new mathematical monographs: 9

Logarithmic Forms and Diophantine Geometry

Alan Baker and Gisbert Wüstholz

CAMBRIDGE

LOGARITHMIC FORMS AND DIOPHANTINE GEOMETRY

A. BAKER
University of Cambridge

G. WÜSTHOLZ
ETH Zentrum, Zürich

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521882682

First published 2007

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

ISBN 978-0-521-88268-2 hardback

Logarithmic Forms and Diophantine Geometry

There is now much interplay between studies on logarithmic forms and deep aspects of arithmetic algebraic geometry. New light has been shed, for instance, on the famous conjectures of Tate and Shafarevich relating to abelian varieties and the associated celebrated discoveries of Faltings establishing the Mordell conjecture. This book gives an account of the theory of linear forms in the logarithms of algebraic numbers with special emphasis on the important developments of the past twenty-five years. The first part concentrates on basic material in transcendental number theory but with a modern perspective including discussion of the Mahler–Manin conjecture, of the Riemann hypothesis over finite fields, of significant new studies on the effective solution of Diophantine problems and of the *abc*-conjecture. The remainder assumes some background in Lie algebras and group varieties and it covers, in certain instances for the first time in book form, more advanced topics including the work of Masser and Wüstholz on zero estimates on group varieties (derived by a new, more algebraic approach that involves Hilbert functions and Poincaré series), the analytic subgroup theorem and its principal applications; these areas reflect substantial original research. The final chapter summarises other aspects of Diophantine geometry including hypergeometric theory and the André–Oort conjecture. A comprehensive bibliography rounds off this definitive survey of effective methods in Diophantine geometry.

ALAN BAKER, FRS, is Emeritus Professor of Pure Mathematics in the University of Cambridge and Fellow of Trinity College, Cambridge. He has received numerous international awards, including, in 1970, a Fields medal for his work in number theory. This is his third authored book: he has edited three others for publication.

GISBERT WÜSTHOLZ is Professor of Mathematics at ETH Zürich. This is his second authored book and he has been involved in the production of three others.

NEW MATHEMATICAL MONOGRAPHS

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing visit http://www.cambridge.org/uk/series/sSeries.asp?code=NMM

1 M. Cabanes and M. Enguehard *Representation Theory of Finite Reductive Groups*
2 J. B. Garnett and D. E. Marshall *Harmonic Measure*
3 P. M. Cohn *Free Ideal Rings and Localization in General Rings*
4 E. Bombieri and W. Gubler *Heights in Diophantine Geometry*
5 Y. J. Ionin and M. S. Shrikhande *Combinatorics of Symmetric Designs*
6 S. Berhanu, P. D. Cordaro and J. Hounie *An Introduction to Involutive Structures*
7 A. Shlapentokh *Hilbert's Tenth Problem*
8 G. O. Michler *Theory of Finite Simple Groups*
9 A. Baker and G. Wüstholz *Logarithmic Forms and Diophantine Geometry*
10 P. Kronheimer and T. Mrowka *Monopoles and Three-Manifolds*
11 B. Bekka, P. de la Harpe and A. Valette *Kazhdan's Property (T)*

Preface

This book has arisen from lectures given by the first author at ETH Zürich in the Wintersemester 1988–1989 under the Nachdiplomvorlesung program and subsequent lectures by both authors in various localities, in particular at an instructional conference organised by the DMV in Blaubeuren. Our object has been to give an account of the theory of linear forms in the logarithms of algebraic numbers with special emphasis on the important developments of the past twenty-five years concerning multiplicity estimates on group varieties.

As will be clear from the text there is now much interplay between studies on logarithmic forms and deep aspects of arithmetic algebraic geometry. New light has been shed for instance on the famous conjectures of Tate and Shafarevich relating to abelian varieties and the associated celebrated discoveries of Faltings establishing the Mordell conjecture. We give a connected exposition reflecting these major advances including the first version in book form of the basic works of Masser and Wüstholz on zero estimates on group varieties, the analytic subgroup theorem and their applications. Our discussion here is more algebraic in character than the original and involves, in particular, Hilbert functions in degree theory and Poincaré series as well as the general background of Lie algebras and group varieties. On the other hand, the first three chapters have been written on a more basic level in the style of Baker [25]; since its publication in 1975, the latter has been the classical introduction to transcendence theory, and especially to the subject of logarithmic forms, and it may still be regarded as the standard

work in this field. The text here gives in essence a new rendering and updating of Chapters 1 to 5 of [25].

We are most grateful to Camilla Grob for her unstinting help in taking down our lecture notes with a view to publication and to S. Gerig, F. Yan and O. Fasching for their generous assistance in connection with the detailed preparation of the text, in particular with the LaTeX typesetting. We are much indebted to Professor D. W. Masser for reading through a draft of the book prior to publication and for making many detailed and helpful suggestions. Further we thank Professor P. Cohen for reviewing aspects of the book, in particular in connection with Chapter 8. Finally we acknowledge with gratitude the generous support of the Forschungsinstitut at ETH in arranging a variety of visits so that we could complete our work.

A. Baker and G. Wüstholz (Cambridge and Zürich)

Contents

1
Transcendence origins

1.1 Liouville's theorem

In 1844 Liouville showed for the first time the existence of transcendental numbers, that is numbers which are not algebraic and so are not roots of any polynomial with integer coefficients [147]. The following approximation theorem by Liouville allowed a certain type of number to be established as transcendental.

Theorem 1.1 (Liouville) *If α is an algebraic number with degree $n > 1$ then, for all rationals p/q ($p, q \in \mathbb{Z}$, $q > 0$), we have*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$$

for some constant $c = c(\alpha) > 0$ (that is, c is only dependent on α).

Proof. Let $P(x)$ be the minimal polynomial for α (that is the irreducible polynomial P with $P(\alpha) = 0$, with the coefficients of P integers, with the leading coefficient positive and with the greatest common divisor of the coefficients equal to 1). We can assume that α is real and that $|\alpha - p/q| < 1$, for otherwise the theorem is trivially valid. By the mean value theorem we have $P(\alpha) - P(p/q) = (\alpha - p/q)P'(\xi)$ for some ξ between α and p/q. Then ξ belongs to $(\alpha - 1, \alpha + 1)$ and therefore $|P'(\xi)| < 1/c$ for some $c = c(\alpha) > 0$. Since $P(\alpha) = 0$ we get

$$\left|\alpha - \frac{p}{q}\right| > c\left|P\left(\frac{p}{q}\right)\right|.$$

Since P is irreducible of degree n, $P(p/q) \neq 0$ and $|q^n P(p/q)|$ is an integer, whence $|P(p/q)| \geq 1/q^n$ and the theorem follows. □

Now let us look at some numbers for which this theorem provides a proof of their transcendence.

Example 1.2 *The number*

$$\xi = \sum_{n=1}^{\infty} 10^{-n!}$$

is transcendental.

For let $p_k = 10^{k!} \sum_{n=1}^{k} 10^{-n!}$ and $q_k = 10^{k!}$ for $k = 1, 2, \ldots$; then p_k, q_k are relatively prime rational integers and

$$\left| \xi - \frac{p_k}{q_k} \right| = \sum_{n=k+1}^{\infty} 10^{-n!} < 10^{-(k+1)!} \sum_{n=0}^{\infty} 10^{-n}$$
$$= \frac{10}{9} q_k^{-(k+1)} < q_k^{-k}.$$

Since k tends to infinity there cannot exist a constant c, as in the theorem, only depending on ξ. Therefore ξ is transcendental. Further, as immediate consequences of Liouville's theorem, we have the following.

Example 1.3 *Any non-terminating decimal of the type*

$$0.a_1 0 \cdots 0 a_2 0 \cdots 0 a_3 0 \cdots,$$

in which blocks of zeros increase in length sufficiently rapidly, is transcendental. Similarly any continued fraction in which the partial quotients increase sufficiently rapidly is transcendental.

In 1906 Maillet published the first book on transcendental numbers [159]. He showed here, amongst other things, that there exist transcendental numbers whose continued fractions have bounded partial quotients.

Example 1.4 *Continued fractions of the type*

$$[1, \ldots, 1, a_1, 1, \ldots, 1, a_2, 1, \ldots, 1, a_3, 1, \ldots]$$

are transcendental, where $a_i \neq 1$ and the number of repeated partial quotients increases sufficiently rapidly.

The subject of continued fractions of Maillet type was taken up by Baker [11] and it continues to be of research interest (see e.g. [180]). Maillet's proof was based on an approximation theorem with quadratic irrationals. In 1961, Güting [122] obtained an elegant theorem of this kind relating to numbers of arbitrary degree. In order to state the result we need the concept of the height of an algebraic number; in fact some notion of height occurs throughout our text. Let α be an algebraic number and let the minimal polynomial for α be

$$P(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n .$$

Definition 1.5 *The (classical) height of α is given by*

$$H(\alpha) = \max(|a_0|, \ldots, |a_n|) .$$

Now let α and β be distinct algebraic numbers with heights a and b, and let l, m be the degrees of β over $\mathbb{Q}(\alpha)$ and α over $\mathbb{Q}(\beta)$ respectively. Then Güting's theorem reads as follows.

Theorem 1.6 *We have*

$$|\alpha - \beta| \gg a^{-l} b^{-m} .$$

Here we are using Vinogradov's notation: by $f \gg g$ for functions f, g we mean $f > cg$ for some positive constant c and similarly by $f \ll g$ we mean $f < cg$. The constant c in Theorem 1.6 is effective and for an explicit expression in terms of l and m see [122].

Proof of Theorem 1.6. Güting's argument is essentially a straightforward generalisation of Liouville's. It depends on the fact that

$$|a_0^l b_0^m N(\alpha - \beta)| \geq 1 ,$$

where a_0 and b_0 are the leading coefficients in the minimal polynomials for α and β, and N denotes the field norm with respect to $\mathbb{Q}(\alpha, \beta)$. The field conjugates $\alpha_j - \beta_j$ of $\alpha - \beta$ have absolute value at most $(1 + |\alpha_j|)(1 + |\beta_j|)$ and estimates for $a_0^l \prod(1 + |\alpha_j|)$ and $b_0^m \prod(1 + |\beta_j|)$

in terms of the heights a and b, where the products are taken over all field conjugates, date back to Landau; see [33, §2]. In fact Theorem 4.2 of LeVeque's book [145] shows that the expressions are at most $6^n a^l$ and $6^n b^m$ respectively where n denotes the degree of $\mathbb{Q}(\alpha, \beta)$ and Theorem 1.6 follows. □

A much deeper result in the context of Liouville's theorem was discovered by Thue [243] in 1909 and Thue's work was subsequently developed in important papers by Siegel [226], Schneider [212], Dyson [81], Gelfond [108] and Roth [204]. Let α be an algebraic number with degree $n > 1$ and consider the inequality

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{\varkappa}}$$

for $c = c(\alpha, \varkappa) > 0$ and p, q rational integers. Then Thue showed that $c(\alpha, \varkappa)$ exists for $\varkappa > \frac{1}{2}n + 1$. The result was sharpened by Siegel to $\varkappa > s + n/(s+1)$ for any positive integer s, in particular to $\varkappa > 2\sqrt{n}$, and this was further improved by Dyson and Gelfond independently to $\varkappa > \sqrt{2n}$. Finally Roth showed that there exists $c(\alpha, \varkappa) > 0$ for any $\varkappa > 2$ and, by continued fraction theory for example, this is best possible.

Theorem 1.7 (Thue–Siegel–Roth) *If $\varkappa > 2$ then there exists $c(\alpha, \varkappa) > 0$ such that the above inequality holds for all rationals p/q $(q > 0)$.*

Thue was motivated by studies on Diophantine equations and one of the main applications of his result was a demonstration of the finiteness of the number of solutions of the equation $F(x, y) = m$ where F is an irreducible binary form with integer coefficients and degree at least 3 (see Section 3.3). Siegel's sharpening led to his famous theorem that there are only finitely many integer points on any algebraic curve of genus at least 1. The works of Thue and Siegel were based on the construction of a polynomial in two variables by means of the box principle and they yielded an estimate for the number of solutions to the equations in question. But they did not furnish an estimate for the sizes of the solutions and so they did not enable one to actually

solve the equations. The reason lay in the ineffectiveness of the constant c in Theorem 1.7 and its earlier versions subsequent to that of Liouville; it arises from a purely hypothetical assumption at the beginning of the proof that α has at least one good approximation p/q with large q. The first effective improvement on Liouville's theorem for some particular algebraic numbers was obtained by Baker [12] using a method involving hypergeometric functions. As an example he showed [13] that

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > 10^{-6}\frac{1}{q^{2.955}}.$$

This immediately yields a bound in terms of m for all integer solutions of the Diophantine equation $x^3 - 2y^3 = m$ and indeed it enables one to solve the equation completely for any reasonably sized m. Many other examples of this type relating to approximation to fractional powers of rationals can be given; see especially [69]. However, it was not until Baker's development of the theory of linear forms in the logarithms of algebraic numbers [15] that one was able to give the first general effective improvement on Liouville's theorem. The latter theory and its ramifications will be the main theme of this book.

Before closing this section it should be mentioned that Bombieri [47] (see also the discussion in [48]) has recently succeeded in obtaining an alternative approach to questions on effective improvements on Liouville's theorem. His work is based on the original Thue–Siegel technique and surprisingly he shows that this can be made effective. But the method based on the theory of logarithmic forms would seem at present to be stronger.

1.2 The Hermite–Lindemann theorem

In 1873 Hermite [127] proved that e is transcendental. His proof was based on Padé approximants to $e^x, \ldots, e^{nx}$. Lindemann [146] extended Hermite's method to $e^{\alpha_1 x}, \ldots, e^{\alpha_n x}$ and showed thereby in 1882 that π is transcendental (see Section 6.3 for further historical details). In fact Lindemann proved a much more general result which includes the transcendence of e and π as special cases.

Theorem 1.8 *Whenever $\alpha_0, \ldots, \alpha_n$ are distinct algebraic numbers and $\beta_0, \ldots, \beta_n$ are non-zero algebraic numbers we have*

$$\beta_0 e^{\alpha_0} + \cdots + \beta_n e^{\alpha_n} \neq 0.$$

Plainly the transcendence of e follows on taking $\alpha_j = j$ and the β as integers or simply on taking $n = 1$, $\alpha_0 = 0$, $\alpha_1 = 1$ and $\beta_1 = -1$. Further, the transcendence of π follows from Euler's equation $e^{i\pi} = -1$. It is also readily seen that Theorem 1.8 implies the transcendence of e^{α} and $\log \alpha$ for algebraic $\alpha \neq 0, 1$, and also the transcendence of the trigonometric functions $\cos \alpha$, $\sin \alpha$ and $\tan \alpha$ for algebraic $\alpha \neq 0$.

Proof of Theorem 1.8. A proof of the theorem is given in [25, Ch. 1, §3]. We shall not repeat the details here but shall give instead a demonstration of the transcendence of π following the same method.

Accordingly suppose that π is algebraic. On defining $\vartheta = i\pi$ and using Euler's identity $e^{i\pi} = -1$ we get $e^{\vartheta} = -1$ whence

$$(e^{\vartheta_1} + 1) \cdots (e^{\vartheta_d} + 1) = 0,$$

where $\vartheta_1, \ldots, \vartheta_d$ denote the conjugates of ϑ. On expanding the left-hand side we obtain a sum of 2^d terms e^{Θ}, where

$$\Theta = \varepsilon_1 \vartheta_1 + \cdots + \varepsilon_d \vartheta_d$$

and $\varepsilon_j = 0$ or 1; we suppose that precisely n of the numbers Θ are non-zero and we denote these by $\alpha_1, \ldots, \alpha_n$. We have then

$$b_0 + b_1 e^{\alpha_1} + \cdots + b_n e^{\alpha_n} = 0,$$

where b_0 is the positive integer $2^d - n$, where $b_1 = \cdots = b_n = 1$ and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers such that $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is a Galois field, that is $\alpha_1, \ldots, \alpha_n$ can be written as complete sets of conjugates. We proceed to show that the equation is impossible; indeed we shall prove this under the more general assumption that the b are arbitrary integers such that for each complete set of conjugates $\alpha_{k_1}, \ldots, \alpha_{k_m}$ the corresponding $b_{k_1}, \ldots, b_{k_m}$ are equal. The latter assumption and the Galois condition hold trivially on taking $\alpha_j = j$ and so our result will then include the transcendence of e.

We define

$$I(t) = \int_0^t e^{t-u} f(u)\, du,$$

where $f(x) = l^{np} x^{p-1} (x - \alpha_1)^p \cdots (x - \alpha_n)^p$; here p denotes a large prime and l is any positive integer such that $l\alpha_1, \ldots, l\alpha_n$ are algebraic integers. Now by iteration of partial integration we get

$$I(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t),$$

where $m = (n+1)p - 1$ and $f^{(j)}$ is the jth derivative of f. Let $\bar{f}$ be the polynomial obtained from f by replacing each coefficient of f with its absolute value; then

$$|I(t)| \leq |t| e^{|t|} \bar{f}(|t|).$$

We shall compare estimates for

$$J = b_1 I(\alpha_1) + \cdots + b_n I(\alpha_n).$$

By the exponential equation and the expression for $I(t)$ above we have

$$\begin{aligned} J &= \sum_{k=1}^{n} b_k e^{\alpha_k} \sum_{j=0}^{m} f^{(j)}(0) - \sum_{k=1}^{n} b_k \sum_{j=0}^{m} f^{(j)}(\alpha_k) \\ &= -b_0 \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} \sum_{k=1}^{n} b_k f^{(j)}(\alpha_k). \end{aligned}$$

Now we know by our Galois assumption that J remains fixed under the automorphisms of $\overline{\mathbb{Q}}$ (algebraic closure of $\mathbb{Q}$) and is therefore a rational integer (note that the coefficients of f are symmetric in the α_j). By the definition of f we have $f^{(j)}(\alpha_k) = 0$ for $j < p$ and $f^{(j)}(0) = 0$ for $j < p - 1$ and

$$f^{(p-1)}(0) = (-1)^n\, (p-1)!\, (l^n \alpha_1 \cdots \alpha_n)^p.$$