CHAPTER 4

Primitive Divisors of Lucas and Lehmer Numbers

C. L. STEWART

Trinity College, Cambridge

1. INTRODUCTION

Let A and B be non-zero integers of an algebraic number field K of degree l. A prime ideal $\mathfrak{p}$ of K is called a primitive divisor of $A^n - B^n$ if $\mathfrak{p} \mid [A^n - B^n]$ and $\mathfrak{p} \nmid [A^m - B^m]$ for $0 < m < n$; here $[x]$ denotes the principal ideal generated by x in K. Schinzel [11] proved that if $([A], [B]) = 1$ and A/B is not a root of unity then $A^n - B^n$ has a primitive divisor for all $n > n_0(d)$ where d is the degree of A/B over Q and $n_0(d)$ is effectively computable. This extended earlier work of Postnikova and Schinzel [8]. By utilizing the contribution of Baker [3] which appears in this volume we are able to make the function $n_0(d)$ completely explicit. We prove:

THEOREM 1. *If* $([A], [B]) = 1$ *and* A/B *is not a root of unity then* $A^n - B^n$ *has a primitive divisor for all* $n > \max\{2(2^d - 1), e^{452}d^{67}\}$ *where* d *is the degree of* A/B.

Theorems of this nature were first established for the rational numbers by Bang [4], Zsigmondy [16] and Birkhoff and Vandiver [5]. In [5] and [16] it was shown that if a and b are coprime non-zero rational integers with $a \neq \pm b$ then $a^n - b^n$ has a primitive divisor for $n > 6$. (Bang dealt only with the case $b = 1$). Similar results have been obtained for the Lucas numbers $t_1, t_2, \ldots$ defined by

$$t_n = (\alpha^n - \beta^n)/(\alpha - \beta) \qquad \text{for } n > 0,$$

where $\alpha + \beta$ and $\alpha\beta$ are relatively prime non-zero integers (so that α, β are roots of a quadratic equation) and α/β is not a root of unity. A primitive divisor of t_n is a prime p which divides t_n but does not divide $(\alpha - \beta)^2 t_2 \dots t_{n-1}$.

In 1913 Carmichael [7] proved that if α and β are real then t_n has a primitive divisor for $n > 12$ and in 1955 Ward [15] proved the analogous result for the Lehmer numbers $u_1, u_2, \dots$ defined by

$$u_n = (\alpha^n - \beta^n)/(\alpha^\delta - \beta^\delta), \qquad n > 0,$$

where δ is 1 if n is odd and 2 if n is even, subject to the weaker condition that $(\alpha + \beta)^2$ and $\alpha\beta$ are relatively prime non-zero integers with α/β not a root of unity; a primitive divisor of a Lehmer number u_n is a prime p which divides u_n but not $(\alpha - \beta)^2(\alpha + \beta)^2 u_3 \dots u_{n-1}$. Some Lucas, similarly Lehmer, sequences have a number of terms which do not possess a primitive divisor. Carmichael [7] gives the example of the Lucas sequence generated by α and β where $\alpha + \beta = 1$ and $\alpha\beta = 2$. This sequence and the related Lehmer sequence have no primitive divisors for the terms with indices 1, 2, 3, 5, 7, 8, 12, 13 and 18.

In [11] Schinzel removed the restriction that α and β be real; he proved that all Lucas and Lehmer numbers have primitive divisors for n sufficiently large. We observe that as a consequence of Theorem 1 every Lucas number t_n with $n > e^{452}2^{67}$ possesses a primitive divisor; for the Lehmer numbers u_n the condition $n > e^{452}4^{67}$ is sufficient. In fact, we are able to improve upon the above results considerably. We prove

THEOREM 2. *There are only finitely many Lucas and Lehmer sequences whose* nth *term,* $n > 6$, $n \neq 8$, 10 *or* 12, *does not possess a primitive divisor and these sequences may be explicitly determined.*

We see immediately from Theorems 1 and 2 that all Lucas numbers t_n and Lehmer numbers u_n with $n > 6$, $n \neq 8$, 10 or 12 which do not have a primitive divisor are, in principle, explicitly computable. Such a computation, however, could only be effected in practice, subject to certain refinements in our estimates, with the aid of a modern computing machine.

We observe that one can prove, by reference to the fact that the p-adic analogue of the equation $y^2 = x^3 + k$ has only finitely many solutions in a fixed algebraic number field, that for the Lucas sequences the restriction $n > 6, n \neq 8$, 10 or 12 in Theorem 2 may be replaced by $n > 4, n \neq 6$. (Details will be supplied in a later note on the subject.) Theorem 2 is, however, a best possible result for Lehmer sequences. We have

THEOREM 3. *For each integer* $m \leqslant 12$, $m \neq 7, 9$ *or* 11, *there exist infinitely many Lehmer sequences* $\{u_n\}$ *for which* u_m *does not have a primitive divisor.*

We mention, finally, that results concerning primitive divisors of Lucas and Lehmer numbers have proved useful in the resolution of certain problems concerning Diophantine equations, for example the equation $x^2 + 7 = 2^n$; see [10] for references to work in this connexion.

2. PRELIMINARIES

Let $f(x, y)$ denote a homogeneous binary form with integer coefficients and assume that $f(x, 1)$ has at least three distinct roots. Further let m be a non-zero rational integer. Baker proved (see [1] and Theorem 4.1 of [2])

LEMMA 1. *If* $f(x, y) = m$ *for integers* x *and* y *then*

$$\max\{|x|, |y|\} < C_0,$$

where C_0 *is a number which is computable in terms of* m *and the coefficients of* f.

We now require a precise estimate from below for a special linear form in two logarithms. We shall deduce this from recent work of Baker [3]. Let α be an algebraic number of height at most $A(\geqslant 4)$ and degree d; further let b_1 and b_2 denote integers with absolute values $\leqslant B(\geqslant 4)$. Set

$$\Lambda = b_1 \log(-1) + b_2 \log \alpha \tag{1}$$

where the logarithms are assumed to take their principal values. We prove

LEMMA 2. *If* $\Lambda \neq 0$ *then*

$$|\Lambda| > \exp(-C \log A \log B)$$

for $C = 2^{435}(3d)^{49}$.

The above value for C improves upon that given by Theorem 2 of [3]. Baker's proof of Theorem 2 may be split into two parts. In the first part he establishes an estimate for

$$\Lambda' = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n$$

subject to the condition

$$[K(\alpha_1^{1/q}, \ldots, \alpha_n^{1/q}) : K] = q^n \tag{2}$$

for some prime $q \geqslant 7$ where $K = Q(\alpha_1, \ldots, \alpha_n)$. In fact for this part of Baker's argument it suffices to choose the parameter k, which arises in the proof, so that

$$k^{\varepsilon/2} \geqslant 2^{14}(nd)^2$$

where $\varepsilon = 1/(3n)$. Thus subject to (2) we have

$$|\Lambda'| > B^{-C_1 \Omega \log \Omega'}$$

where $C_1 = k^2$. On setting $n = 2$ and $q = 7$ we conclude that if $[K(\alpha_1^{1/7}, \alpha_2^{1/7}) : K] = 49$ and if $\Lambda' \neq 0$ then

$$|b_1 \log \alpha_1 + b_2 \log \alpha_2| > B^{-C_2 \log A_1 \log A_2 \log\log A_2} \tag{3}$$

for $C_2 = 2^{384} d^{48}$ where $d = [K : Q]$. (Recall that $A_i \geqslant 4$). We are able to deduce Lemma 2 from (3) by an argument which is different from that utilized by Baker for the second part of his proof and which, furthermore, leads to a sharper estimate for $|\Lambda|$.

Proof of Lemma 2. Recall that

$$\Lambda = b_1 \log(-1) + b_2 \log \alpha.$$

We may assume that $b_1 b_2 \neq 0$ for otherwise the lemma plainly holds. Similarly we may assume that α is not a root of unity.

Let $\zeta = e^{\pi i/7^r}$ where r is the smallest integer $\geqslant 1$ such that $e^{\pi i/7^{r+1}}$ is not an element of $Q(\alpha, \zeta)$. Set $K_1 = Q(\alpha, \zeta)$. Clearly $D \leqslant 6d$ where $D = [K_1 : Q]$ and thus we may write

$$\Lambda = b_1' \log \zeta + b_2 \log \alpha$$

where $b_1' = 7^r b_1 \leqslant 2DB$ and the logarithms take their principal values. We shall now prove that Λ may be written as a linear form in ζ and γ only where $K_1(\zeta^{1/7}, \gamma^{1/7})$ is an extension of degree 49 over K_1.

We first show that if, for some γ in K_1,

$$\alpha = \zeta^s \gamma^{7^t}, \qquad 0 \leqslant s \leqslant D,$$

then $7^t < 61 D^3 \log(A + 1)$ where A is the height of α. This is certainly the case if an integral prime ideal $\mathfrak{p}$ of K_1 divides $[\alpha]$ for then $\mathfrak{p} | [\gamma]$ whence $\mathfrak{p}^{7^t} | [\alpha]$. If $\mathfrak{p}$ lies over the rational prime p then we see, on taking norms, that p^{7^t} divides the denominator of the norm of $[\alpha]$. Thus $A^D \geqslant p^{7^t} \geqslant 2^{7^t}$ and so

$$D \log A \geqslant 7^t \log 2. \tag{4}$$

The argument also applies if $\mathfrak{p} | [\alpha^{-1}]$. If no prime ideal divides either $[\alpha]$ or $[\alpha^{-1}]$, then α, and thus also γ, is a unit. Let σ be the field automorphism of K_1 that sends γ to its conjugate of largest absolute value. We may then write

$$\sigma(\alpha) = \sigma(\zeta^s)(\sigma(\gamma))^{7^t}.$$

It follows from a result of Blanksby and Montgomery [6] that

$$|\sigma(\gamma)| > 1 + (30D^2 \log 6D)^{-1},$$

while, (see p. 5 of [12]), $|\sigma(\alpha)| < A + 1$. Thus

$$\log(A + 1) > 7^t \log(1 + (30D^2 \log 6D)^{-1}).$$

Since $\log(1 + 1/x) > 1/(x + 1)$ for $x > 1$ we have

$$7^t < (1 + 30D^2 \log 6D) \log(A + 1) < 61D^3 \log(A + 1) \tag{5}$$

as required.

We now construct, as far as possible, a sequence

$$\alpha = \zeta^{s_1}\gamma_1^7, \gamma_1 = \zeta^{s_2}\gamma_2^7, \ldots$$

where the γ_i's are in K_1. The sequence terminates for some $t \geqslant 0$ satisfying (5) and on setting $\gamma_t = \gamma$ we may write

$$\alpha = \zeta^s \gamma^{7^t}$$

for some integer s with $0 \leqslant s \leqslant D$. Therefore

$$\log \alpha = s \log \zeta + 7^t \log \gamma + s_0 \cdot 2\pi i$$

where the logarithms take their principal values; here $s_0 \leqslant 7^t$. Thus

$$\log \alpha = s_1 \log \zeta + 7^t \log \gamma$$

where $s_1 = s + 2s_0 \cdot 7^t \leqslant 5D7^t$. Accordingly

$$\Lambda = B_1 \log \zeta + B_2 \log \gamma$$

with $B_1 = b_1' + b_2 s_1$ and $B_2 = 7^t b_2$. We note that

$$B' = \max\{4, |B_1|, |B_2|\} \leqslant 7^{t+1} DB. \tag{6}$$

By construction $[K_1(\zeta^{1/7}) : K_1] = 7$ and, in fact, $[K_1(\zeta^{1/7}, \gamma^{1/7}) : K_1] = 49$ for otherwise, by Lemma 4 of [3], we could write $\gamma = \zeta^{s_t}\gamma_{t+1}^7$ for some γ_{t+1}

in K_1 and some integer s_t, contradicting our choice of γ. Thus from (3) we have

$$|\Lambda| > \exp(-C_3 \log A' \log B')$$

where A' is the larger of 4 and the height of γ and where $C_3 = 2^{384}D^{48}$.

Since $D \leqslant 6d$ it is clear that to prove the lemma we need only verify the inequality

$$\log A' \log B' < 4D \log A \log B. \tag{7}$$

To this end we note first that, by Lemma 1.4 of [13],

$$|\Lambda| > \exp(-2d\, B \log 3A)$$

and so we assume that

$$2dB \log 3A > C \log A \log B$$

and thus

$$B > 2^{400}d^{48}. \tag{8}$$

We next estimate A'. We have

$$\gamma = \zeta^{s/7^t}\alpha^{1/7^t}$$

and by Lemma 5 of [3], we deduce that

$$A' \leqslant 2^D(A + 1)^{1/7^t}A^{D/7^t} \leqslant 2^{D+1}A^{(D+1)/7^t}$$

whence

$$\log A' \leqslant D + \{(D + 1) \log A\}/7^t. \tag{9}$$

From (6), (8) and (9) we have

$$\log A' \log B' \leqslant \max\{4D \log 7^t,\quad 6D \log B,\quad 4(D + 1)(\log A)(\log 7^t)/7^t,$$
$$8(D + 1) \log A \log B/7^t\}.$$

If $t = 0$ then $A' = A$ and $B' \leqslant 2DB$ whence (7) plainly holds. For $t \geqslant 1$ inequality (7) follows from (4), (5) and (8). This completes the proof of the lemma.

3. FURTHER PRELIMINARY LEMMAS

Following Schinzel, we set $Q(A/B) = K_{0'}$, $A/B = \alpha/\beta$ where α and β are integers in K_0 and $([\alpha], [\beta]) = \mathfrak{d}$. Let S be the set of all isomorphic injections of K_0 in the complex field and set

$$\theta(\alpha/\beta) = \log \prod_{\sigma \in S} \max\{|\sigma(\alpha)|, |\sigma(\beta)|\} - \log N\mathfrak{d},$$

where N denotes the absolute norm in K_0. Plainly $\theta(\alpha/\beta)$ is independent of the choice of α, β in K_0.

We note that by assumption A/B, and thus also α/β, is not a root of unity. We assume, without loss of generality, that $|\alpha| \geqslant |\beta|$. We then prove

LEMMA 3. *For $n > 0$ we have*

$$\log 2 + n \log|\alpha| \geqslant \log |\alpha^n - \beta^n| \geqslant n \log|\alpha| - C \log(n+1)(d + \theta(\alpha/\beta))$$

where $C = 2^{436}(3d)^{49}$.

Proof. We have

$$\log|\alpha^n - \beta^n| = n \log|\alpha| + \log|(\beta/\alpha)^n - 1|.$$

Now for any complex number z, either $\frac{1}{2} < |e^z - 1|$ or

$$\tfrac{1}{2}|z - ik\pi| \leqslant |e^z - 1|$$

for some integer k. On setting $z = n \log(\beta/\alpha)$ where the logarithm takes its principal value, it is clear that the proof reduces to establishing a good lower bound for

$$|\Lambda| = |n \log(\beta/\alpha) - ik\pi|$$

over all integers k. Plainly we may assume that $k \leqslant 2n$ whence, on noting that $\Lambda \neq 0$ since α/β is not a root of unity, we have from Lemma 2 that for $n > 0$,

$$|n \log(\beta/\alpha) - k \log(-1)| > \exp(-C \log A \log(n+1)), \tag{10}$$

where $A(\geqslant 4)$ denotes the height of β/α and $C = 2^{436}(3d)^{49}$. The coefficients of the irreducible polynomial

$$N\mathfrak{d}^{-1} \prod_{\sigma \in S} (\sigma(\beta)x - \sigma(\alpha))$$

are rational integers and their absolute values do not exceed

$$N\mathfrak{d}^{-1} \prod_{\sigma \in S} (|\sigma(\beta)| + |\sigma(\alpha)|) \leqslant 2^d e^{\theta(\alpha/\beta)}.$$

Thus $\log A \leqslant d + \theta(\alpha/\beta)$, and the lemma now follows from (10).

Let $\Phi_n(x, y)$ denote the nth cyclotomic polynomial in x and y. We have

LEMMA 4. *If* $\mathfrak{p}$ *is a prime ideal of* K *which divides* $[\Phi_n(A, B)]$ *for* $n > 2(2^d - 1)$ *and if* $\mathfrak{p}$ *is not a primitive divisor of* $[A^n - B^n]$ *then*

$$\operatorname{ord}_{\mathfrak{p}} \Phi_n(A, B) \leqslant \operatorname{ord}_{\mathfrak{p}} n.$$

Proof. This is Lemma 4 of [11].

4. PROOF OF THEOREM 1

Assume that $n > 2(2^d - 1)$. We have

$$\Phi_n(A, B) = B^{\phi(n)}\Phi_n(A/B, 1) = B^{\phi(n)}\Phi_n(\alpha/\beta, 1) = (B/\beta)^{\phi(n)}\Phi_n(\alpha, \beta)$$

and since $[B/\beta] = \mathfrak{d}^{-1}$, where $\mathfrak{d}$ is now considered as an ideal in K, we have

$$[\Phi_n(A, B)] = \mathfrak{d}^{-\phi(n)}[\Phi_n(\alpha, \beta)].$$

Thus

$$(d/l) \log|N_{K/Q}\Phi_n(A, B)| = \log|N\Phi_n(\alpha, \beta)| - \phi(n) \log N\mathfrak{d},$$

where N denotes the norm from K_0 to Q. The right-hand side is given by

$$\Big(\sum_{\sigma\in S} \sum_{m|n} \mu(n/m) \log|(\sigma(\alpha))^m - (\sigma(\beta))^m|\Big) - \phi(n) \log N\mathfrak{d}$$

which, by Lemma 3, is

$$> \phi(n)\theta(\alpha/\beta) - \Big\{ \sum_{\substack{m|n \\ \mu(n/m)=-1}} \log 2 + Cd(d + \theta(\alpha/\beta)) \sum_{\substack{m|n \\ \mu(n/m)=1}} \log(m + 1)\Big\} \tag{11}$$

for $C = 2^{436}(3d)^{49}$. On setting $q(n) = 2^{\omega(n)}$ where $\omega(n)$ denotes the number of distinct prime factors of n we see that the sum in curly brackets in (11) is less than

$$Cd(d + \theta(\alpha/\beta))q(n) \log n, \qquad n > 3,$$

whence

$$(d/l) \log|N_{K/Q}\Phi_n(A, B)| > \phi(n)\theta(\alpha/\beta) - Cd(d + \theta(\alpha/\beta))q(n) \log n. \tag{12}$$

From Lemma 4 it follows that $A^n - B^n$ has a primitive divisor whenever

$N_{K/Q}\Phi_n(A, B) > n^l$, and from (12) this is certainly the case if

$$(\phi(n)/q(n) \log n) > Cd(2d/\theta(\alpha/\beta) + 1) \tag{13}$$

To evaluate (13) we first establish a lower bound for $\theta(\alpha/\beta)$. We have

$$\theta(\alpha/\beta) = \log \prod_{\sigma \in S} \max\{|\sigma(\alpha/\beta)|, 1\} + \log N\beta - \log N\mathfrak{d}.$$

If α/β is not an integer then $[\beta] \neq \mathfrak{d}$ and thus

$$\theta(\alpha/\beta) \geqslant \log N\beta - \log N\mathfrak{d} \geqslant \log 2. \tag{14}$$

On the other hand if α/β is an integer then by a result of Blanksby and Montgomery (Theorem 1 of [6])

$$\theta(\alpha/\beta) \geqslant (52d \log 6d + 1)^{-1} \tag{15}$$

Thus, from (13), (14), and (15), it follows that $A^n - B^n$ has a primitive divisor for those n for which

$$(\phi(n)/q(n) \log n) > 200\, Cd^4. \tag{16}$$

We may assume that $n > e^{450}$ for the theorem does not apply for $n \leqslant e^{450}$. We now estimate $q(n) = 2^{\omega(n)}$ from above. The number of distinct prime factors of n is $\leqslant x$ where

$$\prod_{i=1}^{x} p_i \leqslant n < \prod_{i=1}^{x+1} p_i \tag{17}$$

and p_i denotes the ith prime. We first observe that

$$\log n < (x + 1) \log p_{x+1}$$

which by Theorem 3 of [9] is

$$< (x + 1)(\log(x + 1) + \log(2 \log(x + 1))).$$

Therefore, since $n > e^{450}$, we may assume that $x \log x > 230$, and thus, by Theorem 10 of [9], that

$$\sum_{p \leqslant x \log x} \log p > \cdot 89\, x \log x. \tag{18}$$

From Theorem 3 of [9] we have $p_x > x \log x$ whence from (17) and (18) we conclude that $\cdot 89\, x \log x < \log n$ and thus

$$x < (\tfrac{3}{2} \log n)/\log \log n.$$

Therefore $q(n) = 2^{\omega(n)} \leqslant 2^x$ and so

$$q(n) < n^{\frac{21}{20}(\log\log n)^{-1}}$$

From Theorem 15 of [9] we have $\phi(n) > n/2 \log\log n$ whence, for $n > e^{450}$,

$$(\phi(n)/q(n) \log n) > n^{4/5}.$$

Thus from (16) we see that if

$$n > (200\, Cd^4)^{5/4} > e^{452} d^{67}$$

then $A^n - B^n$ has a primitive divisor. This concludes the proof.

5. PROOF OF THEOREM 2

We shall assume that α and β are algebraic numbers for which α/β is not a root of unity. Further we shall assume that $(\alpha + \beta)^2$ and $\alpha\beta$ are coprime non-zero rational integers. Thus α and β generate a sequence $\{u_n\}$ of Lehmer numbers. If, in addition, $\alpha + \beta$ is an integer then α and β also generate a sequence $\{t_n\}$ of Lucas numbers. It is clear from the definition of Lucas and Lehmer numbers and the identity

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta)$$

that if p is a primitive divisor of u_n or t_n then $p \mid \Phi_n(\alpha, \beta)$. It follows from Lemmas 5 and 7 of [14] that for $n > 6$, $\neq 8$, 10 or 12, u_n and, when $\alpha + \beta$ is an integer, t_n have a primitive divisor whenever $\Phi_n(\alpha, \beta)$ is different from ± 1 and $\pm P(n/(3, n))$; here $P(m)$ denotes the greatest prime factor of m.

If follows from Theorem 1, since the degree of $Q(\alpha, \beta)$ is at most 4, that u_n and t_n both possess a primitive divisor for $n > C = e^{452} 4^{67}$. To prove the theorem we must therefore show that all of the $\leqslant 4C$ equations

$$\Phi_n(\alpha, \beta) = a \tag{19}$$

with $6 < n \leqslant C$; $n \neq 8$, 10 or 12, and with a given by one of ± 1 and $\pm P(n/(3, n))$, have only finitely many solutions in algebraic numbers α and β as above. Plainly it is sufficient to assume only that $(\alpha + \beta)^2$ is an integer since if the above equations have only finitely many solutions with $(\alpha + \beta)^2$ an integer they obviously have only finitely many with $\alpha + \beta$ an integer.

The primitive nth roots of unity are ζ^k, $(k, n) = 1$ where $\zeta = e^{2\pi i/n}$. Now since $(n - k, n) = 1$ when $(k, n) = 1$ we may group the nth roots of unity, for

$n > 2$, into $\phi(n)/2$ pairs (ζ^k, ζ^{-k}). Therefore the nth cyclotomic polynomial $(n > 2)$, which has degree $\phi(n)$, may be written

$$\Phi_n(\alpha, \beta) = (\alpha - \zeta\beta)(\alpha - \zeta^{-1}\beta)\dots(\alpha - \zeta^k\beta)(\alpha - \zeta^{-k}\beta)$$
$$= (\alpha^2 + \beta^2 - (\zeta + \zeta^{-1})\alpha\beta)\dots(\alpha^2 + \beta^2 - (\zeta^k + \zeta^{-k})\alpha\beta),$$

where we now assume that k is the largest integer $< n/2$ for which $(k, n) = 1$. Since we have assumed that both $(\alpha + \beta)^2$ and $\alpha\beta$ are integers, $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$ is an integer. Put $\alpha^2 + \beta^2 = v$ and $\alpha\beta = w$. We then have

$$\Phi_n(\alpha, \beta) = f_n(v, w) = (v - (\zeta + \zeta^{-1})w)\dots(v - (\zeta^k + \zeta^{-k})w)$$

where $f_n(v, w)$ is a homogeneous binary form in integers v and w of degree $\phi(n)/2$. Plainly the roots of $f(v, 1)$, namely, $(\zeta + \zeta^{-1}), \dots, (\zeta^k + \zeta^{-k})$, are distinct real numbers. Indeed they are conjugate algebraic numbers in the maximal totally real subfield of $Q(\zeta)$. The degree of this field is $\phi(n)/2$ for $n > 2$, and we see that the binary form $f_n(v, w)$ has integer coefficients.

If the equations (19) have solutions (α, β) then the corresponding equations with $\Phi_n(\alpha, \beta)$ replaced by $f_n(v, w)$ must have solutions in integers v, w with $v = \alpha^2 + \beta^2$ and $w = \alpha\beta$. However, from Lemma 1, the equation

$$f_n(v, w) = a, \tag{20}$$

where a is a non-zero integer, has only finitely many solutions in integers v and w whenever f_n has at least three roots, in other words when $\phi(n)/2 \geqslant 3$. Furthermore the solutions are effectively computable. Each solution v, w of (20) with a defined by ± 1 or $\pm P(n/(3, n))$ gives rise to a pair (α, β) and $(-\alpha, -\beta)$ of solutions of (19); (α, β) are the roots of $x^2 - |(v + 2w)^{\frac{1}{2}}|x - w$ while $(-\alpha, -\beta)$ are the roots of the same polynomial with x replaced by $-x$. Thus we may find all possible solutions (α, β) of those equations specified by (20) for which $\phi(n) \geqslant 6$. This therefore completes the proof, since $\phi(n) \geqslant 6$ for $n > 6$, $n \neq 8$, 10 or 12.

6. PROOF OF THEOREM 3

We note first that $u_1 = u_2 = 1$ by definition and thus we may assume $m \geqslant 3$. As we observed in the proof of Theorem 2 a primitive divisor p of u_m must divide $\Phi_m(\alpha, \beta)$. Therefore to prove the theorem it is sufficient to show that for each integer m, $3 \leqslant m \leqslant 12$, $m \neq 7$, 9 or 11, there exist infinitely many algebraic numbers α and β for which

$$\Phi_m(\alpha, \beta) = 1,$$

such that $(\alpha + \beta)^2$ and $\alpha\beta$ are coprime non-zero rational integers with α/β not a root of unity. Again, as in the proof of Theorem 2, we have

$$\Phi_m(\alpha, \beta) = f_m(v, w)$$

where $v = \alpha^2 + \beta^2$, $w = \alpha\beta$ and f_m has degree $\phi(m)/2$. We observe that if v and w are coprime non-zero rational integers then $(\alpha + \beta)^2 = v + 2w$ and $\alpha\beta = w$ are also coprime. Furthermore they are non-zero as long as $v \neq 2w$ whence, since $(v, w) = 1$, as long as $\{v, w\} \neq \{2, 1\}$. Now if α/β is a root of unity ζ then, since it is an element of a field of degree at most 4, it is one from a finite set of roots of unity. But we may then write $w = \alpha^2\zeta$ and $v = \alpha^2(1 + \zeta^2)$ and plainly each ζ may be associated with only finitely many pairs of coprime non-zero rational integers v, w. Therefore to prove the theorem it suffices to prove that each equation

$$f_m(v, w) = 1, \qquad 3 \leqslant m \leqslant 12, m \neq 7, 9, 11,$$

has infinitely many solutions in coprime non-zero integers v, w.

For the equations

$$f_6 = v - w = 1, \qquad f_4 = v = 1, \qquad f_3 = v + w = 1$$

the result is obvious. The remaining equations are

$$f_{12} = v^2 - 3w^2 = 1, \qquad f_{10} = v^2 - vw - w^2 = 1,$$
$$f_8 = v^2 - 2w^2 = 1, \qquad f_5 = v^2 + vw - w^2 = 1.$$

It is well known that the Pell's equations $f_{12} = 1$ and $f_8 = 1$ have infinitely many solutions $\{v, w\}$ of the desired kind. Further, $f_{10} = 1$ when

$$v^2 - vw - (w^2 + 1) = 0. \tag{21}$$

This is solvable in integers v and w for a given integer w whenever the discriminant of the above polynomial in v is the square of an integer; in other words, when

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

The above Pell's equation has infinitely many solutions; we must insure, however, that it has infinitely many coprime solutions z, w. Plainly it is sufficient to exhibit infinitely many solutions z, w where z is odd. The minimal solution of (22) is $z = 3$, $w = 1$ and thus the general solution of (22) is given by

$$z_n + w_n\sqrt{5} = \pm 2\left(\frac{3+\sqrt{5}}{2}\right)^n.$$

It follows, therefore, that

$$z_n = \left(\frac{3+\sqrt{5}}{2}\right)^n + \left(\frac{3-\sqrt{5}}{2}\right)^n$$

and setting $\alpha_0 = (3+\sqrt{5})/2$ and $\beta_0 = (3-\sqrt{5})/2$ we see that

$$z_n = \alpha_0^n + \beta_0^n = (\alpha_0^{2n} - \beta_0^{2n})/(\alpha_0^n - \beta_0^n).$$

If we put $n = p$, p a prime > 5, then

$$z_p = \Phi_{2p}(\alpha_0, \beta_0)\cdot\Phi_2(\alpha_0, \beta_0).$$

From Lemma 6 of [14] we see that if $2|z_p$ then $2|\Phi_2 = \alpha_0 + \beta_0$. But $\alpha_0 + \beta_0 = 3$ and thus as n runs through the primes p we find infinitely many solutions of (22) with z odd and hence with z and w coprime. Each solution gives rise to two solutions $\{v, w\}$ of (21). They are

$$\left(\frac{w+z}{2}, w\right) \text{ and } \left(\frac{w-z}{2}, w\right).$$

Thus $f_{10}(v, w)$ has infinitely many solutions in coprime non-zero integers v, w. Finally, it can be shown that $f_5(v, w) = 1$ reduces to the Pell's equation (22) and solutions of $f_5 = 1$ are of the form

$$\left(\frac{-w+z}{2}, w\right) \text{ and } \left(\frac{-w-z}{2}, w\right)$$

where z and w are coprime solutions of (22).

REFERENCES

[1] A. Baker, Contributions to the theory of Diophantine equations I: On the representation of integers by binary forms, *Phil. Trans. Roy. Soc. London*, **A263** (1968), 173–191.

[2] A. Baker, *Transcendental Number Theory* (Cambridge, 1975).

[3] A. Baker, The theory of linear forms in logarithms, *Transcendence Theory: Advances and Applications* (Academic Press, London and New York, 1977) [Chapter 1 of these Proceedings].

[4] A. S. Bang, Taltheoretiske Undersøgelser, *Tidsskrift for Mat.* (5), **4** (1886), 70–80, 130–137.
[5] G. D. Birkhoff and H. S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. of Math.* (2), **5** (1904), 173–180.
[6] P. Blanksby and H. Montgomery, Algebraic integers near the unit circle, *Acta Arith.* **18** (1971), 355–369.
[7] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* (2), **15** (1913), 30–70.
[8] L. P. Postnikova and A. Schinzel, Primitive divisors of the expression $a^n - b^n$ in algebraic number fields (Russian), *Mat. Sbornik*, **75** (1968), 171–177; *Math. USSR Sbornik*, **4** (1968), 153–159.
[9] J. Barkley Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.
[10] A. Schinzel, The intrinsic divisors of Lehmer numbers in the case of negative discriminant, *Ark. Mat.* **4** (1962), 413–416.
[11] A. Schinzel, Primitive divisors of the expression $A^n - B^n$ in algebraic number fields, *J. reine angew. Math.* 268/269 (1974), 27–33.
[12] Th. Schneider, *Einführung in die transzendenten Zahlen* (Berlin, 1957).
[13] C. L. Stewart, *Divisor Properties of Arithmetical Sequences,* Ph.D. Dissertation (Cambridge, 1976).
[14] C. L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.* (to appear).
[15] M. Ward, The intrinsic divisors of Lehmer numbers, *Ann. of Math.* (2) **62** (1955), 230–236.
[16] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math.* **3** (1892), 265–284.