Journal de Théorie des Nombres
de Bordeaux **8** *(1996), 251–274*

Primitive divisors of Lucas and Lehmer sequences, II

par PAUL M VOUTIER

RÉSUMÉ. Soit α et β deux entiers algébriques complexes conjugués. On propose un algorithme dont l'objet est de découvrir des éléments des suites de Lucas ou de Lehmer associées à α et β, n'ayant pas de diviseurs primitifs. On utilise cette algorithme pour démontrer que pour tout α et β tel que $h(\beta/\alpha) \leq 4$, le n-ième terme des suites de Lucas et de Lehmer admet un diviseur primitif dès que $n > 30$. Nous donnons en outre une amélioration d'un résultat de Stewart se rapportant à des suites plus générales.

ABSTRACT Let α and β are conjugate complex algebraic integers which generate Lucas or Lehmer sequences. We present an algorithm to search for elements of such sequences which have no primitive divisors. We use this algorithm to prove that for all α and β with $\mathrm{h}(\beta/\alpha) \leq 4$, the n-th element of these sequences has a primitive divisor for $n > 30$. In the course of proving this result, we give an improvement of a result of Stewart concerning more general sequences.

1. Introduction

Let α and β be algebraic numbers such that $\alpha+\beta$ and $\alpha\beta$ are relatively prime non-zero rational integers and α/β is not a root of unity. The sequence $(u_n)_{n=0}^{\infty}$ defined by $u_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ for $n \geq 0$ is called a *Lucas sequence*.

If, instead of supposing that $\alpha + \beta \in \mathbb{Z}$, we only suppose that $(\alpha+\beta)^2$ is a non-zero rational integer, still relatively prime to $\alpha\beta$, then we define the *Lehmer sequence* $(u_n)_{n=0}^{\infty}$ associated to α and β by

$$u_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd} \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even.} \end{cases}$$

We say that a prime number p is a *primitive divisor* of a Lucas number u_n if p divides u_n but does not divide $(\alpha - \beta)^2 u_2 \ldots u_{n-1}$. Similarly,

Manuscrit reçu le 25 mars 1995

p is a primitive divisor of a Lehmer number u_n if p divides u_n but not $(\alpha^2-\beta^2)^2 u_3 \ldots u_{n-1}$.

Stewart [14, p. 80] showed, as a consequence of his Theorem 1, that if $n > C$ then u_n has a primitive divisor, where $C = e^{452}2^{67}$ for Lucas sequences and $C = e^{452}4^{67}$ for Lehmer sequences. In Theorem 2, we shall obtain an improvement over Theorem 1 of [14] as well as decreasing the size of C.

In an earlier article [16], we enumerated all Lucas and Lehmer sequences whose n-th element has no primitive divisor for certain $n \leq 12$ and all $12 < n \leq 30$. We also presented some evidence to support the conjecture made there that for $n > 30$, the n-th element of any Lucas or Lehmer sequence always has a primitive divisor.

Here, we present some further results concerning this conjecture. Our main result, Theorem 1, states that the conjecture is true if the absolute logarithmic height of α is small. In addition to providing further evidence for the validity of the conjecture (or at least not providing a counterexample), this result will also be useful in a forthcoming work where we shall make further improvements to the size of C.

Throughout this paper, we shall use $\mathrm{h}(\alpha)$ to denote the absolute logarithmic height of the algebraic number α.

THEOREM 1. *Suppose α and β generate a Lucas or Lehmer sequence with $\mathrm{h}(\beta/\alpha) \leq 4$. Then, for all $n > 30$, the n-th element of this sequence has a primitive divisor.*

We prove this result by using Stewart's idea [14, Section 5] of looking at certain Thue equations. For any Lucas or Lehmer sequence $(u_n)_{n=0}^{\infty}$, there is a pair of integers (p, q), dependent only on the sequence, such that if u_n has no primitive divisor then (p, q) is a solution of one of certain finitely many Thue equations associated to n. We use this to show that if, for $n > 30$, u_n is without a primitive divisor then n must be the denominator of a convergent in the continued-fraction expansion of $\arccos(p/(2q))/(2\pi)$. The advantage gained by this is that the convergents of real numbers grow quite quickly and so the problem of checking each n less than $2 \cdot 10^{10}$ is reduced to checking no more than fifty such n.

In fact, we will show that if u_n has no primitive divisor, then the convergent k/n must be an extremely good approximation to $\arccos(p/(2q))/(2\pi)$, so good that except for a few exceptional cases with n small, we can show directly that k/n is not sufficiently close to the number in question and therefore, eliminate n from consideration. In the remaining cases, a direct examination of u_n proves our desired result.

Stewart's upper bound for n, stated above, is quite large and would thus give rise to extremely long calculations just to determine theconvergents. Fortunately it is now possible to reduce this upper bound considerably. Because of its benefit to our work here, we shall determine such a smaller upper bound. In fact, we establish a more general result which is an improvement over Theorem 1 in Stewart's paper [14], whose proof requires little more effort than proving the more specific result which only applies to Lucas and Lehmer sequences.

THEOREM 2. *(i) Suppose α and β are algebraic integers with β/α having degree d_1 over $\mathbb{Q}$, $(\alpha,\beta)=(1)$ and β/α not a root of unity. Then there is a prime ideal $\mathcal{P}$ which divides the ideal $(\alpha^n-\beta^n)$ but does not divide the ideals $(\alpha^m-\beta^m)$ for $1 \le m < n$ for all $n > \max\left\{2(2^{d_1}-1), 4000(d_1\log(3d_1))^{12}\right\}$.*

(ii) *If α and β generate a Lucas or Lehmer sequence then the n-th element of this sequence has a primitive divisor for all $n > 2\cdot 10^{10}$.*

2. Preliminary Lemmas to Theorem 2

We shall first require a lower bound for linear forms in two logarithms. The work of Laurent, Mignotte and Nesterenko [8] will be suitable for our needs. We also need a good lower bound for the height of a non-zero algebraic number which is not a root of unity.

LEMMA 1. *Suppose that γ is a non-zero algebraic number of degree $D \ge 2$ over $\mathbb{Q}$ which is not a root of unity. Then*

$$\mathrm{h}(\gamma) > \frac{2}{D(\log(3D))^3}.$$

Proof. This is Corollary 1 of [17]. □

Now let us continue.

LEMMA 2. *Let γ be a non-zero algebraic number of degree D over $\mathbb{Q}$ which is not a root of unity and let $\log\gamma$ denote the principal value of its logarithm. Put*

$$\Lambda = b_1\log(-1) - b_2\log\gamma = b_1\pi i - b_2\log\gamma,$$

with b_1 a positive integer, b_2 a non-negative integer and

$$B = \max(|b_1|, |b_2|, 2).$$

If $\Lambda \neq 0$ then

$$|\Lambda| > \exp\left(-81.9(D\log(3D))^3 \,\mathrm{h}(\gamma)(\log B)^2\right).$$

Proof. First let us suppose that $|\gamma| \neq 1$. We can write $\gamma = re^{i\theta}$ where $r > 0$ and $-\pi < \theta \leq \pi$. Since $r^2 = \gamma \cdot \overline{\gamma}$, we have

$$2\,\mathrm{h}(r) = \mathrm{h}(r^2) = \mathrm{h}(\gamma \cdot \overline{\gamma}) \leq \mathrm{h}(\gamma) + \mathrm{h}(\overline{\gamma}) = 2\,\mathrm{h}(\gamma),$$

so $\mathrm{h}(r) \leq \mathrm{h}(\gamma)$. Thus, by Liouville's inequality we have

$$|\Lambda| = |b_1 i\pi - b_2 i\theta - b_2 \log r| \geq |\log r| \geq 2^{-D} \exp\left(-D\,\mathrm{h}(\gamma)\right),$$

and the lemma follows by Lemma 1 and the fact that $\mathrm{h}(\gamma) \geq \log 2$ if $D = 1$.

We now turn to the case of $|\gamma| = 1$. Since γ is not a root of unity, $D \geq 2$.

To obtain our lower bound for $|\Lambda|$ in this case we will use Théorème 3 of [8]. However, this result requires that b_1 and b_2 be non-zero, so we must deal specially with the case of $b_1 = 0$.

By Liouville's inequality and Lemma 1,

$$\begin{aligned}|\Lambda| \geq |b_2 \log\gamma| \geq |\log\gamma| \geq 2^{-D}\exp(-D\,\mathrm{h}(\gamma)) \geq \\ \geq \exp\left(-2D^2(\log(3D))^3\,\mathrm{h}(\gamma)\right).\end{aligned}$$

It is now clear that the lemma holds in this case.

To obtain a good constant in our lower bound we show that we may assume $B > 679000$. From Liouville's inequality, we obtain

$$|\Lambda| \geq 2^{-D/2} \exp\left(-\frac{DB\,\mathrm{h}(\gamma)}{2}\right).$$

We can use $D/2$ here instead of D since $\gamma \notin \mathbb{R}$ (see Exercise 3.4 of [18]).

So the lemma is true whenever

$$81.9D^2(\log(3D))^3(\log B)^2 - \frac{B}{2} \geq \frac{\log 2}{2\,\mathrm{h}(\gamma)}.$$

Since $D \geq 2$, applying Lemma 1, this inequality holds if

$$\frac{81.9(\log B)^2}{B} - 0.02174 \geq \frac{0.087}{B}.$$

Using Maple, one can check that this is true for $2 \leq B \leq 679000$.

We now invoke Théorème 3 of [8]. Let $a = \max\{20, 12.85|\log\gamma| + D\,\mathrm{h}(\gamma)/2\}$ and $H = \max\{17, D\log(b_1/(2a) + b_2/(25.7\pi))/2 + 2.3D + 3.25\}$. Then

$$\log|\Lambda| \geq -9aH^2. \tag{1}$$

Since $a \geq 20$ and $1/(2a)+1/(25.7\pi) < 0.0374$, $H \leq \max\{17, (D/2)\log B + 0.657D + 3.25\}$. Moreover, $B > 679000$ implies that $(D/2)\log B + 0.657D + 3.25 < 0.66994 D\log B$. As this last quantity is greater than 17 for $B > 679000$, we have $H < 0.66994 D\log B$.

We also want an upper bound for a in terms of D and $\mathrm{h}(\gamma)$. First notice that $|\log\gamma| \leq \pi$. Therefore, $12.85|\log\gamma| + D\,\mathrm{h}(\gamma)/2 \leq D\,\mathrm{h}(\gamma)(40.37/(D\,\mathrm{h}(\gamma)) + 1/2)$. Since $D \geq 2$, we can apply Lemma 1. We obtain $40.37/(D\,\mathrm{h}(\gamma)) + 1/2 < 20.185(\log(3D))^3 + 1/2 < 20.272(\log(3D))^3$. Therefore, $12.85|\log\gamma| + D\,\mathrm{h}(\gamma)/2 < 20.272(\log(3D))^3 D\,\mathrm{h}(\gamma)$ for all $D \geq 2$. Moreover, this quantity is greater than 20, so $a < 20.272(\log(3D))^3 D\,\mathrm{h}(\gamma)$.

Applying these estimates to (1), we find that our lemma holds. $\square$

Suppose that α and β are algebraic integers in a number field $\mathbb{K}$ of degree d over $\mathbb{Q}$. Letting $\mathbb{K}_1 = \mathbb{Q}(\beta/\alpha)$, a number field of degree d_1 over $\mathbb{Q}$, we set $\beta/\alpha = \beta_1/\alpha_1$, where α_1 and β_1 are algebraic integers in $\mathbb{K}_1$ and $(\alpha_1, \beta_1) = \mathcal{A}_1$. We may assume, without loss of generality, that $|\alpha_1| \geq |\beta_1|$.

We note that, unless we state otherwise, $\log z$ shall always denote the principal branch of the logarithmic function.

Now let us prove:

Lemma 3. *(i) We have*

$$\log 2 + \log|\alpha_1| \geq \log|\alpha_1 - \beta_1| \geq \log|\alpha_1| - d_1(\mathrm{h}(\beta_1/\alpha_1) + \log 2).$$

(ii) For $d_1 \geq 2$ and $n \geq 2$, we have

$$\begin{aligned}\log 2 + n\log|\alpha_1| &\geq \log|\alpha_1^n - \beta_1^n| \\ &\geq n\log|\alpha_1| - 81.97(d_1\log(3d_1))^3\,\mathrm{h}(\beta_1/\alpha_1)(\log n)^2.\end{aligned}$$

Proof. (i) We can write $\alpha_1 - \beta_1 = \alpha_1(1-\beta_1/\alpha_1)$. By Liouville's inequality,

$$\log|\beta_1/\alpha_1 - 1| \geq -d_1(\log 2 + \mathrm{h}(\beta_1/\alpha_1)),$$

and the result follows.

(ii) The upper bound follows directly from the triangle inequality and our assumption that $|\alpha_1| \geq |\beta_1|$.

For the lower bound we write the quantity in question as

$$n\log|\alpha_1| + \log|(\beta_1/\alpha_1)^n - 1|.$$

Applying Lemma 2.3 of [10] with $r = 1/3$ and $z = n\log(\beta_1/\alpha_1)$, we see that either

$$|(\beta_1/\alpha_1)^n - 1| > \frac{1}{3}$$

or

$$|\Lambda| = |n\log(\beta_1/\alpha_1) - 2k\pi i| < 1.3\,|(\beta_1/\alpha_1)^n - 1| < 0.5.$$

In the first case, the lemma holds so we need only consider the second case. Here, we must have

$$|\mathrm{Im}(n\log(\beta_1/\alpha_1)) - 2k\pi| < 0.5.$$

Since we took the principal value of the logarithm of β_1/α_1, we have $-\pi < \mathrm{Im}(\log(\beta_1/\alpha_1)) \leq \pi$ and so $|k| < n/2 + 0.5/(2\pi)$ or $|2k| \leq n$.

As β_1/α_1 is, by assumption, not a root of unity, $\Lambda \neq 0$ and, since $n \geq 2$, we may apply Lemma 2 giving

$$|\Lambda| > \exp\left(-81.9(d_1\log(3d_1))^3\,\mathrm{h}(\beta_1/\alpha_1)(\log n)^2\right).$$

By Lemma 1, we have $\log(1.3) < 0.07((d_1\log(3d_1))^3\,\mathrm{h}(\beta_1/\alpha_1)\log^2 n$, since $d_1 \geq 2$ and $n \geq 2$. Our lemma follows. $\square$

Lemma 4. *Let $\Phi_n(X,Y) = Y^{\varphi(n)}\phi_n(X/Y)$ where $\phi_n(X)$ is the n-th order cyclotomic polynomial. Suppose that $\mathcal{P}$ is a prime ideal in $\mathbb{K}$ which divides $(\Phi_n(\alpha,\beta))$ for $n > 2(2^{d_1}-1)$. This implies that $\mathcal{P}$ divides $(\alpha^n - \beta^n)$. If, in addition, $\mathcal{P}$ divides $(\alpha^m - \beta^m)$ for some $m < n$, then*

$$\mathrm{ord}_{\mathcal{P}}\,\Phi_n(\alpha,\beta) \leq \mathrm{ord}_{\mathcal{P}}\, n.$$

Proof. This is Lemma 4 of [13]. $\square$

Finally we need to bound some arithmetic functions which will appear throughout this article.

Lemma 5. *(i) Let $\omega(n)$ denote the number of distinct prime factors of n. For $n \geq 3$,*

$$\omega(n) < \frac{1.3841 \log n}{\log\log n}.$$

(ii) *For $n \geq 3$,*

$$\varphi(n) \geq \frac{n}{e^{\gamma} \log\log n + 2.50637/\log\log n},$$

where $\gamma = 0.57721\ldots$ is Euler's constant.

Proof. (i) This follows from Théorème 11 of [11].

(ii) This is Theorem 15 of [12]. □

3. Proof of Theorem 2

We may assumethat $d_1 \geq 2$, for otherwise we can write $\alpha = \beta c_1/c_2$ where $c_1, c_2 \in \mathbb{Z}$ with $(c_1, c_2) = 1$ and so $\alpha^n - \beta^n = (c_1^n - c_2^n)(\beta/c_2)^n$. Now Zsigmondy [20] and, independently of him, Birkhoff and Vandiver [2] have shown that for $n > 6$ the n-th element of such sequences always has a primitive divisor.

Therefore, we may also assume that $n > 3900(2\log(3\cdot 2))^{12} 11.74 \cdot 10^{10}$, since Theorem 2 does not apply for smaller n when $d_1 \geq 2$.

We note that

$$\Phi_n(\alpha,\beta) = \beta^{\varphi(n)}\Phi_n(\alpha/\beta, 1) = \beta^{\varphi(n)}\Phi_n(\alpha_1/\beta_1, 1) = (\beta/\beta_1)^{\varphi(n)}\Phi_n(\alpha_1,\beta_1).$$

Letting $\mathcal{A}$ be the extension of $\mathcal{A}_1$ in $\mathbb{K}$, we have $(\beta/\beta_1) = \mathcal{A}^{-1}$, since $(\alpha,\beta) = (1)$, and so

$$\begin{aligned}(d_1/d)\log\left|N_{K/Q}\left(\Phi_n(\alpha,\beta)\right)\right| &= \log\left|N_{K_1/Q}\left(\Phi_n(\alpha_1,\beta_1)\right)\right| \\ &\quad - \varphi(n)\log N_{K_1/Q}\left(\mathcal{A}_1\right).\end{aligned} \tag{2}$$

Since

$$\Phi_n(\alpha_1,\beta_1) = \prod_{m|n} (\alpha_1^m - \beta_1^m)^{\mu(n/m)},$$

the right-hand side of (2) is

$$\left(\sum_{v\in M_\infty(K_1)} \sum_{m|n} \mu(n/m)\log|\alpha_1^m - \beta_1^m|_v\right) - \varphi(n)\log N_{K_1/Q}\left(\mathcal{A}_1\right),$$

where $M_\infty(\mathbb{K}_1)$ denotes the set of all Archimedean absolute values defined on $\mathbb{K}_1$ up to equivalence.

Applying Lemma 3, we see that the inner sum in the first term of this expression is at least

$$\log\{\max(|\alpha_1|_v, |\beta_1|_v)\} \sum_{m|n} \mu(n/m)m - \sum_{\substack{m|n, m>1 \\ \mu(n/m)=-1}} \log 2 -$$
$$- 81.97(d_1 \log(3d_1))^3 \operatorname{h}(\beta_1/\alpha_1) \sum_{\substack{m|n, m>1 \\ \mu(n/m)=1}} (\log m)^2 - d_1(\operatorname{h}(\beta_1/\alpha_1) + \log 2).$$

Combining this lower bound with

$$\sum_{v \in M_\infty(K_1)} \log\max(|\alpha_1|_v, |\beta_1|_v) - \log N_{K_1/Q}(\mathcal{A}_1) = \operatorname{h}(\beta_1/\alpha_1)$$

and

$$\sum_{m|n} m\mu(n/m) = \varphi(n),$$

we obtain

$$\begin{aligned}(d_1/d)\log\left|N_{K/Q}(\Phi_n(\alpha,\beta))\right| \geq {} & \varphi(n)\operatorname{h}(\beta_1/\alpha_1) \\ & - 81.97 d_1^4 (\log(3d_1))^3 \operatorname{h}(\beta_1/\alpha_1) \sum_{\substack{m|n \\ \mu(n/m)=1}} (\log m)^2 \\ & - \sum_{\substack{m|n \\ \mu(n/m)=-1}} d_1 \log 2 - d_1^2(\operatorname{h}(\beta_1/\alpha_1) + \log 2).\end{aligned}$$

Notice that n has $2^{\omega(n)-1}$ factors m which satisfy $\mu(n/m) = 1$ and the same number of factors m satisfying $\mu(n/m) = -1$. Now, by Lemma 1 and our lower bound for n,

$$\begin{aligned} d_1^2(\operatorname{h}(\beta_1/\alpha_1) + \log 2) + \sum_{\substack{m|n \\ \mu(n/m)=-1}} d_1 \log 2 < {} & \\ < 0.005 \cdot 2^{\omega(n)} d_1^4 (\log(3d_1))^3 \operatorname{h}(\beta_1/\alpha_1) \log^2 n. & \end{aligned}$$

Thus

$$(3) \qquad (d_1/d)\log\left|N_{K/Q}\left(\Phi_n(\alpha,\beta)\right)\right| >$$

$$> \varphi(n)\,\mathrm{h}(\beta_1/\alpha_1) - 2^{\omega(n)}40.99 d_1^4(\log(3d_1))^3\,\mathrm{h}(\beta_1/\alpha_1)(\log n)^2,$$

for $d_1 \geq 2$ and $n \geq 1.74 \cdot 10^{10}$.

By Lemma 4, if $\left|N_{K/Q}\left(\Phi_n(\alpha,\beta)\right)\right| > n^d$, then there exists a prime ideal $\mathcal{P}$ which divides $(\alpha^n - \beta^n)$ but does not divide $(\alpha^m - \beta^m)$ for any $m < n$. Using (3) and Lemma 1, as well as our assumptions that $d_1 \geq 2$ and $n > 1.74 \cdot 10^{10}$, this condition is satisfied if

$$(4) \qquad \frac{\varphi(n)}{2^{\omega(n)}(\log n)^2} > 441 d_1^4(\log(3d_1))^3.$$

From Lemma 5, we find that

$$\frac{\varphi(n)}{2^{\omega(n)}(\log n)^2} > n^{0.3495},$$

for such n. Therefore, (4) is satisfied for

$$n > 41200 d_1^{11.45}(\log(3d_1))^{8.59}.$$

Since $d_1 \geq 2$, part (i) of the theorem holds.

(ii) Let $(u_n)_{n=0}^{\infty}$ be a Lucas or Lehmer sequence generated by α and β. Since $\alpha\beta$ and $(\alpha+\beta)^2$ are relatively prime non-zero rational integers, there exist two integers p and q such that α and β are the two roots of $X^2 - \sqrt{p+2q}X + q$. Therefore, $\alpha, \beta = (\sqrt{p+2q} \pm \sqrt{p-2q})/2$ and so either α/β or β/α is equal to $(p + \sqrt{p^2 - 4q^2})/(2q)$. Therefore we can take $d_1 = 2$ and so part (i) of theorem implies part (ii). $\square$

4. Preliminary Lemmas to Theorem 1

Lemma 6. *Let a be a non-negative real number. If $x, y \in \mathbb{R}$ with $-1 \leq x, y \leq 1$ and $|x - y| \leq a$ then*

$$|\arccos x - \arccos y| \leq \pi\sqrt{\frac{a}{2}}.$$

Proof. This result follows from finding the minimum value of the function

$$f(x,y) = \frac{\cos x - \cos y}{(x-y)^2}$$

on the area in $\mathbb{R}^2$ defined by $0 \le x, y \le \pi$, $x \ne y$ which is $2/\pi^2$ and then applying the contrapositive. □

Let us collect here various notations which we shall use throughout the remainder of this article.

Notations. Given a complex-valued function f defined on $\mathbb{C}$, we use $|f|_1$ to denote $\max_{|x|=1} |f(x)|$.

For a positive integer n, we let $g_n(X) \in \mathbb{Z}[X]$ be the minimal polynomial of $2\cos(2\pi/n)$ over $\mathbb{Z}$; its degree is $\varphi(n)/2$ if $n \ge 3$. We shall put $G_n(X,Y) = Y^{\varphi(n)/2} g_n(X/Y)$.

We let m be the greatest odd square-free divisor of n. For such m, we shall write $h_m(X) = (X^m - 1)/\phi_m(X)$.

Finally, for $n > 1$, we let $\mathrm{P}(n)$ denote the largest prime divisor of n.

As we shall see in Section 5, the crucial result needed in the proof of Theorem 1 is a good lower bound for $|g_n'(2\cos(2\pi j/n))|$ for $(j,n) = 1$.

We will show that we need to obtain an upper bound for the absolute value of $h_m(X)$ on the unit circle which we find using an idea and a result of Bateman, Pomerance and Vaughan [1].

Let us start linking these two polynomials now.

Lemma 7. *Let $n \ge 3$, $1 \le j \le n$ with $(j,n) = 1$ and $\zeta_n = \exp(2\pi i/n)$. Then*

$$|g_n'(2\cos(2\pi j/n))| = \left| \frac{\phi_n'(\zeta_n^j)}{2\sin(2\pi j/n)} \right|.$$

Proof. We can write

$$\begin{aligned} \phi_n(X) &= \prod_{\substack{1 \le j < n/2 \\ (j,n)=1}} \left(X - \zeta_n^j\right)\left(X - \zeta_n^{-j}\right) = \prod_{\substack{1 \le j < n/2 \\ (j,n)=1}} \left(X^2 - (\zeta_n^j + \zeta_n^{-j})X + 1\right) \\ &= \prod_{\substack{1 \le j < n/2 \\ (j,n)=1}} \left(X^2 + 1 - 2\cos(2\pi j/n)X\right) = g_n\left(\frac{X^2+1}{X}\right) X^{\varphi(n)/2}. \end{aligned}$$

If $Y = (X^2+1)/X$ then $X = (Y \pm \sqrt{Y^2-4})/2 = f(Y)$ and so

$$g_n(Y) = \frac{\phi_n(f(Y))}{f(Y)^{\varphi(n)/2}} \quad \text{and}$$
$$g_n'(Y) = \frac{2f(Y)\phi_n'(f(Y))f'(Y) - \phi_n(f(Y))\varphi(n)f'(Y)}{2f(Y)^{\varphi(n)/2+1}}.$$

Since $f(2\cos(2\pi j/n)) = \cos(2\pi j/n) \pm i\sin(2\pi j/n)$,

$$g_n'(2\cos(2\pi j/n)) = \frac{\phi_n'(\cos(2\pi j/n) \pm i\sin(2\pi j/n))f'(2\cos(2\pi j/n))}{(\cos(2\pi j/n) \pm i\sin(2\pi j/n))^{\varphi(n)/2}}.$$

Notice that $f'(Y) = (1 \pm Y/\sqrt{Y^2-4})/2$ so that

$$f'(2\cos(2\pi j/n)) = \frac{1}{2}\left(1 \pm i\frac{\cos(2\pi j/n)}{\sin(2\pi j/n)}\right).$$

Hence,

$$|g_n'(2\cos(2\pi j/n))| = \frac{\left|\phi_n'(\zeta_n^j)\right|\sqrt{1+\cot^2(2\pi j/n)}}{2}$$

from which the lemma follows. □

To work with the cyclotomic polynomials we shall need some relationships which they satisfy. We give these in the next lemma.

LEMMA 8. *(i) Let n be a positive integer and let m be its greatest odd square-free divisor. We put $m' = \gcd(2,n)m$. Then*

$$\phi_n(X) = \phi_m\left((-1)^{m'+1}X^{n/m'}\right).$$

(ii) *Let p be a prime number and n any positive integer not divisible by p. Then*

$$\phi_{pn}(X) = \frac{\phi_n(X^p)}{\phi_n(X)}.$$

(iii) *Let m, m' and n be as above. We put $n' = n/\gcd(n,2), h_m(X) = (X^m-1)/\phi_m(X)$ and $\zeta_n = \exp(2\pi i/n)$. Then, for all j with $(j,n) = 1$, we have*

$$\left|\phi_n'(\zeta_n^j)\right| = \frac{n'}{|h_m((-1)^{m'+1}\zeta_{m'}^j)|}.$$

Proof. (i) This assertion follows easily from the two relations:

$$\phi_{2t}(X) = \phi_t(-X) \quad \text{and} \quad \phi_n(X) = \phi_{m'}\left(X^{n/m'}\right),$$

which are parts (iv) and (vi) of Proposition 5.16 from Chapter 2 of Karpilovsky's book [7].

(ii) This is again from Proposition 5.16 from Chapter 2 of [7].

(iii) Applying part (i), we find that

$$\phi_n'(\zeta_n^j) = \frac{(-1)^{m'+1}\zeta_n^{(n/m')-1} n\phi_m'\left((-1)^{m'+1}\zeta_{m'}^j\right)}{m'}.$$

Now $X^m - 1 = h_m(X)\phi_m(X)$ so $mX^{m-1} = h_m(X)\phi_m'(X) + h_m'(X)\phi_m(X)$. Letting $X = (-1)^{m'+1}\zeta_{m'}^j$, which is always a primitive m-th root of unity, we have $(-1)^{(m-1)(m'+1)} m\zeta_{m'}^{j(m-1)} = h_m((-1)^{m'+1}\zeta_{m'}^j)\phi_m'((-1)^{m'+1}\zeta_{m'}^j)$ and the result follows. □

We see now that we have reduced the problem of bounding $|g_n'|$ from below for primitive n-th roots of unity to bounding $|h_m|_1$ from above. To deal with this new problem, we shall now use ideas from [1].

Lemma 9. *Let $m = p_1 \dots p_k$ where $p_1, p_2, \dots, p_k$ are odd primes arranged in increasing order. Then*

$$|h_m(X)|_1 \le 2\prod_{i=1}^{k-1} p_i^{2^{k-i-1}}.$$

In fact, if $k \ge 3$ then the factor of 2 is not needed.

Proof. From Lemma 8(ii),

$$h_m(X) = \frac{(X^m - 1)\phi_{p_1 \dots p_{k-1}}(X)}{\phi_{p_1 \dots p_{k-1}}(X^{p_k})} = h_{p_1 \dots p_{k-1}}(X^{p_k})\phi_{p_1 \dots p_{k-1}}(X). \tag{5}$$

We now use induction on k to prove the lemma.

Since $h_1(X) = 1, h_{p_1}(X) = X - 1$ and $h_{p_1 p_2}(X) = (X^{p_2} - 1)\phi_{p_1}(X)$, the lemma is true for $k \le 2$.

For $k = 3$, we have $|h_{p_1p_2p_3}|_1 \leq |h_{p_1p_2}|_1 |\phi_{p_1p_2}|_1$. Using the result just established for $k = 2$ and a theorem of Carlitz [3] which shows that $|\phi_{p_1p_2}|_1 < p_1p_2/2$, we obtain $|h_{p_1p_2p_3}|_1 < p_1^2 p_2$. This is the desired inequality for $k = 3$.

Suppose now that the lemma holds for some $k \geq 3$. We apply the following estimate of Bateman, Pomerance and Vaughan, which follows from Theorem 1 of their paper [1] and holds for $k \geq 3$,

$$|\phi_{p_1\dots p_k}|_1 < p_k \prod_{i=1}^{k-1} p_i^{2^{k-i-1}}.$$

Thus from (5), we have

$$|h_{p_1\dots p_{k+1}}|_1 \leq |h_{p_1\dots p_k}|_1 |\phi_{p_1\dots p_k}|_1 < \prod_{i=1}^{k-1} p_i^{2^{k-i-1}} \times p_k \prod_{i=1}^{k-1} p_i^{2^{k-i-1}} = \prod_{i=1}^{k} p_i^{2^{k-i}}.$$

Hence the lemma holds. $\square$

We need the next lemma to deal with the case $q = 2$, although we will use it for all q. A simple application of the triangle inequality would quickly yield the inequality below with $3|q|/5$ replaced by $|q|/2$. However, in the case of $q = 2$, this would not be sufficient to prove our theorem: with the lower bound that the previous lemmas imply for $|g_n'(2\cos(2\pi k/n))|$, the upper bound we would obtain for the left-hand side of (11) would not decrease with n but actually grow with n. To refine this trivial estimate, it seems we must resort to an argument like the one which follows.

Lemma 10. *Let $n > 30$ be a positive integer and let p and q be non-zero integers with $q \geq 2, |p| < 2q$ and*

$$|G_n(p,q)| \leq \mathrm{P}(n/(n,3)).$$

For $1 \leq j < n/2$ with $(j,n) = 1$, we put $\beta_n^{(j)} = p - 2q\cos(2\pi j/n)$. Define k by $|\beta_n^{(k)}| = \min_{\substack{j=1\dots n/2 \\ (j,n)=1}} |\beta_n^{(j)}|$. Then

$$\left| \prod_{\substack{j=1 \\ j\neq k,(j,n)=1}}^{n/2} \beta_n^{(j)} \right| > \frac{(3|q|/5)^{\varphi(n)/2} |g_n'(2\cos(2\pi k/n))|}{|q|}.$$

Proof. We first divide the interval $(-2,2)$ into four subintervals and divide the set of integers less than $n/2$ which are relatively prime to n into four associated subsets. Let $\mathcal{A}=(-2,-1), \mathcal{A}'=\{m : n/3<m<n/2, (m,n)=1\}, \mathcal{B}=(-1,0), \mathcal{B}'=\{m : n/4<m<n/3, (m,n)=1\}, \mathcal{C}=(0,1), \mathcal{C}'=\{m : n/6<m<n/4, (m,n)=1\}, \mathcal{D}=(1,2)$ and $\mathcal{D}'=\{m : 0<m<n/6, (m,n)=1\}$. If we let $\varphi(k,q,n)$ denote the number of integers in the interval $(nq/k, n(q+1)/k)$ which are relatively prime to n then $|\mathcal{A}'|=\varphi(6,2,n)=\varphi(n)/2-\varphi(3,0,n), |\mathcal{B}'|=\varphi(3,0,n)-\varphi(4,0,n), |\mathcal{C}'|=\varphi(4,0,n)-\varphi(6,0,n)$ and $|\mathcal{D}'|=\varphi(6,0,n)$.

Using Theorems 5–7 of [9], we have the following inequalities for the cardinalities of these sets of integers:

$$\begin{aligned}
\frac{\varphi(n)-2^{\omega(n)}}{6} &\le |\mathcal{A}'| \le \frac{\varphi(n)+2^{\omega(n)}}{6}\\
\frac{\varphi(n)-3\cdot 2^{\omega(n)}}{12} &\le |\mathcal{B}'| \le \frac{\varphi(n)+3\cdot 2^{\omega(n)}}{12}\\
\frac{\varphi(n)-4\cdot 2^{\omega(n)}}{12} &\le |\mathcal{C}'| \le \frac{\varphi(n)+4\cdot 2^{\omega(n)}}{12}\\
\frac{\varphi(n)-2\cdot 2^{\omega(n)}}{6} &\le |\mathcal{D}'| \le \frac{\varphi(n)+2\cdot 2^{\omega(n)}}{6}.
\end{aligned} \tag{6}$$

Let us observe that $p/q \in \mathcal{A}\cup\mathcal{B}\cup\mathcal{C}\cup\mathcal{D}$ and

$$\left|\prod_{\substack{j=1\\ j\ne k,(j,n)=1}}^{n/2} \beta_n^{(j)}\right| = \left|\prod_{\substack{j=1\\ j\ne k,(j,n)=1}}^{n/2} \left(1-\frac{\beta_n^{(k)}}{\beta_n^{(j)}}\right)^{-1}\right| \left|g_n'(2\cos(2\pi k/n))\right|. \tag{7}$$

If $p/q \in \mathcal{A}$ then $p \le -3$, since $q \ge 2$, and either $k \in \mathcal{A}'$ or k is the largest element of $\mathcal{B}'$. Thus, $\beta_n^{(j)} > 3+4\cos(2\pi j/n)$ for each $j \in \mathcal{C}'\cup\mathcal{D}'$ and so

$$\left|\beta_n^{(k)}\right| \le c_1 = \left(\mathrm{P}(n/(n,3)) \prod_{j\in\mathcal{C}'\cup\mathcal{D}'} (3+4\cos(2\pi j/n))^{-1}\right)^{1/(\varphi(n)/2-|\mathcal{C}'|-|\mathcal{D}'|)}.$$

Combining these inequalities with (7), we obtain

$$\left|\prod_{\substack{j=1\\ j\ne k,(j,n)=1}}^{n/2} \beta_n^{(j)}\right| \ge$$

$$\geq \frac{|q|^{\varphi(n)/2-1}}{2^{|\mathcal{A}'|+|\mathcal{B}'|}} \prod_{j \in \mathcal{C}' \cup \mathcal{D}'} \left(1 + \frac{c_1}{3 + 4\cos(2\pi j/n)}\right)^{-1} |g_n'(2\cos(2\pi k/n))|.$$

Now suppose that $p/q \in \mathcal{B}$. If $\beta_n^{(k)} < 0$ then $\beta_n^{(j)} < 0$ for $j \in \mathcal{C}' \cup \mathcal{D}'$, so $|1 - \beta_n^{(k)}/\beta_n^{(j)}| \leq 1$ for such j and

$$\left| \prod_{\substack{j=1 \\ j \neq k, (j,n)=1}}^{n/2} \beta_n^{(j)} \right| \geq \frac{|q|^{\varphi(n)/2-1}}{2^{|\mathcal{A}'|+|\mathcal{B}'|}} |g_n'(2\cos(2\pi k/n))|.$$

Since the quantity before $|g_n'(2\cos(2\pi k/n))|$ on the right-hand side of this expression is at least as large as the similar quantity obtained for $p/q \in \mathcal{A}$, we can ignore this case.

If $\beta_n^{(k)} > 0$ then $|1 - \beta_n^{(k)}/\beta_n^{(j)}| \leq 1$ for $j \in \mathcal{A}'$ so a similar analysis to that above shows that

$$\left|\beta_n^{(k)}\right| \leq c_2 = \left(\mathrm{P}(n/(n,3)) \prod_{j \in \mathcal{D}'} (1 + 4\cos(2\pi j/n))^{-1} \right)^{1/(\varphi(n)/2 - |\mathcal{D}'|)}$$

and

$$\left| \prod_{\substack{j=1 \\ j \neq k, (j,n)=1}}^{n/2} \beta_n^{(j)} \right| \geq$$

$$\geq \frac{|q|^{\varphi(n)/2-1}}{2^{|\mathcal{B}'|+|\mathcal{C}'|}} \prod_{j \in \mathcal{D}'} \left(1 + \frac{c_2}{1 + 4\cos(2\pi j/n)}\right)^{-1} |g_n'(2\cos(2\pi k/n))|.$$

If $p/q \in \mathcal{C}$ then, by the same reasoning, we obtain

$$\left|\beta_n^{(k)}\right| \leq c_3 = \left(\mathrm{P}(n/(n,3)) \prod_{j \in \mathcal{A}'} (1 - 4\cos(2\pi j/n))^{-1} \right)^{1/(\varphi(n)/2 - |\mathcal{A}'|)}$$

and

$$\left| \prod_{\substack{j=1 \\ j \neq k, (j,n)=1}}^{n/2} \beta_n^{(j)} \right| \geq$$

$$\geq \frac{|q|^{\varphi(n)/2-1}}{2^{|\mathcal{B}'|+|\mathcal{C}'|}} \prod_{j\in\mathcal{A}'} \left(1+\frac{c_3}{1-4\cos(2\pi j/n)}\right)^{-1} |g_n'(2\cos(2\pi k/n))|.$$

If $p/q \in \mathcal{D}$, then

$$\left|\beta_n^{(k)}\right| \leq c_4 = \left(\mathrm{P}(n/(n,3)) \prod_{j\in\mathcal{A}'\cup\mathcal{B}'} (3-4\cos(2\pi j/n))^{-1}\right)^{1/(\varphi(n)/2-|\mathcal{A}'|-|\mathcal{B}'|)}$$

and

$$\left|\prod_{\substack{j=1\\ j\neq k,(j,n)=1}}^{n/2} \beta_n^{(j)}\right| \geq$$

$$\geq \frac{|q|^{\varphi(n)/2-1}}{2^{|\mathcal{C}'|+|\mathcal{D}'|}} \prod_{j\in\mathcal{A}'\cup\mathcal{B}'} \left(1+\frac{c_4}{3-4\cos(2\pi j/n)}\right)^{-1} |g_n'(2\cos(2\pi k/n))|.$$

For $n \leq 210, n=231$ and $n=462$, we can use these estimates to show by direct calculation that our lemma holds.

To deal with $n>210$, we first show that $\max(c_1,c_2,c_3,c_4)<1$ for such n. Using the above expressions for these quantities we see that this holds if $\min(3^{|\mathcal{A}'|}, 3^{|\mathcal{D}'|}) > n$. By (6), both $|\mathcal{A}'|$ and $|\mathcal{D}'|$ are at least $\varphi(n)/6-2^{\omega(n)}/3$, so we need only prove that $(\varphi(n)-2\cdot 2^{\omega(n)})(\log 3) > 6\log n$ for $n>210$.

For $210 < n < 330 = 2\cdot 3\cdot 5\cdot 11$, $2^{\omega(n)} \leq 8 < n^{0.389}$. Lemma 5(ii) yields the lower bound $\varphi(n) > n^{0.719}$ for $n \geq 210$. Since $\log n < n^{0.314}$ for $n>210$, we need only show that $n^{0.075}(n^{0.33}-2)\log 3 > 6$ for n in this range. But this is easily seen to be true.

For $330 \leq n < 2310 = 2\cdot 3\cdot 5\cdot 7\cdot 11$, $2^{\omega(n)} \leq 16 < n^{0.48}$. Moreover, by Lemma 5(i), for $n \geq 2310$, $2^{\omega(n)} < n^{0.9594/\log\log n} < n^{0.47}$. Therefore, for $n \geq 330$, $2^{\omega(n)} < n^{0.48}$. Applying Lemma 5(ii) again, we find that $\varphi(n) > n^{0.73}$ for $n \geq 330$. Since $\log n < n^{0.31}$ for $n \geq 330$, we need only show that $n^{0.17}(n^{0.25}-2)\log 3 > 6$ for n in this range which is also easily seen to be true. Therefore, $\max(c_1,c_2,c_3,c_4) < 1$.

So, from our lower bounds for the absolute values of the products of the $\beta_n^{(j)}$'s given above, to prove the lemma we need to show that

$$\max\Big(2^{|\mathcal{A}'|+|\mathcal{B}'|}(4/3)^{|\mathcal{C}'|+|\mathcal{D}'|}, 2^{|\mathcal{B}'|+|\mathcal{C}'|}(4/3)^{|\mathcal{D}'|}, 2^{|\mathcal{B}'|+|\mathcal{C}'|}(4/3)^{|\mathcal{A}'|},$$

$$2^{|\mathcal{C}'|+|\mathcal{D}'|}(4/3)^{|\mathcal{A}'|+|\mathcal{B}'|}\Big)$$

is less than $(5/3)^{\varphi(n)/2}$.

Let us first show that $2^{|\mathcal{A}'|}(2/3)^{|\mathcal{C}'|} \geq 1$ and $2^{|\mathcal{D}'|}(2/3)^{|\mathcal{B}'|} \geq 1$. These inequalities will show that either the first or the last terms give the maximum in this expression.

For the first of these two inequalities to be true, by (6) we need to show that $0.08\varphi(n) - 0.26 \cdot 2^{\omega(n)} \geq 0$. Similarly, the second inequality requires that the stronger inequality $0.08\varphi(n) - 0.34 \cdot 2^{\omega(n)} \geq 0$ holds. So we need only consider this last inequality which we shall rewrite in the form $0.08/0.34 \geq 2^{\omega(n)}/\varphi(n)$.

For $210 < n < 330$, we saw in a previous paragraph that $2^{\omega(n)}/\varphi(n) < n^{-0.33} < 0.171 < 0.08/0.34$. We also saw that $2^{\omega(n)}/\varphi(n) < n^{-0.25} < 0.235 < 0.08/0.34$ for $n \geq 330$. Therefore, our desired inequalities holds and we need only try to bound $2^{|\mathcal{A}'|+|\mathcal{B}'|}(4/3)^{|\mathcal{C}'|+|\mathcal{D}'|}$ and $2^{|\mathcal{C}'|+|\mathcal{D}'|}(4/3)^{|\mathcal{A}'|+|\mathcal{B}'|}$ from above.

Notice that $|\mathcal{A}' \cup \mathcal{B}'| = \varphi(4, 0, n)$ and that $|\mathcal{C}' \cup \mathcal{D}'| = \varphi(4, 1, n)$. Lehmer [9, p. 351] has noted that $E(4, 1, n) = -E(4, 0, n)$, where $E(k, q, n)$ denotes $\varphi(n) - k\varphi(k, q, n)$, so we need only examine

$$(8/3)^{\varphi(n)/4}(3/2)^{|E(4,0,n)|/4}.$$

Lehmer also gives precise information about $E(4, 0, n)$ in Theorem 6 of [9]. If $n > 4$ and 4 divides n or n is divisible by a prime congruent to 1 mod 4 then $E(4, 0, n) = 0$ and our proof is complete. If neither of these conditions is true then $|E(4, 0, n)| = 2^{\omega(n')}$ where n' is as in the statement of Lemma 8(iii). Notice that when $E(4, 0, n) \neq 0$, n is not

congruent to 0 mod 4, so n' is the odd part of n.

A direct calculation shows that for $210 < n < 750$, with the exceptions of $n = 231$ and 462 which we considered above, $|E(4, 0, n)|/\varphi(n) < 0.05$. Therefore, $(8/3)^{\varphi(n)/4}(3/2)^{|E(4,0,n)|/4} < (5/3)^{\varphi(n)/2}$ for $210 < n < 750, n \neq 231, 462$. Recalling that we showed by calculation that the lemma holds for $30 < n \leq 210$, for $n = 231$ and for $n = 462$, we now know that the lemma holds for $30 < n < 750$.

Notice that if $n < 4389 = 3{\cdot}7{\cdot}11{\cdot}19$ then either $|E(4, 0, n)| = 0$ or $2^{\omega(n')} \leq 8$, since in the latter case n' is odd and without prime divisors congruent to 1 mod 4. Using Lemma 5(ii), $\varphi(n) \geq 160$ and so $|E(4, 0, n)|/\varphi(n) < 0.05$ for $n \geq 750$ and our lemma holds for $30 < n < 4389$.

Applying the inequality $2^{\omega(n)} < n^{0.96/\log\log n}$, which follows from

Lemma 5(i), and part (ii) of this same lemma, we find that

$$\frac{2^{\omega(n)}/4}{\varphi(n)/4} < \frac{n^{0.96/\log\log n}(1.7811\log\log n + 2.51/\log\log n)}{n}.$$

The right-hand side is a monotone-decreasing function for $n \geq 10$ and so it is less than 0.05 for $n \geq 4389$. Therefore $(8/3)^{\varphi(n)/4}(3/2)^{|E(4,0,n)|/4} < (5/3)^{\varphi(n)/2}$ for $n \geq 4389$, which shows that the lemma is true. □

5. Proof of Theorem 1

Let $(u_n)_{n=0}^{\infty}$ be a Lucas or Lehmer sequence generated by α and β. As noted in the proof of Theorem 2, there exist two integers p and q such that α and β are the two roots of $X^2 - \sqrt{p+2q}X + q$. Notice that the n-th element of the sequence generated by $i\alpha$ and $i\beta$ is just $\pm u_n$. Therefore, we can assume that $q = \alpha\beta$ is positive. Also notice $|p| < 2q$ for otherwise α and β are real and Carmichael [4], Ward [19] and Durst [5] have shown that in this case the n-th element of these sequences has a primitive divisor for $n > 12$.

Let us define the $\beta_n^{(j)}$'s and $\beta_n^{(k)}$ as in Lemma 10. Stewart [14, Section 5] has shown that if the n-th element of this sequence has no primitive divisor then

$$|G_n(p,q)| = \prod_{\substack{1\leq j\leq n/2\\(j,n)=1}} \left|\beta_n^{(j)}\right| \leq \mathrm{P}(n/(n,3)) \text{ for } n > 12. \tag{10}$$

Since $|p| < 2q$, upon applying Lemma 10, we obtain

$$\left|\beta_n^{(k)}\right| \leq \frac{\mathrm{P}(n/(3,n))}{\prod_{\substack{1\leq j\leq n/2\\ j\neq k,(j,n)=1}} \left|\beta_n^{(j)}\right|} < \frac{(5/3)^{\varphi(n)/2}\,\mathrm{P}(n/(n,3))}{|g_n'(2\cos(2\pi k/n))||q|^{\varphi(n)/2-1}},$$

for $n > 30$.

Therefore, if we can show that

$$\left|\frac{p}{q} - 2\cos\left(\frac{2\pi k}{n}\right)\right| < \frac{(5/(3|q|))^{\varphi(n)/2}\,\mathrm{P}(n/(n,3))}{|g_n'(2\cos(2\pi k/n))|} < \frac{4}{n^4}, \tag{11}$$

then, by Lemma 10,

$$\left|\frac{1}{2\pi}\arccos\left(\frac{p}{2q}\right) - \frac{k}{n}\right| < \frac{1}{2n^2},$$

and so, by Theorem 184 of [6], k/n must be a convergent in the continued-fraction expansion of $\arccos(p/(2q))/(2\pi)$.

Hence we first want to show that for n sufficiently large, the right-hand inequality of (11) holds. We start by considering the case of $q = 2$, as this is the most difficult one.

5.1. The case $q = 2$

Using the notation of Lemmas 8 and 9, we find, from Lemma 9, that

$$|h_m(X)|_1 \leq m^{2^{k-1}/k} \leq n^{2^{\omega(n)-1}/\omega(n)},$$

for $m > 1$.

If $m = 1$, but $n > 1$, we have $|h_m(X)|_1 = 1 \leq n^{2^{\omega(n)-1}/\omega(n)}$.

Combining this upper bound with Lemmas 7 and 8(iii), we obtain

$$|g_n'(2\cos(2\pi k/n))| > \frac{n}{4n^{2^{\omega(n)-1}/\omega(n)}},$$

for $n > 1$.

Applying this lower bound to the right-hand inequality of (11) and squaring both sides, we want to show that

$$(5/6)^{\varphi(n)} n^{2^{\omega(n)}/\omega(n)} \leq \frac{1}{n^8},$$

for $n > 30$.

To prove that this holds for n sufficiently large, we take the logarithm of both sides, which yields

$$\varphi(n)\log(5/6) + 2^{\omega(n)}(\log n)/\omega(n) + 8\log n \leq 0.$$

From Lemma 5(ii), we see that $\varphi(n) > n^{0.8043}$ for $n \geq 3500$, while for the term involving $\omega(n)$ we use the fact that $2^x/x$ is a monotone increasing function for $x > 1/\log 2$, $2^1/1 = 2^2/2$ and Lemma 5(i). In this manner, our problem is to show that

$$-0.182n^{0.8043} + \frac{n^{0.96/\log\log n}\log\log n}{1.384} + 8\log n \leq 0.$$

For $n \geq 3500$, the sum of the second and third terms is at most $n^{0.5952}$. Therefore, we need only show that $-0.182n^{0.209} + 1 \leq 0$, but this is easily seen to be true for $n \geq 3500$. So we have an initial bound of intermediate size.

Notice though that we did not make full use of the Lemma 9 in this argument. A direct calculation on a computer using the result given in Lemmas 7,8(iii) and 9 shows that the right-hand inequality of (11) holds for all $n > 1260$ when $q = 2$.

In the case of $q = 2$, Lucas and Lehmer sequences can result from $p = -3, -1, 1$ and 3. Since $G_n(p,q)$ is a product of terms of the form $p - 2q\cos(2\pi i/n)$, it is quite easy to calculate $G_n(p,q)$, although care must be taken to maintain sufficient accuracy, and so we can check whether u_n has primitive divisors by means of (10). However, to check u_n for each n up to 1260 in this manner is quite time-consuming. Fortunately, one can quickly extract still more information from (11). Given n, p and q, it is easy to find the integer k with $(k, n) = 1$ which minimizes the far left-hand side of (11). As when considering $1260 < n < 3500$, we can bound from above the middle quantity in (11). For $q = 2, p = -3, -1, 1, 3$ and $330 < n \leq 1260$, we can verify in this way that the left-hand inequality in (11) is violated and so for such n, the n-th element of these sequences has a primitive divisor. But we still need to consider $30 < n \leq 330$. For these n, we use (10) as described earlier in this paragraph.

For $n > 1260$, we have seen that n must be the denominator of a convergent in the continued-fraction expansion for $\arccos(p/(2q))/(2\pi)$.

The question arises of how to deal with these n. We are fortunate that in these cases the middle quantity in (11) is extremely small. For such n, we proceed in the same manner that we checked the left-hand inequality in (11) holds for $330 < n \leq 1260$, except that now we know k too. Theorem 2 tells us that we need only check those convergents k/n with $n \leq 2 \cdot 10^{10}$. For each convergent computed with $n \leq 2 \cdot 10^{10}$, $|p/q - 2\cos(2\pi k/n)|$ was considerably larger than the bound that the left-hand inequality of (11) requires if u_n were to be without a primitive divisor. In Table 1, for $p = -3$, we list the convergents with $n > 1260$ and give the logarithms of the required and actual bounds, denoted d_{req} and d_{act}, respectively. The value of $\log|d_{\mathrm{req}}|$ given in Table 1 is truncated to its integer part, whereas the value of $\log|d_{\mathrm{act}}|$ is truncated to one decimal place.

Proceeding in this same way for $p = -1, 1$ and 3, we are able to conclude that if $(u_n)_{n=0}^{\infty}$ is the Lucas or Lehmer sequence generated by any of the pairs $(\alpha, \beta) = (1 \pm \sqrt{-7})/2, (\sqrt{3} \pm \sqrt{-5})/2, (\sqrt{5} \pm \sqrt{-3})/2$ or $(\sqrt{7} \pm \sqrt{-1})/2$, then u_n has a primitive divisor for $n > 30$.

k	n	$\log\lvert d_{\mathrm{req}}\rvert$	$\log\lvert d_{\mathrm{act}}\rvert$
497	1291	-116.	-12.6
579	1504	-68.	-13.7
1655	4299	-260.	-15.4
3889	10102	-459.	-18.9
52212	135625	-8207.	-22.1
56101	145727	-12970.	-22.4
108313	281352	-8086.	-24.3
381040	989783	-90228.	-26.1
489353	1271135	-90181.	-26.7
870393	2260918	-93683.	-28.3
2230139	5792971	-493472.	-29.5
3100532	8053889	-734197.	-30.8
8431203	21900749	-1745895.	-32.3
11531735	29954638	-1165244.	-33.1
19962938	51855387	-3104401.	-34.1
31494673	81810025	-5404005.	-35.2
51457611	133665412	-5943915.	-35.8
82952284	215475437	-19412834.	-38.5
798028167	2072944345	-144472147.	-41.8
1679008618	4361364127	-374075698.	-42.8
2477036785	6434308472	-293278284.	-44.3
6633082188	17229981071	-1438733756.	-45.4

Table 1: $(p, q) = (-3, 2)$ Verification

5.2. The case of $q > 2$

For such pairs (p, q), we proceed along the same lines. The only difference is that less work is required for small n. We already know that the right-hand inequality of (11) is satisfied for $n > 1260$ by our work in the previous section. We can check directly, as with $1260 < n < 3500$ for $q = 2$, that the right-hand inequality of (11) holds for $n_{q-1} \geq n > n_q$ where n_q is given in Table 2.

As in the case of $30 < n \leq 330$ for $q = 2$, we directly check those u_n with $30 < n \leq n_q$ for primitive divisors and for larger n we compare the required and actual differences of $|p/q - 2\cos(2\pi k/n)|$ in (11) to establish our result. The actual difference is less than the required difference for all $n_q < n \leq 2 \cdot 10^{10}$ and all $3 \leq q \leq 3000$ (this corresponds to all pairs of α and β with $\mathrm{h}(\beta/\alpha) \leq 4$). By Theorem 2, Theorem 1 now follows.

All the calculations in this article were performed using Release 3 of Maple V and UBASIC 8.74 on an IBM-compatible PC with an 486DX2 running at 66 MHz. In total, the calculations required just over 100 hours on this machine. Many of the calculations were performed using both systems to provide a check on the quantities obtained and the results were always identical up to the specified accuracy.

q	n_q
2	1260
3	330
4	210
5	120
6	90
7	78
8	66
9,10,11	60
$12,\ldots,20$	42
≥ 21	30

Table 2: Values of n_q

References

[1] P. T. Bateman, C. Pomerance and R. C. Vaughan,, *On the size of the coefficients of the cyclotomic polynomial*, Topics in Classical Number Theory,, (Budapest, 1981), Colloquia Mathematica Societatis Janos Bolyai, 34, North-Holland, New York, 1984.

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

[3] L. Carlitz, *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly **75** (1968), 372–377.

[4] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) **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*, Oxford University Press, 5th edition, 1978.

[7] G. Karpilovsky, *Field Theory: Classical Foundations and Multiplicative Groups*, Marcel Dekker, New York, 1988.

[8] M. Laurent, M. Mignotte and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory, to appear.

[9] D. H. Lehmer, *The distribution of totatives*, Canadian J. Math. **7** (1955), 347–357.

[10] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*, New Advances in Transcendence Theory (A. Baker, ed.), Cambridge University Press, Cambridge, 1988.

[11] 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. **XLII** (1983), 367–389.

[12] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

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

[14] C. L. Stewart, *Primitive divisors of Lucas and Lehmer sequences*, Transcendence Theory: Advances and Applications (A. Baker and D.W. Masser, eds.), Academic Press, New York, 1977.

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

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

[17] P. M. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith., (to appear).

[18] M. Waldschmidt, *Linear Independence of Logarithms of Algebraic Numbers*, IMSc Report No 116 (1992), The Institute of Mathematical Sciences, Madras.

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

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

Paul M. VOUTIER
Department of Mathematics
City University
Northampton Square
London, EC1V 0HB, UK
Dr.P.Voutier@city.ac.uk