ON DIVISORS OF FERMAT, FIBONACCI, LUCAS AND LEHMER NUMBERS, III

C. L. STEWART

1. *Introduction*

Let r, s, u_0 and u_1 be integers and put $u_n = ru_{n-1} + su_{n-2}$ for $n = 2, 3, \ldots$. We have

$$u_n = a\alpha^n + b\beta^n \tag{1}$$

where α and β are the roots of $X^2 - rX - s$, $a = (u_1 - u_0\beta)/(\alpha - \beta)$ and $b = (u_0\alpha - u_1)/(\alpha - \beta)$ whenever $\alpha \neq \beta$. The binary recurrence sequence $(u_n)_{n=0}^{\infty}$ is said to be non-degenerate if $ab\alpha\beta \neq 0$ and α/β is not a root of unity. For any integer m let $Q(m)$ denote the greatest square-free factor of m with the convention that $Q(0) = Q(\pm 1) = 1$. Thus if $m = p_1^{l_1} \ldots p_r^{l_r}$ where $p_1, \ldots, p_r$ are distinct prime numbers and $l_1, \ldots, l_r$ are positive integers then $Q(m) = p_1 \ldots p_r$. In [12] we proved that if u_n is the n-th term of a non-degenerate binary recurrence sequence, as in (1), then

$$Q(u_n) > C(n/(\log n)^2)^{1/d}, \tag{2}$$

for $n > 1$, where d is the degree of α over the rational numbers and C is a positive number which is effectively computable in terms of a and b only. We also proved that if α is a real number then, for any positive number ε,

$$Q(u_n) > n^{1-\varepsilon}, \tag{3}$$

whenever n is larger than a number which is effectively computable in terms of a, b, α, β and ε. If $u_0 = 0$ and $u_1 = 1$ then

$$u_n = (\alpha^n - \beta^n)/(\alpha - \beta), \tag{4}$$

for $n = 0, 1, 2, \ldots$, and the sequence $(u_n)_{n=0}^{\infty}$ is a Lucas sequence. Also the related sequence $(v_n)_{n=0}^{\infty}$,

$$v_n = \alpha^n + \beta^n, \tag{5}$$

for $n = 0, 1, 2, \ldots$, is known as a Lucas sequence. Lucas numbers include the Mersenne, Fermat and Fibonacci numbers and they arise in many arithmetical settings because of their divisibility properties. In 1930 Lehmer [4] generalized the

Received 3 August, 1982.

This research was supported in part by a grant from the Natural Sciences and Engineering Research Council of Canada.

results of Lucas [5] on the divisibility properties of Lucas numbers to numbers u_n and v_n with $n \geqslant 0$ satisfying

$$u_n = \begin{cases} \dfrac{\alpha^n-\beta^n}{\alpha-\beta}, & \text{for } n \text{ odd}, \\[2ex] \dfrac{\alpha^n-\beta^n}{\alpha^2-\beta^2}, & \text{for } n \text{ even}, \end{cases} \qquad v_n = \begin{cases} \dfrac{\alpha^n+\beta^n}{\alpha+\beta}, & \text{for } n \text{ odd}, \\[2ex] \alpha^n+\beta^n, & \text{for } n \text{ even}. \end{cases} \tag{6}$$

where $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero integers and α/β is not a root of unity. The numbers defined above are known as Lehmer numbers. The purpose of this note is to establish estimates from below for $Q(u_n)$ and $Q(v_n)$, where u_n and v_n are Lucas or Lehmer numbers, which improve upon (2) and (3).

Let α and β be complex numbers such that $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero integers and α/β is not a root of unity. For any positive integer n we denote the n-th cyclotomic polynomial in α and β by $\Phi_n(\alpha, \beta)$, that is,

$$\Phi_n(\alpha, \beta) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (\alpha-\zeta^j\beta), \tag{7}$$

where ζ is a primitive n-th root of unity. Further, for any integer m let $P(m)$ denote the greatest prime factor of m with the convention that $P(0) = P(\pm 1) = 1$. Schinzel [7] proved that

$$P(\Phi_n(\alpha, \beta)) \geqslant n-1, \tag{8}$$

for n sufficiently large; by a result of Stewart [11] it suffices to take n larger than $e^{452}4^{67}$. Furthermore Shorey and Stewart [8, 10] showed that for $n \geqslant 2$,

$$P(\Phi_n(\alpha, \beta)) > C_0 n \log n, \tag{9}$$

where C_0 is a positive number which is effectively computable in terms of α, β and the number of distinct prime factors of n. Since

$$\alpha^n-\beta^n = \prod_{d|n} \Phi_d(\alpha, \beta), \tag{10}$$

and since $v_n = u_{2n}/u_n$ for Lucas and Lehmer numbers, estimates (8) and (9) apply with $Q(u_n)$ and $Q(v_n)$ in place of $P(\Phi_n(\alpha, \beta))$ and this certainly gives an improvement on (2) and (3). In fact we are able to improve substantially on these results. For any positive integer n let $q(n)$ denote the number of square-free divisors of n; thus $q(n) = 2^{\omega(n)}$ where $\omega(n)$ denotes the number of distinct prime factors of n. By an argument which owes much to [8, 9, 10] we shall show that there exists an effectively computable positive constant c such that

$$Q(\Phi_n(\alpha, \beta)) > n^{(c\log n)/(q(n)\log\log n)}, \tag{11}$$

for all integers n larger than a number which is effectively computable in terms of α and β. For any positive integer n let $d(n)$ denote the number of positive divisors of n. We shall employ (11) to prove the following result.

THEOREM 1. *Let* $(\alpha+\beta)^2$ *and* $\alpha\beta$ *be non-zero integers with* α/β *not a root of unity. Let* u_n *and* v_n *be Lucas or Lehmer numbers as in* (4), (5) *or* (6). *There exists an effectively computable positive constant* c *such that*

$$Q(u_n) > n^{c(d(n)\log n)/(q(n)\log\log n)}, \tag{12}$$

for all integers n *larger than a number which is effectively computable in terms of* α *and* β. *Further, inequality* (12) *remains valid if we replace* u_n *by* v_n *provided that we replace* $d(n)$ *by* $d(n|n|_2)$, *where* $|n|_2$ *denotes the* 2*-adic value of* n *normalized so that* $|2|_2 = \frac{1}{2}$.

For any positive integer n, $d(n) \geqslant q(n)$ and $d(n|n|_2) \geqslant q(n)/2$. Thus

$$Q(u_n) > n^{c(\log n)/\log\log n}, \tag{13}$$

for n sufficiently large; the above estimate is also valid for $Q(v_n)$ with $c/2$ in place of c. Further, for any non-zero integers a and b with $a \neq \pm b$, (13) applies with u_n replaced by $a^n - b^n$ or $a^n + b^n$ and c replaced by $c/2$. In particular, there exists an effectively computable positive constant c_1 such that for the Mersenne numbers,

$$\log Q(2^p - 1) > c_1(\log p)^2/\log\log p,$$

for $p > 2$, while for the Fermat numbers

$$\log Q(2^{2^n}+1) > c_1 n^2/\log n,$$

for $n > 2$. Notice also, from (12), that for $n > 2$,

$$\log Q(2^{2^n}-1) > c_2 n^3/\log n,$$

where c_2 is an effectively computable positive constant.

We are able to improve estimate (12) for almost all integers n.

THEOREM 2. *Let* $(\alpha+\beta)^2$ *and* $\alpha\beta$ *be non-zero integers with* α/β *not a root of unity. Let* u_n *and* v_n *be Lucas or Lehmer numbers as in* (4), (5) *or* (6). *For any positive number* ε *and all positive integers* n, *except perhaps for those in a set of asymptotic density zero,*

$$Q(u_n) > n^{(\log n)^{1+\log 2-\varepsilon}}. \tag{14}$$

Further, inequality (14) *remains valid if we replace* u_n *by* v_n.

It follows from Lemma 2, Lemma 3 and (10) that for any Lucas or Lehmer number u_n,

$$Q(u_n) > c_3 n^{d(n)/4}, \tag{15}$$

where c_3 is an effectively computable positive constant. Thus letting n run through the sequence $p_1, p_1p_2, p_1p_2p_3, \ldots$, where $2 = p_1 < p_2 < \ldots$ is the sequence of prime numbers, we see that for any positive number ε,

$$\log Q(u_n) > n^{(\log 2-\varepsilon)/\log\log n}, \tag{16}$$

for infinitely many integers n. Inequality (15) remains valid with v_n in place of u_n for any Lucas or Lehmer number v_n provided that $d(n)$ is replaced by $d(n|n|_2)$ and thus (16) holds with v_n in place of u_n.

2. *Preliminary lemmas*

LEMMA 1. *Let $\varepsilon(n)$ be a real valued function satisfying $\lim_{n\to\infty} \varepsilon(n) = 0$. For all positive integers n, except a set of asymptotic density zero, and for all divisors l of n with $l > n^{1/2}$, there exists an integer s, depending on l, such that if $1 = d_1 < d_2 < \ldots < d_t = l$ are the divisors of l then*

$$d_s/d_{s-1} > n^{\varepsilon(n)}.$$

Proof. We may assume without loss of generality that $\varepsilon(n)$ is positive for all integers n. In the proof of Lemma 11 of [**10**], which was motivated by earlier work of Erdös, we showed that almost all integers n have no divisor between $n^{1/2}$ and $n^{(1/2)+\varepsilon(n)}$. Thus for almost all integers n, all divisors l of n have no divisor between $n^{1/2}$ and $n^{(1/2)+\varepsilon(n)}$; for each divisor l of n with $l > n^{1/2}$ we set s equal to the index of the smallest divisor of l larger than $n^{(1/2)+\varepsilon(n)}$ and our result then follows since $d_{s-1} \leqslant n^{1/2}$.

For brevity we shall denote $\Phi_n(\alpha, \beta)$ by Φ_n.

LEMMA 2. *Let $(\alpha+\beta)^2$ and $\alpha\beta$ be coprime non-zero integers with α/β not a root of unity. If $n > 4$ and $n \neq 6, 12$ then $P(n/(3, n))$ divides Φ_n to at most the first power. All other prime factors of Φ_n are congruent to ± 1 (mod n). Further if $n > e^{452}4^{67}$ then Φ_n has at least one prime factor congruent to ± 1 (mod n).*

Proof. The first two assertions follow from work of Carmichael [**2**], Lehmer [**4**] and Lucas [**5**]: see Lemma 6 of [**10**]. It follows from the proof of Theorem 1 of [**11**] (see also [**7**]) that $|\Phi_n| > n$ for $n > e^{452}4^{67}$. Our third assertion is thus a consequence of the earlier two assertions since $P(n/(3, n)) \leqslant n$.

For any integer $n > 2$ let $Q'(\Phi_n)$ denote the largest square-free divisor of Φ_n composed of prime numbers congruent to ± 1 (mod n).

LEMMA 3. *Let $(\alpha+\beta)^2$ and $\alpha\beta$ be coprime non-zero integers with α/β not a root of unity. Let $n_1, \ldots, n_r$ be distinct integers larger than 12. Then*

$$Q\left(\prod_{i=1}^{r} \Phi_{n_i}\right) \geqslant \prod_{i=1}^{r} Q'(\Phi_{n_i}).$$

Proof. Let n and m be integers larger than 12 with $n > m$. By Lemma 7 of [**10**], (Φ_n, Φ_m) divides $P(n/(3, n))$ and thus, by Lemma 2, $Q'(\Phi_n)$ and $Q'(\Phi_m)$ are coprime. Lemma 3 follows directly.

3. *Proof of Theorem* 1

Denote the greatest common divisor of $(\alpha+\beta)^2$ and $\alpha\beta$ by d and let α' and β' satisfy $(\alpha'+\beta')^2 d = (\alpha+\beta)^2$ and $\alpha'\beta' d = \alpha\beta$. Certainly $(\alpha'+\beta')^2$ and $\alpha'\beta'$ are coprime. Further, by (7), for $n > 2$,

$$\Phi_n(\alpha, \beta) = \prod_{\substack{j=1\\(j,n)=1}}^{[n/2]} \left(\alpha^2+\beta^2-(\zeta^j+\zeta^{-j})\alpha\beta\right);$$

hence $\Phi_n(\alpha, \beta) = d^{\phi(n)/2}\Phi_n(\alpha', \beta')$. Thus, from (10) and the definition of Lucas and Lehmer numbers, it is no loss of generality to assume that $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime.

We shall assume that n exceeds a sufficiently large number C_1, where $C_1, C_2, \ldots$ are positive numbers which are effectively computable in terms of α and β only. We shall denote by $c_1, c_2, \ldots$ effectively computable positive constants. Let $d_0 = 1$ and let $d_1 < \ldots < d_t$ be all the positive divisors of n with $\mu(n/d_r) \neq 0$. Take s to be the smallest integer not less than 1 such that $d_s \geqslant n^{s/t}$. Then

$$d_s/d_{s-1} \geqslant \exp\left((\log n)/q(n)\right). \tag{17}$$

We shall assume that $(\log n)/q(n) \geqslant 9 \log\log n$. By Lemma 2,

$$\Phi_n = p_0 \prod_{i=1}^{k} p_i^{h_i}, \tag{18}$$

where $h_1, \ldots, h_k$ are positive integers, $p_1, \ldots, p_k$ are distinct prime numbers congruent to $\pm 1 \pmod n$ and $\pm p_0$ is 1 or $P(n/(3, n))$. If α and β are real numbers then we may proceed as in the proof of Theorem 1 of [**10**] to compare estimates for

$$\prod_{r=s}^{t} \left(1-(\beta/\alpha)^{d_r}\right)^{\mu(n/d_r)},$$

with the aid of an estimate for linear forms in the logarithms of algebraic numbers due to Baker [**1**]. From (22) and (28) of [**10**] we obtain

$$d_s \log|\alpha/\beta| - \log\log n < C_2 d_{s-1}(\log n)^4 k^{c_1 k} \log p_1 \ldots \log p_k. \tag{19}$$

From (17) and (19) we find that

$$\exp\left((\log n)/q(n)\right) < C_3(\log n)^4 k^{c_1 k} \prod_{i=1}^{k} \log p_i. \tag{20}$$

If α and β are not real then we may proceed as in the proof of Theorem 1 of [**8**]. However, when we employ Lemma 1 of [**8**], a p-adic version of Baker's estimate due to van der Poorten [**6**], we do not make the simplifying assumption that $p_i < n^2$ for $i = 1, \ldots, k$. Therefore $(k \log n)^{c_3 k}$ is replaced by $k^{c_3 k} \log n \prod_{i=1}^{k} \log p_i$ in (9) of [**8**]. On making the corresponding modification in (10) and comparing (6) and (10) of [**8**] we again obtain (20).

Thus, whether α or β are real or not, we have, on taking logarithms in (20),

$$(\log n)/q(n) < C_4 + 4 \log\log n + c_1 k \log k + \log\left(\prod_{i=1}^{k} \log p_i\right). \tag{21}$$

By the arithmetic-geometric mean inequality and (18),

$$\prod_{i=1}^{k} \log p_i \leqslant \left(\left(\sum_{i=1}^{k} \log p_i\right)\Big/k\right)^k \leqslant \left((\log Q'(\Phi_n))/k\right)^k. \tag{22}$$

By assumption $(\log n)/q(n) \geqslant 9 \log\log n$ and therefore, from (21) and (22),

$$(\log n)/2q(n) < c_1 k \log k + k \log\log Q'(\Phi_n), \tag{23}$$

for n sufficiently large. We may assume, without loss of generality, that $c_1 \geqslant 1$. By Lemma 2, $p_i \geqslant n-1$ for $i = 1, \ldots, k$ and $k \geqslant 1$ and therefore if $k \geqslant (\log n)/(8c_1 q(n) \log\log n)$ then, from (18),

$$Q'(\Phi_n) > n^{c_2(\log n)/(q(n) \log\log n)}, \tag{24}$$

as required. If, on the other hand, $k < (\log n)/(8c_1 q(n) \log\log n)$ then $c_1 k \log k \leqslant (\log n)/(8q(n))$ since $c_1 \geqslant 1$. It then follows from (23) that

$$(\log n)/(4q(n)) < k \log\log Q'(\Phi_n),$$

whence

$$Q'(\Phi_n) > e^{(\log n)^2}.$$

Consequently the estimate (24) for $Q'(\Phi_n)$ applies for all integers n with $n) \leqslant (\log n)/(9 \log\log n)$. By Lemma 2, $Q'(\Phi_n) \geqslant n-1$ for n sufficiently large. herefore estimate (24), with c_2 replaced by c_3, in fact applies for all sufficiently large integers n.

Let u_n be the Lucas or Lehmer number associated with α and β. From (10) and Lemma 3 we have

$$Q(u_n) \geqslant \prod_{\substack{l \mid n \\ l \geqslant \sqrt{n}}} Q'(\Phi_l). \tag{25}$$

Since at least $\frac{1}{2}$ of the positive divisors of n are at least $n^{1/2}$ in size it follows from (24) and (25) that

$$Q(u_n) > n^{c_4(d(n) \log n)/(q(n) \log\log n)},$$

as required.

Let v_n be the Lucas or Lehmer number associated with α and β. To establish the result for v_n we first note that $\alpha^n + \beta^n = (\alpha^{2n} - \beta^{2n})/(\alpha^n - \beta^n)$. Thus, from (10) and Lemma 3,

$$Q(v_n) \geqslant \prod_{\substack{l \mid 2n \\ l \nmid n \\ l \geqslant \sqrt{n}}} Q'(\Phi_l). \tag{26}$$

The number of divisors of $2n$ which do not divide n is $d(n|n|_2)$ and the number of divisors which are in addition at least $n^{1/2}$ is at least $(d(n|n|_2))/2$. Our result now follows from (24) and (26).

4. *Proof of Theorem* 2

Let $\varepsilon_1(n) = (\log\log n)^{-1}$ for $n > 3$. For almost all integers n and for each divisor l of n with $l > n^{1/2}$ put $d_0 = 1$ and let $d_1 < \ldots < d_t = l$ be the divisors of l with $\mu(l/d_r) \neq 0$. Then, by Lemma 1, there exists an integer s, depending on l, such that

$$d_s/d_{s-1} > n^{\varepsilon_1(n)}. \tag{27}$$

We may now argue as in the proof of Theorem 1 employing (27) in place of (17). In this way we prove that for almost all integers n and for all divisors l of n with $l > n^{1/2}$,

$$Q'(\Phi_l) > n^{((\varepsilon_1(n))^2 \log n)/\log\log n}; \tag{28}$$

note that for any $\delta > 0$ almost all integers n have fewer than $(\log n)^{\log 2+\delta}$ divisors (see Theorem 432 of [3]) and so the restriction $q(n) \leqslant (\log n)/9 \log\log n$ required initially in the proof of (24) in §3 certainly applies here. Since for any $\delta > 0$ almost all integers n have at least $(\log n)^{\log 2-\delta}$ divisors (see Theorem 432 of [3]), and indeed have at least $(\log n)^{\log 2-\delta}$ divisors larger than $n^{1/2}$, our result for u_n follows from (25) and (28). To establish a comparable estimate for $Q(v_n)$ we first remark that (28) applies for almost all integers n and for all divisors l of $2n$ with $l > n^{1/2}$. Further it is easy to show that for any $\delta > 0$ the number of divisors l of $2n$ which do not divide n and are larger than $n^{1/2}$ is at least $(\log n)^{\log 2-\delta}$ for almost all integers n, since the number of divisors of n is at least $(\log n)^{\log 2-\delta}$ for almost all integers n. Thus, from (26) and (28), we obtain the required estimate for $Q(v_n)$.

References

1. A. BAKER, 'The theory of linear forms in logarithms', *Transcendence theory: advances and applications* (eds. A. Baker and D. Masser, Academic Press, London, 1977), pp. 1–27.
2. R. D. CARMICHAEL, 'On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$', *Ann. of Math.* (2), 15 (1913), 30–70.
3. G. H. HARDY and E. M. WRIGHT, *An introduction to the theory of numbers*, 5th edition (Oxford University Press, Oxford, 1979).
4. D. H. LEHMER, 'An extended theory of Lucas' functions', *Ann. of Math.* (2), 31 (1930), 419–448.
5. E. LUCAS, 'Théorie des fonctions numériques simplement périodiques', *Amer. J. Math.*, 1 (1878), 184–240, 289–321.
6. A. J. VAN DER POORTEN, 'Linear forms in logarithms in the p-adic case', *Transcendence theory: advances and applications* (eds. A. Baker and D. Masser, Academic Press, London, 1977), pp. 29–57.
7. A. SCHINZEL, 'Primitive divisors of the expression $A^n - B^n$ in algebraic number fields', *J. Reine Angew. Math.*, 268/269 (1974), 28–33.
8. T. N. SHOREY and C. L. STEWART, 'On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, II', *J. London Math. Soc.* (2), 23 (1981), 17–23.
9. C. L. STEWART, 'The greatest prime factor of $a^n - b^n$', *Acta Arith.*, 26 (1975), 427–433.
10. C. L. STEWART, 'On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers', *Proc. London Math. Soc.* (3), 35 (1977), 425–447.
11. C. L. STEWART, 'Primitive divisors of Lucas and Lehmer numbers', *Transcendence theory: advances and applications* (eds. A. Baker and D. Masser, Academic Press, London, 1977), pp. 79–92.
12. C. L. STEWART, 'On divisors of terms of linear recurrence sequences', *J. Reine Angew. Math.*, 333 (1982), 12–31.

Department of Pure Mathematics,
University of Waterloo,
Waterloo,
Ontario,
Canada N2L 3G1.