On some arithmetical properties of Lucas and Lehmer numbers

by

K. Győry (Debrecen)

As is well known, the Lucas numbers $u_n$ are defined by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n > 0,$$

where $\alpha + \beta$ and $\alpha \beta$ are relatively prime non-zero rational integers and $\alpha/\beta$ is not a root of unity, while the Lehmer numbers $v_n$ satisfy

$$v_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{for } n \text{ odd,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{for } n \text{ even,} \end{cases}$$

where $(\alpha + \beta)^2$ and $\alpha \beta$ are relatively prime non-zero rational integers and $\alpha/\beta$ is not a root of unity. The Lucas and Lehmer numbers are rational integers.

Let $p_1, \ldots, p_s$ be rational primes with $\max(p_i) = P$ and denote by $S$ the set of rational integers which have only these primes as prime factors. In our joint paper [6] with Kiss and Schinzel we proved that if $u_n$ is a Lucas or a Lehmer number with $n > 6$ and $u_n \in S$ then

$$n \leq \max\{C_1, P + 1\}$$

with $C_1 = \sigma^{42} A^{47}$ and

$$\max\{|a|, |\beta|, |u_n|\} < C_2$$

where $C_2$ is an effectively computable positive number depending only on $P$ and $\sigma$. In proving this theorem we combined an explicit form of a result of Schinzel [10] (i.e. a theorem of Stewart [13]) on Lucas and Lehmer numbers with the effective estimates obtained for the solutions of the Thue–Mahler equation ([9], [13], [7]).
Recently, I have obtained ([5], Corollary 1) improved and explicit upper bounds for the integer solutions of the Thue–Mahler equation, subject to the weaker condition that the form occurring in the equation has at least three distinct linear factors. This together with Stewart’s theorem [15] enables us to establish the following improvements of (2).

**Theorem 1.** Let \( u_n \) be a Lucas number or a Lehmer number defined as above with \( n > 6 \). If \( u_n \in S \), then

\[
\max \{|a|, |\beta|, |u_n|\} < \exp \left\{ (2000 \exp(n)^{8} \log(n)^{3} (5n+2) \log(n)^{2} + 15 \log(n)^{2} + 15) \right\} \times s^{\gamma(n)} (5n+2) \log(n)^{2} + 15 \log(n)^{2} + 15 \log(n)^{2} + 15 \}
\]

where \( \gamma(n) \) denotes Euler’s function.

From (1) and Theorem 1 we obtain the following

**Theorem 2.** Let \( u_n \in S \) be as in Theorem 1 with \( n > 6 \). If \( n \leq C_1 \) then

\[
\max \{|a|, |\beta|, |u_n|\} < \exp \left\{ (2000 \exp(n)^{8} \log(n)^{3} (5n+2) \log(n)^{2} + 15 \log(n)^{2} + 15) \right\} \times s^{\gamma(n)} (5n+2) \log(n)^{2} + 15 \log(n)^{2} + 15 \log(n)^{2} + 15 \}
\]

and if \( n > C_1 \) then

\[
\max \{|a|, |\beta|, |u_n|\} < \exp \left\{ (2000 \exp(n)^{8} \log(n)^{3} (5n+2) \log(n)^{2} + 15 \log(n)^{2} + 15) \right\} \times s^{\gamma(n)} (5n+2) \log(n)^{2} + 15 \log(n)^{2} + 15 \log(n)^{2} + 15 \}
\]

\( P(m) \) and \( \omega(m) \) will signify the greatest prime factor and the number of distinct prime factors of \( m \). From (2) it follows that \( P(u_n) \to \infty \) as \( |u_n| \to \infty \) with \( n > 6 \). Theorem 2 implies this result in a quantitative form. The following theorem allows us to get some new information about the arithmetical structure of Lucas and Lehmer numbers.

**Theorem 3.** Let \( u_n \) be a Lucas or a Lehmer number with \( n > 6 \) and \( |u_n| > C_2 \) where \( C_2 = \exp \exp \left\{ 40 \log(C_1) \log(C_1) \right\} \). Then

\[
4sP^2 \log P > \log \log |u_n| \quad \text{and} \quad P > \frac{1}{2} (\log \log |u_n|)^{1/3}
\]

where \( P = P(u_n) \) and \( s = \omega(u_n) \).

We remark that by the results of Carmichael [1], Ward [18] and Schinzel [9] we have \( P(u_n) \geq n - 1 \) for all sufficiently large integers \( n \). Recently Stewart [16] and Shorey and Stewart [13] obtained more precise lower bounds for \( P(u_n) \) in terms of \( n \) for “almost all” positive integers \( n \) (i.e., except for a set of integers \( n \) of asymptotic density zero). Stewart [14], [16], Erdős and Shorey [4] and Shorey and Stewart [11] established good lower estimates for \( P(u_n) \) as \( n \) runs through certain special but important sets of integers. These estimates do not imply (5) and (6), because the lower bounds in our Theorem 3 depend on \( u_n \) in place of \( n \).

**Corollary.** Let \( S \) be as above. Then the equation

\[
\frac{u^2 - v^2}{u - v} = w
\]

in integers \( u, \; v, \; w \) with \( u > v > 3, \; u > v \geq 1, \; (u, v) = 1, \; w \in S \) implies \( w \leq P \) and

\[
\max (u, w) < \exp \left\{ (2000 \exp(n)^{8} (2000 \exp(n)^{8} \log(n)^{2} + 15 \log(n)^{2} + 15 \log(n)^{2} + 15) \right\} \times \exp \exp \left\{ 40 \log(C_1) \log(C_1) \right\}
\]

**Proof of Theorem 1.** We follow the proof of the theorem of [6]. Suppose that \( u_n \in S \) is a Lucas number or a Lehmer number with \( n > 6 \). Write \( a \beta = B \) and \( a + \beta = A \) or \( a - \beta = A \) according as \( u_n \) is a Lucas or a Lehmer number. Putting \( a \beta = E \), we have \( E = A^2 - 2B \) or \( B = A - 2B \) and \( (A, B) = 1 \).

We denote the \( \delta \)-cyclotomic polynomial in \( x \) and \( y \) by \( \Phi_\delta(x, y) \). We have

\[
u_n = \frac{a^n - \beta^n}{a - \beta} = \prod_{d \mid n} \Phi_\delta(a, \beta), \quad n > 0,
\]

or

\[
u_n = \frac{a^n - \beta^n}{a^n - \beta^n} = \prod_{d \mid n} \Phi_\delta(a, \beta) \quad \text{for} \; n \; \text{even}.
\]

Let \( d \geq 3 \) and \( \zeta = e^{2\pi i/3} \). Then

\[
\Phi_\delta(a, \beta) = \Phi_d(\xi, B, E),
\]

where

\[
\Phi_d(\xi, B, E) = \prod_{i=1}^{d-1} (\xi - (\zeta^i + \zeta^{-i}))
\]

is an irreducible polynomial of degree \( \phi(d)/2 \) with rational integer coefficients. Since \( \Phi_\delta(a, \beta) \neq 0 \), we obtain in both cases

\[
G(B, E) = \prod_{d \mid n} \Phi_d(\xi, B, E) \in S
\]

where \( G(x, y) \) is a homogeneous polynomial with rational integer coefficients and with at least three distinct linear factors in its factorization.

(10) is a Thue–Mahler equation in \( E, B \), so we may apply Corollary 1 of [5]. Denote by \( K = K_0 \), the maximal real subfield of the \( \delta \)-cyclotomic field and let \( K = K_0 \), \( E_K \) and \( h_K \) be the degree, the regulator and the class number of \( K \). [6] and [7] will signify the degree and the maximum of the absolute values of the coefficients of \( G \). Then we have

\[
\max (|E(1)|, |B|) < \exp \left\{ (2000 \exp(n)^{8} \log(n)^{2} + 15 \log(n)^{2} + 15 \log(n)^{2} + 15) \right\} \times \Phi_d(\xi, B, E) \log^2 (E_K h_K) (E_K + h_K \log P)^{s/3} \times (E_K + s h_K \log P + |G| \log |G|).
\]
it is clear that
\[ |G| \leq (n-1)/2 \quad \text{and} \quad |G| \leq 3^{n/2}. \]
Further, by a well-known explicit estimate of Siegel [12]
\[ B_K \leq 4|D_K|^{13} \log |D_K|^{13} \]
where \(D_K\) denotes the discriminant of \(K\). As is known, \(D_K\) divides the
discriminant of the \(n\)th cyclotomic field which can be estimated from above by \(n^{\sigma(n)}\) (see, e.g., \[2\]). So
\[ |D_K| \leq n^{\sigma(n)} \cdot 2. \]
Furthermore, by a theorem of Pohst [8] we have \(B_K \geq 0.373\). This together
with (13), (14), (12) and (11) give
\[ \max(|E|, |B|) < \exp \left[ \left( 20^{12} \sigma(n) \right)^{\frac{1}{2}} \left( \frac{\log n}{n} \right)^{\frac{1}{2}} \left( \log \log n \right)^{\frac{1}{2}} \right] \times \left( \log \log n \right)^{\frac{1}{2}} \left( \log \log \log n \right)^{\frac{1}{2}} < C_4. \]
Thus
\[ \max(|a|, |b|, |b_0|) < (3C)^3 \]
and this implies (3).

Proof of Theorem 3. Let \(p_1, \ldots, p_s\) denote the distinct prime divisors of \(a_n\). In case \(a \leq C_1\) we deduce from (4') that
\[ \log \log |a_n| < C_1(2C_1 \log C_1 + \sigma P + \log P + \log \log P). \]
Since \(P < C_1\) contradicts the assumption \(|a_n| > C_1\), hence \(P > C_1\), and (15)
yields (5). If \(a > C_1\), (5) immediately follows from (4'). Since for \(x 
> 1\) we have \(\pi(x) < 2x/\log x\) (see e.g. [17]), it follows that \(x < \pi(P) < 2P/\log P\).
Thus (5) implies (6).

I owe this reference [17] to Professor A. Schinzel.

Proof of the Corollary. Let \(a, b, c, \alpha\) be an arbitrary but fixed solution of (7) with \(a > 3, b > c > 1, (a, b, c) = 1\) and \(a = b = c\). In [6] we proved that \(x_1 < P\). When \(x > 6\), we may apply Theorem 1 to the equation (7) and (8) follows. For \(x = 4, 5, 6\) we may employ Corollary 1 of [5] and this also gives (8).

References

[1] R. D. Carmichael, On the numerical factors of the arithmetical form \(\alpha^x + \beta^y\),
[4] T. Erdős and P. Erdős, On the greatest prime factor of \(2^n - 1\) for a prime
\(n\) and other expressions, Illid 30 (1970), pp. 267-265.
[5] K. Györy, Explicit upper bounds for the solutions of some diophantine equations,
[6] K. Györy, I. Kiss, and A. Schinzel, A note on Lucas and Lehmer sequences and
their applications to diophantine equations, Colloq. Math. to appear.
fields and approximation of algebraic numbers by algebraic numbers,
[8] M. Pohst, Beugungsdiskussionen für rationale algebraische Zahlkörper, J.
[9] A. Schinzel, The algebraic divisors of Lehmer numbers in the case of negative
[10] ——–, Primitive divisors of the expression \(p^n - b^n\) in algebraic number fields, J.
[13] V. G. Sprindžuk, Rational approximation to algebraic numbers, (Russian),
pp. 427-433.
[15] ——–, Primitiv divisors of Lucas and Lehmer numbers, in: Transcendence theory:
Advances and applications (ed. A. Baker and D. W. Masser), pp. 75-92,
pp. 230-236.

MATHEMATICAL INSTITUTE
KOŠUTH LÁSZLÓ UNIVERSITY
H-6720 Debrecen 16, Hungary

Received on 13.12.1979