Contributions to Discrete Mathematics

Volume 4, Number 1, Pages 92–106
ISSN 1715-0868

CLASSIFYING REAL LEHMER TRIPLES: A REVIVED COMPUTATION

ROBERT JURICEVIC

Abstract. In the 1960's, Schinzel [5] gave a condition on n under which he ensured that all nth terms of any Lehmer sequence have a least two primitive divisors except for a finite list of such sequences. Brillhart and Selfridge determined all of the numbers in Schinzel's list which had at most one primitive prime factor, but the resulting list was lost. In this article, we revisit this problem and exhibit the lost list.

1. Introduction

We begin by defining the notation used in the article.

Definition 1.1. *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 1.2. *Two Lehmer pairs* (α_1, β_1) *and* (α_2, β_2) *are equivalent if*

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

Definition 1.3. *Given a Lehmer pair, we define*

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

where $k(\xi)$ *is the square-free kernel of* ξ.

Received by the editors July 24, 2008, and in revised form March 10, 2009.
2000 *Mathematics Subject Classification.* Primary 11B39; Secondary 11Y05, 11Y11.
Key words and phrases. Lehmer numbers, primitive divisors, factorisation, primality.

Definition 1.4. *Given a Lehmer pair, we define a Lehmer sequence* $(u_n)_{n=0}^{\infty}$ *by*

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

In 1930, Lehmer [2] introduced the sequences $(u_n)_{n=0}^{\infty}$. Lehmer showed that his sequences had similar divisibility properties to those of Lucas [3] sequences, and he used them to extend the Lucas test for primality.

Definition 1.5. *A Lehmer number is a term of the Lehmer sequence* $(u_n)_{n=0}^{\infty}$.

We note that Lehmer numbers satisfy the following recurrence relation

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

and hence that Lehmer numbers are rational integers.

Definition 1.6. *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*

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

Definition 1.7. *A real Lehmer triple is a triple* (n,α,β) *corresponding to a Lehmer number* $u_n(\alpha,\beta)$*, such that* (α,β) *is a real Lehmer pair; plainly* $(\alpha^2,\beta^2) \in \mathbb{R} \times \mathbb{R}$*, or equivalently,* $(\alpha-\beta)^2 > 0$.

Motivated by Ward's [9] remark that nothing appears to be known for complex Lehmer triples, in the 1960's, Schinzel published a series of papers, including [4] and [5] which are included in volume 2 of Schinzel's selected papers [7], extending the known results on real Lehmer triples to complex Lehmer triples.

In the next section we make explicit a result of Schinzel [5] on real Lehmer triples, and thereby classify all real Lehmer triples (n,α,β) up to equivalence, such that (α,β) is a real Lehmer pair, and $u_n(\alpha,\beta)$ has at least 2 primitive divisors. 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. Schinzel [6] remarks that Brillhart and Selfridge have done this, although no reference to their work is given in [6] or [7]. In personal electronic mail correspondence, Brillhart confirmed the computation was done, not published, and since lost.

One purpose of the present article is to fill this gap in the history of computational number theory, as we use Theorem 2.1 in order to establish the main result in [1]. Although we had access to a significant amount of modern day computational power, a direct strategy of factoring all of the Lehmer numbers in question was not fruitful. However, we found by using the underlying structure of the Lehmer sequences under study, that the computer algebra system MAPLE sufficed, running on a personal computer.

2. Classifying real Lehmer triples

The proof of Theorem 2.1 amounts to exhibiting the set $R_0 \cup Q_0$, defined in Lemma 2.2, due to Schinzel [5, Theorem 1], explicitly. We do this in Table 1. We note that the following conditions

$$L > 0, \quad M \neq 0, \quad L - 4M > 0, \quad \gcd(L, M) = 1, \tag{2.1}$$

ensure that we have a real Lehmer pair.

Theorem 2.1. *Let L and M be integers satisfying the conditions (2.1), (α, β) be the associated real Lehmer pair, and let κ and η be defined by Definition 1.3. 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, then $u_n(\alpha, \beta)$ has at least two primitive divisors.*

2.1. Preliminary Lemmas.

Lemma 2.2. *Let L and M be integers satisfying the conditions (2.1), (α, β) be the associated real Lehmer pair, and let κ and η be defined by Definition 1.3. 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*

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

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

Proof. This is part 1 of [5, Theorem 1]. □

Definition 2.3. *We define the cyclotomic polynomial*

$$\Phi_n(x, y) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n} \left(x - \zeta_n^i y\right), \tag{2.2}$$

where

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

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

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

Lemma 2.4. *Let $n>2$, and let (α,β) be a Lehmer pair. Then $\Phi_n(\alpha,\beta)\in\mathbb{Z}$.*

Proof. We remark that although this result is not new (e.g. it appears in Ward's [9] paper), we include an argument as it is instructive.

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

Let

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

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, we have $\alpha\beta\in\mathbb{Z}$, $\alpha^2+\beta^2=(\alpha+\beta)^2-2\alpha\beta\in\mathbb{Z}$, and so $\Phi_n(\alpha,\beta)=F_n(\alpha^2+\beta^2,\alpha\beta)\in\mathbb{Z}$. □

Lemma 2.5. *Let (α,β) be a Lehmer pair. Then*

(1) *For all positive integers n we have $\gcd(\alpha\beta,u_n)=1$.*
(2) *If $d\mid n$, then $u_d\mid u_n$ 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 $4\mid u_m$, 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 $d\mid n$, then $\Phi_n(\alpha,\beta)$ divides u_n/u_d, where $\Phi_n(\alpha,\beta)$ is defined by equation (2.2).*

Proof. These properties go back to Lehmer [2]. See Stewart [8] for a proof. □

Definition 2.6. *For any integer m, we let $P(m)$ denote the largest prime factor of m, with the convention that $P(0)=P(\pm1)=1$.*

Lemma 2.7. *Let (α,β) be a Lehmer pair, and let $\Phi_n(\alpha,\beta)$ be defined by equation (2.2). 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 $\pm1 \pmod n$. 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 $\pm1 \pmod{12}$.*

Proof. This is [8, Lemma 6]. □

Lemma 2.8. *Let (α, β) be a Lehmer pair, $L > 0$, $M \neq 0$, 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

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

and

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

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 2.5 and Lemma 2.7, the primitive divisors of u_n are the prime factors of $\Phi_n(\alpha, \beta)$, except possibly for $P(n/\gcd(n, 3))$. If $M > 0$,

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

We note the following identities relating to the cyclotomic polynomial; for any odd integer $\ell > 1$,

$$\Phi_\ell(x,-y) = \Phi_{2\ell}(x,y); \tag{2.3}$$

for any even integer $\ell > 1$,

$$\Phi_\ell(x,y) = \Phi_{2\ell}(\sqrt{x},\sqrt{y}); \tag{2.4}$$

and for $n > 1$, and n^* the greatest square-free divisor of n,

$$\Phi_n(x,y) = \Phi_{n^*}(x^{n/n^*}, y^{n/n^*}). \tag{2.5}$$

If $M < 0$, and $n \equiv 1 \pmod 2$, by equation (2.3),

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

If $M < 0$, and $n \equiv 2 \pmod 4$, by equation (2.3),

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

If $M < 0$, and $n \equiv 0 \pmod 4$, by equation (2.4),

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

and since $8 \nmid n$, by equation (2.5),

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

□

Lemma 2.9. *Let u_n be defined by Definition 1.4, $\ell > 1$ 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 $p \mid c$. Then $p \mid \ell$. 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 $p \nmid u_i$. By part 3 of Lemma 2.5, we have for all positive integers m and n that

$$\gcd(u_n, u_m) = u_{\gcd(m,n)}. \tag{2.6}$$

It follows from (2.6) 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 $\gcd(\ell, u_i) = 1$. Thus, $p \nmid u_i$ for any $3 \le i \le n-1$, $\gcd(i,n) = 1$. □

Lemma 2.10. *Let $\ell > 1$ be a square-free integer, and let m be a 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,*

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

and

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

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

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

and

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

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

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

and

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

and where $(s \mid m)$, $(t \mid m)$, *and* $(m \mid s)$ *are Jacobi symbols.*

Proof. This is essentially lines (4), (5), and (7) of [4, Theorem 1]. □

2.2. **Proof of Theorem 2.1.**

Proof. By Lemma 2.2, 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 2 and Table 3. 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 2 and Table 3. The remaining elements are the elements of the set $R_0 \cup Q_0$, and are tabulated in Table 1.

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

Table 3: 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.

Let $u_n = \prod_{i=1}^{k} p_i^{a_i}$. Note that the result of calling the function

$$\mathit{ifactors(u_n,Easy)}$$

in the computer algebra system 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

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

Computing $u_n(\alpha, \beta)$ and calling the function *ifactors(u_n,Easy)* in MAPLE, for each triple (n, L, M) from Table 2, we determine that all of the triples from Table 2 have at least two primitive divisors, except for the triples

$$(117, 1, -3), \quad (132, 33, 8), \quad (132, 1, -8) \tag{2.7}$$

and

$$(156, 39, 8), \quad (156, 7, -8), \tag{2.8}$$

the triples in Table 1, and the triples

$$\begin{array}{ccc} (41, 41, 9), & (43, 7, -9), & (51, 5, -3), \\ (82, 5, -9), & (86, 43, 9), & (102, 17, 3), \\ (105, 21, 5), & (140, 3, -8), & (140, 35, 8) \\ (156, 2, -13), & (156, 54, 13). & \end{array} \tag{2.9}$$

We call the function *ifactors(u_n,pollard,n)* in MAPLE for the triples (2.7) and the triples in Table 1, the function *ifactors(u_n,lenstra)* in MAPLE for the triples (2.8), and apply Lemma 2.9 for the triples (2.9), in order to obtain

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],

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

and

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

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 aforementioned triples, 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 2.9.

Similarly, computing $u_n(\alpha, \beta)$ and calling the function *ifactors(u_n,Easy)* in MAPLE, for each triple (n, L, M) from Table 3, we determine that all of the triples from Table 3 have at least two primitive divisors, except for the triples

$$(234, 13, 3), \tag{2.10}$$

$$\begin{array}{cccc}
(259, 9, -7), & (308, 56, 11), & (308, 12, -11), & (364, 56, 13), \\
(364, 4, -13), & (518, 37, 7), & (532, 38, 7), & (532, 10, -7), \\
 & (1860, 62, 15), & (1860, 2, -15), &
\end{array} \tag{2.11}$$

and the triples

$$\begin{array}{cccc}
(165, 1, -11), & (203, 1, -7), & (210, 1, -5), & (220, 22, 5), \\
(220, 2, -5), & (330, 45, 11), & (372, 7, -6), & (372, 31, 6), \\
(406, 29, 7), & (420, 30, 7), & (420, 2, -7), & (561, 51, 11), \\
(583, 9, -11), & (940, 47, 10), & (940, 7, -10), & (1060, 53, 10), \\
(1060, 13, -10), & (1122, 7, -11), & (1166, 53, 11), & (1276, 58, 11), \\
(1276, 14, -11), & (1508, 58, 13), & (1508, 6, -13). &
\end{array} \tag{2.12}$$

We call the function *ifactors(u_n,pollard,n)* in MAPLE for the triple (2.10), and apply Lemma 2.9 for the triples (2.12), in order to obtain

$$234, \quad 13, \quad 3, \qquad [819001577161, \quad 173196209426761],$$

and

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

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

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

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

and

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

On the other hand, for the triples (2.11), we first observe that by Lemma 2.8, the following pairs of Lehmer numbers have the same primitive divisors

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

Hence, it suffices to consider only one Lehmer number in each pairing. Furthermore, note that by Lemma 2.5 and Lemma 2.7, 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 2.10, 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 $N = \eta\kappa \prod_{p \mid n, p \nmid \eta\kappa} p$, for each of the remaining triples (2.11), in order to obtain

$$\Phi^{(1)}_{259,-259}\left(\frac{3+\sqrt{37}}{2}, \frac{3-\sqrt{37}}{2}\right) = \begin{array}{l} 46881867946123593485484605899\backslash \\ 16180894723400737849509490008\backslash \\ 963078078647137569, \end{array}$$

$$\Phi^{(2)}_{259,-259}\left(\frac{3+\sqrt{37}}{2}, \frac{3-\sqrt{37}}{2}\right) = \begin{array}{l} 25602532917287678605527501221\backslash \\ 03255198933323101108540307556\backslash \\ 538691009, \end{array}$$

$$\Phi^{(1)}_{308,154}(\sqrt{14}+\sqrt{3}, \sqrt{14}-\sqrt{3}) = \begin{array}{l} 3671911701277441159379537\backslash \\ 3075885082101401, \end{array}$$

$$\Phi^{(2)}_{308,154}(\sqrt{14}+\sqrt{3}, \sqrt{14}-\sqrt{3}) = \begin{array}{l} 12128860660883292326324236\backslash \\ 60041428753964355298041, \end{array}$$

$$\Phi^{(1)}_{364,182}(1+\sqrt{14}, -1+\sqrt{14}) = \begin{array}{l} 24966459880123360743012097\backslash \\ 65985081733111928329, \end{array}$$

$$\Phi^{(2)}_{364,182}(1+\sqrt{14}, -1+\sqrt{14}) = \begin{array}{l} 11525121307558382647076\backslash \\ 29630081683285276526646\backslash \\ 3808089, \end{array}$$

$$\Phi^{(1)}_{532,266}\left(\frac{\sqrt{38}+\sqrt{10}}{2}, \frac{\sqrt{38}-\sqrt{10}}{2}\right) = \begin{array}{l} 36895658633530016208191\backslash \\ 28171771560577226103402\backslash \\ 94815943469126220024381, \end{array}$$

$$\Phi^{(2)}_{532,266}\left(\frac{\sqrt{38}+\sqrt{10}}{2}, \frac{\sqrt{38}-\sqrt{10}}{2}\right) = \begin{array}{l} 82134836333556034573688\backslash \\ 63499769725714729728684\backslash \\ 66757288047729238221913\backslash \\ 5396021, \end{array}$$

$$\Phi^{(1)}_{1860,930}\left(\frac{\sqrt{62}+\sqrt{2}}{2}, \frac{\sqrt{62}-\sqrt{2}}{2}\right) = \begin{array}{l} 6526317520962088212962172\backslash \\ 2222532598631677902835936\backslash \\ 7649244397566667555602139\backslash \\ 6546184284642268806474345\backslash \\ 6351417323756011962087471\backslash \\ 9055423722960780194820161, \end{array}$$

$$\Phi^{(2)}_{1860,930}\left(\frac{\sqrt{62}+\sqrt{2}}{2}, \frac{\sqrt{62}-\sqrt{2}}{2}\right) = \begin{array}{l} 15315075524366125703399535\backslash \\ 72710157714837872041220167\backslash \\ 75761462681046365723574305\backslash \\ 78578949789494996471945888\backslash \\ 66521969104848023121915071\backslash \\ 21654392425529672601467162\backslash \\ 4981879085017485584079041. \end{array}$$

Since

$$\gcd\left(\Phi^{(1)}_{N,\kappa}(\alpha,\beta),\Phi^{(2)}_{N,\kappa}(\alpha,\beta)\right)=1$$

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 2.5 and Lemma 2.7 that u_n has at least two primitive divisors for each of the triples (2.11). □

Acknowledgements

I would like to express my gratitude to C. L. Stewart for his direction and support during the time this research was undertaken. Moreover, I would like to thank the anonymous referee for their comments.

References

[1] R. Juricevic, *Classifying Lehmer triples*, Acta Arithmetica, to appear.
[2] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. (2) **31** (1930), no. 3, 419–448.
[3] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
[4] A. Schinzel, *On primitive prime factors of $a^n - b^n$*, Proc. Cambridge Phil. Soc. **58** (1962), no. 4, 555–562.
[5] ———, *On primitive prime factors of Lehmer numbers I*, Acta Arith. **VIII** (1963), 213–223.
[6] ———, *On primitive prime factors of Lehmer numbers III*, Acta Arith. **XV** (1968), 48–69, Corrigendum, ibid. 16 (1969), 101.
[7] ———, *Andrzej Schinzel, Selecta*, European Mathematical Society, Zurich, 2007.
[8] C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), 425–447.
[9] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. Math. (2) **62** (1955), 230–236.

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