Lehmer Numbers with at Least 2 Primitive Divisors

by

Robert Juricevic

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada, 2007

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Robert Juricevic

Abstract

In 1878, Lucas [16] investigated the sequences $(\ell_n)_{n=0}^{\infty}$ where

$$\ell_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

$\alpha\beta$ and $\alpha + \beta$ are coprime integers, and where β/α is not a root of unity. Lucas sequences are divisibility sequences; if $m|n$, then $\ell_m|\ell_n$, and more generally, $\gcd(\ell_m, \ell_n) = \ell_{\gcd(m,n)}$ for all positive integers m and n. Matijasevic utilised this divisibility property of Lucas sequences in order to resolve Hilbert's 10th problem.

In 1930, Lehmer [15] introduced the sequences $(u_n)_{n=0}^{\infty}$ where

$$\begin{aligned} u_n &= \frac{\alpha^n - \beta^n}{\alpha^{\epsilon(n)} - \beta^{\epsilon(n)}}, \\ \epsilon(n) &= \begin{cases} 1, & \text{if } n \equiv 1 \pmod 2; \\ 2, & \text{if } n \equiv 0 \pmod 2; \end{cases} \end{aligned}$$

$\alpha\beta$ and $(\alpha+\beta)^2$ are coprime integers, and where β/α is not a root of unity. The sequences $(u_n)_{n=0}^{\infty}$ are known as Lehmer sequences, and the terms of these sequences are known as Lehmer numbers. Lehmer showed that his sequences had similar divisibility properties to those of Lucas sequences, and he used them to extend the Lucas test for primality.

We define a prime divisor p of u_n to be a primitive divisor of u_n if p does not divide

$$(\alpha^2 - \beta^2)^2 u_3 \cdots u_{n-1}.$$

Note that in the list of prime factors of the first $n-1$ terms of the sequence $(u_n)_{n=0}^{\infty}$, a primitive divisor of u_n is a new prime factor.

We let

$$\begin{aligned} \kappa &= k(\alpha\beta \max\{(\alpha-\beta)^2, (\alpha+\beta)^2\}), \\ \eta &= \begin{cases} 1 \text{ if } \kappa \equiv 1 \pmod 4, \\ 2 \text{ otherwise}, \end{cases} \end{aligned}$$

where $k(\alpha\beta \max\{(\alpha-\beta)^2, (\alpha+\beta)^2\})$ is the squarefree kernel of $\alpha\beta \max\{(\alpha-\beta)^2, (\alpha+\beta)^2\}$. On the one hand, building on the work of Schinzel [24], we prove that if $n > 4$, $n \neq 6$,

$n/(\eta\kappa)$ is an odd integer, and the triple (n, α, β), in case $(\alpha - \beta)^2 > 0$, is not equivalent to a triple (n, α, β) from an explicit table, then the nth Lehmer number u_n has at least two primitive divisors. Moreover, we prove that if $n \geq 1.2 \times 10^{10}$, and $n/(\eta\kappa)$ is an odd integer, then the nth Lehmer number u_n has at least two primitive divisors. On the other hand, building on the work of Stewart [30], we prove that there are only finitely many triples (n, α, β), where $n > 6$, $n \neq 12$, and $n/(\eta\kappa)$ is an odd integer, such that the nth Lehmer number u_n has less than two primitive divisors, and that these triples may be explicitly determined. We determine all of these triples (n, α, β) up to equivalence explicitly when $6 < n \leq 30$, $n \neq 12$, and $n/(\eta\kappa)$ is an odd integer, and we tabulate the triples (n, α, β) we discovered, up to equivalence, for $30 < n \leq 500$. Finally, we show that the conditions $n > 6$, $n \neq 12$, are best possible, subject to the truth of two plausible conjectures.

Acknowledgements

I would like to express my gratitude to Dr. C. L. Stewart for his generous assistance in the preparation of this thesis, and for his support over the course of my doctoral studies. In particular, I would like to thank Dr. C. L. Stewart for arranging computer hardware on which the computations were carried out.

I would also like to thank Shonn Martin, Lis D'Alessio, and Kim Gingerich, for their support over the course of my doctoral studies, Dr. S. Pauli for his assistance with the computer algebra system KASH, and Dr. A. Akbary and Z. Friggstad, for their collaboration on a paper referenced in the bibliography. Moreover, I would like to thank my family for their support. In particular, I would like to thank K. Schäcke for assistance with the computer algebra systems, and for support during my thesis quest.

I dedicate this thesis to JSJ and E. M. Lehmer who celebrated 0 and 100 in 2006.

Contents

List of Tables

Chapter 1

The Integer Sequences Studied by Lucas, Lehmer, and Schinzel

1.1 Introduction

We begin by considering for any two integers $L > 0$ and $M \neq 0$ the quadratic polynomial

$$x^2 - \sqrt{L}x + M,$$

and its two roots obtained by the quadratic formula

$$\alpha = \frac{\sqrt{L} + \sqrt{L - 4M}}{2},$$

and

$$\beta = \frac{\sqrt{L} - \sqrt{L - 4M}}{2}.$$

We note that α and β are algebraic integers as they are roots of

$$x^4 - (L - 2M)x^2 + M^2 = (x^2 - \sqrt{L}x + M)(x^2 + \sqrt{L}x + M). \tag{1.1}$$

Moreover, we note that either $(\alpha^2, \beta^2) \in \mathbb{R} \times \mathbb{R}$, or $(\alpha^2, \beta^2) \notin \mathbb{R} \times \mathbb{R}$, since α^2 and β^2 are roots of

$$x^2 - (L - 2M)x + M^2. \tag{1.2}$$

Since $\alpha \neq 0$, let

$$\gamma = \frac{\beta}{\alpha}.$$

We record Lemma 1.1, which summarizes some useful properties of γ for later reference.

Lemma 1.1 *Let $L > 0$ and $M \neq 0$ be fixed integers and let $\gamma = \beta/\alpha$, where α and β are the roots of $x^2 - \sqrt{L}x + M$.*

1. *The algebraic number γ is of degree at most 2.*
2. *If $(\alpha^2, \beta^2) \in \mathbb{R} \times \mathbb{R}$, then $|\alpha| > |\beta|$, and $|\gamma| < 1$.*
3. *If $(\alpha^2, \beta^2) \notin \mathbb{R} \times \mathbb{R}$, then $|\alpha| = |\beta|$, $|\gamma| = 1$, and $\deg \gamma = 2$.*
4. *If $(\alpha^2, \beta^2) \notin \mathbb{R} \times \mathbb{R}$, and $\gcd(L, M) = 1$, then $Mx^2 - (L - 2M)x + M$ is the minimal polynomial of γ over $\mathbb{Q}$.*
5. *If $(\alpha^2, \beta^2) \notin \mathbb{R} \times \mathbb{R}$, and $\gcd(L, M) = 1$, then γ is a root of unity if and only if*

$$(L, M) \in \{(1, 1), (2, 1), (3, 1)\}.$$

Proof In order to see the first item, note that γ and γ^{-1} are the roots of

$$Mx^2 - (L - 2M)x + M. \tag{1.3}$$

Moreover, if $\gcd(L, M) = 1$, then (1.3) is the minimal polynomial of γ over $\mathbb{Q}$, which settles the fourth item. For the second item, $\alpha^2 = (1/2)(L - 2M + \sqrt{L(L - 4M)})$, from which we deduce $\alpha^2 > \beta^2$, $\sqrt{\alpha^2} > \sqrt{\beta^2}$, and the result. For the third item, α^2 and β^2 are complex conjugates, and in particular $\alpha^2 \neq \beta^2$, $|\alpha| = |\beta|$ and $|\gamma| = 1$. If $\deg \gamma = 1$, then $\gamma = \pm 1$ and $\alpha^2 = \beta^2$, a contradiction. Thus $\deg \gamma = 2$. Finally, we consider the fifth item. If $(L, M) \in \{(1, 1), (2, 1), (3, 1)\}$, it follows directly from (1.3), Definition 2.11, and Lemma 2.13, that γ is a root of unity. On the other hand, suppose that γ is a root of unity. Then by (1.3), Definition 2.11, and Lemma 2.13, it follows that $|M| = 1$. Hence, $|L - 2M| = |M||\gamma + \gamma^{-1}| < 2$, from which we deduce that $(L, M) \in \{(1, 1), (2, 1), (3, 1)\}$ (compare with [4, Lemma 1.5]).

QED.

We will see over the course of this introduction that the arithmetic and algebraic properties of the cyclotomic polynomial are the main tools which we use to study the primitive divisors of Lehmer numbers. In fact, the second item of Lemma 1.1 is precisely the property that given a real Lehmer pair, allows Schinzel to obtain clever inequalities for the cyclotomic polynomial of an elementary nature, and the main result of this first chapter, which we utilise in the proof of Theorem 1.1. Moreover, the fifth item of Lemma 1.1 helps characterise the pairs of integers (L, M) which ensure that we have a complex Lehmer pair for the remaining chapters, the third item of Lemma 1.1 shows that in case we have a complex Lehmer pair, γ lies on the unit circle, and hence we need to use estimates for linear forms in 2-logarithms in order to prove Theorem 2.1, while the first and fourth items of Lemma 1.1 allow us to obtain a lower bound for the absolute logarithmic Weil height of γ, which we need in the proof of Theorem 2.1. We now record some fundamental definitions underlying our study.

Definition 1.2 *A Lucas pair is a pair (α, β) of algebraic integers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational integers, and β/α is not a root of unity.*

Definition 1.3 *Two Lucas pairs (α_1, β_1) and (α_2, β_2) are equivalent if*

$$\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1.$$

Definition 1.4 *A Lehmer pair is a pair (α, β) of algebraic integers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers, and β/α is not a root of unity.*

Definition 1.5 *Two Lehmer pairs (α_1, β_1) and (α_2, β_2) are equivalent if*

$$\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm\sqrt{-1}\}.$$

We observe that given a Lucas or Lehmer pair, $(\alpha - \beta)(\alpha + \beta) \neq 0$, since $\beta/\alpha \neq \pm 1$. Moreover, we use the notation $\sqrt{-1}$ instead of Euler's well established notation i, which Euler introduced in 1777, in order to avoid confusion in our later work, when we index by the letter i.

Definition 1.6 *Given a Lucas pair, we define a Lucas sequence* $(\ell_n)_{n=0}^{\infty}$ *by*

$$\ell_n = \ell_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

A Lucas number is a term of the Lucas sequence $(\ell_n)_{n=0}^{\infty}$.

Lemma 1.7 *Lucas numbers satisfy the following recurrence relation*

$$\begin{aligned} \ell_0 &= 0, \\ \ell_1 &= 1, \\ \ell_n &= (\alpha+\beta)\ell_{n-1} - \alpha\beta\ell_{n-2}, \quad , \quad n \geq 2. \end{aligned}$$

Proof This is clear for $n = 0, 1$. Let $n \geq 2$. It remains to show that

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = (\alpha+\beta)\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} - \alpha\beta\frac{\alpha^{n-2} - \beta^{n-2}}{\alpha - \beta}. \tag{1.4}$$

The desired relation follows on clearing denominators in (1.4), and noting that

$$\begin{aligned} & (\alpha+\beta)(\alpha^{n-1} - \beta^{n-1}) - \alpha\beta(\alpha^{n-2} - \beta^{n-2}) \\ = \ & \alpha^n - \alpha\beta^{n-1} + \beta\alpha^{n-1} - \beta^n - \beta\alpha^{n-1} + \alpha\beta^{n-1} \\ = \ & \alpha^n - \beta^n. \end{aligned}$$

QED.

Definition 1.8 *Given a Lucas or Lehmer pair, we define a Lehmer sequence* $(u_n)_{n=0}^{\infty}$ *by*

$$\begin{aligned} u_n &= u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha^{\epsilon(n)} - \beta^{\epsilon(n)}}, \\ \epsilon(n) &= \begin{cases} 1, & \text{if } n \equiv 1 \pmod 2; \\ 2, & \text{if } n \equiv 0 \pmod 2. \end{cases} \end{aligned}$$

A Lehmer number is a term of the Lehmer sequence $(u_n)_{n=0}^{\infty}$.

Lemma 1.9 *Lehmer numbers satisfy the following recurrence relation*

$$\begin{aligned}
u_0 &= 0,\\
u_1 &= 1,\\
u_2 &= 1,\\
u_n &= (1+(\sqrt{-1})^{n-1}\sin(\pi n/2)((\alpha+\beta)^2-1))u_{n-1}-\alpha\beta u_{n-2}, \quad n\geq 3.
\end{aligned}$$

Proof This follows by definition for $n=0,1,2$. Let $n\geq 3$. Note that if $n\equiv 0 \pmod 2$, then $\sin(\pi n/2)=0$, and we must show that

$$\frac{\alpha^n-\beta^n}{\alpha^2-\beta^2}=\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}-\alpha\beta\frac{\alpha^{n-2}-\beta^{n-2}}{\alpha^2-\beta^2},$$

which is equivalent to showing that for some integer $k\geq 2$,

$$\frac{\alpha^{2k}-\beta^{2k}}{\alpha^2-\beta^2}=\frac{\alpha^{2k-1}-\beta^{2k-1}}{\alpha-\beta}-\alpha\beta\frac{\alpha^{2k-2}-\beta^{2k-2}}{\alpha^2-\beta^2}. \tag{1.5}$$

Clearing denominators in (1.5), it remains to show that

$$\alpha^{2k}-\beta^{2k}=(\alpha+\beta)(\alpha^{2k-1}-\beta^{2k-1})-\alpha\beta(\alpha^{2k-2}-\beta^{2k-2}). \tag{1.6}$$

On the other hand, if $n\equiv 1 \pmod 2$, let $n=2k+1$, for some integer $k\geq 1$. Then

$$\sin(\pi n/2)=\cos(\pi k)=(-1)^k,$$

and

$$(\sqrt{-1})^{n-1}=(-1)^k,$$

and we must show that

$$\frac{\alpha^{2k+1}-\beta^{2k+1}}{\alpha-\beta}=(\alpha+\beta)^2\frac{\alpha^{2k}-\beta^{2k}}{\alpha^2-\beta^2}-\alpha\beta\frac{\alpha^{2k-1}-\beta^{2k-1}}{\alpha-\beta}. \tag{1.7}$$

Clearing denominators in (1.7), it remains to show that

$$\alpha^{2k+1}-\beta^{2k+1}=(\alpha+\beta)(\alpha^{2k}-\beta^{2k})-\alpha\beta(\alpha^{2k-1}-\beta^{2k-1}). \tag{1.8}$$

Plainly, by expanding the right hand side of (1.6) or (1.8), we establish equality (1.6) or (1.8).

QED.

We note that by Lemma 1.7 and by Lemma 1.9, it is easily seen that Lucas numbers and Lehmer numbers are rational integers. In 1930, Lehmer [15] introduced the sequences $(u_n)_{n=0}^{\infty}$, and showed that they had similar divisibility properties to those of Lucas sequences. Earlier, in 1878, Lucas [16], in an article in the first volume of the American Journal of Mathematics, had investigated the integer sequences $(\ell_n)_{n=0}^{\infty}$. Both Lucas and Lehmer sequences generalize the sequences $(a^n - b^n)_{n=0}^{\infty}$, where a and b are coprime integers. In this thesis we are interested in studying the primitive divisors of terms of the Lehmer sequence.

Definition 1.10 *Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $\gcd(a,b) = 1$, $|a| > |b| > 0$. A primitive divisor of a term $a^n - b^n$ of the sequence $(a^n - b^n)_{n=0}^{\infty}$ is a prime number p which divides $a^n - b^n$, but does not divide $a^m - b^m$ for $0 < m < n$.*

Definition 1.11 *A primitive divisor of a term $\ell_n = \ell_n(\alpha, \beta)$ of a Lucas sequence is a prime number p which divides ℓ_n, but does not divide the product*

$$(\alpha - \beta)^2 \ell_2 \cdots \ell_{n-1}.$$

Definition 1.12 *A primitive divisor of a term $u_n = u_n(\alpha, \beta)$ of a Lehmer sequence is a prime number p which divides u_n, but does not divide the product*

$$(\alpha^2 - \beta^2)^2 u_3 \cdots u_{n-1}.$$

The reason for introducing the factor $(\alpha^2 - \beta^2)^2$ in Definition 1.12 is that if a prime number $p > 2$ divides $(\alpha - \beta)^2$, then p divides u_p, while if $p > 2$ divides $(\alpha + \beta)^2$, then p divides u_{2p} (see Lemma 1.24, item 7 and 8). We now record some simple observations underlying our study.

Lemma 1.13 *Let $n > 2$, and let (α, β) be a Lucas pair. A prime number p is a primitive divisor of $\ell_n = \ell_n(\alpha, \beta)$ if and only if p is a primitive divisor of $u_n = u_n(\alpha, \beta)$.*

Proof The result follows by Definitions 1.11 and 1.12, and from the observation that $\ell_n = u_n$ if $n \equiv 1 \pmod 2$, whereas $\ell_n = (\alpha+\beta)u_n$ if $n \equiv 0 \pmod 2$.

QED.

Lemma 1.13 means that searching for primitive divisors of a Lucas sequence is a special case of the same problem for Lehmer sequences.

Lemma 1.14 *Let $L \in \mathbb{Z}$, $M \in \mathbb{Z}$, $L > 0$, $M \neq 0$, $L = gL'$, $M = gM'$, where $g = \gcd(L, M) \geq 1$, and $\gcd(L', M') = 1$. Further, let $\alpha = \sqrt{g}\alpha'$, and $\beta = \sqrt{g}\beta'$, where α' and β' are the roots of $x^2 - \sqrt{L'}x + M'$. Then*

$$u_n(\alpha, \beta) = g^{(n-\epsilon(n))/2} u_n(\alpha', \beta'),$$

where $\epsilon(n)$ is defined in Definition 1.8. In particular, the primitive divisors of $u_n(\alpha, \beta)$ coincide with the primitive divisors of $u_n(\alpha', \beta')$.

Proof The first part follows by Definition 1.8. The second part follows from Definition 1.12 on noting $(\alpha^2 - \beta^2)^2 = Lg(L/g - 4M/g)$.

QED.

Lemma 1.14 means that in searching for primitive divisors of a Lehmer sequence we may assume that L and M are coprime.

Lemma 1.15 *Let $L \in \mathbb{Z}$, $M \in \mathbb{Z}$, $L > 0$, $M \neq 0$, α and β be the roots of $x^2 - \sqrt{L}x + M$, and α' and β' be the roots of $x^2 - \sqrt{-L}x - M$. Then*

$$(-1)^{(n-\epsilon(n))/2} u_n(\alpha, \beta) = u_n(\alpha', \beta'),$$

where $\epsilon(n)$ is defined in Definition 1.8. In particular, the primitive divisors of $u_n(\alpha, \beta)$ coincide with the primitive divisors of $u_n(\alpha', \beta')$.

Proof The first part follows by Definition 1.8 on noting $\alpha' = \sqrt{-1}\alpha$ and $\beta' = \sqrt{-1}\beta$. The second part follows by Definition 1.12.

QED.

Lemma 1.15 means that in searching for primitive divisors of a Lehmer sequence we may assume that L is positive.

Definition 1.16 *We define the cyclotomic polynomial*

$$\Phi_n(x,y) = \prod_{\substack{i=1\\(i,n)=1}}^{n} (x - \zeta_n^i y), \tag{1.9}$$

where

$$\zeta_n = \exp(2\pi\sqrt{-1}/n).$$

The next two Lemmas, Lemma 1.17 and Lemma 1.18, are useful in proving Lemma 1.26, and more importantly, in establishing a particular factorisation of $\Phi_n(x,y)$ in Lemma 1.36, which we exploit in proving Theorem 1.1 and Theorem 3.1.

Lemma 1.17 *For any odd integer $\ell > 1$, $\Phi_\ell(x,-y) = \Phi_{2\ell}(x,y)$.*

Proof

$$\begin{aligned}
\Phi_{2\ell}(x,y) &= \prod_{\substack{j=1\\ \gcd(j,2\ell)=1}}^{2\ell} (x - \zeta_{2\ell}^j y) \\
&= \prod_{\substack{j=1\\ \gcd(j,2\ell)=1}}^{\ell} (x - \zeta_{2\ell}^j y) \prod_{\substack{j=\ell+2\\ \gcd(j,2\ell)=1}}^{2\ell} (x - \zeta_{2\ell}^j y) \\
&= \prod_{\substack{k=(\ell+1)/2\\ \gcd(2k-\ell,\ell)=1}}^{\ell} (x - \zeta_{2\ell}^{2k-\ell} y) \prod_{\substack{k=1\\ \gcd(\ell+2k,\ell)=1}}^{(\ell-1)/2} (x - \zeta_{2\ell}^{\ell+2k} y).
\end{aligned}$$

The result follows on noting that $\gcd(2k-\ell,\ell) = 1$ and $\gcd(\ell+2k,\ell) = 1$ imply $\gcd(k,\ell) = 1$, $\zeta_{2\ell}^{\ell} = \zeta_{2\ell}^{-\ell} = -1$, and $\zeta_{2\ell}^{2k} = \zeta_\ell^k$.

QED.

Lemma 1.18 *For any even integer $\ell > 1$, $\Phi_\ell(x,y) = \Phi_{2\ell}(\sqrt{x},\sqrt{y})$.*

Proof

$$\begin{aligned}
\Phi_{2\ell}(\sqrt{x},\sqrt{y}) &= \prod_{\substack{i=1\\ \gcd(i,2\ell)=1}}^{2\ell} (\sqrt{x}-\zeta_{2\ell}^{i}\sqrt{y}) \\
&= \prod_{\substack{i=1\\ \gcd(i,2\ell)=1}}^{\ell} (\sqrt{x}-\zeta_{2\ell}^{i}\sqrt{y})(\sqrt{x}+\zeta_{2\ell}^{i}\sqrt{y}) \\
&= \prod_{\substack{i=1\\ \gcd(i,\ell)=1}}^{\ell} (x-\zeta_{2\ell}^{2i}y) \\
&= \Phi_{\ell}(x,y).
\end{aligned}$$

QED.

Lemma 1.19 is used to establish Lemma 1.20, and Lemma 1.20 is used to establish Lemma 1.21, which is useful in later applying the particular factorisation of $\Phi_n(x,y)$ from Lemma 1.36, and Lemma 2.1, which is crucial to the proof of Theorem 2.1.

Lemma 1.19 *Let $n > 0$. Then*

$$x^n - y^n = \prod_{d|n} \Phi_d(x,y), \tag{1.10}$$

where $\Phi_d(x,y)$ is defined by equation (1.9).

Proof Assume first that $y \neq 0$. Then equation (1.10) follows from the factorisation

$$\begin{aligned}
x^n - y^n &= y^n((x/y)^n - 1) \\
&= y^n \prod_{j=0}^{n-1} (x/y - \zeta_n^j) \\
&= y^n \prod_{d|n} \prod_{\substack{j=1\\ (j,n)=d}}^{n} (x/y - \zeta_n^j),
\end{aligned}$$

since

$$\prod_{d|n} \Phi_d(x,y) = \prod_{d|n} \prod_{\substack{\ell=1\\ (\ell,n/d)=1}}^{n/d} (x - \zeta_{n/d}^{\ell} y).$$

If $y = 0$, the result follows from the fact that

$$\begin{aligned}\prod_{d|n}\Phi_d(x,0) &= \prod_{d|n}\prod_{\substack{j=1\\ \gcd(j,d)=1}}^{d} x\\ &= \prod_{d|n} x^{\phi(d)}\\ &= x^{\sum_{d|n}\phi(d)}\\ &= x^n.\end{aligned}$$

QED.

Lemma 1.20 *Let $n > 0$. Then*

$$\Phi_n(x,y) = \prod_{d|n}(x^d - y^d)^{\mu(n/d)}, \tag{1.11}$$

where $\Phi_n(x,y)$ is defined by equation (1.9).

Proof Applying the Möbius inversion formula to equation (1.10), we obtain (1.11).

QED.

Lemma 1.21 *Let $n > 1$ be an integer, and let n^* denote the greatest squarefree divisor of n. Then*

$$\Phi_n(x,y) = \Phi_{n^*}(x^{n/n^*}, y^{n/n^*}),$$

where $\Phi_n(x,y)$ is defined by equation (1.9).

Proof It follows from equation (1.11) and the definition of the Möbius function that

$$\begin{aligned}\Phi_n(x,y) &= \prod_{d|n}(x^{n/d} - y^{n/d})^{\mu(d)}\\ &= \prod_{d|n^*}(x^{n/d} - y^{n/d})^{\mu(d)}\\ &= \prod_{d|n^*}((x^{n/n^*})^{n^*/d} - (y^{n/n^*})^{n^*/d})^{\mu(d)}\\ &= \Phi_{n^*}(x^{n/n^*}, y^{n/n^*}).\end{aligned}$$

QED.

Definition 1.22 *For any positive integer m, we let $P(m)$ denote the greatest prime factor of m, with the convention that $P(1) = 1$.*

The next three Lemmas, Lemma 1.23, Lemma 1.24, and Lemma 1.25, establish the connection between the arithmetic properties of the cyclotomic polynomial, and the primitive divisors of u_n. More precisely, that given a Lehmer pair (α, β), the prime factors of the cyclotomic polynomial $\Phi_n(\alpha, \beta)$ are the primitive divisors of $u_n(\alpha, \beta)$, except possibly for the prime factor $P(n/\gcd(n, 3))$.

Lemma 1.23 *Let $n > 2$, and let (α, β) be a Lehmer pair. Then $\Phi_n(\alpha, \beta)$ is an integer.*

Proof

$$\begin{aligned}\Phi_n(\alpha,\beta) &= \prod_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\alpha - \zeta_n^j\beta)(\alpha - \zeta_n^{-j}\beta)\\ &= \prod_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\alpha^2 + \beta^2 - (\zeta_n^j + \zeta_n^{-j})\alpha\beta).\end{aligned}$$

Let

$$F_n(x,y) = \prod_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (x - (\zeta_n^j + \zeta_n^{-j})y).$$

Note that $F_n(x, y)$ is a binary form of degree $\phi(n)/2$, with rational integer coefficients since all of its roots lie in $\mathbb{Q}(\zeta_n^j + \zeta_n^{-j})$, the maximal real subfield of $\mathbb{Q}(\zeta_n)$. It remains to note that since (α, β) is a Lehmer pair, thus $\alpha\beta \in \mathbb{Z}$, $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta \in \mathbb{Z}$, and

$$\Phi_n(\alpha, \beta) = F_n(\alpha^2 + \beta^2, \alpha\beta) \in \mathbb{Z}.$$

QED.

Lemma 1.24 *Let (α, β) be a Lehmer pair and $(u_n)_{n=0}^{\infty}$ the corresponding sequence of Lehmer numbers. Then*

1. *For all positive integers n we have $\gcd(\alpha\beta, u_n) = 1$.*

2. *If* $d|n$*, then* $u_d|u_n$ *and* $\gcd(u_n/u_d, u_d)$ *divides* n/d*.*

3. *For all positive integers* m *and* n *we have* $\gcd(u_m, u_n) = u_{\gcd(m,n)}$*.*

4. *If a prime* p *does not divide* $\alpha\beta(\alpha^2 - \beta^2)^2$*, then* p *divides* $u_{p-1}u_{p+1}$*.*

5. *If a prime* p *divides* u_m*, then* p *divides* u_{mp}/u_m*; if* $p > 2$ *then* p *exactly divides* u_{mp}/u_m *(i.e.* $p^2 \nmid u_{mp}/u_m$*).*

6. *If* $4|u_m$*, then* 2 *exactly divides* u_{2m}/u_m*.*

7. *If a prime* $p > 2$ *divides* $(\alpha - \beta)^2$*, then* p *divides* u_p*; if* $p > 3$ *then* p *exactly divides* u_p*.*

8. *If a prime* $p > 2$ *divides* $(\alpha + \beta)^2$*, then* p *divides* u_{2p}*; if* $p > 3$ *then* p *exactly divides* u_{2p}*.*

9. *If* $n > 2$*,* $d < n$ *and* $d|n$*, then* $\Phi_n(\alpha, \beta)$ *divides* u_n/u_d*, where* $\Phi_n(\alpha, \beta)$ *is defined by equation (1.9).*

Proof These properties go back to Lehmer [15], and are proved by Stewart [29]. They are listed in [4, Proposition 2.1].

QED.

Lemma 1.25 *Let* $P(n/\gcd(n, 3))$ *be defined by Definition 1.22,* (α, β) *be a Lehmer pair, and let* $\Phi_n(\alpha, \beta)$ *be defined by equation (1.9). If* $n > 4$ *and* $n \notin \{6, 12\}$*, then* $P(n/\gcd(n, 3))$ *divides* $\Phi_n(\alpha, \beta)$ *to at most the first power. All other prime factors of* $\Phi_n(\alpha, \beta)$ *are congruent to* $\pm 1 \pmod{n}$*. Moreover, if* $n = 12$*, then some divisor of 6 divides* $\Phi_{12}(\alpha, \beta)$ *to at most the first power. All other prime factors of* $\Phi_{12}(\alpha, \beta)$ *are congruent to* $\pm 1 \pmod{12}$*.*

Proof This is [29, Lemma 6].

QED.

We first use Lemma 1.24 and Lemma 1.25 in order to establish Lemma 1.26, which we utilise in order to complete our proof of Theorem 1.1. For example, Lemma 1.26 means that searching for primitive divisors of $u_{219}((1/2)(3 + \sqrt{37}), (1/2)(3 - \sqrt{37}))$ is the same as searching for primitive divisors of $u_{518}((1/2)(3 + \sqrt{37}), (1/2)(-3 + \sqrt{37}))$, and hence it suffices to consider only one of these Lehmer numbers in the proof of Theorem 1.1.

Lemma 1.26 *Let (α, β) be a Lehmer pair, $L = (\alpha+\beta)^2 > 0$, $M = \alpha\beta \neq 0$, α' and β' be roots of*

$$x^2 - \sqrt{\max\{L-4M, L\}}x + |M|,$$

$n > 4$, $n \notin \{6, 12\}$, $8 \nmid n$, and let

$$u'_n = u_n(\alpha', \beta').$$

Then

$$u_n(\alpha,\beta) = \begin{cases} u'_n & \text{if } M > 0, \\ u'_n & \text{if } M < 0 \text{ and } n \text{ is even}, \\ u'_{2n}/u'_n & \text{if } M < 0 \text{ and } n \text{ is odd.} \end{cases}$$

Moreover, the primitive divisors of $u_n(\alpha, \beta)$ coincide with those of u'_n if $M > 0$, with those of u'_{2n} if $M < 0$ and n is odd, with those of $u'_{n/2}$ if $M < 0$ and $n \equiv 2 \pmod 4$, and with those of u'_n if $M < 0$ and $n \equiv 0 \pmod 4$.

Proof If $M > 0$, then $\max\{L-4M, L\} = L$ and $|M| = M$, hence $u_n = u'_n$. On the other hand, in case $M < 0$, then by definition

$$\alpha' = \frac{1}{2}(\sqrt{L-4M} + \sqrt{L}) = \alpha,$$

and

$$\beta' = \frac{1}{2}(\sqrt{L-4M} - \sqrt{L}) = -\beta.$$

It follows that if n is even and $M < 0$ then

$$\begin{aligned} u'_n &= \frac{(\alpha')^n - (\beta')^n}{(\alpha')^2 - (\beta')^2} \\ &= \frac{(\alpha)^n - (-\beta)^n}{(\alpha)^2 - (-\beta)^2} \\ &= \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} \\ &= u_n, \end{aligned}$$

while if n is odd and $M < 0$ then

$$\begin{aligned}\frac{u'_{2n}}{u'_n} &= \frac{(\alpha')^{2n}-(\beta')^{2n}}{(\alpha')^2-(\beta')^2}\frac{\alpha'-\beta'}{(\alpha')^n-(\beta')^n}\\ &= \frac{(\alpha')^n+(\beta')^n}{\alpha'+\beta'}\\ &= \frac{(\alpha')^n-(-\beta')^n}{\alpha'-(-\beta')}\\ &= \frac{\alpha^n-\beta^n}{\alpha-\beta}\\ &= u_n.\end{aligned}$$

By Lemma 1.24 and Lemma 1.25, the primitive divisors of u_n are the prime factors of $\Phi_n(\alpha,\beta)$, except possibly for $P(n/\gcd(n,3))$. If $M > 0$,

$$\Phi_n(\alpha',\beta') = \Phi_n(\alpha,\beta).$$

If $M < 0$, and $n \equiv 1 \pmod 2$, by Lemma 1.17,

$$\Phi_{2n}(\alpha',\beta') = \Phi_n(\alpha,\beta).$$

If $M < 0$, and $n \equiv 2 \pmod 4$, by Lemma 1.17,

$$\Phi_{n/2}(\alpha',\beta') = \Phi_n(\alpha,\beta).$$

If $M < 0$, and $n \equiv 0 \pmod 4$, by Lemma 1.18,

$$\Phi_n(\alpha',\beta') = \Phi_{n/2}(\alpha^2,\beta^2),$$

and since $8 \nmid n$, by Lemma 1.21,

$$\Phi_{n/2}(\alpha^2,\beta^2) = \Phi_n(\alpha,\beta).$$

QED.

The first general result[1] about the existence of primitive divisors of terms of the Lehmer sequence dates back to 1892, when Zsigmondy [37] proved that given an integer Lucas pair

$$(\alpha,\beta) \in \mathbb{Z} \times \mathbb{Z},$$

[1] Earlier, Bang [2] dealt with the case $\alpha \in \mathbb{Z}$ and $\beta = 1$.

if $n > 6$, then u_n has a primitive divisor. This result was obtained independently in 1904 by Birkhoff and Vandiver [5]. Note that their result is best possible since the prime divisors of 63, the 6th term of the sequence $(2^n - 1)_{n=0}^{\infty}$, divide the second or third term.

In 1913, Carmichael [7] extended this result by proving that given a real Lucas pair

$$(\alpha, \beta) \in \mathbb{R} \times \mathbb{R},$$

if $n > 12$, then u_n has a primitive divisor. Note that Carmichael's result is best possible since the prime divisors of 144, the 12th term of the Fibonacci sequence

$$\left(\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)\right)_{n=0}^{\infty},$$

divide the third or fourth term.

In the 1950's, Ward [36] and Durst [9] extended these results to real Lehmer pairs (α, β) such that

$$(\alpha^2, \beta^2) \in \mathbb{R} \times \mathbb{R}.$$

In 1962, motivated by Ward's remark that nothing appears to be known for complex Lehmer pairs (α, β) such that

$$(\alpha^2, \beta^2) \notin \mathbb{R} \times \mathbb{R},$$

Schinzel [22] showed that given a Lehmer pair, there exists a constant $n_1(\alpha, \beta)$, depending on α and β, such that if $n > n_1(\alpha, \beta)$, then u_n has at least one primitive divisor. Later, in 1974, Schinzel [27] showed that, rather surprisingly, the constant $n_1(\alpha, \beta)$, depending on α and β, may be replaced by an absolute constant n_1.

In 1977, Stewart [30] made a remarkable improvement by not only making Schinzel's work explicit by using his estimates on linear forms in 2-logarithms in order to show that we may take

$$n_1 = e^{452}4^{67} \sim 10^{231},$$

but also by showing that there are only finitely many Lehmer sequences whose nth term, $n > 6$, $n \notin \{8, 10, 12\}$, does not possess a primitive divisor, and by establishing a cyclotomic criterion, and thereby an algorithm, from which these exceptional sequences may be explicitly determined by solving the implicated Thue equations. Moreover, Stewart showed that the restrictions $n > 6$, $n \notin \{8, 10, 12\}$, are best possible for the Lehmer sequence $(u_n)_{n=0}^{\infty}$, but may be replaced by the best possible restrictions $n > 4$, $n \neq 6$ for the Lucas sequence $(\ell_n)_{n=0}^{\infty}$.

In the 1990's, Voutier [33] made use of the refinement by Laurent, Mignotte and Nesterenko [14] for linear forms in 2-logarithms, and refined Stewart's constant to

$$n_1 = 2 \times 10^{10}.$$

Furthermore, after implementing Stewart's algorithm in MAPLE, and computing all of the solutions of the implicated Thue equations in the range $n \leq 30$, and the small solutions of the implicated Thue equations in the range $30 < n \leq 250$, Voutier [32] tabulated all Lehmer sequences whose nth term, $6 < n \leq 30$, $n \notin \{8, 10, 12\}$, has no primitive divisor, and conjectured that $n_1 = 30$. Moreover, shortly after, Voutier [34] refined his work and established

$$n_1 = 30030.$$

At the turn of the millennium, in a spectacular display of the interplay between computational number theory and theoretical number theory in helping to resolve an outstanding problem, Bilu, Hanrot, and Voutier [4] established Voutier's conjecture. In particular, they showed

$$n_1 = 30.$$

In order to further motivate our study, let us consider the following problems:

Problem 1.27 *Classify all Lehmer triples (n, α, β) such that (α, β) is a Lehmer pair, and u_n has at least one primitive divisor.*

Problem 1.28 *Classify all Lehmer triples (n, α, β) such that (α, β) is a Lehmer pair, and u_n has at least r primitive divisor(s), where r is a given natural number.*

As already noted, Problem 1.27 has been solved completely by Bilu, Hanrot, and Voutier. In this thesis we concern ourselves with Problem 1.28. It is not clear at the outset that Problem 1.28 is not accounted for by the solution to Problem 1.27. As an example, note that there are Lehmer sequences whose nth term has 2 primitive divisors. In particular, the 7th term of the following Lehmer sequence

$$0, 1, 1, 37, 2 \cdot 31, 1669, 3 \cdot 29 \cdot 37, 7 \cdot 13 \cdot 883, \ldots$$

corresponding to the triple

$$(n, \alpha, \beta) = (7, \sqrt{3} + 2\sqrt{7}, \sqrt{3} - 2\sqrt{7}),$$

has two primitive divisors, namely 13 and 883. Note that 7 divides $(\alpha^2 - \beta^2)^2 = 2^6 \cdot 3 \cdot 7$, and so is not a primitive divisor.

The first general result in the direction of Problem 1.28 was made in 1962 by Schinzel [23]. More precisely, let $n > 0$ be an integer, a and b be relatively prime integers with $|a| > |b| > 0$, $k(ab)$ denote the squarefree kernel of ab, and let

$$\eta_0 = \begin{cases} 1 & \text{if } k(ab) \equiv 1 \pmod 4, \\ 2 & \text{if } k(ab) \equiv 2, 3 \pmod 4. \end{cases}$$

Schinzel showed that if $n/(\eta_0 k(ab))$ is an odd integer, and the triple (n, a, b) is not in Table 1.1, then the nth term of the sequence $(a^n - b^n)_{n=0}^{\infty}$ has at least two primitive divisors. In the same year, Rotkiewicz [21] generalised this theorem to real Lucas sequences.

In 1963, Schinzel [24] generalised Rotkiewicz's theorem to a theorem about the nth term of the Lehmer sequence $(u_n)_{n=0}^{\infty}$ having at least two primitive divisors. In the same year, Schinzel [25] proved a theorem about u_n having at least r primitive divisors, where r is 3, 4 or 6, while a few years later in 1968, Schinzel [26] refined all of his theorems on primitive divisors of Lehmer sequences. Nonetheless, all of Schinzel's theorems had the shape, ignoring other conditions similar to the conditions described above for the sequence $(a^n - b^n)_{n=0}^{\infty}$, that there exists a constant $n_r(\alpha, \beta)$, depending on α and β, such that if $n > n_r(\alpha, \beta)$, then u_n has at least r primitive divisors, where r is a natural number. Later, in 1974, Schinzel [26] showed that for each r, $n_r(\alpha, \beta)$ may be replaced by an absolute constant n_r.

In this thesis, we extend Stewart's program. More precisely, we use the arithmetic and algebraic properties of the cyclotomic polynomial, together with a sharp estimate for linear forms in 2-logarithms determined by Mignotte, and sharp inequalities for the arithmetic functions $\phi(n)$ and $\omega(n)$, in order to make Schinzel's constant n_r for $r = 2$ explicit.

n, a, b	n, a, b
$1, (2^i+1)^2, (2^i-1)^2$	$3, 4, -3$
$1, -(2^i+1)^2, -(2^i-1)^2$	$3, -4, 3$
$1, (p^i+1)^2/4, (p^i-1)^2/4$	$4, \pm 2, \pm 1$
$1, -(p^i+1)^2/4, -(p^i-1)^2/4$	$6, 3, 1$
$2, (2^i+1)^2, -(2^i-1)^2$	$6, -3, -1$
$2, -(2^i+1)^2, (2^i-1)^2$	$6, 4, -1$
$2, (p^i+1)^2/4, -(p^i-1)^2/4$	$6, -4, 1$
$2, -(p^i+1)^2/4, (p^i-1)^2/4$	$6, 4, 3$
$3, 3, -1$	$6, -4, -3$
$3, -3, 1$	$12, \pm 2, \pm 1$
$3, 4, 1$	$12, \pm 3, \pm 2$
$3, -4, -1$	$20, \pm 2, \pm 1$

Table 1.1: A table of all exceptional triples (n, a, b). Note $i \in \mathbb{N}$.

Furthermore, for certain conditions on (n, α, β) similar to the conditions described for the sequence $(a^n - b^n)_{n=0}^{\infty}$, we show that there are only finitely many Lehmer sequences whose nth term has less than two primitive divisors, and we establish a cyclotomic criterion, and thereby an algorithm, from which these exceptional sequences may be explicitly determined by solving the implicated Thue equations. Finally, we show that our work is best possible subject to the truth of two plausible conjectures.

1.2 Classifying real Lehmer triples

In this section we establish a theorem on terms of Lehmer sequences, generated by a real Lehmer pair, with at least two primitive divisors, in the direction of solving a part of Problem 1.28. Our result is obtained by making explicit a result of Schinzel [24]. In particular, Schinzel determines a finite list of Lehmer numbers which might have fewer than 2 primitive divisors, and we shall determine those which do have fewer than 2 primitive divisors. In contrast to the case where (α, β) is a complex Lehmer pair and $\gamma = \beta/\alpha$ lies on the unit circle, the methods used by Schinzel [24] in case (α, β) is a real Lehmer pair rely on the fact that $|\alpha| > |\beta|$, and hence that the algebraic factors of the implied cyclotomic polynomial may be bounded from below using clever inequalities of an elementary nature, and in particular, not inequalities for linear forms in 2-logarithms.

1.2.1 Statement of Theorem 1.1 and Preliminary Lemmas

We note first that the following conditions

$$\begin{aligned} L &> 0, \\ M &\neq 0, \\ L - 4M &> 0, \\ \gcd(L, M) &= 1, \end{aligned} \tag{1.12}$$

ensure that we have a real Lehmer pair. Plainly, the conditions (1.12) imply $(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$, and hence that $(\alpha^2, \beta^2) \in \mathbb{R} \times \mathbb{R}$ and $\beta/\alpha \in \mathbb{R}$. Moreover, β/α is a root of unity in $\mathbb{R}$ if and only if $\beta = \pm\alpha$. If $\beta = \alpha$, then $L - 4M = 0$, while if $\beta = -\alpha$, then $L = 0$, in either case, a contradiction.

Definition 1.29 *For any integer n, we define $k(n)$ to be n divided by the greatest square divisor of n. We note that $k(n)$ is known as the squarefree kernel of n.*

We let

$$\kappa = k(M \max\{L - 4M, L\}), \tag{1.13}$$

and

$$\eta = \begin{cases} 1 & \text{if } \kappa \equiv 1 \pmod 4, \\ 2 & \text{if } \kappa \equiv 2, 3 \pmod 4. \end{cases} \tag{1.14}$$

Theorem 1.1 *Let L and M be integers satisfying the conditions (1.12), (α, β) be the associated real Lehmer pair, and let κ and η be defined by (1.13) and (1.14). If $n > 4$, $n \neq 6$, $n/(\eta\kappa)$ is an odd integer, and the triple (n, α, β) is not equivalent to a triple (n, α, β) from Table 1.2, then $u_n(\alpha, \beta)$ has at least two primitive divisors.*

(n,α,β)	(n,L,M)	p
5 , $(1/2)\sqrt{5}+(1/2)$, $(1/2)\sqrt{5}-(1/2)$	$5,5,1$	11
*5 , $(3/2)+(1/2)\sqrt{5}$, $(3/2)-(1/2)\sqrt{5}$	$5,9,1$	11
7 , $(1/2)\sqrt{3}+(1/2)\sqrt{7}$, $(1/2)\sqrt{3}-(1/2)\sqrt{7}$	$7,3,-1$	13
*10 , $(1/2)+(1/2)\sqrt{5}$, $(1/2)-(1/2)\sqrt{5}$	$10,1,-1$	11
10 , $(1/2)\sqrt{5}+(3/2)$, $(1/2)\sqrt{5}-(3/2)$	$10,5,-1$	11
*12 , 3, -2	$12,1,-6$	61
*12 , 2, -1	$12,1,-2$	13
12 , $(1/2)\sqrt{2}+(1/2)\sqrt{6}$, $(1/2)\sqrt{2}-(1/2)\sqrt{6}$	$12,2,-1$	13
*12 , $1+\sqrt{2}$, $1-\sqrt{2}$	$12,4,-1$	11
12 , $(1/2)\sqrt{6}+(1/2)\sqrt{2}$, $(1/2)\sqrt{6}-(1/2)\sqrt{2}$	$12,6,1$	13
12 , $\sqrt{2}+1$, $\sqrt{2}-1$	$12,8,1$	11
*12, 2, 1	$12,9,2$	13
*12, 3, 2,	$12,25,6$	61
14 , $(1/2)\sqrt{7}+(1/2)\sqrt{3}$, $(1/2)\sqrt{7}-(1/2)\sqrt{3}$	$14,7,1$	13
15 , $(1/2)\sqrt{5}+(1/2)$, $(1/2)\sqrt{5}-(1/2)$	$15,5,1$	31
*20, 2, -1	$20,1,-2$	41
*20, 2, 1	$20,9,2$	41
*30 , $(1/2)+(1/2)\sqrt{5}$, $(1/2)-(1/2)\sqrt{5}$	$30,1,-1$	31

Table 1.2: A table of all exceptional real Lehmer triples (n,α,β) (up to equivalence) and associate triples (n,L,M), such that $L>0$, $M\neq 0$, $L-4M>0$, $\gcd(L,M)=1$, $4<n$, $n\neq 6$, $n/(\eta\kappa)$ is an odd integer, and $u_n(\alpha,\beta)$ has less than two primitive divisors, together with their primitive divisor p. Note that the star $*$ indicates the real Lehmer triples correspond to real Lucas triples.

Lemma 1.30 clarifies the admissible n in Theorem 1.1.

Lemma 1.30 *Let $n > 2$ be a positive integer, m_1 be a squarefree divisor of n, and let $m_2 = 1$ if $m_1 \equiv 1 \pmod 4$, and $m_2 = 2$ otherwise. If $n/(m_1 m_2)$ is an odd integer and m_1 is positive, then n is either an odd integer, or a multiple of 4 not divisible by 8, or a multiple of 2, not divisible by 4, and divisible by a prime $p \equiv 3 \pmod 4$. Moreover, if $n/(m_1 m_2)$ is an odd integer and m_1 is negative, then n is either an odd integer, or a multiple of 4 not divisible by 8, or a multiple of 2, not divisible by 4, and divisible by a prime $p \equiv 1 \pmod 4$.*

Proof Let ℓ be an odd integer. In case m_1 is positive, note that either $m_1 m_2 = 1 + 4z_1$, or $m_1 m_2 = 4(1 + 2z_2)$, or $m_1 m_2 = 2(3 + 4z_3)$, for some nonnegative integers z_1, z_2, z_3, from which it follows that either $n = (1 + 4z_1)\ell$, or $n = 4(1 + 2z_2)\ell$, or $n = 2(3 + 4z_3)\ell$. Similarly, in case m_1 is negative, either $n = (3 + 4z_1)\ell$, or $n = 4(1 + 2z_2)\ell$, or $n = 2(1 + 4z_3)\ell$.

QED.

The proof of Theorem 1.1 amounts to exhibiting the set $R_0 \cup Q_0$, defined in Lemma 1.31, due to Schinzel [24, Theorem 1], explicitly. We do this in Table 1.2. Schinzel [26] remarks that Brillhart and Selfridge have done this, although no reference[2] to their work is given.

Lemma 1.31 *Let L and M be integers satisfying the conditions (1.12), (α, β) be the associated real Lehmer pair, and let κ and η be defined by (1.13) and (1.14). If $n > 4$, $n \neq 6$, and $n/(\eta\kappa)$ is an odd integer, and the triple $(n, L, M) \notin R_0 \cup Q_0$, where*

$$\begin{aligned}
R_0 &= \{(5,9,1),(10,5,-1),(20,1,-2),(20,9,2)\},\\
Q_0 &= \{(n,L,M) \in S_0 \cup T_0 : u_n \textit{ has less than two primitive divisors}\},\\
S_0 &= \{(\eta|\kappa|, L, M) : (L,M) \in S\},\\
T_0 &= \{(3\eta|\kappa|, L, M) : (L,M) \in T\},\\
S &= \{(L,M) : \gcd(L,M) = 1, (L,M) = (12,-25), (112,25), \textit{ or } 1 \le |M| \le 15,\\
&\quad 2M + 2|M| + 1 \le L < \min(64 + 2M - 2|M|, 2M + 2|M| + 4|M|^{1/2} + 1\},\\
T &= \{(L,M) : \gcd(L,M) = 1, (L,M) = (4,-1), (8,1) \textit{ or } 1 \le |M| \le 15,\\
&\quad L = 2M + 2|M| + 1\},
\end{aligned}$$

[2] In personal correspondence, Brillhart confirms the calculation was done, not published, and since lost.

then $u_n(\alpha, \beta)$ has at least two primitive divisors.

Proof This is part 1 of [24, Theorem 1].

QED.

Lemma 1.32 *Let u_n be defined by Definition 1.8, $\ell > 1$ be a divisor of u_n,*

$$a = L(L-4M) \prod_{\substack{i=3 \\ \gcd(i,n)\neq 1}}^{n-1} u_i,$$

$b = \gcd(\ell, a)$, $c = \ell/b$, and $d = \gcd(b, c)$. If $c > 1$ and $d = 1$, then ℓ has at least one divisor, which is a primitive divisor of u_n.

Proof Note first that $\ell = bc$. Since $c > 1$, let $p|c$. Then $p|\ell$. We will show that $p \nmid L(L-4M)u_3 \cdots u_{n-1}$. Since $d = 1$, $p \nmid b$, which implies $p \nmid a$. We are left to show for $3 \le i \le n-1$, $\gcd(n, i) = 1$, that $p \nmid u_i$. Recall part 3 of Lemma 1.24, that for all positive integers m and n

$$\gcd(u_n, u_m) = u_{\gcd(m,n)}. \tag{1.15}$$

It follows from equation (1.15) that for any $3 \le i \le n-1$ for which $\gcd(i, n) = 1$,

$$\gcd(u_n, u_i) = u_{\gcd(i,n)} = u_1 = 1,$$

and hence $\gcd(\ell, u_i) = 1$. Plainly, $p \nmid u_i$ for any $3 \le i \le n-1$, $\gcd(i, n) = 1$.

QED.

Definition 1.33 *Let p be an odd prime number, $a \in \mathbb{Z}$. The values of $(a|p) = (\frac{a}{p})$, called the Legendre symbol, are given by*

$$(a|p) \\ = \begin{cases} 1, & \textit{if} \;\; p \nmid a, \; \textit{and there exists an integer } x \textit{ such that } \; x^2 = a \pmod{p}; \\ 0, & \textit{if} \;\; p|a; \\ -1, & \textit{if} \;\; p \nmid a, \; \textit{and there does not exist an integer } x \textit{ such that } \; x^2 = a \pmod{p}. \end{cases}$$

Definition 1.34 *Let b be an odd integer with prime factorisation $\pm 1 \prod_{i=1}^{r} p_i$. For $a \in \mathbb{Z}$, we define the Jacobi symbol $(a|b)$, as follows:*

$$(a|-1) = (a|1) = 1,$$

and

$$(a|b) = \prod_{i=1}^{r} (a|p_i),$$

a product of Legendre symbols.

Lemma 1.35 *Let $\ell > 1$ be an odd integer, and let m be a divisor of ℓ. Then*

$$\Phi_\ell(x,y) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1 \\ (s|m)=1}}^{\ell} (\sqrt{x} - \zeta_\ell^s \sqrt{y})(\sqrt{x} + \zeta_\ell^s \sqrt{y}) \prod_{\substack{t=1 \\ \gcd(t,\ell)=1 \\ (t|m)=-1}}^{\ell} (\sqrt{x} - \zeta_\ell^t \sqrt{y})(\sqrt{x} + \zeta_\ell^t \sqrt{y}).$$

Proof On dividing the values of j in equation (1.9) into two classes according as $(j|m) = 1$ or $(j|m) = -1$, we obtain

$$\Phi_\ell(x,y) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1 \\ (s|m)=1}}^{\ell} (x - \zeta_\ell^s y) \prod_{\substack{t=1 \\ \gcd(t,\ell)=1 \\ (t|m)=-1}}^{\ell} (x - \zeta_\ell^t y). \tag{1.16}$$

Since ℓ is odd, we have for $\epsilon = \pm 1$ that

$$\{\zeta_\ell^j, j = 1, \ldots, \ell, \gcd(j,\ell) = 1, (j|m) = \epsilon\} = \{\zeta_\ell^{2j}, j = 1, \ldots, \ell, \gcd(j,\ell) = 1, (j|m) = \epsilon(2|m)\}.$$

The result follows on considering $x - \zeta_\ell^s y$ and $x - \zeta_\ell^t y$ in (1.16) as a difference of squares, and factoring.

QED.

Lemma 1.36 *Let $\ell > 1$ be a squarefree integer, and let m be an integer divisor of ℓ such that ℓ/m is an odd integer. Then for $N = \ell$ or $N = 2\ell$, we have*

$$\Phi_N(x,y) = \Phi_{N,m}^{(1)}(x,y)\Phi_{N,m}^{(2)}(x,y), \tag{1.17}$$

where if $N = \ell$ and m is odd,

$$\Phi^{(1)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,\ell)=1\\ (s|m)=1}}^{\ell} (\sqrt{x} - \zeta_\ell^s \sqrt{y}) \prod_{\substack{t=1\\ \gcd(t,\ell)=1\\ (t|m)=-1}}^{\ell} (\sqrt{x} + \zeta_\ell^t \sqrt{y}), \tag{1.18}$$

and

$$\Phi^{(2)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,\ell)=1\\ (s|m)=1}}^{\ell} (\sqrt{x} + \zeta_\ell^s \sqrt{y}) \prod_{\substack{t=1\\ \gcd(t,\ell)=1\\ (t|m)=-1}}^{\ell} (\sqrt{x} - \zeta_\ell^t \sqrt{y}); \tag{1.19}$$

if $N = 2\ell$ and m is odd,

$$\Phi^{(1)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,\ell)=1\\ (s|m)=1}}^{\ell} (\sqrt{x} - \sqrt{-1}\zeta_\ell^s \sqrt{y}) \prod_{\substack{t=1\\ \gcd(t,\ell)=1\\ (t|m)=-1}}^{\ell} (\sqrt{x} + \sqrt{-1}\zeta_\ell^t \sqrt{y}), \tag{1.20}$$

and

$$\Phi^{(2)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,\ell)=1\\ (s|m)=1}}^{\ell} (\sqrt{x} + \sqrt{-1}\zeta_\ell^s \sqrt{y}) \prod_{\substack{t=1\\ \gcd(t,\ell)=1\\ (t|m)=-1}}^{\ell} (\sqrt{x} - \sqrt{-1}\zeta_\ell^t \sqrt{y}); \tag{1.21}$$

if $N = 2\ell$ and m is even,

$$\Phi^{(1)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,4\ell)=1\\ (m|s)=1}}^{4\ell} (\sqrt{x} - \zeta_{4\ell}^s \sqrt{y}), \tag{1.22}$$

and

$$\Phi^{(2)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,4\ell)=1\\ (m|s)=1}}^{4\ell} (\sqrt{x} + \zeta_{4\ell}^s \sqrt{y}); \tag{1.23}$$

and where $(s|m)$, $(t|m)$, and $(m|s)$ are Jacobi symbols, as defined in Definition 1.34.

Proof This is essentially line (4), (5), and (7) of [23, Theorem 1]. Note that our notation and exposition here differs from [23, Theorem 1]. In particular, we have replaced n by ℓ, $\psi_{n,m}(x)$ by $\Phi^{(1)}_{N,m}(x,y)$, we have defined explicitly $\Phi^{(2)}_{N,m}(x,y)$, and we have written the indices for the products under the products. We present an argument based on Schinzel's proof of [23, Theorem 1].

Suppose that ℓ is odd, and m is odd. The equations (1.18) and (1.19) follow from Lemma 1.35 (note in case $m = 1$ the product over t is empty). Furthermore, the equations (1.20) and (1.21) follow from Lemma 1.17, together with Lemma 1.35. On the other hand, if ℓ is even, then m is even since ℓ/m is odd. Let $\ell = 2k_1$ where $\gcd(k_1, 2) = 1$ since ℓ is squarefree. Since ℓ is even, by Lemma 1.18 we have that

$$\Phi_{2\ell}(x,y) = \Phi_\ell(x^2,y^2). \tag{1.24}$$

Further, since $\ell = 2k_1$, and k_1 is odd, we have by Lemma 1.17 that

$$\Phi_\ell(x^2,y^2) = \Phi_{k_1}(x^2,-y^2) = \Phi_{k_1}(x,\sqrt{-1}y)\Phi_{k_1}(x,-\sqrt{-1}y). \tag{1.25}$$

By (1.24) and (1.25), we obtain

$$\Phi_{2\ell}(x,y) = \Phi_{k_1}(x,\sqrt{-1}y)\Phi_{k_1}(x,-\sqrt{-1}y). \tag{1.26}$$

On noting that

$$\sqrt{-1} = \zeta_8^2,$$

we see that we may further factor the right hand side of (1.26) in order to obtain

$$\Phi_{2\ell}(x,y) = \Phi_{k_1}(\sqrt{x},\zeta_8\sqrt{y})\Phi_{k_1}(\sqrt{x},-\zeta_8\sqrt{y})\Phi_{k_1}(\sqrt{x},\zeta_8^3\sqrt{y})\Phi_{k_1}(\sqrt{x},-\zeta_8^3\sqrt{y}). \tag{1.27}$$

Schinzel verifies (see between lines (17) and (18) [23, page 558]) that the right hand side of (1.27) is equal to the product of (1.22) and (1.23).

QED.

1.2.2 Proof of Theorem 1.1

Proof By Lemma 1.31, it suffices to compute the set $R_0 \cup S_0 \cup T_0$, from which we may deduce the set $R_0 \cup Q_0$. The computed set $R_0 \cup S_0 \cup T_0$ of 216 elements appears in Table

1.3 and Table 1.4. The proof consists of sieving out all Lehmer triples (n, α, β) such that (α, β) is a real Lehmer pair, and u_n has more than one primitive divisor, from Table 1.3 and Table 1.4. The remaining elements are the elements of the set $R_0 \cup Q_0$, and are tabulated in Table 1.2.

Let $u_n = \prod_{i=1}^{k} p_i^{a_i}$. Note that the result of calling the function *ifactors(u_n,Easy)* in MAPLE, which is based on the Brillhart and Morrison factoring algorithm, will be either of the form

$$[1, [[p_1, a_1], \ldots, [p_k, a_k]]],$$

or of the form

$$[1, [[p_1, a_1], \ldots, [p_i, a_i], [\ell, 1]]],$$

where ℓ is a composite integer, and

$$[p_1, a_1], \ldots, [p_i, a_i], i < k,$$

were "easy" to compute. In particular, the MAPLE function *ifactors(u_n,Easy)* uses

$$\gcd(u_n, 720720)$$

and

$$\gcd(u_n, \prod_{p=17}^{1699} p).$$

Computing $u_n(\alpha, \beta)$ and calling the function *ifactors(u_n,Easy)* in MAPLE, for each triple (n, L, M) from Table 1.3, we determine that all of the triples from Table 1.3 have at least two primitive divisors, except for the triples

$$(117, 1, -3), (132, 33, 8), (132, 1, -8) \tag{1.28}$$

and

$$(156, 39, 8), (156, 7, -8), \tag{1.29}$$

the triples in Table 1.2, and the triples

$$\begin{aligned}
&(41, 41, 9), (43, 7, -9), (51, 5, -3),\\
&(82, 5, -9), (86, 43, 9), (102, 17, 3),\\
&(105, 21, 5), (140, 3, -8), (140, 35, 8)\\
&(156, 2, -13), (156, 54, 13).
\end{aligned} \tag{1.30}$$

We call the function *ifactors(u_n,pollard,n)* in MAPLE for the triples (1.28) and the triples in Table 1.2, the function *ifactors(u_n,lenstra)* in MAPLE for the triples (1.29), and Lemma 1.32 for the triples (1.30), in order to obtain

$$\begin{array}{rl}
117, 1, -3, & [819001577161, 173196209426761], \\
132, 33, 8, & [29700133, 58739156810797], \\
132, 1, -8, & [29700133, 58739156810797], \\
156, 39, 8, & [18066827, 51378219047], \\
156, 7, -8, & [18066827, 51378219047],
\end{array}$$

$$\begin{array}{rl}
41, 41, 9, & [1559, [.32... \times 10^{23}, 1]], \\
43, 7, -9, & [947, [.11... \times 10^{24}, 1]], \\
51, 5, -3, & [14281, [.10... \times 10^{13}, 1]], \\
82, 5, -9, & [1559, [.85... \times 10^{44}, .26... \times 10^{22}]], \\
86, 43, 9, & [947, [.14... \times 10^{52}, .12... \times 10^{29}]],
\end{array}$$

and

$$\begin{array}{rl}
102, 17, 3 & [14281, [.50... \times 10^{32}, .48... \times 10^{26}]], \\
105, 21, 5, & [211, [.20... \times 10^{20}, 1]], \\
140, 3, -8, & [139, [.20... \times 10^{49}, .24... \times 10^{23}]], \\
140, 35, 8, & [139, [.20... \times 10^{49}, .24... \times 10^{23}]], \\
156, 2, -13, & [157, [.80... \times 10^{62}, .15... \times 10^{34}]] \\
156, 54, 13, & [157, [.80... \times 10^{62}, .15... \times 10^{34}]].
\end{array}$$

Note that the functions *ifactors(u_n,pollard,n)* and *ifactors(u_n,lenstra)* in MAPLE establish a complete factorisation of u_n for the triples aforementioned, and as such we may conclude that for those triples for which these functions are called, we have precisely one primitive divisor, or at least two primitive divisors. Moreover, in each case, we listed the triple together with a certificate vector v, which has the form $[p]$, consisting of one primitive divisor, or the form $[p_1, p_2]$, consisting of two primitive divisors, or the form $[p, [\ell, b]]$, consisting of one primitive divisor and the corresponding $[\ell, b]$ as defined by Lemma 1.32.

Similarly, computing $u_n(\alpha, \beta)$ and calling the function *ifactors(u_n,Easy)* in MAPLE, for each triple (n, L, M) from Table 1.4, we determine that all of the triples from Table 1.4 have at least two primitive divisors, except for the triples

$$(234, 13, 3), \tag{1.31}$$

$$\begin{aligned}&(259, 9, -7), (308, 56, 11), (308, 12, -11), (364, 56, 13), (364, 4, -13)\\&(518, 37, 7), (532, 38, 7), (532, 10, -7), (1860, 62, 15), (1860, 2, -15),\end{aligned} \tag{1.32}$$

and the triples

$$\begin{aligned}&(165, 1, -11), (203, 1, -7), (210, 1, -5), (220, 22, 5), (220, 2, -5)\\&(330, 45, 11), (372, 7, -6), (372, 31, 6), (406, 29, 7), (420, 30, 7),\\&(420, 2, -7), (561, 51, 11), (583, 9, -11), (940, 47, 10), (940, 7, -10),\\&(1060, 53, 10), (1060, 13, -10), (1122, 7, -11), (1166, 53, 11), (1276, 58, 11),\\&(1276, 14, -11), (1508, 58, 13), (1508, 6, -13).\end{aligned} \tag{1.33}$$

We call the function *ifactors(u_n,pollard,n)* in MAPLE for the triple (1.31), and Lemma 1.32 for the triples (1.33), in order to obtain

$$234, 13, 3, [819001577161, 173196209426761],$$

and

$$\begin{aligned}165, 1, -11, &\quad [331, [.57... \times 10^{57}, .25... \times 10^{13}]]\\203, 1, -7, &\quad [176611, [.44... \times 10^{80}, 1]]\\210, 1, -5, &\quad [211, [.16... \times 10^{43}, .78... \times 10^{23}]]\\220, 22, 5, &\quad [881, [.12... \times 10^{50}, .14... \times 10^{14}]]\\220, 2, -5, &\quad [881, [.12... \times 10^{50}, .14... \times 10^{14}]],\end{aligned}$$

$$\begin{array}{rl}
330, 45, 11, & [331, [.14... \times 10^{131}, .64... \times 10^{87}]] \\
372, 7, -6, & [373, [.94... \times 10^{186}, .75... \times 10^{116}]] \\
372, 31, 6, & [373, [.94... \times 10^{186}, .75... \times 10^{116}]] \\
406, 29, 7, & [176611, [.74... \times 10^{164}, .16... \times 10^{85}]] \\
420, 30, 7, & [132973261, [.19... \times 10^{156}, .88... \times 10^{112}]],
\end{array}$$

$$\begin{array}{rl}
420, 2, -7, & [132973261, [.19... \times 10^{156}, .88... \times 10^{112}]] \\
561, 51, 11, & [142228087, [.56... \times 10^{339}, .10... \times 10^{127}]] \\
583, 9, -11, & [2333, [.38... \times 10^{402}, .12... \times 10^{36}]] \\
940, 47, 10, & [194581, [.80... \times 10^{592}, .11... \times 10^{349}]] \\
940, 7, -10, & [194581, [.80... \times 10^{592}, .11... \times 10^{349}]],
\end{array}$$

$$\begin{array}{rl}
1060, 53, 10, & [47701, [.86... \times 10^{736}, .29... \times 10^{435}]] \\
1060, 13, -10, & [47701, [.86... \times 10^{736}, .29... \times 10^{435}]] \\
1122, 7, -11, & [142228087, [.11... \times 10^{688}, .19... \times 10^{475}]] \\
1166, 53, 11, & [2333, [.11 \times 10^{785}, .38... \times 10^{418}]] \\
1276, 58, 11, & [19139, [.72... \times 10^{911}, .51... \times 10^{493}]]
\end{array}$$

and

$$\begin{array}{rl}
1276, 14, -11, & [19139, [.72... \times 10^{911}, .51... \times 10^{493}]] \\
1508, 58, 13, & [459566017, [.13... \times 10^{1016}, .11... \times 10^{553}]] \\
1508, 6, -13, & [459566017, [.13... \times 10^{1016}, .11... \times 10^{553}]].
\end{array}$$

On the other hand, for the triples (1.32), we first observe that by Lemma 1.26, the following pairs of Lehmer numbers have the same primitive divisors

$$\begin{array}{rcl}
u_{259}(\frac{3+\sqrt{37}}{2},\frac{3-\sqrt{37}}{2}) & , & u_{518}(\frac{3+\sqrt{37}}{2},\frac{-3+\sqrt{37}}{2}); \\
u_{308}(\sqrt{14}+\sqrt{3},\sqrt{14}-\sqrt{3}) & , & u_{308}(\sqrt{14}+\sqrt{3},-\sqrt{14}+\sqrt{3}); \\
u_{364}(\sqrt{14}+1,\sqrt{14}-1) & , & u_{364}(\sqrt{14}+1,-\sqrt{14}+1); \\
u_{532}(\frac{\sqrt{38}+\sqrt{10}}{2},\frac{\sqrt{38}-\sqrt{10})}{2}) & , & u_{532}(\frac{\sqrt{38}+\sqrt{10}}{2},\frac{-\sqrt{38}+\sqrt{10}}{2}); \\
u_{1860}(\frac{\sqrt{62}+\sqrt{2}}{2},\frac{\sqrt{62}-\sqrt{2})}{2}) & , & u_{1860}(\frac{\sqrt{62}+\sqrt{2}}{2},\frac{-\sqrt{62}+\sqrt{2}}{2}).
\end{array}$$

Hence, it suffices to consider only one Lehmer number in each pairing. Furthermore, note that by Lemma 1.24 and Lemma 1.25, the primitive divisors of u_n coincide with the prime factors of $\Phi_n(\alpha,\beta)$, except possibly for $P(n/\gcd(n,3))$. By Lemma 1.36, we factor $\Phi_n(\alpha,\beta) = \Phi^{(1)}_{N,\kappa}(\alpha,\beta)\Phi^{(2)}_{N,\kappa}(\alpha,\beta)$, where $\kappa = k(M\max\{L-4M,L\})$, and $N = \eta\kappa\prod_{p|n,p\nmid\eta\kappa} p$, for each of the remaining triples (1.32), in order to obtain[3]

[3] The $*$ indicates that $\Phi^{(j)}_{N,\kappa}(\alpha,\beta)$ is a prime number as determined by the MAPLE function *isprime*.

$$\begin{aligned}
& \Phi^{(1)}_{259,-259}(\frac{3+\sqrt{37}}{2}, \frac{3-\sqrt{37}}{2}) \\
= \;& 4688186794612359348548460589916180894723400737849509490008963078078647137569, \\
& *\Phi^{(2)}_{259,-259}(\frac{3+\sqrt{37}}{2}, \frac{3-\sqrt{37}}{2}) \\
= \;& 2560253291728767860552750122103255198933323101108540307556538691009, \\
& \Phi^{(1)}_{308,154}(\sqrt{14}+\sqrt{3}, \sqrt{14}-\sqrt{3}) \\
= \;& 36719117012774411593795373075885082101401, \\
& \Phi^{(2)}_{308,154}(\sqrt{14}+\sqrt{3}, \sqrt{14}-\sqrt{3}) \\
= \;& 1212886066088329232632423660041428753964355298041, \\
& \Phi^{(1)}_{364,182}(\sqrt{14}+1, \sqrt{14}-1) \\
= \;& 2496645988012336074301209765985081733111928329, \\
& *\Phi^{(2)}_{364,182}(\sqrt{14}+1, \sqrt{14}-1) \\
= \;& 11525121307558382647076296300816832852765266463808089, \\
& \Phi^{(1)}_{532,266}(\frac{\sqrt{38}+\sqrt{10}}{2}, \frac{\sqrt{38}-\sqrt{10}}{2}) \\
= \;& 368956586335300162081912817177156057722610340294815943469126220024381, \\
& \Phi^{(2)}_{532,266}(\frac{\sqrt{38}+\sqrt{10}}{2}, \frac{\sqrt{38}-\sqrt{10}}{2}) \\
= \;& 8213483633355603457368863499769725714729728684667572880477292382219135396021, \\
& \Phi^{(1)}_{1860,930}(\frac{\sqrt{62}+\sqrt{2}}{2}, \frac{\sqrt{62}-\sqrt{2}}{2}) \\
= \;& 65263175209620882129621722222532598631677902835936764924439756666755560213965\cdots \\
& 4618428464226880647434563514173237560119620874719055423722960780194820161, \\
& \Phi^{(2)}_{1860,930}(\frac{\sqrt{62}+\sqrt{2}}{2}, \frac{\sqrt{62}-\sqrt{2}}{2}) \\
= \;& 1531507552436612570339953572710157714837872041220167757614626810463657235743\cdots \\
& 057857894978949499647194588866521969104848023121915071216543924255296726014\cdots \\
& 671624981879085017485584079041.
\end{aligned}$$

Since $\gcd(\Phi^{(1)}_{N,\kappa}(\alpha,\beta), \Phi^{(2)}_{N,\kappa}(\alpha,\beta)) = 1$ and $\Phi^{(j)}_{N,\kappa}(\alpha,\beta) > n$ for each $(n, N, \kappa, \alpha, \beta)$ presented above and $j \in \{1, 2\}$, we deduce by Lemma 1.24 and Lemma 1.25 that u_n has at least two primitive divisors for each of the triples (1.32).

QED.

(n, L, M, v)	(n, L, M, v)	(n, L, M, v)
$5, 5, 1, [11]$	$22, 49, 11, [197, 14783]$	$76, 2, -9, [457, 20521]$
$5, 9, 1, [11]$	$23, 7, -4, [137, 25253]$	$76, 38, 9, [457, 20521]$
$7, 3, -1, [13]$	$26, 12, -13, [131, 3821]$	$78, 13, 3, [79, 157]$
$7, 8, -7, [13, 419]$	$28, 4, -7, [281, 28729]$	$82, 5, -9, [1559]$
$7, 12, -25, [13, 883]$	$28, 32, 7, [281, 28729]$	$84, 2, -3, [337, 1429]$
$9, 1, -12, [19, 163]$	$30, 1, -1, [31]$	$84, 14, 3, [337, 1429]$
$10, 1, -1, [11]$	$30, 27, 5, [29, 2459]$	$86, 43, 9, [947]$
$10, 5, -1, [11]$	$30, 64, 15, [31, 15391]$	$91, 11, -13, [181, 50051]$
$11, 5, -11, [197, 14783]$	$33, 48, 11, [461, 46861]$	$92, 10, -9, [643, 827]$
$11, 8, -9, [89, 4091]$	$34, 1, -4, [307, 28663]$	$92, 46, 9, [643, 827]$
$12, 1, -6, [61]$	$35, 8, -5, [281, 4339]$	$94, 47, 9, [1787, 5923]$
$12, 1, -2, [13]$	$36, 1, -6, [37, 73]$	$102, 1, -4, [103, 409]$
$12, 2, -1, [13]$	$36, 25, 6, [37, 73]$	$102, 17, 3, [14281]$
$12, 4, -1, [11]$	$37, 37, 9, [1481, 18797]$	$105, 21, 5, [211]$
$12, 6, 1, [13]$	$38, 19, 4, [37, 151]$	$110, 45, 11, [220159501, 292589551]$
$12, 8, 1, [11]$	$39, 1, -3, [79, 157]$	$111, 37, 9, [223, 300367]$
$12, 9, 2, [13]$	$41, 41, 9, [1559]$	$114, 7, -3, [113, 569]$
$12, 25, 6, [61]$	$42, 5, -4, [83, 20327]$	$115, 3, -5, [229, 691]$
$13, 64, 13, [131, 3821]$	$43, 7, -9, [947]$	$117, 1, -3, []$
$14, 7, 1, [13]$	$44, 3, -2, [43, 571]$	$132, 1, -8, []$
$14, 36, 7, [13, 419]$	$44, 6, -11, [43, 3037]$	$132, 10, -11, [1321, 3167]$
$14, 112, 25, [13, 883]$	$44, 11, 2, [43, 571]$	$132, 33, 8, []$
$15, 4, -15, [31, 15391]$	$44, 50, 11, [43, 3037]$	$132, 54, 11, [1321, 3167]$
$15, 5, 1, [31]$	$46, 23, 4, [137, 25253]$	$140, 3, -8, [139]$
$15, 7, -5, [29, 2459]$	$47, 11, -9, [1787, 5923]$	$140, 35, 8, [139]$
$17, 17, 4, [307, 28663]$	$51, 5, -3, [14281]$	$143, 8, -11, [12011, 349207]$
$18, 49, 12, [19, 163]$	$51, 17, 4, [103, 409]$	$145, 29, 5, [1451, 108751]$
$19, 3, -4, [37, 151]$	$52, 5, -2, [727, 5147]$	$148, 5, -8, [149, 4441]$
$20, 1, -2, [41]$	$52, 13, 2, [727, 5147]$	$148, 37, 8, [149, 4441]$
$20, 4, -9, [19, 3739]$	$55, 1, -11, [220159501, 292589551]$	$156, 2, -13, [157]$
$20, 9, -10, [61, 5521]$	$57, 19, 3, [113, 569]$	$156, 7, -8, []$
$20, 9, 2, [41]$	$60, 4, -5, [59, 601]$	$156, 39, 8, []$
$20, 40, 9, [19, 3739]$	$60, 24, 5, [59, 601]$	$156, 54, 13, [157]$
$20, 49, 10, [61, 5521]$	$66, 4, -11, [461, 46861]$	$159, 5, -12, [317, 3499]$
$21, 21, 4, [83, 20327]$	$70, 28, 5, [281, 1889]$	$164, 9, -8, [11317, 150881]$
$22, 44, 9, [89, 4091]$	$74, 1, -9, [1481, 18797]$	$164, 41, 8, [11317, 150881]$

Table 1.3: A table of candidate real Lehmer triples $(n, L, M) \in R_0 \cup S_0 \cup T_0$ such that $n < 165$, together with their certificate vectors v.

(n, L, M, v)	(n, L, M, v)	(n, L, M, v)
$165, 1, -11, [331]$	$372, 31, 6, [373]$	$1020, 51, 10, [1021, 2039]$
$165, 55, 12, [331, 659]$	$390, 60, 13, [333451, 696637889]$	$1034, 3, -11, [1033, 1110517]$
$172, 11, -8, [859, 54869]$	$396, 1, -8, [397, 6337]$	$1060, 13, -10, [47701]$
$172, 43, 8, [859, 54869]$	$396, 33, 8, [397, 6337]$	$1060, 53, 10, [47701]$
$177, 59, 12, [353, 13451]$	$406, 29, 7, [176611]$	$1122, 7, -11, [142228087]$
$182, 63, 13, [181, 50051]$	$420, 2, -7, [132973261]$	$1166, 53, 11, [2333]$
$183, 13, -12, [4027, 9151]$	$420, 30, 7, [132973261]$	$1218, 29, 7, [13399, 267961]$
$195, 8, -13, [333451, 696637889]$	$434, 3, -7, [433, 1303]$	$1254, 57, 11, [8779, 11287]$
$203, 1, -7, [176611]$	$462, 33, 7, [8779, 20327]$	$1276, 14, -11, [19139]$
$210, 1, -5, [211]$	$476, 6, -7, [1429, 2857]$	$1276, 58, 11, [19139]$
$217, 31, 7, [433, 1303]$	$476, 34, 7, [1429, 2857]$	$1378, 1, -13, [108863, 32622773]$
$220, 2, -5, [881]$	$517, 47, 11, [1033, 1110517]$	$1430, 55, 13, [1429, 5864431]$
$220, 22, 5, [881]$	$518, 37, 7, []$	$1482, 5, -13, [2963, 5927]$
$222, 1, -9, [223, 300367]$	$532, 10, -7, []$	$1508, 6, -13, [459566017]$
$230, 23, 5, [229, 691]$	$532, 38, 7, []$	$1508, 58, 13, [459566017]$
$231, 5, -7, [8779, 20327]$	$546, 11, -7, [1093, 1637]$	$1534, 59, 13, [3067, 99709]$
$234, 13, 3, []$	$561, 51, 11, [142228087]$	$1586, 9, -13, [4759, 298169]$
$259, 9, -7, []$	$583, 9, -11, [2333]$	$1596, 1, -14, [105337, 28198129]$
$260, 6, -5, [1039, 967201]$	$609, 1, -7, [13399, 267961]$	$1596, 57, 14, [105337, 28198129]$
$260, 26, 5, [1039, 967201]$	$627, 13, -11, [8779, 11287]$	$1612, 10, -13, [6449, 88661]$
$273, 39, 7, [1093, 1637]$	$630, 1, -5, [187111, 1435141]$	$1612, 62, 13, [6449, 88661]$
$286, 52, 11, [12011, 349207]$	$689, 53, 13, [108863, 32622773]$	$1652, 3, -14, [24781, 2914129]$
$290, 9, -5, [1451, 108751]$	$715, 3, -13, [1429, 5864431]$	$1652, 59, 14, [24781, 2914129]$
$308, 12, -11, []$	$741, 57, 13, [2963, 5927]$	$1708, 5, -14, [3702943, 9677914009]$
$308, 56, 11, []$	$767, 7, -13, [3067, 99709]$	$1708, 61, 14, [3702943, 9677914009]$
$315, 21, 5, [187111, 1435141]$	$793, 61, 13, [4759, 298169]$	$1830, 61, 15, [1831, 18301]$
$318, 53, 12, [317, 3499]$	$820, 1, -10, [821, 36901]$	$1860, 2, -15, []$
$330, 7, -12, [331, 659]$	$820, 41, 10, [821, 36901]$	$1860, 62, 15, []$
$330, 45, 11, [331]$	$860, 3, -10, [859, 16339]$	$2067, 53, 13, [33073, 152959]$
$348, 5, -6, [349, 1741]$	$860, 43, 10, [859, 16339]$	$2460, 1, -10, [49201, 135301]$
$348, 29, 6, [349, 1741]$	$915, 1, -15, [1831, 18301]$	$2460, 41, 10, [49201, 135301]$
$354, 11, -12, [353, 13451]$	$940, 7, -10, [194581]$	$2745, 1, -15, [21961, 32941]$
$364, 4, -13, []$	$940, 47, 10, [194581]$	$4134, 1, -13, [33073, 152959]$
$364, 56, 13, []$	$1012, 2, -11, [1013, 4049]$	$4788, 1, -14, [4789, 67033]$
$366, 61, 12, [4027, 9151]$	$1012, 46, 11, [1013, 4049]$	$4788, 57, 14, [4789, 67033]$
$372, 7, -6, [373]$	$1020, 11, -10, [1021, 2039]$	$5490, 61, 15, [21961, 32941]$

Table 1.4: A table of candidate real Lehmer triples $(n, L, M) \in R_0 \cup S_0 \cup T_0$ such that $n \geq 165$, together with their certificate vectors v.

Chapter 2

Lehmer Numbers with at Least 2 Primitive Divisors

In this chapter, we establish a theorem on terms of Lehmer sequences, generated by a real or complex Lehmer pair, with at least two primitive divisors, in the direction of solving a part of Problem 1.28. More precisely, Schinzel [26] proved that there exists an absolute constant n_2 such that if L and M are integers such that $L > 0$, $M \neq 0$, $L - 4M \neq 0$, $\gcd(L, M) = 1$, $(L, M) \notin \{(1, 1), (2, 1), (3, 1)\}$, (α, β) is the associated Lehmer pair, $n > n_2$, and $n/(\eta\kappa)$ is an odd integer, then $u_n(\alpha, \beta)$ has at least two primitive divisors. In this chapter we show that we may take

$$n_2 = 1.2 \times 10^{10}.$$

We highlight that the case where (α, β) is a complex Lehmer pair and $\gamma = \beta/\alpha$ lies on the unit circle, requires delicate estimates and refined inequalities for linear forms in 2-logarithms, and for the arithmetic functions $\phi(n)$ and $\omega(n)$.

2.1 Statement of Theorem 2.1 and Preliminary Lemmas

First, by Lemma 1.1, we note that the following conditions

$$\begin{aligned} L &> 0, \\ M &\neq 0, \\ L - 4M &< 0, \\ \gcd(L, M) &= 1, \\ (L, M) &\notin \{(1,1),(2,1),(3,1)\}, \end{aligned} \tag{2.1}$$

ensure that we have a complex Lehmer pair (α, β).

Theorem 2.1 *Let L and M be integers satisfying conditions (1.12) or (2.1), (α, β) be the corresponding Lehmer pair, and let κ and η be defined by equations (1.13) and (1.14). If $n \geq 1.2 \times 10^{10}$, and $n/(\eta\kappa)$ is an odd integer, then the nth term $u_n(\alpha, \beta)$ of the Lehmer sequence has at least 2 primitive divisors.*

We note that by Theorem 1.1, if L and M are integers satisfying conditions (1.12), then the constant 1.2×10^{10} may be replaced by 31. Furthermore, if L and M are integers satisfying conditions (2.1), then $M > 0$, for otherwise $L - 4M > 0$. It therefore suffices to prove Theorem 2.1 in case (α, β) is a complex Lehmer pair, and $M = \alpha\beta > 0$. We now state and prove the Lemmas we use to establish Theorem 2.1.

Lemma 2.1 *Let $n > 0$, (α, β) be a Lehmer pair, and $\gamma = \beta/\alpha$. Then*

$$\log|\Phi_n(\alpha, \beta)| = \phi(n)\log|\alpha| - \sum_{\substack{d|n \\ \mu(n/d)=-1}} \log|1 - \gamma^d| + \sum_{\substack{d|n \\ \mu(n/d)=1}} \log|1 - \gamma^d|.$$

Proof Note that equation (1.11) from Lemma 1.20 may be written as

$$|\Phi_n(\alpha, \beta)| = \prod_{d|n} |\alpha|^{d\mu(n/d)} \prod_{d|n} |1 - \gamma^d|^{\mu(n/d)}.$$

Since

$$\phi(n) = n \sum_{t|n} \frac{\mu(t)}{t},$$

$$\begin{aligned}\prod_{d|n} |\alpha|^{d\mu(n/d)} &= |\alpha|^{\sum_{d|n} d\mu(n/d)} \\ &= |\alpha|^{\sum_{dt=n} d\mu(n/d)} \\ &= |\alpha|^{n\sum_{t|n} \mu(t)/t} \\ &= |\alpha|^{\phi(n)}.\end{aligned}$$

QED.

Lemma 2.2 *Let L and M be integers satisfying conditions (1.12) or (2.1), and let κ and η be defined by equations (1.13) and (1.14). Further, let $n > 1$ be an integer such that $n/(\eta\kappa)$ is an odd integer, $\nu = \eta\kappa \prod_{\substack{p|n \\ p\nmid\eta\kappa}} p$, $\ell = \kappa \prod_{p|n, p\nmid\eta\kappa} p$, and $N = \nu$. Then*

$$\Phi_n(\alpha, \beta) = \Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}),$$

where $\Phi_n(\alpha, \beta)$ is defined by equation (1.9), $\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})$ is defined by equations (1.18), (1.20) or (1.22), and $\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})$ is defined by equations (1.19), (1.21), or (1.23).

Proof This is observed by Schinzel [24]. It follows directly from Lemmas 1.21 and 1.36.

QED.

Lemma 2.3 *Let L and M be integers satisfying conditions (2.1), and let κ and η be defined by equations (1.13) and (1.14). Further, let $n > 4$, $n \neq 6$, be an integer such that $n/(\eta\kappa)$ is an odd integer, $\nu = \eta\kappa \prod_{\substack{p|n \\ p\nmid\eta\kappa}} p$, $\ell = \kappa \prod_{p|n, p\nmid\eta\kappa} p$, and $N = \nu$. Then the numbers $\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})$ and $\delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})$, where $\delta = k(L)^{-(\phi(n)/4 - \lfloor \phi(n)/4 \rfloor)}$, are relatively prime rational integers. Note if $4|\phi(n)$ or $k(L) = 1$, then $\delta = 1$. Otherwise, $n = 2q^a$ for some prime number $q \equiv 3 \pmod 4$ and positive integer a, and $\delta = q^{-1/2}$.*

Proof This is [24, Lemma 2]. For the note plainly if $\phi(n) \equiv 0 \pmod 4$ or $\kappa(L) = 1$, then $\delta = 1$. Otherwise, $4 \nmid \phi(n)$, and $\kappa(L) \neq 1$. Since $n \neq 1, 2, 4$, and $4 \nmid \phi(n)$, we have for

some prime number $q \equiv 3 \pmod 4$ and positive integer a that $n = q^a$ or $n = 2q^a$. Suppose $n = q^a$. Since $n \equiv 0 \pmod{\kappa}_1$, $\kappa_1 = 1$ or $\kappa_1 = q$. If $\kappa_1 = q$, then $\eta_1 = 2$, and $2|n$, a contradiction. If $\kappa_1 = 1$, then since $\kappa_1 \equiv 0 \pmod{\kappa}(L)$, $\kappa(L) = 1$, a contradiction. Hence $n \neq q^a$. Let $n = 2q^a$. Since $n \equiv 0 \pmod{\kappa}(L)$, thus $\kappa(L) = 2$ or $\kappa(L) = q$. If $\kappa(L) = 2$, then $\kappa_1 \equiv 2 \pmod 4$, hence $\eta_1 = 2$, and $4|n$, a contradiction. Thus $\kappa(L) = q$. Further, let $q = 3 + 4k$, and note that the fractional part of $\phi(2q^a)/4 = (3+4k)^{a-1}(k+1/2)$ is $1/2$.
QED.

Lemma 2.4 *Let L and M be integers satisfying conditions (2.1), and let κ and η be defined by equations (1.13) and (1.14). Further, let $n > 4$, $n \neq 6$, be an integer such that $n/(\eta\kappa)$ is an odd integer, $\nu = \eta\kappa \prod_{\substack{p|n \\ p\nmid\eta\kappa}} p$, $\ell = \kappa \prod_{p|n, p\nmid\eta\kappa} p$, and $N = \nu$. If*

$$\min(|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|, |\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|) > n, \tag{2.2}$$

then u_n has at least two primitive divisors.

Proof By Lemma 2.2 and Lemma 2.3, either

$$|\Phi_n(\alpha, \beta)| = |\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})||\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|, \tag{2.3}$$

where

$$\begin{aligned} \Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) &\in \mathbb{Z}, \\ \Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) &\in \mathbb{Z}, \end{aligned}$$

and

$$\gcd(\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}), \Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})) = 1, \tag{2.4}$$

or $n = 2q^a$ for some prime $q \equiv 3 \pmod 4$ and positive integer a, and

$$|\Phi_{2q^a}(\alpha, \beta)| = |q^{-1/2}\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})||q^{-1/2}\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|q, \tag{2.5}$$

where

$$\begin{aligned} q^{-1/2}\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) &\in \mathbb{Z}, \\ q^{-1/2}\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) &\in \mathbb{Z}, \end{aligned}$$

and

$$\gcd(q^{-1/2}\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}),q^{-1/2}\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}))=1. \tag{2.6}$$

By Lemma 1.25, the prime divisors of $|\Phi_n(\alpha,\beta)|$ coincide with the primitive divisors of u_n except for $P(n/\gcd(n,3))$, which if it divides $\Phi_n(\alpha,\beta)$, it divides $\Phi_n(\alpha,\beta)$ with exponent 1. Plainly, if equation (2.2) holds, since $n \geq P(n/\gcd(n,3))$, then in equation (2.3),

$$\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})$$

and

$$\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})$$

have a prime divisor different from $P(n/\gcd(n,3))$, and hence the result follows from equation (2.4). Moreover, in case $n=2q^a$, equation (2.2) implies

$$|q^{-1/2}\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})|>1$$

and

$$|q^{-1/2}\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})|>1$$

in equation (2.5), and since $q=P(2q^a/\gcd(2q^a,3))$, the result follows by equation (2.6) and Lemma 1.25 in case $n=2q^a$.

QED.

Lemma 2.5 *Let $\chi(r)$ be an arbitrary character modulo m, $m>1$, $c\neq 0$ and let $x\in\mathbb{C}$, $|x|=1$. Then*

$$\prod_{\substack{r=1\\ \gcd(r,m)=1\\ \chi(r)=c}}^{m} |x-\zeta_m^r| < \exp(2\sqrt{m}(\log m)^2).$$

Proof This is [24, Lemma 3].

QED.

Lemma 2.6 *Let L and M be integers satisfying conditions (2.1), (α,β) be the associated complex Lehmer pair, and let κ and η be defined by equations (1.13) and (1.14). Further,* *let $n > 4$, $n \neq 6$, be an integer such that $n/(\eta\kappa)$ is an odd integer, $\nu = \eta\kappa \prod_{\substack{p|n \\ p\nmid\eta\kappa}} p$, $\ell = \kappa \prod_{p|n, p\nmid\eta\kappa} p$, and $N = \nu$. Then*

$$\max(|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|, |\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|) < |\alpha|^{\phi(n)/2} \exp(4\sqrt{n}(\log n)^2).$$

Proof We have three cases to consider, according to the residue of κ modulo 4. We prove the case $\kappa \equiv 1 \pmod 4$ for $|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|$. The other cases are similar. Let $\gamma = \beta/\alpha$. By equation (1.18), we have that

$$\begin{aligned}
|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})| &= \prod_{\substack{s=1 \\ \gcd(s,\ell)=1 \\ (s|\kappa)=1}}^{\ell} |\sqrt{\alpha^{n/\nu}} - \zeta_\ell^s \sqrt{\beta^{n/\nu}}| \prod_{\substack{t=1 \\ \gcd(t,\ell)=1 \\ (t|\kappa)=-1}}^{\ell} |\sqrt{\alpha^{n/\nu}} + \zeta_\ell^t \sqrt{\beta^{n/\nu}}| \\
&= \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\ell} |\sqrt{\alpha^{n/\nu}} - (s|\kappa)\zeta_\ell^s \sqrt{\beta^{n/\nu}}| \\
&= \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\ell} |\beta|^{n/(2\nu)} |(\gamma^{-1})^{n/(2\nu)} - (s|\kappa)\zeta_\ell^s|,
\end{aligned}$$

from which it follows that

$$\begin{aligned}
|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})| &= (|\beta|^{n/(2\nu)})^{\phi(\ell)} \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\ell} |(\gamma^{-1})^{n/(2\nu)} - (s|\kappa)\zeta_\ell^s| \\
&= (|\beta|^{n/(2\nu)})^{\phi(\ell)} \prod_{\substack{s=1 \\ \gcd(s,\ell)=1 \\ (s|\kappa)=1}}^{\ell} |(\gamma^{-1})^{n/(2\nu)} - \zeta_\ell^s| \prod_{\substack{s=1 \\ \gcd(t,\ell)=1 \\ (t|\kappa)=-1}}^{\ell} |-(\gamma^{-1})^{n/(2\nu)} - \zeta_\ell^t|.
\end{aligned}$$

By Lemma 1.1, $|\alpha| = |\beta|$, and $|\pm(\gamma^{-1})^{n/(2\nu)}| = 1$. It follows by Lemma 2.5 that

$$|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})| < (|\alpha|^{n/(2\nu)})^{\phi(\ell)} \exp(4\sqrt{\ell}(\log \ell)^2).$$

Since $\ell \leq n$, it remains to show that

$$\frac{n\phi(\ell)}{2\nu} \leq \frac{\phi(n)}{2},$$

or equivalently, since $\kappa \equiv 1 \pmod 4$, $\eta = 1$, and $\ell = \nu$, that

$$\frac{\phi(\nu)}{\nu} \leq \frac{\phi(n)}{n}.$$

Since $\nu = \prod_{p|n} p$,

$$\frac{\phi(\nu)}{\nu} = \frac{\phi(n)}{n}.$$

QED.

Lemma 2.7 *Let L and M be integers satisfying conditions (2.1), (α, β) be the associated complex Lehmer pair, and let κ and η be defined by equations (1.13) and (1.14). If $n > 4$, $n \neq 6$, $n/(\eta\kappa)$ is an odd integer, and*

$$\log|\Phi_n(\alpha, \beta)| - (1/2)\phi(n)\log|\alpha| - 4\sqrt{n}(\log n)^2 - \log n > 0,$$

then the nth term u_n of the Lehmer sequence has at least 2 primitive divisors.

Proof By Lemma 2.4, it suffices to establish that

$$\min(|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|, |\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|) > n,$$

which, by Lemma 2.2, is equivalent to

$$\frac{|\Phi_n(\alpha, \beta)|}{\max(|\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|, |\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})|)} > n. \tag{2.7}$$

By Lemma 2.6, in order to prove equation (2.7), it suffices to show that

$$\frac{|\Phi_n(\alpha, \beta)|}{|\alpha|^{\phi(n)/2}\exp(4\sqrt{n}(\log n)^2)} > n. \tag{2.8}$$

It remains to take the logarithm of both sides of inequality (2.8).

QED.

Lemma 2.8 *Let $n > 1$. Then*

$$\sum_{\substack{d|n \\ \mu(n/d)=1}} 1 = \sum_{\substack{d|n \\ \mu(n/d)=-1}} 1 = 2^{\omega(n)-1}.$$

Proof By [10, page 264],

$$\sum_{d|n} |\mu(n/d)| = 2^{\omega(n)}.$$

The result follows from the fact that

$$\sum_{\substack{d|n \\ \mu(n/d)=1}} 1 + \sum_{\substack{d|n \\ \mu(n/d)=-1}} 1 = \sum_{d|n} |\mu(n/d)|,$$

and since $\sum_{d|n} \mu(d) = 0$ for $n > 1$ that

$$\sum_{\substack{d|n \\ \mu(n/d)=1}} 1 = \sum_{\substack{d|n \\ \mu(n/d)=-1}} 1.$$

QED.

Lemma 2.9 *Let (α, β) be a complex Lehmer pair, $\gamma = \beta/\alpha$, and $n > 1$. Then*

$$\sum_{\substack{d|n \\ \mu(n/d)=-1}} \log|1 - \gamma^d| \leq 2^{\omega(n)-1} \log 2.$$

Proof Since $|\gamma| = 1$, it follows by the triangle inequality that $|1 - \gamma^d| \leq 2$. It remains to apply Lemma 2.8. QED.

Definition 2.10 *Let K be a number field, and let $\alpha \in K$. The minimal polynomial of α is*

$$f(X) = \sum_{j=0}^{d} a_j X^j = a_d \prod_{j=1}^{d} (X - \alpha^{(j)}),$$

where $f(X)$ is nonzero and of smallest degree which has α as a root, has coprime coefficients in K, and has positive leading coefficient.

Definition 2.11 *The Mahler measure of α is*

$$M(\alpha) = |a_d| \prod_{j=1}^{d} \max\{1, |\alpha^{(j)}|\}.$$

Definition 2.12 *The absolute logarithmic Weil height of α is*

$$h(\alpha) = \frac{1}{d} \log M(\alpha).$$

Lemma 2.13 *Let ϵ be a non-zero algebraic integer. Then*

$$M(\epsilon) = 1$$

if and only if

$$\epsilon \textit{ is a root of unity.}$$

Proof This is attributed to Kronecker. See Waldschmidt [35].

QED.

Lemma 2.14 *Let (α, β) be a complex Lehmer pair. Then*

$$h(\beta/\alpha) = \log|\alpha| \geq \frac{\log 2}{2}.$$

Proof By Lemma 1.1, we know that the minimal polynomial of $\gamma = \beta/\alpha$ is

$$\alpha\beta X^2 - (\alpha^2 + \beta^2)X + \alpha\beta,$$

and that

$$|\gamma| = |\gamma^{-1}| = 1.$$

If $|\alpha\beta| = 1$, then by Definition 2.11, $\mathrm{M}(\gamma) = 1$, and by Lemma 2.13 it follows that γ is a root of unity, a contradiction to the fact that (α, β) is a Lehmer pair. Hence, $|\alpha\beta| \geq 2$, so that

$$\mathrm{M}(\gamma) \geq 2,$$

It follows by Definition 2.12 that

$$\mathrm{h}(\gamma) \geq \frac{1}{2} \log 2.$$

On the other hand,

$$\begin{aligned}\mathrm{h}(\gamma) &= \frac{1}{2}\log(|\alpha\beta| \max\{1,|\gamma|\} \max\{1,|\gamma^{-1}|\}) \\ &= \frac{1}{2}\log|\alpha\beta| \\ &= \log|\beta| \\ &= \log|\alpha|,\end{aligned}$$

from which we deduce our result.

QED.

Lemma 2.15 *For any* $z = |z|\exp(i\arg z) \in \mathbb{C}$*, with* $|z| = 1$*, and* $-\pi \le \arg z \le \pi$*,*

$$|z-1| \ge \frac{2}{\pi}|\arg z|.$$

Proof Let $\arg z = \theta$. Then since $|z| = 1$, we must show that for $-\pi \le \theta \le \pi$,

$$|\exp(i\theta) - 1| - \frac{2}{\pi}|\theta| \ge 0. \tag{2.9}$$

Since $\exp(i\theta) = \cos\theta + i\sin\theta$, showing equation (2.9) is equivalent to showing that for $-\pi \le \theta \le \pi$,

$$\sqrt{2 - 2\cos\theta} - \frac{2}{\pi}|\theta| \ge 0. \tag{2.10}$$

Recall the identity

$$\cos\theta = 1 - 2(\sin(\theta/2))^2. \tag{2.11}$$

Substituting identity (2.11) into equation (2.10), and making the change of variable $\theta = 2u$, we see that we are left to show for $-\pi/2 \le u \le \pi/2$, that

$$|\sin u| \ge (2/\pi)|u|.$$

By symmetry, it suffices to show that for $u \in [0, \pi/2]$

$$\sin u \ge (2/\pi)u. \tag{2.12}$$

First note that (2.12) holds for $u = 0$ and $u = \pi/2$. For $u \in (0, \pi/2)$, let $f(u) = \sin u/u$. Since for $u \in (0, \pi/2)$,

$$u^2 f'(u) = \cos u(u - \tan u) < 0,$$

therefore for $u \in (0, \pi/2)$,

$$f(u) > f(\pi/2).$$

QED.

Lemma 2.16 *Let γ be a complex algebraic number with $|\gamma| = 1$, but not a root of unity, $\log\gamma$ the principal value of the logarithm, and $\Lambda = b_1\sqrt{-1}\pi - b_2 \log\gamma$, where b_1, b_2 are positive integers. Further, let $\lambda \in \mathbb{R}, 1.8 \leq \lambda \leq 3$,*

$$\begin{aligned} \rho &= \exp(\lambda), \\ t &= \frac{1}{6\pi\rho} - \frac{1}{48\pi\rho(1 + 2\pi\rho/(3\lambda))}, \\ k &= \left(\frac{1/3 + \sqrt{1/9 + 2\lambda t}}{\lambda}\right)^2, \\ D' &= [\mathbb{Q}(\gamma) : \mathbb{Q}]/2, \\ a &= 0.5\rho\pi + D'h(\gamma), \\ B &= \max\{527, b_1, b_2\}, \end{aligned}$$

and

$$\mathcal{H} = D'\left(\log B + \log\left(\frac{1}{\pi\rho} + \frac{1}{2a}\right) - \log\sqrt{k} + 0.886\right) + \frac{3\lambda}{2} + \frac{1}{k}\left(\frac{1}{6\rho\pi} + \frac{1}{3a}\right) + 0.023.$$

Then

$$\log|\Lambda| > -(8\pi k\rho\lambda^{-1}\mathcal{H}^2 + 0.23)a - 2\mathcal{H} - 2\log\mathcal{H} + 0.5\lambda + 2\log\lambda - (D' + 2)\log 2.$$

Proof This is [4, Theorem A.1.3].

QED.

Lemma 2.17 *Let $d \in \mathbb{N}$, $d' = \max\{527, d\}$, (α, β) be a complex Lehmer pair, and $\gamma = \beta/\alpha$. Then*

$$\log|1 - \gamma^d| > -([(24.89)(\log d')^2 + 0.23][\log|\alpha| + 9.503] + 2\log(d'\log d') + 0.572).$$

Proof By Lemma 2.15,

$$|1-\gamma^d| \geq \frac{2}{\pi}|\arg\gamma^d|. \tag{2.13}$$

Furthermore, we may assume that $0 < \arg\gamma < \pi$, replacing γ by its complex conjugate if necessary. Put $b_2 = d$ and let b_1 be the nearest even integer to $d(\arg\gamma)/\pi$. Then $0 < b_1 \leq d$, and

$$|\arg\gamma^d| = |b_1\sqrt{-1}\pi - b_2\log\gamma|.$$

By equation (2.13), it follows that

$$\log|1-\gamma^d| \geq \log|b_1\sqrt{-1}\pi - b_2\log\gamma| + \log 2 - \log\pi. \tag{2.14}$$

Let $\lambda = 1.8$ in Lemma 2.16. Then

$$\begin{aligned} \rho &= 6.04..., \\ t &= 0.008..., \\ k &= .2946..., \\ D' &= 1, \\ a &= \log|\alpha| + 9.5027..., \\ B &= \max\{527, b_1, d\}, \\ d' &= \max\{527, d\}. \end{aligned}$$

By Lemma 2.14,

$$\log|\alpha| \geq \frac{\log 2}{2}.$$

It follows that

$$\begin{aligned} \mathcal{H} &\leq \log d' - 0.604... \\ &< \log d'. \end{aligned}$$

By Lemma 2.16,

$$\log|b_1\sqrt{-1}\pi - b_2\log\gamma| \quad > \quad -(c_1(\log d')^2 + 0.23)a - 2\log d' - 2\log\log d' - c_2,$$

where $c_1 = 24.88...$, and $c_2 = 0.12....$ By (2.14) and (2.15) we deduce the result.

QED.

Lemma 2.18 *Let $n \geq 527$, (α, β) be a complex Lehmer pair, and $\gamma = \beta/\alpha$. Then*

$$\sum_{\substack{d|n \\ \mu(n/d)=1}} \log|1-\gamma^d| > -2^{\omega(n)-1}F(n,\alpha),$$

where

$$F(n,\alpha) = [(24.89)(\log n)^2 + 0.23][\log|\alpha| + 9.503] + 2\log(n\log n) + 0.572.$$

Proof This follows directly from Lemma 2.8 and Lemma 2.17, since $\log d' \leq \log n$.

QED.

Lemma 2.19 *For $n > 6915878970$,*

$$\phi(n) > (0.496866...)\frac{n}{\log\log n}. \tag{2.15}$$

Moreover, (2.15) is false for $n = 6915878970$.

Proof This follows directly from the proof of [1, Proposition 4.1]. In particular, ordering first the pairs $(p(n), n)$, where $p(n) = n/(\phi(n)\exp(\gamma)\log\log n)$, for the 6569 exceptions to

$$\phi(n) > \frac{n}{(1.07)\exp(\gamma)\log\log n},$$

by $p(n)$ in decreasing order, and then extracting the subset of these pairs ordered by n in increasing order, we obtain a finite sequence of pairs $(p(n), n)$,

$$(1.136..., 6915878970), (1.129..., 12939386460), ..., (1.0705..., 234576762718813941966540),$$

from which we deduce the result on noting

$$\frac{1}{(1.13)\exp(\gamma)} = 0.496866....$$

QED.

Lemma 2.20 *For $n \geq 3$,*

$$\omega(n) \leq (1.38401...)\frac{\log n}{\log\log n},$$

with equality when $n = 223092870$.

Proof This is [18, Théorème 11].

QED.

2.2 Proof of Theorem 2.1

Proof We already observed that it suffices to prove the theorem in case (α, β) is a complex Lehmer pair and $\alpha\beta > 0$. We recall that $\gamma = \beta/\alpha$.
By Lemma 2.1,

$$\log|\Phi_n(\alpha,\beta)| = \phi(n)\log|\alpha| - \sum_{\substack{d|n \\ \mu(n/d)=-1}} \log|1-\gamma^d| + \sum_{\substack{d|n \\ \mu(n/d)=1}} \log|1-\gamma^d|.$$

By Lemma 2.7, it suffices to show that

$$(1/2)\phi(n)\log|\alpha| - \sum_{\substack{d|n \\ \mu(n/d)=-1}} \log|1-\gamma^d| + \sum_{\substack{d|n \\ \mu(n/d)=1}} \log|1-\gamma^d| - 4\sqrt{n}(\log n)^2 - \log n > 0.$$

By Lemma 2.9, it suffices to show that

$$(1/2)\phi(n)\log|\alpha| - 2^{\omega(n)-1}\log 2 + \sum_{\substack{d|n \\ \mu(n/d)=1}} \log|1-\gamma^d| - 4\sqrt{n}(\log n)^2 - \log n > 0.$$

By Lemma 2.18, it suffices to show for $n \geq 527$, that

$$(1/2)\phi(n)\log|\alpha| - 2^{\omega(n)-1}\log 2 - 2^{\omega(n)-1}F(n,\alpha) - 4\sqrt{n}(\log n)^2 - \log n > 0, \qquad (2.16)$$

where

$$F(n,\alpha) = [(24.89)(\log n)^2 + 0.23][\log|\alpha| + 9.503] + 2\log(n\log n) + 0.572.$$

By Lemma 2.14,

$$\frac{1}{\log|\alpha|} \leq \frac{2}{\log 2}.$$

Hence,

$$\frac{F(n,\alpha)}{\log|\alpha|} \leq F_1(n),$$

where

$$\begin{aligned} & F_1(n) \\ = \; & (24.89(\log n)^2 + 0.23)\,(1 + 2(9.503)/\log 2) + (4/\log 2)\log(n\log n) + 2(0.572)/\log 2 \\ = \; & (707.37...)(\log n)^2 + (5.77...)\log(n\log n) + (8.18...). \end{aligned}$$

Multiplying equation (2.16) by $2(\log|\alpha|)^{-1}$, and applying Lemma 2.14, it suffices to show that

$$\phi(n) - 2^{\omega(n)} F_1^*(n) - (16/\log 2)\sqrt{n}(\log n)^2 - (4/\log 2)\log n > 0, \tag{2.17}$$

where

$$F_1^*(n) = 707.38(\log n)^2 + 5.78\log(n\log n) + 10.19.$$

Since $n > 10^{10}$,

$$\begin{aligned} & \sqrt{n}(\log n)^2\left(\frac{16}{\log 2} + \frac{4}{\log 2}\cdot\frac{1}{\sqrt{n}(\log n)}\right) \\ < \;& \sqrt{n}(\log n)^2\left(\frac{16}{\log 2} + \frac{4}{\log 2}\cdot\frac{1}{\sqrt{10^{10}}(10\log 10)}\right) \\ = \;& (23.083123...)\sqrt{n}(\log n)^2, \end{aligned} \tag{2.18}$$

and

$$\begin{aligned} F_1^*(n) &= (\log n)^2\left(707.38 + 5.78\frac{\log(n\log n)}{(\log n)^2} + \frac{10.19}{(\log n)^2}\right) \\ &< (\log n)^2\left(707.38 + \frac{2(5.78)}{(10\log 10)} + \frac{10.19}{(10\log 10)^2}\right) \\ &= (707.901...)(\log n)^2. \end{aligned} \tag{2.19}$$

Substituting inequalities (2.18) and (2.19) in (2.17), we see that it suffices to show that

$$\phi(n) - (707.91)2^{\omega(n)}(\log n)^2 - (23.084)\sqrt{n}(\log n)^2 > 0.$$

By Lemma 2.19, and Lemma 2.20, it suffices to show that

$$(0.49686)\frac{n}{\log\log n} - (707.91)2^{1.3841\log n/\log\log n}(\log n)^2 - (23.084)\sqrt{n}(\log n)^2 > 0.$$

Since $n > 10^{10}$,

$$\begin{aligned} (1.3841\log n/\log\log n)\log 2 &< (1.3841\log 2/\log(10\log 10))\log n \\ &= (0.305866...)\log n, \end{aligned}$$

and we see that it suffices to show that

$$(0.49686)\frac{n}{\log\log n} - (707.91)n^{0.306}(\log n)^2 - (23.084)\sqrt{n}(\log n)^2 > 0,$$

or equivalently,

$$L(n) > 0,$$

where

$$L(n) = \frac{0.49686\sqrt{n}}{(\log n)^2 \log\log n} - \frac{707.91}{n^{0.194}} - 23.084. \tag{2.20}$$

Note that

$$\begin{aligned} L(1.1 \times 10^{10}) &= -0.026..., \\ L(1.2 \times 10^{10}) &= 1.206.... \end{aligned}$$

It suffices to show that $L(n)$ is increasing for $n > 10^{10}$. Since by definition (2.20),

$$\begin{aligned} & L'(n) \\ = \; & \frac{0.49686n^{-1/2}((1/2)(\log n)^2 \log\log n - \log n(1 + 2\log\log n))}{(\log n)^4(\log\log n)^2} + \frac{707.91(0.194)}{n^{1.194}}, \\ = \; & 0.49686\left(\frac{1}{2\sqrt{n}(\log n)^2 \log\log n} - \frac{1 + 2\log\log n}{\sqrt{n}(\log n)^3(\log\log n)^2}\right) + \frac{707.91(0.194)}{n^{1.194}}, \end{aligned}$$

and for $n > 10^{10}$

$$\frac{1 + 2\log\log n}{(\log n)(\log\log n)} < 0.1007...,$$

it follows that

$$L'(n) > 0,$$

for $n > 10^{10}$.

QED.

Chapter 3

Classifying Lehmer Triples

In this chapter we extend Stewart's algorithm [30, Theorem 2] for classifying Lehmer triples with at least one primitive divisor, to an algorithm for classifying Lehmer triples with at least two primitive divisors.

3.1 Statement of Theorem 3.1 and Preliminary Lemmas

Let (α, β) be a Lehmer pair,

$$\kappa = k(\alpha\beta \max\{(\alpha-\beta)^2, (\alpha+\beta)^2\}),$$

and η be defined by (1.14).

Theorem 3.1 *There are only finitely many triples (n, α, β), where $n > 6$, $n \neq 12$, (α, β) is a Lehmer pair, and $n/(\eta\kappa)$ is an odd integer, such that $u_n(\alpha, \beta)$ has less than two primitive divisors. Furthermore, these triples may be explicitly determined.*

By Theorem 1.1, and the remark following the statement of Theorem 2.1, we see that it suffices to prove Theorem 3.1 assuming $\alpha\beta > 0$. We now state and prove the Lemmas we use to establish Theorem 3.1.

Lemma 3.1 *Let $n > 4, n \neq 6$. The nth term u_n of the Lehmer sequence has no primitive divisor if and only if*

$$|\Phi_n(\alpha,\beta)| \in \begin{cases} \{1,2,3,6\}, & \textit{if } n = 12; \\ \{1, P(n/\gcd(n,3))\}, & \textit{otherwise}; \end{cases}$$

where $\Phi_n(\alpha,\beta)$ is defined by equation (1.9), and $P(\cdot)$ is defined by Definition 1.22.

Proof This is implied by the proof of [30, Theorem 2]. See [4, Theorem 2.4].

QED.

Lemma 3.2 *Let $n > 4, n \neq 6$ be a positive integer, (α,β) be a Lehmer pair such that $\alpha\beta > 0$, and $n/(\eta\kappa)$ be an odd integer where $\kappa = k(\alpha\beta(\alpha+\beta)^2)$ and η is defined by (1.14). If the nth term $u_n = u_n(\alpha,\beta)$ of the Lehmer sequence has less than 2 primitive divisors, then for ($j = 1$ and $j = 2$) in case u_n has no primitive divisors, and for ($j = 1$ or $j = 2$) in case u_n has one primitive divisor, it follows that*

$$|\delta\Phi^{(j)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})| \in \begin{cases} \{1,2,3,6\}, & \textit{if } n = 12; \\ \{1, P(n/\gcd(n,3))\}, & \textit{otherwise}; \end{cases} \tag{3.1}$$

where

$$\delta = k((\alpha+\beta)^2)^{-(\phi(n)/4-\lfloor\phi(n)/4\rfloor)},$$

$\nu = \eta\kappa\prod_{\substack{p|n \\ p\nmid\eta\kappa}} p$, $\ell = \kappa\prod_{\substack{p|n \\ p\nmid\eta\kappa}} p$, and $N = \nu$, $\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})$ is defined by equations (1.18), (1.20) or (1.22), and $\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})$ is defined by equations (1.19), (1.21), or (1.23).

Proof By Lemma 2.2 and Lemma 2.3, it follows that

$$|\Phi_n(\alpha,\beta)| = |\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})||\delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})|\delta^{-2}, \tag{3.2}$$

where

$$\delta = k((\alpha+\beta)^2)^{-(\phi(n)/4-\lfloor\phi(n)/4\rfloor)},$$

$$\begin{aligned} \delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}) &\in \mathbb{Z}, \\ \delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}) &\in \mathbb{Z}, \end{aligned}$$

and

$$\gcd(\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}), \delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})) = 1. \tag{3.3}$$

If u_n has no primitive divisor, then by Lemma 3.1, and equation (3.2), the result follows. Suppose that u_n has exactly one primitive divisor p_1. Since by Lemma 1.24 and Lemma 1.25, the prime divisors of $|\Phi_n(\alpha, \beta)|$ coincide with the primitive divisors of u_n, except possibly for $P(n/\gcd(n, 3))$, which exactly divides $\Phi_n(\alpha, \beta)$ if at all, we see that $p_1|\Phi_n(\alpha, \beta)$. Suppose $p_1 \neq P(n/(\gcd(n, 3))$. By equations (3.2) and (3.3), we may assume without loss of generality that

$$p_1|\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}).$$

If $|\delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})| \neq 1$, let p be a prime divisor of $\delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu})$, and so of $\Phi_n(\alpha, \beta)$. By equation (3.3), $p \neq p_1$. By Lemma 1.24 and Lemma 1.25, it follows that

$$p = \begin{cases} 2 \text{ or } 3, & \text{if } n = 12; \\ P(n/\gcd(n, 3)), & \text{otherwise}; \end{cases}$$

from which we conclude (3.1).

Suppose now that $p_1 = P(n/\gcd(n, 3))$. Then $p_1|n$, from which it follows that

$$\begin{aligned} \gcd(p_1 + 1, n) &= 1, \\ \gcd(p_1 - 1, n) &= 1. \end{aligned}$$

On the other hand, since p_1 is a primitive divisor, $p_1 \nmid (\alpha^2 - \beta^2)^2$, from which it follows by Lemma 1.24 item 4 that

$$p_1|u_{p_1-1}u_{p_1+1}.$$

Since $\gcd(u_{p_1-1}, u_{p_1+1}) = u_{\gcd(p_1-1,p_1+1)} = 1$, therefore either

$$p_1|\gcd(u_{p_1-1}, u_n) = u_{\gcd(p_1-1,n)} = 1,$$

or

$$p_1|\gcd(u_{p_1+1}, u_n) = u_{\gcd(p_1+1,n)} = 1,$$

in either case, a contradiction.

QED.

Following Brent [6], we use Lemma 3.3.

Lemma 3.3 *Let* $F(x) = \prod_{s=1}^{n}(x-\xi_s) = \sum_{s=0}^{n} a_s x^{n-s}$, *where* $a_0 = 1$. *Then the coefficients* $a_s, s = 1, ..., n$ *may be computed recursively by the formulas*

$$a_s = -\frac{1}{s}\sum_{j=0}^{s-1} p_{s-j}a_j, \quad p_{s-j} = \sum_{\ell=1}^{n} \xi_\ell^{s-j}. \tag{3.4}$$

Proof See Kalman [13]. The formulas (3.4) are attributed to Newton (1707), and are commonly called Newton's identities.

QED.

Lemma 3.4 *Let* $m, n \in \mathbb{N}$. *Then*

$$\sum_{\substack{h=1\\ \gcd(h,n)=1}}^{n} \zeta_n^{hm} = \frac{\phi(n)\mu(n/\gcd(n,m))}{\phi(n/\gcd(n,m))}.$$

Proof This is [10, Theorem 272].

QED.

Lemma 3.5 *Let* $m, n \in \mathbb{N}$, m *odd. Then*

$$\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\zeta_n^j + \zeta_n^{-j})^m = \phi(n)\sum_{\ell=0}^{(m-1)/2}\left(\begin{array}{c} m \\ \ell \end{array}\right)\frac{\mu(n/\gcd(n,m-2\ell))}{\phi(n/\gcd(n,m-2\ell))}.$$

Proof We note first that by the binomial theorem and the fact that m is odd we have that

$$\begin{aligned}\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\zeta_n^j + \zeta_n^{-j})^m &= \sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor}\sum_{\ell=0}^{m}\left(\begin{array}{c} m \\ \ell \end{array}\right)\zeta_n^{j(m-\ell)}\zeta_n^{-j\ell} \\ &= \sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor}\sum_{\ell=0}^{(m-1)/2}\left(\begin{array}{c} m \\ \ell \end{array}\right)(\zeta_n^{j(m-2\ell)} + \zeta_n^{-j(m-2\ell)}) \\ &= \sum_{\ell=0}^{(m-1)/2}\left(\begin{array}{c} m \\ \ell \end{array}\right)\left(\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor}\zeta_n^{j(m-2\ell)} + \sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor}\zeta_n^{-j(m-2\ell)}\right).\end{aligned}$$

It remains to observe that

$$\begin{aligned}\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} \zeta_n^{-j(m-2\ell)} &= \sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} \zeta_n^{(n-j)(m-2\ell)}\\ &= \sum_{\substack{k=\lceil n/2\rceil\\ \gcd(k,n)=1}}^{n-1} \zeta_n^{k(m-2\ell)},\end{aligned}$$

and to apply Lemma 3.4.

QED.

Lemma 3.6 *If $m, n \in \mathbb{N}$, m even. Then*

$$\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\zeta_n^j + \zeta_n^{-j})^m = \sum_{\ell=0}^{m/2-1} \begin{pmatrix} m\\ \ell \end{pmatrix} \frac{\phi(n)\mu(n/\gcd(n, m-2\ell))}{\phi(n/\gcd(n, m-2\ell))} + \xi(n) \begin{pmatrix} m\\ m/2 \end{pmatrix},$$

where

$$\xi(n) = \begin{cases} \phi(n)/2, & \text{if } n \text{ is odd;}\\ \phi(n/2), & \text{if } n \text{ is even.}\end{cases}$$

Proof As in the proof of Lemma 3.5, since m is even, we have that

$$\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\zeta_n^j + \zeta_n^{-j})^m = \sum_{\ell=0}^{m/2-1} \begin{pmatrix} m\\ \ell \end{pmatrix} \sum_{\substack{j=1\\ \gcd(j,n)=1}}^{n-1} \zeta_n^{j(m-2\ell)} + \begin{pmatrix} m\\ m/2 \end{pmatrix} \sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} 1.$$

It remains to apply Lemma 3.4 and to note that

$$\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} 1 = \xi(n).$$

QED.

Lemma 3.7 *Let* $\chi \pmod{m}$ *be a character of conductor* f*, and let* $a = ga_0 \in \mathbb{N}$ *and* $m = gm_0 \in \mathbb{N}$*, where* $g = \gcd(a, m)$ *and* $\gcd(a_0, m_0) = 1$*. If* $f|m_0$*, then*

$$\sum_{\substack{x \pmod{m} \\ \gcd(x,m)=1}} \chi(x)\zeta_m^{ax} = \frac{\phi(m)}{\phi(m_0)}\mu(m_0/f)\chi(m_0/f)\overline{\chi}(a_0) \sum_{x \pmod{f}} \chi(x)\zeta_f^x.$$

Proof This is [11, Theorem IV, page 449].

QED.

Lemma 3.8 *Let* χ *be a quadratic character of conductor* $f \in \mathbb{N}$*,* $\mu(f) \neq 0$*. Then*

$$\sum_{x \pmod{f}} \chi(x)\zeta_f^x = \begin{cases} \sqrt{f}, & \textit{if } \chi(-1) = 1; \\ \sqrt{-f}, & \textit{if } \chi(-1) = -1; \end{cases}$$

where $\sqrt{f} > 0$*.*

Proof This is [11, Theorem XI, page 471].

QED.

Lemma 3.9 *Let* $n, m \in \mathbb{N}$*, and let* d *be an odd divisor of* n*. If* $n/\gcd(n, m) \equiv 0 \pmod{d}$ *and* $\mu(d) \neq 0$*, then*

$$\sum_{\substack{h=1 \\ \gcd(h,n)=1}}^{n} (h|d)\zeta_n^{hm} = \frac{\phi(n)\mu(\frac{n}{d\gcd(n,m)})(\frac{n}{d\gcd(n,m)}|d)(\frac{m}{\gcd(n,m)}|d)\sqrt{\epsilon d}}{\phi(n/\gcd(n, m))},$$

where

$$\epsilon = \begin{cases} 1, & \textit{if } d \equiv 1 \pmod{4}; \\ -1, & \textit{if } d \equiv -1 \pmod{4}. \end{cases}$$

Proof Let $\chi(h) = (h|d)$. Note that $\chi(h)$ is a quadratic character of conductor d, and $\overline{\chi}(h) = \chi(h)$. Let $m = gm_0$, and $n = gn_0$, where $g = \gcd(m, n)$ and $\gcd(m_0, n_0) = 1$. By Lemma 3.7,

$$\sum_{\substack{h=1 \\ \gcd(h,n)=1}}^{n} (h|d)\zeta_n^{hm} = \frac{\phi(n)}{\phi(n_0)}\mu(n_0/d)\chi(n_0/d)\overline{\chi}(m_0)\sum_{h=1}^{d}(h|d)\zeta_d^h.$$

By Lemma 3.8,

$$\sum_{h=1}^{d}(h|d)\zeta_d^h = \begin{cases} \sqrt{d}, & \text{if } (-1|d) = 1; \\ \sqrt{-d}, & \text{if } (-1|d) = -1. \end{cases}$$

It remains to note that d is odd and $(-1|d) = (-1)^{(d-1)/2}$.

QED.

Lemma 3.10 *Let n be an odd positive integer, ν be the greatest squarefree divisor of n, $d \equiv 1 \pmod 4$ be a divisor of ν, $d = d_2 d_3$, and let m be an odd positive integer. Then*

$$\begin{aligned} &\sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} \left\{\pm(i|d)\sqrt{d_3^{n/\nu}}(\zeta_\nu^i + \zeta_\nu^{-i})\right\}^m \\ = \quad & \pm d_3^{\frac{m(n/\nu)+1}{2}}\sqrt{d_2} \sum_{\substack{\ell=0 \\ \frac{\nu}{\gcd(\nu,m-2\ell)}\equiv 0 \pmod d}}^{(m-1)/2} \left(\begin{array}{c} m \\ \ell \end{array}\right) \frac{\phi(\nu)\mu(\frac{\nu}{d\gcd(\nu,m-2\ell)})(\frac{\nu}{d\gcd(\nu,m-2\ell)}|d)(\frac{m-2\ell}{\gcd(\nu,m-2\ell)}|d)}{\phi(\nu/\gcd(\nu,m-2\ell))}. \end{aligned}$$

Proof By the binomial theorem and the fact that m is odd and $(-1|d) = 1$ we have that

$$\begin{aligned} &\sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} \left\{\pm(i|d)\sqrt{d_3^{n/\nu}}(\zeta_\nu^i + \zeta_\nu^{-i})\right\}^m \\ = \quad & \pm d_3^{m(n/\nu)/2} \sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} (i|d) \sum_{\ell=0}^{m} \left(\begin{array}{c} m \\ \ell \end{array}\right) \zeta_\nu^{i(m-\ell)}\zeta_\nu^{-i\ell} \\ = \quad & \pm d_3^{m(n/\nu)/2} \sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} (i|d) \sum_{\ell=0}^{(m-1)/2} \left(\begin{array}{c} m \\ \ell \end{array}\right) (\zeta_\nu^{i(m-2\ell)} + \zeta_\nu^{-i(m-2\ell)}), \end{aligned}$$

$$\begin{aligned} &\sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} (i|d) \sum_{\ell=0}^{(m-1)/2} \left(\begin{array}{c} m \\ \ell \end{array}\right) (\zeta_\nu^{i(m-2\ell)} + \zeta_\nu^{-i(m-2\ell)}) \\ = \quad & \sum_{\ell=0}^{(m-1)/2} \left(\begin{array}{c} m \\ \ell \end{array}\right) \left(\sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} (i|d)\zeta_\nu^{i(m-2\ell)} + \sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} (i|d)\zeta_\nu^{-i(m-2\ell)} \right), \end{aligned}$$

and

$$\begin{aligned}
&\sum_{\substack{i=1\\ \gcd(i,\nu)=1}}^{\lfloor \nu/2\rfloor} (i|d)\zeta_\nu^{i(m-2\ell)} + \sum_{\substack{i=1\\ \gcd(i,\nu)=1}}^{\lfloor \nu/2\rfloor} (i|d)\zeta_\nu^{-i(m-2\ell)}\\
=\;& \sum_{\substack{i=1\\ \gcd(i,\nu)=1}}^{\lfloor \nu/2\rfloor} (i|d)\zeta_\nu^{i(m-2\ell)} + \sum_{\substack{k=\lceil \nu/2\rceil\\ \gcd(k,\nu)=1}}^{\nu-1} (k|d)\zeta_\nu^{k(m-2\ell)}.
\end{aligned}$$

It remains to apply Lemma 3.9.

QED.

Lemma 3.11 *Let n be an odd positive integer, ν be the greatest squarefree divisor of n, d be a divisor of ν, $d = d_2 d_3$, and let m be an even positive integer. Then*

$$\begin{aligned}
&\sum_{\substack{i=1\\ \gcd(i,\nu)=1}}^{\lfloor \nu/2\rfloor} \left\{\pm(i|d)\sqrt{d_3^{n/\nu}}(\zeta_\nu^i+\zeta_\nu^{-i})\right\}^m\\
=\;& d_3^{\frac{m(n/\nu)}{2}}\phi(\nu)\left(\sum_{\ell=0}^{m/2-1}\binom{m}{\ell}\frac{\mu(\nu/\gcd(\nu,m-2\ell))}{\phi(\nu/\gcd(\nu,m-2\ell))}+\frac{1}{2}\binom{m}{m/2}\right).
\end{aligned}$$

Proof This follows as in the proof of Lemma 3.6, on noting that since $\gcd(i,d)=1$ and m is even, $\{\pm(i|d)\}^m = 1$.

QED.

Lemma 3.12 *Let n be an even positive integer, ν be the greatest squarefree divisor of n, $d \equiv 3 \pmod 4$ be a divisor of ν, $d = d_2 d_3$, and let m be an odd positive integer. Then*

$$\begin{aligned}
&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor} \left\{\pm\sqrt{-d_3^{n/\nu}}(i|d)(\zeta_{\nu/2}^i-\zeta_{\nu/2}^{-i})\right\}^m = \pm(-1)^{\frac{m+1}{2}}d_3^{\frac{m(n/\nu)+1}{2}}\sqrt{d_2}\times\\
&\sum_{\substack{\ell=0\\ \frac{\nu/2}{\gcd(\nu/2,m-2\ell)}\equiv 0 \pmod d}}^{(m-1)/2}\binom{m}{\ell}\frac{(-1)^\ell\phi(\nu/2)\mu(\frac{\nu/2}{d\gcd(\nu/2,m-2\ell)})(\frac{\nu/2}{d\gcd(\nu/2,m-2\ell)}|d)(\frac{m-2\ell}{\gcd(\nu/2,m-2\ell)}|d)}{\phi((\nu/2)/\gcd(\nu/2,m-2\ell))}.
\end{aligned}$$

Proof By the binomial theorem and the fact that m is odd and $(-1|d) = -1$, we have that

$$\begin{aligned}
&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} \left\{ \pm\sqrt{-d_3^{n/\nu}}(i|d)(\zeta_{\nu/2}^{i} - \zeta_{\nu/2}^{-i}) \right\}^m \\
= \ & \pm(-1)^{\frac{m}{2}} d_3^{\frac{m(n/\nu)}{2}} \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d) \sum_{\ell=0}^{m} \left(\begin{array}{c} m \\ \ell \end{array} \right) (-1)^{\ell} \zeta_{\nu/2}^{i(m-\ell)} \zeta_{\nu/2}^{-i\ell},
\end{aligned}$$

$$\begin{aligned}
&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d) \sum_{\ell=0}^{m} \left(\begin{array}{c} m \\ \ell \end{array} \right) (-1)^{\ell} \zeta_{\nu/2}^{i(m-\ell)} \zeta_{\nu/2}^{-i\ell} \\
= \ & \sum_{\ell=0}^{(m-1)/2} \left(\begin{array}{c} m \\ \ell \end{array} \right) (-1)^{\ell} \left(\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d)\zeta_{\nu/2}^{i(m-2\ell)} + (-1)^{m-2\ell} \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d)\zeta_{\nu/2}^{-i(m-2\ell)} \right),
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d)\zeta_{\nu/2}^{i(m-2\ell)} + (-1)^{m-2\ell} \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d)\zeta_{\nu/2}^{-i(m-2\ell)} \\
= \ & \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d)\zeta_{\nu/2}^{i(m-2\ell)} + \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (-i|d)\zeta_{\nu/2}^{-i(m-2\ell)} \\
= \ & \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (i|d)\zeta_{\nu/2}^{i(m-2\ell)} + \sum_{\substack{k=\lceil \nu/4 \rceil\\ \gcd(k,\nu/2)=1}}^{\nu/2} (k|d)\zeta_{\nu/2}^{k(m-2\ell)}.
\end{aligned}$$

It remains to apply Lemma 3.9.

QED.

Lemma 3.13 *Let n be an even positive integer, ν be the greatest squarefree divisor of n, d be an odd divisor of ν, $d = d_2 d_3$, and let m be an even positive integer. Then*

$$\begin{aligned}&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor} \left\{\pm\sqrt{-d_3^{n/\nu}}(i|d)(\zeta_{\nu/2}^{i}-\zeta_{\nu/2}^{-i})\right\}^m \\ = \;& (-1)^{\frac{m}{2}} d_3^{\frac{m(n/\nu)}{2}} \phi(\nu/2)\left(\sum_{\ell=0}^{m/2-1}\left(\begin{array}{c} m\\ \ell\end{array}\right)\frac{(-1)^{\ell}\mu((\nu/2)/\gcd(\nu/2,m-2\ell))}{\phi((\nu/2)/\gcd(\nu/2,m-2\ell))}+\frac{(-1)^{m/2}}{2}\left(\begin{array}{c} m\\ m/2\end{array}\right)\right).\end{aligned}$$

Proof By the binomial theorem and the fact that m is even we have that

$$\begin{aligned}&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor} \left\{\pm\sqrt{-d_3^{n/\nu}}(i|d)(\zeta_{\nu/2}^{i}-\zeta_{\nu/2}^{-i})\right\}^m \\ = \;& (-1)^{\frac{m}{2}} d_3^{\frac{m(n/\nu)}{2}} \sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor}\sum_{\ell=0}^{m}\left(\begin{array}{c} m\\ \ell\end{array}\right)(-1)^{\ell}\zeta_{\nu/2}^{i(m-\ell)}\zeta_{\nu/2}^{-i\ell},\end{aligned}$$

and

$$\begin{aligned}&\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor}\sum_{\ell=0}^{m}\left(\begin{array}{c} m\\ \ell\end{array}\right)(-1)^{\ell}\zeta_{\nu/2}^{i(m-\ell)}\zeta_{\nu/2}^{-i\ell} \\ = \;& \sum_{\ell=0}^{m/2-1}\left(\begin{array}{c} m\\ \ell\end{array}\right)(-1)^{\ell}\left(\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor}\zeta_{\nu/2}^{i(m-2\ell)}+(-1)^{m-2\ell}\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor}\zeta_{\nu/2}^{-i(m-2\ell)}\right)+ \\ & +(-1)^{m/2}\left(\begin{array}{c} m\\ m/2\end{array}\right)\sum_{\substack{i=1\\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4\rfloor}1.\end{aligned}$$

It remains to note $(-1)^{m-2\ell}=1$ and to apply Lemma 3.4.

QED.

Lemma 3.14 *Let n be an even positive integer, ν be twice the greatest squarefree divisor of n, n/ν be an odd integer, $d \equiv 2 \pmod 4$ be a divisor of $\nu/2$, $d = d_2 d_3$, and let m be an* *odd positive integer. Then*

$$\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \left\{\pm\sqrt{d_3^{n/\nu}}(\zeta_{2\nu}^{i}+\zeta_{2\nu}^{-i})\right\}^{m} =$$

$$\pm \sum_{\substack{\ell=0\\ \frac{2\nu}{\gcd(2\nu,m-2\ell)}\equiv 0 \pmod{4d}}}^{(m-1)/2} \begin{pmatrix} m \\ \ell \end{pmatrix} \frac{d_3^{\frac{m(n/\nu)+1}{2}}\sqrt{d_2}\phi(2\nu)\mu(\frac{2\nu}{4d\gcd(2\nu,m-2\ell)})\chi(\frac{2\nu}{4d\gcd(2\nu,m-2\ell)})\chi(\frac{m-2\ell}{\gcd(2\nu,m-2\ell)})}{\phi(2\nu/\gcd(2\nu,m-2\ell))},$$

where

$$\chi(i) \;=\; (-1)^{(i-1)(i-1+d)/8}(i|d/2).$$

Proof By the binomial theorem and the fact that m is odd we deduce that

$$\begin{aligned} &\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \left\{\pm\sqrt{d_3^{n/\nu}}(\zeta_{2\nu}^{i}+\zeta_{2\nu}^{-i})\right\}^{m} \\ &= \pm d_3^{m(n/\nu)/2} \sum_{\ell=0}^{(m-1)/2} \begin{pmatrix} m \\ \ell \end{pmatrix} \left(\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \zeta_{2\nu}^{i(m-2\ell)} + \sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \zeta_{2\nu}^{-i(m-2\ell)} \right), \end{aligned}$$

$$\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \zeta_{2\nu}^{i(m-2\ell)} + \sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \zeta_{2\nu}^{-i(m-2\ell)} \;=\; \sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{2\nu} \zeta_{2\nu}^{i(m-2\ell)},$$

and

$$\begin{aligned} \sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{2\nu} \zeta_{2\nu}^{i(m-2\ell)} &= \frac{1}{2} \sum_{\substack{i=1\\ \gcd(i,2\nu)=1}}^{2\nu} (d|i)\zeta_{2\nu}^{i(m-2\ell)} \\ &= \frac{1}{2} \sum_{\substack{i=1\\ \gcd(i,2\nu)=1}}^{2\nu} (-1)^{(i-1)(i-1+d)/8}(i|d/2)\zeta_{2\nu}^{i(m-2\ell)}. \end{aligned}$$

It remains to apply Lemma 3.7 and Lemma 3.8 using the fact that $\chi(i) = (d|i)$ is a quadratic character modulo 2ν of conductor $4d$.

QED.

Lemma 3.15 *Let n be an even positive integer, ν be twice the greatest squarefree divisor of n, n/ν be an odd integer, d be a divisor of $\nu/2$, $d = d_2 d_3$, and let m be an even positive integer. Then*

$$\begin{aligned}&\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \left\{\pm\sqrt{d_3^{n/\nu}}(\zeta_{2\nu}^{i}+\zeta_{2\nu}^{-i})\right\}^m \\ = \quad & \frac{d_3^{m(n/\nu)/2}\phi(2\nu)}{2}\left(\sum_{\ell=0}^{m/2-1}\begin{pmatrix} m \\ \ell \end{pmatrix}\frac{\mu(2\nu/\gcd(2\nu,m-2\ell))}{\phi(2\nu/\gcd(2\nu,m-2\ell))}+\frac{1}{2}\begin{pmatrix} m \\ m/2 \end{pmatrix}\right)\end{aligned}$$

Proof By the binomial theorem and the fact that m is even, we note that

$$\begin{aligned}&\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{\nu} \left\{\pm\sqrt{d_3^{n/\nu}}(\zeta_{2\nu}^{i}+\zeta_{2\nu}^{-i})\right\}^m \\ = \quad & d_3^{m(n/\nu)/2}\left(\sum_{\ell=0}^{m/2-1}\begin{pmatrix} m \\ \ell \end{pmatrix}\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{2\nu}\zeta_{2\nu}^{i(m-2\ell)}+\begin{pmatrix} m \\ m/2 \end{pmatrix}\frac{\phi(2\nu)}{4}\right),\end{aligned}$$

and

$$\sum_{\substack{i=1\\ \gcd(i,2\nu)=1\\ (d|i)=1}}^{2\nu}\zeta_{2\nu}^{i(m-2\ell)} = \frac{1}{2}\sum_{\substack{i=1\\ \gcd(i,2\nu)=1}}^{2\nu}\zeta_{2\nu}^{i(m-2\ell)}.$$

It remains to apply Lemma 3.4.

QED.

Lemma 3.16 *Let $F(X, Y)$ be a binary form with integer coefficients and with at least three pairwise non-proportional linear factors in its factorisation over $\mathbb{C}$. Let m be a non-zero integer. If x and y are rational integers satisfying $F(X, Y) = m$, then*

$$\max\{|x|, |y|\} \leq C_1 |m|^{C_2},$$

for some computable numbers C_1 and C_2 depending only on F.

Proof This is [28, Theorem 5.1]. We highlight that Baker (1968) established the first such bound. Feldman (1971) and Baker (1973) independently established the stated result.

QED.

Lemma 3.17 *Let $f(x)$ be a polynomial with integer coefficients, and suppose that $f(x)$ has at least two simple roots. Further, let $b \in \mathbb{Z}$, and let $3 \leq m \in \mathbb{Z}$. If $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ satisfy $f(x) = by^m$, then*

$$\max\{|x|, |y|\} \leq C,$$

for some computable number C, depending on b, m, and f.

Proof This is [28, Theorem 6.1]. We highlight that Baker (1969) established this bound.

QED.

Lemma 3.18 *Let $f(x) = \prod_{i=1}^{m}(x - r_i)$ and $g(x) = \prod_{j=1}^{n}(x - s_j)$ be polynomials with integer coefficients, and let R denote the resultant of $f(x)$ and $g(x)$. Then there exist polynomials $a(x)$ and $b(x)$ with integer coefficients such that*

$$a(x)f(x) + b(x)g(x) = R.$$

Proof This is proved in [31, page 104–105].

QED.

Lemma 3.19 *Let $n \in \mathbb{N}, n > 2$, $L = \mathbb{Q}(\cos(2\pi/n))$, $M = \mathbb{Q}(\zeta_n)$, and let D_L and D_M denote the discriminant of L and M respectively. Then $\mathbb{Q} \subset L \subset M$, and*

$$\begin{aligned} D_M &\equiv 0 \pmod{D_L}, \\ D_M &= (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}. \end{aligned}$$

Proof Note that $\cos(2\pi/n) = (1/2)(\zeta_n + \zeta_n^{-1})$, and that L is a real subfield of M. The congruence for D_M follows from the composition theorem on discriminants [12, page 443], while the equality for D_M is proved by Hasse [12, page 523–525].

QED.

Lemma 3.20 *Let $n \in \mathbb{N}, n > 2$, $L' = \mathbb{Q}(\sin(2\pi/n))$, $M' = \mathbb{Q}(\zeta_n, \sqrt{-1})$, and let $D_{L'}$ and $D_{M'}$ denote the discriminant of L' and M' respectively. Then $\mathbb{Q} \subset L' \subset M'$, and*

$$\begin{aligned} D_{M'} &\equiv 0 \pmod{D_{L'}}, \\ D_{M'} &= -4\frac{n^{2\phi(n)}}{\prod_{p|n} p^{2\phi(n)/(p-1)}}. \end{aligned}$$

Proof Note that $\sin(2\pi/n) = (-1/2)\sqrt{-1}(\zeta_n - \zeta_n^{-1})$, and that L' is a real subfield of M'. The congruence for $D_{M'}$ follows from the composition theorem on discriminants [12, page 443]. Moreover, in the notation of Lemma 3.19, since $\mathbb{Q} \subset M \subset M'$, $[M' : M] = 2$, and $D_{M'/M} = -4$, by the composition theorem on discriminants

$$\begin{aligned} D_{M'} &= \mathrm{Norm}(D_{M'/M}) D_M^{[M':M]} \\ &= -4D_M^2, \end{aligned}$$

from which we deduce the result by the formula for D_M in Lemma 3.19.

QED.

Lemma 3.21 *Let $2 \leq c \in \mathbb{Z}$, $(\alpha+\beta)^2 = z_2^2$, and $\alpha\beta = z_3^2$, where $z_2 \in \mathbb{Z}$, $z_3 \in \mathbb{Z}$.*

$$\Phi_{3^c}(\alpha,\beta) = \prod_{\substack{i=1 \\ \gcd(i,3^c)=1}}^{\lfloor 3^c/2 \rfloor} (z_2 - (\zeta_{3^c}^i + \zeta_{3^c}^{-i})z_3) \prod_{\substack{i=1 \\ \gcd(i,3^c)=1}}^{\lfloor 3^c/2 \rfloor} (z_2 + (\zeta_{3^c}^i + \zeta_{3^c}^{-i})z_3).$$

Proof This follows directly by definition, factoring a difference of squares, and pairing $(\zeta_{3^c}^i, \zeta_{3^c}^{-i})$.

QED.

Lemma 3.22 *Let $2 \leq c \in \mathbb{Z}$, $(\alpha+\beta)^2 = d_2 z_2^2$, and $\alpha\beta = d_3 z_3^2$, where $(d_2, d_3) \in \{(3,1),(1,3)\}$, $z_2 \in \mathbb{Z}$, $z_3 \in \mathbb{Z}$.*

$$\Phi_{2\cdot 3^c}(\alpha,\beta) = \prod_{\substack{i=1 \\ \gcd(i,3^c)=1}}^{\lfloor 3^c/2 \rfloor} (\sqrt{d_2}z_2 - \sqrt{-1}(\zeta_{3^c}^i - \zeta_{3^c}^{-i})\sqrt{d_3}z_3) \prod_{\substack{i=1 \\ \gcd(i,3^c)=1}}^{\lfloor 3^c/2 \rfloor} (\sqrt{d_2}z_2 + \sqrt{-1}(\zeta_{3^c}^i - \zeta_{3^c}^{-i})\sqrt{d_3}z_3).$$

Proof This follows directly by Lemma 1.17, factoring a difference of squares, and pairing $(\zeta_{3^c}^i, \zeta_{3^c}^{-i})$.

QED.

3.2 Proof of Theorem 3.1

Proof We first note that by Theorem 2.1, we have that $n < 1.2 \times 10^{10}$. We fix

$$6 < n < 1.2 \times 10^{10}, \ \ n \neq 12.$$

It follows by Lemma 3.2 for $j \in \{1, 2\}$ that

$$\delta\Phi_{N,\kappa}^{(j)}(\alpha^{n/\nu}, \beta^{n/\nu}) \in \{\pm 1, \pm P(n/\gcd(n, 3))\}, \tag{3.5}$$

where

$$\begin{array}{rcl} \delta & = & k((\alpha+\beta)^2)^{-(\phi(n)/4 - \lfloor \phi(n)/4 \rfloor)}, \\ \kappa & = & k(\alpha\beta(\alpha+\beta)^2), \\ \nu & = & \eta\kappa \displaystyle\prod_{p \mid n, p \nmid \eta\kappa} p, \\ \ell & = & \kappa \displaystyle\prod_{p \mid n, p \nmid \eta\kappa} p, \\ N & = & \nu. \end{array}$$

Note that since κ is squarefree, we have three cases to consider, namely

$$\kappa \equiv 1, 2, 3 \pmod 4.$$

In case $\kappa \equiv 1 \pmod 4$, note that $\Phi^{(1)}_{N,\kappa}(\cdot)$ and $\Phi^{(2)}_{N,\kappa}(\cdot)$ in equations (3.5) are defined by equations (1.18) and (1.19), with

$$\begin{aligned} \nu &= \kappa \prod_{p|n, p\nmid\kappa} p, \\ \ell &= \nu, \\ N &= \nu, \\ x &= \alpha^{n/\nu}, \\ y &= \beta^{n/\nu}. \end{aligned}$$

Note further that

$$(-s|\kappa) = (-1|\kappa)(s|\kappa),$$

and since $\kappa \equiv 1 \pmod 4$ that

$$(-1|\kappa) = (-1)^{(\kappa-1)/2} = 1.$$

Hence, s and $-s$ both appear in the product indexed by s. We may group the ℓth roots of unity into $\phi(\ell)/2$ pairs $(\zeta_\ell^s, \zeta_\ell^{-s})$ with respect to the index s, and similarly, $\phi(\ell)/2$ pairs $(\zeta_\ell^t, \zeta_\ell^{-t})$ with respect to the index t. Then equations (1.18) and (1.19) become

$$\Phi^{(1)}_{\nu,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\lfloor \ell/2 \rfloor} (x_1 - (s|\kappa)(\zeta_\ell^s + \zeta_\ell^{-s})x_2), \tag{3.6}$$

and

$$\Phi^{(2)}_{\nu,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\lfloor \ell/2 \rfloor} (x_1 + (s|\kappa)(\zeta_\ell^s + \zeta_\ell^{-s})x_2), \tag{3.7}$$

where each of (3.6) and (3.7) is a binary form of degree $\phi(\ell)/2$ in x_1 and x_2,

$$x_1 = \alpha^{n/\nu} + \beta^{n/\nu}, \tag{3.8}$$

and

$$x_2 = (\alpha\beta)^{n/(2\nu)}. \tag{3.9}$$

Since n/ν is an odd integer, we note the identity

$$\frac{\alpha^{n/\nu}+\beta^{n/\nu}}{\alpha+\beta}=((\alpha+\beta)^2)^{(n/\nu-1)/2}-\sum_{k=1}^{(n/\nu-1)/2}\left(\begin{array}{c} n/\nu \\ k \end{array}\right)(\alpha\beta)^k\frac{\alpha^{n/\nu-2k}+\beta^{n/\nu-2k}}{\alpha+\beta}. \quad (3.10)$$

We observe that since (α,β) is a Lehmer pair, then by induction and the identity (3.10), it follows that

$$\frac{\alpha^{n/\nu}+\beta^{n/\nu}}{\alpha+\beta}=z_1,$$

for some integer z_1. Furthermore, since

$$(\alpha+\beta)^2=k((\alpha+\beta)^2)z_2^2,$$

for some integer z_2, we write

$$x_1=z_1z_2\sqrt{k((\alpha+\beta)^2)}.$$

On the other hand, since

$$\alpha\beta=k(\alpha\beta)z_3^2$$

for some integer z_3, we write

$$x_2=z_3^{n/\nu}\sqrt{(k(\alpha\beta))^{n/\nu}}.$$

We define

$$\begin{aligned}
&f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(x,y)\\
=&\prod_{\substack{s=1\\ \gcd(s,\nu)=1}}^{\lfloor\nu/2\rfloor}(\sqrt{k((\alpha+\beta)^2)}x-(s|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_\nu^s+\zeta_\nu^{-s})y),\\
&f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(x,y)\\
=&\prod_{\substack{s=1\\ \gcd(s,\nu)=1}}^{\lfloor\nu/2\rfloor}(\sqrt{k((\alpha+\beta)^2)}x-(-1)(s|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_\nu^s+\zeta_\nu^{-s})y).
\end{aligned}$$

Then equations (3.6) and (3.7) become

$$\begin{aligned} & f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ = & \sum_{s=0}^{\phi(\nu)/2} a_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(\nu)/2-s}(z_1z_2)^{\phi(\nu)/2-s}(z_3^{n/\nu})^s, \end{aligned} \tag{3.11}$$

and

$$\begin{aligned} & f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ = & \sum_{s=0}^{\phi(\nu)/2} b_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(\nu)/2-s}(z_1z_2)^{\phi(\nu)/2-s}(z_3^{n/\nu})^s. \end{aligned} \tag{3.12}$$

Because of Lemma 3.3, we may write the a_s's and the b_s's in the form

$$\begin{aligned} a_0 &= 1, \\ a_s &= -\frac{1}{s}\sum_{j=0}^{s-1} p^{(a)}_{s-j}a_j, s = 1, \ldots, \phi(\nu)/2, \\ p^{(a)}_{s-j} &= \sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} \left\{(i|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_\nu^i + \zeta_\nu^{-i})\right\}^{s-j}, s-j = 1, \ldots, \phi(\nu)/2, \end{aligned}$$

and

$$\begin{aligned} b_0 &= 1, \\ b_s &= -\frac{1}{s}\sum_{j=0}^{s-1} p^{(b)}_{s-j}b_j, s = 1, \ldots, \phi(\nu)/2, \\ p^{(b)}_{s-j} &= \sum_{\substack{i=1 \\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} \left\{-(i|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_\nu^i + \zeta_\nu^{-i})\right\}^{s-j}, s-j = 1, \ldots, \phi(\nu)/2. \end{aligned}$$

We note that there are only finitely many equations (3.11) and (3.12), since n/κ is an odd integer, and $\kappa = k((\alpha+\beta)^2)k(\alpha\beta)$ since $\gcd(L, M) = 1$. For the application of the next two Lemmas, we let

$$\begin{aligned} d &= \kappa, \\ d_2 &= k((\alpha+\beta)^2), \\ d_3 &= k(\alpha\beta). \end{aligned} \tag{3.13}$$

It follows by Lemma 3.10 in case $s-j\equiv 1 \pmod 2$, that

$$\begin{aligned} p_{s-j}^{(a)} &= \left((k(\alpha\beta))^{\frac{(s-j)(n/\nu)+1}{2}} \sum_{\substack{\ell=0 \\ \frac{\nu}{\gcd(\nu,s-j-2\ell)}\equiv 0 \pmod{\kappa}}}^{(s-j-1)/2} \begin{pmatrix} s-j \\ \ell \end{pmatrix} \times \right. \\ & \left. \frac{\phi(\nu)\mu(\frac{\nu}{\kappa\gcd(\nu,s-j-2\ell)})(\frac{\nu}{\kappa\gcd(\nu,s-j-2\ell)}|\kappa)(\frac{s-j-2\ell}{\gcd(\nu,s-j-2\ell)}|\kappa)}{\phi(\nu/\gcd(\nu,s-j-2\ell))} \right) \sqrt{k((\alpha+\beta)^2)}, \end{aligned}$$

and that $p_{s-j}^{(b)}=-p_{s-j}^{(a)}$. Since n/ν is odd and $s-j$ is odd, we see that $(s-j)(n/\nu)+1$ is even. Furthermore, we note that

$$\phi(\nu)\equiv 0 \pmod{\phi(\nu/\gcd(\nu,s-j-2\ell))}.$$

Hence, in case $s-j\equiv 1 \pmod 4$, both $p_{s-j}^{(a)}$ and $p_{s-j}^{(b)}$ have the form $u_1\sqrt{k((\alpha+\beta)^2)}$ for some integer u_1. Similarly, by Lemma 3.11 in case $s-j\equiv 0 \pmod 2$,

$$\begin{aligned} p_{s-j}^{(a)} &= (k(\alpha\beta))^{\frac{(s-j)(n/\nu)}{2}}\phi(\nu)\times \\ & \left(\sum_{\ell=0}^{(s-j)/2-1} \begin{pmatrix} s-j \\ \ell \end{pmatrix} \frac{\mu(\nu/\gcd(\nu,s-j-2\ell))}{\phi(\nu/\gcd(\nu,s-j-2\ell))} + \frac{1}{2}\begin{pmatrix} s-j \\ (s-j)/2 \end{pmatrix} \right), \end{aligned}$$

and $p_{s-j}^{(a)}=p_{s-j}^{(b)}$. Since $s-j$ is even, we see that $(s-j)(n/\nu)$ is even. Furthermore, we note that $\phi(\nu)$ is even. Hence, in case $s-j\equiv 0 \pmod 2$, both $p_{s-j}^{(a)}$ and $p_{s-j}^{(b)}$ have the form u_2 for some integer u_2. It follows from the above Newton's identitites that a_s and b_s have the form

$$\begin{array}{ll} q_1\sqrt{k((\alpha+\beta)^2)}, & \text{if} \quad s\equiv 1 \pmod 2; \\ q_2, & \text{otherwise}; \end{array}$$

for some rational numbers q_1 and q_2. On the other hand, a_s and b_s are elementary symmetric functions of

$$\pm(s|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_\nu^s+\zeta_\nu^{-s}),$$

and thus are algebraic integers. It follows that a_s and b_s have the form

$$\begin{array}{ll} u_3\sqrt{k((\alpha+\beta)^2)}, & \text{if} \quad s\equiv 1 \pmod 2; \\ u_4, & \text{otherwise}; \end{array} \tag{3.14}$$

where u_3 and u_4 are integers.

Plainly, in case $\kappa = 1$, the coefficients of the equations (3.11) and (3.12) defining $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$, for $j = 1$ and $j = 2$, are integers. In case $\kappa > 1$, it follows from $\kappa \equiv 1 \pmod 4$, $\phi(\kappa) \equiv 0 \pmod 4$, and

$$\phi(\nu) = \phi(\kappa)\phi(\prod_{\substack{p|n \\ p\nmid\kappa}} p),$$

that $\phi(\nu)/2$ is an even integer. We observe (3.14), and the fact that $\phi(\nu)/2$ is an even integer, imply that the coefficients of the equations (3.11) and (3.12) are integers.
By Lemma 3.16, for $j = 1$ and $j = 2$, we deduce that each of the equations

$$f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) = m, \tag{3.15}$$

where $f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$ is defined by (3.11) and $f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$ is defined by (3.12), and

$$m \in \{\pm 1, \pm P(n/\gcd(n,3))\}$$

is a non-zero integer, has only finitely many solutions in integers $(z_1z_2, z_3^{n/\nu})$, whenever each of $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$, $j = 1, 2$ have at least three distinct roots.
Plainly, on recalling the identities

$$\begin{aligned} \zeta_\nu^s + \zeta_\nu^{-s} &= 2\cos(2\pi s/\nu), \qquad (3.16)\\ -\cos(2\pi s/\nu) &= \cos(\pi - 2\pi s/\nu), \end{aligned}$$

it is easily seen that each of $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$, $j = 1, 2$ has at least three distinct roots whenever

$$\phi(\nu)/2 \geq 3,$$

which is true provided we assume

$$\prod_{p|n}(p-1) \geq 6, \tag{3.17}$$

since

$$\prod_{p|n}(p-1) = \phi(\prod_{p|n} p) = \phi(\nu).$$

In case $\kappa \equiv 3 \pmod 4$, note that $\Phi^{(1)}_{N,\kappa}(\cdot)$ and $\Phi^{(2)}_{N,\kappa}(\cdot)$ in equations (3.5) are defined by equations (1.20) and (1.21), with

$$\begin{aligned} \nu &= 2\kappa \prod_{p|n, p\nmid 2\kappa} p, \\ \ell &= \nu/2, \\ N &= \nu, \\ x &= \alpha^{n/\nu}, \\ y &= \beta^{n/\nu}. \end{aligned}$$

Note further that

$$(-s|\kappa) = (-1|\kappa)(s|\kappa),$$

and since $\kappa \equiv 3 \pmod 4$ that

$$(-1|\kappa) = (-1)^{(\kappa-1)/2} = -1.$$

Hence, for every s appearing in the product indexed by s, there is a $-s$ appearing in the product indexed by t. We may group the ℓth roots of unity into $\phi(\ell)/2$ pairs $(\zeta_\ell^s, \zeta_\ell^{-s})$ with $(s|\kappa) = 1$ and $(-s|\kappa) = -1$. Then equations (1.20) and (1.21) become

$$\Phi^{(1)}_{\nu,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\lfloor \ell/2 \rfloor} (x_1 - (s|\kappa)\sqrt{-1}(\zeta_\ell^s - \zeta_\ell^{-s})x_2), \tag{3.18}$$

and

$$\Phi^{(2)}_{\nu,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\lfloor \ell/2 \rfloor} (x_1 + (s|\kappa)\sqrt{-1}(\zeta_\ell^s - \zeta_\ell^{-s})x_2), \tag{3.19}$$

where each of (3.18) and (3.19) is a binary form of degree $\phi(\ell)/2$ in x_1 and x_2, and x_1 and x_2 are defined by equations (3.8) and (3.9) respectively, with respect to the definition of ν

in this case. We define

$$\begin{aligned} & f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(x,y) \\ = & \prod_{\substack{s=1 \\ \gcd(s,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (\sqrt{k((\alpha+\beta)^2)}x - (s|\kappa)\sqrt{-(k(\alpha\beta))^{n/\nu}}(\zeta^s_{\nu/2} - \zeta^{-s}_{\nu/2})y), \\ & f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(x,y) \\ = & \prod_{\substack{s=1 \\ \gcd(s,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} (\sqrt{k((\alpha+\beta)^2)}x - (-1)(s|\kappa)\sqrt{-(k(\alpha\beta))^{n/\nu}}(\zeta^s_{\nu/2} - \zeta^{-s}_{\nu/2})y). \end{aligned}$$

Then equations (3.18) and (3.19) become

$$\begin{aligned} & f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ = & \sum_{s=0}^{\phi(\nu)/2} \lambda_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(\nu)/2-s}(z_1z_2)^{\phi(\nu)/2-s}(z_3^{n/\nu})^s, \end{aligned} \tag{3.20}$$

and

$$\begin{aligned} & f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ = & \sum_{s=0}^{\phi(\nu)/2} \rho_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(\nu)/2-s}(z_1z_2)^{\phi(\nu)/2-s}(z_3^{n/\nu})^s. \end{aligned} \tag{3.21}$$

Because of Lemma 3.3, we may write the λ_s's and the ρ_s's in the form

$$\begin{aligned} \lambda_0 &= 1, \\ \lambda_s &= -\frac{1}{s}\sum_{j=0}^{s-1} p^{(\lambda)}_{s-j}\lambda_j, s = 1, \ldots, \phi(\nu)/2, \\ p^{(\lambda)}_{s-j} &= \sum_{\substack{i=1 \\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} \left\{\sqrt{-(k(\alpha\beta))^{n/\nu}}(i|\kappa)(\zeta^i_{\nu/2} - \zeta^{-i}_{\nu/2})\right\}^{s-j}, s-j = 1, \ldots, \phi(\nu)/2, \end{aligned}$$

and

$$\begin{aligned}
\rho_0 &= 1, \\
\rho_s &= -\frac{1}{s}\sum_{j=0}^{s-1} p_{s-j}^{(\rho)}\rho_j, s = 1, \ldots, \phi(\nu)/2, \\
p_{s-j}^{(\rho)} &= \sum_{\substack{i=1 \\ \gcd(i,\nu/2)=1}}^{\lfloor \nu/4 \rfloor} \left\{-\sqrt{-(k(\alpha\beta))^{n/\nu}}(i|\kappa)(\zeta_{\nu/2}^{i} - \zeta_{\nu/2}^{-i})\right\}^{s-j}, s-j = 1, \ldots, \phi(\nu)/2.
\end{aligned}$$

We note that there are only finitely many equations (3.20) and (3.21), since $n/(2\kappa)$ is an odd integer, and $\kappa = k((\alpha+\beta)^2)k(\alpha\beta)$. With respect to equations (3.13), it follows by Lemma 3.12 in case $s - j \equiv 1 \pmod 2$, that $p_{s-j}^{(\lambda)}$ and $p_{s-j}^{(\rho)}$ have the form $u_5\sqrt{k((\alpha+\beta)^2)}$ for some integer u_5, and by Lemma 3.13 in case $s-j \equiv 0 \pmod 2$, that $p_{s-j}^{(\lambda)}$ and $p_{s-j}^{(\rho)}$ have the form u_6 for some integer u_6. On the other hand, λ_s and ρ_s are elementary symmetric functions of

$$\pm(s|\kappa)\sqrt{-(k(\alpha\beta))^{n/\nu}}(\zeta_{\nu/2}^{s} - \zeta_{\nu/2}^{-s}),$$

and thus are algebraic integers. It follows from the above Newton's identities that λ_s and ρ_s have the form

$$\begin{array}{lll} u_7\sqrt{k((\alpha+\beta)^2)}, & \text{if} & s \equiv 1 \pmod 2; \\ u_8, & \text{otherwise}; & \end{array} \tag{3.22}$$

where u_7 and u_8 are integers.

Since $\kappa > 1$, we consider the cases $\omega(\kappa) = 1$ and $\omega(\kappa) > 1$. Plainly, in case that $\omega(\kappa) = 1$, since $\phi(\kappa) \equiv 2 \pmod 4$, it follows that $\phi(\nu)/2$ is an odd integer, and that

$$\delta = \frac{1}{\sqrt{k((\alpha+\beta)^2)}}.$$

On the other hand, in case that $\omega(\kappa) > 1$, since $\phi(\kappa) \equiv 0 \pmod 4$, it follows that $\phi(\nu)/2$ is an even integer, and that

$$\delta = 1.$$

We observe (3.22), and the above discussion on the parity of $\phi(\nu)/2$ and the value of δ, together imply that the coefficients defining

$$\delta f_{n,k((\alpha+\beta)^2),k(\alpha\beta)}^{(j)}(z_1z_2, z_3^{n/\nu}),$$

for $j = 1$ and $j = 2$, where the coefficients of $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$ are given by the equations (3.20) and (3.21), are integers.
By Lemma 3.16, for $j = 1$ and $j = 2$, we deduce that each of the equations

$$\delta f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) = m, \tag{3.23}$$

where $f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$ is defined by (3.20) and $f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$ is defined by (3.21), and

$$m \in \{\pm 1, \pm P(n/\gcd(n,3))\}$$

is a non-zero integer, has only finitely many solutions in integers $(z_1z_2, z_3^{n/\nu})$, whenever each of $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu})$, $j = 1, 2$ have at least three distinct roots.
Plainly, on recalling the identities

$$\begin{aligned} \zeta^s_{\nu/2} - \zeta^{-s}_{\nu/2} &= 2\sqrt{-1}\sin(4\pi s/\nu)), \\ -\sin(4\pi s/\nu) &= \sin(-4\pi s/\nu), \end{aligned} \tag{3.24}$$

it is easily seen that each of $f^{(j)}_{n,\kappa}(z_1z_2, z_3^{n/\nu})$, $j = 1, 2$ have at least three distinct roots under the assumption (3.17), since in this case $\phi(\nu)/2 \geq 3$.

Finally, in case $\kappa \equiv 2 \pmod 4$, note that $\Phi^{(1)}_{N,\kappa}(\cdot)$ and $\Phi^{(2)}_{N,\kappa}(\cdot)$ in equations (3.5) are defined by equations (1.22) and (1.23), with

$$\begin{aligned} \nu &= 2\kappa \prod_{p|n, p\nmid 2\kappa} p, \\ \ell &= \nu/2, \\ N &= \nu, \\ x &= \alpha^{n/\nu}, \\ y &= \beta^{n/\nu}. \end{aligned}$$

Note further that by definition

$$(\kappa| - s) = (\kappa|s) = 1.$$

Hence, s and $-s$ both appear in the product indexed by s. We may group the 4ℓth roots of unity into $\phi(4\ell)/4$ pairs $(\zeta^s_{4\ell}, \zeta^{-s}_{4\ell})$ with $(\kappa|s) = 1$ and $(\kappa| - s) = 1$. Then equations (1.22) and (1.23) become

$$\Phi^{(1)}_{\nu,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}) = \prod_{\substack{s=1\\ \gcd(s,4\ell)=1\\ (\kappa|s)=1}}^{2\ell} (x_1 - (\zeta_{4\ell}^{s} + \zeta_{4\ell}^{-s})x_2), \tag{3.25}$$

and

$$\Phi^{(2)}_{\nu,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}) = \prod_{\substack{s=1\\ \gcd(s,4\ell)=1\\ (\kappa|s)=1}}^{2\ell} (x_1 + (\zeta_{4\ell}^{s} + \zeta_{4\ell}^{-s})x_2), \tag{3.26}$$

where each of (3.25) and (3.26) is a binary form of degree $\phi(4\ell)/4$ in x_1 and x_2, and x_1 and x_2 are defined by equations (3.8) and (3.9) respectively, with respect to the definition of ν in this case. We define

$$\begin{aligned} & f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(x,y) \\ = & \prod_{\substack{s=1\\ \gcd(s,2\nu)=1\\ (\kappa|s)=1}}^{\nu} (\sqrt{k((\alpha+\beta)^2)}x - \sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_{2\nu}^{s} + \zeta_{2\nu}^{-s})y), \\ & f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(x,y) \\ = & \prod_{\substack{s=1\\ \gcd(s,2\nu)=1\\ (\kappa|s)=1}}^{\nu} (\sqrt{k((\alpha+\beta)^2)}x - (-1)\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_{2\nu}^{s} + \zeta_{2\nu}^{-s})y). \end{aligned}$$

Then equations (3.25) and (3.26) become

$$\begin{aligned} & f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ = & \sum_{s=0}^{\phi(2\nu)/4} \gamma_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(2\nu)/4-s}(z_1z_2)^{\phi(2\nu)/4-s}(z_3^{n/\nu})^s, \end{aligned} \tag{3.27}$$

and

$$\begin{aligned} & f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ = & \sum_{s=0}^{\phi(2\nu)/4} \delta_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(2\nu)/4-s}(z_1z_2)^{\phi(2\nu)/4-s}(z_3^{n/\nu})^s. \end{aligned} \tag{3.28}$$

Because of Lemma 3.3, we may write the γ_s's and the δ_s's in the form

$$\begin{aligned}
\gamma_0 &= 1, \\
\gamma_s &= -\frac{1}{s}\sum_{j=0}^{s-1} p_{s-j}^{(\gamma)}\gamma_j, s = 1, \ldots, \phi(2\nu)/4, \\
p_{s-j}^{(\gamma)} &= \sum_{\substack{i=1 \\ \gcd(i,2\nu)=1 \\ (\kappa|i)=1}}^{\nu} \left\{\sqrt{(k(\alpha\beta))^{n/\nu}}(\zeta_{2\nu}^{i}+\zeta_{2\nu}^{-i})\right\}^{s-j}, s-j = 1, \ldots, \phi(2\nu)/4,
\end{aligned}$$

and

$$\begin{aligned}
\delta_0 &= 1, \\
\delta_s &= -\frac{1}{s}\sum_{j=0}^{s-1} p_{s-j}^{(\delta)}\delta_j, s = 1, \ldots, \phi(2\nu)/4, \\
p_{s-j}^{(\delta)} &= \sum_{\substack{i=1 \\ \gcd(i,2\nu)=1 \\ (\kappa|i)=1}}^{\nu} \left\{-\sqrt{(k(\alpha\beta)^{n/\nu}}(\zeta_{2\nu}^{i}+\zeta_{2\nu}^{-i})\right\}^{s-j}, s-j = 1, \ldots, \phi(2\nu)/4.
\end{aligned}$$

We note that there are only finitely many equations (3.27) and (3.28), since $n/(2\kappa)$ is an odd integer, and $\kappa = k((\alpha+\beta)^2)k(\alpha\beta)$. With respect to equations (3.13), It follows by Lemma 3.14 in case $s-j \equiv 1 \pmod 2$, that $p_{s-j}^{(\gamma)}$ and $p_{s-j}^{(\delta)}$ have the form $u_9\sqrt{k((\alpha+\beta)^2)}$ for some integer u_9, and by Lemma 3.15 in case $s-j \equiv 0 \pmod 2$, that $p_{s-j}^{(\gamma)}$ and $p_{s-j}^{(\delta)}$ have the form u_{10} for some integer u_{10}. On the other hand, γ_s and δ_s are elementary symmetric functions of

$$\pm\sqrt{(k(\alpha\beta)^{n/\nu}}(\zeta_{2\nu}^{s}+\zeta_{2\nu}^{-s}),$$

and thus are algebraic integers. It follows from the above Newton's identities that γ_s and δ_s have the form

$$\begin{array}{ll}
u_{11}\sqrt{k((\alpha+\beta)^2)}, \quad \text{if} \quad s \equiv 1 \pmod 2; \\
u_{12}, \quad \text{otherwise};
\end{array} \tag{3.29}$$

where u_{11} and u_{12} are integers.

Since $n \neq 4$ and $\kappa \equiv 2 \pmod 4$, $\kappa = 2\kappa'$, where $\kappa' > 1$, $\gcd(2, \kappa') = 1$, and $\phi(\kappa') \equiv 0 \pmod 2$. It follows that $\phi(2\nu)/4$ is an even integer, which together with (3.29), implies that the coefficients of the equations (3.27) and (3.28) are integers.

By Lemma 3.16, for $j = 1$ and $j = 2$, we deduce that each of the equations (3.15), where $f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1 z_2, z_3^{n/\nu})$ is defined by (3.27) and $f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1 z_2, z_3^{n/\nu})$ is defined by (3.28), has only finitely many solutions in integers $(z_1 z_2, z_3^{n/\nu})$, whenever each of $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1 z_2, z_3^{n/\nu})$, $j = 1, 2$ have at least three distinct roots.

Plainly, on noting the identity

$$\zeta_{2\nu}^{s} + \zeta_{2\nu}^{-s} = 2\cos(\pi s/\nu),$$

it is easily seen that each of $f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1 z_2, z_3^{n/\nu})$, $j = 1, 2$ has at least three distinct roots whenever

$$\phi(2\nu)/4 > 3,$$

which holds provided we assume that

$$\prod_{\substack{2<p|n \\ 4|n}} (p-1) \geq 4, \tag{3.30}$$

since for $\nu = 4\nu'$, $\gcd(2, \nu') = 1$,

$$\phi(2\nu)/4 = \phi(8\nu')/4 = \phi(\nu'),$$

and by (3.30)

$$\phi(\nu') \geq 4.$$

In summary, in any case $\kappa \equiv 1, 2, 3 \pmod 4$, we have shown that there are only finitely many triples

$$(n, L, M) = (n, \kappa((\alpha+\beta)^2) z_2^2, \kappa(\alpha\beta) z_3^2),$$

under the assumptions (3.17) and (3.30), which completes the argument. We now consider the remaining cases.

Suppose that $\prod_{\substack{p|n \\ 4\nmid n}}(p-1) = 4$. Let $n = 5^c$ and $n/\nu = 5^{c-1}$, $c \geq 2$. It suffices to show that the equations

$$u_2(z_1 z_2)^2 + u_3(z_1 z_2) z_3^{n/\nu} + u_4(z_3^{n/\nu})^2 = m_1, \tag{3.31}$$

have finitely many solutions in integers z_1z_2, z_3, where $m_1 \in \{\pm 1, \pm 5\}$, and

$(k((\alpha{+}\beta)^2), k(\alpha\beta), u_2, u_3, u_4) \in \{(1,1,1,\pm 1,-1),(5,1,5,\mp 5,1),(1,5,1,\mp 5^{(n/\nu+1)/2}, 5^{n/\nu})\}$.

Moreover, if $\prod_{\substack{2<p|n \\ 4|n}}(p-1) = 2$, let $n = 4 \cdot 3^c$ and $n/\nu = 3^{c-1}$, where $c \geq 2$. It suffices to show that the equations

$$u_5(z_1z_2)^2 + u_6(z_1z_2)z_3^{n/\nu} + u_7(z_3^{n/\nu})^2 = m_2 \tag{3.32}$$

have finitely many solutions in integers z_1z_2, z_3, where $m_2 \in \{\pm 1, \pm 3\}$, and

$$\begin{aligned}&(k((\alpha+\beta)^2), k(\alpha\beta), u_5, u_6, u_7) \in \\ &\{(2,1,2,\mp 2,-1),(1,2,1,\mp 2^{(n/\nu+1)/2}, -2^{n/\nu}),(6,1,6,\mp 6,1), \\ &(3,2,3,\mp 2^{(n/\nu+1)/2}\cdot 3, 2^{n/\nu}),(2,3,2,\mp 2\cdot 3^{(n/\nu+1)/2}, 3^{n/\nu}),(1,6,1,\mp 6^{(n/\nu+1)/2}, 6^{n/\nu})\}.\end{aligned}$$

The finiteness result in either case $n = 5^c$ or $n = 4 \cdot 3^c$ follows by Lemma 3.17, on recalling equations (3.31) and (3.32), and noting that the equations (3.31) are solvable in integers (z_1z_2, z_3) for a given integer z_3 provided

$$(u_3^2 - 4u_4)z_3^{2n/\nu} = w_1^2 - 4m_1, \tag{3.33}$$

for some integer w_1, while the equations (3.32) are solvable in integers (z_1z_2, z_3) for a given integer z_3 provided

$$(u_6^2 - 4u_7)z_3^{2n/\nu} = w_2^2 - 4m_2, \tag{3.34}$$

for some integer w_2.

On the other hand, we consider the case that $\prod_{\substack{p|n \\ 4\nmid n}}(p-1) = 2$. Let $n = 3^c$, where $c \geq 2$. By Lemma 3.21, we have a factorisation

$$\Phi_{3^c}(\alpha,\beta) = f_{3^c}^{(1)}(z_2,z_3)f_{3^c}^{(2)}(z_2,z_3). \tag{3.35}$$

It is easily seen that $f_{3^c}^{(j)}(z_2,z_3) \in \mathbb{Z}$ for $j = 1$ and $j = 2$ by Lemma 3.3, Lemma 3.5, and Lemma 3.6. By Lemma 3.18, any common divisor of $f_{3^c}^{(1)}(z_2,z_3)$ and $f_{3^c}^{(2)}(z_2,z_3)$ divides the resultant of $f_{3^c}^{(1)}(z_2,z_3)$ and $f_{3^c}^{(2)}(z_2,z_3)$, and hence the discriminant of $\mathbb{Q}(\zeta_{3^c} + \zeta_{3^c}^{-1})$.

By Lemma 3.19, the discriminant of $\mathbb{Q}(\zeta_{3^c}+\zeta_{3^c}^{-1})$ divides the discriminant of $\mathbb{Q}(\zeta_{3^c})$, and by the formula for the discriminant of $\mathbb{Q}(\zeta_{3^c})$ in Lemma 3.19, we deduce that the greatest common divisor of $f_{3^c}^{(1)}(z_2,z_3)$ and $f_{3^c}^{(2)}(z_2,z_3)$ divides $3\alpha\beta$. Since $\gcd(u_{3^c}(\alpha,\beta),\alpha\beta)=1$ and $3^c \nmid (3\pm 1)$, it follows that

$$\gcd(f_{3^c}^{(1)}(z_2,z_3), f_{3^c}^{(2)}(z_2,z_3)) = 1.$$

By an argument similar to the proof of Lemma 3.2, we deduce for $j=1$ and $j=2$ that

$$f_{3^c}^{(j)}(z_2,z_3) = m, \tag{3.36}$$

where $m \in \{\pm 1, \pm 3\}$. It remains to note that each $f_{3^c}^{(j)}(z_2,z_3)$ has at least three distinct roots on recalling the identities (3.16), since $3^{c-1} \geq 3$. Hence Lemma 3.16 implies the finiteness of the solutions (z_2,z_3) of equations (3.36). Moreover, the case $n = 2\cdot 3^c$, where $c \geq 2$, follows similarly, but with Lemma 3.22, the argument underlying Lemma 3.12 and Lemma 3.13, by Lemma 3.20, by the identites (3.24), and with respect to the implied integer Thue equations

$$\delta f_{2\cdot 3^c}^{(j)}(z_2,z_3) = m. \tag{3.37}$$

QED.

Chapter 4

Determining the Exceptional Lehmer Triples

In this chapter, we determine the triples (n, α, β) from Theorem 3.1, up to equivalence, explicitly for

$$6 < n \leq 30, n \neq 12,$$

by solving the implicated Thue equations (3.15) and (3.23), (3.36) and (3.37), and by solving the Thue equations corresponding to the superelliptic equations (3.33) and (3.34). Furthermore, we search for more exceptions among the small solutions of the aforementioned Thue equations, for

$$30 < n \leq 500.$$

More precisely, we let

$$\begin{aligned} d_2 &= k((\alpha+\beta)^2), \\ d_3 &= k(\alpha\beta), \\ L &= d_2 z_2^2, \\ M &= d_3 z_3^2. \end{aligned}$$

For the Thue equations (3.15) and (3.23), we code and execute Lemmas 3.10, 3.11, 3.12, 3.13, 3.14, and 3.15 in MAPLE in order to generate the coefficient vectors of the implicated binary forms. In practice, we do not solve the superelliptic equations (3.33) and (3.34), but rather, we rewrite the equations (3.31) and (3.32), using the identity

$$\begin{aligned} f(1, d_2, d_3, z_2, z_3) &= 1, \\ f(n/\nu, d_2, d_3, z_2, z_3) &= d_2^{(n/\nu-1)/2} z_2^{n/\nu-1} - \sum_{k=1}^{(n/\nu-1)/2} \binom{n/\nu}{k} (d_3 z_3^2)^k f(n/\nu - 2k, d_2, d_3, z_2, z_3), \end{aligned} \tag{4.1}$$

where

$$\nu = \eta\kappa \prod_{\substack{p \mid n \\ p \nmid \eta\kappa}} p,$$

as equations in only the variables z_2 and z_3, and thereby we recover binary forms, with nonzero discriminant. Similarly, we recover the coefficient vectors of the binary forms implied by the Thue equations (3.36) and (3.37) by appealing to the identity (4.1), and the equation

$$f(3^c, d_2, d_3, z_2, z_3) z_2 + u_1 z_3^{3^c} = m,$$

where $m \in \{\pm 1, \pm 3\}$, and in case $n = 3^c$, $c \geq 2$,

$$(d_2, d_3, u_1) \in \{(1, 1, \pm 1)\},$$

while in case $n = 2 \cdot 3^c$, $c \geq 2$,

$$(d_2, d_3, u_1) \in \{(3, 1, 1, \pm 1), (1, 3, \pm 3^{(3^c+1)/2})\}.$$

In each case $n = 3^c$, $n = 2 \cdot 3^c$, $n = 5^c$, or $n = 4 \cdot 3^c$, $c \geq 2$, solving the implicated Thue equations gives us finitely many 4 tuples (d_2, d_3, z_2, z_3), from which we compute finitely many candidate triples (n, L, M). For these candidates, we use the methods of the first chapter in order to determine the triples (n, α, β) such that u_n has less than two primitive divisors. On the other hand, for the Thue equations (3.15) and (3.23), we consider two cases. In case $n/\nu = 1$, we observe by identity (3.10) that $z_1 = 1$, and we recover the finitely many triples (n, L, M) directly from the solutions of the Thue equations as described above. On the other hand, in case $n/\nu > 1$, we consider $n/\nu = 3, 5, 7, \ldots$ in order. In each case, we run over all divisors of $z_1 z_2$ in order to form all finite possibilities $(d_2, d_3, z_1, z_2, z_3^{n/\nu})$.

For each of these 5 tuples $(d_2, d_3, z_1, z_2, z_3^{n/\nu})$, we compute L and M, and retain those pairs (L, M) which satisfy the identity (3.10) as candidates. For example,

$$L - 3M = z_1,$$

in case

$$n/\nu = 3.$$

We then recover the exceptions by the methods of the first chapter. Finally, we note that we have already determined all of the exceptional triples (n, α, β), up to equivalence, implied by Theorem 3.1, in case $\alpha\beta < 0$. The triples (n, α, β), up to equivalence, such that $\alpha\beta < 0$, are tabulated in Table 1.2. Plainly, in case $\alpha\beta < 0$, $L - 4M > 0$, and (α, β) is a real Lehmer pair.

4.1 Statement of Theorem 4.1

Theorem 4.1 *Let L and M be integers satisfying the conditions $L > 0$, $M \neq 0$, $L-4M \neq 0$, $\gcd(L, M) = 1$, and $(L, M) \notin \{(1, 1), (2, 1), (3, 1)\}$, (α, β) be the associated Lehmer pair, and let κ and η be defined by (1.13) and (1.14). If $6 < n \leq 30$, $n \neq 12$, $n/(\eta\kappa)$ is an odd integer, and the triple (n, α, β) is not equivalent to a triple (n, α, β) from Table 4.1, or Table 4.2, then $u_n(\alpha, \beta)$ has at least two primitive divisors.*

4.2 Proof of Theorem 4.1

Before proving Theorem 4.1, we note first that finding all of the integer solutions of the Thue equation $F(X, Y) = m$ in practice, where $F(X, Y)$ is a binary form with integer coefficients, and with at least three pairwise non-proportional linear factors in its factorisation over $\mathbb{C}$, and m is a non-zero integer, can be achieved, subject to computational limitations, by using the computer algebra system KASH [8]. In particular, using the KASH function *ThueSolve*, which is an implementation of the Baker-Bilu-Hanrot [3] algorithm.

We use the KASH function *ThueSolve* in order to establish Theorem 4.1.

(n, α, β)	(n, L, M)	p
$*7, (1/2) + (1/2)\sqrt{-15}, (1/2) - (1/2)\sqrt{-15}$	$7, 1, 4$	13
$*7, (1/2) + (1/2)\sqrt{-35}, (1/2) - (1/2)\sqrt{-35}$	$7, 1, 9$	41
$*7, (3/2) + (1/2)\sqrt{-7}, (3/2) - (1/2)\sqrt{-7}$	$7, 9, 4$	13
$*7, 2 + \sqrt{-77}, 2 - \sqrt{-77}$	$7, 16, 81$	167
$*7, (5/2) + (1/2)\sqrt{-39}, (5/2) - (1/2)\sqrt{-39}$	$7, 25, 16$	71
$7, (1/2)\sqrt{3} + (1/2)\sqrt{7}, (1/2)\sqrt{3} - (1/2)\sqrt{7}$	$7, 3, -1$	13
$*9, (1/2) + (1/2)\sqrt{-15}, (1/2) - (1/2)\sqrt{-15}$	$9, 1, 4$	19
$*9, (1/2) + (1/2)\sqrt{-35}, (1/2) - (1/2)\sqrt{-35}$	$9, 1, 9$	53
$*9, (3/2) + (1/2)\sqrt{-7}, (3/2) - (1/2)\sqrt{-7}$	$9, 9, 4$	17
$*10$, $(1/2) + (1/2)\sqrt{5}$, $(1/2) - (1/2)\sqrt{5}$	$10, 1, -1$	11
10 , $(1/2)\sqrt{5} + (3/2)$, $(1/2)\sqrt{5} - (3/2)$	$10, 5, -1$	11
$*13, (3/2) + (1/2)\sqrt{-7}, (3/2) - (1/2)\sqrt{-7}$	$13, 9, 4$	181
$13, (1/2)\sqrt{13} + (1/2)\sqrt{-3}, (1/2)\sqrt{13} - (1/2)\sqrt{-3}$	$13, 13, 4$	4211
$*13, (7/2) + (1/2)\sqrt{-3}, (7/2) - (1/2)\sqrt{-3}$	$13, 49, 13$	235871
$14, (1/2)\sqrt{7} + (1/2)\sqrt{3}, (1/2)\sqrt{7} - (1/2)\sqrt{3}$	$14, 7, 1$	13
$14, (1/2)\sqrt{7} + (3/2)\sqrt{-1}, (1/2)\sqrt{7} - (3/2)\sqrt{-1}$	$14, 7, 4$	13
$14, (1/2)\sqrt{7} + (1/2)\sqrt{-29}, (1/2)\sqrt{7} - (1/2)\sqrt{-29}$	$14, 7, 9$	13
$*14, 2 + \sqrt{-3}, 2 - \sqrt{-3}$	$14, 16, 7$	127
$*14, (5/2) + (1/2)\sqrt{-3}, (5/2) - (1/2)\sqrt{-3}$	$14, 25, 7$	251
$14, \sqrt{7} + \sqrt{-2}, \sqrt{7} - \sqrt{-2}$	$14, 28, 9$	113
$14, (3/2)\sqrt{7} + (1/2)\sqrt{-37}, (3/2)\sqrt{7} - (1/2)\sqrt{-37}$	$14, 63, 25$	379
$14, (13/2)\sqrt{7} + (1/2)\sqrt{-753}, (13/2)\sqrt{7} - (1/2)\sqrt{-753}$	$14, 1183, 484$	30757
$15, (1/2)\sqrt{5} + (1/2), (1/2)\sqrt{5} - (1/2)$	$15, 5, 1$	31
$*15, (3/2) + (1/2)\sqrt{-7}, (3/2) - (1/2)\sqrt{-7}$	$15, 9, 4$	89
$*15, (3/2) + (1/2)\sqrt{-11}, (3/2) - (1/2)\sqrt{-11}$	$15, 9, 5$	31
$*15, 2 + \sqrt{-1}, 2 - \sqrt{-1}$	$15, 16, 5$	241
$*15, 2 + \sqrt{-5}, 2 - \sqrt{-5}$	$15, 16, 9$	479
$15, (7/2)\sqrt{5} + (1/2)\sqrt{-11}, (7/2)\sqrt{5} - (1/2)\sqrt{-11}$	$15, 245, 64$	65521

Table 4.1: A table of all exceptional Lehmer triples (n, α, β) (up to equivalence) and associate triples (n, L, M), such that $L > 0$, $M \neq 0$, $L - 4M \neq 0$, $\gcd(L, M) = 1$, $(L, M) \neq (1, 1)$, $(2, 1)$, or $(3, 1)$, $6 < n < 18$, $n \neq 12$, $n/(\eta\kappa)$ is an odd integer, and $u_n(\alpha, \beta)$ has less than two primitive divisors, together with their primitive divisor p. Note that the star $*$ indicates the Lehmer triples correspond to Lucas triples.

(n,α,β)	(n,L,M)	p
$*18,(1/2)+(1/2)\sqrt{-11},(1/2)-(1/2)\sqrt{-11}$	$18,1,3$	17
$18,(1/2)\sqrt{3}+(1/2)\sqrt{-13},(1/2)\sqrt{3}-(1/2)\sqrt{-13}$	$18,3,4$	17
$*18,1+\sqrt{-2},1-\sqrt{-2}$	$18,4,3$	19
$18,\sqrt{3}+\sqrt{-22},\sqrt{3}-\sqrt{-22}$	$18,12,25$	251
$18,(3/2)\sqrt{3}+(1/2)\sqrt{-37},(3/2)\sqrt{3}-(1/2)\sqrt{-37}$	$18,27,16$	127
$*20,(1/2)+(1/2)\sqrt{-7},(1/2)-(1/2)\sqrt{-7}$	$20,1,2$	19
$*20,(1/2)+(1/2)\sqrt{-31},(1/2)-(1/2)\sqrt{-31}$	$20,1,8$	179
$*20,(1/2)+(1/2)\sqrt{-39},(1/2)-(1/2)\sqrt{-39}$	$20,1,10$	179
$20,(1/2)\sqrt{5}+(1/2)\sqrt{-3},(1/2)\sqrt{5}-(1/2)\sqrt{-3}$	$20,5,2$	61
$20,\sqrt{2}+\sqrt{-7},\sqrt{2}-\sqrt{-7}$	$20,8,9$	461
$*20,2,1$	$20,9,2$	41
$20,(5/2)\sqrt{5}+(1/2)\sqrt{-3},(5/2)\sqrt{5}-(1/2)\sqrt{-3}$	$20,125,32$	37201
$*20,2,-1$	$20,1,-2$	41
$21,(1/2)\sqrt{7}+(1/2)\sqrt{-5},(1/2)\sqrt{7}-(1/2)\sqrt{-5}$	$21,7,3$	461
$22,(1/2)\sqrt{11}+(1/2)\sqrt{-5},(1/2)\sqrt{11}-(1/2)\sqrt{-5}$	$22,11,4$	109
$*28,(1/2)+(1/2)\sqrt{-7},(1/2)-(1/2)\sqrt{-7}$	$28,1,2$	29
$28,\sqrt{2}+\sqrt{-5},\sqrt{2}-\sqrt{-5}$	$28,8,7$	11311
$28,2\sqrt{2}+\sqrt{-1},2\sqrt{2}-\sqrt{-1}$	$28,32,9$	4423
$*30,(1/2)+(1/2)\sqrt{-11},(1/2)-(1/2)\sqrt{-11}$	$30,1,3$	29
$30,(1/2)\sqrt{3}+(1/2)\sqrt{-13},(1/2)\sqrt{3}-(1/2)\sqrt{-13}$	$30,3,4$	61
$30,(1/2)\sqrt{3}+(1/2)\sqrt{-17},(1/2)\sqrt{3}-(1/2)\sqrt{-17}$	$30,3,5$	89
$30,(1/2)\sqrt{3}+(1/2)\sqrt{-61},(1/2)\sqrt{3}-(1/2)\sqrt{-61}$	$30,3,16$	691
$*30,1+\sqrt{-2},1-\sqrt{-2}$	$30,4,3$	29
$30,(1/2)\sqrt{5}+(1/2)\sqrt{-7},(1/2)\sqrt{5}-(1/2)\sqrt{-7}$	$30,5,3$	151
$30,\sqrt{3}+\sqrt{-2},\sqrt{3}-\sqrt{-2}$	$30,12,5$	719
$*30,(1/2)+(1/2)\sqrt{5},(1/2)-(1/2)\sqrt{5}$	$30,1,-1$	31

Table 4.2: A table of all exceptional Lehmer triples (n,α,β) (up to equivalence) and associate triples (n,L,M), such that $L>0$, $M\neq 0$, $L-4M\neq 0$, $\gcd(L,M)=1$, $(L,M)\neq(1,1)$, $(2,1)$, or $(3,1)$, $18\leq n\leq 30$, $n/(\eta\kappa)$ is an odd integer, and $u_n(\alpha,\beta)$ has less than two primitive divisors, together with their primitive divisor p. Note that the star $*$ indicates the Lehmer triples correspond to Lucas triples.

Proof We may assume $\kappa > 0$. Note that since $6 < n \leq 30$, $n \neq 12$, and $n/(\eta\kappa)$ is an odd integer,

$$n \in \{7, 9, 11, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 25, 27, 28, 29, 30\}.$$

We generate the coefficient vectors of the implicated binary forms as described at the beginning of this chapter, using MAPLE. The coefficient vectors, together with the triple (n, d_2, d_3), and the discriminant of the implicated binary forms in case $n \in \{9, 18, 25, 27\}$, are tabulated in Tables 4.3 and 4.4. We solve the implicated Thue equations using the KASH [8] function *ThueSolve*. We determine the exceptional triples (n, α, β) such that u_n has one primitive divisor as described at the beginning of this chapter. We tabulate these triples, up to equivalence, in Table 4.1, or Table 4.2, together with those we found in case $\kappa < 0$, and tabulated in Table 1.2.

QED.

4.3 Searching for Exceptional Lehmer Triples

In this section we go beyond the range $6 < n \leq 30$, $n \neq 12$, in order to determine whether or not there are other exceptional Lehmer triples outside of those already found and tabulated in Table 1.2, and Table 4.1. We have determined that there are other exceptional Lehmer triples outside of those we already found. More precisely, we compute the coefficients of the implicated binary forms $F(X, Y)$ in the range $30 < n \leq 500$, as described at the beginning of this chapter, and search for small solutions. For each $|y| \leq 100$, and $m \in \{\pm 1, \pm P(n/\gcd(n, 3))\}$, we form $P(X) = F(X, y) - m$, and use the MAPLE function *factors* in order to factor $P(X)$ over the integers. Our findings are tabulated in Table 4.5.

(n, d_2, d_3)	*Coefficient Vectors of Binary Forms, Discriminant (if applicable)*
7, 1, 1	$[1, 1, -2, -1], [1, -1, -2, 1]$
9, 1, 1	$[1, 0, -3, 1], [1, 0, -3, -1]$, 3^4
11, 1, 1	$[1, 1, -4, -3, 3, 1], [1, -1, -4, 3, 3, -1]$
13, 1, 1	$[1, 1, -5, -4, 6, 3, -1], [1, -1, -5, 4, 6, -3, -1]$
13, 13, 1	$[2197, -2197, 169, 338, -52, -13, 1], [2197, 2197, 169, -338, -52, 13, 1]$
13, 1, 13	$[1, -13, 13, 338, -676, -2197, 2197], [1, 13, 13, -338, -676, 2197, 2197]$
14, 7, 1	$[7, 7, 0, -1], [7, -7, 0, 1]$
14, 1, 7	$[1, 7, 0, -49], [1, -7, 0, 49]$
15, 1, 1	$[1, -1, -4, 4, 1], [1, 1, -4, -4, 1]$
15, 5, 1	$[25, -25, -10, 10, 1], [25, 25, -10, -10, 1]$
15, 1, 5	$[1, -5, -10, 50, 25], [1, 5, -10, -50, 25]$
17, 1, 1	$[1, 1, -7, -6, 15, 10, -10, -4, 1], [1, -1, -7, 6, 15, -10, -10, 4, 1]$
17, 17, 1	$[83521, -83521, 4913, 19652, -6647, 0, 272, -34, 1]$,
	$[83521, 83521, 4913, -19652, -6647, 0, 272, 34, 1]$
17, 1, 17	$[1, -17, 17, 1156, -6647, 0, 78608, -167042, 83521]$,
	$[1, 17, 17, -1156, -6647, 0, 78608, 167042, 83521]$
18, 3, 1	$[3, 0, -3, 1], [3, 0, -3, -1]$, 3^4
18, 1, 3	$[1, 0, -9, 9], [1, 0, -9, -9]$, 3^6
19, 1, 1	$[1, 1, -8, -7, 21, 15, -20, -10, 5, 1], [1, -1, -8, 7, 21, -15, -20, 10, 5, -1]$
20, 2, 1	$[4, -4, -6, 6, -1], [4, 4, -6, -6, -1]$
20, 1, 2	$[1, -2, -6, 12, -4], [1, 2, -6, -12, -4]$
20, 10, 1	$[100, -100, 10, 10, -1], [100, 100, 10, -10, -1]$
20, 5, 2	$[25, -50, 10, 20, -4], [25, 50, 10, -20, -4]$
20, 2, 5	$[4, -20, 10, 50, -25], [4, 20, 10, -50, -25]$
20, 1, 10	$[1, -10, 10, 100, -100], [1, 10, 10, -100, -100]$
21, 1, 1	$[1, -1, -6, 6, 8, -8, 1], [1, 1, -6, -6, 8, 8, 1]$
21, 21, 1	$[9261, -9261, 1764, 882, -378, 42, -1], [9261, 9261, 1764, -882, -378, -42, -1]$
21, 7, 3	$[343, -1029, 588, 882, -1134, 378, -27], [343, 1029, 588, -882, -1134, -378, -27]$
21, 3, 7	$[27, -189, 252, 882, -2646, 2058, -343], [27, 189, 252, -882, -2646, -2058, -343]$
21, 1, 21	$[1, -21, 84, 882, -7938, 18522, -9261], [1, 21, 84, -882, -7938, -18522, -9261]$
22, 11, 1	$[121, 121, 0, -33, -11, -1], [121, -121, 0, 33, -11, 1]$
22, 1, 11	$[1, 11, 0, -363, -1331, -1331], [1, -11, 0, 363, -1331, 1331]$
23, 1, 1	$[1, 1, -10, -9, 36, 28, -56, -35, 35, 15, -6, -1], [1, -1, -10, 9, 36, -28, -56, 35, 35, -15, -6, 1]$

Table 4.3: A Table of coefficient vectors of the implicated binary forms for $6 < n \leq 23$, $n \neq 12$.

(n, d_2, d_3)	*Coefficient Vectors of Binary Forms, Discriminant (if applicable)*
25, 1, 1	$[1, 0, -10, 0, 35, 1, -50, -5, 25, 5, -1], [1, 0, -10, 0, 35, -1, -50, 5, 25, -5, -1]$, 5^{17}
25, 1, 5	$[1, 0, -50, 0, 875, 125, -6250, -3125, 15625, 15625, 3125]$, $[1, 0, -50, 0, 875, -125, -6250, 3125, 15625, -15625, 3125]$, 5^{57}
25, 5, 1	$[3125, 0, -6250, 0, 4375, -125, -1250, 125, 125, -25, 1]$, $[3125, 0, -6250, 0, 4375, 125, -1250, -125, 125, 25, 1]$, 5^{57}
27, 1, 1	$[1, 0, -9, 0, 27, 0, -30, 0, 9, 1], [1, 0, -9, 0, 27, 0, -30, 0, 9, -1]$, 3^{22}
28, 2, 1	$[8, 8, -20, -20, 8, 8, 1], [8, -8, -20, 20, 8, -8, 1]$
28, 1, 2	$[1, 2, -10, -20, 16, 32, 8], [1, -2, -10, 20, 16, -32, 8]$
28, 14, 1	$[2744, -2744, 196, 588, -224, 28, -1], [2744, 2744, 196, -588, -224, -28, -1]$
28, 7, 2	$[343, -686, 98, 588, -448, 112, -8], [343, 686, 98, -588, -448, -112, -8]$
28, 2, 7	$[8, -56, 28, 588, -1568, 1372, -343], [8, 56, 28, -588, -1568, -1372, -343]$
28, 1 ,14	$[1, -14, 14, 588, -3136, 5488, -2744], [1, 14, 14, -588, -3136, -5488, -2744]$
29, 1, 1	$[1, 1, -13, -12, 66, 55, -165, -120, 210, 126, -126, -56, 28, 7, -1]$, $[1, -1, -13, 12, 66, -55, -165, 120, 210, -126, -126, 56, 28, -7, -1]$
29, 29, 1	$[17249876309, -17249876309, 594823321, 4758586568, -1435780430, -307667235, 200160523, -14145620, -7804480, 1658452, -37004, -20184, 2262, -87, 1]$, $[17249876309, 17249876309, 594823321, -4758586568, -1435780430, 307667235, 200160523, 14145620, -7804480, -1658452, -37004, 20184, 2262, 87, 1]$
29, 1, 29	$[1, -29, 29, 6728, -58870, -365835, 6902087, -14145620, -226329920, 1394758132, -902490556, -14275759704, 46396219038, -51749628927, 17249876309]$, $[1, 29, 29, -6728, -58870, 365835, 6902087, 14145620, -226329920, -1394758132, -902490556, 14275759704, 46396219038, 51749628927, 17249876309]$
30, 3, 1	$[9, 9, -6, -6, -1], [9, -9, -6, 6, -1]$
30, 1, 3	$[1, 3, -6, -18, -9], [1, -3, -6, 18, -9]$
30, 15, 1	$[225, 225, 60, 0, -1], [225, -225, 60, 0, -1]$
30, 5, 3	$[25, 75, 60, 0, -9], [25, -75, 60, 0, -9]$
30, 3, 5	$[9, 45, 60, 0, -25], [9, -45, 60, 0, -25]$
30, 1, 15	$[1, 15, 60, 0, -225], [1, -15, 60, 0, -225]$

Table 4.4: A Table of coefficient vectors of the implicated binary forms for $23 < n \leq 30$.

n, α, β	n, L, M	p
$*36, (1/2) + (1/2)\sqrt{-7}, (1/2) - (1/2)\sqrt{-7}$	$36, 1, 2$	37
$36, (1/2)\sqrt{2} + (1/2)\sqrt{-10}, (1/2)\sqrt{2} - (1/2)\sqrt{-10}$	$36, 2, 3$	251
$36, (1/2)\sqrt{3} + (1/2)\sqrt{-5}, (1/2)\sqrt{3} - (1/2)\sqrt{-5}$	$36, 3, 2$	71
$36, \sqrt{2} + \sqrt{-1}, \sqrt{2} - \sqrt{-1}$	$36, 8, 3$	71
$*42, (1/2) + (1/2)\sqrt{-11}, (1/2) - (1/2)\sqrt{-11}$	$42, 1, 3$	41
$*42, 1 + \sqrt{-2}, 1 - \sqrt{-2}$	$42, 4, 3$	167
$*44, (1/2) + (1/2)\sqrt{-7}, (1/2) - (1/2)\sqrt{-7}$	$44, 1, 2$	131
$*60, (1/2) + (1/2)\sqrt{-7}, (1/2) - (1/2)\sqrt{-7}$	$60, 1, 2$	59
$60, (1/2)\sqrt{3} + (1/2)\sqrt{-5}, (1/2)\sqrt{3} - (1/2)\sqrt{-5}$	$60, 3, 2$	59
$60, (1/2)\sqrt{6} + (1/2)\sqrt{-14}, (1/2)\sqrt{6} - (1/2)\sqrt{-14}$	$60, 6, 5$	20639
$60, \sqrt{2} + \sqrt{-1}, \sqrt{2} - \sqrt{-1}$	$60, 8, 3$	2399
$60, \sqrt{2} + \sqrt{-3}, \sqrt{2} - \sqrt{-3}$	$60, 8, 5$	19681
$84, (1/2)\sqrt{3} + (1/2)\sqrt{-5}, (1/2)\sqrt{3} - (1/2)\sqrt{-5}$	$84, 3, 2$	1259

Table 4.5: A table of exceptional Lehmer triples (n, α, β) (up to equivalence) and associate triples (n, L, M) we found, such that $L > 0$, $M > 0$, $L - 4M \neq 0$, $\gcd(L, M) = 1$, $(L, M) \neq (1, 1)$, $(2, 1)$, or $(3, 1)$, $30 < n \leq 500$, $n/(\eta\kappa)$ is an odd integer, $u_n(\alpha, \beta)$ has less than two primitive divisors, and $|y| \leq 100$, together with their primitive divisor p. Note that the star $*$ indicates the Lehmer triples correspond to Lucas triples. Furthermore, note that these may not be all of the exceptional Lehmer triples in the range $30 < n \leq 500$, because we have yet to consider $|y| > 100$ in the range $30 < n \leq 500$.

Chapter 5

Classifying Lucas Triples

One might expect that the conditions $n > 6$, $n \neq 12$ in Theorem 3.1 may be improved when (α, β) is a Lucas pair, by analogy with Stewart's work [30, Theorem 2]. However, we expect that the conditions $n > 6$, $n \neq 12$ in Theorem 3.1 cannot be improved when (α, β) is a Lucas pair. In this chapter, we show in Theorem 5.1 that the conditions $n > 6$, $n \neq 12$ in Theorem 3.1, cannot be improved, and so are best possible, when (α, β) is a Lucas pair, under the assumption of two plausible conjectures.

5.1 Statement of Theorem 5.1 and Preliminary Conjectures

Let (α, β) be a Lucas pair, κ be defined by (1.13), and η be defined by (1.14).

Theorem 5.1 *There are infinitely many triples (n, α, β), where $n = 1$, (α, β) is a Lucas pair, and $n/(\eta\kappa)$ is an odd integer, such that $u_n(\alpha, \beta)$ has no primitive divisor. There are infinitely many triples (n, α, β), where $n \in \{3, 4, 6\}$, (α, β) is a Lucas pair, and $n/(\eta\kappa)$ is an odd integer, such that $u_n(\alpha, \beta)$ has one primitive divisor. If Conjecture 5.1 is true, then there are infinitely many triples (n, α, β), where $n = 5$, (α, β) is a complex Lucas pair, and $n/(\eta\kappa)$ is an odd integer, such that $u_n(\alpha, \beta)$ has one primitive divisor. If Conjecture 5.2 is true, then there are infinitely many triples (n, α, β), where $n = 12$, (α, β) is a complex Lucas pair, and $n/(\eta\kappa)$ is an odd integer, such that $u_n(\alpha, \beta)$ has one primitive divisor.*

Conjecture 5.1 *There are infinitely many prime numbers $p > 5$ such that*

$$\frac{1}{5}\left((1+\sqrt{5})\left(\frac{3+\sqrt{5}}{2}\right)^{2p}+(1-\sqrt{5})\left(\frac{3-\sqrt{5}}{2}\right)^{2p}+3\right)$$

is a prime number.

Conjecture 5.2 *There are infinitely many prime numbers $p > 5$ such that*

$$\frac{1}{3}\Big((1+\sqrt{3})(2+\sqrt{3})^{2p}+(1-\sqrt{3})(2-\sqrt{3})^{2p}+1\Big)$$

is a prime number.

Remark on Conjecture 5.1 and 5.2

We begin by observing that

$$\begin{aligned}
&\frac{1}{5}\left((1+\sqrt{5})\left(\frac{3+\sqrt{5}}{2}\right)^{2(809)}+(1-\sqrt{5})\left(\frac{3-\sqrt{5}}{2}\right)^{2(809)}+3\right)\\
= \quad & 12446621431030381415405301862363257781013596833501\\
& 92083343017891789193185773851514016621312897928267\\
& 48875624007132315418452099171324145310587700583341\\
& 64545325821460602474844901671257624222416610754405\\
& 32790160536095482324378838916768365657749775725754\\
& 10383441223406262901555610839260349827342419744709\\
& 00124616310478930921966463394055605713932564528271\\
& 29542629743623587531707484784078168595199682159158\\
& 59020513259295888907779445192916824749853188087217\\
& 78219733695472410512649922278306845179704832367710\\
& 32169875883990334212399550067220467475640093047177\\
& 94099792141880086556500425521887888378356216636237\\
& 54286768790367215254474044835996101347608965036844\\
& 8024830826515990428303369 59,
\end{aligned}$$

a rational prime number as determined by the MAPLE function *isprime*. The truth of Conjecture 5.1 is suggested by considerations of probability. The inequality [20, Corollary 1]

$$\#\{p \leq x\} > \frac{x}{\log x}, \qquad x \geq 17,$$

implies the probability that a number $m \geq 17$ is prime is at least $1/\log m$. Therefore, the total expectation of the number of primes $q(p)$ of the form given by Conjecture 5.1, assuming that there are no special reasons why a number $q(n)$ of the form given by Conjecture 5.1 should be likely to be a prime number, which is a reasonable assumption since $q(809)$ is probably[1] a prime number, is at least

$$\sum_{p=7}^{\infty} \frac{1}{\log q(p)} > \frac{1}{8} \sum_{p=7}^{\infty} \frac{1}{p}, \tag{5.1}$$

and $\sum_p 1/p$ diverges [10, Theorem 19]. We observe that inequality (5.1) holds since

$$\begin{array}{rcl} 5q(p) - 3 & < & 4^{2p+1} - \dfrac{1}{2^{2p}} \\ q(p) & < & 4^{2p+2} \\ \log q(p) & < & 8p. \end{array}$$

Similarly, the truth of Conjecture 5.2 is suggested by considerations of probability. We may assume that there are no special reasons why a number $r(n)$ of the form given by Conjecture 5.2 should be likely to be a prime number because $r(n)$ is a prime number for

$$n \in \{1, 4, 6, 16, 204, 246, 304, 357, 556, 2106, 2374, 2556, 2572, 2734, 6016\},$$

as determined by the MAPLE function *isprime*.

5.2 Proof of Theorem 5.1

Proof

[1] One may "prove" $q(809)$ to be a prime number by using the freely available elliptic curve primality proving (ECPP) software by F. Morain [17].

In case $n = 1$, we observe that since $u_1 = 1$, the result follows from the fact that $n/(\eta\kappa)$ is an odd integer implies $\kappa = 1$, and $L > 0$ and $M > 0$ may be chosen to be distinct squares infinitely often.

Let $L = d_2 z_2^2$, and $M = d_3 z_3^2$, where $d_2 \in \mathbb{N}$, $d_3 \in \mathbb{N}$, $z_2 \in \mathbb{N}$, and $z_3 \in \mathbb{N}$.

In case $n = 3$, since $n/(\eta\kappa)$ is an odd integer implies $d_2 = d_3 = 1$, we deduce that

$$u_3 = (z_2 - z_3)(z_2 + z_3).$$

There are infinitely many coprime solutions to the equations

$$\begin{aligned} z_2 - z_3 &= 1, \\ z_2 + z_3 &= p, \end{aligned}$$

given by $z_2 = t + 1$, $z_3 = t$, $t \in \mathbb{N}$, where p is a prime number, since there are infinitely many odd prime numbers. Since $p = L - M$, $p \nmid L(L - 4M)u_1 u_2$.

In case $n = 4$, since $n/(\eta\kappa)$ is an odd integer and (α, β) a Lucas pair implies $(d_2, d_3) = (1, 2)$, we deduce that

$$u_4 = (z_2 - 2z_3)(z_2 + 2z_3).$$

There are infinitely many coprime solutions to the equations

$$\begin{aligned} z_2 - 2z_3 &= 1, \\ z_2 + 2z_3 &= p, \end{aligned}$$

given by $z_2 = 2t + 1$, $z_3 = t$, $t \in \mathbb{N}$, where p is a prime number, since there are infinitely many prime numbers congruent to $1 \pmod 4$. Since $\gcd(u_1 u_2 u_3, u_4) = 1$, and $p = L - 2M$, $p \nmid L(L - 4M)u_1 u_2 u_3$.

In case $n = 6$, since $n/(\eta\kappa)$ is an odd integer and (α, β) a Lucas pair implies $(d_2, d_3) = (1, 3)$, we deduce that

$$u_6 = u_3(z_2 - 3z_3)(z_2 + 3z_3).$$

There are infinitely many coprime solutions to the equations

$$\begin{aligned} z_2 - 3z_3 &= 1, \\ z_2 + 3z_3 &= p, \end{aligned}$$

given by $z_2 = 3t+1$, $z_3 = t$, $t \in \mathbb{N}$, where p is a prime number, since there are infinitely many prime numbers congruent to 1 (mod 6). Since $p = L - 3M$, $\gcd(u_1u_2u_3u_4u_5, p) = 1$, and $p \nmid L(L-4M)u_1u_2u_3u_4u_5$.

In case $n = 5$, we begin by noting that

$$\begin{aligned} u_5(\alpha,\beta) &= \frac{\alpha^5-\beta^5}{\alpha-\beta} \\ &= \Phi_5(\alpha,\beta) \\ &= \prod_{\substack{j=1 \\ \gcd(j,5)=1}}^{5} (\alpha - \zeta_5^j\beta) \\ &= \Phi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta})\Phi^{(2)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}), \end{aligned}$$

where

$$\begin{aligned} \Phi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1 \\ \gcd(s,5)=1 \\ (s|k(\alpha\beta))=1}}^{5} (\sqrt{\alpha} - \zeta_5^s\sqrt{\beta}) \prod_{\substack{t=1 \\ \gcd(t,5)=1 \\ (t|k(\alpha\beta))=-1}}^{5} (\sqrt{\alpha} + \zeta_5^t\sqrt{\beta}), \\ \Phi^{(2)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1 \\ \gcd(s,5)=1 \\ (s|k(\alpha\beta))=1}}^{5} (\sqrt{\alpha} + \zeta_5^s\sqrt{\beta}) \prod_{\substack{t=1 \\ \gcd(t,5)=1 \\ (t|k(\alpha\beta))=-1}}^{5} (\sqrt{\alpha} - \zeta_5^t\sqrt{\beta}). \end{aligned}$$

Since $5/(\eta\kappa)$ is an odd integer, and (α,β) is a Lucas pair, it suffices to establish the result with $k(\alpha\beta) = 1$, $\alpha+\beta = x$, and $\alpha\beta = y^2$, for some integers x, y. It follows that

$$\begin{aligned} \Phi^{(1)}_{1}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1 \\ \gcd(s,5)=1 \\ (s|1)=1}}^{5} (\sqrt{\alpha} - \zeta_5^s\sqrt{\beta}) \\ &= (\alpha+\beta-(\zeta_5^1+\zeta_5^4)\sqrt{\alpha\beta})(\alpha+\beta-(\zeta_5^2+\zeta_5^3)\sqrt{\alpha\beta}), \end{aligned}$$

$$\begin{aligned} \Phi^{(2)}_{1}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1 \\ \gcd(s,5)=1 \\ (s|1)=1}}^{5} (\sqrt{\alpha} + \zeta_5^s\sqrt{\beta}) \\ &= (\alpha+\beta+(\zeta_5^1+\zeta_5^4)\sqrt{\alpha\beta})(\alpha+\beta+(\zeta_5^2+\zeta_5^3)\sqrt{\alpha\beta}), \end{aligned}$$

and

$$u_5(\alpha,\beta) = f^{(1)}(x,y)f^{(2)}(x,y),$$

where

$$\begin{aligned} f^{(1)}(x,y) &= (x-(1/2)(-1+\sqrt{5})y)(x-(-1/2)(1+\sqrt{5})y) \\ &= x^2+xy-y^2, \end{aligned}$$

$$\begin{aligned} f^{(2)}(x,y) &= (x+(1/2)(-1+\sqrt{5})y)(x+(-1/2)(1+\sqrt{5})y) \\ &= x^2-xy-y^2. \end{aligned}$$

We observe that

$$\gcd(f^{(1)}(x,y), f^{(2)}(x,y)) = 1$$

by Lemma 1.25 and Lemma 1.24, since any common divisor divides

$$(x^2-3xy+y^2)\cdot f^{(1)}(x,y) + (-x^2+xy+3y^2)\cdot f^{(2)}(x,y) = -2^2\cdot(\alpha\beta)^2.$$

In summary, we have established the factorisation

$$u_5(\alpha,\beta) = (x^2+xy-y^2)(x^2-xy-y^2),$$

where $\alpha+\beta = x \in \mathbb{Z}$, $\alpha\beta = y^2, y \in \mathbb{Z}$, and

$$\gcd(x^2+xy-y^2, x^2-xy-y^2) = 1.$$

Stewart [30, page 90] observed that

$$x^2 - xy - (y^2+1) = 0 \tag{5.2}$$

is solvable in integers x and y for a given integer y whenever

$$z^2 - 5y^2 = 4, \tag{5.3}$$

for some $z \in \mathbb{Z}$. Although equation (5.3) has infinitely many solutions by the theory of *Pell's equation*, Stewart argued that in fact it has infinitely many coprime solutions (z, y), given in general, as $p > 5$ runs over the sequence of primes, by

$$\begin{aligned} z_p + y_p\sqrt{5} &= 2\left(\frac{3+\sqrt{5}}{2}\right)^p, \\ z_p &= \left(\frac{3+\sqrt{5}}{2}\right)^p + \left(\frac{3-\sqrt{5}}{2}\right)^p, \\ y_p &= \frac{1}{\sqrt{5}}\left(\left(\frac{3+\sqrt{5}}{2}\right)^p - \left(\frac{3-\sqrt{5}}{2}\right)^p\right). \end{aligned}$$

Each solution (z_p, y_p) of (5.3) gives rise to two solutions (x_p, y_p) of (5.2), namely

$$(x_p, y_p) = \left(\frac{y_p + z_p}{2}, y_p\right),$$

and

$$(x_p, y_p) = \left(\frac{y_p - z_p}{2}, y_p\right).$$

In particular, it is easily verified that

$$\left(\frac{y_p + z_p}{2}\right)^2 - 4y_p^2 < 0,$$

and hence that (x_p, y_p) generate a complex Lucas pair. It suffices now to argue that for infinitely many prime numbers p,

$$x_p^2 + x_p y_p - y_p^2$$

is a prime number $q(p)$. To this end, we note that

$$\begin{aligned}
& \left(\frac{y_p+z_p}{2}\right)^2+\left(\frac{y_p+z_p}{2}\right)y_p-y_p^2 \\
= \;& \frac{z_p^2-y_p^2}{4}+y_pz_p \\
= \;& \frac{1}{4}\left(\frac{4}{5}\left(\frac{3+\sqrt{5}}{2}\right)^{2p}+\frac{12}{5}\left(\frac{3+\sqrt{5}}{2}\right)^{p}\left(\frac{3-\sqrt{5}}{2}\right)^{p}+\frac{4}{5}\left(\frac{3-\sqrt{5}}{2}\right)^{2p}\right)+ \\
& \frac{1}{\sqrt{5}}\left(\left(\frac{3+\sqrt{5}}{2}\right)^{2p}-\left(\frac{3-\sqrt{5}}{2}\right)^{2p}\right) \\
= \;& \frac{1}{5}\left((1+\sqrt{5})\left(\frac{3+\sqrt{5}}{2}\right)^{2p}+(1-\sqrt{5})\left(\frac{3-\sqrt{5}}{2}\right)^{2p}+3\right),
\end{aligned}$$

and appeal to Conjecture 5.1. We observe that for each prime p such that $q(p)$ is prime, $q(p)$ is a primitive divisor. Note first if $q(p)$ divides $L(L-4M)=x_p^2(x_p^2-4y_p^2)$, then since $\gcd(x_p,y_p)=1$, $q(p)|x_p^2$ or $q(p)|(x_p^2-4y_p^2)$, in either case a contradiction to the definition of $q(p)$. Further, we note that for $1\le i<5$,

$$\gcd(u_i,q(p))=\gcd(u_i,u_5)=u_{\gcd(i,5)}=u_1=1.$$

On the other hand, in case $n=12$, we observe that

$$\begin{aligned}
u_{12}(\alpha,\beta) &= \prod_{\substack{d|12\\ d\neq 1,2}}\Phi_d(\alpha,\beta) \\
&= \Phi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta})\Phi^{(2)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta})\prod_{\substack{d|12\\ d\neq 1,2,12}}\Phi_d(\alpha,\beta),
\end{aligned}$$

where

$$\begin{aligned}
\Phi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1\\ \gcd(s,24)=1\\ (k(\alpha\beta)|s)=1}}^{24} (\sqrt{\alpha}-\zeta_{24}^{s}\sqrt{\beta}),\\
\Phi^{(2)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1\\ \gcd(s,24)=1\\ (k(\alpha\beta)|s)=1}}^{24} (\sqrt{\alpha}+\zeta_{24}^{s}\sqrt{\beta}).
\end{aligned}$$

Since $12/(\eta k(\alpha\beta))$ is an odd integer, and (α,β) is a Lucas pair, it suffices to establish the result with $k(\alpha\beta)=2$, $\alpha+\beta=x$, and $\alpha\beta=2y^2$, for some integers x,y. It follows that

$$\begin{aligned}
\Phi^{(1)}_{2}(\sqrt{\alpha},\sqrt{\beta}) &= (\alpha+\beta-(\zeta_{24}^{1}+\zeta_{24}^{23})\sqrt{\alpha\beta})(\alpha+\beta-(\zeta_{24}^{7}+\zeta_{24}^{17})\sqrt{\alpha\beta}),\\
\Phi^{(2)}_{2}(\sqrt{\alpha},\sqrt{\beta}) &= (\alpha+\beta+(\zeta_{24}^{1}+\zeta_{24}^{23})\sqrt{\alpha\beta})(\alpha+\beta+(\zeta_{24}^{7}+\zeta_{24}^{17})\sqrt{\alpha\beta}),
\end{aligned}$$

and

$$u_{12}(\alpha,\beta)=f_2^{(1)}(x,y)f_2^{(2)}(x,y)\prod_{\substack{d|12\\ d\neq 1,2,12}}\Phi_d(\alpha,\beta),$$

where

$$\begin{aligned}
f_2^{(1)}(x,y) &= x^2-2xy-2y^2,\\
f_2^{(2)}(x,y) &= x^2+2xy-2y^2.
\end{aligned}$$

We observe that

$$\gcd(f_2^{(1)}(x,y),f_2^{(2)}(x,y))=1$$

by Lemma 1.24 and Lemma 1.25, since any common divisor divides

$$(x^2+6xy+6y^2)\cdot f_2^{(1)}(x,y)+(-x^2-2xy+10y^2)\cdot f_2^{(2)}(x,y)=-2^3\cdot(\alpha\beta)^2.$$

Plainly, the equation

$$x^2-2xy-(2y^2+1)=0 \tag{5.4}$$

is solvable in integers x and y for a given integer y whenever

$$z^2 - 12y^2 = 4, \tag{5.5}$$

for some $z \in \mathbb{Z}$. The minimal solution of (5.5) is $(z, y) = (4, 1)$, and thus the general solution of (5.5) is given by (see [19, ex. 18, page 144])

$$z_n + 2y_n\sqrt{3} = \pm 2(2 + \sqrt{3})^n.$$

It follows that

$$\begin{aligned} z_n &= (2+\sqrt{3})^n + (2-\sqrt{3})^n \\ y_n &= \frac{1}{2\sqrt{3}}\left((2+\sqrt{3})^n - (2-\sqrt{3})^n\right). \end{aligned}$$

Let $p > 5$ be a prime number, $\alpha_0 = 2 + \sqrt{3}$, and $\beta_0 = 2 - \sqrt{3}$. Note that (α_0, β_0) is a real Lucas pair, and that

$$\begin{aligned} z_p &= \alpha_0^p + \beta_0^p = \Phi_{2p}(\alpha_0, \beta_0)\Phi_2(\alpha_0, \beta_0), \\ y_p &= \frac{1}{2\sqrt{3}}\left(\alpha_0^p - \beta_0^p\right) = \Phi_p(\alpha_0, \beta_0). \end{aligned}$$

Plainly, $z_p \equiv 0 \pmod 2$, since $2|\Phi_2(\alpha_0, \beta_0) = 4$, and $y_p \equiv 1 \pmod 2$ by Lemma 1.25, since $p \neq 2$, and all prime factors of $\Phi_p(\alpha_0, \beta_0)$, aside from p, are congruent to $\pm 1 \pmod p$.

Hence, as n runs through the primes $p > 5$, we find infinitely many solutions (z_p, y_p) of (5.5) with z_p even and y_p odd, and hence, by equation (5.5), with z_p and y_p coprime. Each solution (z_p, y_p) of (5.5) gives rise to two solutions (x_p, y_p) of (5.4), namely

$$(x_p, y_p) = \left(\frac{2y_p + z_p}{2}, y_p\right),$$

and

$$(x_p, y_p) = \left(\frac{2y_p - z_p}{2}, y_p\right).$$

In particular, it is easily verified that

$$\left(\frac{2y_p + z_p}{2}\right)^2 - 8y_p^2 < 0,$$

and hence that (x_p, y_p) generate a complex Lucas pair. It suffices now to argue that for infinitely many prime numbers p,

$$x_p^2 + 2x_p y_p - 2y_p^2$$

is a prime number $r(p)$. To this end, we appeal to Conjecture 5.2, and note

$$\begin{aligned}
& \left(\frac{2y_p + z_p}{2}\right)^2 + 2\left(\frac{2y_p + z_p}{2}\right) y_p - 2y_p^2 \\
= \; & (1/4)z_p^2 + 2y_p z_p + y_p^2 \\
= \; & \frac{3}{12}\left(\alpha_0^{2p} + 2\alpha_0^p\beta_0^p + \beta_0^{2p}\right) + \frac{1}{12}\left(\alpha_0^{2p} - 2\alpha_0^p\beta_0^p + \beta_0^{2p}\right) + \frac{1}{\sqrt{3}}\left(\alpha_0^{2p} - \beta_0^{2p}\right) \\
= \; & \frac{1}{3}\left((1+\sqrt{3})(2+\sqrt{3})^{2p} + (1-\sqrt{3})(2-\sqrt{3})^{2p} + 1\right).
\end{aligned}$$

Finally, as in case $n = 5$, we observe that for each prime p such that $r(p)$ is prime, $r(p)$ is a primitive divisor. Plainly, $r(p)$ does not divide $L(L - 4M)$. Further, we note that for $1 \le i < 12$,

$$\gcd(u_i, u_{12}) = u_{\gcd(i,12)} \in \{1, u_3, u_4, u_6\} = \{1, L - M, L - 2M, (L - M)(L - 3M)\},$$

and

$$u_{12} = (L - M)(L - 2M)(L - 3M)r(p),$$

together with the fact that $r(p) > L - jM$ for $j = 1, 2, 3$ imply, for $1 \le i < 12$, that

$$\gcd(u_i, r(p)) = 1.$$

QED.

Bibliography

[1] A. Akbary, Z. Friggstad, and R. Juricevic. Explicit upper bounds for $\prod_{p \le p_{\omega(n)}} p/(p-1)$. *Contributions to Discrete Mathematics, To Appear*, 2007.

[2] A. S. Bang. Taltheoretiske Undersogelser. *Tidsskrift for Mat. (5)*, 4:70–80, 130–137, 1886.

[3] Y. Bilu and G. Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60:373–392, 1996.

[4] Y. Bilu, G. Hanrot, P. M. Voutier, and with an appendix by M. Mignotte. Existence of primitive divisors of Lucas and Lehmer numbers. *J. reine angew. Math.*, 539:72–122, 2001.

[5] G. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. Math. (2)*, 5:173–180, 1904.

[6] R. P. Brent. On computing factors of cyclotomic polynomials. *Math. Comp.*, 61 no. 203:131–149, 1993.

[7] P. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. Math. (2)*, 15:30–70, 1913.

[8] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, and K. Wildanger. Kant v4. *J. Symbolic Comp.*, 24:267–283, 1997.

[9] L. K. Durst. Exceptional real Lehmer sequences. *Pacific J. Math*, 9:437–441, 1959.

[10] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers; fifth edition.* Clarendon Press, Oxford, 1979.

[11] H. Hasse. *Vorlesungen über Zahlentheorie.* Springer-Verlag, Berlin, 1964.

[12] H. Hasse. *Number Theory.* (Classics in Mathematics) Springer-Verlag, Berlin, 2002.

[13] Dan Kalman. A matrix proof of Newton's identities. *Math. Mag.*, 73:313–315, 2000.

[14] M. Laurent, M. Mignotte, and Y. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory*, 55:285–321, 1995.

[15] D. H. Lehmer. An extended theory of Lucas' functions. *Ann. Math. (2)*, 31, no.3:419–448, 1930.

[16] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. Math.*, 1:184–240, 289–321, 1878.

[17] F. Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp.*, 76:493–505, 2007.

[18] G. Robin. Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. *Acta Arith.*, 42:367–389, 1983.

[19] H. E. Rose. *A Course in Number Theory, second edition.* Clarendon Press, Oxford, 1994.

[20] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[21] A. Rotkiewicz. On Lucas numbers with two intrinsic divisors. *Bull. Acad. Polon. Sci. Ser. Math. Astr. Phys.*, 10:229–232, 1962.

[22] A. Schinzel. The intrinsic divisors of Lehmer numbers in the case of negative discriminant. *Ark. Mat.*, 4:413–416, 1962.

[23] A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Phil. Soc.*, 58, Part 4:555–562, 1962.

[24] A. Schinzel. On primitive prime factors of Lehmer numbers I. *Acta Arith.*, VIII:213–223, 1963.

[25] A. Schinzel. On primitive prime factors of Lehmer numbers II. *Acta Arith.*, VIII:251–257, 1963.

[26] A. Schinzel. On primitive prime factors of Lehmer numbers III. *Acta Arith.*, XV:48–69, 1968.

[27] A. Schinzel. On primitive divisors of the expression $a^n - b^n$ in algebraic number fields. *J. reine angew. Math.*, 268/269:27–33, 1974.

[28] T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations. Cambridge Tracts in Mathematics, 87.* Cambridge University Press, Cambridge-New York, 1986.

[29] C. L. Stewart. On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. *Proc. London Math. Soc. (3)*, 35:425–447, 1977.

[30] C. L. Stewart. Primitive divisors of Lucas and Lehmer numbers, in: A. Baker and D. W. Masser eds. *Transcendence Theory: Advances and Applications, Academic Press*, pages 79–92, 1977.

[31] B. L. van der Waerden. *Algebra, Volume 1.* Frederick Ungar Publishing Co., Inc., New York, 1970.

[32] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences. *Math. Comp.*, 64, no. 210:869–888, 1995.

[33] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences II. *J. Th. Nombres Bordeaux*, 8:251–274, 1996.

[34] P. M. Voutier. Primitive divisors of Lucas and Lehmer sequences III. *Proc. Cambridge Phil. Soc.*, 123:407–419, 1998.

[35] M. Waldschmidt. *Diophantine Approximation on Linear Algebraic Groups*. Springer-Verlag, Berlin, Germany, 2000.

[36] M. Ward. The intrinsic divisors of Lehmer numbers. *Ann. Math. (2)*, 62:230–236, 1955.

[37] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math.*, 3:165–284, 1892.