

TRANSCENDENTAL NUMBERS AND DIOPHANTINE APPROXIMATIONS¹

BY SERGE LANG

ABSTRACT. This is a survey article on the state of knowledge concerning the transcendence and algebraic independence of various numbers, obtained as values of certain classical functions, mostly of exponential and logarithmic type. The diophantine approximation considerations are taken from the point of view of quantitative results concerning the above numbers, i.e. give an explicit lower bound for values $P|\alpha_1, \dots, \alpha_n|$, where P is a polynomial with integer coefficients, and $\alpha_1, \dots, \alpha_n$ are the numbers under consideration. The lower bound should depend on the degree of P , the size of its coefficients, and the numbers α_i . Some discussion is given as to what "best possible" such lower bounds have been or could be obtained.

Let f be a classical function (for instance exponential, elliptic, zeta, etc.). Starting with the rational numbers, one can construct a field inductively by adjoining values of f with arguments in the field already obtained, taking algebraic closure, and iterating these operations (as already suggested in [48]). We may call the numbers so obtained the "classical" numbers. Our point of view is that the theory of transcendental numbers determines which of the numbers so obtained are transcendental (over the rational numbers \mathbb{Q}). This is the qualitative theory. Given numbers w_1, \dots, w_n in this field, and a nonzero polynomial $F(X_1, \dots, X_m)$ with integer coefficients, one then wants to give a lower bound for the absolute value

$$|F(w_1, \dots, w_n)|,$$

as a function of the degree of F , the absolute value of its coefficients and of course the w_i . This is the quantitative theory, and we view diophantine approximations from this point of view in the present survey. (If w_1, \dots, w_n have already been proved to be algebraically independent then $F(w_1, \dots, w_n) \neq 0$. Otherwise, one has to assume this latter condition.) Because of the present point of view, I do not discuss the full range of the theory of diophantine approximations

AMS 1970 subject classifications. Primary 10F35, 10F40; Secondary 10F45, 33A10, 33A35, 32A20, 14L10.

Key words and phrases. Transcendental numbers, diophantine approximations, exponentials, logarithms, several complex variables.

¹ A survey article printed by invitation of the editors; received by the editors March 12, 1971.

Copyright © American Mathematical Society 1971

and a large body of results are omitted which would otherwise find their place.

The number of monographs on these subjects is still small. We refer the reader generally to Siegel [87], Gelfond [44], Schneider [80], and Lang [49] for transcendental numbers; and to Cassels [24], Khintchine [46], Schmidt [77] and Lang [50], for diophantine approximations. More precise references are given in the course of the report.

The theory of transcendental numbers offers ground for research over a very broad spectrum of tastes. One can work on the ground floor of mathematics, with very little knowledge, and still prove very deep results, or one may wish to work in the general context of the parametrization of algebraic varieties by uniformizing maps, and formulate or prove transcendence results for such objects. I have included a report of both types of results. The reader can always disregard those aspects which he may dislike. On the other hand, solutions of problems which have simple statements (e.g. Siegel's theorem on the finiteness of integral points on curves of genus ≥ 1) require machinery for their proofs which is fairly elaborate, so that such proofs are out of the reach of those who dislike, say, abelian or automorphic functions. Furthermore, the present relations with the theory of several complex variables are clearly becoming very fruitful, and may draw the analysts into number theory, or vice versa.

The present report attempts to cast results in fairly comprehensive terms. Especially in diophantine approximations, where results are less extensive at present than comparable results in transcendental numbers, I have attempted to tie together what I regard as very partial results by making conjectures. We are dealing with a branch of mathematics where practically any example is already a theorem.

TRANSCENDENTAL NUMBERS

1. The ordinary exponential function. The theory of transcendental numbers started with Hermite's proof [45] that

(1.1) *e is transcendental.*

A few years afterwards, this result was extended by Lindemann [56] who showed that:

(1.2) *If α is algebraic $\neq 0$, then e^α is transcendental. In particular, π is transcendental (because $e^{2\pi i} = 1$).*

Lindemann proved much more, namely:

(1.3) *If $\alpha_1, \dots, \alpha_n$ are algebraic numbers linearly independent over the rationals, then*

$$e^{\alpha_1}, \dots, e^{\alpha_n}$$

are algebraically independent.

(By algebraically independent, we always mean over the rationals, unless otherwise specified.)

These results were to be extended in two directions, stemming from the differential equation satisfied by e^z , or from its addition theorem. They fit in the general context of determining conditions under which classical functions, suitably normalized, take on transcendental values at algebraic points. More generally, under suitable conditions one expects that algebraically independent functions take on algebraically independent values at a certain point, unless there is a "structural" reason for it being otherwise. We shall see later concrete examples of this. In the case of the Lindemann theorem, the functions are $e^{\alpha_i t}$, $i = 1, \dots, n$, with algebraic α_i , linearly independent over the rational numbers \mathbb{Q} . However, proofs of algebraic independence results are considerably more difficult at present than proofs for transcendence results.

In the same line as above, we also have the classical theorem of Gelfond-Schneider [44], [80], [87], [49]:

(1.4) *If α, β are algebraic, $\alpha \neq 1$, and β irrational, then α^β is transcendental.*

This was extended in a significant way recently by Baker [11], who shows:

(1.5) *If $\alpha_1, \dots, \alpha_n$ are non zero algebraic numbers, multiplicatively independent (or equivalently, whose logarithms, together with $2\pi i$, are linearly independent over the rationals), and β_1, \dots, β_n are algebraic, and such that $1, \beta_1, \dots, \beta_n$ are linearly independent over the rationals, then*

$$\alpha^{\beta_1} \dots \alpha^{\beta_n}$$

is transcendental. Furthermore, the numbers

$$\log \alpha_1, \dots, \log \alpha_n$$

are linearly independent over the algebraic numbers.

We shall return to this later in connection with diophantine approximations.

The preceding results use the differential equation, as well as the addition theorem. Using only the addition theorem, one obtains the following statement.

- (1.6) *Let β_1, β_2 be complex numbers, linearly independent over \mathbb{Q} , and let z_j ($j=1, 2, 3$) be complex numbers, also linearly independent over \mathbb{Q} . Then at least one of the numbers*

$$e^{\beta_1 z_j}, e^{\beta_2 z_j} \quad (j = 1, 2, 3)$$

is transcendental.

Thus for instance, if y is real and x^y is algebraic for all positive rational $x \neq 0$, then y is rational. Although this statement was known to Siegel [9], I rediscovered it independently and Siegel wrote me once that the proof I gave in [49] apparently was the first in the literature. Since this proof is the simplest in the theory of transcendental numbers, but also exhibits some basic features from all proofs, we shall summarize it below.

In investigating values of α^β when β is transcendental and α is algebraic, there may be one algebraic α such that α^β is algebraic. For instance,

$$2^{\frac{\log 3}{\log 2}} = 3.$$

By the Gelfond-Schneider theorem, $\log 3 / \log 2$ is transcendental, and constitutes such a number β for which 2^β is algebraic. The previous theorem shows that there are at most two multiplicatively independent possibilities, and conjecturally there is only one, i.e. one can shrink 3 to 2 in Theorem (1.6).

The most general conjecture concerning transcendence and algebraic independence of values of the exponential function is due to Schanuel, and runs as follows.

- (1.7) *Let $\alpha_1, \dots, \alpha_n$ be complex numbers, linearly independent over the rationals. Then the transcendence degree of the field*

$$\mathbb{Q}(\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n})$$

is at least n .

For instance, this implies Lindemann's Theorem (1.3), and also implies the old conjecture that the logarithms of multiplicatively independent algebraic numbers are algebraically independent. (Baker's theorem 1.5 concerns their linear independence.) Note that it is unknown even if $\log 2$ and $\log 3$ are algebraically independent, or even

if $(\log 2)(\log 3)$ is algebraic. It is unknown if $e+\pi$ is algebraic. The algebraic independence of e, π would follow from Schanuel's conjecture by considering $1, 2\pi i, e, e^{2\pi i}$. In fact, Schanuel's conjecture implies at once all other known conjectures concerning values of the exponential function. For instance, I had conjectured that π cannot lie in the field obtained by starting with the algebraic numbers, adjoining values of the exponential function, taking algebraic closure, and iterating these two operations. This follows from Schanuel's conjecture as follows. Let $\alpha=(\alpha_1, \dots, \alpha_n)$ be linearly independent algebraic numbers. Use vector notation, so that $e^\alpha=(e^{\alpha_1}, \dots, e^{\alpha_n})$. By (1.7) it follows from the linear independence of $(\alpha, 2\pi i)$ that

$$\alpha, 2\pi i, e^\alpha, 1$$

has transcendence degree $\geq n+1$, whence π is transcendental over the field F_1 obtained by adjoining all values e^α to \mathcal{Q} . Now take n large, let $u=(u_1, \dots, u_n)$ be algebraic over F_1 and linearly independent over F_1 . Consider

$$\alpha, e^\alpha, u, 2\pi i; \quad e^\alpha, e^{e^\alpha}, e^u, 1.$$

Selecting u to have sufficiently many elements, one sees again from (1.7) that $2\pi i$ is transcendental over $\mathcal{Q}(e^\alpha, u)$. One then proceeds by induction.

Schanuel also formulated his conjecture for formal power series in lieu of complex numbers. In this context the conclusion amounts to the algebraic independence of formal power series. This was proved by Ax [10].

The theory of transcendental numbers can also be developed p -adically. Let \mathbf{C}_p be the completion of the algebraic closure of the p -adic numbers \mathcal{Q}_p . Then \mathbf{C}_p plays for the p -adic absolute value the same role as \mathbf{C} for the ordinary absolute value. Mahler first extended the transcendence proof of e^α and α^β to the p -adic case [57]. For further results, see also Adams [7]. Brumer [23] proved the p -adic analogue of Baker's theorem, and thereby showed that Leopoldt's p -adic regulator does not vanish [54], for abelian extensions of the rationals. The p -adic analogue of (1.6) given in [49] has been used by Serre in his theory of p -adic representations [82]. The methods of complex variables in the standard case can be replaced by the p -adic Schnirelman integral and Cauchy formula. For a convenient exposition, see Adams [7].

2. Sketch of proofs. Gelfond was the first to realize explicitly the connection between transcendence problems and algebraic values of

entire, or meromorphic functions. Many years before he proved the α^β theorem, investigating special cases in 1929 (cf. [43]), he saw that such a problem was related with a question (I believe raised by Polya) concerning the possibility of an entire function taking integral values at integers, and the interpolation problem arising from it. If f, g are, say, entire functions taking algebraic values in a set S , then one reduces the study of S to an analytic problem concerning *zeros* of an auxiliary function, a polynomial in f, g , namely

$$F = \sum a_{ij} f^i g^j,$$

with coefficients in a number field (finite extension of the rationals). From the assumption that f, g take on values in the number field in S , one can construct such a function F having many zeros by a simple lemma of Siegel concerning linear equations with integral coefficients, [87] or [49]. For simplicity we state Siegel's lemma over the ordinary integers \mathbf{Z} .

(2.1) *Let*

$$\begin{aligned} u_{11}x_1 + \cdots + u_{1n}x_n &= 0, \\ &\dots \\ u_{r1}x_1 + \cdots + u_{rn}x_n &= 0, \end{aligned}$$

be a system of linear equations with integer coefficients u_{ij} . Let A be a bound for the absolute values of all u_{ij} , and assume $n > r$. Then this system has a solution in integers x_j not all 0, satisfying

$$\max |x_j| \leq (nA)^{r/(n-r)}.$$

Suppose that f, g take on values in the integers \mathbf{Z} , and are algebraically independent. On the one hand, using the lemma, one can construct a function F having enough zeros in the set S so that at some point w of S , the value $F(w)$ is very small. On the other hand, if S has sufficiently many elements, one can also pick w so that $F(w) \neq 0$, and since $F(w)$ is an integer, one gets the contradiction.

A function like F was used first by Siegel when he proved transcendence results for the Bessel function (stated precisely later). A similar function led to other results like the transcendence of α^β . As an example, we shall now sketch a proof of (1.6), in a special case, with the functions

$$f(t) = e^{\beta_1 t} \quad \text{and} \quad g(t) = e^{\beta_2 t},$$

showing that they cannot take on values in \mathbf{Z} at three points z_1, z_2, z_3

linearly independent over \mathcal{Q} . Suppose that they did. We let n be a large integer, assumed square free for convenience. Let $r = (4n)^{3/2}$. By Siegel's lemma we can find integers a_{ij} not all 0 such that the function $F = \sum_{i,j=1}^r a_{ij} f^i g^j$ has a zero at every point

$$k \cdot z = k_1 z_1 + k_2 z_2 + k_3 z_3, \quad 1 \leq k_\nu \leq n.$$

This amounts to solving linear equations in r^2 unknowns, with $r^2 = (4n)^3$ and the number of equations is equal to n^3 . The coefficients of these equations are bounded by $C^{n^{3/2}}$ for some constant C . Hence by Siegel's lemma, we can find integers a_{ij} not all 0, satisfying a similar bound. Since f, g are algebraically independent, it follows that F is not identically zero, and takes on values in \mathcal{Z} for all arguments $k \cdot z$. On the other hand, F cannot vanish at all such linear combinations, with all triples of integers k , because the linear combinations $k \cdot z$ are not discrete, or alternatively because F is entire of order 1, and in a circle of large radius R , there are more such linear combinations than the bound $O(R)$ for the number of possible zeros of F . Let s be the largest integer such that $F(k \cdot z) = 0$, for all k with $1 \leq k_\nu \leq s$. Then $s \geq n$. Let

$$w = k_1 z_1 + k_2 z_2 + k_3 z_3,$$

with some $k_\nu = s + 1$, and $1 \leq k_\nu \leq s + 1$ for all ν , and $F(w) \neq 0$. Then

$$|F(w)| \leq C^{s^{3/2}},$$

with a suitable constant C . We now estimate $|F(w)|$ by considering the expression

$$F(w) = \frac{F(t)}{\prod (t - k \cdot z)} \prod (w - k \cdot z) \Big|_{t=w},$$

the products being taken over all k_ν with $1 \leq k_\nu \leq s$. There are s^3 terms in the product. The function on the right of this last equality is an entire function, and we apply the maximum modulus principle on a circle of radius $R = s^{3/2}$. Note that for $|t| = R$, we have $|t - k \cdot z| \geq R/2$ (for s large), and also

$$\frac{|w - k \cdot z|}{|t - k \cdot z|} \leq \frac{C_1 s}{R} \leq \frac{C_1}{s^{1/2}}$$

for some constant C_1 and s large. Hence

$$\log |F(w)| \ll \log |F|_R + s^3 - \frac{1}{2} s^3 \log s,$$

where the sign \ll means that the left-hand side is smaller or equal to a

constant times the right-hand side (Vinogradov's notation), and $|F|_R$ is the maximum of F on the circle of radius R . A trivial estimate shows that

$$\log |F|_R \ll s^3,$$

whence

$$\log |F(w)| \ll s^3 - s^3 \log s.$$

For n (and hence s) large, this contradicts the fact that $|F(w)| \geq 1$, and completes the proof.

The extension to number fields and algebraic values involves only minor technique in algebraic numbers. If K is a number field (finite extension of \mathcal{Q}), let $\{\sigma\}$ range over the embeddings of K in \mathbf{C} . For any element α in K , we call $\{\sigma\alpha\}$ the conjugates of α . A positive integer d such that $d\alpha$ is an algebraic integer is called a denominator for α . We let

$$\text{size}(\alpha) = \max(\log d, \log |\sigma\alpha|),$$

where d is the smallest denominator for α , and $\sigma\alpha$ range over the conjugates of α . Taking the norm of $d\alpha$, which is an ordinary integer $\neq 0$ if $\alpha \neq 0$, one gets the fundamental inequality

$$(2.2) \quad -2[K:\mathcal{Q}] \text{size}(\alpha) \leq \log |\sigma\alpha|,$$

for any σ . This inequality then can be used to replace the last part of the argument in the preceding proof. Generally speaking, working with algebraic numbers in this context is no harder than working with ordinary integers.

As an example, we shall give one of Baker's theorems [11], concerning an effective lower bound for linear combinations of logarithms of algebraic numbers, with algebraic coefficients. Baker's proof used previous ideas of Gelfond [44] and Feldman (cf. his list of papers). Although Gelfond's method was effective, it applied only to the case of two logarithms, and Baker saw how to extend it to linear combinations of n logarithms. The importance of doing this had already been observed by Gelfond, who remarked that such an extension would lead to an effective improvement of Liouville's inequality (see below). Baker's theorem is as follows.

(2.3) *Let $\alpha_1, \dots, \alpha_{n+1}$ be algebraic numbers, whose logarithms are linearly independent over the rational numbers. Let $\tau > n+2$. Then there exists an effectively computable constant $c(\alpha) = c$ such that for any algebraic numbers β_1, \dots, β_n of size $\leq h$ we have*

$$\log |\beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n - \log \alpha_{n+1}| > -ch^\tau.$$

We now sketch Baker's proof, and assume that β_1, \dots, β_n are such that

$$\log |\beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n - \log \alpha_{n+1}| \ll -h^\tau,$$

with $h \geq c(\alpha)$ size β . We construct the auxiliary function

$$F(z_1, \dots, z_{n+1}) = \sum a_{(j)} \alpha_1^{jz_1} \dots \alpha_n^{jz_n} (\alpha_1^{\beta_1} \dots \alpha_n^{\beta_n})^{j_{n+1}z_{n+1}}$$

to have zeros of high order at certain points. We shall use vector notation, so that we write

$$F(z) = \sum a_{(j)} \alpha^{jz} (\alpha^\beta)^{j_{n+1}z_{n+1}}.$$

The sum is taken for $0 \leq j_\nu < J$, with a suitable integer J . Using vector notation, we abbreviate this in the form $j \leq J$. Let $\lambda = (\lambda_1, \dots, \lambda_n)$. Let

$$D^\lambda = D_1^{\lambda_1} \dots D_n^{\lambda_n}$$

be the standard differential operator, and for an integer $k \geq 0$ consider

$$D^\lambda F(k, \dots, k) = \sum a_{(j)} \alpha^{jk} \alpha^\beta {}^{j_{n+1}k} (j + j_{n+1}\beta)^\lambda.$$

We shall want to make this derivative essentially equal to 0 for certain values of k and λ . This amounts to solving linear equations. Indeed, α_{n+1} is very close to $\alpha_1^{\beta_1} \dots \alpha_n^{\beta_n}$, and one solves the corresponding linear equations with α^β replaced by α_{n+1} . Let

$$G_\lambda(k) = \sum_{j < J} a_{(j)} \alpha^{jk} \alpha_{n+1}^{j_{n+1}k} (j + j_{n+1}\beta)^\lambda.$$

Select δ such that $1 < \delta < \tau/(n+2)$. Let

$$J \doteq h^\delta \quad \text{and} \quad L \doteq h^{\delta + (\delta-1)/n}.$$

(Since for instance h is not necessarily an integer, by these equalities \doteq we mean that J or L are equal to the largest integers less than or equal to the right-hand sides.) Solve the linear equations

$$G_\lambda(k) = 0$$

for $\lambda \leq L$ and $1 \leq k \leq h$. Then the number of variables is approximately equal to J^{n+1} , the number of equations is approximately equal to $L^n h$, and the size of the coefficients is $\ll Lh$. Note that the number of variables is approximately equal to the number of equations. By using

the existence of zeros of high order, and the usual estimate with the maximum modulus principle, one then finds that

$$(*) \quad \log |D^\lambda F(k, \dots, k)| \ll -h^\tau$$

for $1 \leq k \leq h$. Proceeding inductively, we wish to achieve the inequality (*) for

$$k \leq h_\nu = h^{1+\nu(\delta-1)/n} \quad \text{and} \quad \lambda \leq L/2^\nu,$$

with ν ranging from 1 to approximately n^3 . The inductive step is done by taking $l \leq h_{\nu+1}$ and $\lambda \leq L/2^{\nu+1}$. Let

$$f(t) = D^\lambda F(t, \dots, t).$$

Then

$$\frac{f(l)}{\prod_{k \leq h_\nu} (l - k)^{L/2^{\nu+1}}} = \frac{f(t)}{\prod_{k \leq h} (t - k)^{L/2^{\nu+1}}} \Bigg|_{t=l}.$$

We use the maximum modulus principle with a circle of radius

$$R = h^{1 + \frac{(\delta-1)}{n} + \nu \frac{(\delta-1)}{n}}$$

and estimate $\log |f(l)|$. From the fundamental inequality (2.2) we conclude that $G_\lambda(l) = 0$ by induction. (It is this inductive step which represents the improvement by Baker over the earlier Gelfond method.)

Thus our inductive procedure ultimately gets us to

$$G_0(k) = \sum_{j \leq J} a_{(j)} \alpha^{jk} \alpha_{n+1}^{j_{n+1}k} = 0$$

for $k \leq h^{\delta(n+1)}$. This is a system of linear equations, whose matrix of coefficients has a Vandermonde determinant, whence the contradiction which proves Baker's theorem.

Baker's theorem has gone through successive improvements, lowering the exponent τ , and recent papers of his adjust the arguments to avoid the Vandermonde determinant at the end. This is advantageous because in more complicated situations requiring an extension of the proof, it is not obvious to show that the corresponding determinant does not vanish. One of these deals with elliptic functions. Cf. the papers of Baker and Coates on this subject.

3. Algebraic values of meromorphic functions. The importance of solutions to differential equations in connection with transcendence

results first appeared in Siegel's results on the Bessel function [86]. We state these in §5. Schneider [79] gave a general criterion under which an entire, or meromorphic function satisfying a certain type of algebraic differential equation with algebraic coefficients can take on values in a number field at only a finite number of points. His type of differential equation was sufficiently general to include the ordinary exponential function, the Weierstrass elliptic function, and the elliptic modular function. Using Schneider's ideas properly, and proving the right estimates, I then extended the result to the most general algebraic differential equation (needed for other applications e.g. abelian functions). We recall that an entire function f on \mathbf{C} is said to be of strict order $\leq \rho$ if

$$\log |f|_R \ll R^\rho.$$

A meromorphic function is said to be of strict order $\leq \rho$ if it can be expressed as a quotient of entire functions of order $\leq \rho$. We then have [49]:

- (3.1) *Let K be a number field. Let f_1, \dots, f_N be meromorphic functions of strict order $\leq \rho$. Assume that the field $K(f_1, \dots, f_N)$ has transcendence degree ≥ 2 over K , and that the derivative $D = d/dt$ maps the ring $K[f_1, \dots, f_N]$ into itself. Let w_1, \dots, w_m be distinct complex numbers not lying among the poles of the f_i such that*

$$f_i(w_\nu) \in K$$

for all $i = 1, \dots, N$ and $\nu = 1, \dots, m$. Then $m \leq 20\rho [K:\mathbf{Q}]$.

The transcendence of e^α then follows by considering the ring $K[t, e^t]$. Assuming that e^α is algebraic, one takes K to contain both α and e^α . Then the infinite number of points $\alpha, 2\alpha, 3\alpha, \dots$ provides the contradiction. Similarly, for α^β one considers $K[e^t, e^{\beta t}]$. Still following Schneider, one gets the transcendence of $\wp(\alpha)$ for a Weierstrass \wp -function, with algebraic α , and algebraic g_2, g_3 by considering the ring $K[\wp, \wp']$.

Schneider had proved the transcendence of the periods of abelian functions by dealing with several complex variables [78]. I formulated a theorem analogous to (3.1) in several variables [49]. To get a similar bound on the set of points where the functions take on values in K , I had to assume that the set S of such points was a product of sets on the coordinate axes, to be able to use Cauchy's formula in several variables as an iteration of the formula in one variable (as Schneider had done). The product condition was unnatural, as one sees from the example of functions

$$z_1, \dots, z_n, e^{P(z_1, \dots, z_n)}$$

where P is a polynomial with integer coefficients. These functions are algebraically independent and take on algebraic values at the algebraic zeros of P . By using deep techniques from the theory of several complex variables (potential theory and Hörmander L^2 -estimates) Bombieri was able to remove the product condition, and proved the following theorem [21].

(3.2) *Let K be a number field and let $f = (f_1, \dots, f_N)$ be meromorphic functions in \mathbf{C}^d of strict order $\leq \rho$. Assume that the transcendence degree of $K(f)$ is $\geq d+1$, and that the partial derivatives $D_i = \partial/\partial z_i$ map the ring $K[f]$ into itself. Then the set of points $w \in \mathbf{C}^d$ where $f(w)$ is defined and $f(w) \in K^N$ is contained in an algebraic hypersurface of degree*

$$\leq d(d+1)\rho[K:\mathbf{Q}] + 2d.$$

In the simple case when the above set of points S is of type

$$S = S_1 \times \dots \times S_d,$$

where $S_j \subset \mathbf{C}$, then Bombieri's theorem implies the bound which I had obtained for the cardinality of S , of the form $b\rho[K:\mathbf{Q}]$, for some easily computable constant b depending on d . This special case is actually sufficient for a number of applications (see below, and [49]).

When no differential equation is available, then one has to rely on other properties of the set of points where the functions take on values in K . Usually such a set S is expressed as a union of subsets $\{S_n\}$, where each S_n is contained in a ball of radius $\ll n$, and where the functions have a specified arithmetic order of growth, e.g. there exists a constant C such that for all n and all $z \in S_n$ we have

$$\text{size } f(z) \leq Cn^\rho.$$

Schneider first formulated such a theorem [79] in one variable. For useful variants and applications, see [49]. We shall state the applications on group varieties in §4, including the several variables version.

We note that instead of taking values in a number field, one may take values in a finitely generated extension, provided that one assumes a condition to replace (2.2). See [49] for the appropriate statements, raising possibilities for an inductive argument. In dimension 1, Waldschmidt [92] eliminated the extra condition. We discuss this again in connection with diophantine approximations.

4. General exponential functions. A group variety is a group in affine or projective space, which is also an algebraic variety (con-

nected), i.e. its points are the set of solutions of algebraic equations, and such that the law of composition and inverse have graphs which are also algebraic varieties. An important example is the linear group $GL(m)$ of invertible $m \times m$ matrices. If K is a subfield of the complex numbers, we say that the group variety is defined over K if all the above mentioned algebraic equations can be chosen to have coefficients in K . If that is the case, then we denote by G_K the set of points of G having coordinates in K , and it follows that G_K is a group. When K is a number field, we view G_K as a discrete group. When $K = \mathbf{C}$, we view $G_{\mathbf{C}}$ as a complex analytic manifold, i.e. a complex analytic group.

Let G be a group variety. By a 1-parameter subgroup of G we mean a complex analytic homomorphism $\phi: \mathbf{C} \rightarrow G_{\mathbf{C}}$ of the complex line into $G_{\mathbf{C}}$ whose derivative at the origin is injective. Thus ϕ is an analytic curve in $G_{\mathbf{C}}$. We define a d -parameter subgroup $\phi: \mathbf{C}^d \rightarrow G_{\mathbf{C}}$ in a similar way. For instance, when G is the linear group, a 1-parameter subgroup is given by the exponential series

$$t \mapsto \sum \frac{t^k M^k}{k!}$$

where M is a matrix. We are interested both in conditions under which a point $\phi(z)$ is algebraic, and also under which the image of ϕ is an algebraic subgroup (i.e. is closed). Most of the time, of course, the image just winds around (in the compact case). Indeed, the compact case is obtained as follows. We take a lattice L of real dimension $2n$ in complex n -space. Let us assume that the factor group \mathbf{C}^n/L can be embedded complex analytically in projective space $P_{\mathbf{C}}^N$, so that its image in projective space is necessarily an algebraic group (Chow's Theorem, for instance). Let us also assume that this group is defined over a number field. A 1-parameter subgroup may be viewed as winding around the torus \mathbf{C}^n/L , which is called an abelian manifold. The algebraic group corresponding to it in projective space is called an abelian variety. In dimension $n = 1$, the parametrization of the abelian variety is done by means of the Weierstrass elliptic function,

$$z \mapsto (1, \wp(z), \wp'(z)),$$

the coordinates on the right being projective coordinates, on the elliptic curve

$$y^2 = 4x^3 - g_2x - g_3.$$

An analytic subgroup of an abelian variety is closed if and only if it is an abelian subvariety (i.e. an algebraic subgroup). If this analytic

subgroup is algebraic and has dimension 1, it is an elliptic curve.

For 1-parameter subgroups, we have the following theorem [49].

- (4.1) *Let G be a linear group variety or an abelian variety, defined over the field of algebraic numbers. Let $\phi: \mathbf{C} \rightarrow G_{\mathbf{C}}$ be a 1-parameter subgroup. Let Γ be a subgroup of \mathbf{C} having at least three linearly independent elements over \mathbf{Z} in the linear case, and seven in the abelian case. If $\phi(\Gamma)$ is contained in the group of algebraic points of G , then the image of ϕ is closed, i.e. it is an algebraic subgroup of $G_{\mathbf{C}}$.*

(In the mixed case of a product, say, one has to take the maximum of three and seven to get the same conclusion.)

The proof follows the same lines as the proof given in §2, but to make the required estimates in the abelian case, one must use the quadratic form of Néron-Tate [64]. Conjecturally, the numbers 3 and 7 can be shrunk to 2, as for (1.6).

The extension of (4.1) presented difficulties of two types. The first concerns pure analysis, namely the need for a Schwarz lemma in several variables. It was surmounted by Bombieri-Lang [22], who prove the following result. Let λ be a positive number. Let $\{S_n\}$ be a sequence of subsets of \mathbf{C}^d . Let B_r be the ball of radius $r > 0$, centered at the origin in \mathbf{C}^d . We say that the family $\{S_n\}$ is λ -distributed in B_r , if the following condition is satisfied. There exists N_0 such that given $w \in B_r$ and $N \geq N_0$ there exists a point $u \in S_N$ such that

$$|u - w| \leq 1/2N^\lambda.$$

If Γ is a finitely generated subgroup of \mathbf{C}^d , with generators $\{u_1, \dots, u_m\}$ then we let S_n be the set of all linear combinations

$$k_1 u_1 + \dots + k_m u_m, \quad |k_j| \leq n.$$

We have:

- (4.2) *Let G be a linear or abelian group variety. Let $\phi: \mathbf{C}^d \rightarrow G_{\mathbf{C}}$ be a d -parameter subgroup, and let Γ be a finitely generated subgroup of \mathbf{C}^d , which is λ -distributed in a ball B_r . Assume that $\lambda > (d+1)/2$ in the linear case, and $> d+1$ in the abelian case. If $\phi(\Gamma)$ is contained in the group of algebraic points of G , then $\phi(\mathbf{C}^d)$ is an algebraic subgroup of $G_{\mathbf{C}}$, i.e. it is closed.*

The condition of λ -distribution is a condition of diophantine approximation. For further comments on it, cf. [22]. The p -adic analogue of (4.2) was done by Serre [83]. It is a deep problem to reduce

the value of λ , and to prove that it has the "expected" value arising from the theory of diophantine approximations.

If V is a variety (algebraic, irreducible) defined over a number field K , and (x_1, \dots, x_n) are affine coordinates for a point on V , then we say that this point is rational over K if $K(x) = K$, algebraic over K if $K(x)$ is algebraic over K , and transcendental over K if $K(x)$ is not algebraic over K , i.e. if at least one coordinate is transcendental over K . The other type of theorem which one has on group varieties can then be stated as follows [49].

(4.3) *Let G be a group variety defined over the field of algebraic numbers. Let $\phi: \mathbf{C} \rightarrow G_{\mathbf{C}}$ be a 1-parameter subgroup, whose differential at the origin is algebraic. If $\alpha \in \mathbf{C}$, $\alpha \neq 0$ is algebraic and $\phi(t)$ is not an algebraic function of t , then $\phi(\alpha)$ is a transcendental point on $G_{\mathbf{C}}$. On the other hand, if there exists a point $u \neq 0$ in \mathbf{C} such that $\phi(u)$ is algebraic, then $\phi(\mathbf{C})$ is an algebraic subgroup of $G_{\mathbf{C}}$.*

The first assertion of (4.3) had been conjectured by Cartier. The two formulations generalize the Lindemann theorem (1.2) and the Gelfond-Schneider theorem (1.4). In the first case, the 1-parameter group is

$$t \mapsto e^t,$$

and in the second case, it is

$$t \mapsto (e^t, e^{\beta t}).$$

The only case when $\phi(t)$ is an algebraic function of t occurs in the linear case, and when ϕ is formed with the exponential series of a nilpotent matrix, in which case ϕ is even a rational function of t .

Theorem (4.3) applied to abelian varieties yields the transcendence of the period vectors, originally proved by Schneider [78]. It also shows that in the representation

$$\Theta: \mathbf{C}^n \rightarrow A_{\mathbf{C}}$$

of an abelian variety as a quotient of \mathbf{C}^n , normalized to have algebraic derivative at the origin, the image of an algebraic point in \mathbf{C}^n is a transcendental point on $A_{\mathbf{C}}$, by considering the line passing through the point in \mathbf{C}^n , and its image under Θ .

Under the normalization at the origin by means of the differential equation (algebraic derivative), Theorem (4.3) extends to the higher dimensional case of a d -parameter subgroup

$$\phi: \mathbf{C}^d \rightarrow G_{\mathbf{C}}.$$

Instead of one point u , one must then assume the existence of d points linearly independent over \mathbf{C} , whose values under ϕ are algebraic [49]. Note the similarity with (4.2), where we do not normalize the map, but then assume the existence of more points linearly independent over \mathbf{Z} (not \mathbf{C}).

In the 1-dimensional case, Schneider had proved:

(4.4) *Let j be the elliptic modular function. If τ is algebraic and not imaginary quadratic, then $j(\tau)$ is transcendental.*

By means of the higher dimensional results, one then gets a higher dimensional analogue as follows [49].

(4.5) *Let A be an abelian variety parametrized as above, $\Theta: \mathbf{C}^n \rightarrow A_{\mathbf{C}}$, normalized to have algebraic derivative at the origin. Assume that the period matrix is normalized so that the principal matrix has the usual canonical form, and let the period matrix be $\Omega = (W_1, W_2)$. Let $T = W_2 W_1^{-1}$. If T is algebraic, then T (viewed as a linear transformation) maps the period lattice tensored with \mathbf{Q} into itself.*

When $n=1$, then $T=\tau$, $W_1=\omega_1$ and $W_2=\omega_2$. Note that $W_1^{-1}W_2$ is the moduli point associated with the abelian variety in the Siegel upper half space H_n . The theorem concerns $W_2 W_1^{-1}$, and the relation between these points is not clear.

One may attempt to formulate the Schanuel conjecture in the present context. One then has to consider a point in the product space

$$(\alpha, \Theta(\alpha)) \in \mathbf{C}^n \times A_{\mathbf{C}}.$$

The general expectation is that the transcendence degree is $\geq n$ under obvious conditions on the curve passing through α . The Riemann relations provide a counterexample to the analogue of Schanuel's conjecture in this context, but hopefully, if one stays away from the period relations, i.e. if α is not a period point, then the expected lower bound for the transcendence degree will hold up. For a general discussion, cf. [49]. Grothendieck has also formulated a conjecture concerning the possible polynomial relations for the elements of the period matrix, to the effect that they should all be due to algebraic cycles on the product of the variety with itself. The situation is as follows. Let W be a variety defined, say, over the rational numbers. Let $\{\gamma_i\}$ be a basis for its homology $H_*(W, \mathbf{Q})$, and let $\{\omega_j\}$ be a basis for $H^*(W, \mathbf{Q})$, where H^* is the cohomology defined by the algebraic complex of differential forms of De Rham. We assume that the basis $\{\omega_j\}$ is obtained by taking together bases for the Hodge spaces

$H^{p,q}$. Let Z be a subvariety of W , of dimension k . Then $Z \sim \sum n_i \gamma_i$. If ω is a differential form not of type (k, k) , then

$$\sum n_i \int_{\gamma_i} \omega = \int_Z \omega = 0.$$

In this way we obtain a linear relation among the periods, with rational coefficients. Consider this when $W = V^r$ is the product of a variety V with itself taken r times. Then $H^*(W, \mathcal{Q})$ is the tensor product of $H^*(V, \mathcal{Q})$ with itself r times, and applying the above shows that an algebraic cycle on V^r gives rise to a polynomial relation of degree k among the periods.

The graph of a nontrivial endomorphism of an elliptic curve (complex multiplication) gives an example, which would explain the algebraic (linear) dependence between two fundamental periods over the algebraic numbers.

The simplest ‘‘Riemann’’ relation is the Legendre relation (it involves the multiplicative group), arising from the parametrization of the group variety associated with integrals of the second kind by the map

$$\mathbb{C} \times \mathbb{C} \rightarrow G_{\mathbb{C}}$$

given by

$$(t, u) \mapsto (1, \wp(t), \wp'(t), u - \zeta(t)),$$

where ζ is the Weierstrass zeta function. This map has periods (ω_1, η_1) and (ω_2, η_2) (classical notation), and the Legendre relation

$$\eta_1 \omega_2 - \eta_2 \omega_1 = 2\pi i$$

is nothing but the Riemann relation for this case. It is of degree 2. On the other hand:

(4.6) *Any nonvanishing linear combination of $\eta_1, \eta_2, \omega_1, \omega_2, 2\pi i$ with algebraic coefficients is transcendental.*

Without the $2\pi i$, this was proved by Baker [13], and the more general statement is due to Coates [28]. The technique of proof extends Baker’s technique.

If G is a commutative group variety, defined over a number field K , then its tangent space at the origin can be identified with \mathbb{C}^n ($n = \dim G$). Then the general exponential map

$$\phi: \mathbb{C}^n \approx T_{\mathbb{C}} \rightarrow G_{\mathbb{C}}$$

provides a geometric setting generalizing the ordinary function e^z . Its inverse mapping is a generalized log, and the points in \mathbf{C}^n which map on 0 are the (vector) periods.

One can also look at the parametrization of curves and varieties of higher genus. Thus already in [48], I conjectured that if

$$\phi: D \rightarrow V_{\mathbf{C}}$$

is the uniformizing map of a curve V of genus ≥ 2 , from the disc D centered at the origin, normalized so as to have algebraic derivative at the origin, and if α is an algebraic point of the disc $\neq 0$, then $\phi(\alpha)$ is transcendental on V . (We assume that the curve is defined over a number field.) One can take the upper half plane instead of the disc. Curves can also be parametrized by the "noncompact" case of modular functions, so that I was thus led to the conjecture that if τ is a point of the upper half plane, not equivalent to i or $\rho = e^{2\pi i/3}$ under the modular group (i.e. such that $j'(\tau) \neq 0$) and such that $j(\tau)$ is algebraic, then $j'(\tau)$ is transcendental. Siegel [88] also makes remarks concerning the possible transcendence of $j'(\tau)$ at quadratic imaginary irrationalities other than i or ρ . If one normalizes g_2, g_3 to be algebraic, and if one takes into account the formula relating the derivative j' with j (cf. Siegel [88] or the seminar on complex multiplication [84]), then one sees that the conjecture concerning the transcendence of $j'(\tau)$ is equivalent to the following concrete statement: *Let g_2, g_3 be algebraic, and let ω be a nonzero period of the corresponding \wp -function. Then ω^2/π is transcendental. Indeed, one has the relation*

$$j'(z) = \frac{9\omega^2 g_3}{\pi i g_2} j(z).$$

(The formula in Siegel [88] is not yet properly normalized so that the ω^2 does not appear in it. The point is that g_2, g_3 can be viewed as functions of lattices, and one has to take a lattice in the given class which makes g_2, g_3 algebraic. Then ω^2 appears as the quotient of ω^6 by ω^4 .) The problem is analogous here to determining the transcendence of $(\log 2)^2/\log 3$, say.

Observe that the parametrizations of the curves by j (or the parametrization of curves of higher genus corresponding to modular functions of level N), and the parametrizations of the curves by the universal covering map normalized to send the origin of the disc to an algebraic point, and to have algebraic derivative at the origin, correspond to two different normalizations of the uniformizing map. (The fact that the fundamental domain of j is not compact is not es-

sential here, the same phenomenon occurs in the compact case, as in the work of Shimura.)

As an incidental question for the parametrization of V_C as above, one can ask if the radius of the disc D is transcendental when ϕ is normalized as stated in [48].

For some results concerning the field generated by values of the j -function and its derivatives over the algebraic numbers, cf. Ramachandra [70], who makes use directly of the differential equation satisfied by the j -function. For instance, he proves:

(4.7) *Let f be a modular form having algebraic q -expansion coefficients (classical terminology). Then the singular values $f(\tau)$, $f'(\tau)$, $f''(\tau)$, \dots for τ taking values in an imaginary quadratic field of discriminant d lie in the field*

$$\bar{\mathbb{Q}}(\pi, \Delta^{1/m}(\sqrt{d}))$$

for a suitable positive integer m .

(The integer m is made explicit, but this gets too technical here.) As usual, Δ is the modular discriminant.

One can extend the above discussion to bounded symmetric domains with compact quotients which are algebraic varieties defined over number fields. These form one possible generalization of curves of higher genus, and one may even wonder if these varieties do not satisfy the Mordell property (of having only a finite number of rational points, or points rational over a given number field). Whenever one wants to conjecture such a statement about a variety, one must be sure that there is no obvious geometric reason why the variety could have many rational points. I know of three such reasons: An infinite group of automorphisms, the function field contained in a purely transcendental extension of the constants, and the variety containing "blown up" points, or straight lines. I am told by experts that the first two conditions are known not to prevail, and that the third is probably not known in general, but probably does not prevail either, for the varieties mentioned above.

Although I have omitted a discussion of values of zeta functions (principally for lack of competence) I would like to refer the reader to at least one paper which makes a connection between such values and values of functions of exponential and automorphic type, namely that of Damerell [30], who studies values of Hecke L -series at, say, $1/2$, in connection with the Birch-Swinnerton Dyer conjecture concerning the rank of the Mordell-Weil group of an elliptic curve.

In looking at 1-parameter subgroups of abelian varieties, and to

prove certain estimates, especially from below for theta functions, I was led to conjecture [49]:

- (4.8) *Let B be a 1-parameter subgroup of an abelian variety, embedded in projective space, and let H be a hyperplane section. Assume that B is Zariski dense in A . Then the intersection of B with H is infinite, unless B is algebraic (in which case Bezout's theorem applies).*

This was proved by Ax [10], who also discovered a general phenomenon concerning the intersection of analytic subgroups and algebraic subsets of a group variety, as follows:

- (4.9) *Let A be an algebraic group and B an analytic subgroup. Let V be an algebraic subvariety of A . Assume that V , B pass through the origin. If locally at the origin the intersection of V and B has an analytic component W of excessive dimension, and if V is the Zariski closure of W in A , then there exists an analytic subgroup A' at the origin containing both V and B such that the intersection of V and B with respect to A' is not excessive.*

Of course, by excessive, we mean that if W is an analytic component of the intersection of V and B on A , then

$$\dim W > \dim V + \dim B - \dim A.$$

Ax relates this with the function theoretic formulation of Schanuel's conjecture. Thus we see throughout this section that the theory of transcendental numbers intermingles very closely with the theory of functions of several complex variables.

5. *E*-functions. Siegel [86], [87] defined an *E*-function to be a function which admits a power series expansion

$$f(z) = \sum \alpha_n z^n / n!$$

with complex coefficients α_n belonging to a number field K , satisfying the following conditions:

- E1.** There is some constant c such that all conjugates of α_n are bounded in absolute value by c^n .
- E2.** There exists a sequence of integers $d_n > 0$ such that d_n is a denominator for α_k ($k=0, \dots, n$) and $d_n \leq c^n$.

The ordinary exponential function e^z is an *E*-function, and so is the Bessel function

$$J_0(z) = \sum z^{2n} / (n!)^2.$$

Siegel [87] gives other examples similar to these. The product and sum of E -functions are E -functions.

(5.1) *Let $Q = (Q_{ij})$ ($i, j = 1, \dots, s$) be a matrix of rational functions in $K(z)$ over a number field K . Let F be the column vector formed by E -functions f_1, \dots, f_s , and assume that it satisfies the linear differential equation $F' = QF$. Assume that the functions f_1, \dots, f_s are algebraically independent over $K(z)$. Let $\alpha \in K$ be distinct from 0 and from the poles of the rational functions Q_{ij} . Then the values $f_1(\alpha), \dots, f_s(\alpha)$ are algebraically independent.*

Siegel [86] originally proved this theorem for the Bessel function and its derivative, and extended it to the more general case under an extra condition. Shidlovsky showed how to eliminate this condition by formulating and proving the appropriate lemma [85]. An exposition is also given in [49].

Extensions have been given by Sprindzuk [89]. It is a problem both to weaken the conditions on the coefficients of the power series, and to prove that certain functions are E -functions (e.g. Bessel functions J_λ with algebraic λ).

In the applications, it is also necessary to prove that certain functions are algebraically independent. We refer to Siegel for this [87].

The main part of Siegel's arguments is linear. It remains an open problem to see to what extent one can replace "algebraic independence" by "linear independence" throughout the statement of the Siegel-Shidlovsky theorem.

Also, the p -adic analogue of the transcendence theorem for E -functions is not known. Siegel's arguments depend on an essential way on the factorials in the denominators, and no substitutes are known at present.

DIOPHANTINE APPROXIMATIONS

6. Metrical results. Let α be a real number, and assume that α is not rational. We denote by $\|\alpha\|$ the distance of α to the closest integer. If this distance is less than $1/2$, then there is a unique integer p such that $\|\alpha\| = |\alpha - p|$. Thus the norm which we have defined is essentially the distance on the circle. More generally, one can consider vectors X in \mathbf{R}^n , and define their norm $\|X\|$ on the torus \mathbf{R}^n/L , where L is a lattice. We concentrate mostly on single numbers.

We are interested in the distribution of the numbers $q\alpha$ on the circle, i.e. on \mathbf{R}/\mathbf{Z} , when q ranges over the positive integers, and we want to give quantitative results concerning this distribution. We

look mainly at the homogeneous case, i.e. how close $\|q\alpha\|$ can come to the origin. The first observation is due to Dirichlet:

(6.1) *Let N be a positive integer. There exists an integer q , $0 < q \leq N$, such that $\|q\alpha\| < 1/N$.*

The proof is easy, so we give it. Cut up the interval $[0, 1]$ into N equal parts of length $1/N$, and consider the $N+1$ numbers $0\alpha, 1\alpha, 2\alpha, \dots, N\alpha$ modulo \mathbf{Z} . Two of them must lie in the same segment (mod \mathbf{Z}), say $r\alpha$ and $s\alpha$ with $r < s$. We let $q = s - r$, and obtain

$$\|q\alpha\| < 1/N \leq 1/q,$$

as desired.

Note that $\|q\alpha\| = |q\alpha - p|$ for $\|q\alpha\|$ sufficiently small. The inequality $\|q\alpha\| < 1/q$ can also be written in the form

$$|q\alpha - p| < 1/q \quad \text{or} \quad |\alpha - p/q| < 1/q^2.$$

Thus depending on how we write these inequalities, we get an exponent of 1 or 2 on the q of the right-hand side. The last inequality shows that we are dealing with the approximation of α by rational numbers.

In higher dimensional space, we take vectors A_1, \dots, A_r in n -space. Then the same type of argument shows that there exist integers q_i such that

$$\|q_1 A_1 + \dots + q_r A_r\| < 1/N \quad \text{and} \quad |q_i| \leq N^{n/r}.$$

Davenport and Schmidt [32] prove that such inequalities cannot be improved for almost all numbers. More generally, one considers linear forms L_1, \dots, L_m in n variables. We let

$$\delta(m, n) = (n - m)/m$$

be the "Dirichlet exponent," and we consider the simultaneous inequalities

$$|L_i(Q)| \ll 1/q^{\delta(m, n)}$$

where $Q = (q_1, \dots, q_n)$ is a vector of integers, and $q = \max |q_i|$.

We recall that a set of numbers is said to have measure 0 if given $\epsilon > 0$ the set can be covered by a countable number of intervals such that the sum of the lengths of these intervals is $< \epsilon$. Khintchine proved:

(6.2) *Let ψ be a positive function such that $\sum_{q=1}^{\infty} \psi(q)$ converges.*

Then for almost all numbers α (i.e. outside a set of measure 0), there is only a finite number of solutions to the inequality

$$\|q\alpha\| < \psi(q).$$

If ψ is decreasing, and the above sum diverges, then for almost all numbers α , there exist infinitely many solutions to the inequality $\|q\alpha\| < \psi(q)$.

The proof of the second assertion is harder and we refer to Khintchine [46] for it. The proof of the first assertion is easy and we give it. We may restrict our attention to those numbers α lying in the interval $[0, 1]$. Consider those for which the inequality has infinitely many solutions. Given ϵ select q_0 such that

$$\sum_{q \geq q_0}^{\infty} \psi(q) < \epsilon.$$

For each $q \geq q_0$ consider the intervals of radius $\psi(q)/q$ surrounding the rational numbers

$$0/q, 1/q, \dots, (q - 1)/q.$$

Every one of our α will lie in one of these intervals because for such α we have

$$|\alpha - p/q| < \psi(q)/q.$$

The measure of the union of these intervals is bounded by the sum

$$\sum_{q \geq q_0} q \frac{2\psi(q)}{q} < 2\epsilon,$$

as was to be shown.

For example we can take $\psi(q) = 1/(\log q)^{1+\epsilon}$ for any $\epsilon > 0$.

Let ψ be a decreasing function with divergent sum. For each (real) number α , let $\lambda(N)$ (λ depends on α and ψ) be the number of solutions in integers p, q of the inequalities

$$0 < q\alpha - p < \psi(q) \quad \text{and} \quad 1 \leq q < N.$$

(6.3) For almost all numbers α , we have the asymptotic relation

$$\lambda(N) \sim \int_1^N \psi(x) dx.$$

A special case of (6.3) was first stated by LeVeque [55]. The general theorem was proved by Erdős [33] and Schmidt [73]. We

note especially that Schmidt obtains important generalizations to the higher dimensional case, with certain error terms.

7. The type of a number. Results as in §6 which hold almost everywhere are said to be metrical results. They suggest a first order of magnitude for the typical behavior of numbers given as values of classical functions, suitably normalized. For instance, as expressed in [48], I would expect all such numbers to satisfy the property that

$$\|q\alpha\| > 1/q^{1+\epsilon}$$

for all but a finite number of q . However, let us call a number α of bounded type if there exists a constant $c > 0$ such that

$$\|q\alpha\| > c/q$$

for all integers $q > 0$. It can be shown that a number is of bounded type if and only if its continued fraction has bounded entries, and that the set of numbers of bounded type has measure 0. More importantly from our point of view, we have:

(7.1) *A number α is of bounded type if and only if for any positive function ψ with convergent sum $\sum \psi(q)$, the inequality*

$$\|q\alpha\| < \psi(q)$$

has only a finite number of solutions.

(For the proof, see [50]. Schanuel showed me how to prove one of the implications, namely that the convergent sum condition implies bounded type.) Consequently the metrical theorems cannot be held as models beyond this first sort of approximation, and one must look for a more subtle invariant, which will be associated with any particular number, or class of numbers, under considerations.

With this point of view, I defined the type of a number [50]. There are alternative definitions. Let f be a positive increasing function (not necessarily strictly). We say that α has type $\leq f$ if

$$\|q\alpha\| \geq 1/xf(q)$$

for all sufficiently large q . This condition implies that for all sufficiently large integers N , there exists a solution in relatively prime integers $p, q > 0$ of the inequalities

$$|q\alpha - p| < 1/q \quad \text{and} \quad N/f(N) \leq q < N,$$

and the converse is almost true, when f does not grow too fast. See [50] for details. (The proofs use continued fractions.) One can then

formulate a basic problem in diophantine approximations: Determine a type for the classical numbers.

To say that for all sufficiently large q we have

$$\|q\alpha\| \geq 1/q^{1+\epsilon}$$

amounts to saying that α has type $\leq q^\epsilon$. (Here, as always, we suppose that this holds for each $\epsilon > 0$.) However, it is more fruitful to work with the function f so that $f(q)$ appears as a factor of q , rather than with the ϵ in the exponent, because as shown in [50], the function f appears in an essential way in other estimates associated with the number. We recall two of these here.

If x is a real number, let $R(x)$ be the remainder of x modulo \mathbf{Z} , i.e. the unique number such that $0 \leq x < 1$ and such that $x - R(x)$ is an integer. Let us form the sum

$$S_N(\alpha) = \sum_{n=1}^N R(n\alpha).$$

One expects the values of $R(n\alpha)$ to be somewhat evenly distributed around $1/2$. Using the type, one then finds the following estimate:

(7.2) *Let α be of type $\leq f$ and assume that the function $f(t)/t$ is decreasing. Then*

$$S_N(\alpha) = \frac{1}{2} N + O\left(\int_1^N \frac{f(t)}{t} dt\right).$$

Relations between rational approximations to α and the sum S_N had been noted by Behnke [19] and Ostrowski [65], but the above statement (which has a very simple proof) was first given in [50]. The essential thing here is the appearance of a canonical error term as an integral involving the type. A similar integral error term appears for the function λ discussed in (6.3). If α has type $\leq f$, let us write $\psi(t) = \omega(t)/t$. Under simple conditions on the type in relation to ω , but especially that ω tends to infinity faster than the type, one finds that

$$(7.3) \quad \lambda(N) = \int_1^N \psi(t) dt + O\left(\int_1^N \frac{\omega(t)^{1/2} f(t)^{1/2}}{t} dt\right).$$

Thus if ω grows much faster than f , then the first integral dominates the second integral. In particular, if $\omega(t) = at$ with $0 < a \leq 1$, then this amounts to the usual "equidistribution" function, and we have

$$\lambda(N) = aN + O\left(\int_1^N \frac{f(t)^{1/2}}{t^{1/2}} dt\right).$$

If $f(t)/t$ tends to 0 as t becomes large, then the error term is $o(N)$. This gives a quantitative description of the equidistribution of the numbers $q\alpha$ on the circle, in terms of the type for α . For the proofs, see [50].

Because of Khintchine's convergence theorem (6.2) one sees that almost all numbers have type $(\log t)^{1+\epsilon}$ (for instance) so that the above asymptotic results apply for almost all numbers. But their formulation in terms of the type makes them applicable to specific numbers, and thus reduces the study of such asymptotic estimates to a determination of the type. However it is clear from the form of the error terms above that they are significant only for "good" types (e.g. satisfying the condition $f(t)/t \rightarrow 0$). Only for algebraic numbers or a few isolated transcendental ones is such a type known at present.

Adams [5] extended these theorems to the higher dimensional case, when the type is defined by an inequality

$$\|q_1\alpha_1 + \cdots + q_n\alpha_n\| > 1/q^n f(q)$$

and $q = \max |q_i|$. According to Schmidt [74], the measure theoretic expectancy is that $\lambda(N)$ is asymptotic to

$$\int_1^N \psi(t)^n dt$$

and Adams proves this with an integral error term generalizing (7.3). Schmidt [75] did it for the basis of a real algebraic number field.

When the function ω does not grow faster than the type f , then the above error terms break down and each number will be expected to exhibit its own peculiarities. We discuss some special types in the next two sections. Here we still mention the connection with the asymptotic function λ in the few known cases.

The Liouville inequality (see below) shows that quadratic numbers are of bounded type. In that case, I proved [50]:

(7.4) *Let α be a real quadratic number. Let c be a number such that the inequalities*

$$0 < q\alpha - p < 1/q \quad \text{and} \quad 1 \leq q \leq N$$

have infinitely many solutions. Let $\lambda(N)$ be the number of solutions. Then $\lambda(N) \sim c_1 \log N$ for some constant c_1 .

This was extended to a basis of a real algebraic number field by Adams [6].

Adams [2] also gives the value of λ for e and numbers having the same kind of continued fraction, namely Hurwitz numbers (cf. Perron [66]). His result for e is typical:

(7.5) Let $g(x)$ be the inverse function of the function $4^x\Gamma(x+3/2)$, so that $g(x)$ is asymptotic to $\log x/\log \log x$. Let $\lambda(N)$ be the number of solutions of the inequalities

$$0 < qe - p < 1/q \quad \text{and} \quad 1 \leq q \leq N.$$

Then

$$\lambda(N) = \frac{1}{6}(2g(N))^{3/2} + O(g(N)).$$

Using the same technique as Adams, looking at the continued fraction, I determined the type of e as being $\leq 2g + O(1)$. This is best possible in the sense that subtracting a sufficiently large constant is not a type. Cf. [50]. In this case, the type is such that the function

$$\psi(q) = 1/qr(q)$$

has a divergent sum. The number e is behaving better than almost all numbers from the point of view of being badly approximable by rationals.

No other sharp statements like these are known at present. For instance, a type for e^3 similar to the above is not known. Computations confirm that a power of the log should be an expected upper bound for the types of classical numbers [8]. The computations actually suggest that the types differ from the log by a factor having lower order of magnitude.

I believe that the continued fraction for e , which has a "formula"

$$[2, 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots],$$

is accidental in the sense that, say for algebraic numbers of degree > 2 , the continued fraction should be essentially random. It would lead us too far to discuss continued fractions in detail here. We just mention a couple of their properties. If α is real, irrational, we let $a_0 = [\alpha]$ be the largest integer $\leq \alpha$. Then $\alpha - a_0 = 1/\alpha_1$ and $\alpha_1 > 1$. Write $\alpha_1 = a_1 + 1/\alpha_2$ with a positive integer a_1 , and continue like this. Then $[a_0, a_1, a_2, \dots]$ is called the continued fraction for α . What matters for us is that the partial fractions

$$[a_0, a_1, \dots, a_n] = p_n/q_n$$

provide solutions of the fundamental inequality

$$|q_n\alpha - p_n| < 1/q_n,$$

and that $q_{n+1} \leq a_{n+1}q_n$. Thus the integers a_n ($n \geq 1$) in some way measure how far apart solutions of the fundamental inequality may be. The n th such solution, given by the continued fraction, has an order of magnitude equal to the product $a_1 \cdot \dots \cdot a_n$. In the case of e

and numbers like it, this is something like $n!$ (the precise function is given by (7.5)). For proofs, see [2], or [50].

8. **Algebraic numbers.** If α is algebraic of degree $n > 1$ (over \mathcal{Q}), then Liouville remarked that one has the trivial inequality

$$|\alpha - p/q| \geq c(\alpha)/q^n,$$

for some number $c(\alpha)$ which is easily computable in terms of the degree and discriminant of α . Indeed, let

$$f(X) = c \prod_{i=1}^n (X - \alpha_i)$$

be the irreducible polynomial of $\alpha = \alpha_1$ over \mathcal{Q} , taken with relatively prime integer coefficients, so that c is an integer ≥ 1 . If p/q is close to α , then p/q is at a distance from any conjugate α_i of α approximately equal to $|\alpha_i - \alpha|$. Since $f(p/q) \neq 0$, we get the inequality

$$1/q^n \leq |f(p/q)| = |c| \prod_{i=1}^n |p/q - \alpha_i|.$$

The Liouville inequality follows at once from this factorization. (For generalizations of the Liouville inequality to polynomials in several variables, cf. Feldman [35], [36], [38], and [50] where some of Feldman's results are reproduced.)

In particular, if α is quadratic, then α is of bounded type. I would conjecture that no other "natural" number has bounded type, although random continued fractions with bounded entries provide random examples of such numbers. By "natural," I mean algebraic of degree > 2 , or transcendental in the field mentioned previously, generated by values of classical functions suitably normalized. It is however unknown except in a few cases like e whether any such numbers are of bounded type. In particular, it is unknown for any algebraic number of degree > 2 , say $2^{1/3}$, and for e^3 .

Improvements on the exponent n in Liouville's theorem have proved to be very difficult to obtain. Thue and Siegel reduced this exponent significantly, in a manner depending on the degree, but Roth [72] gave the best exponent (conjectured by Siegel), namely:

(8.1) *If α is algebraic irrational, then there are only a finite number of solutions to the inequality $\|q\alpha\| < 1/q^{1+\epsilon}$.*

The first time that the correct exponent $1+\epsilon$ appeared in the literature was in Schneider's paper [81]. However, in parts of his proof, the arguments were still too weak to give the full result, and

Schneider could only prove that solutions q of the above inequality have to tend rapidly to infinity.

Following an idea of Siegel, Schneider considered a sequence of solutions p_i/q_i for the approximation

$$|\alpha - p_i/q_i| < 1/q_i^{2+\epsilon}$$

and constructed a polynomial in several variables $F(X_1, \dots, X_m)$ such that the Taylor expansion

$$\begin{aligned} F(p/q) &= F\left(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\right) \\ &= \sum F^{(j)}(\alpha, \dots, \alpha) \left(\frac{p_1}{q_1} - \alpha\right)^{j_1} \cdots \left(\frac{p_m}{q_m} - \alpha\right)^{j_m} \end{aligned}$$

starts only with a zero of high order, the order being measured by the special weights

$$\frac{j_1}{r_1} + \dots + \frac{j_m}{r_m}$$

where r_1, \dots, r_m are the degrees of F in X_1, \dots, X_m respectively. By taking m large, solving appropriate linear equations, and taking sufficiently big gaps between the fractions p_i/q_i , one sees that the value $F(p/q)$ is small from the right-hand side if the p_i/q_i approximate α very closely. On the other hand, one can show that the linear equations achieving this can be solved with integer coefficients, and a denominator for $F(p/q)$ is at most

$$q_1^{r_1} \cdots q_m^{r_m}.$$

If $F(p/q) \neq 0$, then multiplying by such a denominator one gets an integer of absolute value ≥ 1 , in other words, one gets an inequality on the left which contradicts the inequality on the right. Schneider's argument to find the polynomial F such that $F(p/q) \neq 0$ required large gaps between the fractions p_i/q_i . Roth improved this part of the proof, and showed that even if one gets a polynomial F such that $F(p/q) = 0$, then some suitable derivative of F will not vanish at p/q , thus getting his theorem. About 20 years had elapsed since Schneider's proof in 1936.

Even though the method of proof yields a bound on m (for complements on this, see Davenport and Roth [31]), it does not yield a bound on the size of the approximating fractions. Thus Roth's theorem is called "noneffective."

Contrary to statements sometimes made that Roth's theorem gives

a “best possible approximation inequality,” one can ask for a better one, namely one can ask for the determination of a type for algebraic numbers having a lower order of growth than epsilon in the exponent. As far as I know, this was first mentioned in [48], with the possibility of a type $(\log t)^{1+\epsilon}$, in line with the Khintchine convergence principle.

It is difficult to make precisely correct guesses, because within the range of the logarithm as a type, each number will exhibit its own peculiar behavior. It is conceivable that even a type $\log t$ occurs (even though the sum $\sum 1/q \log q$ diverges!). A few computations for some transcendental numbers definitely suggest such a low order of growth, fairly close to the \log [8]. The Adams result for e , and further experience confirm that it is not likely that one gets precisely the logarithm as a type, but rather various small perturbations of it, depending on each particular number.

For algebraic numbers of degree > 2 , I expect basically a random behavior for the continued fraction, or at most a small departure from the random behavior. Some tables for continued fractions of a few algebraic numbers confirm this [96]. There occur some exceptionally large values among a generally uniform random behavior. This suggests the problem of determining whether such relatively large values continue to occur throughout the continued fraction, or whether they stop. If they do not stop, then the problem is to determine how they affect an otherwise rather smooth type. The existence of some exceptionally large integers in the continued fractions of numbers related to values of the modular function had already been observed by Brillhart (cf. Churchhouse and Muir [95], and also a forthcoming paper by Stark [97]).

Another regularity lies in the frequency count of the numbers in the continued fraction. According to a theorem of Kuzmin (see [46]) for almost all numbers α , the probability that the n th number a_n in the continued fraction for α is equal to a positive integer k is given by

$$\log_2 \frac{(k+1)^2}{k(k+2)}.$$

For $k=1$ and almost all numbers, this means that the probability for $a_n=1$ is approximately .41. Among the first thousand a_n for $2^{1/3}$, $5^{1/3}$, $7^{1/3}$ (say) we find that 1 occurs respectively 422, 433, 409 times, which is rather close to the Kuzmin number.

The structure of Schneider’s argument exhibiting the exponent $2+\epsilon$ in the inequality $|\alpha - p/q| < 1/q^{2+\epsilon}$ is purely combinatorial, and as such is applicable to more general contexts (e.g. function fields

with algebraically closed constant fields). It is when dealing with algebraic numbers (or function fields over finite fields) that one can expect q^ϵ to be replaced by a function of q growing more like the log.

Recently Schmidt [76] gave a far reaching generalization of Roth's theorem, by extending it to vectors of algebraic numbers.

(8.2) *Let $1, \alpha_1, \dots, \alpha_n$ be algebraic, linearly independent over the rationals. Then the inequality*

$$\|q_1\alpha_1 + \dots + q_n\alpha_n\| < 1/q^{n+\epsilon}, \quad q = \max |q_i|,$$

has only a finite number of solutions.

A standard transference principle of Khintchine [24], [77], shows that (8.2) is equivalent with

(8.3) *If $1, \alpha_1, \dots, \alpha_n$ are linearly independent over the rationals, then the simultaneous inequalities*

$$\|q_i\alpha_i\| < \frac{1}{q_i^{n+\epsilon}}$$

have only a finite number of solutions.

Schmidt's proof uses the same techniques as Schneider and Roth, but also relies heavily on Mahler's theory of compound convex bodies [62]. For more details, I refer the reader to Schmidt [76], [77]. He also proves theorems concerning the approximation of algebraic numbers by other algebraic numbers. If P is a polynomial with integer coefficients, we let $H = H(P)$ be the height of P , namely the maximum of the absolute values of its coefficients. If β is algebraic and P is the irreducible polynomial for β with relatively prime integer coefficients, we let $H(\beta)$ be the height of β . Schmidt proves:

(8.4) *Let α be algebraic and let n be a positive integer. There are only finitely many algebraic numbers β of degree $\leq n$ such that*

$$|\alpha - \beta| < \frac{1}{H(\beta)^{n+1+\epsilon}}.$$

This generalizes results of Wirsing [93], who had the weaker exponent $2n + \epsilon$. Schmidt's exponent is best possible. It is easily seen that (8.4) follows from (8.2). Schmidt's results, coming 15 years after Roth's theorem, again constitute an impressive advance in the subject.

Schmidt's theorem (8.4) has substance only if n is smaller than the

degree d of α . Indeed, one has superficially at the level of a Liouville estimate the better result:

(8.5) *Let α be algebraic of degree d . Then there are only finitely many algebraic numbers β such that*

$$|\alpha - \beta| < \frac{1}{H(\beta)^{d+\epsilon}}.$$

A result of Wirsing gives the possibility of using the inequality (8.5), or even weaker ones, as a criterion for algebraicity or transcendence. Indeed, Wirsing proves [94]:

(8.6) *If w is a real transcendental number, then the inequality*

$$|w - \beta| < \frac{1}{H(\beta)^{(n+1)/2+1-\epsilon}}$$

has infinitely many solutions in algebraic numbers β of degree $\leq n$.

The essential thing here is that the exponent depending on n may be arbitrarily large, whereas for algebraic numbers, it is bounded as in (8.5). This result of Wirsing relates to the classification of numbers by Mahler and Koksma [47] (see also Schneider [80]), considering the lower bound for a polynomial $|P(w)|$.

Roth's theorem has p -adic analogues [71]. It can also be axiomatized to cover cases in algebraic geometry, and a finite number of absolute values, satisfying the product formula [52], e.g. in the function field case. However, when the constant field is, say, algebraically closed, one does not expect the type q^ϵ to be improvable. Only when the constant field is finite would I expect again an improvement in the type, to a power of the log (assuming that the irrationality α has only tame ramification).

The first improvement on the Liouville inequality which was effective is due to Baker [14], [15]. By using the same method as that for linear combinations of logarithms (2.3) he proves:

(8.7) *Let α be algebraic of degree $n \geq 3$ and let $k > n + 1$. Then there is a computable constant $c = c(\alpha, k)$ such that*

$$\|q\alpha\| > c \frac{e^{(\log q)^{1/k}}}{q^n}$$

(This is improved to $k > 1$ in the joint paper with Stark [18].) Thus the effective result is still quite far from having the best exponent on q . In fact, it does not yet yield the possibility of lowering the exponent n

in the denominator by ϵ . However, it is significant because it allows us to give effective bounds for solutions of a wide class of diophantine equations.

Note that Coates gives p -adic extensions to Baker's results [27], also announced by Feldman [40].

9. Some transcendence measures. Given classical numbers x_1, \dots, x_n one is interested in a lower bound for linear combinations

$$|q_0 + q_1x_1 + \dots + q_nx_n| > F(q), \quad q = \max |q_i|,$$

with sufficiently large q . Such a function F is called a measure of linear independence for the numbers x_1, \dots, x_n . Historically, there have been three levels of difficulty in determining the function F , namely:

Stage 1. When $F(q) = 1/q^{\phi(q)}$, and ϕ is increasing to infinity.

Stage 2. When $F(q) = 1/q^c$ for some fixed number c .

Stage 3. When $F(q) = 1/q^{n+\epsilon}$, the best possible expected exponent of q , in view of Dirichlet's theorem.

Ultimately, one wants the even better results involving the type, namely $1/q^{nf(q)}$, where f grows like the log, or a power of the log. No such results are known at present except those mentioned in §7. We could call this *Stage 4*. This is the point of view taken in [50].

In dealing with one number x which is transcendental, one considers the numbers $x_i = x^i$, so that the linear combination above can be written as a polynomial in x of degree n , namely

$$|q_0 + q_1x + \dots + q_nx^n| > F(q).$$

The function F is then called a measure of transcendence for x . We shall summarize some of the known results, which should be regarded as very tentative.

Even though the sharpest type for e became known only in 1966, it had been known long before that e is of type $\leq q^e$, in other words $\|qe\| < 1/q^{1+\epsilon}$ has only a finite number of solutions. In fact, Popken had proved [67]:

(9.1) *Let $P(X)$ be a polynomial of degree n with integer coefficients, and let $H = H(P)$ be the maximum of the absolute value of the coefficients. Then there is a number c depending only on n such that*

$$|P(e)| > \frac{1}{H^{n+c/\log \log H}}.$$

In particular,

$$\|qe\| > \frac{1}{q^{1+c/\log \log q}}.$$

For the proof and explicit dependence of c on n , due to Mahler, cf. Schneider's book [80]. In [48], I had already verified that the same argument also works for e^a , where a is rational. In this connection, Mahler [63] uses some of the original formulas by Hermite to get similar approximation estimates to exponential and logarithms of rational numbers. Even though these formulas have disappeared from the picture for transcendence proofs, it seems that they still contain germs of methods which would be useful for measures of approximation, more closely related to continued fractions.

When α is irrational algebraic, and one wants to study e^α from the present point of view, one meets difficulties analogous to those of Roth's theorem.

Siegel had a Roth type theorem for values of the Bessel function J_0 , namely the inequality

$$\|q_1 J_0(\alpha) + q_2 J_0'(\alpha)\| < 1/q^{2+\epsilon}$$

has only a finite number of solutions whenever α is rational $\neq 0$, and similarly for a polynomial in $J_0(\alpha)$, $J_0'(\alpha)$ [86]. Here again, the problem is open for algebraic α , or when one deals with J_λ and λ is algebraic irrational. (Actually in this case it is unknown if J_λ is an E -function.) Once Shidlovsky had proved his transcendence result, it was easy to extend Siegel's estimates to arbitrary E -functions (see e.g. [49]).

It is unknown if a single value of the Bessel function $J_0(a)$, with a rational, is of type $\leq q^\epsilon$.

Popken also had the statement analogous to (9.1) for approximations with algebraic numbers, namely:

(9.2) *For all algebraic α of degree n and height $H \geq 3$, one has*

$$|e - \alpha| > 1/H^{n+1+c/\log \log H},$$

where c depends only on n .

Lower bounds which are somewhat worse for numbers α^β with α algebraic, β algebraic have been obtained by Gelfond and Feldman. Cf. Gelfond [44], Schneider [80], also for further reference to the literature. The Gelfond result does not show that α^β has type $\leq q^\epsilon$. It is weaker, roughly like

$$q^{(\log \log q)^\tau},$$

where τ is a low number like 5. The situation has been going through various improvements, so one must check the latest bulletins to know how much the 5 is reduced. From our point of view here, what matters is that the exponent of q is not even a fixed number, independent of q . The situation here is still in Stage 1.

For logarithms of algebraic numbers, the situation is slightly better. Mahler [58] had proved that for α algebraic,

$$\|q \log \alpha\| > 1/q^c$$

with some fixed number c , depending only on α . Feldman, following results of Gelfond, improved these results, and also obtained similar results for approximation by algebraic numbers [59], [60], [80]. For π , Mahler [60] had shown that for all positive q we have

$$\|q\pi\| > 1/q^{42}.$$

(The exponent 42 can be reduced if one allows a constant factor on the right.) None of these results has any semblance of finality.

The result of Baker, whose proof we sketched in §2, represented the first effective lower bound for linear forms in logarithms of several algebraic numbers. Current research is somewhere between Stage one and two. For instance, Feldman has reached Stage two for linear combinations of n logarithms of algebraic numbers, with $F(q) = q^{-c}$, where c depends on n and the logarithms [40].

Baker has also proved analogous results in Stage one for elliptic functions, and periods of elliptic functions [12], [13]. Through Baker's ideas, the whole theory is now in a considerable state of flux, with continuous extensions of Baker's method by Baker and Feldman [18], [41]. Here again one can formulate general conjectures for generalized logarithms on algebraic groups, especially toruses [51]. We shall mention these in connection with the applications to diophantine analysis.

Finally we mention that Baker type results can be used to give an upper bound for the discriminant of an imaginary quadratic field of class number 1 and 2 (again, consult the latest bulletins for improvements on this). It would take us here too far afield to give more details, and we refer the reader to the latest papers of Baker and Stark [18], [16], [91].

The Riemann Hypothesis would give a very good and very effective lower bound for the class number in terms of the discriminant via the Brauer-Siegel theorem. It is not clear (to me) from the present

proofs of Baker and Stark if very good results in estimates for linear forms of logarithms of algebraic numbers would give as good a bound as the Riemann Hypothesis. It is also not clear to me if such results might in fact prove the absence of zeros of the zeta function of (quadratic) fields near 1.

10. A criterion of Gelfond. Gelfond gave a useful criterion to prove that two numbers are algebraically independent, namely:

- (10.1) *Let x be a complex number. Let σ be a strictly monotone increasing real function tending to infinity, and assume that there is a number $a_0 > 1$ such that $\sigma(N+1) < a_0\sigma(N)$ for all integers $N > N_0$. Assume that for each integer $N > N_0$ there exists a nonzero polynomial F_N with integer coefficients, such that*

$$|F_N(x)| < e^{-C\sigma(N)},$$

where $C = 50a_0^2$, and

$$\max(\deg F_N, \log |F_N|) \leq \sigma(N).$$

Then x is algebraic.

(*Notation.* $|F_N|$ is the height of F_N .) In his book [44], he proved only a weaker version. I gave a proof in [48]. Waldschmidt has extended this theorem and proved interesting new applications by separating σ into two functions, describing independently how the degree and the height of the polynomials F_N grow [92].

It should be noted that the conjecture expressed at the end of [48], attempting to give a generalization to a criterion of algebraic independence for several numbers, is not valid. The expected exponent for polynomials F_N in several variables would be σ^{n+1} . However, Bombieri pointed out to me that Cassels [24] proves the existence of numbers whose linear combinations tend to 0 very rapidly. Indeed, by Theorem XIV of Chapter V, loc. cit, for every function $\psi(t)$, decreasing to 0, there exist numbers α_1, α_2 having the following property. For large positive integers q , there exist q_1, q_2 with $|q_i| < q$ such that

$$0 < \|q_1\alpha_1 + q_2\alpha_2\| < \psi(q).$$

Thus the polynomials F_q have degree 1. This is a phenomenon which appears only when $n \geq 2$. It is a problem to formulate those supplementary hypotheses which must be added to generalize the Gelfond criterion to several variables.

11. Applications to diophantine analysis. The Baker theorem (8.4) still corresponds to Stage 1 in the approximation theory. However, its effective improvement on the Liouville estimate allows affective bounds for the solutions in integers of a wide class of diophantine equations. For instance, let

$$F(X, Y) = a_n X^n + a_{n-1} X^{n-1} Y + \dots + a_0 Y^n$$

be a binary form of degree ≥ 3 with integer coefficients. Let m be a positive integer. Any improvement of the Liouville inequality immediately shows that the equation

$$F(X, Y) = m$$

has only a finite number of solutions. Namely, we factor F into factors of degree 1, which are of the form $(X - \alpha^{(i)} Y)$ where the $\alpha^{(i)}$ are conjugates of an algebraic number α (if F is irreducible), otherwise split into families of conjugates. If p, q are integers such that $F(p, q) = m$, then it follows immediately from any improvement of Liouville's inequality that the number of such p, q is finite. With his effective improvement, Baker is led to an estimate [14]:

$$\log \max(|p|, |q|) < (nH)^{(10n)^5} + (\log m)^{2n+2},$$

where H is the height of F .

Using his theorem on diophantine approximations, Siegel [86] has shown:

(11.1) *If a curve of genus ≥ 1 is defined by an equation $f(X, Y) = 0$ with an irreducible polynomial f having algebraic coefficients, then this curve has only a finite number of points (x, y) with x, y lying in the ring of algebraic integers of a number field.*

Mahler extended this by using p -adic analogues of the Thue-Siegel theorem, and in fact the result holds for arbitrary finitely generated rings (without divisors of 0) over the integers \mathbf{Z} . Cf. [52]. Siegel's argument is based on a geometric version of the diophantine approximation inequality. If $P = (\alpha_0, \dots, \alpha_n)$ is a point in projective space, represented with projective coordinates, one can define its height. For instance, if the α_i are relatively prime integers, then the height $H(P)$ is the maximum of the absolute values $|\alpha_i|$. The definition in number fields is similar. The inequality of Roth's theorem

$$|\alpha - p/q| < 1/q^{2+\epsilon}$$

then has a geometric analogue as follows.

(11.2) *Let V be a curve defined over a number field K . Let ϕ be a non-constant rational function in $K(V)$. Let r be the maximum of the orders of zeros of ϕ . Then there are only finitely many rational points P of V in K satisfying the inequality*

$$|\phi(P)| < 1/H(P)^{2r+\epsilon}.$$

This is easily reduced to Roth's theorem. For instance, if V is a rational curve, with function field $K(x)$, then a rational function $R(x)$ has a factorization

$$R(x) = \prod (x - \alpha_i)^{r_i}$$

where the r_i are the multiplicities of the zeros and poles, and the α_i are algebraic numbers. Say $K = \mathbf{Q}$. A rational point is a fraction p/q , and $R(p/q)$ is small if and only if p/q approximates one of the roots of $R(x)$. In that case, such a fraction stays away from the other roots, and the equivalence between (11.2) and Roth's theorem is obvious. When V is not a rational curve, one reduces the proof of (11.2) to the case of a rational curve by projecting. Cf. [52].

Siegel [86] had an analogous theorem to (11.2), but corresponding to the weaker approximation result which he had available at that time.

In dealing with an integral point P , or say a point P such that $\phi(P)$ is an integer, one gets trivially an inequality like (11.2), except that the exponent of $H(P)$ on the right is much larger than the desired $2r+\epsilon$. For curves of genus 1, using the group law arising from the theory of elliptic functions, one can then reduce the exponent to an arbitrarily small one, whence the result. For curves of higher genus, Siegel [86] used abelian functions, and the analytic representation of the Jacobian variety of the curve. The arguments can be algebraicized, and in fact one can express the idea geometrically by saying that to reduce the exponent so as to apply (11.2) one must go to a covering of the given curve, by restricting to the curve the unramified covering of the Jacobian, obtained by division of the periods, i.e. the mapping

$$a \mapsto na$$

on the Jacobian, for a large integer n . Cf. [52].

These arguments are not effective in two ways: first in the non-effectiveness of the Roth theorem, and second in the use of the Mordell-Weil theorem when jacking up the diophantine approximation to unramified coverings of the curve.

For curves of genus 1, Baker and Coates [17] gave a different argument. Using the Riemann-Roch theorem, they reduce the study

of integral points on a curve of genus 1 to that of a curve in standard form, $Y^2=f(X)$, which can then be handled by a reduction to Baker's theorem (2.3), whence they get an effective upper bound for its integral points. So far, this method has no analogue to curves of higher genus, or abelian varieties, but it is worth emphasizing that the Coates-Baker argument represents a new approach to the finiteness problems we have been discussing.

By considering generalized logarithms on an elliptic curve, and using the idea that they should behave from the point of view of diophantine approximations so as to be of type $\leq q^e$, I conjectured that (11.2) should generalize as follows [51]:

(11.3) *Let A be an elliptic curve defined over a number field K . Let ϕ be a nonconstant function in $K(A)$. Let r be the maximum multiplicity of its zeros, and let m be the rank of the group of rational points A_K of A in K . Then there should be only a finite number of points P in A_K satisfying the inequality*

$$|\phi(P)| \leq 1/h(P)^{r(m+1)/2+\epsilon}$$

where $h(P) = \log H(P)$ is the logarithmic height.

Observe here that we are dealing with a lower order of magnitude on the right-hand side than in (11.2). Of course, a similar conjecture can be made in terms of a type for the logarithms of algebraic points, replace the $h(P)^\epsilon$ which corresponds to q^e . The inequality of (11.3) is equivalent to an inequality involving logs of algebraic points. Indeed, let P_1, \dots, P_m be free generators of A_K modulo the torsion group. Let $u_j = \log P_j$. Let ω_1, ω_2 be fundamental periods. Let

$$P = q_1 P_1 + \dots + q_m P_m + Q$$

where Q is in the torsion group. Since this torsion group is finite, we may assume that when we consider infinitely many P , the same Q appears. Such points P have a point of accumulation P_0 . We let $u_0 = \log(P_0 - Q)$. Then the inequality of (11.3) amounts to

$$|-u_0 + q_1 u_1 + \dots + q_m u_m + q_{m+1} \omega_1 + q_{m+2} \omega_2| \leq 1/q^{m+1+\epsilon},$$

which has the standard recognizable form. The same remark applies of course to ordinary logarithms.

BIBLIOGRAPHY

1. W. W. ADAMS, *Asymptotic Diophantine approximations to e* , Proc. Nat. Acad. Sci. U.S.A. **55** (1966), 28-31. MR **32** #4085.
2. ———, *Asymptotic Diophantine approximations and Hurwitz numbers*, Amer. J. Math. **89** (1967), 1083-1108. MR **36** #5082.

3. ———, *Simultaneous asymptotic Diophantine approximations to a basis of a real cubic number field*, J. Number Theory **1** (1969), 179–194. MR **39** #1409.
4. ———, *A lower bound in asymptotic Diophantine approximations*, Duke Math. J. **35** (1968), 21–35. MR **36** #5083.
5. ———, *Simultaneous asymptotic Diophantine approximations*, Mathematika **14** (1967), 173–180. MR **36** #3730.
6. ———, *Simultaneous asymptotic Diophantine approximation to a basis of a real number field*, Nagoya Math. J. (to appear).
7. ———, *Transcendental numbers in the P -adic domain*, Amer. J. Math. **88** (1966), 279–308. MR **33** #5564.
8. W. ADAMS AND S. LANG, *Some computations in Diophantine approximations*, J. Reine Angew. Math. **220** (1965), 163–173. MR **32** #91.
9. L. ALAOGU AND P. ERDÖS, *On highly composite and similar numbers*, Trans. Amer. Math. Soc. **56** (1944), 448–469. MR **6**, 117.
10. J. AX, *On Schannuel's conjecture*, Ann. of Math. (2) **93** (1971), 252–268 (and another paper to appear).
11. A. BAKER, *Linear forms in the logarithms of algebraic numbers*. I, II, III, Mathematika **13** (1966), 204–216; *ibid.* **14** (1967), 102–107, 220–228. MR **36** #3732.
12. ———, *An estimate for the \mathcal{O} -function at an algebraic point*, Amer. J. Math. (to appear).
13. ———, *On the quasi-periods of the Weierstrass zeta function*, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II **1969**, 145–157.
14. ———, *Contributions to the theory of Diophantine equations*. I. *On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London Ser. A **263** (1967/68), 173–191; II. *The Diophantine equation $Y^2 = X^3 + k$* , *ibid.*, 193–208. MR **37** #4005; #4006.
15. ———, *The Diophantine equation $Y^2 = ax^3 + bx^2 + cx + d$* , J. London Math. Soc. **43** (1968), 1–9. MR **38** #111.
16. ———, *Imaginary quadratic fields with class number 2*, Ann. of Math. (to appear).
17. A. BAKER AND J. COATES, *Integer points on curves of genus 1*, Proc. Cambridge Philos. Soc. **67** (1970), 595–602. MR **41** #1638.
18. A. BAKER AND H. STARK, *On a fundamental inequality in number theory*, Ann. of Math. (to appear).
19. H. BEHNKE, *Über die Verteilung von Irrationalitäten mod 1*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 252–267.
20. ———, *Zur Theorie der diophantischen Approximationen*, Abh. Math. Sem. Univ. Hamburg **3** (1924), 261–318.
21. E. BOMBIERI, *Algebraic values of meromorphic maps*, Invent. Math. **10** (1970), 267–287.
22. E. BOMBIERI AND S. LANG, *Analytic subgroups of group varieties*, Invent. Math. **11** (1970), 1–14.
23. A. BRUMER, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124. MR **36** #3746.
24. J. W. S. CASSELS, *An introduction to Diophantine approximation*, Cambridge Tracts in Math. and Math. Phys., no. 45, Cambridge Univ. Press, New York, 1957. MR **19**, 396.
25. J. COATES, *An effective p -adic analogue of a theorem of Thue*, Acta Arith. **15** (1968/69), 279–305. MR **39** #4095.
26. ———, *Construction of rational functions on a curve*, Proc. Cambridge Philos. Soc. **68** (1970), 105–123.
27. ———, *An effective p -adic analogue of a theorem of Thue*. II. *The greatest prime factor*

- of a binary form, *Acta Arith.* **17** (1970), 399–412; *The Diophantine equation $Y^2 = X^3 + k$* , *ibid.*, 425–435.
28. ———, *The transcendence of linear forms in $\omega_1, \omega_2, \eta_1, \eta_2, 2\pi i$* (to appear).
29. A. BAKER AND J. COATES, *Integer points on curves of genus 1*, *Proc. Cambridge Philos. Soc.* **67** (1970), 595–602. MR **41** #1638.
30. R. M. DAMERELL, *L-functions of elliptic curves with multiplication*. I, *Acta Arith.* **17** (1970), 287–301.
31. H. DAVENPORT AND K. ROTH, *Rational approximations to algebraic numbers*, *Mathematika* **2** (1955), 160–167. MR **17**, 1060.
32. H. DAVENPORT AND W. SCHMIDT, *Dirichlet's theorem on Diophantine approximations*. II, *Acta Arith.* **17** (1970), 413–424.
33. P. ERDÖS, *Some results on Diophantine approximation*, *Acta Arith.* **5** (1959), 359–369. MR **22** #12091.
34. N. I. FELDMAN, *Approximation of certain transcendental numbers*. I: *The approximation of logarithms of algebraic numbers*; II: *The approximation of certain numbers associated with the Weierstrass function*, *Izv. Akad. Nauk SSSR Ser. Mat.* **15** (1951), 53–74, 153–176; English transl., *Amer. Math. Soc. Transl.* (2) **59** (1966), 224–270. MR **12**, 595; MR **13**, 117.
35. ———, *Simultaneous approximation of the periods of an elliptic function by algebraic numbers*, *Izv. Akad. Nauk SSSR Ser. Mat.* **22** (1958), 563–576; English transl., *Amer. Math. Soc. Transl.* (2) **59** (1966), 271–284. MR **20** #5895.
36. ———, *Approximation of the logarithms of algebraic numbers by algebraic numbers*, *Izv. Akad. Nauk SSSR Ser. Mat.* **24** (1960), 475–492; English transl., *Amer. Math. Soc. Transl.* (2) **58** (1966), 125–142. MR **22** #5623b.
37. ———, *On the measure of transcendence of π* , *Izv. Akad. Nauk SSSR Ser. Mat.* **24** (1960), 357–368; English transl., *Amer. Math. Soc. Transl.* (2) **58** (1966), 110–124. MR **22** #5632a.
38. ———, *Arithmetic properties of the solutions of a transcendental equation*, *Vestnik Moskov. Univ. Ser. I Mat. Meh.* **1964**, no. 1, 13–20; English transl., *Amer. Math. Soc. Transl.* (2) **66** (1968), 145–153. MR **28** #2091.
39. ———, *Estimate for a linear form of logarithms of algebraic numbers*, *Mat. Sb.* **76** (118) (1968), 304–319 = *Math. USSR Sb.* **5** (1968), 291–307. MR **37** #4025.
40. ———, *Improved estimate for a linear form of the logarithms of algebraic numbers*, *Mat. Sb.* **77** (119) (1968), 423–436 = *Math. USSR Sb.* **6** (1968), 398–406. MR **38** #1059.
41. ———, *A certain inequality for a linear form in the logarithms of algebraic numbers*, *Mat. Zametki* **5** (1969), 681–689. (Russian) MR **40** #2610.
42. A. O. GELFOND AND N. I. FELDMAN, *On the measure of relative transcendentality of certain numbers*, *Izv. Akad. Nauk SSSR Ser. Mat.* **14** (1950), 493–500. (Russian) MR **12**, 679.
43. A. O. GELFOND, *Sur les propriétés arithmétiques des fonctions entières*, *Tôhoku Math. J.* **30** (1929), 280–285.
44. ———, *Transcendental and algebraic numbers*, GITTL, Moscow, 1952; English transl., Dover, New York, 1960. MR **15**, 292; MR **22** #2598.
45. C. HERMITE, “Sur la fonction exponentielle,” in *Oeuvres*, Vol. III, pp. 150–181.
46. A. YA. KHINCHIN (A. JA. HINČIN), *Continued fractions*, Fizmatgiz, Moscow, 1961; English transl., Univ. of Chicago Press, Chicago, Ill., 1964. MR **28** #5037.
47. J. F. KOKSMA, *Über die Mahlersche Klasseneinteilung der transzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen*, *Monatsh. Math. Phys.* **48** (1939), 176–189. MR **1**, 137.

48. S. LANG, *Report on Diophantine approximations*, Bull. Soc. Math. France **93** (1965), 177–192. MR **33** #1286.
49. ———, *Introduction to transcendental numbers*, Addison-Wesley, Reading, Mass., 1966. MR **35** #5397.
50. ———, *Introduction to Diophantine approximations*, Addison-Wesley, Reading, Mass., 1966. MR **35** #129.
51. ———, *Diophantine approximations on toruses*, Amer. J. Math. **86** (1964), 521–533. MR **29** #2220.
52. ———, *Diophantine geometry*, Interscience Tracts in Pure and Appl. Math., no. 11, Interscience, New York, 1962. MR **26** #119.
53. ———, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
54. H. W. LEOPOLDT, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209** (1962), 54–71. MR **25** #3034.
55. W. J. LEVEQUE, *On the frequency of small fractional parts in certain real sequences*. II, Trans. Amer. Math. Soc. **94** (1960), 130–149. MR **22** #12089.
56. F. LINDEMANN, *Über die Zahl π* , Math. Ann. **20** (1882), 213–225.
57. K. MAHLER, *Über transzendente p -adische Zahlen*, Compositio Math. **2** (1935), 259–275.
58. ———, *Zur Approximation der Exponentialfunktion und des Logarithmus*, J. Reine Angew. Math. **66** (1932), 118–150.
59. ———, *On the approximation of logarithms of algebraic numbers*, Philos. Trans. Roy. Soc. London Ser. A **245** (1953), 371–398. MR **14**, 624.
60. ———, *On the approximation of π* , Nederl. Akad. Wetensch. Proc. Ser. A. **56** = Indag. Math. **15** (1953), 30–42. MR **14**, 957.
61. ———, *Ein Übertragungsprinzip für konvexe Körper*, Casopis Pěst. Mat. Fys. **68** (1939), 93–102. MR **1**, 202.
62. ———, *On compound convex bodies*. I, Proc. London Math. Soc. (3) **5** (1955), 358–379. MR **17**, 589.
63. ———, *Applications of some formulae by Hermite to the approximation of exponentials and logarithms*, Math. Ann. **168** (1967), 200–227. MR **34** #5754.
64. A. NÉRON, *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Ann. of Math. (2) **82** (1965), 249–331. MR **31** #3424.
65. A. OSTROWSKI, *Bemerkungen zur Theorie der Diophantischen Approximationen*, Abh. Math. Sem. Univ. Hamburg **1** (1921), 77–98.
66. O. PERRON, *Die Lehre von den Kettenbrüchen*, 2nd ed., Chelsea, New York, 1950. MR **12**, 254.
67. J. POPKEN, *Sur la nature arithmétique du nombre e* , C. R. Acad. Sci. Paris **186** (1928), 1505–1507.
68. ———, *Zur Transzendenz von e* , Math. Z. **29** (1929), 525–541.
69. ———, *Zur Transzendenz von π* , Math. Z. **29** (1929), 542–448.
70. K. RAMACHANDRA, *Some applications of Kronecker's limit formulas*, Ann. of Math. (2) **80** (1964), 104–148. MR **29** #2241.
71. D. RIDOUT, *Rational approximations to algebraic numbers*, Mathematika **4** (1957), 125–131. MR **20** #32.
72. K. ROTH, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20; corrigendum, 168. MR **17**, 242.
73. W. SCHMIDT, *A metrical theorem in Diophantine approximation*, Canad. J. Math. **12** (1960), 619–631. MR **22** #9482.
74. ———, *Metrical theorems on fractional parts of sequences*, Trans. Amer. Math. Soc. **110** (1964), 493–518. MR **28** #3018.

75. ———, *Simultaneous approximation to a basis of a real numberfield*, Amer. J. Math. **88** (1966), 517–527. MR **34** #2529.
76. ———, *Simultaneous approximation to algebraic numbers by rationals*, Acta Math. **21** (1970), 189–201.
77. ———, *Lectures on Diophantine approximation*, University of Colorado, Boulder, Colo., 1970.
78. T. SCHNEIDER, *Zur Theorie der Abelschen Funktionen und Integrale*, J. Reine Angew. Math. **183** (1941), 110–128. MR **3**, 266.
79. ———, *Ein Satz über ganzwertige Funktionen als Prinzip für Transzendenzbeweise*, Math. Ann. **121** (1949), 131–140. MR **11**, 160.
80. ———, *Einführung in die transzendenten Zahlen*, Springer-Verlag, Berlin, 1957. MR **19**, 252.
81. ———, *Über die Approximation algebraischer Zahlen*, J. Reine Angew. Math **175** (1936), 182–192.
82. J.-P. SERRE, *Abelian l -adic representations*, Benjamin, New York, 1968.
83. ———, “Dependence d’exponentielle p -adiques,” in *Séminaire Delange-Pisot-Poitou*, 1965/66, Exposé 15, Secrétariat mathématique, Paris, 1967. MR **35** #6507.
84. A. BOREL, ET AL., *Seminar on complex multiplication*, Lecture Notes in Math., no. 21, Springer-Verlag, Berlin and New York, 1966. MR **34** #1278.
85. A. B. ŠIDLOVSKĀ, *On criteria for algebraic independence of values of a class of integral functions*, Izv. Akad. Nauk SSSR Ser. Mat. **23** (1959), 35–66; English transl., Amer. Math. Soc. Transl. (2) **22** (1962), 339–370. MR **21** #1295.
86. C. L. SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. **1929**, 1–41.
87. ———, *Transcendental numbers*, Ann. of Math. Studies, no. 16, Princeton Univ. Press, Princeton, N. J., 1949. MR **11**, 330.
88. ———, *Bestimmung der elliptischen Modulfunktion durch eine Transformationsgleichung*, Abh. Math. Sem. Univ. Hamburg **27** (1964/65), 32–38. MR **29** #2391.
89. V. G. SPRINDŽUK, *The irrationality of the values of certain transcendental functions*, Izv. Akad. SSSR Ser. Mat. **32** (1968), 93–107 = Math. USSR Izv. **2** (1968), 89–104. MR **36** #5087.
90. H. STARK, *A historical note on complex quadratic fields with class-number one*, Proc. Amer. Math. Soc. **21** (1969), 254–255. MR **38** #5743.
91. ———, *A transcendence theorem for class number problems*, Ann. of Math. (to appear).
92. M. WALDSCHMIDT, *Independence algébrique des valeurs de la fonction exponentielle*, Bull. Soc. Math. France (to appear).
93. E. WIRSING, *On approximations of algebraic numbers by algebraic numbers of bounded degree*, Proc. Sympos. Pure Math., vol. 20, Amer. Math. Soc., Providence, R. I., 1971, pp. 213–247.
94. ———, *Approximation mit algebraischen Zahlen beschränkter Grades*, J. Reine Angew. Math. **206** (1960), 67–77, MR **26** #79.
95. CHURCHOUSE AND MUIR, *Continued fractions, algebraic numbers and modular invariants*, J. Inst. Math. Appl. (1969), 318–328.
96. S. LANG AND H. TROTTER, *Continued fractions of some algebraic numbers*, J. Reine Angew. Math. (to appear).
97. H. STARK, *An explanation of some exotic continued fractions found by Brillhart* (to appear).