ACTA ARITHMETICA
137.3 (2009)

Classifying Lehmer triples

by

Robert Juricevic (Waterloo)

Dedicated to A. Schinzel

1. Introduction. Before providing a historical perspective on the study of primitive divisors of Lehmer numbers, we define some notation.

Definition 1. Let $z \in \mathbb{C}$ and $w \in \mathbb{C}$ be such that $w^2 - z = 0$. We define $z = |z| \exp(\sqrt{-1} \arg(z))$, where $-\pi < \arg(z) \le \pi$, and $w = |w| \exp(\sqrt{-1} \arg(w))$, where $-\pi/2 < \arg(w) \le \pi/2$.

Definition 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. A *real Lucas pair* is such that $(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$. A *complex Lucas pair* is such that $(\alpha, \beta) \notin \mathbb{R} \times \mathbb{R}$.

Definition 3. 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. A *real Lehmer pair* is such that $(\alpha^2, \beta^2) \in \mathbb{R} \times \mathbb{R}$. A *complex Lehmer pair* is such that $(\alpha^2, \beta^2) \notin \mathbb{R} \times \mathbb{R}$.

Definition 4. Given a Lucas or Lehmer pair, we define

$$L = (\alpha+\beta)^2, \qquad \kappa = k(\xi),$$

$$M = \alpha\beta, \qquad \eta = \begin{cases} 1 & \text{if } \kappa \equiv 1 \pmod 4, \\ 2 & \text{otherwise}, \end{cases}$$

$$\xi = M \max\{L - 4M, L\},$$

where $k(\xi)$ is the squarefree kernel of ξ.

Definition 5. Given a Lucas or Lehmer pair, we define a *Lehmer sequence* $(u_n)_{n=0}^{\infty}$ by

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

2000 *Mathematics Subject Classification*: Primary 11B39; Secondary 11Y05, 11Y11.
Key words and phrases: Lehmer numbers, primitive divisors, factorisation, primality.

DOI: 10.4064/aa137-3-3

In 1930, Lehmer [11] introduced the sequences $(u_n)_{n=0}^{\infty}$. He showed that his sequences had similar divisibility properties to those of Lucas [12] sequences, and he used them to extend the Lucas test for primality.

Definition 6. A *Lehmer number* is a term of the Lehmer sequence $(u_n)_{n=0}^{\infty}$.

Definition 7. A *real Lehmer triple* is a triple (n, α, β) corresponding to a Lehmer number $u_n(\alpha, \beta)$ and such that (α, β) is a real Lehmer pair.

Definition 8. A *complex Lehmer triple* is a triple (n, α, β) corresponding to a Lehmer number $u_n(\alpha, \beta)$ and such that (α, β) is a complex Lehmer pair.

We note that Lehmer numbers satisfy the following recurrence relation:

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

and hence that Lehmer numbers are rational integers.

Definition 9. A *primitive divisor* of a Lehmer number $u_n = u_n(\alpha, \beta)$ 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 first general result about the existence of primitive divisors of Lehmer numbers is attributed to Zsigmondy [30], and dates back to 1892. In 1904, Birkhoff and Vandiver [3] rediscovered Zsigmondy's result. In 1913, Carmichael [4] extended Zsigmondy's result to include in particular the Fibonacci sequence. After a long break corresponding to the period dominated by the two world wars, the study was revived in the 1950's by Ward [29], who extended Carmichael's result to real Lehmer triples, and Durst [5], who continued Ward's work. Motivated by Ward's remark that nothing appears to be known for complex Lehmer triples, in the 1960's, Schinzel published a series of papers extending Ward's and Durst's results to complex Lehmer triples. In particular, Schinzel [15] 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 $u_n(\alpha, \beta)$ has at least one primitive divisor. Later, in 1974, Schinzel [20] 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 [23] 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

$$n_1 = e^{452} 4^{67},$$

but also by showing that there are only finitely many Lehmer sequences whose nth term, $n > 6$, $n \notin \{8, 10, 12\}$, does not have 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 $(u_n)_{n=0}^{\infty}$ in case (α, β) is a Lehmer pair, but may be replaced by the best possible restrictions $n > 4$, $n \neq 6$ in case (α, β) is a Lucas pair. In the 1990's, Voutier made a number of refinements of Stewart's work ([25]–[27]), and in particular established that one may take

$$n_1 = 30030,$$

and conjectured that one may take $n_1 = 30$. 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 [2] established the optimal value

$$n_1 = 30.$$

In order to further motivate this article, consider the following problem:

Problem 1. *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* n *exceeds some bound, and* r *is a given natural number.*

The case $r = 1$ in Problem 1 has been completely resolved by Bilu, Hanrot and Voutier. In this article we consider the case $r = 2$. 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

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

In 1962, Schinzel showed that if $n/(\eta_0 k(ab))$ is an odd integer, and the triple (n, a, b) is not from an explicit table, 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 [14] generalised this theorem to real Lucas pairs ($(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$). In 1963, Schinzel [17] generalised Rotkiewicz's theorem to a result about the nth term of the Lehmer sequence $(u_n)_{n=0}^{\infty}$ having at least two primitive divisors. In the same year, Schinzel [18] 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 [19] refined all of his theorems on primitive divisors of Lehmer numbers. 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 [20] showed that for each r, $n_r(\alpha, \beta)$ may be replaced by an absolute constant n_r.

In the next section we establish Theorem 1 on Lehmer numbers, generated by a real or complex Lehmer pair, in the direction of solving a part of Problem 1. More precisely, Schinzel [20] proved that there exists an absolute constant n_2 such that if L and M are integers such that $L > 0$, $M > 0$, $L - 4M < 0$, $\gcd(L,M) = 1$, $(L,M) \notin \{(1,1),(2,1),(3,1)\}$, $n > n_2$, and $n/(\eta\kappa)$ is an odd integer, then $u_n(\alpha,\beta)$ has at least two primitive divisors. We show that we may take $n_2 = 1.2 \cdot 10^{10}$. Moreover, we extend Stewart's algorithm [23, 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. Finally, we show that the conditions $n > 6$, $n \neq 12$ in Theorem 1 cannot be improved, and so are best possible, when (α,β) is a Lucas pair, under the assumption of two plausible conjectures.

2. Classifying Lehmer triples.

2. Classifying Lehmer triples. We state our main result, which depends on the following two conjectures on primes.

Conjecture 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 2. *There are infinitely many prime numbers $p > 5$ such that*

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

is a prime number.

Theorem 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 fewer than two primitive divisors. Furthermore, the conditions $n > 6$, $n \neq 12$ are best possible, subject to the truth of Conjectures 1 and 2.*

2.1. *Preliminary lemmas*

Definition 10. We define the *cyclotomic polynomial*

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

where

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

Lemma 1. *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 the following factorisation of the cyclotomic polynomial* $\Phi_N(x,y)$:

$$\Phi_N(x,y) = \Phi^{(1)}_{N,m}(x,y)\Phi^{(2)}_{N,m}(x,y),$$

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

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

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

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

$$\Phi^{(1)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,\ell)=1\\ (s|m)=1}}^{\ell} (\sqrt{x}-\sqrt{-1}\,\zeta_\ell^s\sqrt{y}) \prod_{\substack{t=1\\ \gcd(t,\ell)=1\\ (t|m)=-1}}^{\ell} (\sqrt{x}+\sqrt{-1}\,\zeta_\ell^t\sqrt{y}), \tag{3}$$

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

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

$$\Phi^{(1)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,4\ell)=1\\ (m|s)=1}}^{4\ell} (\sqrt{x}-\zeta_{4\ell}^s\sqrt{y}), \tag{5}$$

$$\Phi^{(2)}_{N,m}(x,y) = \prod_{\substack{s=1\\ \gcd(s,4\ell)=1\\ (m|s)=1}}^{4\ell} (\sqrt{x}+\zeta_{4\ell}^s\sqrt{y}). \tag{6}$$

Here $(s|m)$, $(t|m)$, *and* $(m|s)$ *are Jacobi symbols.*

Proof. This is essentially line (4), (5), and (7) of [16, Theorem 1]. ∎

LEMMA 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. If the* n*th Lehmer number* u_n *has fewer than two 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*

$$|\delta\Phi^{(j)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})| \in \begin{cases} \{1,2,3,6\} & \textit{if } n=12, \\ \{1,P(n/\gcd(n,3))\} & \textit{otherwise}, \end{cases} \tag{7}$$

where

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

$\nu = \eta\kappa\prod_{p\mid n,\, p\nmid\eta\kappa} p$, $\ell = \kappa\prod_{p\mid n,\, p\nmid\eta\kappa} p$, *and* $N=\nu$, $\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})$ *is defined by equations* (1), (3) *or* (5), *and* $\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})$ *is defined by equations* (2), (4), *or* (6).

Proof. Schinzel [17, Lemma 2] deduced that

$$|\Phi_n(\alpha,\beta)| = |\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})|\,|\delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})|\delta^{-2}, \tag{8}$$

where

$\delta = k((\alpha+\beta)^2)^{-(\phi(n)/4-\lfloor\phi(n)/4\rfloor)}$, $\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}), \delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}) \in \mathbb{Z}$,

and

$$\gcd(\delta\Phi^{(1)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu}), \delta\Phi^{(2)}_{N,\kappa}(\alpha^{n/\nu},\beta^{n/\nu})) = 1. \tag{9}$$

If u_n has no primitive divisor, then by [23, Theorem 2], and (8), the result follows. Suppose that u_n has exactly one primitive divisor p_1. Since by [24, Lemma 6], the prime divisors of $|\Phi_n(\alpha,\beta)|$ coincide with the primitive divisors of u_n, except possibly for $P(n/\gcd(n,3))$, the greatest prime factor of $n/\gcd(n,3)$, which exactly divides $\Phi_n(\alpha,\beta)$ if at all, we see that $p_1 \mid \Phi_n(\alpha,\beta)$. Suppose $p_1 \neq P(n/\gcd(n,3))$. By (8) and (9), we may assume without loss of generality that

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

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 (9), $p \neq p_1$. By [24, Lemma 6] 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 deduce (7). Suppose now that $p_1 = P(n/\gcd(n,3))$. Then $p_1 \mid n$, from which it follows that

$$\gcd(p_1+1,n)=1, \qquad \gcd(p_1-1,n)=1.$$

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

$$p_1 \mid u_{p_1-1}u_{p_1+1}.$$

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

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

or

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

in both cases, a contradiction. ∎

LEMMA 3. *Let $m, n \in \mathbb{N}$, m odd. Then*

$$\sum_{\substack{j=1\\ \gcd(j,n)=1}}^{\lfloor n/2\rfloor} (\zeta_n^j + \zeta_n^{-j})^m = \phi(n) \sum_{l=0}^{(m-1)/2} \binom{m}{l} \frac{\mu(n/\gcd(n, m-2l))}{\phi(n/\gcd(n, m-2l))}.$$

Proof. This follows from [6, Theorem 272] and the binomial theorem. ∎

LEMMA 4. *Let $m, n \in \mathbb{N}$, m even. Then*

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

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. This follows from [6, Theorem 272] and the fact that

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

LEMMA 5. *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*

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

where

$$\varepsilon = \begin{cases} 1 & \text{if } d \equiv 1 \pmod{4},\\ -1 & \text{if } d \equiv -1 \pmod{4}. \end{cases}$$

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 [7, Theorem IV],

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

By [7, Theorem XI],

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

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

Lemma 6. *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*

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

$$= \pm\, d_3^{\frac{m(n/\nu)+1}{2}} \sqrt{d_2} \sum_{\substack{l=0 \\ \nu/\gcd(\nu,m-2l)\equiv 0 \,(\mathrm{mod}\, d)}}^{(m-1)/2} \binom{m}{l}$$
$$\times \frac{\phi(\nu)\mu\big(\frac{\nu}{d\gcd(\nu,m-2l)}\big)\big(\frac{\nu}{d\gcd(\nu,m-2l)}\big|d\big)\big(\frac{m-2l}{\gcd(\nu,m-2l)}\big|d\big)}{\phi(\nu/\gcd(\nu,m-2l))}.$$

Proof. This follows from Lemma 5 and the binomial theorem. ∎

Lemma 7. *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*

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

$$= d_3^{\frac{mn/\nu}{2}} \phi(\nu)\bigg(\sum_{l=0}^{m/2-1}\binom{m}{l}\frac{\mu(\nu/\gcd(\nu,m-2l))}{\phi(\nu/\gcd(\nu,m-2l))} + \frac{1}{2}\binom{m}{m/2}\bigg).$$

Proof. This follows as in the proof of Lemma 4, on noting that since $\gcd(i,d) = 1$ and m is even, $\{\pm(i|d)\}^m = 1$. ∎

Lemma 8. *Let $2 \le c \in \mathbb{Z}$, $(\alpha+\beta)^2 = z_2^2$, and $\alpha\beta = z_3^2$, where $z_2 \in \mathbb{Z}$, $z_3 \in \mathbb{Z}$. Then*

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

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

Lemma 9. *Let* $2 \le c \in \mathbb{Z}$, $(\alpha+\beta)^2 = d_2 z_2^2$, *and* $\alpha\beta = d_3 z_3^2$, *where* $(d_2, d_3) \in \{(3,1),(1,3)\}$, $z_2 \in \mathbb{Z}$, $z_3 \in \mathbb{Z}$. *Then*

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

Proof. This follows directly from the identity $\Phi_l(x,-y) = \Phi_{2l}(x,y)$, valid for any odd integer $l > 1$, factoring a difference of squares, and pairing $(\zeta_{3^c}^i, \zeta_{3^c}^{-i})$. ■

Lemma 10. *Let L and M be integers such that* $L > 0$, $M > 0$, $L - 4M < 0$, $\gcd(L,M) = 1$, $(L,M) \notin \{(1,1),(2,1),(3,1)\}$, (α,β) *be the corresponding Lehmer pair, and let κ and η be as in Definition* 4. *If* $n > 4$, $n \ne 6$, $n/(\eta\kappa)$ *is an odd integer, and*

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

then the nth Lehmer number u_n has at least two primitive divisors.

Proof. We use the notation of Lemma 2. It suffices to establish that

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

which is equivalent to

$$\frac{|\Phi_n(\alpha,\beta)|}{\max(|\delta\Phi_{N,\kappa}^{(1)}(\alpha^{n/\nu},\beta^{n/\nu})|, |\delta\Phi_{N,\kappa}^{(2)}(\alpha^{n/\nu},\beta^{n/\nu})|)} > n. \tag{10}$$

By [21], in order to prove (10), it suffices to show that

$$\frac{|\Phi_n(\alpha,\beta)|}{|\alpha|^{\phi(n)/2}\exp(4\sqrt{n}\,(\log n)^2)} > n. \tag{11}$$

It remains to take the logarithm of both sides of (11). ■

Lemma 11. *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. Plainly,

$$|1-\gamma^d| \ge \frac{2}{\pi}\,|\arg\gamma^d|. \tag{12}$$

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 $0 < b_1 \le d$, and

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

By (12), it follows that

$$\log|1-\gamma^d| \ge \log|b_1\sqrt{-1}\,\pi - b_2\log\gamma| + \log 2 - \log\pi. \tag{13}$$

Let $\lambda = 1.8$ in [2, Theorem A.1.3]. Then

$$\varrho = 6.04\ldots,\qquad t = 0.008\ldots,\qquad k = 0.2946\ldots,\qquad D' = 1,$$
$$a = \log|\alpha| + 9.5027\ldots,\qquad B = \max\{527, b_1, d\},\qquad d' = \max\{527, d\}.$$

Since

$$\log|\alpha| \ge \frac{\log 2}{2},$$

it follows that

$$\mathcal{H} \le \log d' - 0.604\ldots < \log d'.$$

By [2, Theorem A.1.3],

$$\begin{aligned}\log|b_1\sqrt{-1}\,\pi - b_2\log\gamma|&\\ > -(c_1(\log d')^2 + 0.23)a &- 2\log d' - 2\log\log d' - c_2,\end{aligned} \tag{14}$$

where $c_1 = 24.88\ldots$ and $c_2 = 0.12\ldots$. By (13) and (14) we deduce the result. ∎

Lemma 12. *Let $n \ge 527$, (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

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

and Lemma 11, since $\log d' \le \log n$. ∎

Lemma 13. *Let L and M be integers such that $L > 0$, $M > 0$, $L - 4M < 0$, $\gcd(L,M) = 1$, $(L,M) \notin \{(1,1),(2,1),(3,1)\}$, (α,β) be the corresponding Lehmer pair, and let κ and η be as in Definition 4. If $n \ge 1.2\cdot 10^{10}$, and $n/(\eta\kappa)$ is an odd integer, then the nth term $u_n(\alpha,\beta)$ of the Lehmer sequence has at least two primitive divisors.*

Proof. Let $\gamma = \beta/\alpha$. It follows from

$$\Phi_n(\alpha,\beta) = \prod_{d\mid n}(\alpha^d - \beta^d)^{\mu(n/d)} \quad \text{and} \quad \phi(n) = n\sum_{t\mid n}\frac{\mu(t)}{t}$$

that

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

By Lemma 10, it suffices to show that

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

Since

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

it suffices to show that

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

By Lemma 12, it suffices to show that, for $n \ge 527$,

$$\frac{1}{2}\,\phi(n)\log|\alpha| - 2^{\omega(n)-1}\log 2 - 2^{\omega(n)-1}F(n,\alpha) \\ - 4\sqrt{n}\,(\log n)^2 - \log n > 0, \tag{15}$$

where

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

Since

$$\frac{1}{\log|\alpha|} \le \frac{2}{\log 2}, \tag{16}$$

it follows that

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

where

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

Multiplying (15) by $2(\log|\alpha|)^{-1}$, and applying (16), it suffices to show that

$$(17)\quad \phi(n) - 2^{\omega(n)}F_1^*(n) - (16/\log 2)\sqrt{n}\,(\log n)^2 - (4/\log 2)\log n > 0,$$

where

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

Since $n > 10^{10}$, we have

$$(18)\qquad \begin{aligned}\sqrt{n}\,(\log n)^2\biggl(\frac{16}{\log 2} + \frac{4}{\log 2}\cdot\frac{1}{\sqrt{n}\,(\log n)}\biggr)&\\ < \sqrt{n}\,(\log n)^2\biggl(\frac{16}{\log 2} + \frac{4}{\log 2}\cdot\frac{1}{\sqrt{10^{10}}\,(10\log 10)}\biggr)&\\ = (23.083123\ldots)\sqrt{n}\,(\log n)^2,&\end{aligned}$$

and

$$(19)\qquad \begin{aligned}F_1^*(n) &= (\log n)^2\biggl(707.38 + 5.78\,\frac{\log(n\log n)}{(\log n)^2} + \frac{10.19}{(\log n)^2}\biggr)\\ &< (\log n)^2\biggl(707.38 + \frac{2\cdot 5.78}{10\log 10} + \frac{10.19}{(10\log 10)^2}\biggr)\\ &= (707.901\ldots)(\log n)^2.\end{aligned}$$

Substituting inequalities (18) and (19) in (17), we see that it suffices to show that

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

Since by [1, Proposition 4.1],

$$\phi(n) > (0.496866\ldots)\,\frac{n}{\log\log n}\qquad \text{for } n > 6915878970,$$

and by [13, Théorème 11],

$$\omega(n) \le (1.38401\ldots)\,\frac{\log n}{\log\log n}\qquad \text{for } n \ge 3,$$

it suffices to show that

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

Since $n > 10^{10}$,

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

and we see that it suffices to show that

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

or equivalently,

$$L(n) > 0,$$

where

$$L(n) = \frac{0.49686\sqrt{n}}{(\log n)^2 \log\log n} - \frac{707.91}{n^{0.194}} - 23.084. \tag{20}$$

Note that

$$L(1.1 \cdot 10^{10}) = -0.026\ldots, \qquad L(1.2 \cdot 10^{10}) = 1.206\ldots.$$

It suffices to show that $L(n)$ is increasing for $n > 10^{10}$. Since by the definition (20),

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

and for $n > 10^{10}$,

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

it follows that $L'(n) > 0$ for $n > 10^{10}$. ∎

Lemma 14. *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 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 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.*

Proof. 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 $n/(\eta\kappa)$ being 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

$$z_2 - z_3 = 1, \qquad z_2 + z_3 = p,$$

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 $p = L - M$, $p \nmid L(L-4M)u_1u_2$.

In case $n = 4$, since $n/(\eta\kappa)$ being 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

$$z_2 - 2z_3 = 1, \qquad z_2 + 2z_3 = p,$$

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 (mod 4). Since $\gcd(u_1u_2u_3, u_4) = 1$, and $p = L - 2M$, $p \nmid L(L-4M)u_1u_2u_3$.

In case $n = 6$, since $n/(\eta\kappa)$ being 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

$$z_2 - 3z_3 = 1, \qquad z_2 + 3z_3 = p,$$

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

$$\begin{aligned} u_5(\alpha, \beta) = \frac{\alpha^5 - \beta^5}{\alpha - \beta} = \varPhi_5(\alpha, \beta) &= \prod_{\substack{j=1 \\ \gcd(j,5)=1}}^{5} (\alpha - \zeta_5^j \beta) \\ &= \varPhi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha}, \sqrt{\beta})\varPhi^{(2)}_{k(\alpha\beta)}(\sqrt{\alpha}, \sqrt{\beta}), \end{aligned}$$

where

$$\varPhi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha}, \sqrt{\beta}) = \prod_{\substack{s=1 \\ \gcd(s,5)=1 \\ (s|k(\alpha\beta))=1}}^{5} (\sqrt{\alpha} - \zeta_5^s \sqrt{\beta}) \prod_{\substack{t=1 \\ \gcd(t,5)=1 \\ (t|k(\alpha\beta))=-1}}^{5} (\sqrt{\alpha} + \zeta_5^t \sqrt{\beta}),$$

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

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

$$\begin{aligned}\Phi_1^{(1)}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1\\ \gcd(s,5)=1\\ (s|1)=1}}^{5} (\sqrt{\alpha}-\zeta_5^s\sqrt{\beta})\\ &= (\alpha+\beta-(\zeta_5^1+\zeta_5^4)\sqrt{\alpha\beta})(\alpha+\beta-(\zeta_5^2+\zeta_5^3)\sqrt{\alpha\beta}),\\ \Phi_1^{(2)}(\sqrt{\alpha},\sqrt{\beta}) &= \prod_{\substack{s=1\\ \gcd(s,5)=1\\ (s|1)=1}}^{5} (\sqrt{\alpha}+\zeta_5^s\sqrt{\beta})\\ &= (\alpha+\beta+(\zeta_5^1+\zeta_5^4)\sqrt{\alpha\beta})(\alpha+\beta+(\zeta_5^2+\zeta_5^3)\sqrt{\alpha\beta}),\end{aligned}$$

and

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

where

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

We observe that

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

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 [23, p. 90] observed that

$$x^2-xy-(y^2+1) = 0 \tag{21}$$

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

$$z^2-5y^2 = 4 \tag{22}$$

for some $z\in\mathbb{Z}$. Although equation (22) 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

$$z_p + y_p\sqrt{5} = 2\left(\frac{3+\sqrt{5}}{2}\right)^p,$$

where

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

Each solution (z_p, y_p) of (22) gives rise to two solutions (x_p, y_p) of (21), namely

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

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) generates 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

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

and appeal to Conjecture 1. We observe that if $q(p)$ is prime, then $q(p)$ is a primitive divisor. Note first that if $q(p)$ divides $L(L-4M) = x_p^2(x_p^2 - 4y_p^2)$, then since $\gcd(x_p, y_p) = 1$, $q(p) \mid x_p^2$ or $q(p) \mid (x_p^2 - 4y_p^2)$, 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

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

where

$$\Phi^{(1)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}) = \prod_{\substack{s=1 \\ \gcd(s,24)=1 \\ (k(\alpha\beta)|s)=1}}^{24} (\sqrt{\alpha} - \zeta_{24}^s\sqrt{\beta}),$$

$$\Phi^{(2)}_{k(\alpha\beta)}(\sqrt{\alpha},\sqrt{\beta}) = \prod_{\substack{s=1 \\ \gcd(s,24)=1 \\ (k(\alpha\beta)|s)=1}}^{24} (\sqrt{\alpha} + \zeta_{24}^s\sqrt{\beta}).$$

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

$$\begin{aligned}\Phi_2^{(1)}(\sqrt{\alpha},\sqrt{\beta})&=(\alpha+\beta-(\zeta_{24}^{1}+\zeta_{24}^{23})\sqrt{\alpha\beta})(\alpha+\beta-(\zeta_{24}^{7}+\zeta_{24}^{17})\sqrt{\alpha\beta}),\\ \Phi_2^{(2)}(\sqrt{\alpha},\sqrt{\beta})&=(\alpha+\beta+(\zeta_{24}^{1}+\zeta_{24}^{23})\sqrt{\alpha\beta})(\alpha+\beta+(\zeta_{24}^{7}+\zeta_{24}^{17})\sqrt{\alpha\beta}),\end{aligned}$$

and

$$u_{12}(\alpha,\beta)=f_2^{(1)}(x,y)f_2^{(2)}(x,y)\prod_{\substack{d\mid 12\\ d\neq 1,2,12}}\Phi_d(\alpha,\beta),$$

where

$$f_2^{(1)}(x,y)=x^2-2xy-2y^2,\qquad f_2^{(2)}(x,y)=x^2+2xy-2y^2.$$

We observe that

$$\gcd(f_2^{(1)}(x,y),f_2^{(2)}(x,y))=1,$$

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

$$x^2-2xy-(2y^2+1)=0 \tag{23}$$

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

$$z^2-12y^2=4 \tag{24}$$

for some $z\in\mathbb{Z}$. The minimal solution of (24) is $(z,y)=(4,1)$, and thus the general solution of (24) is given by

$$z_n+2y_n\sqrt{3}=\pm 2(2+\sqrt{3})^n.$$

It follows that

$$z_n=(2+\sqrt{3})^n+(2-\sqrt{3})^n,\qquad y_n=\frac{1}{2\sqrt{3}}\,((2+\sqrt{3})^n-(2-\sqrt{3})^n).$$

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

$$z_p=\alpha_0^p+\beta_0^p=\Phi_{2p}(\alpha_0,\beta_0)\Phi_2(\alpha_0,\beta_0),\qquad y_p=\frac{1}{2\sqrt{3}}\,(\alpha_0^p-\beta_0^p)=\Phi_p(\alpha_0,\beta_0).$$

Plainly, $z_p\equiv 0 \pmod 2$, since $2\mid\Phi_2(\alpha_0,\beta_0)=4$, and $y_p\equiv 1 \pmod 2$ by [24, Lemma 6], 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 (24) with z_p even and y_p odd, and hence, by equation

(24), with z_p and y_p coprime. Each solution (z_p, y_p) of (24) gives rise to two solutions (x_p, y_p) of (23), namely

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

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 now suffices 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 2, and note

$$\left(\frac{2y_p + z_p}{2}\right)^2 + 2\left(\frac{2y_p + z_p}{2}\right) y_p - 2y_p^2$$
$$= \frac{1}{3}\left((1+\sqrt{3})(2+\sqrt{3})^{2p} + (1-\sqrt{3})(2-\sqrt{3})^{2p} + 1\right).$$

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 $1 \le i < 12$,

$$\begin{aligned}\gcd(u_i, u_{12}) &= u_{\gcd(i,12)} \in \{1, u_3, u_4, u_6\}\\ &= \{1, L-M, L-2M, (L-M)(L-3M)\},\end{aligned}$$

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

$$\gcd(u_i, r(p)) = 1. \ \blacksquare$$

2.2. *Proof of Theorem 1.* By [9, Theorem 1], it suffices to prove Theorem 1 assuming $L > 0$, $M > 0$, $L - 4M < 0$, $\gcd(L, M) = 1$ and $(L, M) \notin \{(1,1), (2,1), (3,1)\}$. By Lemma 13, we have $n < 1.2 \cdot 10^{10}$. We fix

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

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

$$\delta \Phi_{N,\kappa}^{(j)}(\alpha^{n/\nu}, \beta^{n/\nu}) \in \{\pm 1, \pm P(n/\gcd(n,3))\}, \tag{25}$$

where

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

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

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

We handle the case $\kappa \equiv 1 \pmod 4$. The other cases are similar. In case $\kappa \equiv 1 \pmod 4$, note that $\Phi^{(1)}_{N,\kappa}(\cdot)$ and $\Phi^{(2)}_{N,\kappa}(\cdot)$ in equations (25) are defined by equations (1) and (2), with

$$\nu = \kappa \prod_{p \mid n, p \nmid \kappa} p, \qquad \ell = \nu, \qquad N = \nu, \qquad x = \alpha^{n/\nu}, \qquad y = \beta^{n/\nu}.$$

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) and (2) become

$$\Phi^{(1)}_{\nu,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\lfloor \ell/2 \rfloor} (x_1 - (s|\kappa)(\zeta_\ell^s + \zeta_\ell^{-s})x_2), \tag{26}$$

$$\Phi^{(2)}_{\nu,\kappa}(\alpha^{n/\nu}, \beta^{n/\nu}) = \prod_{\substack{s=1 \\ \gcd(s,\ell)=1}}^{\lfloor \ell/2 \rfloor} (x_1 + (s|\kappa)(\zeta_\ell^s + \zeta_\ell^{-s})x_2), \tag{27}$$

where each of (26) and (27) is a binary form of degree $\phi(\ell)/2$ in x_1 and x_2,

$$x_1 = \alpha^{n/\nu} + \beta^{n/\nu}, \tag{28}$$

$$x_2 = (\alpha\beta)^{n/(2\nu)}. \tag{29}$$

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

$$\begin{aligned} &\frac{\alpha^{n/\nu} + \beta^{n/\nu}}{\alpha + \beta} \\ &\quad = ((\alpha+\beta)^2)^{(n/\nu-1)/2} - \sum_{k=1}^{(n/\nu-1)/2} \binom{n/\nu}{k} (\alpha\beta)^k \frac{\alpha^{n/\nu-2k} + \beta^{n/\nu-2k}}{\alpha+\beta}. \end{aligned} \tag{30}$$

We observe that since (α, β) is a Lehmer pair, it follows by induction and the identity (30) 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

$$x_1 = z_1 z_2\sqrt{k((\alpha+\beta)^2)}.$$

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

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

Then equations (26) and (27) become

$$\begin{aligned} (31)\quad &f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ &\quad = \sum_{s=0}^{\phi(\nu)/2} a_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(\nu)/2-s}(z_1z_2)^{\phi(\nu)/2-s}(z_3^{n/\nu})^s, \\ (32)\quad &f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2, z_3^{n/\nu}) \\ &\quad = \sum_{s=0}^{\phi(\nu)/2} b_s(\sqrt{k((\alpha+\beta)^2)})^{\phi(\nu)/2-s}(z_1z_2)^{\phi(\nu)/2-s}(z_3^{n/\nu})^s. \end{aligned}$$

Because of Newton's identities [10], we may write the a_s's and the b_s's in the form

$$a_0 = 1,\qquad a_s = -\frac{1}{s}\sum_{j=0}^{s-1} p^{(a)}_{s-j}a_j,\qquad s=1,\dots,\phi(\nu)/2,$$

$$p^{(a)}_{s-j} = \sum_{\substack{i=1\\ \gcd(i,\nu)=1}}^{\lfloor \nu/2\rfloor} \{(i|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}\,(\zeta_\nu^i+\zeta_\nu^{-i})\}^{s-j},\qquad s-j=1,\dots,\phi(\nu)/2,$$

and

$$b_0 = 1, \quad b_s = -\frac{1}{s}\sum_{j=0}^{s-1} p_{s-j}^{(b)} b_j, \quad s = 1, \dots, \phi(\nu)/2,$$

$$p_{s-j}^{(b)} = \sum_{\substack{i=1\\ \gcd(i,\nu)=1}}^{\lfloor \nu/2 \rfloor} \{-(i|\kappa)\sqrt{(k(\alpha\beta))^{n/\nu}}\,(\zeta_\nu^i + \zeta_\nu^{-i})\}^{s-j}, \quad s-j = 1, \dots, \phi(\nu)/2.$$

We note that there are only finitely many equations (31) and (32), 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

$$d = \kappa, \quad d_2 = k((\alpha+\beta)^2), \quad d_3 = k(\alpha\beta). \tag{33}$$

It follows by Lemma 6 in case $s - j \equiv 1 \pmod 2$, that

$$p_{s-j}^{(a)} = \Bigg((k(\alpha\beta))^{((s-j)(n/\nu)+1)/2} \sum_{\substack{l=0\\ \nu/\gcd(\nu,s-j-2l)\equiv 0 \,(\mathrm{mod}\,\kappa)}}^{(s-j-1)/2} \binom{s-j}{l} \\ \times \frac{\phi(\nu)\mu\big(\frac{\nu}{\kappa\gcd(\nu,s-j-2l)}\big)\big(\frac{\nu}{\kappa\gcd(\nu,s-j-2l)}\big|\kappa\big)\big(\frac{s-j-2l}{\gcd(\nu,s-j-2l)}\big|\kappa\big)}{\phi(\nu/\gcd(\nu,s-j-2l))}\Bigg)\sqrt{k((\alpha+\beta)^2)},$$

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

$$\phi(\nu) \equiv 0 \ (\mathrm{mod}\ \phi(\nu/\gcd(\nu, s-j-2l))).$$

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 7 in case $s-j \equiv 0 \pmod 2$,

$$p_{s-j}^{(a)} = (k(\alpha\beta))^{(s-j)(n/\nu)/2}\phi(\nu) \\ \times \Bigg(\sum_{l=0}^{(s-j)/2-1}\binom{s-j}{l}\frac{\mu(\nu/\gcd(\nu,s-j-2l))}{\phi(\nu/\gcd(\nu,s-j-2l))} + \frac{1}{2}\binom{s-j}{(s-j)/2}\Bigg),$$

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

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

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

$$\begin{cases} u_3\sqrt{k((\alpha+\beta)^2)} & \text{if } s\equiv 1 \pmod 2,\\ u_4 & \text{otherwise,}\end{cases} \tag{34}$$

where u_3 and u_4 are integers. Plainly, in case $\kappa=1$, the coefficients of the equations (31) and (32) 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

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

that $\phi(\nu)/2$ is an even integer. We observe that (34), and the fact that $\phi(\nu)/2$ is an even integer, imply that the coefficients of the equations (31) and (32) are integers.

By [22, Theorem 5.1], for $j=1$ and $j=2$, we deduce that each of the equations

$$f^{(j)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2,z_3^{n/\nu})=m, \tag{35}$$

where $f^{(1)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2,z_3^{n/\nu})$ and $f^{(2)}_{n,k((\alpha+\beta)^2),k(\alpha\beta)}(z_1z_2,z_3^{n/\nu})$ are defined by (31) and (32) respectively, and

$$m\in\{\pm1,\pm P(n/\gcd(n,3))\}$$

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

Plainly, on recalling the identities

$$\zeta_\nu^s+\zeta_\nu^{-s}=2\cos(2\pi s/\nu),\qquad -\cos(2\pi s/\nu)=\cos(\pi-2\pi s/\nu), \tag{36}$$

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

$$\phi(\nu)/2\ge 3$$

which is true provided we assume

$$\prod_{p|n}(p-1)\ge 6, \tag{37}$$

since

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

Plainly, in any case $\kappa\equiv 1,2,3 \pmod 4$, 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 (37) and

$$\prod_{\substack{2<p|n\\4|n}}(p-1)\geq 4, \tag{38}$$

where (38) appears after considering the case $\kappa\equiv 2 \pmod 4$.

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

$$u_2(z_1z_2)^2+u_3(z_1z_2)z_3^{n/\nu}+u_4(z_3^{n/\nu})^2=m_1 \tag{39}$$

have finitely many solutions in integers z_1z_2, z_3, where $m_1\in\{\pm1,\pm5\}$, and

$$(k((\alpha+\beta)^2),k(\alpha\beta),u_2,u_3,u_4)\in\{(1,1,1,\pm1,-1),(5,1,5,\mp5,1),\\ (1,5,1,\mp5^{(n/\nu+1)/2},5^{n/\nu})\}.$$

Moreover, if $\prod_{2<p|n,\,4|n}(p-1)=2$, let $n=4\cdot3^c$ and $n/\nu=3^{c-1}$, where $c\geq 2$. It suffices to show that the equations

$$u_5(z_1z_2)^2+u_6(z_1z_2)z_3^{n/\nu}+u_7(z_3^{n/\nu})^2=m_2 \tag{40}$$

have finitely many solutions in integers z_1z_2, z_3, where $m_2\in\{\pm1,\pm3\}$, and

$$(k((\alpha+\beta)^2),k(\alpha\beta),u_5,u_6,u_7)\\ \in\{(2,1,2,\mp2,-1),(1,2,1,\mp2^{(n/\nu+1)/2},-2^{n/\nu}),(6,1,6,\mp6,1),\\ (3,2,3,\mp2^{(n/\nu+1)/2}\cdot3,2^{n/\nu}),(2,3,2,\mp2\cdot3^{(n/\nu+1)/2},3^{n/\nu}),\\ (1,6,1,\mp6^{(n/\nu+1)/2},6^{n/\nu})\}.$$

The finiteness result in either case $n=5^c$ or $n=4\cdot3^c$ follows by [22, Theorem 6.1], on recalling (39) and (40), and noting that equations (39) are solvable in integer z_1z_2 for a given integer z_3 only if

$$(u_3^2-4u_4)z_3^{2n/\nu}=w_1^2-4m_1 \tag{41}$$

for some integer w_1, while equations (40) are solvable in integer z_1z_2 for a given integer z_3 only if

$$(u_6^2-4u_7)z_3^{2n/\nu}=w_2^2-4m_2 \tag{42}$$

for some integer w_2.

On the other hand, we consider the case that $\prod_{p|n,\,4\nmid n}(p-1)=2$. Let $n=3^c$, where $c\geq 2$. By Lemma 8, we have a factorisation

$$\Phi_{3^c}(\alpha,\beta)=f_{3^c}^{(1)}(z_2,z_3)f_{3^c}^{(2)}(z_2,z_3). \tag{43}$$

It is easily seen that $f_{3^c}^{(j)}(z_2,z_3)\in\mathbb{Z}$ for $j=1$ and $j=2$ by Newton's identities and Lemmas 3 and 4. By [28, pp. 104–105], 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 [8, pp. 443, 523–525], 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 [8, pp. 443, 523–525], 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 $3^c\nmid(3\pm1)$, 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 2, we deduce for $j=1$ and $j=2$ that

$$f_{3^c}^{(j)}(z_2,z_3)=m, \tag{44}$$

where $m\in\{\pm1,\pm3\}$. It remains to note that each $f_{3^c}^{(j)}(z_2,z_3)$ has at least three distinct roots on recalling the identities (36), since $3^{c-1}\geq 3$. Hence, [22, Theorem 5.1] implies the finiteness of the solutions (z_2,z_3) of (44). Moreover, the case $n=2\cdot 3^c$, where $c\geq 2$, follows similarly, but with Lemma 9, the argument underlying the analogue of Lemma 6 and Lemma 7 in case $\kappa\equiv 3 \pmod 4$, by the analogue of [8, pp. 443, 523–525], by the analogue of the identities (36) in case $\kappa\equiv 3 \pmod 4$, and with respect to the implied integer Thue equations

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

Finally, by Lemma 14, we note that the conditions $n>6$, $n\neq 12$ are best possible subject to the truth of Conjectures 1 and 2. ∎

Acknowledgements. I would like to express my gratitude to C. L. Stewart for his direction and support during the time this research was undertaken.

References

[1] A. Akbary, Z. Friggstad and R. Juricevic, *Explicit upper bounds for $\prod_{p\leq p_{\omega(n)}}\frac{p}{p-1}$*, Contrib. Discrete Math. 2 (2007), 153–160.

[2] Y. Bilu, G. Hanrot and P. M. Voutier (with an appendix by M. Mignotte), *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. 539 (2001), 72–122.

[3] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. (2) 5 (1904), 173–180.

[4] P. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, ibid. 15 (1913), 30–70.

[5] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441.

[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, 1979.

[7] H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Springer, Berlin, 1964.

[8] —, *Number Theory*, Classics Math., Springer, Berlin, 2002.

[9] R. Juricevic, *Classifying real Lehmer triples*: *a revived computation*, to appear.

[10] D. Kalman, *A matrix proof of Newton's identities*, Math. Mag. 73 (2000), 313–315.

[11] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) 31 (1930), 419–448.

[12] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. 1 (1878), 184–240, 289–321.

[13] 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 (1983), 367–389.

[14] A. Rotkiewicz, *On Lucas numbers with two intrinsic divisors*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 10 (1962), 229–232.

[15] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416.

[16] —, *On primitive prime factors of* $a^n - b^n$, Proc. Cambridge Philos. Soc. 58 (1962), 555–562.

[17] —, *On primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), 213–223.

[18] —, *On primitive prime factors of Lehmer numbers II*, ibid. 8 (1963), 251–257.

[19] —, *On primitive prime factors of Lehmer numbers III*, ibid. 15 (1968), 49–70; Corrigendum, ibid. 16 (1969), 101.

[20] —, *On primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33.

[21] —, *On primitive prime factors of Lehmer numbers*, Chapter I.2 of *Andrzej Schinzel*, *Selecta*, Eur. Math. Soc., Zürich, 2007, 1051 (Lemma 3), 1055 (Theorem A1).

[22] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, Cambridge, 1986.

[23] C. L. Stewart, *Primitive Divisors of Lucas and Lehmer Numbers*, in: Transcendence Theory: Advances and Applications, A. Baker and D. W. Masser (eds.), Academic Press, 1977, 79–92.

[24] —, *On divisors of Fermat*, *Fibonacci*, *Lucas and Lehmer numbers*, Proc. London Math. Soc. (3) 35 (1977), 425–447.

[25] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. 64 (1995), 869–888.

[26] —, *Primitive divisors of Lucas and Lehmer sequences II*, J. Théor. Nombres Bordeaux 8 (1996), 251–274.

[27] —, *Primitive divisors of Lucas and Lehmer sequences III*, Math. Proc. Cambridge Philos. Soc. 123 (1998), 407–419.

[28] B. L. van der Waerden, *Algebra*, Vol. 1, Frederick Ungar, New York, 1970.

[29] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.

[30] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. 3 (1892), 265–284.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada
E-mail: rjuricevic@math.uwaterloo.ca

Received on 15.2.2008
and in revised form on 17.9.2008 (5604)