Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 67–73*

ON SOME ARITHMETICAL PROPERTIES OF LUCAS AND LEHMER NUMBERS, II.

Kálmán Győry* **(Debrecen)**

Dedicated to the memory of Professor Péter Kiss

Abstract. Denote by S the set of non-zero integers composed only of finitely many given primes. We proved with Kiss and Schinzel [7] that if u_n is a Lucas or Lehmer number with $n>6$ and $u_n \in S$, then $|u_n|$ can be estimated from above in terms of S. An explicit upper bound for $|u_n|$ was given later in our article [5]. In the present paper a significant improvement of this bound is established which implies, among other things, that $P(u_n) > \frac{1}{4}(\log\log|u_n|)^{1/2}$ if $n>30$ or if $30 \geq n > 6$ and $|u_n|$ is sufficiently large.

AMS Classification Number: 11B39, 11D61

1. Introduction

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

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

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 non-zero rational integers.

*Supported in part by the Netherlands Organization for Scientific Research, the Hungarian Academy of Sciences and by grants 29330, 38225 and 42985 of the Hungarian National Foundation for Scientific Research.

Let $p_1, \dots, p_s$ be rational primes with $\max_i p_i = P$, and denote by S the set of non-zero rational integers not divisible by primes different from $p_1, \dots, p_s$. We proved with Kiss and Schinzel [7] that if u_n is a Lucas number or a Lehmer number with $n > 6$ and $u_n \in S$ then

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

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

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

where C_2 is an effectivelly computable positive number depending only on P and s. The proof of (1) was based on a result of Stewart [15] which asserts that for $n > C_1$, the Lucas and Lehmer numbers u_n always have a primitive prime divisor. To prove (2), we reduced the problem to Thue–Mahler equations and used the bound available at that time for the solutions of such equations. Later, in [5], I made C_2 completely explicit by means of an explicit and improved bound from [4] on the solutions of Thue–Mahler equations. As a consequence, I showed in [5] that if u_n is a Lucas or Lehmer number with $n > 6$ and $|u_n| > \exp\exp\{4C_1^3 \log C_1\}$ then

$$4sP^2 \log P > \log\log |u_n| \tag{3}$$

and

$$P > \frac{1}{2}(\log\log |u_n|)^{1/3}, \tag{4}$$

where $P = P(u_n)$ and $s = \omega(u_n)$. Here $P(u_n)$ and $\omega(u_n)$ signify the greatest prime factor and the number of distinct prime factors of u_n (with the convention that $P(\pm 1) = 1, \omega(\pm 1) = 0$).

As is known, there are various lower bounds for $P(u_n)$ in terms of n, valid for all or "almost all" n, see e.g. [3], [16], [12], [14], [13], [8], [17] and the references given there. However, these estimates do not imply (3) and (4), because the lower bounds in (3) and (4) depend on u_n and not on n. Theorem 2 of [8] gives also a lower bound of the form

$$c(\log\log |u_n|)^2 \log\log\log |u_n|, \text{ if } |u_n| > c'.$$

for $P(u_n)$. In contrast with (4), the constants c, c' depend, however, on α, β and S as well.

Recently, Bilu, Hanrot and Voutier [1] significantly improved Stewart's result [15] by showing that for $n > 30, u_n$ has a primitive prime divisor. This will enable us to prove (1) with C_1 replaced by 30. Furthermore, in 1998 I succeeded (cf. [6]) to improve upon the previous bound of [4] on the solutions of Thue–Mahler equations, that is, in another formulation, on the S-integral solutions of Thue equations. Using this improvement from [6] and following the arguments of [5], we shall derive (2) with an explicit bound C_2 which is much better than the previous one in [5]. As a consequence, we obtain also some improvements of (3) and (4).

Keepeng the above notation, let $\varphi(n)$ denote Eurler's function.

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

$$n \leq \max\{30, P+1\}. \tag{5}$$

Further,

$$\max\{|\alpha|, |\beta|, |u_n|\}$$

is bounded above by

$$\exp\{(k(s+1))^{9k(s+2)} P^k (\log P)^{sk+2}\}, \tag{6}$$

where $k = \varphi(n)/2$.

The inequality (5) is a significant improvement of (1), while (6) improves upon considerably (3) of [5].

From (5) and (6) we deduce the following improvements of (3) and (4).

Corollary. *Let u_n be a Lucas or a Lehmer number with $n > 30$, or with $30 \geq n > 6$ and $|u_n| > \exp\exp\{7040\}$. Then we have*

$$9(s+2)P\log P > \log\log|u_n| \tag{7}$$

and

$$P > \frac{1}{4}(\log\log|u_n|)^{1/2}, \tag{8}$$

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

2. Proofs

Proof of the Theorem. We follow the proof of Theorem 1 of [5]. Let $u_n \in S$ be a Lucas number or a Lehmer number with $n > 6$. Then (5) follows in the same way as (1) was proved in [7] if we raplace Stewart's result [15] by the above-mentioned theorem of Bilu, Hanrot and Voutier [1] on primitive prime divisors.

To prove (6), we first introduce some notation. Put $\alpha\beta = B$ and $\alpha + \beta = A$ or $(\alpha+\beta)^2 = A$ according as u_n is a Lucas or a Lehmer number. Setting $\alpha^2 + \beta^2 = E$, we get $E = A^2 - 2B$ or $E = A - 2B$ and $\gcd(E, B) = 1$.

Denote by $\Phi_d(x,y)$ the d-th cyclotomic polynomial in homogeneous form. Then we have

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

or

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

If $\zeta = e^{2\pi i/d}$ and $d \geq 3$, then

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

where

(9) $$F_d(z,1) = \prod_{\substack{\gcd(t,d)=1 \\ 1 \leq t < d/2}} (z - (\zeta^t + \zeta^{-t}))$$

is an irreducibile polynomial of degree $\varphi(d)/2$ with coefficients from $\mathbf{Z}$. We infer now in both cases that there are non-negative integers $z_1, \ldots, z_s$ such that

(10) $$G(E,B) = \prod_{\substack{d \mid n \\ d \geq 3}} F_d(E,B) = \pm p_1^{z_1} \cdots p_s^{z_s}.$$

Here $G(x,y)$ is a homogeneous polynomial with coefficients from $\mathbf{Z}$. Further, in view of $n > 6$, the degree of G, denoted by g, satisfies

$$3 \leq g \leq \frac{n-1}{2}.$$

We note that $G(x,y)$ is not irreducibile in general, but its linear factors over $\bar{\mathbf{Q}}$ are pairwise linearly independent. Putting

$$z_i = g z_i^{'} + z_i^{''} \text{ with integers } z_i^{'} \geq 0, 0 \leq z_i^{''} < g, 1 \leq i \leq s,$$

and

$$D = p_1^{z_1^{'}} \cdots p_s^{z_s^{'}}, b = \pm p_1^{z_1^{''}} \cdots p_s^{z_s^{''}},$$

(10) implies

(11) $$G\left(\frac{E}{D}, \frac{B}{D}\right) = b$$

which can be regarded as a Thue equation in the S-integers $\frac{E}{D}, \frac{B}{D}$.

We apply *) now Theorem 1 of [6] with $m = 2$ to equation (11). Denote by $K = K_n$ the maximal real subfield of the n-th cyclotomic field. Its degree is $k = \varphi(n)/2$. Let h_K, R_K, D_K and R_S be the class number, regulator, discriminant and $S-$regulator (for its definition see e.g. [6]) of K. Further, we write $\log^* \alpha$ for $\max\{\log \alpha, 1\}$. Then using Theorem 1 of [6], one can deduce the estimate

$$(12) \quad \begin{aligned} &\max(|E|, |B|) < \exp\{c_1 P^k R_S(\log^* R_S). \\ &(\log^*(PR_S)/\log^* P)(R_K + h_K \log Q + 2g + \log |b|)\}, \end{aligned}$$

where

$$c_1 = n(k(s+1))^{8ks+9k+11}.$$

As is known, (see e.g. [6])

$$\log^*(PR_S)/\log^* P \leq 2\log^* R_S \text{ and } R_S \leq h_K R_K (k^s W)^k,$$

where $W = (\log p_1)\cdots(\log p_s)$. Further, we use as in [5] that

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

and

$$R_K \geq 0.373, \quad |D_K| \leq n^k.$$

For $n \geq 3$, we also have (cf. [10]),

$$n/\varphi(n) < e^\gamma \log\log n + 5/(2\log\log n),$$

where γ denotes Euler's constant.
Finally, we have

$$\log Q \leq s \log P \text{ and } \log |b| \leq gs \log P.$$

Now it is easy to verify that (12) gives the bound (6) for $\max\{|\alpha|, |\beta|, |u_n|\}$.

Proof of the Corollary. First suppose that $k \leq P/2$. In view of $k \leq \frac{n-1}{2}$ and (5), this is always the case if $n > 30$. In this case (7) can be easily deduced from (6) by using

$$(13) \quad s \leq 1.25506P/\log P \text{ for } s \geq 1$$

(cf. [10]). Further, one can easily check that

$$(14) \quad s + 2 \leq 1.777777P/\log P \text{ if } 1 \leq s \leq 7.$$

*) We remark that in case of $\phi(n)/2 \geq 3$, i.e. except for the cases n=8,10,12,(10) could also be reduced to an irreducibile Thue–Mahler equation to which a recent theorem of Bugeaud and the author [2] also applies.

Now using (13) if $s \geq 8$ and (14) if $1 \leq s \leq 7$, we get from (7) the estimate (8).

Next suppose that $P/2 < k$. Then, by (5), it follows that $n \leq 30$ and hence $k \leq 14$. This gives $P \leq 23$ and so $s \leq 9$. Now we infer from (6) that $\log\log|u_n| \leq 7040$. Hence, if $6 < n \leq 30$ and

$$|u_n| > \exp\exp\{7040\},$$

then we must have $k \leq P/2$ and, as was proved above, (7) and (8) follow.

References

[1] Bilu, Yu., Hanrot, G. and Voutier, P. M., Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.*, **539**, (2001), 75–122.

[2] Bugeaud, Y. and Győry, K., Bounds for the solutions of Thue–Mahler equations and norm form equations, *Acta Arithmetica*, **74**, (1996), 273–292.

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

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

[5] Győry, K., On some arithmetical properties of Lucas and Lehmer numbers, *Acta Arithmetica*, **40**, (1982), 369–373.

[6] Győry, K., Bounds for the solutions of decomposable form equations, *Publ. Math. Debrecen*, **52**, (1998), 1–31.

[7] Győry, K., Kiss, P. and Schinzel, A., On Lucas and Lehmer sequences and their applications to diophantine equations, *Colloqu. Math.*, **45**, (1981), 75–80.

[8] Győry, K., Mignotte, M. and Shorey, T. N., On some arithmetical properties of weighted sums of S-units, *Math. Pannonica*, **1**/2, (1990), 25–43.

[9] Robin, G., Estimation de la fonction de Tchebycheff Θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de n, *Acta Arithmetica*, **42**, (1983), 367–389.

[10] Rosser, J. B. and Schoenfeld, L., Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6**, (1962), 64–94.

[11] Rosser, J. B. and Schoenfeld, L., Sharper bounds for the Chebyshev functions $\Theta(x)$ and $\Psi(x)$, *Math. Comp.*, **29**, (1975), 243–296.

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

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

[14] Stewart, C. L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.*, **24**, (1977), 425–447.

[15] Stewart, C. L., *Primitive divisors of Lucas and Lehmer numbers,* In: *Transcendence theory: Advances and applications*, Acad. Press, London, New York, San Francisco, 1977, 79–92.

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

[17] Kunrui, Yu. and Ling-kei Hung., On binary recurrence sequences, *Indag. Math. N. S.*, **6** (3), (1995), 341–354.

Kálmán Győry
Number Theory Research Group of the
Hungarian Academy of Sciences,
Institute of Mathematics
University of Debrecen
H–4010 Debrecen P.O. Box 12.
Hungary
e-mail: gyory@math.klte.hu