Astérisque

ALAN BAKER

Some aspects of transcendence theory

Astérisque, tome 24-25 (1975), p. 169-175

<http://www.numdam.org/item?id=AST_1975__24-25__169_0>

Société Mathématique de France
Astérisque 24-25 (1975)

SOME ASPECTS OF TRANSCENDENCE THEORY

by

Alan BAKER

-:-:-:-

I. - INTRODUCTION. - There have been in recent years two rather surprising developments in the theory of transcendental numbers, the first being its increasing application to studies concerning the distribution of the primes, and the second being the utilization of its techniques to yield elementary proofs of the Riemann hypothesis for curves The greater part of my talk today will be devoted to the first topic, and at the end I shall say a little about the second.

II. - CONJECTURE OF ERDÖS. - In 1965, Erdös conjectured that $P(2^n - 1)/n \to \infty$ as $n \to \infty$, where $P(m)$ denotes the greatest prime factor of m. The elementary result that $P(a^n - b^n) \geq n+1$ when $n > 2$ and $a > b > 0$ was first proved by Zsigmondy in 1892 and the result was rediscovered by Birkhoff and Vandiver in 1904 It was improved by Schinzel in 1962 ; he showed that $P(a^n - b^n) \geq 2n+1$ if ab is a square or twice a square provided that one excludes three special cases. Recently, a student of mine, C. L. Stewart, has proved that certainly $P(a^n - b^n)/n \to \infty$

as n runs through the sequence of primes and, in fact, more generally as n runs through a certain set of integers of density 1 which includes the primes [6]. In the simplest case the proof depends on a comparison of estimates for $R = a^p/(a^p - b^p)$, where p is a prime. Clearly $\log R < (b/a)^{p-1}$ and

$$R^{-1} = a^{-p}(a-b)\Phi_p ,$$

where Φ_p denotes the p th cyclotomic polynomial. Now by an old result of Sylvester we have :

$$\Phi_p = p_o \prod_{j=1}^{k} p_j^{h_j} ,$$

where $p_1, \ldots, p_k$ are primes congruent to 1 (mod p) and $p_o = 1$ or p. Thus on applying transcendence theory or, more precisely, recent results on linear forms in the logarithms of algebraic numbers [1, III], we deduce that either k or one of the quotients p_j/p must exceed any given bound as $p \to \infty$; in either case we have the desired conclusion.

III. - RESULT OF SCHINZEL. - This leads me to some recent work of Schinzel on primitive divisors of $a^n - b^n$. Zsigmondy, again, proved in 1892 that if $(a, b) = 1$ and $n > 2$, then there exists a prime p dividing $a^n - b^n$ but not $a^m - b^m$ for $m < n$; this holds except in the cases $2^3 + 1$, $2^6 - 1$. It was long conjectured that a result of this kind holds more generally for algebraic a, b, not merely rational integers, and the conjecture was recently proved by Schinzel [3]; he has shown, in fact, that if α, β are algebraic integers, $(\alpha, \beta) = 1$ and α/β is not a root of unity then primitive prime divisors of $\alpha^n - \beta^n$ exist for all $n > n_o(d)$, where d is the degree of α/β. As in the previous problem, the proof depends on an application of one of the latest theorems on linear forms in logarithms of algebraic numbers [1, I], used, in this case, to estimate $\log |\alpha^n - \beta^n|$.

IV. - RESULT OF TIJDEMAN. - In another direction the theory of linear forms in logarithms has been employed by Tijdeman to solve an old problem of Wintner. Wintner asked whether there exists a sequence $p_1, p_2, \ldots$ of primes such that if $n_1, n_2, \ldots$ is the sequence of all natural numbers formed from their power products, then $n_{i+1} - n_i \to \infty$ as $i \to \infty$. Clearly the sequence of all primes will not suffice here, for in this case $n_{i+1} - n_i = 1$ for all i. Tijdeman has shown that the answer to Wintner's problem is in the affirmative [7] ; indeed he has proved that for any θ with $0 < \theta < 1$ there exists a sequence $p_1, p_2, \ldots$ of primes such that if $n_1, n_2, \ldots$ is the sequence as above then $n_{i+1} - n_i > n_i^{1-\theta}$. For the proof one takes $p_1 = 3$ and assumes that $p_1, \ldots, p_r$ have been chosen so that $b-a > a^{1-\theta}$ for all integers a, b $(a<b)$ composed of these primes. Now if $a = p_1^{\alpha_1} \ldots p_r^{\alpha_r} p^{\alpha}$ and $b = p_1^{\beta_1} \ldots p_r^{\beta_r} p^{\beta}$ satisfy $0 < b-a < a^{1-\theta}$ then

$$|(\beta_1 - \alpha_1) \log p_1 + \ldots + (\beta_r - \alpha_r) \log p_r + (\beta - \alpha) \log p| < a^{-\theta}$$

and the theory of linear forms in logarithms [1, II] shows that $\alpha, \beta < c$ and $\alpha_j, \beta_j < c \log p$ for some c depending only on r. This implies that the number of primes p in the interval $\frac{1}{2} T \leq p < T$ for which integers a, b as above exist cannot exceed $c' T^{1-\theta} (\log T)^{2r}$ for some c' depending only on r. But there are at least $\frac{1}{4} T / \log T$ primes in the interval and so one can select a prime p so that $b-a > a^{1-\theta}$ for all a, b in question. The theorem follows by induction.

V. - RESULT OF RAMACHANDRA AND SHOREY. - Let $n_1, n_2, \ldots$ be the sequence of all natural numbers which have at least one prime factor exceeding k. It is easily seen that $n_{i+1} - n_i = O(k)$ for all i. Erdös proved that indeed $n_{i+1} - n_i = O(k/\log k)$ and conjectured that in fact the bound could be replaced by $\pi(k)$. Erdös'argument gave a value 3 for the constant in the O-term, and this

was reduced to 1 by Ramachandra using work of Halberstam and Roth. Later Tijdeman reduced the constant to $1/2$. Recently Ramachandra and his pupil T. N. Shorey [2] have applied the theory of linear forms in logarithms and have thereby succeeded in proving that $n_{i+1} - n_i = o(k/\log k)$; the best result to date is

$$n_{i+1} - n_i = O\left(\frac{k \log\log\log k}{\log k \log\log k}\right) .$$

This implies, in particular, that $p_{i+1} - p_i = o(p_i / \log p_i)$, a weak form of the Hoheisel-Ingham result ; but in fact the latter is used in the proof.

VI. - LINEAR FORMS IN LOGARITHMS. - As we have seen, all the above work depends on the theory of linear forms in the logarithms of algebraic numbers, and I should like to record here the latest result in this context [1, III]. This states that if $\alpha_1, \ldots, \alpha_n$ are non-zero algebraic numbers with degrees at most d and heights at most $A_1, \ldots, A_n$ respectively, and if

$$\Lambda = b_1 \log \alpha_1 + \ldots + b_n \log \alpha_n ,$$

where $b_1, \ldots, b_n$ are rational integers with absolute values at most B then either $\Lambda = 0$ or $|\Lambda| > B^{-C\Omega \log \Omega}$, where $\Omega = \log A_1 \ldots \log A_n$, and C is an effectively computable number depending only on n and d. The result is best possible with respect to B when the A's are fixed and, apart from the $\log \Omega$ factor, also with respect to each A_j when B is regarded as fixed. A weaker form of this result was recently employed by Stark [5] to improve my estimate for the size of all solutions of the equation $y^2 = x^3 + k$ from $\exp\{(10^{10}|k|)^{10^4}\}$ to $\exp(c\,|k|^{1+\varepsilon})$, where $\varepsilon > 0$ is arbitrary and c depends only on ε. It seems likely that estimates of the latter kind will be capable of still further improvement in the light of recent progress.

VII. - APPLICATION TO THE RIEMANN HYPOTHESIS FOR CURVES. - To illustrate some of the typical arguments utilized in transcendence theory, I shall give now a short, elementary proof, following the work of Stepanov and Schmidt [4], of the Riemann hypothesis for the curve

$$y^2 = ax^3 + bx^2 + cx + d \qquad (a \neq 0)$$

defined over the finite field F with q elements, where q is an odd prime. The theorem in question states that the number s of solutions of the above equation in elements x, y in F satisfies $|s-q| \ll q^{1/2}$, where the implied constant is absolute.

Let $f(x)$ denote the cubic on the right of the above equation, let $g(x) = (f(x))^{(q-1)/2}$, and let S, S' be the number of solutions of $g(x) = 1$ and $g(x) = -1$ respectively. Clearly, for every x in F, either $f(x) = 0$ or $(f(x))^{q-1} = 1$, and so $S+S' \geq q-3$. We proceed to prove that both S and S' are at most $\frac{1}{2}q + O(q^{1/2})$; then $|S-\frac{1}{2}q| \ll q^{1/2}$, and since every solution of $g(x) = 1$ gives rise to two solutions of $y^2 = f(x)$, it follows that $|s-q| \ll q^{1/2}$, as required. It will in fact suffice to establish the estimate for S, since the demonstration for S' is similar.

The proof depends on the construction of an auxiliary polynomial

$$\Phi(x) = \sum_{j=0}^{J-1} \sum_{k=0}^{l} p_{jk}(x)\, x^{qj}\, (g(x))^k ,$$

where the $p_{jk}(x)$ are polynomials, not all identically 0, with coefficients in F and with degrees at most $\frac{1}{2}(q-7)$. It is readily verified that the terms in the above sum have distinct degrees and so $\Phi(x)$ does not vanish identically. Now Φ is constructed so that $D^{\ell}\Phi(x) = 0$ $(0 \leq \ell < L)$ for all x satisfying $g(x) = 1$, where D^{ℓ} denotes the ℓ th derivative with respect to x. Plainly $D^{\ell}\Phi$ has the same form as Φ but with $p_{jk}(x)$ replaced by $p_{jk\ell}(x) / (f(x))^{\ell}$, where $p_{jk\ell}$ signifies

a polynomial with degree at most $\frac{1}{2}q + 3\ell$. Since $x^q = x$ for all x, it follows that one has to solve a system of at most $(\frac{1}{2}q + 3L + J)L$ linear equations in the $J(q-5)$ unknown coefficients of the p_{jk}. This is possible if $L = O(q^{1/2})$ with a sufficiently small implied constant, and $J = \frac{1}{2}L + O(1)$. Finally one notes that $\Phi(x)$ has degree at most $(J+3)q$ and, since $L<q$, it has a zero at each solution of $g(x) = 1$ with order at least L; hence

$$S \leq (J+3)\, q/L = 1/2\, q + O(q^{1/2}),$$

provided that $L \gg q^{1/2}$, and this proves the theorem.

-:-:-:-

REFERENCES

[1] A. BAKER. - A sharpening of the bounds for linear forms in logarithms. I, II, III, Acta Arithmetica 21 (1972), 117-129 ; 24 (1973), 33-36 ; 27 (1974), 247-252.

[2] K. RAMACHANDRA and T. N. SHOREY. - On gaps between numbers with a large prime factor. Acta Arithmetica 24 (1973), 99-111 ; part II by T. N. SHOREY ibid. 25 (1974), 365-373.

[3] A. SCHINZEL. - On primitive prime divisors of the expression $A^n - B^n$ in algebraic number fields. J. reine angew. Math. 269 (1974), 27-33.

[4] W. M. SCHMIDT. - Zur Methode von Stepanov. Acta Arithmetica 24 (1973) 347-367.

[5] H. M. STARK. - Effective estimates of solutions of some diophantine equations. Acta Arithmetica 24 (1973), 251-259.

[6] C. L. STEWART. - The greatest prime factor of $a^n - b^n$. Acta Arithmetica (to appear).

[7] R. TIJDEMAN. - On integers with many small prime factors. Compositio Math. 26 (1973), 319-330.

-:-:-:-

Alan BAKER
Trinity College
CAMBRIDGE
(England)