

Integer Points on Algebraic Curves

東エ大理 平田典子 (N. HIRATA-KOHNO)

§1 Introduction

代数曲線の整数点の考察に近似不等式を応用する手法には3種類の方法があると筆者は考えている。一つは Roth の近似不等式を用いる場合で、この不等式及び拡張版により代数曲線上の整数点や有理点の有限性を論じることが、Siegel, Thue, Mordell, Leveque, Faltings, Vojta, Bombieri らによって行われてきた。この方法では整数点や有理点の個数を上から評価することは可能であっても、整数点や有理点の存在範囲を表す「高士」と呼ばれる数を effective に評価すること、即ち点を求めるアルゴリズムを定めることは全くできない。

第二の方法は Baker の近似不等式を使うもので、代数的数の対数の一次結合を近似するこの不等式を応用すると、代数曲線の定義方程式が $y^m = f(x)$ などごく特殊な形をしている場合、及びそれに帰着できる種数1の場合などに、代数曲線上の全ての整数点の高士の effective な評価を得ることが出来る。Baker の近似といかなる形の定義式の代数曲線に対して使えるかということ、例えば Baker 著「Transcendental Number Theory」(Cambridge UP) や Shorey-Tijdeman 著

「Exponential Diophantine Equations」 (Cambridge Tracts in Math vol 87) 等 に書かれてあるが、どうしても扱える定義方程式が限定されてしまい、一般の代数曲線の整数点や有理点の考察には役立たない。

第三の方向は Baker の近似のアナロジーをアーベル多様体上考えるものである。このような近似不等式が得られれば代数曲線の整数点の高さの評価に使えることを Lang が 1960 年から 70 年代半ばにかけて言っている。この場合の長所は種数 1 以上の非特異完備代数曲線の整数点の高さを上から評価できて、曲線の定義方程式が特別な形である必要のないことであるが、短所はこの評価がヤコビ多様体のモデルがエイク群の生成元の高さに依ってしまう点である。しかしこのようなものに依ることとをたとえ許しても、整数点の高さを求めることは自明ではない。この方向に役立つ近似不等式については Baker, Feldman, Coates, Lang, Masser, Bertrand, Philippon-Waldschmidt, 筆者などによ、て考察されている。

本稿ではこの近似を同時近似に拡張したものを利用すると、種数 1 以上の非特異完備代数曲線のヤコビ多様体が simple である場合に整数点の高さの評価を simple に限らないとせに比べ改良できることを述べる。またこの同時近似による定量的な結果が、超越数論の定性的な Wüstholz の定理を含み：

とに注意する。

§ 2 Notations

$\bar{\mathbb{Q}}$ を代数的数全体, A を $\bar{\mathbb{Q}}$ 上定義せられた次元 g のアーベル多様体とし, $\bar{\mathbb{Q}}$ 上のうめ-みにより $\mathbb{P}^N$ に含まれるとする。

T_A を A の原点における接空間とし, $\mathbb{C}^g$ と同一視する。

A の指数写像 $\exp_A : T_A \rightarrow A$ と $T_A \simeq \mathbb{C}^g$ の同一視及び

$A \subset \mathbb{P}^N$ のうめ-みを合成した $\mathbb{C}^g \rightarrow \mathbb{P}^N$ の写像を改めて $\exp_A$ と書くことにする。 $z = (z_1, \dots, z_g) \in \mathbb{C}^g$ に対して

$\|z\| = (|z_1|^2 + \dots + |z_g|^2)^{\frac{1}{2}}$ と定め, $T_A \simeq \mathbb{C}^g$ の

同一視によりこのノルムを T_A 上にも induce する。 A の原点に

対する $P \in A$ からの距離 $d(P)$ を $\text{Min} \{ \|u\| : \exp_A u = P \}$

により定義する。 $\Omega := \ker \exp_A$ の $\mathbb{R}$ -base とし, τ

いる 1 組の基本周期 $(\omega_1, \dots, \omega_g)$ と T_A の基底を固定する。

K_0 を A , A のうめ-み, T_A の基底が全て定義される代数

体とする。 K を K_0 の有限次拡大体とする。 M_K を K の互い

に同値でない正規化された絶対値の集合, $M_K^\infty \subset M_K$ をその

うちのアルキメデス的なもの全体の集合とする。

$P \in A(K) \subset \mathbb{P}^N(K)$ に対しその射影座標を $(X_0(P), \dots, X_N(P))$

と書いて $H_K(P) := \prod_{v \in M_K} \max \{ |X_0(P)|_v, \dots, |X_N(P)|_v \}^{[K_0:Q_0]}$

と定める。そして更に logarithmic absolute height h を

$$h(P) := \frac{1}{[K:\mathbb{Q}]} \log H_K(P)$$

と定義する。この定義が well-defined であること、及び諸性質については [Si] chap. 8 にある。

§3. アーベル多様体の代数点の下からの評価

アーベル多様体 A が simple である場合には次のような評価が得られる。これは A が simple でない場合の評価の改良である。記述が複雑だが要するに $P \in A(K)$ が $P \neq 0$ ならばその $d(P)$ が下から評価されるということを行っている。

定理1 K_0 を有限次代数体、 A を K_0 上定義された $(2g)$ アーベル多様体、 O をその K_0 上の原点とし、 K_0 上 $\mathbb{P}^N$ に埋め込まれているとする。 A を simple と仮定する。次のような effective 正整数 C_1 が存在する。 K を $D = [K:K_0] < \infty$ の K_0 の拡大体、 $P \in A(K)$ 、 r を $A(K)$ の rank とする。 $(P_1, \dots, P_r, P_{r+1}, \dots, P_m)$ を $A(K)$ の生成元で $P_1, \dots, P_r$ が自由部分、 $P_{r+1}, \dots, P_m$ をねじれ部分のものとする。 $n_1, \dots, n_m \in \mathbb{Z}$ を $P = n_1 P_1 + \dots + n_m P_m$ なる数とする。 $N := \max\{|n_1|, \dots, |n_m|, e^e\}$ とする。 $U_i \in \mathbb{C}^g$ を $\exp_A U_i = P_i$ ($1 \leq i \leq m$) とする。 $g_{i,j}$ ($1 \leq i \leq m, 1 \leq j \leq 2g$) $\in \mathbb{R}$ を

$u_i = g_{i,1} u_1 + \dots + g_{i,2g} u_{2g}$ なる数 g がある. $Q :=$

$\max_{\substack{1 \leq i \leq m \\ 1 \leq j \leq 2g}} \{1, |g_{i,j}|\}$ とする. $V_1, \dots, V_m, V \in \mathbb{R}$ と

$$\log V_i \geq \max \left(h(P_i), \frac{\|u_i\|^2}{D}, \frac{1}{D} \right) \quad (1 \leq i \leq n)$$

$$\log V_i \geq \max \left(\frac{\|u_i\|^2}{D}, \frac{1}{D} \right) \quad (n < i \leq m)$$

$$V = \max_{(1 \leq i \leq m)} V_i \quad \text{と} \quad \text{する.}$$

このとき $P = O$ かもしれない

$$\log d(P) > -c_1 D^{2(m+g)+1+\frac{1}{g}} (\log(NQ) + \log(D \log V))$$

$$\times (\log \log(NQ) + \log(D \log V))^{m+2g+\frac{1}{g}} \times \prod_{i=1}^m (\log V_i)$$

が成り立つ.

上の式の複雑さには目が回る場合はこの定理を次のように理解すれば良い。(この言いかえは h & u Néron-Tate height の性質から出る [H2]).

定理 1' K 代数体

A/K 次元 g の $\mathcal{A}$ -バシ多様体 $\subset \mathbb{P}^N$, simple

$P \in A(K)$ とする. $r = \text{rank } A(K)$ とおく.

今 $h(P) \leq \log H$ なる $H \in \mathbb{R}$, $H \geq e^{e^e}$ とする.

このとき $P = 0$ かもしれない $\exists c_1' > 0$:

$$\log d(P) > -c_1' (\log \log H) (\log \log \log H)^{n+4g+\frac{1}{g}}$$

となる.

A が simple とは限らない場合に対する [H2] の評価と比べると 定理1' では

$$\begin{aligned} \log d(P) &> -c_1 D^{2g(m+g)+2} (\log(NQ) + \log(D \log V)) \\ &\quad \times (\log \log(NQ) + \log(D \log V))^{g(m+2g)+1} \times \left(\prod_{i=1}^m (\log V_i)^g \right) \end{aligned}$$

定理1' では

$$\log d(P) > -c_1' (\log \log H) (\log \log \log H)^{g(n+4g)+1}$$

である。ちなみにこの手の近似が 定理1' で

$$\log d(P) > -C \log \log H \quad \text{となり } C \text{ も } 2 \text{ も } 1 \text{ くらい}$$

になると、Rothの近似くらいよい近似が Bakerの一般化型で得られるということになり、大事件であるが、今のところ難しくてもできない。

尚 定理1: 定理1' は Baker の近似のアーベル多様体上の
アナロジーの同時近似版 [H1] の応用として得られる:

同時近似 A が simple なとき $\rightarrow$ 改良

単なる近似 A が simple でなくともよい

§4. ヤコビ多様体が simple な代数曲線の整数点.

以下記号を説明する.

K 代体

C curve/ K 種数 $g \geq 1$. 非特異完備.

K 上の埋め込みにより $C \subset \mathbb{P}^n$ と見做すとする.

$C(K) := C \cap \mathbb{P}^n(K)$ とし, $(X_0, \dots, X_n) \in \mathbb{P}^n$ に

対し適当な変数変換により $C \not\subset \{X_n = 0\}$ と考えてよい.

ことに注意して $P = (X_0(P), \dots, X_{n-1}(P), 1) \in C(K)$

なる点を考察する。この $C \subset \mathbb{P}^n$ なる埋め込みに関する

logarithmic absolute height h および H_K を与える。

更に「絶対値」 M_K と「denominator」 δ_K を次のように定める:

$$M_K(P) := \prod_{v \in M_K^\infty} \max \{ |X_0(P)|_v, \dots, |X_{n-1}(P)|_v, 1 \} \quad [K_v:Q_v]$$

$$\delta = \delta_K(P) := \prod_{v \in M_K \setminus M_K^\infty} \max \{ |X_0(P)|_v, \dots, |X_{n-1}(P)|_v, 1 \} \quad [K_v:Q_v]$$

$$\forall K \quad \Delta = \Delta_K(P) = \max(\delta_K(P), e^{e^e}) \text{ とする。}$$

すると明らかに $H_K(P) = M_K(P) \cdot S_K(P)$ となる。

$$h(P) = \frac{1}{[K:\mathbb{Q}]} \{ \log M_K(P) + \log S_K(P) \} \text{ となる.}$$

J を $\mathcal{C}$ のヤコビ多様体. ψ を $\mathcal{C} \rightarrow J$ への rational map とする。

$\mathcal{C}(K) \neq \emptyset$ なら ψ, J とともに K 上定義されることが知られているので $\mathcal{C}(K) \neq \emptyset$ と仮定する。($\mathcal{C}(K) = \emptyset$ なら そもそも以下の定理は無意味。)

J は K 上 $\mathbb{P}^N$ に埋められるとし。

有限個である $\mathcal{C}$ の無限遠点 ($X_n = 0$ となる点) P_∞ について

$\psi(P_\infty) \in J(\mathbb{Q})$ であることはわかるが $\psi(P_\infty) \in J(K)$

まで仮定する。(即ち K を適当に有限次拡大しておく。)

$J(K)$ の生成元を固定する。 また $\ker \exp_J$ の

$\mathbb{R}$ -base となっている 1 組の基本周期 および T_J の基底を

固定する。 $r = \text{rank } J(K)$ と書く。

定理 2 J を simple と仮定する。 次のような正定数 C_2 が存在する。 $X_n(P) \neq 0$ なる任意の $P \in \mathcal{C}(K)$ に対し

$$h(P) < \frac{1}{[K:\mathbb{Q}]} \log \delta + C_2 (\log \log \Delta) (\log \log \log \Delta)^{r+4g+\frac{1}{g}}$$

この評価は $J \in \text{simple}$ と限らない [H2] Th 3.1 により決まる。

$$h(P) < \frac{1}{[K:\mathbb{Q}]} \log \delta + C'_2 (\log \log \Delta) (\log \log \log \Delta)^{g(r+4g)+1}$$

この定理2の C_2 は固定したすべての情報. 即ち $K, \psi, C \subset P^n$ の n のみ, $J \subset P^N$ の N のみ, C と J の定義方程式 (正確にはその係数の height の最大値), g, T_J の基底, $\ker \exp_J$ の 1 組の基本周期, $J(K)$ のランクと生成元の height による. C が楕円曲線の場合は [D] によりこの定数は explicit に表示されるので E を楕円曲線とすると $E(K)$ のランクと生成元が与えられる E の整数点を求めることが出来る. E の整数点のこの方法による求め方は N. Tzanakis が例を計算しているところである. (楕円曲線の場合には $K = \mathbb{Q}$ のとき Baker, Coates が K の有限次拡体の場合には Schmidt が Siegel の方法を用いて整数点の height を explicit に評価していることに注意しなければならない) この我々の求め方は [Z][Si] にも示されている.

この定理2は定理1' を用いて証明される [H3].

定理2において C_2 を explicit に書き下すことはなまやさしいことではない. ただいま努力中である.

また定理2の右辺の δ, Δ つまり $\delta_K(P)$ は S -integer では有限の値とならないのでこの定理2は S -integer では意味をもたない. S -integer に応用するには定理1の非アル

キメダスの絶対値への書きかえが必要であり、これも努力中である（決して自明でない）。

§ 5 超越数論における定量的定理と定性的定理の関係

K は代数体、 G を K 上の可換代数群、 $u \in T_G \in \exp_G u \in G(K)$ なる点とし、 $\mathcal{L}$ を K の元を係数とする T_G 上の 1 次形式とする。

我々の同時近似は次のような状況にある。

Wüstholz の定性的定理 [Wü]

ある条件 $\Rightarrow \mathcal{L}(u) \neq 0$

我々の同時近似 [H1] の系

上と同じ条件 $\Rightarrow |\mathcal{L}(u)| > \exists c > 0$

従って [H1] が [Wü] を含むことは自明である。[H1] は同時近似であるが、同時にない単なる近似において筆者の前の近似の証明には [Wü] を用いているのでもちろん [Wü] は含まれていると言えない。[H1] で筆者ははじめに [Wü] を含む結果を示せた。（[H1] は Philippon - Waldschmidt の近似の改良となるが、彼らの言及はすべて [Wü] を含んでいる。）

文献

- [D] S. David "Minors de formes linéaires de logarithmes elliptiques" Preprint
- [H1] N. Hirata-Kohno "Approximations simultanées sur les groupes algébriques commutatifs" Compositio Math. (to appear)
- [H2] N. Hirata-Kohno "Une relation entre les points entiers sur une courbe algébrique et les points rationnels de la jacobienne" The proceedings of the 3rd Canadian Number Theory Conference (to appear)
- [H3] N. Hirata-Kohno "Les points entiers sur une courbe algébrique ayant la jacobienne simple" (to appear)
- [Si] J. H. Silverman "The arithmetic of elliptic curves" GTM 106 Springer (1986)
- [Z] D. Zagier "Large integral points on elliptic curves" Math. Computation 48 No. 177 (1987) 425-436