数理解析研究所講究録
第837巻 1993年 101-111

Integer Points on Algebraic Curves

東工大理　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種類の方向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らによって行なわれてきた。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「高さ」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。

第二の方向は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さのeffectiveな評価を得ることができる。Bakerの近似を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は、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ーデルヴェイユ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, 筆者などによって考察されている。

本稿ではこの近似を同時近似に拡張したものを用いると、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 に限らないとき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 の定理を含むこ

とに注意する．

§2 Notations

$\overline{\mathbb{Q}}$を代数的数全体，Aを$\overline{\mathbb{Q}}$上定義された次元gのアーベル多様体とし，$\overline{\mathbb{Q}}$上のうめこみにより$\mathbb{P}^N$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 $\exp_A : T_A \longrightarrow A$ と $T_A \simeq \mathbb{C}^g$ の同一視及び $A \subset \mathbb{P}^N$ のうめこみを合成した $\mathbb{C}^g \longrightarrow \mathbb{P}^N$ への写像を改めて $\exp_A$ と書くことにする。 $\boldsymbol{z} = (z_1, \ldots, z_g) \in \mathbb{C}^g$ に対して $\|\boldsymbol{z}\| = (|z_1|^2 + \cdots + |z_g|^2)^{\frac{1}{2}}$ 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 $\mathrm{Min}\{\|u\| : \exp_A u = P\}$ によって定義する。 $\Omega := \mathrm{Ker}\exp_A$ の$\mathbb{R}$-baseとなっている1組の基本周期$(\omega_1, \ldots, \omega_{2g})$と$T_A$の基底を固定する．

K_0をA，Aのうめこみ，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 $(X_0(P), \ldots, X_N(P))$ と書いて $H_K(P) := \prod_{v \in M_K} \mathrm{Max}\{|X_0(P)|_v, \ldots, |X_N(P)|_v\}^{[K_v:\mathbb{Q}_v]}$

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 $P \neq O$ ならばその $d(P)$ が下から評価されるということを言っている。

定理 1　K_0 を有限次代数体，A を K_0 上定義された（次元 g の）アーベル多様体，O をその K_0 上の原点とし，K_0 上 $\mathbb{P}^N$ にうめこまれているとする。A を simple と仮定する。次のような effective 正定数 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 $P = n_1P_1 + \cdots + n_mP_m$ なる数とする。$N := \mathrm{Max}\{|n_1|, \dots, |n_r|, e^e\}$ とする．$u_i \in \mathbb{C}^g$ を $\exp_A u_i = P_i$ $(1 \le i \le m)$ とする。$g_{i,j}$ $(1 \le i \le m,\ 1 \le j \le 2g) \in \mathbb{R}$ を

$u_i = q_{i,1}\omega_1 + \cdots + q_{i,2g}\omega_{2g}$ なる数とする. $Q := \underset{\substack{1\le i\le m \\ 1\le j\le 2g}}{\mathrm{Max}} \{1, |q_{i,j}|\}$ とする. $V_1, \ldots, V_m, V \in \mathbb{R}$ を

$$\log V_i \geqq \mathrm{Max}\left(h(P_i), \frac{\|u_i\|^2}{D}, \frac{1}{D}\right) \quad (1\le i\le r)$$

$$\log V_i \geqq \mathrm{Max}\left(\frac{\|u_i\|^2}{D}, \frac{1}{D}\right) \quad (r< i\le m)$$

$$V = \mathrm{Max}\, V_i \quad (1\le i\le m)$$ とする.

このとき $P = O$ かもしくは

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

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

が成りたつ.

上の式の複雑さに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 及び Néron-Tate height の性質から出る [H2]).

定理 1′ K 代数体

A/K 次元 g のアーベル多様体 $\subset \mathbb{P}^N$, simple

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

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

このとき　$P = 0$ かもしくは　$\exists c_1' > 0$:

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

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

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

定理1′では

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

であった。ちなみにこの手の近似が定理1′で

$$\log d(P) > -C \log\log H$$

となり C もとても小さい数になると、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 → 改良

単なる近似……　Aがsimpleでなくてもよい

§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　代数体

C　curve$/K$　種数 $g \geqslant 1$．非特異完備．

K上のうめこみにより $C \subset \mathbb{P}^n$ となっているとする．

$C(K) := C \cap \mathbb{P}^n(K)$ とし．$(X_0, \ldots, X_n) \in \mathbb{P}^n$ 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 $P = (X_0(P), \ldots, X_{n-1}(P), 1) \in C(K)$ なる点を考察する。この $C \subset \mathbb{P}^n$ なるうめこみに関する logarithmic absolute height h および さきの H_K を考える．

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

$$M_K(P) := \prod_{v \in M_K^\infty} \mathrm{Max}\{|X_0(P)|_v, \ldots, |X_{n-1}(P)|_v, 1\}^{[K_v : \mathbb{Q}_v]}$$

$$\delta = \delta_K(P) := \prod_{v \in M_K \setminus M_K^\infty} \mathrm{Max}\{|X_0(P)|_v, \ldots, |X_{n-1}(P)|_v, 1\}^{[K_v : \mathbb{Q}]}$$

また $\Delta = \Delta_K(P) = \mathrm{Max}(\delta_K(P), e^{e^e})$ とする。

すると明らかに $H_K(P) = M_K(P)\cdot\delta_K(P)$ なので

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

J を $\mathcal{C}$ のヤコビ多様体，ψ を $\mathcal{C} \longrightarrow J$ への rational map とする。$\mathcal{C}(K) \neq \phi$ なら ψ，J とも K 上定義されることが知られているので $\mathcal{C}(K) \neq \phi$ と仮定する。（$\mathcal{C}(K) = \phi$ ならそもそも以下の定理は無意味。）J は K 上 $\mathbb{P}^N$ にうめこまれるとし，有限個である $\mathcal{C}$ の無限遠点（$X_n = 0$ に関する）P_∞ について $\psi(P_\infty) \in J(\overline{\mathbb{Q}})$ 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。またここで $\operatorname{Ker}\exp_J$ 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。$r = \operatorname{rank} J(K)$ 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 を simple と限らない [H2] Th 3.1 では次となる。

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

この定理2のC_2は固定したすべての情報，即ちK，ψ，$\mathcal{C}\subset\mathbb{P}^n$のうめこみ，$J\subset\mathbb{P}^N$のうめこみ，$\mathcal{C}$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，$\mathrm{Ker}\exp_J$の1組の基本周期，$J(K)$のランクと生成元のheightによる。$\mathcal{C}$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/Kを楕円曲線とすると$E(K)$のランクと生成元が与えられれば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では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が有限次代数体の場合には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に拡張するには定理1の非アル

キメデス的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を代数体、GをK上の可換代数群．$u \in T_G$を$\exp_G u \in G(K)$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で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]は含んでいると言えない。[H1]で筆者ははじめて[Wü]を含む結果を示せた。（[H1]はPhilippon‐Waldschmidtの近似の改良となるが、彼らの記述はすでに[Wü]を含んでいる。）

文献

[D] S. David "Minorations 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