COLLOQUIUM MATHEMATICUM

VOL. XLV 1981 FASC. 1

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

$$u_n = \frac{\alpha_1^n - \beta_1^n}{\alpha_1 - \beta_1}, \qquad n > 0,$$

and

$$v_n = \begin{cases} \dfrac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2} & \text{if } 2 \nmid n, \\ \dfrac{\alpha_2^n - \beta_2^n}{\alpha_2^2 - \beta_2^2} & \text{if } 2 \mid n, \end{cases}$$

respectively, where α_1, β_1 are roots of the trinomial $x^2 - Ax + B$, α_2, β_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 α_1/β_1 and α_2/β_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 Wasén [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 $(\alpha_1 - \beta_1)^2 u_2 \ldots u_{n-1}$. Similarly, p is called a *primitive prime divisor of* v_n if p divides v_n but does not divide $(\alpha_2 - \beta_2)^2(\alpha_2 + \beta_2)^2 v_3 \ldots v_{n-1}$. 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 $e^{452} \cdot 4^{67}$ 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 primitive prime 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 $\max_i(p_i) = P$ 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*

$$t_x \in S, \tag{1}$$

then

$$x \leqslant \max\{e^{452} \cdot 4^{67}, P+1\}$$

and

$$\max(|A|, |B|) < c_1, \qquad |t_x| < c_2,$$

where c_1 and c_2 are effectively computable numbers depending only on P and s.

We remark that for $x \leqslant 6$ or for $x \leqslant 4$ 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 $m \geqslant 2$ whose auxiliary polynomial has at least two distinct roots, then the set of positive 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*

$$\frac{u^x - v^x}{u - v} = w \tag{2}$$

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

$$x \leqslant P \quad \text{and} \quad \max\{u, w\} < c_3,$$

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

Denote by $P(n)$ and $\nu(n)$ 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*

$$\frac{u^x - v^x}{u - v} = n^y \tag{3}$$

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

$$x \leqslant P(n) \quad \text{and} \quad \max\{u, y\} < c_4,$$

where c_4 is an effectively computable number depending only on $P(n)$ and $\nu(n)$.

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 $x \geqslant 4$, then $x \leqslant \max(4, q+1)$. Put

$$n_1 = \max\{e^{452} \cdot 4^{67},\ P+1\}.$$

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 $x \leqslant n_1$.

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

$$\Phi_d(\alpha, \beta) = \prod_{\substack{(t,d)=1 \\ 1 \leqslant t < d/2}} \left((\alpha - \xi^t\beta)(\alpha - \xi^{-t}\beta)\right) = \prod_{\substack{(t,d)=1 \\ 1 \leqslant t < d/2}} \left((\alpha^2 + \beta^2) - (\xi^t + \xi^{-t})\alpha\beta\right) \tag{4}$$
$$= F_d(E, B),$$

where $F_d(y, z)$ 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 $6 < x \leqslant n_1$. Then we obtain

$$t_x = \frac{\alpha^x - \beta^x}{\alpha - \beta} = \prod_{\substack{d \mid x \\ d > 1}} \Phi_d(\alpha, \beta) \quad \text{or} \quad t_x = \frac{\alpha^x - \beta^x}{\alpha^2 - \beta^2} = \prod_{\substack{d \mid x \\ d > 3}} \Phi_d(\alpha, \beta),$$

whence, by (4), we have

$$\prod_{\substack{d \mid x \\ d > 3}} F_d(E, B) \in S. \tag{5}$$

Thus

$$F_x(E, B) \in S. \tag{6}$$

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 $\varphi(x)/2 \geqslant 3$ 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 $c_5(P, s)$ 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 $4t_5 = (2B - 3A^2)^2 - 5A^4$, $3t_6 = A[(3B - 2A^2)^2 - A^4]$ 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 $ax^m + \beta y^n$ with $m = 2$, $n = 4$ the relations $t_5 \in S$ or $t_6 \in S$ 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 $x > 3$, $u > v \geqslant 1$, $(u, v) = 1$, $w \in S$. 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, $n \leqslant p$ (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 $x \leqslant P$. But if $x = 6$, $u = 2$, $v = 1$ and $u_x \in S$, then S must contain 7, and so $x \leqslant P$ 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

[1] A. Baker, *The theory of linear forms in logarithms*, p. 1-27 in: *Transcendence theory: Advances and applications*, Proceedings of the Conference, Cambridge 1976, London - New York - San Francisco 1977.

[2] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Annals of Mathematics (2) 5 (1904), p. 173-180.

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

[4] M. E. Hugh, *The exponential diophantine equation* $1 + a + a^2 + \ldots + a^{x-1} = p^y$, The American Mathematical Monthly 81 (1974), p. 758-759.

[5] S. V. Kotov, *Über die maximale Norm der Idealteiler des Polynoms* $ax^m + \beta y^n$ *mit algebraischen Koeffizienten*, Acta Arithmetica 31 (1976), p. 219-230.

[5a] С. В. Котов и В. Г. Спринджук, *Уравнение Туэ-Малера в относительном поле и приближение алгебраических чисел алгебраическими числами*, Известия Академии наук СССР 41 (1977), p. 723-751.

[6] K. K. Kubota, *On a conjecture of Morgan Ward, I*, Acta Arithmetica 33 (1977), p. 11-28.

[7] — *On a conjecture of Morgan Ward, II*, ibidem 33 (1977), p. 29-48.

[8] — *On a conjecture of Morgan Ward, III*, ibidem 33 (1977), p. 99-109.

[9] J. H. Loxton and A. J. van der Poorten, *On the growth of recurrence sequences*, Mathematical Proceedings of the Cambridge Philosophical Society 81 (1977), p. 369-376.

[10] M. Mignotte, *A note on linear recursive sequences*, Journal of the Australian Mathematical Society 20 (1975), p. 242-244.

[11] — *Intersection des images de certaines suites récurrentes linéaires* (to appear).

[12] A. J. van der Poorten, *Effectively computable bounds for the solutions of certain diophantine equations*, Acta Arithmetica 33 (1977), p. 195-207.

[13] A. Rotkiewicz and R. Wasén, *Lehmer's numbers*, ibidem 36 (1980), p. 203-217.

[14] A. Schinzel, *On primitive prime factors of Lehmer numbers, I*, ibidem 8 (1963), p. 213-223.

[15] — *On primitive prime factors of Lehmer numbers, II*, ibidem 8 (1963), p. 251-257.

[16] — *On primitive prime factors of Lehmer numbers, III*, ibidem 15 (1968), p. 49-70.

[17] — *On two theorems of Gelfond and some of their applications*, ibidem 13 (1967), p. 177-236.

[18] — *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, Journal für die reine und angewandte Mathematik 268/269 (1974), p. 27-33.

[19] T. N. Shorey and R. T. Tijdeman, *New applications of diophantine approximations to diophantine equations*, Mathematica Scandinavica 39 (1976), p. 5-18.

[20] В. Г. Спринджук, *О рациональных приближениях к алгебраическим числам*, Известия Академии наук СССР 35 (1971), p. 991-1007.

[21] C. L. Stewart, *Divisor properties of arithmetical sequences*, Ph. D. thesis, University of Cambridge, 1976.

[22] — *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proceedings of the London Mathematical Society 35 (1977), p. 425-447.

[23] — *Primitive divisors of Lucas and Lehmer numbers*, p. 79-92 in: *Transcendence theory: Advances and applications*, Proceedings of the Conference, Cambridge 1976, London - New York - San Francisco 1977.

[24] K. Szymiczek, *On the equation* $a^x - b^x = (a-b)c^y$, Wiadomości Matematyczne 7 (1964), p. 233-236 (in Polish).

[25] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte für Mathematik 3 (1892), p. 266-284.

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