ACTA ARITHMETICA
XL (1982)

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 α/β is not a root of unity, while the Lehmer numbers u_n satisfy

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

where $(\alpha+\beta)^2$ and $\alpha\beta$ are relatively prime non-zero rational integers and α/β 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

$$n \leqslant \max\{C_1, P+1\} \tag{1}$$

with $C_1 = e^{452}4^{67}$ and

$$\max\{|\alpha|, |\beta|, |u_n|\} < C_2 \tag{2}$$

where C_2 is an effectively computable positive number depending only on P and s. In proving this theorem we combined an explicit form of a result of Schinzel [10] (i.e. a theorem of Stewart [15]) on Lucas and Lehmer numbers with the effective estimates obtained for the solutions of the Thue–Mahler equation ([3], [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*

$$\max\{|\alpha|, |\beta|, |u_n|\} < \exp\left\{(20n\varphi(n))^{s\varphi(n)(3\varphi(n)/4+11/2)+13\varphi(n)+24} \times \times s^{s\varphi(n)(\varphi(n)+11)/2+11\varphi(n)+20} P^{\varphi(n)/2} (\log P)^{s\varphi(n)/2+9}\right\} \tag{3}$$

where $\varphi(n)$ 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 $n \leqslant C_1$ then*

$$\max\{|\alpha|, |\beta|, |u_n|\} < \exp\left\{\left(C_1^{2sC_1} s^{sC_1} P (\log P)^s\right)^{C_1}\right\} \tag{4}$$

and if $n > C_1$ then

$$\max\{|\alpha|, |\beta|, |u_n|\} < \exp\{(sP^{7/4})^{sP^2}\}. \tag{4'}$$

$P(m)$ 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 $|u_n| > C_3$ where $C_3 = \exp\exp\{4C_1^3 \log C_1\}$. Then*

$$4sP^2 \log P > \log\log |u_n| \tag{5}$$

and

$$P > \tfrac{1}{2}(\log\log |u_n|)^{1/3} \tag{6}$$

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 $P(u_n) \geqslant n-1$ for all sufficiently large integers n. Recently Stewart [16] and Shorey and Stewart [11] 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], Erdös 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*

$$\frac{u^x - v^x}{u - v} = w \tag{7}$$

in integers x, u, v, w with $x > 3$, $u > v \geqslant 1$, $(u, v) = 1$, $w \in S$ implies $x \leqslant P$ and

$$\max(u, w) < \exp\{s^{sP(P+30)/2}(20P^2)^{sP(P+6)+14(P+2)}\}. \tag{8}$$

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 $\alpha\beta = B$ and $\alpha+\beta = A$ or $(\alpha+\beta)^2 = A$ according as u_n is a Lucas or a Lehmer number. Putting $\alpha^2+\beta^2 = E$, we have $E = A^2-2B$ or $E = A-2B$ and $(E, B) = 1$.

We denote the dth cyclotomic polynomial in x and y by $\Phi_d(x, y)$. We have

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_{\substack{d \mid n \\ d > 1}} \Phi_d(\alpha, \beta), \quad n > 0,$$

or

$$u_n = \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} = \prod_{\substack{d \mid n \\ d \geqslant 3}} \Phi_d(\alpha, \beta) \quad \text{for } n \text{ even}.$$

Let $d \geqslant 3$ and $\zeta = e^{2\pi i/d}$. Then

$$\Phi_d(\alpha, \beta) = F_d(E, B),$$

where

$$F_d(z, 1) = \prod_{\substack{(t,d)=1 \\ 1 \leqslant t < d/2}} \left(z - (\zeta^t + \zeta^{-t})\right) \tag{9}$$

is an irreducible polynomial of degree $\varphi(d)/2$ with rational integer coefficients. Since $\Phi_2(\alpha, \beta) \neq 0$, we obtain in both cases

$$G(E, B) = \prod_{\substack{d \mid n \\ d \geqslant 3}} F_d(E, B) \in S \tag{10}$$

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 $K = K_n$ the maximal real subfield of the nth cyclotomic field and let $k = \varphi(n)/2$, R_K and h_K be the degree, the regulator and the class number of K. $|G|$ and $\|G\|$ will signify the degree and the maximum of the absolute values of the coefficients of G. Then we have

$$\max(|E|, |B|) < \exp\left\{|G|^2 (25(k+sk+2)k)^{2sk^2+11sk+22k+20} \times \times P^k (\log P)^6 R_K \log^3(R_K h_K)(R_K + h_K \log P)^{sk+2} \times \times (R_K + sh_K \log P + |G| \log \|G\|)\right\}. \tag{11}$$

It is clear that

$$|G| \leqslant (n-1)/2 \quad \text{and} \quad \|G\| \leqslant 3^{n/2}. \tag{12}$$

Further, by a well-known explicit estimate of Siegel [12]

$$R_K h_K < 4\,|D_K|^{1/2}(\log |D_K|)^{k-1} \tag{13}$$

where D_K denotes the discriminant of K. As is known, D_K^2 divides the discriminant of the nth cyclotomic field which can be estimated from above by $n^{\varphi(n)}$ (see, e.g., [2]). So

$$|D_K| \leqslant n^{\varphi(n)/2}. \tag{14}$$

Furthermore, by a theorem of Pohst [8] we have $R_K \geqslant 0.373$. This together with (13), (14), (12) and (11) give

$$\max(|E|, |B|) < \exp\left\{(20n\varphi(n))^{s\varphi(n)(3\varphi(n)/4+11/2)+13\varphi(n)+23} \times \right.$$
$$\left. \times s^{s\varphi(n)(\varphi(n)+11)/2+11\varphi(n)+20} P^{\varphi(n)/2}(\log P)^{s\varphi(n)/2+9}\right\} = C_4.$$

Thus

$$\max(|\alpha|, |\beta|, |u_n|) < (3C_4)^n$$

and this implies (3).

Proof of Theorem 3. Let $p_1, \ldots, p_s$ denote the distinct prime divisors of u_n. In case $n \leqslant C_1$ we deduce from (4) that

$$\log\log|u_n| < C_1(2sC_1\log C_1 + sC_1\log s + \log P + s\log\log P). \tag{15}$$

Since $P \leqslant C_1$ contradicts the assumption $|u_n| > C_3$, hence $P > C_1$ and (15) yields (5). If $n > C_1$, (5) immediately follows from (4′). Since for $x > 1$ we have $\pi(x) \leqslant 2x/\log x$ (see e.g. [17]), it follows that $s \leqslant \pi(P) \leqslant 2P/\log P$. Thus (5) implies (6).

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

Proof of the Corollary. Let x, u, v, w be an arbitrary but fixed solution of (7) with $x > 3$, $u > v \geqslant 1$, $(u, v) = 1$ and $w \in S$. In [6] we proved that $x \leqslant P$. When $x > 6$, we may apply Theorem 1 to the equation (7) and (8) follows. For $x = 4, 5$ and 6 we may employ Corollary 1 of [5] and this also gives (8).

References

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

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, London and New York, 1967.

[3] J. Coates, *An effective p-adic analogue of a theorem of Thue. II. The greatest prime factor of a binary form*, Acta Arith. 16 (1970), pp. 399–412.

[4] P. Erdös and T. N. Shorey, *On the greatest prime factor of* 2^p-1 *for a prime p and other expressions*, ibid. 30 (1976), pp. 257–265.

[5] K. Győry, *Explicit upper bounds for the solutions of some diophantine equations*, Ann. Acad. Sci. Fenn. Ser. AI. Math. 5 (1980), pp. 3–12.

[6] K. Győry, P. Kiss, and A. Schinzel, *A note on Lucas and Lehmer sequences and their applications to diophantine equations*, Colloq. Math. to appear.

[7] S. V. Kotov and V. G. Sprindžuk, *The Thue–Mahler equation in relative fields and approximation of algebraic numbers by algebraic numbers* (Russian), Izv. Akad. Nauk SSSR 41 (1977), pp. 723–751.

[8] M. Pohst, *Regulatorabschätzungen für total reelle algebraische Zahlkörper*, J. Number Theory 9 (1977), pp. 459–492.

[9] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), pp. 413–416.

[10] — *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), pp. 27–33.

[11] T. N. Shorey and C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers II*, J. London Math. Soc. 23 (1981), pp. 17–23.

[12] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen, Math. Phys. Kl. (1969), pp. 71–86.

[13] V. G. Sprindžuk, *Rational approximation to algebraic numbers* (Russian), Izv. Akad. Nauk SSSR 35 (1971), pp. 991–1007.

[14] C. L. Stewart, *The greatest prime factor of* $a^n - b^n$, Acta Arith. 26 (1975), pp. 427–433.

[15] — *Primitive divisors of Lucas and Lehmer numbers*, in: *Transcendence theory: Advances and applications* (ed. A. Baker and D. W. Masser), pp. 79–92, London–New York–San Francisco 1977.

[16] — *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. 24 (1977), pp. 425–447.

[17] E. Trost, *Primzahlen*, 2te Auflage, Birkhäuser Verlag, 1968.

[18] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), pp. 230–236.

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
H-4010 Debrecen 10, Hungary

Received on 13.12.1979 (1188)