数理解析研究所講究録
599巻 1986年 82-94

Diophantine Equations and Transcendental Methods

By Michel WALDSCHMIDT
Université de Paris VI
(written by Noriko HIRATA)

Abstract

This lecture will be divided into three parts. We begin with the result of J.Liouville on diophantine equations, and the refinement called the Thue-Siegel-Roth theorem. In the second part, we give some results on integral points on certain curves. After that, we will consider a connection between this subject and transcendental numbers, via Baker's method.

§1. Some approximations.

Let us recall the theorem of Liouville:

THEOREM 1 (Liouville, 1844). *Let* α *be an algebraic number of degree* $d \geq 2$. *Then there exists* $C(\alpha) > 0$ *such that for all rational numbers* $\frac{p}{q}$ *with* $q > 0$, *we have*

$$|\alpha - \frac{p}{q}| > \frac{C(\alpha)}{q^d},$$

where $C(\alpha)$ *is easily computable.*

This result was the first tool to construct a transcendental number. The point is that, if we take a real number, very well approximated by rational numbers, then it can not be an algebraic number.

We will give a proof of this result in a special case.

Proof in a special case; $|\sqrt[3]{2} - \frac{p}{q}| > \frac{1}{6q^3}$. We would like to get the constant $C(\sqrt[3]{2}) = \frac{1}{6}$. For this, looking at the minimal polynomial of $\sqrt[3]{2}$, that is, $X^3 - 2$, we remark that $p^3 - 2q^3 \neq 0$ because $X^3 - 2$ has no rational roots, and also $p^3 - 2q^3 \in \mathbf{Z}$. Then we know $|p^3 - 2q^3| \geq 1$. On the other hand, if $p \leq \frac{3}{2}q$, we have

$$|p^3 - 2q^3| = |p - \sqrt[3]{2}q| \cdot |p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2| < |p - \sqrt[3]{2}q| \cdot 6q^2$$

and if $p > \frac{3}{2}q$, we have

$$|\frac{p}{q} - \sqrt[3]{2}| > |\frac{3}{2} - \sqrt[3]{2}| > \frac{1}{6}.$$

By combining these inequalities, the result follows. (q.e.d.)

A.Thue improved Liouville's theorem. His improvement is essential because we can apply it to diophantine equations.

THEOREM 2 (Thue). *Let* α *be an algebraic number of degree* $d \geq 3$. *Then there exist* δ *with* $0 < \delta < d$ *and* $C'(\alpha) > 0$ *such that for all rational numbers* $\frac{p}{q}$ *with* $q > 0$, *we have*

$$|\alpha - \frac{p}{q}| > \frac{C'(\alpha)}{q^{\delta}}.$$

COROLLARY 3. *Let* $f \in \mathbf{Z}[X,Y]$ *be a homogeneous polynomial of degree* $d \geq 3$. *Then for all non-zero integers* k, *the equation* $f(x,y) = k$ *has only finitely many solutions* $(x,y) \in \mathbf{Z}^2$.

Proof of Corollary 3 in a special case. We shall use the result (without proof):

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

We consider a diophantine equation $x^3 - 2y^3 = k$ and we start from $(x,y) \in \mathbf{Z}^2$ satisfying this equation. So we have

$$|k| = |x^3 - 2y^3| = |x - \sqrt[3]{2}y||x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2|$$
$$\geq |x - \sqrt[3]{2}y| \cdot \frac{3}{4}x^2.$$

We may suppose $|x| \geq |y|$, and we get

$$\frac{1}{10^6|x|^{2.955-1}} \leq \frac{1}{10^6|y|^{2.955-1}} \leq |x - \sqrt[3]{2}y| \leq \frac{4|k|}{3x^2},$$

namely, $|x| \leq 10^{137}|k|^{23}$. (q.e.d.)

We can see that all the solutions of this diophantine equation are bounded by some explicit number. We should say that when δ is less than d, it is difficult to compute $C'(\alpha)$ in an effective way, so if we use the method of Thue, we cannot give always such an explicit upper bound for the solutions.

§2. Diophantine equations.

Let K be a number field and $\mathcal{O}_K$ be the ring of integers in K. We shall consider several curves and the integral points on these curves. Here we denote unknowns in $\mathcal{O}_K$ by x and y.

We make a list of diophantine equations that have only finitely many solutions in $\mathcal{O}_K$.

(M) **Mordell's equation.** *Let* k *be a non-zero element of* K. *Then Mordell's equation* $y^2 = x^3 + k$ *has only finitely many solutions* $(x,y) \in \mathcal{O}_K \times \mathcal{O}_K$.

(E) **Elliptic equation.** *Let* $f \in K[X]$ *be a polynomial of degree* 3 *with three distinct complex roots. Then the elliptic equation* $y^2 = f(x)$ *has only finitely many solutions* $(x,y) \in \mathcal{O}_K \times \mathcal{O}_K$.

(HE) **Hyperelliptic equation.** *Let* $f \in K[X]$ *be a polynomial of degree* ≥ 3 *with at least three simple complex roots. Then the hyperelliptic equation* $y^2 = f(x)$ *has only finitely many solutions* $(x,y) \in \mathcal{O}_K \times \mathcal{O}_K$.

These three results are special cases of the result of C.L.Siegel, that is, if we take a curve $f(x,y) = 0$ which has a genus at least one, then on this curve there are only finitely many integral points. But for the above equations, we have some effective results, while for Siegel's theorem, we have not

an effective result. Now, further equations are the following:

(SE) **Superelliptic equation.** *Let* $f \in K[X]$ *be a polynomial with at least two complex roots whose orders of multiplicity are prime to* m, *where* m *is a natural number at least three. Then the superelliptic equation* $y^m = f(x)$ *has only finitely many solutions* $(x,y) \in \mathcal{O}_K \times \mathcal{O}_K$.

(T) **Thue's equation.** *Let* k *be a non-zero element of* K. *Let* $\alpha_1,\cdots,\alpha_n$ *be elements of* K *such that* α_1,α_2 *and* α_3 *are distinct. Then Thue's equation* $(x - \alpha_1 y)\cdots(x - \alpha_n y) = k$ *has only finitely many solutions* $(x,y) \in \mathcal{O}_K \times \mathcal{O}_K$.

(S) **Siegel's equation.** *Let* a *and* a' *be elements of* K. *Let* u *and* u' *be unknown units in* K. *Then Siegel's equation* $au + a'u' = 1$ *has only finitely many solutions* u,u', *units in* K.

We can remark that J.-H.Evertse generalized Siegel's result to the equation $\varepsilon_1 + \cdots + \varepsilon_n = 0$ where $\varepsilon_1,\cdots,\varepsilon_n$ are called S-units. Evertse's result has not yet been made effective while Siegel's result is effective.

Now we would like to explain the proof that each equation has only finitely many solutions. For this, we begin with the connections between these equations. For example, the hyperelliptic equation is more general than the elliptic equation,

the elliptic equation is more general than Mordell's equation, and the superelliptic equation can take the exponent 3, so it is easy to see that the superelliptic equation is more general than Mordell's equation with the transformation with x replaced by y and y replaced by x. But there are some connections which are not trivial. Denoting a trivial relation by $\to$, and a non-trivial relation by $\Rightarrow$, we have the following relations.

$$\begin{array}{ccccc} T & \Rightarrow & SE & \to & M \\ \Downarrow & \swarrow & & & \uparrow \\ S & \Rightarrow & HE & \to & E \end{array}$$

We first explain the two trivial relations $M \to S$ and $T \to S$.

Proof of $M \to S$. Look at the equation $au + a'u' = 1$. The unit group is finitely generated, so we can write $u = y^2 b$, where b is an element of the set of the units divided by the squares of units, so b belongs to a certain finite set. In the same way, we can write $u' = x^3 c$ with c in a finite set. Then we have $y^2 ab = - x^3 a'c + 1$ which yields Mordell's equation if we multiply both sides by $(ab)^3 (a'c)^2$. (q.e.d.)

Proof of $T \to S$. We write $u = x^3 b$, $u' = y^3 c$ with b,c in a finite set, and we have the equation $x^3 ab + y^3 a'c = 1$ which gives Thue's equation. (q.e.d.)

We now give an outline of the proofs which are not

trivial.

Proof of T $\Rightarrow$ SE. We start from an equation (SE). We write this equation as

$$y^m = a_0(x - \beta_1)^{t_1}(x - \beta_2)^{t_2} \cdots (x - \beta_h)^{t_h}$$

where $m \geqq 3$, $h \geqq 2$, the numbers $\beta_1,\cdots,\beta_h$ are distinct, and at least two numbers of $t_1,\cdots,t_h$, say t_1 and t_2, are prime to m. For simplicity, we suppose $a_0,\beta_1,\cdots,\beta_h \in \mathcal{O}_K$. We consider the solution $(x,y) \in \mathcal{O}_K \times \mathcal{O}_K$ of this equation. We can write ideals as

$$(x - \beta_i) = \mathfrak{a}_i^m \mathfrak{B}_i \qquad \text{for } i = 1,2,$$

where $\mathfrak{B}_i$ is not divisible by any m-th power of prime ideals. Since the common factors of $x - \beta_i$ and $x - \beta_j$ divide $\beta_i - \beta_j$, and further t_i $(i = 1,2)$ is prime to m, it is easy to see that each $\mathfrak{B}_i$ divides $(a_0 \prod_{i \neq j}(\beta_i - \beta_j))^m$, so we may suppose that $\mathfrak{B}_i$ is a "fixed" ideal. Select $\mathfrak{a}_i'$, $\mathfrak{B}_i'$ from a fixed set of representatives for the ideal classes, and such that $\mathfrak{a}_i \mathfrak{a}_i'$ and $\mathfrak{B}_i \mathfrak{B}_i'$ are principal. Multiplying the above equality by $\mathfrak{a}_i'^m \mathfrak{B}_i'$ we obtain

$$\mathfrak{a}_i'^m \mathfrak{B}_i'(x - \beta_i) = (\mathfrak{a}_i \mathfrak{a}_i')^m \mathfrak{B}_i \mathfrak{B}_i'.$$

Then, by some algebraic argument, we see that it is possible to write

$$x - \beta_i = w_i^m \delta_i \qquad \text{for } i = 1,2,$$

with δ_i in some fixed finite set of algebraic numbers and $w_i \in \mathcal{O}_K$ (see [1,p.41]). From this we have

$$\beta_1 - \beta_2 = w_2^m \delta_2 - w_1^m \delta_1.$$

We can consider that the unknowns are $w_1, w_2 \in \mathcal{O}_K$. We see that this is a "fixed" polynomial which is homogeneous in w_1, w_2 with $m \geq 3$. This is exactly the situation of Thue's equation, and there are only finitely many solutions (w_1, w_2) in $\mathcal{O}_K \times \mathcal{O}_K$, so the number of solutions (x,y) is also finite. (q.e.d.)

Proof of S $\Longrightarrow$ T. Assume that (S) is known, and consider Thue's equation

$$(x - \alpha_1 y) \cdots (x - \alpha_n y) = k,$$

where $k \in \mathcal{O}_K$, $k \neq 0$, fixed. We know that $x - \alpha_i y$ are distinct for $i = 1,2,3$, and that $x - \alpha_i y$ divides k, which means that the field norm of $x - \alpha_i y$ is bounded. Then, by using properties of the unit group, we can write

$$x - \alpha_i y = \beta_i \varepsilon_i,$$

with β_i in a "fixed" finite set of integers in K, and with a unit ε_i. Now we consider the three equations

$$x - \alpha_1 y = \beta_1 \varepsilon_1, \tag{1}$$

$$x - \alpha_2 y = \beta_2 \varepsilon_2, \tag{2}$$

$$x - \alpha_3 y = \beta_3 \varepsilon_3. \tag{3}$$

By elimination with (1) $\times$ $(\alpha_2 - \alpha_3)$ + (2) $\times$ $(\alpha_3 - \alpha_1)$ + (3) $\times$ $(\alpha_1 - \alpha_2)$, we obtain an equation of the form

$$a_1 \varepsilon_1 + a_2 \varepsilon_2 + a_3 \varepsilon_3 = 0$$

with $a_i \in \mathcal{O}_K$ "fixed" and non-zero. Dividing it by $a_3 \varepsilon_3$, we get

$$\frac{a_1\varepsilon_1}{-a_3\varepsilon_3} + \frac{a_2\varepsilon_2}{-a_3\varepsilon_3} = 1.$$

For $u = \varepsilon_1/\varepsilon_3$, $u' = \varepsilon_2/\varepsilon_3$, this is (S), and it has only finitely many solutions u and u'. The problem is to find ε_3 which satisfies

$$\varepsilon_1 = u\varepsilon_3, \tag{4}$$

$$\varepsilon_2 = u'\varepsilon_3. \tag{5}$$

Put (4) and (5) into (1),(2),(3), and we eliminate ε_i to get

$$\begin{cases} \beta_3(x - \alpha_1 y) = \beta_1 u(x - \alpha_3 y), \\ \beta_3(x - \alpha_2 y) = \beta_2 u'(x - \alpha_3 y). \end{cases}$$

If $\beta_3 = \beta_1 u$, we have $\beta_3\alpha_1 = \beta_1\alpha_3 u = \beta_3\alpha_3$, which means $\beta_3 = 0$. So we get $\beta_3 \neq \beta_1 u$. Put

$$b = \frac{\alpha_1\beta_3 - \alpha_3\beta_1 u}{\beta_3 - \beta_1 u}.$$

We get $x = by$, and therefore $y^n(b - \alpha_1)\cdots(b - \alpha_n) = k$, and this is a simple equation to solve, which has only finitely many solutions y. (q.e.d.)

Proof of S $\Longrightarrow$ HE. Here we consider

$$f(X) = a_0 \prod_{i=1}^{s} (X - e_i)^{t_i}$$

where $a_0 \in \mathcal{O}_K$, $e_i \in \mathcal{O}_K$ $(1 \leqq i \leqq s)$ distinct, t_1, t_2, t_3 odd numbers. The ideal class group of K is finite, so we put

R_1 = a finite set of ideals which represent each class of the class group,

and

R_2 = the set of ideals of the form $\prod_{\ell} \mathfrak{p}_\ell^{k_\ell}$ with $k_\ell = 0$ or 1, where $\{\mathfrak{p}_\ell\}$ is the set of prime ideals which divide $(a_0 \prod_{i\neq j} (e_i - e_j))$.

We denote also by S_1 the finite set of elements of K of the form $\zeta\varepsilon_1^{k_1}\cdots\varepsilon_r^{k_r}.\frac{\beta}{\gamma}$, where $\varepsilon_1,\cdots,\varepsilon_r$ is a fixed fundamental basis of the unit group, ζ is any root of unity in K, $k_i = 0$ or 1, β is a generator of $\mathcal{B}\mathcal{B}'$ with $\mathcal{B} \in R_2$ and $\mathcal{B}' \in R_1$ which represents the class of $\mathcal{B}^{-1}$, and γ is a generator of $\mathcal{C}^2\mathcal{D}$ with $\mathcal{C} \in R_1$ and $\mathcal{D} \in R_1$ which represents the class of $\mathcal{C}^{-2}$.

Let $L = K(\{\sqrt{\delta},\ \delta \in S_1\})$. We choose generators β_1,β_2,β_3 of principal ideals of L such that (β_k) divides $(e_i - e_j)$ with $\{i,j,k\} = \{1,2,3\}$. We put $a = -\beta_1/\beta_3$, $a' = -\beta_2/\beta_3$ and we know that $au + au' = 1$ has only finitely many solutions u and u', units of L. Put further

$$S_2 = \{(u,u') \mid au + a'u' = 1\}$$

and

$$S_3 = \{\lambda \in L \mid (\beta_1 u + \beta_2 u')\lambda^2 = \frac{e_3-e_1}{\beta_2 u'} - \frac{e_2-e_3}{\beta_1 u} \text{ for some } (u,u') \in S_2\}.$$

We shall show that (x,y) satisfying $y^2 = f(x)$ can be written as

$$x = e_3 + \frac{1}{4}\left\{-\beta_1\lambda u + \frac{e_3-e_2}{\beta_1\lambda u}\right\}^2 \quad \text{for } \lambda \in S_3, \qquad (*)$$

which will give the finiteness of the set of solutions of

(HE).

For this, we decompose for $j = 1,2,3$,

$$(x - e_j) = a_j^2 \mathcal{B}_j,$$

where $\mathcal{B}_j$ has no square factors. Regarding the equation

$$y^2 = (x - e_j)^{t_j} \cdot a_0 \prod_{i \neq j} (x - e_i)^{t_i}, \qquad j = 1,2,3,$$

with odd numbers t_j, we get that $\mathcal{B}_j$ belongs to R_2. Let $\mathcal{B}_j' \in R_1$ which represents $\mathcal{B}_j^{-1}$ and $a_j' \in R_1$ which represents a_j^{-1}. So we can deduce that the ideal

$$(x - e_j) a_j'^2 \mathcal{B}_j' = (a_j a_j')^2 \mathcal{B}_j \mathcal{B}_j'$$

is a principal ideal. Then, by the same argument as mentioned in the proof of T $\Rightarrow$ SE, we can write

$$x - e_j = z_j^2 \delta_j, \qquad j = 1,2,3,$$

with $z_j \in \mathcal{O}_K$, $\delta_j \in S_1$. In L, we can decompose

$$e_i - e_j = (z_j\sqrt{\delta_j} - z_i\sqrt{\delta_i})(z_j\sqrt{\delta_j} + z_i\sqrt{\delta_i}),$$

then there exist units $u_i \in L$ $(1 \leq i \leq 3)$ such that

$$\begin{cases} z_1\sqrt{\delta_1} - z_2\sqrt{\delta_2} = \beta_3 u_3, \\ z_2\sqrt{\delta_2} - z_3\sqrt{\delta_3} = \beta_1 u_1, \\ z_3\sqrt{\delta_3} - z_1\sqrt{\delta_1} = \beta_2 u_2. \end{cases}$$

Then $u = u_1/u_3$ and $u' = u_2/u_3$ satisfy $au + au' = 1$, so $(u_1/u_3, u_2/u_3) \in S_2$. If we take $\lambda = u_3$, we have

$$2z_3\sqrt{\delta_3} = -\beta_1 \lambda u + \frac{e_3 - e_2}{\beta_1 \lambda u} = \beta_2 \lambda u' + \frac{e_1 - e_3}{\beta_2 \lambda u'},$$

so $\lambda \in S_3$. Now, from this and $x - e_3 = z_3^2 \delta_3$, we obtain (*).

(q.e.d.)

§3. Baker's method.

We shall finish this lecture by Baker's method. This method gives an effective way to prove (S).

THEOREM 4 (A.Baker). *Let* K *be an algebraic number field and let* a,a' *be elements of* K. *Take a fundamental basis* $\varepsilon_1,\cdots,\varepsilon_r$ *of the unit group of* K, *and let* ζ,ζ' *be roots of unity. If*

$$u = \zeta\cdot\varepsilon_1^{m_1}\cdots\varepsilon_r^{m_r} \quad \textit{and} \quad u' = \zeta'\cdot\varepsilon_1^{m_1'}\cdots\varepsilon_r^{m_r'}$$

$(m_1,\cdots,m_r,m_1',\cdots,m_r' \in \mathbf{Z})$ *satisfy the equation*

$$au + a'u' = 1,$$

then

$$\max_{1\leqq i\leqq r} (|m_i|, |m_i'|) \leqq C,$$

where C *is a constant which can be effectively computed in terms of* ε_i $(1 \leqq i \leqq r)$,K,a,a'.

This theorem makes it possible to solve explicitly the diophantine equations that we have mentioned.

Now we state an open problem on this subject.

Open problem. If we take a curve of genus two over a number field, it is known by Siegel's theorem that this curve has only finitely many integral points. We can say that this curve corresponds to (HE) by a birational transformation, but

this transformation doesn't conserve the integral points. It is not yet known how to give an upper bound of solutions even in the case of genus two.

References

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

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