ON LUCAS AND LEHMER SEQUENCES
AND THEIR APPLICATIONS TO DIOPHANTINE EQUATIONS

BY

K. GYÖRY (DEBRECEN), P. KISS (EGER) AND A. SCHINZEL (WARSZAWA)

Consider a Lucas sequence \( \{u_n\} = U(A, B) \) and a Lehmer sequence \( \{v_n\} = V(A, B) \) defined by

\[
u_n = \frac{a_1^n - \beta_1^n}{a_1 - \beta_1}, \quad n > 0,
\]

and

\[
v_n = \begin{cases} 
\frac{a_2^n - \beta_2^n}{a_2 - \beta_2} & \text{if } 2 \nmid n, \\
\frac{a_2^n - \beta_2^n}{a_2^2 - \beta_2^2} & \text{if } 2|n,
\end{cases}
\]

respectively, where \( a_1, \beta_1 \) are roots of the trinomial \( x^2 - Ax + B \), \( a_2, \beta_2 \) are roots of the trinomial \( x^2 - A^{1/2}x + B \), and \( A \) and \( B \) are relatively prime non-zero rational integers such that \( a_1/\beta_1 \) and \( a_2/\beta_2 \) are not roots of unity. As is known, \( u_n \) and \( v_n \) are rational integers. It is also known that for every integer \( m > 1 \) with \( (m, B) = 1 \) both \( \{u_n\} \) and \( \{v_n\} \) have infinitely many terms divisible by \( m \), and that the sets of prime divisors of \( u_n \) and of \( v_n \) \( (n = 2, 3, \ldots) \) are infinite. There is an extensive literature of the linear recursive sequences and their applications; for recent general results we refer to the papers by Schinzel [14]-[18], Mignotte [10], [11], Stewart [21]-[23], Loxton and van der Poorten [9], Kubota [6]-[8], Rotkiewicz and Wasen [13], and to the references mentioned therein.

A prime \( p \) is called a primitive prime divisor of a Lucas number \( u_n \) if \( p \) divides \( u_n \) but does not divide \( (a_1 - \beta_1)^2 u_2 \cdots u_{n-1} \). Similarly, \( p \) is called a primitive prime divisor of \( v_n \) if \( p \) divides \( v_n \) but does not divide \( (a_2 - \beta_2)^2(a_2 + \beta_2)^2 v_3 \cdots v_{n-1} \). By a more general theorem of Schinzel (see Theorem 1 and its Corollary 2 in [18]), for any Lucas sequence \( \{u_n\} \) and for any Lehmer sequence \( \{v_n\} \) the numbers \( u_n \) and \( v_n \) have primitive prime divisors for \( n > n_0 \), where \( n_0 \) is an effectively computable absolute
constant. Using a recent result of Baker [1], Stewart [21] (see also [23])
computed explicitly the constant occurring in Theorem 1 of Schinzel [18],
and so he obtained the explicit value \( e^{453 \cdot 4^{67}} \) for \( n_0 \). Furthermore, Stewart
proved in [21], [23] that there are only finitely many Lucas and Lehmer
sequences whose \( n \)-th term, \( n > 6, n \neq 8, 10 \) or \( 12 \), does not have a primiti
te divisor and these sequences may be explicitly determined.

In this note we show that the above-quoted theorems of Schinzel [18]
and Stewart [21], [23] together with the effective estimates obtained for
the solutions of the Thue-Mahler equation (see, e.g., Coates [3], Sprindžuk
[20], and Kotov and Sprindžuk [5a]) and a recent result of Kotov [5]
imply the following

**Theorem.** Let \( p_1, \ldots, p_s \) be a finite set of primes with \( \max(p_i) = P \)
and denote by \( S \) the set of non-zero integers which have only these primes
as prime factors. If \( t_x \) is the \( x \)-th term of a Lucas sequence \( U(A, B) \) or a Lehmer
sequence \( V(A, B) \), \( x > 4 \) or \( x > 6 \), respectively, and

\[
t_x \in S,
\]

then

\[
x \leq \max\{e^{453 \cdot 4^{67}}, P + 1\}
\]

and

\[
\max(|A|, |B|) < c_1, \quad |t_x| < c_3,
\]

where \( c_1 \) and \( c_3 \) are effectively computable numbers depending only on \( P \) and \( s \).

We remark that for \( x \leq 6 \) or for \( x \leq 4 \) and Lucas sequences our
theorem does not remain valid in general.

Recently Loxton and van der Poorten [9] have proved that if \( \{u_n\} \)
is a fixed non-degenerate linear integer recurrence of order \( m \geq 2 \) whose
auxiliary polynomial has at least two distinct roots, then the set of posi
tive integers \( n \) such that \( u_n \in S \) has density zero.

An easy corollary to our Theorem is as follows:

**Corollary 1.** Let \( S \) be defined as in the Theorem. Then the equation

\[
\frac{u^x - v^x}{u - v} = w
\]
in integers \( x, u, v, w \) with \( x > 3, u > v \geq 1, (u, v) = 1, w \in S \) implies

\[
x \leq P \quad \text{and} \quad \max\{u, w\} < c_3,
\]

where \( c_3 \) is an effectively computable number depending only on \( P \) and \( s \).

Denote by \( P(n) \) and \( v(n) \) the greatest prime factor and the number of
distinct prime factors of a positive integer \( n \), respectively. The following
corollary is a special case of Corollary 1.
COROLLARY 2. Let \( n > 1 \) be a fixed rational integer. Then the equation

\[
\frac{u^x - v^x}{u - v} = n^y
\]

in integers \( x, y, u, v \) with \( x > 3, y \geq 1, u > v \geq 1, (u, v) = 1 \) implies

\[ x \leq P(n) \quad \text{and} \quad \max\{u, y\} < c,
\]

where \( c \) is an effectively computable number depending only on \( P(n) \) and \( n \).

Remarks. 1. Similar corollaries can be obtained by applying our Theorem to special Lehmer sequences.

2. Szymiczek [24] proved that, for fixed \( u, v \), equation (3) has at most one solution in positive integers \( x, y \).

3. In [19] Shorey and Tijdeman obtained a number of conditions each of which implies the finiteness of the number of solutions of the equation

\[
a \frac{u^x - 1}{u - 1} = bn^y
\]

in integers \( x > 2, y > 1, u > 1, n > 1 \). From their result our Corollaries 1 and 2 follow in the special case \( v = 1 \).

4. Some special cases of equations (2) and (3) have been collected by Hugh [4]. For further related equations and results the reader may consult the papers [24], [4], [19] and [12].

Proof of the Theorem. Let \( t_x \) be the \( x \)-th term of a Lucas sequence \( U(A, B) \) or a Lehmer sequence \( V(A, B) \). It is known (cf. [22]) that if \( q \) is a primitive prime divisor of \( t_x \) and \( x \geq 4 \), then \( x \leq \max(4, q + 1) \). Put

\[
n_1 = \max\{4^{\log_2 4}, 4^{67}, P + 1\}.
\]

If \( x > n_1 \), by the above-quoted theorem of Stewart [21], [23] \( t_x \) has a prime factor different from \( p_1, \ldots, p_s \). So \( t_x \in S \) yields \( x \leq n_1 \).

Let \( d \geq 3 \) be an integer and denote by \( \Phi_d(y, x) \) the \( d \)-th cyclotomic polynomial in a homogeneous form. Let \( \xi = e^{2\pi i/d} \) and let \( \alpha \) and \( \beta \) be roots of the equation \( x^d - Kx + B = 0 \), where \( K = A \) or \( K = A^{1/2} \). Clearly, \( \alpha + \beta = K \) and \( a \beta = B \). Put \( E = \alpha^2 + \beta^2 \), where, obviously, \( E = K^2 - 2B \). Following Stewart [21], [23], we get

\[
\Phi_d(\alpha, \beta) = \prod_{\frac{1}{d} \leq d \leq \frac{\varphi(d)}{d}} ((\alpha - \xi^i \beta)(\alpha - \xi^{-i} \beta)) = \prod_{\frac{1}{d} \leq d \leq \frac{\varphi(d)}{d}} ((\alpha^2 + \beta^2) - (\xi^i + \xi^{-i})a \beta) = F_d(E, B),
\]

where \( F_d(y, x) \) is a homogeneous irreducible polynomial of degree \( \varphi(d)/2 \) with rational integer coefficients. The maximum absolute value of its coefficients can be estimated from above by an explicit expression in \( d \).
Suppose now that \( t_x \in S \) and \( 6 < x \leq n_1 \). Then we obtain
\[
 t_x = \frac{a^x - \beta^x}{\alpha - \beta} = \prod_{d \mid x \geq 1} \Phi_d(\alpha, \beta) \quad \text{or} \quad t_x = \frac{\alpha^x - \beta^x}{\alpha^x - \beta^x} = \prod_{d \mid x} \Phi_d(\alpha, \beta),
\]
whence, by (4), we have
\[
 \prod_{d \mid x} F_d(E, B) \in S.
\]
(5)

Thus
\[
 F_x(E, B) \in S.
\]
(6)

In view of \( (A, B) = 1 \) we have \( (E, B) = 1 \).

If \( x \neq 8, 10 \) and 12, then \( F_x(E, B) \) is of degree \( \varphi(x)/2 \geq 3 \) and, by the theorem of Coates [3] or Sprindžuk [20], the Thue-Mahler equation (6) has only finitely many solutions in integers \( E, B \), and an effectively computable upper bound \( c_6(P, s) \) can be given for \( \max(|E|, |B|) \) and so also for \( \max(|A|, |B|) \). In cases \( x = 8, 10 \) and 12 the left-hand side of equation (5) has at least three distinct linear factors in \( E \) and \( B \) and, using an appropriate formulation of a recent theorem of Kotov and Sprindžuk [5a], we also get \( \max(|A|, |B|) < c_6 \) with an effectively computable number \( c_6 \) depending only on \( P \) and \( s \).

It remains to consider the case \( t_x = u_x, \ x = 5 \) or 6. We have \( 4t_x = (2B - 3A^2)^2 - 5A^4 \), \( 3t_6 = A[(3B - 2A^2)^2 - A^4] \) and, since \( (A, B) = 1 \), we obtain \( (2B - 3A^2, A)|2 \) and \( (3B - 2A^2, A)|3 \).

By a theorem of Kotov [5] on the greatest prime factor of \( \alpha x^m + \beta y^n \) with \( m = 2, \ n = 4 \) the relations \( t_x \in S \) or \( t_x \in S \) imply
\[
 \max(|2B - 3A^2|, |A|) < c_7(P, s) \quad \text{or} \quad \max(|3B - 2A^2|, |A|) < c_7(P, s),
\]
which gives an upper bound \( \max(|A|, |B|) \).

Proof of Corollary 1. Suppose that (2) holds for some integers \( x, u, v, w \) with \( x > 3, \ u > v \geq 1, \ (u, v) = 1, \ w \in S \). Then \( (u^x - v^x)/(u - v) \) is the \( x \)-th term of the Lucas sequence \( \{u_n\} = U(A, B) \), where \( A = u + v > 0, \ B = uv > 0 \) and \( (A, B) = 1, \ D = A^2 - 4B \neq 0 \).

First we derive the required upper bound for \( x \). If \( p \) is a prime, \( p|u_n \) and \( p \nmid u_m \) for \( 0 < m < n \), then, as is known, \( n \leq p \) (since \( D \) is a perfect square). Furthermore, if \( n > 2, \ u_n \) has a primitive prime divisor except for \( n = 6, \ u = 2, \ v = 1 \) (see [25] or [2]). Therefore, apart from \( x = 6, \ u = 2, \ v = 1, \ u_x \in S \) implies \( x \leq P \). But if \( x = 6, \ u = 2, \ v = 1 \) and \( u_x \in S \), then \( S \) must contain 7, and so \( x \leq P \) also holds.

In case \( x > 4 \) we may apply our Theorem and we get \( \max(u, w) < c_8(P, s) \) with an effectively computable number \( c_8(P, s) \). Finally, for \( x = 4, 5 \) and 6 it follows from the result of Coates [3] and Sprindžuk [20] that (2) has only finitely many solutions in \( u, v, w \) and \( \max(u, w) < c_9 \) with an effectively computable number \( c_9 \) depending only on \( P \) and \( s \).
REFERENCES


Reçu par la Rédaotion le 10. 10. 1978;
en version modifiée le 15. 2. 1979