A. BAKER
C. L. STEWART

Further aspects of transcendence theory

Astérisque, tome 41-42 (1977), p. 153-163
<http://www.numdam.org/item?id=AST_1977__41-42__153_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.153-163

FURTHER ASPECTS OF TRANSCENDENCE THEORY

by A. Baker and C.L. Stewart

1. Introduction. This is a sequel to the talk given by the first author at the Journées Arithmétiques held in Bordeaux in 1974 [4]. Since then, there have been two main developments in transcendence theory, one relating to Diophantine equations and the other concerning divisor properties of arithmetical sequences.[†] The advances depend upon recent progress concerning the theory of linear forms in the logarithms of algebraic numbers, and we shall begin by recording the latest results in this field.

2. Linear forms in logarithms. Let

$$\Lambda = \beta_o+\beta_1 \log \alpha_1+\ldots+\beta_n \log \alpha_n,$$

where the α's and β's denote algebraic numbers; we shall assume that the α's are not 0 or 1, that the β's are not all 0, and that the logarithms have their principal values. We shall suppose that α_j and β_j have heights at most $A_j(\geq 4)$ and $B(\geq 4)$ respectively, and that the field K generated by the α's and β's over the rationals has degree

[†] For other developments, concerning for example elliptic functions, see the papersby D.W. Masser and M. Waldschmidt in these Proceedings.

at most d. Further we shall assume that $\Lambda \neq 0$. Then we have (see [6])

$$|\Lambda| > (B\Omega)^{-C\Omega\log\Omega'}, \quad \text{where} \quad C = (16nd)^{200n},$$

$$\Omega = \log A_1 \ldots \log A_n, \text{ and } \Omega' = \Omega/\log A_n .$$

In the special case when $\beta_o = 0$ and $\beta_1,\ldots,\beta_n$ are rational integers, the bracketed factor Ω has been eliminated to yield $|\Lambda| > B^{-C\Omega\log\Omega'}$. These theorems include many earlier results in the field (cf. the introduction to [6]);and, apart from numerical constants, it would seem difficult to improve substantially upon their degree of precision. In fact, if one neglects second order terms, then the estimates are best possible with respect to each of the parameters $A_1,\ldots,A_n$ and B separately when the others are regarded as fixed; moreover, even the elimination of the factor $\log\Omega'$ or the replacement of nd in C by d would seem to involve some new idea. An expression for C of the above form occurred first in some work of Shorey [13], and the presence of Ω' rather than Ω is a consequence of [3] together with an observation of van der Poorten [9]. The latter refinement is of interest, in particular, since in view of the trivial Liouville-type inequality, applicable in the rational case, namely[†] $|\Lambda| > (3A)^{-ndB}$, where $A = \max A_j$, we obtain at once an

[†] This is slightly more precise than the form given in [1]; see [18] for details.

inequality announced by Chudnovsky to the effect that $|\Lambda| > B^{-C\Omega \log B}$. It will be noted that the dependence on A and n in the trivial inequality is best possible; but, from the point of view of applications, it is essential to have a stronger dependence on B. The proofs of the theorems mentioned here will appear in the Proceedings of the conference on transcendence theory which was held in Cambridge early in 1976; and the latter will contain also a paper by van der Poorten on p-adic aspects of the subject [11].

3. Diophantine equations. Among the first applications of the theory of linear forms in logarithms were the effective resolutions of the Thue equation $f(x,y) = m$, where f denotes an irreducible binary form with integer coefficients and degree at least 3, and of the hyperelliptic equation $y^m = f(x)$, where f is any polynomial with integer coefficients and with at least three simple zeros, and m is any integer ≥ 2 (see [5]). These equations possess just two integer variables x and y, and, though the results were generalized p-adically so as to incorporate certain prime powers, this binary character nevertheless seemed to be an essential feature of the work. The recent advances in the theory of linear forms in logarithms, however, have led to the resolution of a much wider class of equations having now three and indeed, in some cases, even four independent integer variables.

This latest development was begun by Tijdeman when he succeeded in showing that the Catalan equation $x^m-y^n = 1$ has only finitely many solutions in integers x,y,m,n (all > 1) and, furthermore, that they can all be effectively determined. The method of proof can be readily illustrated by considering the simpler equation $ax^n-by^n = c$, where a,b,c are given positive integers, and we seek all solutions in integers x,y,n (all > 2). We shall assume that $y \geq x$, as we may without loss of generality. Plainly the equation gives $|\Lambda| \ll y^{-n}$, where

$$\Lambda = \log(a/b) + n \log(x/y),$$

and the implied constant depends only on a,b and c. On the other hand, from the results recorded in §2, we have

$$\log|\Lambda| \gg -\log y \log n.$$

A comparison of estimates yields at once a bound for n in terms of a,b,c, and the theorem on the hyperelliptic equation referred to above then furnishes bounds for x and y. Thus, in principle, the equation can be solved completely. It will be seen that the success of the method depends critically on the fact that the dependence on A_n in the estimate for Λ cited in §2 is best possible. This feature, which first entered into the theory via [3], is also crucial to Tijdeman's work on the Catalan equation (see [21]).

The latter arguments have recently been generalized p-adically by van der Poorten; he has shown, for instance, how one can solve in integers x,y,z,m,n the equation $x^m-y^n = z^\ell$, where ℓ is the lowest common multiple of m and n, and z is composed solely of powers of fixed sets of primes (see [10]). Further, Schinzel and Tijdeman [12] have recently proved that the original hyperelliptic equation $y^m = f(x)$ has only finitely many solutions in integers x,y,m (with $|y| > 1$, $m > 1$) and, again, they can be determined effectively. Furthermore, it is shown in [16] that if $f(x)$ is replaced by a binary form $f(x,z)$ with at least two distinct linear factors then, in principle, the equation is soluble in integers x,y,z,m, where z is composed solely of powers of primes from a fixed set, and $(x,z) = 1$, $|y| > 1$, $m > 2$. These results represent some remarkable progress in our knowledge.

4. Polynomial divisors. Størmer proved in 1897, using properties of the Pellian equation, that $P(x(x+1)) \to \infty$ as $x \to \infty$, where $P(m)$ denotes the greatest prime factor of m. Pólya extended this result in 1918 to include all quadratic polynomials with integer coefficients and distinct zeros, and Siegel further extended the result in 1921 to polynomials of arbitrary degree; the latter work depended on the famous Thue-Siegel theorem. Mahler later generalized Siegel's result, by means of p-adic methods, to binary forms.

The quantitative estimate $P(f(x)) \gg \log\log x$, where the implied constant depends only on f, was established by Chowla, Mahler and Nagell in the 1930's for certain quadratic and cubic polynomials f, and, in 1967, Schinzel, using a theorem of Gelfond, obtained the corresponding sharpening of Pólya's result. Further, in 1969, Keates, appealing to bounds for the solutions of the equation $y^2 = f(x)$ (see [2]), obtained a similar proposition for cubic f. The work was much extended by Coates in 1970 [7]. Applying the p-adic theory of linear forms in logarithms, he showed that $P(f(x,y)) \gg (\log\log X)^{1/4}$ for all binary forms f with at least three distinct linear factors, where $X = \max(|x|,|y|)$ and $(x,y) = 1$. Recent advances in this field have now yielded the result $P(f(x,y)) \gg \log\log X$ (see [16], and for earlier work [17, 8]; see also [15] for related work on certain polynomial products).

In another direction, the recent theorems concerning linear forms in logarithms have been used by Shorey and Tijdeman [14] to prove that $P(x^n+b) \to \infty$ as $n \to \infty$ uniformly in x, and in fact van der Poorten has shown more generally that $P(ax^n+by^n) \to \infty$ as $n \to \infty$ uniformly in x and y, where a,b are any non-zero integers (see [10]). Further, a similar generalization has been obtained in connexion with Mahler's well-known theorem to the effect that $P(ax^m+by^n) \to \infty$ as $\max(|x|,|y|) \to \infty$, where $(x,y) = 1$; indeed it has now been established that the same holds as $\max(|x|,|y|,n) \to \infty$, assuming that a,b and m are fixed (see [16]).

5. Lucas and Lehmer numbers. As remarked in Bordeaux, the second author proved some three years ago, in connexion with a conjecture of Erdős, that, for any integers $a > b > 0$, $P(a^n-b^n)/n \to \infty$ as n runs through a certain set of integers of density 1 which includes the primes. Since then, the work has been much extended to include the Lucas and Lehmer numbers and many other arithmetical sequences [19].

In 1886, Lucas, generalizing the well-known Fibonacci sequence 1,1,2,3,5,..., defined integers $t_1, t_2, \ldots$ by

$$t_n = (\alpha^n-\beta^n)/(\alpha-\beta),$$

where $\alpha+\beta$ and $\alpha\beta$ are relatively prime integers (so that α, β are roots of a quadratic equation) and α/β is not a root of unity; he proceeded to demonstrate the efficacy of the sequences in tests for primality, in researches concerning continued fractions, and in work on the Pellian equation. The studies were extended by Lehmer in 1930; he defined a sequence $u_1, u_2, \ldots$ of positive integers in the same way as Lucas for n odd, by

$$u_n = (\alpha^n-\beta^n)/(\alpha^2-\beta^2)$$

for n even, and subject to the weaker condition that $(\alpha+\beta)^2$ and $\alpha\beta$ be relatively prime integers. Carmichael proved in 1913 that if α, β are real and $n > 12$ then $P(t_n) \ge n-1$, and Ward showed in 1955 that the same holds for u_n. It has recently been demonstrated by means of the theory of linear forms in logarithms that $P(t_n) >> n \log n/(q(n))^{4/3}$, where $q(n)$ denotes the number of square-free divisors of n and the implied constant depends only on α and β. In fact the same holds for u_n and indeed for a^n-b^n; thus, in particular, we have $P(a^p-b^p) >> p \log p$ for all primes p. Moreover, it has been proved similarly that for the Fermat numbers the estimate

$$P(2^{2^n}+1) >> n2^n$$

is valid for all positive integers n, where now the implied constant is absolute.

Other work in this field has concerned, for instance, the sequences $n!+1$, n^n+1, $p_1 \ldots p_n+1$ $(n = 1,2,\ldots)$, where p_n denotes the n^{th} prime, and furthermore solutions v_n of the general linear recurrence relation

$$v_n = a_1v_{n-1} + a_2v_{n-2}+\ldots+ a_rv_{n-r},$$

where $a_1,\ldots,a_r$ are rational integers; in the binary case (when $r = 2$), for example, it has been shown that $P(v_n) >> (n/\log n)^{1/3}$ (see [18]). The results described here are illustrations of the successful application of the estimates for linear forms in logarithms to the study of arithmetical sequences of exponential growth which are at present not treatable by more conventional means. The difficulties inherent in applying sieve methods to study such sparse sequences have been analysed by Hooley.[†]

There have also been some new developments in connexion with the result of Schinzel mentioned in Bordeaux, to the effect that there exist primitive prime divisors of $\alpha^n-\beta^n$ for relatively prime algebraic integers α,β with α/β not a root of unity, and with n sufficiently large in terms of the degree of α/β. Schinzel's result applies in particular to the Lucas and Lehmer numbers, and explicit calculations, using the work referred to in §2, have shown that these indeed possess primitive prime divisors for $n > 10^{300}$. In fact rather more has been proved; it has been shown namely that, except possibly for finitely many exceptions, all Lucas and Lehmer numbers possess primitive prime divisors if $n > 6$ and $n \neq 8$, 10 or 12. Further, this result is best possible, for one can specify infinitely many Lehmer sequences for which u_n does not have a primitive prime divisor for each remaining n. Furthermore, the exceptional cases can, in principle, be effectively determined (see [20]).

[†] Applications of sieve methods (Cambridge Univ. Press, 1976); see Chapter 7.

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers IV, Mathematika 15 (1968), 204-216.

[2] A. Baker, The Diophantine equation $y^2 = ax^3+bx^2+cx+d$, J. London Math. Soc. 43 (1968), 1-9.

[3] A. Baker, A sharpening of the bounds for linear forms in logarithms, Acta Arith. 21 (1972), 117-129.

[4] A. Baker, Some aspects of transcendence theory, Astérisque 24-25 (1975), 169-175.

[5] A. Baker, Transcendental number theory (Cambridge Univ. Press, 1975).

[6] A. Baker, The theory of linear forms in logarithms, Advances in transcendence theory (Academic Press, London and New York, 1977).

[7] 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), 399-412.

[8] S.V. Kotov, Greatest prime factor of a polynomial, Mat. Zametki 13 (1973), 515-522.

[9] A.J. van der Poorten, On Baker's inequality for linear forms in logarithms, Math. Proc. Camb. Phil. Soc. (to appear).

[10] A.J. van der Poorten, Effectively computable bounds for the solutions of certain Diophantine equations, Acta Arith. (to appear).

[11] A.J. van der Poorten, Linear forms in logarithms in the p-adic case, Advances in transcendence theory (Academic Press, London and New York, 1977).

[12] A. Schinzel and R. Tijdeman, On the equation $y^m = P(x)$, Acta Arith. (to appear).

[13] T.N. Shorey, On linear forms in the logarithms of algebraic numbers, Acta Arith. 30 (1976), 27-42.

[14] T.N. Shorey and R. Tijdeman, New applications of Diophantine approximations to Diophantine equations (to appear).

[15] T.N. Shorey and R. Tijdeman, On the greatest prime factors of polynomials at integer points, Compositio Math. (to appear).

[16] T.N. Shorey, A.J. van der Poorten, A. Schinzel and R. Tijdeman, Applications of the Gelfond-Baker method to Diophantine equations, Advances in transcendence theory (Academic Press, London and New York, 1977).

[17] V.G. Sprindžuk, The greatest prime divisor of a binary form, Doklady Akad. Nauk. BSSR, 15 (1971), 389-391.

[18] C.L. Stewart, Divisor properties of arithmetical sequences, Ph.D. dissertation (Cambridge, 1976).

[19] C.L. Stewart, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, Proc. London Math. Soc. (to appear).

[20] C.L. Stewart, Primitive divisors of Lucas and Lehmer numbers, Advances in transcendence theory (Academic Press, London and New York, 1977).

[21] R. Tijdeman, On the equation of Catalan, Acta Arith. 29 (1976), 197-209.

Trinity College
Cambridge