On Some Applications of Diophantine Approximations

(a translation of Carl Ludwig Siegel's *Über einige Anwendungen diophantischer Approximationen* by Clemens Fuchs)

edited by
Umberto Zannier

with a commentary and the article *Integral points on curves: Siegel's theorem after Siegel's proof* by Clemens Fuchs and Umberto Zannier

EDIZIONI
DELLA
NORMALE

2

QUADERNI

MONOGRAPHS

Umberto Zannier
Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa, Italia

Clemens Fuchs
University of Salzburg
Department of Mathematics
Hellbrunnerstr. 34/I
5020 Salzburg, Austria

On Some Applications of Diophantine Approximations

On Some Applications of Diophantine Approximations

(a translation of Carl Ludwig Siegel's *Über einige Anwendungen diophantischer Approximationen* by Clemens Fuchs)

edited by
Umberto Zannier

with a commentary and the article *Integral points on curves: Siegel's theorem after Siegel's proof* by Clemens Fuchs and Umberto Zannier

EDIZIONI
DELLA
NORMALE

ISBN 978-88-7642-519-6
ISBN 978-88-7642-520-2 (eBook)

Contents

Preface

In 1929 Carl Ludwig Siegel published the paper *Über einige Anwendungen diophantischer Approximationen* (appeared in Abh. Preuß. Akad. Wissen. Phys.-math. Klasse, 1929 and reproduced in Siegel's collected papers Ges. Abh. Bd. I, Springer-Verlag 1966, 209-266). It was devoted to Diophantine Approximation and applications of it, and became a landmark work, also concerning a number of related subjects. Siegel's paper was written in German and this volume is devoted to a translation of it into English (including also the original version in German).

Siegel's paper introduced simultaneously many new methods and ideas. To comment on this in some detail would occupy a further paper (or several papers), and here we just limit ourselves to a brief discussion. The paper is, roughly, divided into two parts:

(a) The first part was devoted to proving transcendence of numbers obtained as values (at algebraic points) of certain special functions (including hypergeometric functions and Bessel functions). In this realm, Siegel's paper systematically developed ideas introduced originally by Hermite in dealing with the exponential function; a main point is to approximate with rational functions a function expressed by a power series, and to draw by specialisation numerical approximations to its values. These numerical approximations, if accurate enough, allow, through standard comparison estimates, to prove the irrationality (or transcendence) of the values of the function in question.

Siegel exploited and extended this principle in great depth, obtaining results which were (and are) spectacularly general in the topic, especially at that time.

Probably this was the first paper giving to transcendence theory some coherence.

This study also introduced related concepts, like the one of 'E-function' and of 'G-function' (*cf.* [1,8]), and led naturally to algebraical and arithmetical studies on systems of linear differential equations (with polynomial coefficients), which eventually inspired several different directions of research, all important and deep.

(b) The second part was devoted to diophantine equations, more precisely to the study of integral points o algebraic curves. In this realm too, the paper

introduced several further new ideas, also with respect to previous important papers of Siegel.[1] Some instances for the new ideas contained in the second part are:

- The paper used the embedding of a curve (of positive genus) into its Jacobian, and the finite generation of the rational points in this last variety (which had been proved by L. J. Mordell for elliptic curves and by A. Weil in general); this provided a basic instance of the intimate connection of diophantine analysis with algebraic geometry and complex analysis, which became unavoidable since that time.
- It used and developed the concept of 'height' of algebraic points and its properties related to rational transformations, especially on algebraic curves; this went sometimes beyond results by A. Weil, who had introduced the concept and had also pointed out transformation properties.
  Again, this represented one of the very first examples of how the link between arithmetic and geometry can be used most efficiently, leading to profound results.
- It exploited to a new extent the diophantine approximation to algebraic numbers. This had been used by A. Thue around 1909 in the context of the special curves defined by the so-called 'Thue equations'. For general curves, the diophantine approximation drawn from integer solutions is not sharp enough to provide directly the sought information, hence Siegel had to go much deeper into this. By taking covers of the curve (inside its Jacobian) he improved the Diophantine approximation; then he was able to conclude through a suitable refinement of Thue's theorem, also proved in the paper. This refinement was not as strong as K.F. Roth's theorem (proved only in 1955), creating further complications to the proof; Siegel had to use simultaneous approximations to several numbers to get a sharp enough estimate. (For this task, Siegel used ideas introduced in the first part of the paper.)

On combining all of this, Siegel produced his theorem on integral points on curves, which may be seen as a final result in this direction. At that time, this was especially impressive, since Diophantine equations were often treated by *ad hoc* methods, with little possibility of embracing whole families. (One of the few exceptions occurred with Thue's methods, alluded to above.)

The theorem also bears a marked geometrical content: *an affine curve may have infinitely many integral points only if it has non-negative Euler characteristic*. (This is defined as $2 - 2g - s$ where g is the genus of a smooth projective model of the curve and where s is the number of points at infinity, namely those

[1] For instance, Siegel had written (chronologically) right before another remarkable paper on integral points by proving their finiteness for hyperelliptic equations $y^2 = f(x)$ under appropriate assumptions (this result was extracted from a letter to Mordell and was published under the pseudonym X in [47]).

missing on the affine curve with respect to a smooth complete model.) Conversely, this condition becomes sufficient (for the existence of infinitely many integral points) if we allow a sufficiently large number field and a sufficiently large (fixed) denominator for the coordinates.[2]

Each of the numerous results and ideas that we have mentioned would have represented at that time a major advance in itself. Hence it is difficult to overestimate the importance of this paper and its influence, even thinking of contemporary mathematics.

The paper, however, being written in German, is not accessible for a direct reading to all mathematicians. There are of course modern good or excellent expositions in English of some of the results, however we believe it may be of interest for many to go through the original source for a precise understanding of some principles, as really conceived by Siegel. In addition, we think that this paper is a model also from the viewpoint of exposition; the ideas and methods are presented in a limpid and simultaneously precise way.

All of this led the second author to the idea of translating the paper into English, and of publishing the result by the 'Edizioni della Normale'. After some partial attempts for a translation, this was finally carried out by the first author, and here is the output. The translation was made literally and keeping the style used by Siegel as far as possible, instead of rephrasing the text in more modern style. (In particular, Siegel is not using the engaging 'we' but instead uses the comprehensive 'one'. The reader should have this in mind when reading the translation.)

It has been eventually possible also to include the original text in this volume, which provides additional information.

We have also added to the translated text a small number of footnotes (marked as "FOOTNOTE BY THE EDITORS") to highlight a few points that we think are worth noting for the convenience of the reader. Further, after the translation, we have included into this publication an article by the two of us, describing some developments in the topic of integral points, and three modern proofs of Siegel's theorem (two of them being versions of the original argument). We have also inserted a few references to other work arising from the paper of Siegel.

ACKNOWLEDGEMENTS. We thank the Edizioni della Normale for having welcome this project. We especially thank Mrs. Luisa Ferrini of the 'Centro Edizioni', whose great care and attention have made it possible to reach the sought goal.

Clemens Fuchs and Umberto Zannier

[2]Note that *affine* implies $s > 0$; however, in view of Faltings' theorem - see 2.1 below - all of this remains true also for projective curves, *i.e.* when $s = 0$.

On some applications of Diophantine approximations*

Clemens Fuchs

Essays of the Prussian Academy of Sciences.
Physical-Mathematical Class 1929, No. 1

The well-known simple deduction rule according to which for any distribution of more than n objects to n drawers at least one drawer contains at least two objects, gives rise to a generalization of the Euclidean algorithm, which by investigations due to DIRICHLET, HERMITE and MINKOWSKI turned out to be the source of important arithmetic laws. In particular it implies a statement on how precisely the number 0 can be at least approximated by a linear combination

$$L = h_0\omega_0 + \cdots + h_r\omega_r$$

of suitable rational integers $h_0, \ldots, h_r$, which in absolute value are bounded by a given natural number H and do not vanish simultaneously, and of given numbers $\omega_0, \ldots, \omega_r$; in fact for the best approximation it certainly holds

$$|L| \leq (|\omega_0| + \cdots + |\omega_r|)H^{-r},$$

an assertion that does not depend on deeper arithmetic properties of the numbers $\omega_0, \ldots, \omega_r$.

The expression L is called an approximation form. If one then asks, how precisely the number 0 can at best be approximated by the approximation form $h_0\omega_0 + \cdots + h_r\omega_r$, then obviously any non-trivial answer will certainly depend on the arithmetic properties of the given numbers $\omega_0, \ldots, \omega_r$.

This question particularly contains the problem to investigate whether a given number ω is transcendental or not; one just has to choose $\omega_0 = 1, \omega_1 = \omega, \ldots, \omega_r = \omega^r$, $H = 1, 2, 3, \ldots$, $r = 1, 2, 3, \ldots$. The additional assumption, to come up even with a non-zero lower bound for $|L|$ as a function in H and r, gives a positive turnaround to the transcendence problem.

Also, the upper bound for the number of lattice points on an algebraic curve, thus in particular the study of the finiteness of this number, leads, as will turn out later, to the determination of a positive lower bound for the absolute value of a certain approximation form.

Analogous to the arithmetic problems of bounding $|L|$ from above and from below is an algebraic question. Let $\omega_0(x), \ldots, \omega_r(x)$ be series in powers of a

*CARL LUDWIG SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, In: "Gesammelte Abhandlungen", Band I, Springer-Verlag, Berlin-Heidelberg-New York, 1966, 209–266.

variable x and let $h_0(x), \dots, h_r(x)$ be polynomials of degree at most H, not all identically zero and having the property that the power series expansion of the approximation form

$$L(x) = h_0(x)\omega_0(x) + \cdots + h_r(x)\omega_r(x)$$

starts with a fairly large power of x; the goal is to get a lower and an upper bound for the exponent of this power of x. The algebraic problem is of easier nature than the arithmetic one; it leads to the determination of the rank of a system of linear equations.

These two problems, the algebraic and the arithmetic one, are connected by choosing for x a special rational number ξ from the common region of convergence of the power series and by assuming that the coefficients of these power series are rational numbers. Then in turn also the coefficients of the polynomials $h_0(x), \dots, h_r(x)$ can chosen to be rational; and on multiplying with the common denominator of the rational numbers $h_0(\xi), \dots, h_r(\xi)$ the algebraic approximation form $L(x)$ turns into an arithmetic one, unless the numbers $h_0(\xi), \dots, h_r(\xi)$ are all equal to zero. However, in general the best algebraic approximation will not be turned into the best arithmetic approximation in this way.

To bound the expression $|h_0\omega_0 + \cdots + h_r\omega_r|$ from below under the conditions $|h_0| \le H, \dots, |h_r| \le H$ there is the following possibility:

Let the numbers $\omega_0, \dots, \omega_r$ be not all equal to zero. The $r+1$ approximation forms

$$L_k = h_{k0}\omega_0 + \cdots + h_{kr}\omega_r, \qquad (k = 0, \dots, r)$$

shall be considered with coefficients that are rational integers and bounded in absolute value by H. Let the value of the determinant $|h_{kl}|$ be different from zero and denote by M the maximum of the $r+1$ numbers $|L_k|$. Let L be a further approximation form and let h be the largest among the absolute values of its coefficients. Since the $r+1$ forms $L_0, \dots, L_r$ are linearly independent, one can choose r of them, say $L_1, \dots, L_r$, which are linearly independent with L. Let (λ_{kl}) be the inverse of the matrix of the coefficients of $L, L_1, \dots, L_r$; then the following estimates for the absolute value of the elements λ_{kl} hold

$$|\lambda_{k0}| \le r!H^r \qquad (k = 0, \dots, r)$$
$$|\lambda_{kl}| \le r!hH^{r-1}. \qquad (k = 0, \dots, r; l = 1, \dots, r)$$

From the equalities

$$\omega_k = \lambda_{k0}L + \lambda_{k1}L_1 + \cdots + \lambda_{kr}L_r, \qquad (k = 0, \dots, r) \tag{1}$$

it follows that

$$|L| \ge \frac{|\omega_k|}{r!H^r} - \frac{rMh}{H}. \tag{2}$$

If now for growing H the number M, which depends on H, is approaching 0 *faster than H^{1-r}, then* (2) *gives a positive lower bound for $|L|$.* This condition is therefore sufficient for the linear independence of the quantities $\omega_0, \ldots, \omega_r$ over the field of rational numbers.

An analogous criterion holds for the linear independence of power series over the field of rational functions. In fact, let $\omega_0(x), \ldots, \omega_r(x)$ be power series, not all identically zero; let

$$L_k(x) = h_{k0}(x)\omega_0(x) + \cdots + h_{kr}(x)\omega_r(x), \qquad (k = 0, \ldots, r)$$

be $r+1$ approximation forms with polynomial coefficients $h_{kl}(x)$ of degree H and let M be the smallest exponent which really appears in the power series expansions of $L_0, \ldots, L_r$. Assume that the determinant $|h_{kl}(x)|$ is not identically zero. Let $L(x)$ be a further approximation form with coefficients of degree h. Let μ and μ_k be the smallest exponents in the power series $L(x)$ and $\omega_k(x), k = 0, \ldots, r$. On observing that the determinant $|h_{kl}|(x)$ has degree $rH + h$, then the estimate

$$rH + h + \mu_k \geq \min(\mu, M) \qquad (k = 0, \ldots, r) \tag{3}$$

follows from an equality similar to (1).

If now the difference $M - rH$ diverges for growing H, then (3) gives an upper bound for μ. In particular, this is sufficient for the linear independence of the power series $\omega_0(x), \ldots, \omega_r(x)$ over the field of rational functions.

When applying this criterion the difficulty lies in the claim of the non-vanishing of the determinant $|h_{kl}(x)|$. To get to cases in which this difficulty can be mastered, from now on the functions $\frac{d\omega_o(x)}{dx}, \ldots, \frac{d\omega_r(x)}{dx}$ are assumed to be expressible homogeneously and linearly by the functions $\omega_0(x), \ldots, \omega_r(x)$ themselves and moreover with coefficients that are rational functions in x. It then holds a homogeneous system of first order linear differential equations

$$\frac{d\omega_k}{dx} = a_{k0}\omega_0 + \cdots + a_{kr}\omega_r; \qquad (k = 0, \ldots, r) \tag{4}$$

and by differentiating an approximation form $L(x)$ another one is obtained, if one multiplies by the polynomial that appears as common denominator of the coefficients of $\omega_0, \ldots, \omega_r$. Iterating this r-times, one has in sum $r+1$ approximation forms. However, it can happen that the determinant of this system of $r+1$ approximation forms is identically zero; then also the determinant $\Delta(x)$ of the system of the $r+1$ linear forms $L, \frac{dL}{dx}, \ldots, \frac{d^rL}{dx^r}$ vanishes and vice versa. The importance of identical vanishing of Δ follows from the following *lemma*:

Let

$$\omega_k = c_0\omega_{k0} + \cdots + c_r\omega_{kr}, \qquad (k = 0, \ldots, r)$$

where $c_0, \ldots, c_r$ are arbitrary constants, be the general solution of the system (4). *The determinant of the system of the $r+1$ linear forms $L(x) =$*

$h_0(x)\omega_0(x) + \cdots + h_r(x)\omega_r(x), \frac{dL}{dx}, \ldots, \frac{d^rL}{dx^r}$ of $\omega_0, \ldots, \omega_r$ vanishes identically if and only if the $r+1$ functions

$$f_l = h_0\omega_{0l} + \cdots + h_r\omega_{rl} \qquad (l = 0, \ldots, r)$$

are related by a homogeneous linear equation with constant coefficients.

If

$$\frac{d^kL}{dx^k} = b_{k0}\omega_0 + \cdots + b_{kr}\omega_r, \qquad (k = 0, \ldots, r)$$

with $b_{0l} = h_l$, $b_{k+1,l} = \frac{db_{kl}}{dx} + b_{k0}a_{0l} + \cdots + b_{kr}a_{rl}$ for $k = 0, \ldots, r-1$ and $l = 0, \ldots, r$, then from the assumption of $|b_{kl}| = \Delta$ vanishing identically one gets an equation

$$g_0\frac{d^sL}{dx^s} + g_1\frac{d^{s-1}L}{dx^{s-1}} + \cdots + g_sL = 0,$$

where $s \leq r$ and $g_0, \ldots, g_s$ denote certain sub-determinants of $\Delta(x)$ from which g_0 does not vanish identically. The function

$$L = \sum_{k=0}^{r} h_k\omega_k = \sum_{k=0}^{r} h_k \sum_{l=0}^{r} c_l\omega_{kl} = \sum_{l=0}^{r} c_l f_l,$$

satisfies this linear differential equation of order s, so do any of the $r+1$ functions $f_0, \ldots, f_r$; since their number is bigger than s, they are related by a homogeneous linear equation with constant coefficients. Conversely, it follows from such a relation by differentiating r-times, that the determinant $\left|\frac{d^kf_l}{dx^k}\right|$ is identically zero, and from the matrix relation

$$\left(\frac{d^kf_l}{dx^k}\right) = (b_{kl})(\omega_{kl})$$

one obtains the equation $|b_{kl}| = \Delta = 0$, if one takes into account that the values of the solutions $\omega_{0l}, \ldots, \omega_{rl}, l = 0, \ldots, r$ in a regular point can be chosen so that the determinant $|\omega_{kl}|$ in this point is not 0 and hence is not identically zero.

An example is given by taking $\omega_k = e^{kx}$, so $\omega_{kl} = e^{kx}e_{kl}$, where (e_{kl}) denotes the identity matrix. Then $f_l = h_l(x)e^{lx}$ and there is no homogeneous linear equation with constant coefficients relating $f_0, \ldots, f_r$, since e^x is not an algebraic function. Thus the determinant Δ does not vanish identically in this case.

Now suppose again that the power series $\omega_0(x), \ldots, \omega_r(x)$ have only rational coefficients and that ξ is a rational number. Then one obtains from the system of the algebraic approximation forms for the functions $\omega_0(x), \ldots, \omega_r(x)$ a system of arithmetic approximation forms for the numbers $\omega_0(\xi), \ldots, \omega_r(\xi)$. The most

important point of all these investigations is now the construction of approximation forms for which for the number $\Delta(\xi) \neq 0$ holds. For this one uses the following consideration, which was already used in a special case by THUE.

Let γ be the smallest exponent in the power series expansion of the approximation form L. Multiplying by the common denominator $N(x)$ of the rational functions a_{kl} from (4) one obtains from $\frac{dL}{dx}$ an approximation form L_1, whose power series does not contain powers in x smaller than $\gamma - 1$. One now considers the determinant $D(x)$ of the $r+1$ approximation forms $L, N\frac{dL}{dx} = L_1, N\frac{dL_1}{dx} = L_2, \ldots, N\frac{dL_{r-1}}{dx} = L_r$. If ν is an upper bound for the degree of the $(r+1)^2+1$ polynomials N, Na_{kl}, and if the coefficients of the form L have degree H, then $D(x)$ has degree $H + (H+\nu) + \cdots + (H+r\nu) = (r+1)H + \frac{r(r+1)}{2}\nu$. On the other hand, it is possible to express $D(x)\omega_k(x)$ linearly homogeneously in $L, L_1, \ldots, L_r$, say

$$D\omega_k = \Lambda_{k0}L + \Lambda_{k1}L_1 + \cdots + \Lambda_{kr}L_r, \qquad (k = 0, \ldots, r) \tag{5}$$

and moreover with coefficients Λ_{kl}, which are polynomials in x. Therefore the function $D(x)\omega_k(x)$ vanishes at $x = 0$ with order at least $\gamma - r$. If one supposes that not all the power series $\omega_0, \ldots, \omega_r$ are divisible by x, which otherwise could be eliminated by division, then it follows that $D(x)$ vanishes at a non-zero value $x = \xi$ with order at most $(r+1)H + \frac{r(r+1)}{2}\nu + r - \gamma$, unless $D(x)$ is identically equal to zero. Now, through a suitable choice of L, it is possible to obtain $\gamma \geq (r+1)h + r$; in fact the $r+1$ polynomials $h_0(x), \ldots, h_r(x)$ of degree H contain $(r+1)(H+1)$ numbers as coefficients, which necessarily satisfy γ homogeneous linear equations. But then $D(x)$ vanishes at $x = \xi$ with order s, which is below the H-independent bound $\frac{r(r+1)}{2}\nu$, and the sth derivative of $D(x)$ is not zero at $x = \xi$. Moreover, equation (5) holds *identically* in $\omega_0, \ldots, \omega_r$; differentiating it s-times and using (4) to eliminate the derivatives of $\omega_0, \ldots, \omega_r$, then the resulting equation also holds identically in $\omega_0, \ldots, \omega_r$. Putting also $N\frac{dL_r}{dx} = L_{r+1}, \ldots, \frac{dL_{r+s-1}}{dx} = L_{r+s}$, then by (5) the expression $N^s(\xi)D^{(s)}(\xi)\omega_k$ ia a homogeneous linear relation of $L(\xi), L_1(\xi), \ldots, L_{r+s}(\xi)$ identically in $\omega_0, \ldots, \omega_r$. Assuming further that $N(\xi) \neq 0$, *i.e.* that ξ is different from the singular points of the system (4), then one obtains $\omega_0, \ldots, \omega_r$ as linear relation of $L(\xi), L_1(\xi), \ldots, L_{r+s}(\xi)$; among the $r+s+1$ forms $L(\xi), \ldots, L_{r+s}(\xi)$ there are hence $r+1$ which are linearly independent. In this way one finds $r+1$ arithmetic approximation forms for the numbers $\omega_0(\xi), \ldots, \omega_r(\xi)$ with determinant $\neq 0$.

For applications in number theory it is still necessary that the approximation forms, constructed above, lead to favorable arithmetic approximations in the sense explained earlier, *i.e.* that the coefficients of $L(x), \ldots, L_{r+s}(x)$ do not contain "too large" rational integer numbers. Since the number s is below a bound which does not depend on H, essentially one just needs a good estimate for the coefficients of the polynomials $h_0(x), \ldots, h_r(x)$ in $L = h_0\omega_0 + \cdots + h_r\omega_r$.

This can be easily demonstrated in the previously mentioned example $\omega_k(x) = e^{kx}$, because the coefficients can be expressed explicitly in terms of r and H; in this way one obtains a proof of the transcendence of e in the first of HERMITE's versions and, at the same time, a positive lower bound for the distance of an arbitrary algebraic number to e. It should also be noted that from HERMITE's formulae one immediately gets the transcendence of π and even a positive lower bound for the distance of an arbitrary algebraic number to π, when one takes into account that the norm of a non-zero algebraic integer has absolute value ≥ 1.

Another example, but only in the case $r = 1$, is given by the well-known continued fractions for the quotients of hypergeometric series. In particular, the continued fraction expansion of the function $(1-x)^{\alpha}$ was used by THUE to investigate the approximation of roots of natural numbers by rational numbers, and this was the starting point for the discovery of THUE's theorem on Diophantine equations.

In other cases one does not find an estimate beyond the trivial one for the numerical coefficients of the algebraically favorable approximation form, whose power series is divisible by $x^{(r+1)(H+1)-1}$, and the trivial bound is not sufficient, as one easily sees, in order to apply the arithmetic criterion. Therefore the strategy, that has led to a system of arithmetic approximation forms for $\omega_0(\xi), \ldots, \omega_r(\xi)$ having non-vanishing determinant, has to be slightly modified. One has to optimize between the two necessities of a good algebraic and arithmetic approximation to 0 by admitting for the number γ a smaller value than the one taken earlier, for the number s thus a bigger one, and so one gets better bounds for the coefficients of $h_0(x), \ldots, h_r(x)$ as a gain. This idea again was first applied by THUE. The estimate for the coefficients is obtained by using DIRICHLET's deduction rule, which was mentioned at the beginning, and which is here demonstrated in the form of a *lemma*:

Let

$$\begin{aligned} y_1 &= a_{11}x_1 + \cdots + a_{1n}x_n \\ &\vdots \\ y_m &= a_{m1}x_1 + \cdots + a_{mn}x_n \end{aligned}$$

be m linear forms in n variables with rational integer coefficients. Let $n > m$. Let the absolute values of the mn coefficients a_{kl} be not bigger than a given natural number A. Then the homogeneous linear equations $y_1 = 0, \ldots, y_m = 0$ are solvable in rational integer numbers $x_1, \ldots, x_n$, which are not all zero, but are all smaller than $1 + (nA)^{\frac{m}{n-m}}$ in absolute value.

For the proof let each of the variables $x_1, \ldots, x_n$ independently run through the values $0, \pm 1, \ldots, \pm H$; one obtains in sum $(2H+1)^n$ lattice points in the space given by orthogonal Cartesian coordinates $y_1, \ldots, y_m$, which however are not necessarily all different from each other. Each coordinate of each of these lattice points lies between the values $-nAH$ and $+nAH$. There are exactly $(2nAH+1)^m$ different lattice points in the m-dimensional space, whose co-

ordinate lie between $-nAH$ and $+nAH$. If now

$$(2nAH+1)^m < (2H+1)^n, \tag{6}$$

then two lattice points $y_1, \ldots, y_m$ belonging to different systems $x_1, \ldots, x_n$ coincide; and by subtracting these two systems one obtains a solution of $y_1 = 0, \ldots, y_m = 0$ in rational integer numbers $x_1, \ldots, x_n$, which are not all zero and in absolute value are $\leq 2H$. But the condition (6) is satisfied if the even integer number, which lies in the interval

$$(nA)^{\frac{m}{n-m}} - 1 \leq 2H < (nA)^{\frac{m}{n-m}} + 1,$$

is chosen for $2H$.

The method, which was sketched before, to determine a positive lower bound for the expression $|h_0\omega_0 + \cdots + h_r\omega_r|$ shall be applied in this exposition to two different problems. The first part mainly deals with the proof of the transcendence of the values of the cylindrical function evaluated at any non-zero algebraic number. The second part is concerned with the task of finding all algebraic curves which pass through infinitely many lattice points of the plane or, more generally, of the n-dimensional space; it will be shown that this can only happen in case of lines and hyperbolas and for certain other curves obtained from these by easy transformations and having also genus 0.

The motivation to study the problems in the first part came from W. MAIER's beautiful investigations on irrationality. The second part has its origin in the important results on the arithmetic properties of algebraic curves, which were discovered and recently published by A. WEIL in his thesis.

Part I: On transcendental numbers.

Dedicated to MAX DEHN.

By the theorems due to HERMITE and LINDEMANN the question of the arithmetic properties of the values of the exponential function at algebraic arguments has been answered. While the additivity of the exponential function reduces every algebraic equation between values of this function to a linear equation, something comparable does not exist anymore for other functions; and there lies the difficulty of generalizing HERMITE's arguments. For none of the other functions, which are of importance in calculus, a theorem of analogous strength like that for the exponential function has been found.

The irrationality of the cylindrical function

$$J_0(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!n!} \left(\frac{x}{2}\right)^{2n}$$

has been studied by different authors. HURWITZ and STRINSBERG proved that $J_0(x)$ is irrational for every non-zero rational value of x^2 and MAIER, going beyond that, showed in an extremely clever way that for such x the value $J_0(x)$ is not even a quadratic irrationality.

In what follows it will be shown that $J_0(x)$ is transcendental for every algebraic non-zero x. The method even gives the more general result that between the numbers $J_0(x)$ and $J_0'(x)$ no algebraic relation with rational coefficients can exist since it is shown that a positive lower bound for the absolute value of an arbitrary polynomial in $J_0(x)$ and $J_0'(x)$, whose coefficients are rational numbers, exists in terms of these coefficients. More generally, an analog of LINDEMANN's theorem will be shown, that between the numbers $J_0(\xi_1), J_0'(\xi_1), \dots, J_0(\xi_k), J_0'(\xi_k)$ no algebraic relation with rational coefficients exists if $\xi_1^2, \dots, \xi_k^2$ are pairwise distinct non-zero algebraic numbers.

The proof is done with the method that was discussed in the introduction. In particular to apply the first lemma a theorem is needed assuring that the function $J_0(x)$ is not solution of any first-order differential equation whose coefficients are polynomials in x. The previously stated theorem, that for algebraic non-zero values x no algebraic relation with algebraic coefficients exists between the numbers $J_0(x)$ $J_0'(x)$ and x, is merely a consequence of the theorem that assures that no algebraic equation identically in x between the functions $J_0(x)$ $J_0'(x)$ holds. This might indicate that even in more general cases numerical relations can be obtained by specialization of functional equations, so that calculus contains arithmetic in this sense.

§1. Tools from complex analysis.

In this paragraph it will be investigated which algebraic functional equations exist between the solutions of the BESSEL differential equation

$$\frac{d^2y}{dx^2} + \frac{1}{x}\frac{dy}{dx} + \left(1 - \frac{\lambda^2}{x^2}\right) y = 0, \tag{7}$$