{3 + \text{ord}_5(i)}$ and $X + 3i = 2^{r + 5} \cdot 5^{\text{ord}_5(i)}$. These give the solutions stated in the Corollary.

Let $i \in \{3, 6\}$. Then $2^r - 5^s = \pm 9 = \pm 3^2$. Since $\min(2^r, 5^s) > 16$, we observe from Lemma 2.11 that there is no solution.

Let $i = 7$. Then $2^r - 5^s = \pm 21$. Let $s$ be even. Since $2^r > 16$, taking modulo 8, we find that $-1 \equiv \pm 21$ (modulo 8) which is not possible. Hence $s$ is odd. Then $2^r - 5^s \equiv 2^r + 2^s \equiv 0$ modulo 7. Since $2^r, 2^s \equiv 1, 2, 4$ modulo 7, we get a contradiction. \hfill \Box

3. Proof of Theorem 3

Let $D = 4, 3$ according as $d = 2, 3$, respectively. Let $v = \frac{m}{\pi k}$. Assume that

$$P(\Delta(m, d, k)) = P(m(m + d) \cdots (m + (k - 1)d) < Dk,$$

then

$$\omega(\Delta(m, d, k)) \leq \pi(Dk) - 1. \quad (12)$$

For every prime $p \leq Dk$ dividing $\Delta$, we delete a term $m + i\mu d$ such that $\text{ord}_p(m + i\mu d)$ is maximal. Note that $p|m + id$ for at most one $i$ if $p \geq k$. Then we are left with a set $T$ with $1 + t := |T| \geq k - \pi(Dk) + 1 := 1 + t_0$. Let $t_0 \geq 0$ which we assume in this section to ensure that $T$ is non-empty. We arrange the elements of $T$ as $m + i_0' d < m + i_1' d < \cdots < m + i_{t_0} d < .. < m + i'_d$. Let $\mathbb{P}$

$$\mathbb{P} := \prod_{\nu=0}^{t_0} (m + i'_\nu d) \geq d^{k - \pi(Dk) + 1} \frac{\prod_{i=0}^{k - \pi(Dk)} (v k + i)}. \quad (13)$$

We now apply [LaSh04b, Lemma 2.1, (14)] to get

$$\mathbb{P} \leq (k - 1)!d^{-\text{ord}_d(k - 1)!}. \quad (14)$$

Comparing the upper and lower bounds of $\mathbb{P}$, we have

$$d^{\pi(Dk)} \geq \frac{d^{k+1} \prod_{i=0}^{k-\pi(Dk)} (v k + i)}{(k - 1)!d^{-\text{ord}_d(k - 1)!}}$$

which imply

$$d^{\pi(Dk)} \geq \frac{d^{k+1}d^\text{ord}_d(k - 1)! (v k)^{k - \pi(Dk)}}{(k - 1)!} \quad (14) \quad (vd^k)^{\pi(Dk)} \geq \frac{(vd^k)^{k+1}d^{k-1/d-1}(k - 1)^{-1}}{\sqrt{2(k - 1)!}}e^{\cdot e^{12(k - 1)}}$$

By using the estimates for $\text{ord}_d((k - 1)!)$ and $(k - 1)!$ given in Lemma 2.1, we obtain

$$= \left( evd^k \frac{k}{k - 1} \right)^k \frac{v \sqrt{k}}{\pi k} \sqrt{\frac{k}{k - 1}} e^{\cdot e^{12(k - 1)}}\sqrt{2\pi} \sqrt{\frac{k}{k - 1}} e^{\cdot e^{12(k - 1)}}$$
implying
\begin{equation}
\pi(Dk) > \frac{k \log(\nu d^{\frac{d}{d-1}}) + (k + \frac{1}{2}) \log(\frac{k}{k-1}) - \frac{1}{12(k-1)} + \frac{1}{2} \log \frac{v^2 k}{2\pi e^2 d^{\frac{d}{d-1}}}}{\log(\nu d k)}.
\end{equation}
Again by using the estimates for \(\pi(\nu)\) given in Lemma 2.1 and \(\frac{\log(\nu d k)}{\log(Dk)} = 1 + \frac{\log \nu d}{\log(Dk)}\), we derive
\begin{equation}
0 > \frac{1}{2} \log \frac{v^2 k}{2\pi e^2 d^{\frac{d}{d-1}}} - \frac{1}{12(k-1)} + k \left( \log(\nu d^{\frac{d}{d-1}}) - D \left( 1 + \frac{\log \nu d}{\log(Dk)} \right) \left( 1 + \frac{1.2762}{\log(Dk)} \right) \right).
\end{equation}
Let \(v\) be fixed with \(v d \geq D\). Then expression
\[ F(k, v) := \log(\nu d^{\frac{d}{d-1}}) - D \left( 1 + \frac{\log \nu d}{\log(Dk)} \right) \left( 1 + \frac{1.2762}{\log(Dk)} \right) \]
is an increasing function of \(k\). Let \(k_1 := k_1(v)\) be such that \(F(k, v) > 0\) for all \(k \geq k_1\). Then we observe that the right hand side of (16) is an increasing function for \(k \geq k_1\). Let \(k_0 := k_0(v) \geq k_1\) be such that the right hand side of (16) is positive. Then (16) is not valid for all \(k \geq k_0\) implying (15) and hence (14) are not valid for all \(k \geq k_0\).

Also for a fixed \(k\), if (16) is not valid at some \(v = v_0\), then (14) is also not valid at \(v = v_0\). Observe that for a fixed \(k\), if (14) is not valid at some \(v = v_0\), then (14) is also not valid when \(v \geq v_0\).

Therefore for a given \(v = v_0\) with \(v_0 d \geq D\), the inequality (14) is not valid for all \(k \geq k_0(v_0)\) and \(v \geq v_0\).

3(a). Proof of Theorem 3 for the case \(d = 3\)

Let \(d = 3\) and let the assumptions of Theorem 3 be satisfied. Let \(2 \leq k \leq 11\) and \(m > 3k\). Observe that \(k - \pi(3k) + 1 = 0\) for \(k \leq 8\) and \(k - \pi(3k) + 1 = 1\) for \(9 \leq k \leq 11\). If \(T \neq \phi\), then \(m \leq 2^3 \times 5 \times 7 = 280\).

By Corollary 2.10, we may assume that \(2 \leq k \leq 8\), \(m \geq 6450\) and \(T = \phi\). Further \(i_p\) exists for each prime \(p \leq 3k\), \(p \neq 3\) and \(i_p \neq i_q\) for \(p \neq q\) otherwise \(|T| \geq k - \pi(3k) + 1 + 1 > 0\). Also \(pq \nmid (m + id)\) for any \(i\) whenever \(p, q \geq k\) otherwise \(T \neq \phi\). Thus \(P((m + 3i_2)(m + 3i_3)) = 5\) if \(k < 8\). For \(k = 8\), we get \(P((m + 3i_2)(m + 3i_3)) \leq 7\) with \(P((m + 3i_2)(m + 3i_3)) = 7\) only if \(7|m\) and \(\{i_2, i_3\} \cap \{0, 7\} \neq \phi\).

Let \(k \leq 7\) or \(k = 8\) with \(P((m + 3i_2)(m + 3i_3)) = 5\). Let \(j_0 = \min(i_2, i_3), X = m + 3j_0\) and \(i = |i_2 - i_3|\). Then \(X \geq 6450\) and this is excluded by Corollary 2.12.
Let $k = 8$ and $P((m + 3i_2)(m + 3i_3)) = 7$. Then $7|m$ and $\{i_2, i_3\} \cap \{0, 7\} \neq \phi$. Hence $i_7 = 0$ or 7 and $7 \in \{i_2, i_3\}$ if $i_7 = 0$ and 0 $\in \{i_2, i_3\}$ if $i_7 = 7$. If $5 \nmid m(m+21)$, then $\{i_2, i_7\} = \{0, 7\}$ and either
\[ m = 7 \times 2^r, \quad m + 21 = 7^{1+s} \text{ or } m = 7^{1+s}, \quad m + 21 = 7 \times 2^r \]
implies $2^r - 7^s = \pm 3$. Since $2^r \geq \frac{m}{7} > 40$, we get by taking modulo 8 that $(-1)^{s+1} \equiv \pm 3$ which is a contradiction. Thus $5|m(m+21)$ implying $2 \times 5 \times 7|m(m+21)$. By taking the prime factorization, we obtain
\[ m = 2^{a_0}5^{b_0}7^{c_0}, \quad m + 21 = 2^{a_1}5^{b_1}7^{c_1} \]
with $\min(a_0, a_1) = \min(b_0, b_1) = 0$, $\min(c_0, c_1) = 1$ and further $b_0 + b_1 = 1$ if $i_2 \in \{0, 7\}$ and $a_0 + a_1 \leq 2$ if $i_5 \in \{0, 7\}$. From the identity $\frac{m+21}{7} - \frac{m}{7} = 3$, we obtain one of
\[ (i) \quad 2^a - 5 \cdot 7^c = \pm 3 \quad \text{or} \quad (ii) \quad 5 \cdot 2^a - 7^c = \pm 3 \]
or (iii) $5^b - 2^\delta \cdot 7^c = \pm 3$ or (iv) $2^\delta \cdot 5^b - 7^c = \pm 3$
with $\delta \in \{1, 2\}$. Further from $m \geq 6450$, we obtain $c \geq 3$ and
\[ a \geq 9, a \geq 7, b \geq 4, b \geq 3 \]
according as (i), (ii), (iii), (iv) hold, respectively. These equations give rise to a Thue equation
\[ X^3 + AY^3 = B \]
with integers $X, Y, A > 0, B > 0$ given by

<table>
<thead>
<tr>
<th>$c \pmod{3}$</th>
<th>Equation</th>
<th>$A$</th>
<th>$B$</th>
<th>$X$</th>
<th>$Y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) 0, 1</td>
<td>$2^a - 5 \cdot 7^c = \pm 3$</td>
<td>$5 \cdot 2^a \cdot 7^c$</td>
<td>$3 \cdot 2^a$</td>
<td>$\pm 2^{a+c} \cdot 7^c$</td>
<td>$\pm 7^{c+c'}$</td>
</tr>
<tr>
<td>(ii) 0, 1</td>
<td>$5 \cdot 2^a - 7^c = \pm 3$</td>
<td>$25 \cdot 2^a \cdot 7^c$</td>
<td>$75 \cdot 2^a$</td>
<td>$\pm 5 \cdot 2^{a+2} \cdot 7^c$</td>
<td>$\pm 7^{c+c'}$</td>
</tr>
<tr>
<td>(iii) 0, 1</td>
<td>$5^b - 2^\delta \cdot 7^c = \pm 3$</td>
<td>$2^\delta \cdot 5^b \cdot 7^c$</td>
<td>$3 \cdot 5^b$</td>
<td>$\pm 5 \cdot 2^a \cdot 7^c$</td>
<td>$\pm 7^{c+c'}$</td>
</tr>
<tr>
<td>(iv) 0, 1</td>
<td>$2^\delta \cdot 5^b - 7^c = \pm 3$</td>
<td>$2^{3-\delta} \cdot 5^b \cdot 7^c$</td>
<td>$2^{3-\delta} \cdot 5^b$</td>
<td>$\pm 2 \cdot 5 \cdot 2^{a+c} \cdot 7^c$</td>
<td>$\pm 7^{c+c'}$</td>
</tr>
<tr>
<td>(v) 2</td>
<td>$2^a - 5 \cdot 7^c = \pm 3$</td>
<td>$175 \cdot 2^a$</td>
<td>$525$</td>
<td>$\pm 5 \cdot 7^{c+c'}$</td>
<td>$\pm 2^{a+c} \cdot 7^c$</td>
</tr>
<tr>
<td>(vi) 2</td>
<td>$5 \cdot 2^a - 7^c = \pm 3$</td>
<td>$35 \cdot 2^a$</td>
<td>$21$</td>
<td>$\pm 7^{c+c'}$</td>
<td>$\pm 2^{a+c} \cdot 7^c$</td>
</tr>
<tr>
<td>(vii) 2</td>
<td>$5^b - 2^\delta \cdot 7^c = \pm 3$</td>
<td>$2^{3-\delta} \cdot 5^b \cdot 7^c$</td>
<td>$21 \cdot 2^{3-\delta}$</td>
<td>$\pm 2 \cdot 7^{c+c'}$</td>
<td>$\pm 5^{c+c'}$</td>
</tr>
<tr>
<td>(viii) 2</td>
<td>$2^\delta \cdot 5^b - 7^c = \pm 3$</td>
<td>$2^{3-\delta} \cdot 5^b$</td>
<td>$21$</td>
<td>$\pm 7^{c+c'}$</td>
<td>$\pm 5^{c+c'}$</td>
</tr>
</tbody>
</table>

where $0 \leq a', b' < 3$ are such that $X, Y$ are integers and $c' = 0, 1$ according as $c(\text{mod } 3) = 0, 1$, respectively. For example, $2^a - 5 \cdot 7^c = \pm 3$ with $c \equiv 0, 1(\text{mod } 3)$ implies $(\pm 2^{a+c})^3 + 5 \cdot 2^a \cdot 7^c = \pm 7^{c+c'}$ where $a'$ is such that $3|a + a'$. This give a Thue equation (18) with $A = 5 \cdot 2^a \cdot 7^c$ and $B = 3 \cdot 2^a$.

By using (17), we see that at least two of
\[ \text{ord}_2(XY) \geq 2 \text{ or } \text{ord}_5(XY) \geq 1 \text{ or } \text{ord}_7(XY) \geq 1 \]
hold except for (vi) and (viii) where $\text{ord}_2(XY) \geq 1$, $\text{ord}_7(XY) \geq 1$ in case of (vi) and $\text{ord}_2(XY) = 0$, $\text{ord}_7(XY) \geq 1$ in case of (viii). Using the command
in Kash, we compute all the solutions in integers $X, Y$ of the above Thue equations. We find that none of solutions of Thue equations satisfy (19).

Hence we have $k \geq 12$. For the proof of Theorem 3, we may suppose from Corollaries 2.10 and 2.3 that

$$m \geq \max(6450, 10.6 \times 3k).$$

Let $12 \leq k \leq 19$. Since $t_0 \geq 1, 2$ for $12 \leq k \leq 16$ and $17 \leq k \leq 19$, respectively, we have

$$m \leq \sqrt[3]{3} \leq \sqrt[4]{4 \times 8 \times 5^2 \times 7^2 \times 11 \times 13} < 6450$$

if $12 \leq k \leq 16$.

$$m \leq \frac{3}{4} \sqrt[3]{3} \leq \frac{3}{4} \sqrt[4]{4 \times 8 \times 16 \times 5^3 \times 7^2 \times 11 \times 13 \times 17} < 6450$$

if $17 \leq k \leq 19$.

This is not possible by (20).

Thus $k \geq 20$. Then $m \geq 6450$ and $v \geq 10.6$ by (20) satisfying $v_0 d \geq D = d = 3$. Now we check that $k_0 \leq 180$ for $v = 10.6$. Therefore (14) is not valid for $k \geq 180$ and $v \geq 10.6$. Thus $k < 180$. Further we check that (15) is not valid for $20 \leq k < 180$ at $v = \frac{6450}{3k}$ except when $k \in \{21, 25, 28, 37, 38\}$. Hence (14) is not valid for $20 \leq k < 180$ when $v \geq \frac{6450}{3k}$ except when $k \in \{21, 25, 28, 37, 38\}$. Thus it suffices to consider $k \in \{21, 25, 28, 37\}$ where we check that (14) is not valid at $v = \frac{6450}{3k}$ and hence it is not valid for all $v \geq \frac{6450}{3k}$. Finally we consider $k = 38$ where we find that (14) is not valid at $v = \frac{8000}{3k}$. Thus $m < 8000$. For $l \in \{1, 2\}$ and $p_{i,3,l} \leq 8000$, we find that $\delta_2(i, 3, l) < 90$ implying the set $\{m, m+3, \ldots, m+3(38-1)\}$ contains a prime. Hence the assertion follows since $m > 3k$. \qed

3(b). Proof of Theorem 3 for $d = 2$

Let $d = 2$ and let the assumptions of Theorem 3 be satisfied. The assertion for Theorem 3 with $k \geq 2$ and $m \leq 4k$ follows from Corollary 2.4. Thus $m > 4k$. For $2 \leq k \leq 37, k \neq 35$, Lemma 2.8 gives the result. Hence for the proof of Theorem 3, we may suppose that $k = 35$ or $k \geq 38$. Further from Corollaries 2.3 and 2.7, we may assume that

$$m \geq \max(M_0, 131 \times 2k).$$

Let $k = 35, 38$. Then $t_0 = 1, 2$ for $k = 35, 38$, respectively and we have

$$m \leq \sqrt[3]{3} \leq \sqrt[4]{27 \cdot 9 \cdot 5 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31} < 10^{10}$$

if $k = 35$.

$$m \leq \frac{3}{4} \sqrt[3]{3} \leq \frac{3}{4} \sqrt[4]{27 \cdot 9^2 \cdot 25 \cdot 5^2 \cdot 7^2 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37} < 10^{10}$$

if $k = 38$.

This is not possible by (21).

Thus we assume that $k \geq 39$. Let $v \geq 131$ and we check that $k_0 \leq 500$ for $v = 131$. Therefore (14) is not valid for $k \geq 500$ and $v \geq 131$. Hence from (21), we get $k < 500$. \qed
Further \( v \geq \frac{M_6}{25} \geq 10^7 \). We check that \( k_0 \leq 70 \) at \( v = 10^7 \) implying (14) is not valid for \( k \geq 70 \) and \( v \geq 10^7 \). Thus \( k < 70 \). For each \( 39 \leq k < 70 \), we find that (14) is not valid at \( v = \frac{M_6}{25} \) and hence for all \( v \geq \frac{M_6}{25} \). This is a contradiction.

\[ \square \]

4. PROOF OF THEOREMS 1 AND 2

Recall that \( q = u + \frac{a}{d} \) with \( 1 \leq \alpha < d \). We observe that if \( G(x) \) has a factor of degree \( k \), then it has a cofactor of degree \( n - k \). Hence we may assume from now on that if \( G(x) \) has a factor of degree \( k \), then \( k \leq \frac{n}{2} \). The following result is [ShTi10, Lemma 10.1].

**Lemma 4.1.** Let \( 1 \leq k \leq \frac{n}{2} \) and
\[
d \leq 2\alpha + 2 \quad \text{if} \quad (k, u) = (1, 0).
\]
If there is a prime \( p \) with
\[
p|(\alpha + (n + u - k)d) \cdots (\alpha + (n + u - 1)d), \quad p \nmid a_0a_n.
\]
such that
\[
p \geq \begin{cases} (k + u - 1)d + \alpha + 1 & \text{if } u > 0 \\ (k + u - 1)d + \alpha + 2 & \text{if } u = 0 \\ \end{cases}
\]
Then \( G(x) \) has no factor of degree \( k \).

Let \( d = 3 \). By putting \( m = \alpha + 3(n - k) \) and taking \( p = P(\Delta(m, 3, k)) \), we find from Lemma 4.1 and Theorem 3 that \( G_{k\frac{1}{2}} \) and \( G_{\frac{k}{3}} \) do not have a factor of degree \( k \geq 2 \) except possibly when \( k = 2, \alpha = 2, m = 2 + 3(n - 2) = 125 \). This gives \( n = 43 \) and we use [ShTi10, Lemma 2.13] with \( p = 2, r = 2 \) to show that \( G_{\frac{k}{3}} \) do not have a factor of degree \( 2 \). Further except possibly when \( m = \alpha + 3(n - 1) = 2^4 \) for positive integers \( l, G_{\frac{k}{3}} \) and \( G_{\frac{k}{2}} \) do not have a linear factor. This proves Theorem 1.

Let \( d = 2 \). Let \( k = 1, u = 0 \). We have \( P(1 + 2(n - 1)) \geq 3 \) and hence taking \( p = P(1 + 2(n - 1)) \) in Lemma 4.1, we find that \( G_{\frac{k}{2}} \) does not have a factor of degree \( k \). Hence from now on, we may suppose that \( k \geq 2 \) and \( 0 \leq u \leq k \).

For \( (m, k) \in \{(5, 2), (7, 2), (9, 4), (13, 5), (17, 6), (15, 7), (21, 8), (19, 9)\} \), we check that \( P(\Delta(m, 2, k)) \geq m \). For \( 0 \leq u \leq k \), by putting \( m = 1 + 2(n + u - k) \), we find from \( n \geq 2k \) and Theorem 3 that
\[
P(\Delta(m, 2, k)) > 2(k + u) = \begin{cases} \min(2(k + u), 3.5k) & \text{if } u \leq 0.5k \\ \min(2(k + u), 4k) & \text{if } 0.5k < u \leq k \\ \end{cases}
\]
extcept when \( k = 2 \), \( (u, m) \in \{(1, 25), (2, 25), (2, 243)\} \). Observe that if \( p > 2(k + u) \), then \( p \geq 2(k + u) + 1 \). Now we take \( p = P(\Delta(m, 2, k)) \) in Lemma 4.1 to obtain that \( G_{u+\frac{1}{2}} \) do not have a factor of degree \( k \) with \( k \geq 2 \) except possibly when \( k = 2, u = 1, n = 13 \) or \( k = 2, u = 2, n \in \{12, 121\} \). We use [ShTi10, Lemma 2.13] with \( (p, r) = (3, 1), (7, 1) \) to show that \( G_{u+\frac{1}{2}} \) do not have a factor of degree \( 2 \) when \( (u, u) = (1, 13), (2, 12) \) and \( (u, n) = (2, 121) \), respectively. \( \square \)
References


Stat-Math Unit, India Statistical Institute, 7, S. J. S. Sansanwal Marg, New Delhi, 110016, India

E-mail address: shanta@isid.ac.in

Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India

E-mail address: shorey@math.iitb.ac.in