数理解析研究所講究録
599巻 1986年 128-145

Transcendence Problems in Several Variables

By Michel WALDSCHMIDT
Université de Paris VI
(written by Isao WAKABAYASHI)

Abstract

We explain Gel'fond-Schneider method in several variables, showing at the same time that methods in transcendence number theory give a proof of Siegel's theorem on Diophantine equations. Then we give a new proof of Baker's theorem, and show that this new idea gives a result in the direction of the 4-exponentials problem.

§1. Siegel's theorem and transcendence method.

We have the following result of C.L.Siegel [14] which is fundamental for the theory of Diophantine equations, as shown by S.Lang in [6] and [8].

THEOREM 1 (Siegel). *Let* K *be a number field, and let* a *and* a' *be fixed numbers in* K. *Then there are only finitely many units* u *and* u' *in* K *satisfying the equation*

$$au + a'u' = 1. \qquad (1)$$

In the following, we explain the transcendence methods which derive such a result. There are several possible proofs, and the proof which we explain was initiated by A.O.Gel'fond [5]. But Gel'fond did not give an upper bound for the absolute values of the solutions, so it was an ineffective proof, and A.Baker [1, 2] made it effective.

PROOF. Let $\varepsilon_1, \cdots, \varepsilon_r$ be a basis of the group of units of K modulo torsion, which means that we can write

$$u = \zeta \varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}, \qquad u' = \zeta' \varepsilon_1^{m_1'} \cdots \varepsilon_r^{m_r'}, \tag{2}$$

where ζ and ζ' are some roots of unity and $m_1, \cdots, m_r, m_1', \cdots, m_r'$ are rational integers. We need some information on the m_i. So we first notice that, without loss of generality, we can choose an embedding of K into **C** such that

$$|u| \geqq \max_{\sigma} |u^{\sigma}|, \qquad |u| \geqq \max_{\sigma} |u'^{\sigma}|,$$

where $|u|$ is the absolute value of u corresponding to the embedding, and σ runs over the conjugates of K. Note that, in the second inequality, it is u and not u', and so this is not an equality in general.

Now it is not difficult to see, by just looking at the inequalities of norm and using properties of basis of units, that

$$\max_{1 \leqq i \leqq r} |m_i| \leqq C_0 \log |u|, \qquad \max_{1 \leqq i \leqq r} |m_i'| \leqq C_0 \log |u|,$$

with a constant C_0 which can be explicitly given. As our aim is to prove the finiteness of solutions u and u' of (1), which is equivalent to the finiteness of m_i and m'_i, we may assume that u is large.

Now starting from the equation (1), we write it as

$$1 - \left(-\frac{a'u'}{au}\right) = \frac{1}{au}$$

which is small, and we express this by (2) as

$$\left|1 - \left(\frac{-a'\zeta'}{a\zeta} \cdot \varepsilon_1^{m_1'-m_1} \cdots \varepsilon_r^{m_r'-m_r}\right)\right| = \frac{1}{|au|}.$$

So this can be written as

$$|1 - \alpha_1^{b_1} \cdots \alpha_n^{b_n}| \leqq \exp\left(-C_1 \max_{1 \leqq i \leqq n} |b_i|\right), \qquad (3)$$

where $n = r + 1$, $\alpha_i = \varepsilon_i$ $(1 \leqq i \leqq r)$, $\alpha_n = -\frac{a'\zeta'}{a\zeta}$, $b_i = m_i' - m_i$ $(1 \leqq i \leqq r)$, $b_n = 1$, and C_1 is an explicit constant. Thus we have such an inequality where α_i are fixed algebraic numbers and b_i are integers. Noting that $\max_{1 \leqq i \leqq r} |m_i - m_i'|$ is large since u is large, we may assume that $\max_{1 \leqq i \leqq n} |b_i|$ is large.

Now what we need is a lower bound of the value of the left-hand side of (3). It is possible to give a lower bound by using the Liouville arguments, but the lower bound will be essentially of the same quality and we shall not get any thing. So the main problem is to get a lower bound which is better than (3), and which gives a contradiction if $\max_i |b_i|$ is large.

Let $B = \max_i |b_i|$, and let

$$(*) = |1 - \alpha_1^{b_1} \cdots \alpha_n^{b_n}|.$$

Then the following results are obtained.

Lower bound by Gel'fond [5]: *For any positive* ε *there exists a positive constant* $B_0(\varepsilon)$ *such that for all* $B > B_0(\varepsilon)$ *we have*

$$(*) > \exp(-\varepsilon B).$$

If we take $\varepsilon < C_1$, then together with (3), we get a contradiction and the Siegel theorem is proved.

But Gel'fond used the Roth theorem, so B_0 was not effective. Therefore, even though the finiteness of solutions u and u' of (1) was proved, we could not obtain an upper bound for the absolute values of solutions u and u'. And Baker succeeded to give an effective result.

Lower bound by Baker (see the references in [2]): *There exist two effective constants* C *and* κ *such that for all* $B > 1$ *we have*

$$(*) > \exp(-C(\log B)^{\kappa}).$$

After that, N.I.Fel'dman obtained a better estimate which is in fact the best possible in terms of B.

Lower bound by Fel'dman [4]: *There exists an effective constant* C *such that for all* $B > 1$ *we have*

$$(*) > B^{-C}.$$

The last two lower bounds enable us therefore to find all the solutions of (1).

One explicit lower bound in a slightly different situation is given by Y. Morita in these proceedings.

These results are obtained in the following manner.

To get a lower bound for (*) is essentially equivalent to the problem to get a lower bound for the value

$$b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n + 2k\pi i,$$

and the method comes in fact from Baker's solution of the following problem of transcendence.

THEOREM 2 (Baker [1,2]). *Let* $\alpha_1,\cdots,\alpha_n$ *be algebraic numbers different from* 0. *Choose* $\log \alpha_1,\cdots,\log \alpha_n$, *and suppose they are linearly independent over* $\mathbf{Q}$. *Then,* 1, $\log \alpha_1,\cdots,\log \alpha_n$ *are linearly independent over the field* $\overline{\mathbf{Q}}$ *of algebraic numbers.*

This is the transcendence theorem which Baker proves, and the same proof essentially gives the above lower bound.

Now this theorem has the following corollaries.

COROLLARY 1 (Hermite-Lindemann theorem). *If* α *is a non-*

zero algebraic number and $\log \alpha$ *is non-zero, then* $\log \alpha$ *is a transcendental number.*

PROOF. Apply the theorem for $n = 1$.

COROLLARY 2 (Gel'fond-Schneider theorem). *If* α_1 *and* α_2 *are non-zero algebraic numbers and* $\log \alpha_1/\log \alpha_2$ *is not a rational number, then* $\log \alpha_1/\log \alpha_2$ *is a transcendental number.*

PROOF. Apply the theorem for $n = 2$.

§ 2. Method of Gel'fond-Schneider in one variable.

The method of Baker is a development of the method of Gel'fond, so here we recall the two methods of Gel'fond and Schneider in one variable, and in §3 we explain their extension to several variables.

We want to prove Gel'fond-Schneider theorem (Corollary 2). So we suppose the following.

ASSUMPTION 1. Let α_1, α_2 be non-zero algebraic numbers and let β be an irrational algebraic number. We suppose $\log \alpha_2 = \beta \log \alpha_1$.

From this assuption we want to get a contradiction. We explain first the method of Schneider, and next the method of Gel'fond.

1° Method of Schneider.

Starting point. The two functions z and $\alpha_1^z = e^{z \log \alpha_1}$ are entire functions with moderate growth, and they are algebraically independent, that is, for any non-zero polynomial P in $\mathbf{Q}[X,Y]$, the function $P(z,\alpha_1^z)$ is not identically zero. And they take algebraic values simultaneously at a lot of points, namely, at all the points of $\mathbf{Z} + \mathbf{Z}\beta$. Under Assumption 1, these facts will give a contradiction, by allowing us to construct a polynomial P with $P(z,\alpha_1^z) = 0$. The proof will be divided in two steps.

Step 1. *Construction of* P. Let S be a sufficiently large integer. We construct a polynomial P in $\mathbf{Z}[X,Y]$ such that the function $F(z) = P(z,\alpha_1^z)$ has many zeros, that is, it satisfies $F(h_1+h_0\beta) = 0$ for all integers h_1, h_0 with $0 \leq h_j \leq S$.

In fact this is possible because the condition is defined by $(S + 1)^2$ linear homogeneous equations whose unknowns are the coefficients of P, and if we choose the degree of P sufficiently large in such a way that the number of coefficients of P is greater than $(S + 1)^2$, then just by linear algebra we can find a solution. In addition, it is possible by the well-known Siegel lemma, to bound the absolute values of the coefficients of P if we allow the degree of P to be sufficiently large.

Step 2. *Vanishing of* F. In order to prove that F(z) is identically zero, we prove the following two properties $(A_{S'})$ and $(B_{S'})$ by induction on S' which is any integer with $S' \geqq S$.

$(A_{S'})$ $F(h_1 + h_0\beta) = 0$ for $1 \leqq h_j \leqq S'$.

$(B_{S'})$ $\sup_{|z| \leqq cS'} |F(z)| < \exp(-S'^2)$ with $c = 1 + |\beta|$.

The proof is as follows.

i) (A_S) is true by the construction of P. So the induction hypothesis holds.

ii) $(B_{S'}) \Longrightarrow (A_{S'})$. By $(B_{S'})$, the function F is small on the disk $(|z| \leqq cS')$, so the value $F(h_1+h_0\beta)$ is small for $1 \leqq h_j \leqq S'$. Furthermore this value is an algebraic number by Assumption 1. Then, by the arithmetic fact that, like an rational integer, an algebraic number can not be too small if it is not zero (Liouville inequality), we can easily prove that $F(h_1+h_0\beta) = 0$.

iii) $(A_{S'}) \Longrightarrow (B_{S'+1})$. This is a consequence of the classical Schwarz lemma for one variable which says that if a function with moderate growth has a lot of zeros, then its value is small in some disks.

Thus by i),ii),iii), the properties $(A_{S'})$ and $(B_{S'})$ hold for all $S' \geqq S$. Especially the fact that $(B_{S'})$ holds for all $S' \geqq S$, implies that F(z) is identically zero. But this is a contradiction. So Assumption 1 was false, and the Gel'fond-Schneider theorem is proved.

2° Method of Gel'fond.

The structure of Gel'fond's proof is essentially the same. The difference is at the starting point, and the derivatives of the functions are also used.

Starting point. The two functions e^z and $e^{\beta z}$ are entire, and they are algebraically independent over **Q**, since β is irrational. They take algebraic values at $\mathbf{Z}\log \alpha_1$. So we have less values than in Schneider's proof, that is, we have only a **Z**-module of rank 1. But since β is algebraic, these functions satisfy differential equations with algebraic coefficients, which was not the case for Schneider's proof.

Step 1. *Construction of* P. We construct a polynomial P in $\mathbf{Z}[X,Y]$ such that the function $F(z) = P(e^z, e^{\beta z})$ has many zeros of high order, that is, for large S we have

$$\frac{d^{h_0}}{dz^{h_0}} F(h_1 \log \alpha_1) = 0 \qquad \text{for } 0 \leq h_j \leq S.$$

This is possible by the same argument as above, since the values to be considered, namely, all the derivatives of F(z) at $\mathbf{Z}\log \alpha_1$ are algebraic.

Step 2. *Vanishing of* F. The proof of the vanishing of F is the same as above in principle. We use arithmetical properties of algebraic numbers, and Schwarz's lemma. And we get again a contradiction.

§ 3. Gel'fond-Schneider method in several variables.

We explain the proof of Baker's theorem (Theorem 1). Baker uses functions of several variables by generalizing Gel'fond's method.

For the sake of simplicity, we shall prove Baker's theorem in a slightly weaker form. So we suppose the following, and we want to get a contradiction.

ASSUMPTION 2. Let $\alpha_1,\cdots,\alpha_{n+1}$ be non-zero algebraic numbers such that $\log \alpha_1,\cdots,\log \alpha_{n+1}$ are linearly independent over $\mathbf{Q}$, and let $\beta_1,\cdots,\beta_n$ be algebraic numbers. We suppose

$$\beta_1\log \alpha_1 + \cdots + \beta_n\log \alpha_n = \log \alpha_{n+1}. \tag{4}$$

1° Generalization of Gel'fond's method.

Starting point. The n+1 functions of n variables $e^{z_1},\cdots,e^{z_n}$ and $e^{\beta_1 z_1+\cdots+\beta_n z_n}$ are analytic on $\mathbf{C}^n$, and they are algebraically independent over $\mathbf{Q}$. They take simultaneously algebraic values at $\mathbf{Z}(\log \alpha_1,\cdots,\log \alpha_n)$ by (4). Further these functions satisfy partial differential equations with algebraic coefficients.

Step 1. *Construction of* P. We construct a polynomial P in $\mathbf{Z}[X_1,\cdots,X_{n+1}]$ such that the function of n variables

$$F(z_1,\cdots,z_n) = P(e^{z_1},\cdots,e^{z_n},e^{\beta_1 z_1+\cdots+\beta_n z_n})$$

has zeros of high order at many points of the form $(h \log \alpha_1, \cdots, h \log \alpha_n)$.

Step 2. *Vanishing of* F. In order to prove that $F(z_1,\cdots,z_n)$ is identically zero, we use arithmetical arguments and Schwarz's lemma. But the difficulty is with Schwarz's lemma. We have now a function of several variables, and in this case, even if we know that it has a lot of zeros in some disk, it does not give an upper bound for its values. Baker's idea is to consider a complex line passing the origin, and he succeeded to use the Schwarz lemma only for functions of one variable. In fact, he succeeded by considering the function of one variable defined by

$$\phi(\zeta) = F(\zeta \log \alpha_1,\cdots,\zeta \log \alpha_n).$$

2° Generalization of Schneider's method.

Starting point. The n+1 functions $z_1,\cdots,z_n$ and $\alpha_1^{z_1}\cdots\alpha_n^{z_n}$ are analytic on $\mathbf{C}^n$, and they are algebraically independent over $\mathbf{Q}$. They take simultaneously algebraic values at $\mathbf{Z}^n + \mathbf{Z}(\beta_1,\cdots,\beta_n) \quad (\subset \mathbf{C}^n)$.

Step 1. *Construction of* P. We construct a polynomial P in $\mathbf{Z}[X_1,\cdots,X_{n+1}]$ such that the function of n variables

$F(z_1,\cdots,z_n) = P(z_1,\cdots,z_n,\alpha_1^{z_1}\cdots\alpha_n^{z_n})$ vanishes at many points of the form $(h_1+h_0\beta_1,\cdots,h_n+h_0\beta_n)$.

Step 2. *Vanishing of* F. As in Gel'fond's method, the difficulty is with Schwarz's lemma. But for Schneider's method, we succeeded to prove a Schwarz lemma for several variables which is applicable to this situation [15]. See also [11]. However, we had to assume that the β's are real numbers, which is a little bit undesirable. Admitting this restriction, we can thus prove Baker's theorem.

But what is more unpleasant, is that in the proof of our Schwarz lemma for several variables, we had to use the results of W.M.Schmidt on the simultaneous approximation of algebraic numbers. Because of it, our proof of Baker's theorem was not effective, which is really undesirable for the applications. So we want to give another proof of Baker's theorem which works in both cases, and which gives some further results.

§ 4. New proof of Baker's theorem.

We explain it for Schneider's method in several variables, but it is the same for Gel'fond's method.

Starting point. The same as §3,2°.

Step 1. *Construction of* P. We construct a polynomial P in $\mathbf{Z}[X_1,\cdots,X_{n+1}]$ such that the function

$$F(z_1,\cdots,z_n) = P(z_1,\cdots,z_n,\alpha_1^{z_1}\cdots\alpha_n^{z_n}) \tag{5}$$

has small derivatives at the origin, that is, for sufficiently small ε and sufficiently large T, it satisfies

$$\left| \frac{\partial^{\tau}}{\partial z_1^{\tau_1} \cdots \partial z_n^{\tau_n}} F(0) \right| \leqq \varepsilon,$$

for $0 \leqq \tau_i \leqq T$ and $1 \leqq i \leqq n$. Moreover, the degree of P can be bounded from above by some explicit constant depending on T.

Here we just ask inequalities, and the important thing is that we do not use the β's. In the proof we neither use the fact that the α's are algebraic. So it is not at all arithmetic, and we do not use Siegel's lemma. However, it is easy to solve this system of linear inequalities by using the Dirichlet box principle like in the proof of Siegel's lemma and by the same arguments (see [16]).

Step 2. Upper bound for F. Corresponding to (B_S), we prove that for some small ε' and some large R,

$$\sup_{|\underline{z}| \leqq R} |F(\underline{z})| < \varepsilon',$$

where $\underline{z} = (z_1, \cdots, z_n)$.

We note that R is much greater than the cS which we had before.

For the proof, we use Schwarz's lemma for one variable. To obtain an upper bound for $|F(\underline{z}_0)|$ with $|\underline{z}_0| \leqq R$, we consider the function $\phi(\zeta) = F(\zeta \cdot \underline{z}_0)$ of one variable. We look at its Taylor expansion at the origin

$$\phi(\zeta) = \sum_{m=0}^{T} a_m \zeta^m + \sum_{m>T} a_m \zeta^m.$$

The first term of the right-hand side is small for $|\zeta| \leqq 1$

because for $m \leqq T$, a_m are small by the construction in Step 1. The second term has a zero of high order at the origin, so for $|\zeta| \leqq 1$, we can get a small upper bound for its value by Schwarz's lemma.

Step 3. *Vanishing of* F *at many points*. Corresponding to (A_S), we prove that for some large H,

$$F(h_1+h_0\beta_1,\cdots,h_n+h_0\beta_n) = 0,$$

if $0 \leqq h_j \leqq H$.

For the proof, we use the same arguments as in the proof of the implication $(B_{S'}) \Longrightarrow (A_{S'})$.

We note that H is in fact rather large, and so F vanishes at much more points than can be attained by use of Siegel's lemma. And this will imply a contradiction as is shown in the next step.

Step 4. *Use of a zero estimate*. In order to get a contradiction, we use a so called zero estimate which is the main difficulty of the proof. Roughly speaking, a zero estimate is a lower bound for the degrees of the polynomials which vanish at given points. One of the typical zero estimates is as follows.

Zero estimate by D.W.Masser [9]. *Let* $y_1,\cdots,y_\ell$ *be fixed vectors of* $\mathbf{C}^n$ *which are linearly independent over* $\mathbf{Q}$. *For each positive integer* H *we set*

$$Y(H) = \{h_1y_1 + \cdots + h_\ell y_\ell \in \mathbf{C}^n \mid 0 \leqq h_j \leqq H,\ h_j \in \mathbf{Z}\}.$$

Then there exist positive constants c_1, c_2 *and* μ *such that*

$$c_1 H^{\mu} \leqq \min_{P} \deg P \leqq c_2 H^{\mu},$$

where P *runs over all poynomials in* $\mathbf{C}[X_1,\cdots,X_n]$ *satisfying* $P(y) = 0$ *for all* y *of* Y(H). *Further* c_1 *and* μ *are explicit constants.*

Zero estimates have been developed by Gel'fond [5], R.Tijdeman and others for exponential polynomials in one variable, namely, for functions defined by polynomials of z or exponential functions. After that, zero estimates for several variables have been developed by Masser, Yu.V.Nesterenko, W.D.Brownawell, G.Wüstholz, P.Philippon in a very general context of commutative algebraic groups. Masser [10] and D.Bertrand [3] give surveys on this subject.

In our situation, the zero estimates show that, if a function of the form (5) vanishes at all the points $(h_1+h_0\beta_1,\cdots,h_n+h_0\beta_n)$ with $0 \leqq h_j \leqq H$, then the degree of P is bounded from below by some explicit constant depending on H. This constant becomes greater than the degree of our polynomial P if T is sufficiently large, which gives a contradiction. Thus Baker's theorem is proved.

§ 5. The five exponentials theorem.

As an application of our method, we get new results by mixing Gel'fond's method and Schneider's method. Let us recall the 6 exponentials theorem [6, 12].

THEOREM 3 (Six exponentials theorem). *Let* x_1, x_2 *be complex numbers linearly independent over* $\mathbf{Q}$, *and let* y_1, y_2, y_3 *be complex numbers linearly independent over* $\mathbf{Q}$. *Then, one of the* 6 *numbers* $e^{x_i y_j}$, $1 \leqq i \leqq 2$, $1 \leqq j \leqq 3$, *is transcendental.*

CONJECTURE (Four exponentials conjecture [7, 12, 13]). *Let* x_1, x_2 *be complex numbers linearly independent over* $\mathbf{Q}$, *and let* y_1, y_2 *be complex numbers linearly independent over* $\mathbf{Q}$. *Then one of the* 4 *numbers* $e^{x_i y_j}$, $1 \leqq i \leqq 2$, $1 \leqq j \leqq 2$, *is transcendental.*

This conjecture is not yet solved. The result we got in this direction is as follows. We quote it as 5 exponentials theorem.

THEOREM 4 (Five exponentials theorem). *Let* x_1, x_2 *be complex numbers linearly independent over* $\mathbf{Q}$, *and let* y_1, y_2 *be complex numbers linearly independent over* $\mathbf{Q}$. *Then, one of the* 5 *numbers* $e^{x_i y_j}$, $1 \leqq i \leqq 2$, $1 \leqq j \leqq 2$, *and* e^{x_2/x_1} *is transcendental.*

This is only a special case. In fact, we get a general result [17] on algebraic groups which contains this, and which contains also the result of Baker, the result of Wüstholz [3] and some other results [16] related with Schneider's method in several variables.

References

[1] A. Baker, *Transcendental number theory*, Cambridge Univ. Press, 2nd ed., 1979.

[2] A. Baker, The theory of linear forms in logarithms, in *Transcendence theory: Advances and applications*, Academic Press, 1977, pp.1-27.

[3] D. Bertrand, Lemmes de zéros et nombres transcendants, *Séminaire Bourbaki*, 38ème année (1985/86), n°652, 1-23.

[4] N. I. Fel'dman, An improvement of the estimate of a linear form in the logarithms of algebraic numbers, Math. USSR-Sb. **6** (1968), 393-406.

[5] A. O. Gel'fond, *Transcendental and algebraic numbers*, Moscow, 1952; Dover, 1960.

[6] S. Lang, *Fundamentals of Diophantine geometry*, Springer, 1983.

[7] S. Lang, *Introduction to transcendental numbers*, Addison-Wesley, 1966.

[8] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren 231, Springer, 1978.

[9] D. W. Masser, On polynomials and exponential polynomials in several complex variables, Invent. Math., **63** (1981), 81-95.

[10] D. W. Masser, Zero estimates on group varieties, Proc. International Congress Mathematiciens, Warszawa, 1983.

[11] J.-C. Moreau, Lemmes de Schwarz en plusieurs variables et applications arithmétiques, *Séminaire Lelong-Skoda*, 1978/79, Springer Lecture Notes 822 (1980), 174-190.

[12] K. Ramachandra, Contributions to the theory of transcendental numbers (I), Acta Arith., **14** (1968), 65-72, (II), ibid., 73-88.

[13] Th. Schneider, *Introduction aux nombres transcendants*, Springer, 1957, Gauthier-Villars, 1959.

[14] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss., n°1 (1929), Ges. Abh., n°16, 209-266.

[15] M. Waldschmidt, *Nombres transcendants et groupes algébriques*, Astérisque 69-70, Soc. Math. France, 1979.

[16] M. Waldschmidt, Transcendance et exponentielles en plusieurs variables, Invent. Math., **63** (1981), 247-267.

[17] M. Waldschmidt, Gel'fond-Schneider method in several variables, in preparation.