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

\[
  u_n = a\alpha^n + b\beta^n
\]

(1)

where \( \alpha \) and \( \beta \) 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 \( \alpha/\beta \) 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 \( m = p_1^{l_1} \ldots p_l^{l_l} \) where \( p_1, \ldots, p_l \) are distinct prime numbers and \( l_1, \ldots, l_l \) are positive integers then \( Q(m) = p_1 \ldots p_l \). In [12] we proved that if \( u_n \) is the \( n \)-th term of a non-degenerate binary recurrence sequence, as in (1), then

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

(2)

for \( n > 1 \), where \( d \) is the degree of \( \alpha \) 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 \( \alpha \) is a real number then, for any positive number \( \varepsilon \),

\[
  Q(u_n) > n^{1-\varepsilon},
\]

(3)

whenever \( n \) is larger than a number which is effectively computable in terms of \( a, b, \alpha, \beta \) and \( \varepsilon \). If \( u_0 = 0 \) and \( u_1 = 1 \) then

\[
  u_n = (\alpha^n - \beta^n)/(\alpha - \beta),
\]

(4)

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

\[
  v_n = a\alpha^n + b\beta^n,
\]

(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 \( n \geq 0 \) satisfying

\[
\begin{align*}
    u_n &= \begin{cases} 
        \frac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{for } n \text{ odd}, \\
        \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{for } n \text{ even},
    \end{cases} \\
    v_n &= \begin{cases} 
        \frac{\alpha^n + \beta^n}{\alpha + \beta}, & \text{for } n \text{ odd}, \\
        \frac{\alpha^n + \beta^n}{\alpha^2 + \beta^2}, & \text{for } n \text{ even}.
    \end{cases}
\end{align*}
\]  

(6)

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

\[
\Phi_n(\alpha, \beta) = \prod_{\substack{j=1 \atop (j, n) = 1}}^{n} (\alpha - \zeta^j \beta),
\]

(7)

where \(\zeta\) 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

\[
P(\Phi_n(\alpha, \beta)) \geq n - 1,
\]

(8)

for \(n\) sufficiently large; by a result of Stewart [11] it suffices to take \(n\) larger than \(e^{452.457}\). Furthermore Shorey and Stewart [8, 10] showed that for \(n \geq 2\),

\[
P(\Phi_n(\alpha, \beta)) > C_0 n \log n,
\]

(9)

where \(C_0\) is a positive number which is effectively computable in terms of \(\alpha, \beta\) and the number of distinct prime factors of \(n\). Since

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

(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

\[
Q(\Phi_n(\alpha, \beta)) \geq n^{c (\log n)(\log \log n)},
\]

(11)

for all integers \(n\) larger than a number which is effectively computable in terms of \(\alpha\) and \(\beta\). 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 \(\alpha/\beta\) 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
\[
Q(u_n) > n^{d(n) \log n / (\log \log n)}
\]
for all integers \(n\) larger than a number which is effectively computable in terms of \(\alpha\) and \(\beta\). 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 \(n\), \(d(n) \geq q(n)\) and \(d(n|n_2) \geq q(n)/2\). Thus
\[
Q(u_n) > n^{c(\log n) / (\log \log n)},
\]
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 \(\alpha/\beta\) 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 \(\varepsilon\) and all positive integers \(n\), except perhaps for those in a set of asymptotic density zero,
\[
Q(u_n) > n^{(\log n)^2 + \log 2 - \varepsilon}.
\]
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 \(u_n\),
\[
Q(u_n) > c_3 n^{d(n)/4},
\]
where \(c_3\) is an effectively computable positive constant. Thus letting \(n\) run through the sequence \(p_1, p_1 p_2, p_1 p_2 p_3, \ldots\), where \(2 = p_1 < p_2 < \ldots\) is the sequence of prime numbers, we see that for any positive number \(\varepsilon\),
\[
\log Q(u_n) > n^{(\log 2 - \varepsilon) / (\log \log n)},
\]
for almost all \(n\).
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 \( 1 = d_1 < d_2 < \ldots < d_s = l \) 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 Erdős, 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 \( d_s/d_{s-1} > n^{\varepsilon(n)} \).

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

**Lemma 2.** Let \( (\alpha+\beta)^2 \) and \( \alpha\beta \) be coprime non-zero integers with \( \alpha/\beta \) not a root of unity. If \( n > 4 \) and \( n \neq 6, 12 \) then \( P(n/(3, n)) \) divides \( \Phi_n \) to at most the first power. All other prime factors of \( \Phi_n \) are congruent to \( \pm 1 \pmod{n} \). Further if \( n > e^{652.467} \) then \( \Phi_n \) has at least one prime factor congruent to \( \pm 1 \pmod{n} \).

**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 \( n > e^{652.467} \). Our third assertion is thus a consequence of the earlier two assertions since \( P(n/(3, n)) \leq n \).

For any integer \( n > 2 \) let \( Q(\Phi_n) \) denote the largest square-free divisor of \( \Phi_n \) composed of prime numbers congruent to \( \pm 1 \pmod{n} \).

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

\[
Q\left(\prod_{i=1}^r \Phi_{n_i}\right) \geq \prod_{i=1}^r Q(\Phi_{n_i}).
\]

**Proof.** Let \( n \) and \( m \) be integers larger than 12 with \( n > m \). By Lemma 7 of [10], \( (\Phi_n, \Phi_m) \) 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 \(\alpha'\) and \(\beta'\) 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 \(n > 2\),
\[
\Phi_n(\alpha, \beta) = \prod_{\gamma = 1}^{[\alpha/2]} (\alpha^2 + \beta^2 - (\zeta^l + \zeta^{-l})\alpha \beta);
\]
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 \(\alpha\) and \(\beta\) only. We shall denote by \(c_1, c_2, \ldots\) effectively computable positive constants. Let \(d_0 = 1\) and let \(d_1 < \ldots < d_i\) be all the positive divisors of \(n\) with \(\mu(n/d_i) \neq 0\). Take \(s\) to be the smallest integer not less than 1 such that \(d_s \geq n^{n!}\). Then
\[
d_s/d_{s-1} \geq \exp\left((\log n)/q(n)\right) .
\]
We shall assume that \((\log n)/q(n) \geq 9 \log \log n\). By Lemma 2,
\[
\Phi_n = p_0 \prod_{i=1}^{k} p_i^{h_i},
\]
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 \(\pm p_0 = 1\) or \(P(n/(3, n))\). If \(\alpha\) and \(\beta\) are real numbers then we may proceed as in the proof of Theorem 1 of [10] to compare estimates for
\[
\prod_{r=2}^{t} \left(1 - \frac{\beta}{\alpha \gamma^d} \right)^{\mu(n/d)},
\]
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
\[
d_s \log |\alpha/\beta| - \log \log n < C_2 d_{s-1} (\log n)^4 k^{c_4} \log p_1 \ldots \log p_k.
\]
From (17) and (19) we find that
\[
\exp\left((\log n)/q(n)\right) < C_3 (\log n)^4 k^{c_4} \prod_{i=1}^{k} \log p_i .
\]
If \(\alpha\) and \(\beta\) 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 \((k \log n)^{c_4}\) is replaced by \(k^{c_4} \log n \prod_{i=1}^{k} \log p_i\) in (9) of [8]. On making the corresponding modification in (10) and comparing (6) and (10) of [8] we again obtain (20).
Thus, whether \( \alpha \) or \( \beta \) are real or not, we have, on taking logarithms in (20),

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

(21)

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

\[
\prod_{i=1}^{k} \log p_i \leq \left( \left( \sum_{i=1}^{k} \log p_i \right)/k \right)^k \leq \left( \log Q'(\Phi_n)/k \right)^k.
\]  

(22)

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

\[
(\log n)/2q(n) < c_1 k \log k + k \log \log Q'(\Phi_n),
\]  

(23)

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

\[
Q'(\Phi_n) > n^{c_2(\log n)/(q(n) \log \log n)},
\]  

(24)

as required. If, on the other hand, \( k < (\log n)/(8c_1 q(n) \log \log n) \) then \( c_1 k \log k \leq (\log n)/(8q(n)) \) since \( c_1 \geq 1 \). 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 \( n \leq (\log n)/(9 \log \log n) \). By Lemma 2, \( Q'(\Phi_n) \geq n - 1 \) for \( n \) sufficiently large. Therefore 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 \( \alpha \) and \( \beta \). From (10) and Lemma 3 we have

\[
Q(u_n) \geq \prod_{\frac{1}{2} \leq l \mid n} Q'(\Phi_l).
\]  

(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

\[
Q(u_n) > n^{c_2(d(n)/(\log n) \log \log n)},
\]

as required.

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

\[
Q(v_n) \geq \prod_{\frac{1}{2} \leq l \mid n} Q'(\Phi_l).
\]  

(26)

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

Let \( \epsilon_2(n) = (\log \log n)^{-1} \) for \( p > 3 \). For almost all integers \( n \) and for each divisor \( l \) of \( n \) with \( l > n^{1/2} \) put \( d_0 = 1 \) and let \( d_1 < \ldots < d_\ell = l \) be the divisors of \( l \) with \( \mu(l/d_i) \neq 0 \). Then, by Lemma 1, there exists an integer \( s \), depending on \( l \), such that

\[
d_{s}/d_{s-1} > n^{\epsilon_2(n)}.
\]

(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 \( l > n^{1/2} \),

\[
Q(\Phi_l) > n^{(\log_l(n))^{2+\log \log \log n}};
\]

(28)

We 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 \( q(n) \leq (\log n)/9 \log \log n \) 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 \( u_4 \) follows from (25) and (28). To establish a comparable estimate for \( Q(\nu_4) \) 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 \( Q(\nu_4) \).

References

2. R. D. Carmichael, 'On the numerical factors of the arithmetic forms \( a^\pm b \)', Ann. of Math. (2), 15 (1913), 30–70.