数理解析研究所講究録 1200 巻 2001 年 210-219

Finiteness and Infiniteness of the Solutions to a System of Diophantine Inequalitites

A survey of a joint work with J.-H. Evertse

Noriko HIRATA-KOHNO 平田典子

Department of Mathematics
College of Science and Technology
Nihon University
Suruga-dai, Kanda, Chiyoda, Tokyo 101-8308, Japan
email hirata@math.cst.nihon-u.ac.jp
日本大学　理工学部　数学科

代数的整数論の研究集会にて、再び講演の機会を与えていただいたことに、心より感謝申し上げます。

今回は、オランダ Leiden 大学の Prof. J.-H. Evertse 氏との共同研究を話の中心にすえながら、

* ディオファントス不等式の解の有限性についての過去の結果の復習

* ディオファントス不等式の連立不等式（ Wirsing System ）の解の有限性と無限性について、いろいろ面白い現象がおきている

という状況を、皆さんにご報告したいのであります [E-H]。

それにしても一世紀以上も前から極められている主題にしては、分からないことが多く、私自身、これから少しずつていねいに調べてゆきたいと思っております。

1. Introduction

まず、いつもながら、ディオファントス不等式の金字塔である K. F. Roth の定理 [R] を復習する。

定理 (Thue-Siegel-Roth の定理、Roth 1955)

α を代数的数とする。ε、C を任意の正の数とする。このとき有理数 $\frac{p}{q}$（ただし $p, q \in \mathbf{Z}, q > 0, (p, q) = 1$）で次を満たすものは有限個しか存在しない。

$$|\alpha - \frac{p}{q}| < \frac{C}{\max\{|p|, q\}^{2+\epsilon}}$$

注意

通常は$C = 1$として述べていることが多い。また、αの次数は定理の主張にはいっていない。それから、αが有理数のときは自明、αが有理数体上2次のときは、1844年のLiouvilleの定理（[Schm3]の114ページ定理1A)よりすぐ出るし、αが虚数のときもRothの定理は自明なので、αは有理数体上2次以上とか3次以上の実代数的数と書くことが多い。

このRothの定理はいろんな本（[Schm3] [Schm4] [Sil]）に紹介されているように、best possibleの指数2に至るまでに、Liouvilleの定理、そしてThue、Siegel、Dyson、...らの指数の改良があって、Rothがbest possibleの$2+\varepsilon$でフィールズ賞となった。

さて、これから考えるのは、この有理数$\frac{p}{q}$が$\mathbf{Q}$上有限次の代数的数になったらどうなるか、という素朴な疑問である。

代数的数に対して、$\max\{|p|, q\}$の代わりになるのは高さと呼ばれるもので、いろいろな種類の高さが有るが、ここではMahler Measureとよばれるものを採用する。

定義

多項式　$f(X) = a_0(X-\xi_1)\cdots(X-\xi_t) \in \mathbf{C}[X]$に対し、$f(X)$のMahler Measureは

$$M(f) = |a_0| \prod_{i=1}^{t} \max(1, |\xi_i|)$$

と定める。

多項式$f \in \mathbf{Z}[X]$がprimitiveとは、その整数係数がgcd 1で、かつleading coefficient > 0のときに言うとする。

$\mathbf{Q}$上有限次の代数的数ξのMahler Measureは、ξの$\mathbf{Z}$上の最小多項式を$f \in \mathbf{Z}[X]$としたとき、つまり、primitive、$\mathbf{Z}$上既約な$f \in \mathbf{Z}[X]$で$f(\xi) = 0$をみたすものを取ったとき、

$$M(\xi) = M(f)$$

と定める。

ここで $\mathbf{Q}$ 上 t 次の代数的数 ξ のいわゆる logarithmic absolute hieight を $h(\xi)$ とおくと、

$$h(\xi) = \frac{1}{t} \log M(\xi)$$

となっている (証明はたとえば [B] の lemma 11)。

さらに、$\mathbf{Q}$ 上 t 次の代数的数 ξ の $\mathbf{Q}$ 上共役な元 $\xi^{(1)}, \ldots, \xi^{(t)}$ に対しては、何でも良いから、ひとつ順序を定めることにする。

では、まずは第一に、単純に

問題

α を代数的数、ε を任意の正の数とする。このとき代数的数 ξ で

$$|\alpha - \xi| < \frac{1}{M(\xi)^{2+\varepsilon}}$$

をみたすものは有限個か、と問う。

ところが、これは嘘である。理由はいろんなことから出るが、たとえば以下の事実 1 からも反例が簡単に作れるし、[Schm3] 259 ページにある、Wirsing の定理 3B からもわかる。

では、つぎにどうすれば有限個であるための十分条件を作れるか、ということであるが、次の 3 通りの考え方をする。

問題

1) 未知数 ξ のはいる代数体を固定する。

2) 未知数 ξ の $\mathbf{Q}$ 上の次数を固定する。

3) $|\alpha - \xi|$ のかわりに、たとえば $\max_{\sigma \in Gal(\overline{\mathbf{Q}}/\mathbf{Q})} |\alpha - \sigma(\xi)|$ のようなものを考え、未知数は $\xi \in \overline{\mathbf{Q}}$ の中を自由に動かす 。

まず、(1) であるが、これは W. J. Leveque によって 1955 年に示されている。彼の証明には少しギャップがあるが、これは例えばその後の W. M. Schmidt の部分空間定理 ([Schm3] の 153 ページ定理 1F) の H.P. Schlickewei による代数体版 ([Schl1] [Schl2]、定理の形は例えば [Schm4] の 177 ページ定理 1D) からも出る。

次に、(3) であるが、これは Absolute Subspace Theorem という名前で呼ばれており、Evertse と Schlickewei によって証明されている（証明はまだ未出版 [E-Schl2] だが、定理の形は [E-Schl1] の Corollary 6)。

2. Wirsing System

我々は問題 (2) を考えることにしよう。つまり、考えるディオファントス不等式を次の形とする。

t を正整数、$\kappa > 0$ とする。α を代数的数とする。$\mathbf{Q}$ 上 t 次の代数的数 ξ で、次の不等式をみたすものを考える。

$$(A) \qquad |\alpha - \xi| < M(\xi)^{-\kappa}$$

この (A) についてはいくつか結果が有るが、1971 年に E. Wirsing が $\kappa > 2t$ ならば (A) の解 ξ は有限個（Roth の予想であった）を示し [W]、1970 年にこれとは独立に Schmidt が　$\kappa > t+1$ ならば (A) は有限個の解しか持たないことを証明した [Schm1]。これは、Schmidt の部分空間定理からも出る。$\kappa > t+1$ のほうが良い結果であり、$t = 1$ のとき、2 つとも Roth の定理になる。

事実 1 [E3]

任意の $\varepsilon > 0$ をとる。$\kappa = t+1-\varepsilon$ とおく。このとき (A) が無限個の解を持つ代数的数 α の例が作れる（証明は Evertse によるが、[Schm3] 278 ページ 10 行目にも言及してある）なお、$\kappa = t+1$ とすると Roth の定理の定数 C に当たるものが 1 でないといけなくなる ([Schm3] の 6 ページ定理 2F で $C = \frac{1}{\sqrt{5}}$ というような意味）なので、これで $t+1$ は best possible と言って良い。

注意

上の事実 1 は、α が代数的数の場合である。ここで、任意の $\varepsilon > 0$ をとり、α が「t 次以下の代数的数」ではない任意の実数、つまり、α は、任意の実超越数か、または、任意の $t+1$ 次以上の実代数的数、とする。このとき、ある定数 C が α、ε、t に依存して存在し、

$$|\alpha - \xi| < \frac{C}{M(\xi)^{t+1-\epsilon}}$$

は無限個の $\mathbf{Q}$ 上 t 次の代数的数の解 ξ を持つ、という主張は、$t = 1$ と $t = 2$ の場合以外は、今現在でも未解決予想で、Wirsing の 1961 年の結果が、α に余計な条件をつけないものとしては best known である（Dirichlet の定理の高次版）。

次にこれを連立不等式として考える。すると、このように $t+1$ で解の有限、無限がハッキリする事態がなくなるということが起こる。

では、Wirsing System (W) を定義しよう。

定義

I を $\{1, \ldots, t\}$ の空でない部分集合とする。γ_i $(i \in I)$ を代数的数とし、φ_i $(i \in I)$ を非負実数とする。

$$(W) \qquad |\gamma_i - \xi^{(i)}| < M(\xi)^{-\varphi_i} \quad (i \in I)$$

を、$\mathbf{Q}$ 上 t 次の代数的数 ξ を未知数として考える。このディオファントス連立不等式 (W) を、最初に考えた [W] にちなんで、Wirsing System と呼ぶ。

Wirsing [W] は、どんな代数的数の組 γ_i $(i \in I)$ と、

$$\sum_{i \in I} \varphi_i > 2t \cdot \sum_{k=1}^{\#I} \frac{1}{2k-1}$$

をみたすどんな非負実数の組 φ_i $(i \in I)$ に対しても、次数 t の代数的数 ξ で (W) をみたすものは、有限個であることを示した。Evertse は、この同じ条件下で、個数の上からの評価を示した [E4]。

我々の方向は以下の通りである。平田は、主にこの Wirsing System の解の有限性の十分条件を Wirsing の上の条件よりもゆるく

$$\sum_{i \in I} \varphi_i > 2t$$

とすることを考えていて（定理 1）、Evertse は次に定義する Resultant Inequality を考えていた。ところが、その二つの解の有限性は同値だったのである（定理 2）。さらに、同じ指数なのに、解が無限個にも有限個になる例

が、それぞれことなる γ_i をとってみることによって起こることに気付いた（定理３）。

従って、(A) のように、κ つまり $\sum_{i\in I}\varphi_i$ のみで解の無限性と有限性が分かれないのである。

3. Resultant Inequality

Resultant Inequality (R) を定義しよう。

定義

まず、２個の多項式 $f,g\in\mathbf{Z}[X]$ をとり 、f の次数は r、g の次数は t とする。

$f=a_0X^r+a_1X^{r-1}+\cdots+a_r\quad(a_0\neq 0)$、$g=b_0X^t+\cdots+b_t\quad(b_0\neq 0)$ と表す。

f,g の Resultant とは、位数 $r+t$ の行列式

$$R(f,g)=\begin{vmatrix} a_0 & a_1 & \dots & \dots & a_r & & \\ & \ddots & & & & \ddots & \\ & & a_0 & a_1 & \dots & \dots & a_r \\ b_0 & b_1 & \dots & b_t & & & \\ & \ddots & & & \ddots & & \\ & & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \dots & b_t \end{vmatrix}$$

（最初の t 行は f の係数、最後の r 行は g の係数）。

良く知られているように、もし $f(X)=a_0\prod_{i=1}^{r}(X-\alpha_i)$, $g(X)=b_0\prod_{j=1}^{t}(X-\xi_j)$, と書くと、

$$R(f,g)=a_0^tb_0^r\prod_{i=1}^{r}\prod_{j=1}^{t}(\alpha_i-\xi_j).$$

である。これよりすぐ $|R(f,g)|\leq 2^{rt}M(f)^tM(g)^r$ であることも従う。f,g に共通解がなければ整数係数の行列式なので、$|R(f,g)|\geq 1$ である事実に注意。

定義

$f\in\mathbf{Z}[X]$ の次数は r とし、この f は固定。$\kappa>0$ とする。$g\in\mathbf{Z}[X]$ の次数は t とし、この g を未知方程式として、

$$(R) \qquad 0 < |R(f,g)| < M(g)^{r-\kappa}$$

をみたすものを考える。

注意

ここで、右辺は$M(g)^{r-\kappa}$であって、$\frac{M(f)^r}{M(g)^\kappa}$ではないので、念のため（$M(f)^r$なんてのは、定数で、$g$に関係ない）。また、$r < \kappa$のときは、(R) の右辺は1未満なので、$|R(f,g)| \geq 1$とあわせると (R) は解なしである。

さて、Ru-Wong の結果（[Ru-Wong]、証明は Schmidt の部分空間定理の応用） から、定理1が導かれる。

定理 1

I を $\{1,\ldots,t\}$ の空でない部分集合とする。γ_i $(i \in I)$ を代数的数とし、φ_i $(i \in I)$ を非負実数で $\sum_{i\in I} \varphi_i > 2t$ をみたすとする。

$$(W) \qquad |\gamma_i - \xi^{(i)}| < M(\xi)^{-\varphi_i} \quad (i \in I)$$

は、$\mathbf{Q}$ 上 t 次の代数的数の解 ξ を有限個しかもたない。

この、指数の部分の条件は、新しい。

そして、この Wirsing System の解の有限性と、Resultant Inequality のそれとは、次のような同値性がある。

定理 2

$f \in \mathbf{Z}[X]$ を次数 r で、重根のない多項式とする。$\kappa_0 > 0$ とする。次の2つの命題は、同値である。

(i) 任意の $\kappa > \kappa_0$ に対し、(R) は t 次の primitive な既約多項式 $g \in \mathbf{Z}[X]$ を有限個しか解に持たない。

(ii) I を $\{1,\ldots,t\}$ の空でない任意の部分集合とする。γ_i $(i \in I)$ を $f \in \mathbf{Z}[X]$ の解である代数的数（同じものがあっても良い）とし、φ_i $(i \in I)$ を任意の非負実数で $\sum_{i\in I} \varphi_i > \kappa_0$ をみたすものとする。

このとき (W) は次数 t の代数的数 ξ を、有限個しか解に持たない。

証明は、(i) から (ii) は簡単、(ii) から (i) には、Wirsing の議論を用いる。

定理 1 から、$\kappa_0 \geq 2t$ で (R)(W) の解の有限性が成り立つことになるが、(i) において注意を要するのは、解は t 次の primitive な既約多項式 $g \in \mathbf{Z}[X]$ で考えているということである。$\kappa_0 \geq 2t$ で (R) の解の個数の上からの評価は Evertse によって得られ、$\kappa_0 \geq 2t$ で (W) の解の個数の上からの評価は平田によって得られている（いずれも準備中）。

ここで、$\kappa_0 \geq 2t$ で (R) の解の個数の上からの評価を、t 次の多項式 $g \in \mathbf{Z}[X]$、ただし、primitive ではないか、または既約ではないものも許して考えるとする。

もしもそういう解の 個数 の上からの評価が得られたとすると（解の高さではない、ただの解の個数の上からの評価だけなのに !! ）ある難しいディオファントス不等式についての 高さ の effective な評価という大予想（effective symmetric Liouville という）を従えてしまうので [E-H]、それは現在では手が出ないということである。

あるディオファントス不等式の解の 個数 の上からの評価だけが、別のディオファントス不等式の解の 高さ の effective な評価を従えるという事実は他にも有り、解の 個数 の上からの評価だけでも、難しい（従って、とても意味がある、ただしこういう場合は残念ながら一つも出来た例はない）。

4. 解を無限個もつ例

定理 3

全ての整数 $t \geq 1$ について、次をみたす代数的数 $\gamma_1, \ldots, \gamma_t$ と、正定数 C_0 が存在する。

$$|\gamma_i - \xi^{(i)}| < C_0 \cdot M(\xi)^{-2}$$

は t 次の代数的数 ξ を、無限個解に持つ。

注意

つまり、任意の $\delta > 0$ に対し、非負実数 $\varphi_1, \ldots, \varphi_t$ で $\varphi_1 + \cdots + \varphi_t = 2t - \delta$ なるときに無限個解を持つ (W) の例有り、ということである。よって、「一般」 には (W) については $2t$ が指数としては最良である。

ところが、ここで疑問なのは、指数が $2t$ より大ではなく、より弱い、$\varphi_1 + \cdots + \varphi_t > t+1$ でも、γ_i に別の強い条件を科すと、(R) (従って、定理 1 より (W) の) 解の有限性も成り立つという定理が Schmidt によって証明されているということである [Schm2]。これは、定理 3 とあわせると $2t > \varphi_1 + \cdots + \varphi_t > t+1$ で、解が、無限と有限の両方の場合が出てくることを意味するのだから、と

ても興味深い。Schmidt の部分空間定理なども、考えている一次形式の一次独立性を仮定したときのことしか考えていないが、これはいわば一次形式がすごく沢山有って一次形式が一次従属であっても、解の無限性と有限性の考察ができることを暗示している。

このあたりのことを、なんとかきちんと分かりたいのです。

以下、文献をあげる。

References

[B] Bertrand, D., Approximations diophantiennes p-adiques sur les courbes elliptiques adnettant une multiplication complexe. Compositio Math. 37 (1978), 21–50.

[E1] Evertse, J.-H., An explicit version of Faltings' Product Theorem and an improvement of Roth's lemma. Acta Arith. 73 (1995), 215–248.

[E2] — An improvement of the quantitative Subspace theorem. Compos. Math. 101 (1996), 225–311.

[E3] — personal communication, (1997).

[E4] — The number of algebraic numbers of given degree approximating a given algebraic number. In: Analytic Number Theory, Proc. conf. Kyoto, (1997), 53–83, Cambridge Univ. Press.

[E-H] Evertse, J.-H., Hirata-Kohno, N., Wirsing systems and Resultant inequalities. submitted.

[E-Schl1] Evertse, J.-H., Schlickewei, H.P., The Absolute Subspace Theorem and linear equations with unknown from a multiplicative group. In: Number Theory in Progress, Proceedings of the conference in honor of the 60th birthday of A. Schinzel, Walter de Gruyter, (1999), 121–142.

[E-Schl2] — A quantitative version of the Absolute Subspace Theorem. submitted.

[R] Roth, K.F., Rational approximations to algebraic numbers. Mathematika 2 (1955), 1–20.

[Roy-Th] Roy, D., Thunder, J.L., An absolute Siegel's Lemma. J. reine

angew. Math. 476 (1996), 1–26.

[Ru-Wong] Ru, M., Wong, P.M., Integral points of $\mathbf{P}^n\backslash\{2n+1$ hyperplanes in general position$\}$ Invent. Math. 106 (1991), 195–216.

[Schl1] Schlickewei, H.P., The $\wp$-adic Thue-Siegel-Roth-Schmidt theorem. Arch. Math. 29 (1977), 267–270.

[Schl2] — The quantitative Subspace Theorem for number fields. Compos. Math. 82 (1992), 245–274.

[Schm1] Schmidt, W.M., Simultaneous approximation to algebraic numbers by rationals. Acta Math. 125 (1970), 189–201.

[Schm2] — Inequalities for resultants and for decomposable forms. In: Diophantine Approximation and its Applications, Proc. conf. Washington D.C., Academic Press, New York (1973), 235–253.

[Schm3] — Diophantine Approximation, Lecture Notes Math.785, (1980), Springer-Verlag.

[Schm4] — Diophantine Approximations and Diophantine Equations. Lecture Notes Math.1467, (1991), Springer-Verlag.

[Sil] Silverman, J.-H., The Arithmetic of Elliptic Curves. GTM 106 (1986), Springer-Verlag.

[W] Wirsing, E., On approximations of algebraic numbers by algebraic numbers of bounded degree. In: Proc. Symp. Pure Math. 20, A.M.S., Providence, (1971), 213–248.