数理解析研究所講究録
第 304 巻 1977 年 11-23

Thue-Siegel-Rothの不等式について

早稲田大学　理工学部　　足立恒雄

§1 序論

C. L. Siegel ([1]) は genus が正の代数曲線上には有限個しか整数点(座標がすべて整数である点)が存在しえないことを証明した。この有名な定理の non-standard method による再証明が近年 A. Robinson と P. Roquette によって与えられた([2])。このように non-standard method は主に既に証明された定理の証明の整理，もう少し詳しくいえば，たとえば Siegel の天才のみが解決しえた凡人には理解出来ない，その必然性の理解しえない計算や手法が整然とした形で再証明される，一口にいえば，証明の"合理化"がこの手法，non-standard method の本領であるように思える。

しかしながら，亡くなった A. Robinson の遺稿，ほんの数枚の notes, をもとにして竹内外史教授が完成された近々公表

が予定されている論文（［3］）は，この non-standard method に対する評価があてはまらない数少ない例外の一つである。

genus が正の代数曲線上には整数点が有限個しか存在しないことは解った，しかし，その全ての解を求めることが出来るのかどうか，これは明らかに別の問題である。もっと端的にいえば，方程式が与えられた時，その整数解の大きさの限界がその方程式の係数から定められるであろうか。

特に，代数曲線が hyper elliptic，その他いくつかの場合には，解の限界がその曲線の方程式から "explicit" に与えられることが，A. Baker によって証明されている（たとえば，［4］，［6］）。

genus が 0 の代数曲線，即ち，有理曲線の場合には，整数点は無限のこともあり，0 を含めて有限個のこともある。勿論，どの場合に有限なのか無限なのか判定することも出来る。だから positive genus の場合が大切なのである。

さて，A. Robinson - G. Takeuti は次の事柄を証明した：

α を代数的数とし，その次数 n は $n \geqq 2$ であるとする。κ を $\kappa > 2$ なる実数とする。Roth（［7］，［8］）によれば，適当な正定数 $C = C(\alpha, \kappa)$ をとれば，いかなる有理数 x/y（$y>0$）に対しても

$$|\alpha - \frac{x}{y}| > \frac{c}{y^\kappa} \qquad \cdots\cdots (1)$$

がなりたつ。

ところでこの c は α, κ から effective に定まるであろうか。もしも，任意の α，任意の κ (>2) に対して O.K.，即ち c が α, κ から effective に定まるのであれば，positive genus の代数曲線の整数点の限界は effective に求まる。

これが Robinson - Takeuti の結果である。つまり，"任意" の代数曲線の話が Roth の不等式という "特定" の話に還元された，Roth の不等式に話は押しこめられたのである。

筆者がこの論文においてなすことは，Roth の不等式の話を更にある（後述の）定数の計算に話をつめることにある。

もっとも Roquette 教授に伺ったところによると，教授は上述の論文の証明を改良して，証明が絶対的になるように，即ち，Roth の不等式を証明から "消去" しようと試みておられるそうである。私見では，non-standard method は上のような reduction，話の煮つめには有力であるが，新しい証明の編みだしにはやや難点があるように思われる。

我々が本論文に述べる方法は，Roth の不等式 (1) に，A. Baker の開発した *linear form of logarithms* の結果を応用する。定理の正確な formulation の前にいくつかの結果ないし目標との前後関係を述べよう。

まず上述のように終極的目標は次である：

(A) αを次数nが$n \geqq 3$なる代数的数とする。またκを$n > \kappa > 2$なる実数とする。しからばαとκとからeffectiveに計算できる実数$C = C(\alpha, \kappa) > 0$がとれて，任意の整数$x$, y（但し$y > 0$）に対して(1)がなりたつ。

<u>Remark</u> (i) $n = 2$の場合には$\kappa > 2 = n$により，定数Cは容易に計算できるので$n \geqq 3$としておく。

(ii) κは整数解の限界を求めるという目的のためならば，$\kappa < n$をみたすαと無関係な定数でありさえすればよく，"2より大"の2にこだわることはない。更に，Roquette教授によれば，κはある条件のもとでnにdependしてもよい。

A. Bakerが[4]において証明しているように，(A)は次の(B)から平均値の定理を用いて簡単に導かれる：

(B) $f(x, y)$を整数係数の既約多項式とし，x, yについて同次であるとする。fの次数nは$n \geqq 3$とする。κは$2 < \kappa < n$なる実数とする。mが整数であれば，

$$f(x, y) = m$$

を満たす整数x, yはすべて

$$\mathrm{Max}(|x|, |y|) < C m^{\frac{1}{n-\kappa}}$$

を満たす。ここにCはκとnと，fの係数とからeffectiveに計算できる正定数である。

ところで(A)は次の(A')と同値である：

(A')　αを次数$n \geqq 3$なる代数的数とする。κを$n > \kappa > 2$なる実数とする。またcは正実数とする。このとき

$$|\alpha - \frac{x}{y}| < \frac{c}{y^{\kappa}} \qquad \cdots\cdots (2)$$

を満たすような整数x, y ($y > 0$)に対しては常に

$$y < C \qquad \cdots\cdots (3)$$

がなりたつようなα, κ, cから effective に計算できる定数Cが存在する。

(A)と(A')との同値性は比較的容易であるから略する。特に(B) ⇒ (A')である。(A')における(3)のCはc, κのどういう order なのか明示されていない。一般には方程式より弱い形の不等式に関する結果が方程式の結果から導かれているので弱い結果となっているのである。(A')を仮定すれば、よく知られた Thue の元来の方法によって(B)の弱い形：

(B')　仮定は(B)と同じとする。しからば

$$\mathrm{Max}(|x|, |y|) < C,$$

ここにCはn, m, およびfの係数から effective に定まる定数である。

が得られる。以上から

$$(B) \Rightarrow (A) \Leftrightarrow (A') \Rightarrow (B')$$

であることを知る。(A)の強い形，即ち，(2)のcに関するorder が入った評価が得られれば，それから(B)は(A')から

(B') を導いたようにして導かれる。我々の結果は k を十分 n に近くとるとそのような強い形の結果を得るともいいあらわせる。

§2　定理とその証明

A. Baker は [5] において次の結果を示した；

(C) $\alpha_1, \cdots, \alpha_n$ を 0 でない代数的数とし，それらの次数はすべて d を越えないとし，height はすべて A' を越えないとする。α_0 を 0 でない代数的数とし次数は d を越えず，また height は A を越えないとする。$b_1, \cdots, b_n$ を整数とし，$\max_j |b_j| \leq B$ とする。$\Lambda = b_1 \log\alpha_1 + \cdots + b_n \log\alpha_n - \log\alpha_0$ とおけば，$\Lambda = 0$ であるか，または任意の $\varepsilon > 0$ に対して

$$|\Lambda| > A^{-C} e^{-\varepsilon B}$$

がなりたつ。ここに C は ε, A', n, d から effective に計算できる定数である。

Baker が述べているように，(C) から (1) がなりたつような α, c から effective に計算できる $k\ (<n)$ が存在することがいえる。これは (C) から (B) がある k についてなりたつことを導き，それからその k について (A) がなりたつことを意味する。

さて我々の証明する結果は次である；

<u>定理</u>　α を次数 $n \geqq 3$ なる代数的数とする。c を正実数と

とする。しからば，α から effective に計算できる $\kappa\,(<n)$ が存在して，(2) を満たす任意の整数 x，$y\,(y>0)$ に対して常に

$$y<(C_1 C)^{\frac{1}{n-\kappa}}$$

がなりたつ。ここに C_1 は α だけによって effective に計算される定数である。

κ が $2<\kappa<n$ なる任意の実数になれば，その結果は最も強い結果となる。

<u>Remark</u> (1) κ は実は，$Q(\alpha)$ が Q 上の Galois の時，

$$\kappa \geqq \frac{n}{1+\frac{1}{2C}}$$

にとればよい。この C は証明中にあらわれる特定の $\alpha_1,\cdots,\alpha_r$ によって定まる (C) 中にあらわれる Baker の定数 C である。従って特別な場合に (C) の中の定数 C がどれ位小さくとれるかが次の課題となる。

(2) κ は実際は n と α の height だけから定められることがわかる。

さて定理の証明を考えよう。手続は (C) から (B) を導く手続に類似しているから，Baker の [4]，PP 188-190 又は [6]，PP　　-　　を参照しながら進めることにする。

まず，ある κ と x，y に対して (2) がなりたっているとす

る。いい忘れたが，α は代数的整数であるとしても一般性を失わない，一定整数 a をかけて $a\alpha$ を代数的整数にできるからで，ac を c としておけばよいからである。

$K = Q(\alpha)$ を有理数体に α を添加した代数体とし，$r = s + t - 1$ は通常のように定める。(s，t は K の実共役体の個数，および虚の共役体の個数の半分である。)

次に $\beta = x - \alpha y$ とおく。β は代数的整数である。(2) から

$$|\beta| < c\, y^{1-\kappa} \qquad \cdots (4)$$

また根の分離ということから

$$c_1 y < |\beta^{(j)}| < c_2 y \qquad (j=2,\cdots,n) \quad \cdots (5)$$

ここに，そして以下においても，c_k は"α から" effective に計算される正定数である。また (j) は共役写像をあらわす。(1) と (2) から

$$|N\beta| < c c_3\, y^{n-\kappa} \qquad \cdots (6)$$

ここに N は K からの絶対ノルムを表わす。

<u>Lemma 1</u> (Landau-Siegel) 次の条件をみたすような K の単数 $\eta_1, \cdots, \eta_r$ が存在する；

$$\left|\log|\eta_k^{(j)}|\right| < c_4 \quad (k=1,\cdots,r;\ j=1,\cdots,r+1) \cdots (7)$$

かつ $\Delta = \begin{vmatrix} \log|\eta_1^{(1)}| & \cdots & \log|\eta_1^{(r+1)}| \\ \cdots & \cdots & \cdots \\ \log|\eta_r^{(1)}| & \cdots & \log|\eta_r^{(r+1)}| \end{vmatrix}$ とおくとき $|\Delta| > c_5$ ---- (8)

この Lemma はよく知られたものである。

Lemma 2　整数 $b_1, \cdots, b_r$ に対して $\gamma = \beta\eta_1^{b_1}\cdots\eta_r^{b_r}$ とおくと，

$$|\log|e^{b_0}\gamma^{(j)}|| < c_6 \quad (j=1, 2, \cdots, r+1) \quad \cdots (9)$$

をみたすように整数 $b_0, b_1, \cdots, b_r$ を選ぶことができる。従って，(9) の和をとって

$$|\log|\gamma^{(j)}/\gamma^{(k)}|| < c_7 \quad (j, k=1, 2, \cdots, r+1) \quad \cdots (10)$$

証明は，$(1, \cdots, 1) \in \mathbb{R}^{r+1}$，$(\log|\eta_j^{(1)}|, \cdots, \log|\eta_j^{(r+1)}|)$ $(j=1, \cdots, r) \in \mathbb{R}^{r+1}$ は $\mathbb{R}$ 上一次独立なベクトルであり，(7)，(8) によってこれらのベクトルの張る平行体の大きさが限定されることから，容易に導かれる。

Lemma 3　$\gamma^{(j)}/\gamma^{(k)}$ は全て次数が $n(n-1)$ 以下，height が $c^{n-1}c_8\, y^{(n-k)(n-1)}$ 以下の代数的数である。K/Q が，とくに，ガロワ拡大であれば，$\gamma^{(j)}/\gamma^{(k)}$ の次数は n 以下，height は高々 $cc_8 y^{n-k}$ となる。

証明　$\gamma^{(j)}/\gamma^{(k)}$ は整係数の多項式 $\prod_{j\neq k}(\gamma^{(k)}x - \gamma^{(j)}) = \prod_{j,k}(\gamma^{(k)}x - \gamma^{(j)})/(\prod_j \gamma^{(j)})(x-1)^n$ の根である。

右辺の分子 $= (N\gamma)^n \prod_{j,k}\left(x - \dfrac{\gamma^{(j)}}{\gamma^{(k)}}\right)$

右辺の分母 $= N\gamma\cdot(x-1)^n$

$N\gamma = N\beta$ と(6) により $|N\gamma| < cc_3 y^{n-k}$. これと(10) によって結果を得る。ガロワ拡大の場合には，$\gamma^{(j)}/\gamma^{(k)}$ は $N(\gamma^{(k)}x -$

$\gamma^{(j)}$)の零点だからLemmaの主張の通りである。

<u>Lemma 4</u>　λを$0<\lambda \leqq \mathrm{Min}\left\{\frac{\kappa+1}{2}, \kappa-1\right\}$なる実数とすると，$\left|\frac{\beta^{(1)}}{\beta^{(2)}}\right| < c\, y^{-\lambda} e^{-c_9 H}$がなりたつ，ここに$H$は$\mathrm{Max}\{|b_0|, |b_1|, \cdots, |b_r|\}$である。

<u>証明</u>　$|\log|e^{b_0}\gamma^{(j)}/\beta^{(j)}||$の最大値が$j=J$のとき与えられるとしよう。しからば，$|\log|e^{b_0}\gamma^{(J)}/\beta^{(J)}|| > c_{10}H$，故に

$|\log|\beta^{(J)}|| \geqq |\log|e^{b_0}\gamma^{(J)}/\beta^{(J)}|| - |\log|e^{b_0}\gamma^{(J)}|| > c_{10}H - c_6$

もしも$\log|\beta^{(J)}| \geqq 0$ならば$J \neq 1$，というのは$|\beta^{(1)}|<1$だから。(4)，(5)によって

$|\beta^{(1)}\beta^{(J)}| < c\,c_2\, y^{2-\kappa}$　故にHが十分大ならば$|\beta^{(1)}| < c\, y^{2-\kappa} e^{-c_{11}H}$

もしも$\log|\beta^{(J)}|<0$ならば$J=1$．$\therefore |\beta^{(1)}| < e^{c_6-c_{10}H} < e^{-c_{12}H}$

これと(4)とから$|\beta^{(1)}| < \bar{c}\, y^{\frac{1-\kappa}{2}} e^{-\frac{c_{12}}{2}H}$．

一方，(5)から$|\beta^{(2)}| > c_1 y$であるから，上のいずれの場合にもLemmaがなりたつ。

<u>Lemma 5</u>　$\alpha_j = \frac{\eta_j^{(2)}}{\eta_j^{(3)}}$　$(j=1, 2, \cdots, r)$，さらに　$\alpha_0 = \frac{(\alpha^{(3)}-\alpha^{(1)})\gamma^{(2)}}{(\alpha^{(2)}-\alpha^{(1)})\gamma^{(3)}}$とおく。すると

$$H(\alpha_j) < c_{13} \quad (j=1, 2, \cdots, r), \quad H(\alpha_0) < c_{14}(c\, y^{d-\kappa})^{(n-1)(n-2)}$$

ここに$H(\alpha_j)$は，勿論，α_jのheightを表わす。とくに，K/Qがガロワ拡大であれば　$H(\alpha_0) < c_{14}\, c\, y^{d-\kappa}$である。

証明　α_0 は整係数の多項式 $\prod\{(\alpha^{(j)}-\alpha^{(k)})\gamma^{(l)}x-(\alpha^{(l)}-\alpha^{(k)})\gamma^{(j)}\}$ の零点である。ここに積は相異なる j,k,l のすべてをわたる。Lemma 3 のようにしてあとは示される。

$z=b_1\log\alpha_1+\cdots+b_r\log\alpha_r-\log\alpha_0$ とおく。log は主値をとるものとしておく。さらに $\omega=\alpha_1^{b_1}\cdots\alpha_r^{b_r}-\alpha_0$ とおけば,

$$\omega=-\frac{(\alpha^{(3)}-\alpha^{(1)})}{(\alpha^{(2)}-\alpha^{(1)})}\cdot\frac{\beta^{(1)}}{\beta^{(2)}}\cdot\frac{\gamma^{(2)}}{\gamma^{(3)}} \quad \text{---- (11)}$$

がなりたつ。従って $\omega/\alpha_0=e^z-1$ である。Lemma 4 により, $|e^z-1|<1/4$ であるから, $|z-ib\pi|<4|e^z-1|$ を満足する $b\in\mathbb{Z}$ が存在する。証明は [ ], P176 にある。

そこで $\Lambda=z-b\log(-1)$, $B=2rH$ とおく。すると $|b|<B$, $|b_j|<B$ $(j=1,\cdots,r)$, 明らかに $\Lambda\neq0$ がなりたつ。

ここで定理(C)を利用しよう。Lemma 5 と併せると

$$|\Lambda|>\left\{c_{14}(c\,y^{n-k})^{(n-1)(n-2)}\right\}^{-c_{15}(\varepsilon)}e^{-\varepsilon B} \quad \text{---- (12)}$$

である。ここに $c_{15}(\varepsilon)$ は ε と α から effective に計算できる正数である。

一方, (11) と Lemma 4 を用いると

$$|\Lambda|<4|e^z-1|=4|\omega/\alpha_0|<c\,c_{16}\,y^{-\lambda}e^{-c_9H} \quad \text{---- (13)}$$

(12) と (13) とから

$$e^{(c_{17}-\varepsilon)B}<c'\,y^{c_{15}(\varepsilon)(n-1)(n-2)(n-k)-\lambda}$$

がなりたつ。c' は α と c と ε とから effective に計算できる定

数である。故に $c''=c_{15}(\varepsilon)(n-1)(n-2)$ とおけば

$$c''(n-k)-\lambda \leqq 0$$

のとき，たとえば，$\lambda=k/2$ とすれば $k \geqq \dfrac{n}{1+(2c'')^{-1}}$ のとき，$H<B<\dfrac{\log c'}{c_{17}-\varepsilon}$ をえる。Lemma 2 と併せて

$$|\beta^{(2)}|<c'^{\,c_{19}(\varepsilon)} \qquad \therefore\ y<\frac{|\beta^{(2)}|}{c_1}<c'^{\,c_{20}(\varepsilon)}$$

$c'=c^{(n-1)(n-2)c_{15}(\varepsilon)}c_{14}^{c_{15}(\varepsilon)}$ であるから，k を

$$(n-1)(n-2)c_{15}(\varepsilon)\,c_{20}\leqq\frac{1}{n-k}$$

にとれば定理は示されたことになる。

とくに，$K/\mathbb{Q}$ が Galois 拡大であれば，$c''=c_{15}(\varepsilon)$ である。たとえば，(A') において $k>\dfrac{n}{2}$ と出来るためには，

$$c_{15}(\varepsilon)\leqq\frac{1}{2}$$

が示されればよいことになる。

文献

[1] Siegel, C. L., "Über einige Anwendungen Diophantischer Approximationen", Abh. Preuss. Akad. Wiss. Phys. Math. (1929)

[2] Robinson, A. - Roquette, P., "On the finiteness theorem of Siegel and Mahler concerning Diophantine equations, J. Number Th. 7 (1975)

[3] Robinson, A., "A relatively effective procedure getting all quasi-integer solutions of diophantine equations with positive genusses" (written by G. Takeuti), to appear,

[4] Baker, A., "Contributions to the theory of Diophantine Equations," Philosophical Transactions of Roy. Soc. London, Vol. 263 (1968),

[5] Baker, A., "A sharpening of the bounds for linear forms in logarithms II," Acta Arith. XXIV (1973),

[6] Baker, A., Transcendental Number Theory, Cambridge, 1975,

[7] Roth, K. F., "Rational approximations to algebraic numbers," Mathematika 2 (1955),

[8] Lang, S., "Diophantine Geometry," Interscience.