ON THE GREATEST PRIME FACTOR OF TERMS OF A LINEAR RECURRENCE SEQUENCE

C.L. STEWART

In memory of R.A. Smith and E.G. Straus

The purpose of this note is to survey the results which have been obtained concerning the greatest prime factor and also the greatest square-free factor of terms of linear recurrence sequences. We shall first discuss the results which apply to general linear recurrence sequences. Next we shall consider binary recurrence sequences and finally, Lucas and Lehmer sequences.

For any integer \( n \), let \( P(n) \) denote the greatest prime factor of \( n \) with the convention that \( P(0) = P(\pm 1) = 1 \). Further, let \( Q(n) \) denote the greatest square-free factor of \( n \) with the convention that \( Q(0) = Q(\pm 1) = 1 \). Thus, if \( n = p_1^{h_1} \cdots p_r^{h_r} \) with \( p_1, \ldots, p_r \) distinct primes and \( h_1, \ldots, h_r \) positive integers, then \( Q(n) = p_1 \cdots p_r \).

Let \( r_1, \ldots, r_k \) and \( u_0, \ldots, u_{k-1} \) be integers and put \( u_n = r_1 u_{n-1} + \cdots + r_k u_{n-k} \), for \( n = k, k + 1, \ldots \). The sequence \( (u_n)_{n=0}^{\infty} \) is a linear recurrence sequence. Denote the field of rational numbers by \( \mathbb{Q} \). It is well known (see page 63 of [14]) that, for \( n \geq 0 \),

\[
(1) \quad u_n = f_1(n) \alpha_1^n + \cdots + f_t(n) \alpha_t^n,
\]

where \( f_1, \ldots, f_t \) are non-zero polynomials in \( n \) with degrees less than \( \alpha_1, \ldots, \alpha_t \), respectively, and with coefficients from \( \mathbb{Q}(\alpha_1, \ldots, \alpha_t) \), where \( \alpha_1, \ldots, \alpha_t \) are the non-zero roots of the characteristic polynomial of the sequence, \( x^k - r_1 x^{k-1} \cdots - r_k \), and \( \alpha_1, \ldots, \alpha_t \) are their respective multiplicities. We shall say that the sequence \( (u_n)_{n=0}^{\infty} \) is non-degenerate if \( t > 1 \), \( f_i \neq 0 \), for \( 1 \leq i \leq t \), and \( \alpha_i/\alpha_j \), for \( 1 \leq i < j \leq t \), are not roots of unity.

In 1921, Pólya [22] showed that if \( u_n \) is the \( n \)-th term of a non-degenerate linear recurrence sequence, then \( \lim \sup_{n \to \infty} P(u_n) = \infty \). In 1935, Mahler

Received by the editors October 12, 1983.

This research was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

Copyright © 1985 Rocky Mountain Mathematics Consortium
[18] proved, by means of a $p$-adic argument introduced two years earlier by Skolem, that

$$|u_n| \to \infty \text{ as } n \to \infty,$$

whenever $u_n$ is the $n$-th term of a non-degenerate linear recurrence sequence. This result, however, is ineffective; that is to say, given a positive integer $m$, the result does not yield a number $C(m)$ which is effectively computable in terms of $m$ such that $|u_n| > m$ whenever $n > C(m)$. For a short proof of Mahler’s result, see [20]. In 1977, Loxton and van der Poorten [15] extended the Skolem-Mahler argument to prove that if $(u_n)_{n=0}^\infty$ is a non-degenerate linear recurrence sequence, then, for any integer $m$, the set of integers $n$ with $P(u_n) < m$ is of asymptotic density zero. Recently, van der Poorten and Schlickewei [24], [25] have used Schlickewei’s work [34] on the $p$-adic version of the Thue-Siegel-Roth-Schmidt theorem to prove that, in fact,

$$P(u_n) \to \infty \text{ as } n \to \infty.$$ 

This result is also ineffective. For any rational $r$, put $P(r) = \max\{P(a), P(b)\}$, where $r = a/b$, $b$ is positive and $a$ and $b$ are coprime integers. Evertse [10] gave an independent proof of (3). He proved, more generally, that if $(u_n)_{n=0}^\infty$ is a non-degenerate linear recurrence sequence, then

$$\lim_{n \to \infty} P\left(\frac{u_n}{u_n^{(1)}}\right) = \infty.$$ 

Evertse’s result is ineffective since it also depends upon Schlickewei’s [35] $p$-adic version of the Thue-Siegel-Roth-Schmidt theorem.

The results which we have so far discussed have all been ineffective. To date, no effective version of Mahler’s theorem (2) has been established. Of course, if one of the roots of the associated characteristic equation of the recurrence sequence is larger in absolute value than the other roots, then, by (1), it is trivial to show that $|u_n| \to \infty$, as $n \to \infty$ effectively. One of the few non-trivial effective results known is due to Mignotte [21]. He proved, by means of a result of Baker [2] on linear forms in the logarithms of algebraic numbers, that if $u_n$ is the $n$-th term of a non-degenerate linear recurrence sequence, as in (1), and if at most three of the roots $\alpha_1, \ldots, \alpha_r$ of the associated characteristic equation have largest modulus and they are all simple, then, for $n > C_8$,

$$|u_n| > C_1 |\alpha_1|^n n^{-C_2},$$

whenever

$$f_1 \alpha_1^n + \cdots + f_r \alpha_r^n \neq 0,$$
where $C_1$, $C_2$ and $C_3$ are positive numbers which are effectively computable in terms of $\alpha_1, \ldots, \alpha_\ell$ and $f_1, \ldots, f_\ell$. In 1982, Stewart [46] obtained effective estimates for the greatest prime factor and the greatest square-free factor of $u_n$, the $n$-th term of a non-degenerate linear recurrence sequence, when there is only one root of the characteristic equation of largest modulus. In particular, if $u_n \neq f_1(n)\alpha_1^n$, then, for any $\varepsilon > 0$,

\begin{equation}
P(u_n) > (1 - \varepsilon)\log n
\end{equation}

and

\begin{equation}
Q(u_n) > n^{1-\varepsilon},
\end{equation}

for $n > C_1$, a number which is effectively computable in terms of $\varepsilon, \alpha_1, \ldots, \alpha_\ell$ and $f_1, \ldots, f_\ell$. For the proof of (6) and (7), a version, due to Waldschmidt [47], of Baker's theorem on linear forms in logarithms was employed. Sharlinskiĭ [41] independently proved the estimate (6) for $P(u_n)$, in the case that $f_1(n)$ is a non-zero constant and with $1 - \varepsilon$ replaced by a small positive number $C_1$.

I shall now discuss the special case, when $k = 2$ in (1), of binary recurrence sequences. If $u_n$ is the $n$-th term of a binary recurrence sequence, then, for $n \geq 0$,

\begin{equation}
\begin{aligned}
u_n &= a\alpha^n + b\beta^n,
\end{aligned}
\end{equation}

where $\alpha$ and $\beta$ are the roots of $x^2 - r_1x - r_2$ and

\begin{align*}
a &= (u_0\beta - u_1)/\beta - \alpha, \quad b = (u_1 - u_0\alpha)/\beta - \alpha,
\end{align*}

whenever $\alpha \neq \beta$. The binary recurrence sequence $(u_n)_{n=0}^\infty$ is non-degenerate whenever $ab\alpha\beta \neq 0$ and $\alpha/\beta$ is not a root of unity. We shall assume henceforth that $|\alpha| \geq |\beta|$. If $\alpha$ and $\beta$ are complex conjugates so that $|\alpha| = |\beta|$, then it is a non-trivial matter to show that $|u_n| \to \infty$ as $n \to \infty$. This follows, however, from the more general results of Mahler (2) and Mignotte (5) mentioned above. It also follows from other work of Mahler [17], [19] and of Schinzel [32]. The sharpest estimate for $|u_n|$ available at present is due to Shorey and Stewart (see Lemma 5 of [40]). They show that if $u_n$ is the $n$-th term of a non-degenerate binary recurrence sequence, as in (8), then

\begin{equation*}
|u_n| > |\alpha|^n n^{-C_1},
\end{equation*}

for $n > C_2$, where $C_1$ and $C_2$ are positive numbers which are effectively computable in terms of $a$ and $b$ only.

In 1934, Mahler [17] proved, by means of a $p$-adic version of the Thue-Siegel theorem, that if $u_n$ is the $n$-th term of a non-degenerate binary recurrence sequence, then
Mahler's result is ineffective. In 1967, Schinzel [32], extended earlier work of Gelfond on linear forms in two logarithms of algebraic numbers and as a consequence he was able to provide an effective version of (9). Schinzel proved that

\[ P(u_n) > C n^{c_1} (\log n)^{c_2}, \]

where \( C \) is a positive number which is effectively computable in terms of \( a, b, \alpha \) and \( \beta \) and where \( c_1 = 1/84 \) and \( c_2 = 7/12 \) if \( \alpha \) and \( \beta \) are integers, \( c_1 = 1/133 \) and \( c_2 = 7/19 \) otherwise. In 1982, Stewart [46] used a version due to Waldschmidt, of Baker's estimates for linear forms in the logarithms of algebraic numbers in conjunction with the \( p \)-adic analogue of these estimates, which had been established by van der Poorten [23], to prove that if \( u_n \) is the \( n \)-th term of a non-degenerate binary recurrence sequence, as in (8), then

\[ P(u_n) > C_1(n/\log n)^{1/(d+1)} \]

and

\[ Q(u_n) > C_2(n/(\log n)^2)^{1/d}, \]

where \( d \) is the degree of \( \alpha \) over the rationals and \( C_1 \) and \( C_2 \) are positive numbers which are effectively computable in terms of \( a \) and \( b \) only. Shorey [36] generalized (10). He proved that if \( m \) and \( n \) are integers with \( n > m \geq 0 \) and \( u_m \) and \( u_n \) non-zero, then

\[ P(u_n/u_m) > C_3(n/\log n)^{1/(d+1)}, \]

where \( C_3 \) is a positive number which is effectively computable in terms of \( a, b, \alpha \) and \( \beta \). This result was further generalized by Evertse to obtain (4). Stewart [46] also proved, by means of an elementary argument, that, for all integers \( n \), except perhaps for a set of asymptotic density zero,

\[ P(u_n) > \varepsilon(n) n \log n, \]

where \( \varepsilon(n) \) is any real valued function for which \( \lim_{n \to \infty} \varepsilon(n) = 0 \). By a related argument, Shorey [37] has obtained estimates for the greatest prime factor of the product of blocks of consecutive terms in binary recurrence sequences. Also, Shorey [38] has recently shown that, for \( n > c_1 \),

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

where \( c_1 \) and \( c_2 \) are positive numbers which are effectively computable in terms of \( a, b, \alpha \) and \( \beta \), and, apart from the dependence of \( c_1 \) and \( c_2 \) on \( \alpha \) and \( \beta \), this improves upon (11). Shorey used Baker's estimate [3] for linear forms in the logarithms of algebraic numbers as well as the \( p \)-adic analogue of this estimate due to van der Poorten [23] in his proof.
Finally, we shall turn our attention to Lucas and Lehmer sequences. A Lucas sequence \((u_n)_{n=0}^\infty\) is a non-degenerate binary recurrence sequence with initial conditions \(u_0 = 0\) and \(u_1 = 1\). Thus \(u_n = (\alpha^n - \beta^n)/(\alpha - \beta)\), for \(n \geq 0\). The related sequence \(v_n = \alpha^n + \beta^n\), for \(n \geq 0\), is also known as a Lucas sequence. The Fibonacci numbers, Mersenne numbers and Fermat numbers are all Lucas numbers. In 1878 Lucas [16] undertook an extensive analysis of the divisibility properties of these numbers; Euler, Lagrange, Gauss, Dirichlet and others had worked on this topic earlier (see Chapter XVII of [7]). In 1930 Lehmer [13] generalized the results of Lucas on the divisibility properties of Lucas numbers to numbers \(u_n\) and \(v_n\), with \(n \geq 0\), satisfying

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

where \((\alpha + \beta)^2\) and \(\alpha\beta\) are non-zero integers and \(\alpha/\beta\) is not a root of unity. These numbers, which are integers, have come to be known as Lehmer numbers. We shall assume henceforth that the Lucas and Lehmer sequences we discuss are such that \((\alpha + \beta)^2\) and \(\alpha\beta\) are coprime integers.

We shall 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, \(p\) is a primitive divisor of a Lehmer number \(u_n\) if \(p\) divides \(u_n\) but does not divide \((\alpha - \beta)^2 (\alpha + \beta)^2 u_3 \ldots u_{n-1}\). Denote the \(n\)-th cyclotomic polynomial in \(\alpha\) and \(\beta\) by \(\Phi_n(\alpha, \beta)\), so that,

\[
\Phi_n(\alpha, \beta) = \prod_{\zeta^n = 1, \zeta \neq 1} (\alpha - \zeta^i \beta),
\]

where \(\zeta\) is a primitive \(n\)-th root of unity. Notice that if \((\alpha + \beta)^2\) and \(\alpha\beta\) are integers, then \(\Phi_n(\alpha, \beta)\) is also an integer for \(n\) greater than two. We have,

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

hence,

\[
(14) \quad P(u_n) \geq P(\Phi_n(\alpha, \beta)).
\]

Further, if \(p\) is a primitive divisor of a Lucas or Lehmer number \(u_n\), for \(n > 2\), then \(p\) divides \(\Phi_n(\alpha, \beta)\). Furthermore, if \(p\) is a prime divisor of \(\Phi_n(\alpha, \beta)\), for \(n > 4\), \(n \neq 6\), and \(p\) doesn't divide \(n\), then \(p\) is a primitive divisor of \(u_n\) (see [13] or [44]). However, if \(n > 4\) and \(n \neq 6, 12\) the only possible prime divisor of \(n\) and \(\Phi_n(\alpha, \beta)\) is \(P(n/(3, n))\) and it divides \(\Phi_n(\alpha, \beta)\) to at most the first power; 2 and 3 divide \(\Phi_{12}(\alpha, \beta)\) to at most the
first power. All other prime factors of $\Phi_n(\alpha, \beta)$, for $n > 4, n \neq 6$, are congruent to $\pm 1 \pmod{n}$ (see Lemma 6 of [44]). Further, if $p$ is a primitive divisor of a Lucas or Lehmer number $u_n$, for $n > 6$, then $p$ does not divide $n$, and so $p$ is congruent to $\pm 1 \pmod{n}$ and

$$P(u_n) \geq n - 1.$$  

To establish that $u_n$ has a primitive divisor, it suffices, by the above discussion, to show that

$$|\Phi_n(\alpha, \beta)| > n.$$  

In 1892, Zsigmondy [49] and, in 1904, Birkhoff and Vandiver [5] proved that if $\alpha$ and $\beta$ are integers and $n > 6$, then the Lucas numbers $u_n$ possess a primitive divisor, hence, (15) holds. In fact, primitive divisors in this case are congruent to $1 \pmod{n}$ and so (15) holds with $n + 1$ in place of $n - 1$, for $n > 6$. Bang [4], in 1886, proved the result of Zsigmondy and Birkhoff and Vandiver for the special case when $\beta = 1$. In 1912 Carmichael [6] extended this work to include Lucas numbers $u_n$ with $\alpha$ and $\beta$ real numbers. In this case we may assume that $|\alpha| > |\beta|$ and it is not difficult to show that (16) holds for $n$ sufficiently large. Carmichael proved in this manner that $u_n$ has a primitive divisor, for $n > 12$. In a similar fashion Ward [48] established in 1955 (see also Durst [8]) that if $u_n$ is a Lehmer number with $\alpha$ and $\beta$ real numbers and $n > 12$ then $u_n$ has a primitive divisor and, as a consequence, (15) holds. In 1962, Schinzel [28] proved, using a result of Gelfond on linear forms in two logarithms, that if $u_n$ is a Lehmer number and $n > C(\alpha, \beta)$, a number which is effectively computable in terms of $\alpha$ and $\beta$, then $u_n$ has a primitive divisor. In 1974, Schinzel [33] showed, using a result of Baker's on linear forms in logarithms, that the number $C(\alpha, \beta)$ above could be replaced by $C_0$, an effectively computable positive constant. Stewart [43] made the result of Schinzel explicit by proving that a Lehmer number $u_n$ has a primitive divisor whenever $n > e^{452267}$; for the Lucas numbers the condition $n > e^{452267}$ is sufficient. In fact, much more is true, as Stewart [43] also proved that there are only finitely many Lucas and Lehmer sequences whose $n$-th term, $n > 6, n \neq 8, 10$ or 12, does not possess a primitive divisor and these sequences may be explicitly determined. The effective estimates, due to Baker [1], for the size of integer solutions $x$ and $y$ of the equation $f(x, y) = m$, where $f(x, y)$ is a homogeneous binary form with integer coefficients, $f(x, 1)$ has at least three distinct roots and $m$ is a non-zero integer, are used in the proof. The determination of the exceptional Lehmer sequences appears to be a formidable computational task. The result is best possible for Lehmer sequences (see Theorem 3 of [43]) since, for each integer $m \leq 12$ with $m \neq 7, 9$ or 11, there exist infinitely many Lehmer sequences $(u_n)_{n=1}^{\infty}$ for which $u_n$ does not have a primitive divisor. For Lucas sequences, the
restriction \( n > 6, n \neq 8, 10 \text{ or } 12 \) above may be replaced by \( n > 4, n \neq 6 \). For further work in this connection see \([11]\) and \([12]\). We remark that Schinzel \([27]\), for the case that \( \alpha \) and \( \beta \) are integers, Rotkiewicz \([26]\), for the case of Lucas numbers, and Schinzel again \([29], [30], [31]\) for the case of Lehmer numbers, determined conditions which ensure the existence of two primitive divisors of \( u_n \).

Since \( v_n = u_{2n}/u_n \) for Lucas or Lehmer numbers \( u_n \) and \( v_n \),

\[
P(v_n) \geq P(\Phi_2(\alpha, \beta)),
\]

and, thus, by \([43]\),

\[
P(v_n) \geq 2n - 1
\]

whenever \( n > e^{462467} \). Notice, to estimate \( P(u_n) \) and \( P(v_n) \) from below it suffices, by \((14)\) and \((17)\), to estimate \( P(\Phi_n(\alpha, \beta)) \) from below. Estimates which improve upon \((15)\) and \((18)\) when the number of distinct prime factors of \( n \) is not too large were first obtained by Stewart \([42]\) for the case when \( \alpha \) and \( \beta \) are integers. These estimates were extended to Lucas and Lehmer numbers \( u_n \) and \( v_n \) by Stewart \([44]\) when \( \alpha \) and \( \beta \) are real and by Shorey and Stewart \([39]\) when \( \alpha \) and \( \beta \) are not real. For any positive integer \( n \) let \( \omega(n) \) denote the number of distinct prime factors of \( n \), put \( q(n) = 2^{\omega(n)} \), the number of squarefree divisors of \( n \), and let \( \phi(n) \) denote the number of positive integers less than or equal to \( n \) and coprime to \( n \). They showed that if \( (\alpha + \beta)^2 \) and \( \alpha \beta \) are non-zero coprime integers with \( \alpha/\beta \) not a root of unity, then for any \( \kappa \) with \( 0 < \kappa < 1/\log 2 \) and any integer \( n \ (>3) \) with at most \( \kappa \log \log n \) distinct prime factors,

\[
P(\Phi_n(\alpha, \beta)) > C(\phi(n)\log n)/q(n),
\]

where \( C \) is a positive number which is effectively computable in terms of \( \alpha, \beta \) and \( \kappa \) only. Thus, in particular, if \( p \) is a prime,

\[
P(u_p) \geq P(\Phi_p(\alpha, \beta)) > C_1 p \log p,
\]

for \( C_1 = C_1(\alpha, \beta) > 0 \). For the proof of \((19)\), estimates for linear forms in logarithms due to Baker \([3]\) and in the \( p \)-adic case due to van der Poorten \([23]\) are employed. By using a result of Stewart \([44]\), which extended earlier work of Erdős \([9]\), on the average distribution of the divisors of integers, Shorey and Stewart \([39], [44]\) also showed that, for all integers \( n \), except perhaps for those in a set of asymptotic density zero,

\[
P(\Phi_n(\alpha, \beta)) > \epsilon(n) n(\log n)^2/\log \log n,
\]

where \( \epsilon(n) \) is any real valued function for which \( \lim_{n \to \infty} \epsilon(n) = 0 \). This yields an improvement of \((12)\) for Lucas and Lehmer numbers \( u_n \) and \( v_n \) by virtue of \((14)\) and \((17)\).
In [45], Stewart showed that there exists an effectively computable positive constant \( c \) such that

\[
Q(\Phi_n(\alpha, \beta)) > n^{(\log n) / (\log \log n)}
\]

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 \( n \). Using (20), Stewart showed that if \( u_n \) is a Lucas or Lehmer number, then there is an effectively computable positive constant \( c_1 \) such that

\[
Q(u_n) > \max\{n^{(\log n) / (\log \log n)}, n^{d(n)/4}\}
\]

for all integers \( n \) larger than a number which is effectively computable in terms of \( \alpha \) and \( \beta \). Inequality (21) remains valid if we replace \( u_n \) by \( v_n \), provided that we replace \( d(n) \) by \( d(n|n|) \), where \( |n|_2 \) denotes the 2-adic value of \( n \) normalized so that \( |2|_2 = 1/2 \). For any positive integer \( n \), \( d(n) \geq q(n) \) and \( d(n|n|_2) \geq q(n)/2 \), hence, there is a positive number \( c_2 \) such that

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

for \( n \) sufficiently large; this result was generalized by Shorey [38] to binary recurrence sequences (recall (13)). Finally, Stewart [45] showed that, for any positive number \( e \) and all positive integers \( n \), except perhaps for those in a set of asymptotic density zero,

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

for any Lucas or Lehmer sequence \((u_n)_{n=0}^\infty\). Further, inequality (22) remains valid if we replace \( u_n \) by \( v_n \).

REFERENCES


6. R. D. Carmichael, *On the numerical factors of the arithmetic forms \( \alpha^n \pm \beta^n \)*, Ann. of Math. (2) 15 (1913), 30–70.


DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO CANADA N2L 3G1