数理解析研究所講究録
958巻 1996年 82-89

DIOPHANTINE APPROXIMATION ON ELLIPTIC CURVES

NORIKO HIRATA-KOHNO (平田典子. 日大理工)

Department of Mathematics, College of Science and Technology,
Nihon University, Suruga-Dai, Kanda, Chiyoda, Tokyo 101, Japan

ABSTRACT

In this paper we prove a refinement for a lower bound of linear forms in elliptic logarithms concerning with an exponential map assiciated to an algebraic group which contains a non-trivial extention of elliptic curves by the additive groups. This result improves the previous results of the author [H1] [H2] for such a special group and generalizes transcendence measures due to E. Reyssat [R].

1. Introduction

Let $\wp$ be Weierstrass' elliptic function with algebraic invariants g_2, g_3. For $1 \leq i \leq d$, let u_i be non-zero complex numbers such that either u_i is a period of $\wp$ or $\wp(u_i)$ is algebraic. Let $\beta_0, \beta_1, \cdots, \beta_d$ be algebraic numbers not all 0, and put

$$\Lambda = \beta_0 + \beta_1 u_1 + \cdots + \beta_d u_d.$$

In 1932, when $d = 1$, C. L. Siegel showed that there exists a non-zero period u_1 of $\wp$ such that $\Lambda \neq 0$. This means that there exists a transcendental period of $\wp$. Th. Schneider generalized this result in 1937 showing that we have always $\Lambda \neq 0$ when $d = 1$. D. W. Masser obtained in 1975 that for any d, if $\wp$ has complex multiplications, Λ does not vanish when $u_1, \cdots, u_d$ are linearly independent over the corresponding quadratic field of complex multiplications. In non-complex multiplications case, we have a theorem due to D. Bertrand and Masser which says that for any d, if $\wp$ has no complex multiplications, Λ does not vanish when $u_1, \cdots, u_d$ are linearly independent over $\mathbf{Q}$. Thses results correspond to an elliptic anlog of Baker's theorem on linear forms in usual logarithms.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Now a natural question is to make quantitative these transcendence results namely to give a lower bound for Λ when we have non-vanishing Λ. In 1951, N. I. Fel'dman gave a lower bound when $d = 1$ and u_1 is a period of $\wp$. Fel'dman in 1974 and Masser in 1975 obtained lower bounds for Λ if $d = 2$, $\beta_0 = 0$ and u_1, u_2 are period of $\wp$. When $\wp$ has complex multiplications, Masser showed a lower bound for Λ for any d if $\beta_0 = 0$. Coates-Lang theorem in 1976 refined Masser's bound, and Masser improved in 1978 their bound. In no complex multiplications case for any d, the first bound is due to P. Philippon and M. Waldschmidt (1988); in fact, their lower bound is not only both with complex multiplications and without complex multiplications cases of elliptic function, but also for exponential maps associated with any commutative algebraic groups defined over an algebraic number field. In 1991, the author refined Philippon-Waldschmidt lower bound when $d \geq 2$ (when $d = 1$, Baker's bound is already best possible for the height of coefficients $\beta's$). We remark that the author's lower bound of 1991 is exactly the same as Masser's lower bound of 1978 for dependence of the height of coefficients $\beta's$ if we retrict the situation to elliptic case with complex multiplications, and also that the author's is the first lower bound which gives an "up to ε" best possible bound for any $d \geq 2$ and for any commutative algebraic groups, especially in elliptic case with no complex multiplications (see a histrical survey for example in [B] and [H1]).

Now we return to our primitive question if we can give any lower bound for Λ which is really best possible for dependence of the height of coefficients $\beta's$ in elliptic case. We are looking for any example that has better bound than the author's bound, and there exist some bounds due to E. Reyssat [R] when $d = 1$, which give slightly refined bounds than the author's when the algebraic group is an extension of elliptic curves by the additive groups. Thus our motivation is to see if we can adapt this special better phenomenon to our situations. We restrict us to the case where the points u_i are not only the periods of $\wp$ (the period case is to be treated by completely different method of Choodnovsky) and we obtain a slight refinement for any d when our algebraic group contains an extension of elliptic curves by the additive groups.

Notations and results

Let K be a number field of degree D over $\mathbf{Q}$. For $d \geq 2, d \in \mathbf{Z}$, let $E_2, \cdots, E_d$ be elliptic curves defined over K, supposed to be defined by Weierstrass' equation

$$E_i : y^2 = 4x^3 - g_{2,i}x - g_{3,i}$$

with $g_{2,i}, g_{3,i} \in K \quad (2 \leq i \leq d)$.

For each i, $2 \leq i \leq d$, let $\wp_i$ be Weierstrass' elliptic function attached to E_i and be

$$\Omega_i = \omega_{1,i}\mathbf{Z} + \omega_{2,i}\mathbf{Z}$$

the period lattice of $\wp_i$. Let ζ_i be Weierstrass' zeta function associated to $\wp_i$. We assume that E_i and E_j are non-isogenous over K for $2 \leq i < j \leq d$. Let G_1 be a non trivial extension of E_2 by $\mathbf{G}_a$, namely obtained by

$$0 \longrightarrow \mathbf{G}_a \longrightarrow G_1 \longrightarrow E_2 \longrightarrow 0$$

with $\exp_{G_1}(z_1, z_2) = (P_2(z_2), z_1 + a\zeta_2(z_2))$ where $a \in K, a \neq 0$ and $P_2(z_2) = (1, \wp_2(z_2), \wp_2'(z_2)) \in \mathbf{P}^2$.

We identify $\mathbf{C}^d$ with $T_{G_1}(\mathbf{C}) \oplus T_{E_3}(\mathbf{C}) \oplus \cdots \oplus T_{E_d}(\mathbf{C})$, which is a direct sum of tangent spaces of $G_1, E_3, \cdots, E_d$ at the origins. Put $G = G_1 \times E_3 \times \cdots \times E_d$. We consider also $\exp_G$ an exponential map of G, normalized as above, namely composed with an embedding of G into a projective space and with an identification of tangent spaces and $\mathbf{C}^d$, written by

$$\exp_G : (z_1, \cdots, z_d) \longrightarrow (P_2(z_2), z_1 + a\zeta_2(z_2), P_3(z_3), \cdots, P_d(z_d))$$

with $P_i(z_i) = (1, \wp_i(z_i), \wp_i'(z_i)) \quad (2 \leq i \leq d)$.
We remark that this $\exp_G$ is polynomial in z_1.

For $\mathbf{z} \in \mathbf{C}^h, \mathbf{z} = (z_1, \cdots, z_h) \quad (1 \leq h \leq d)$, we write

$$\| \mathbf{z} \| = (| z_1 |^2 + \cdots + | z_h |^2)^{1/2}$$

the Euclidean norm on $\mathbf{C}^h$.

Let M_K the set of non-equivalent absolute values of K normalized such that for $x \in \mathbf{Q}$ and a prime $p \in \mathbf{Z}$, we have, $| x |_v = \max(x, -x)$ for infinite $v \in M_K$ and $| p |_v = 1/p$ for finite $v \in M_K$.
For $P = (p_0, p_1, \cdots, p_N) \in \mathbf{P}^N(K)$, define $H_K(P)$ by

$$H_K(P) = \prod_{v \in M_K} \max\{| p_0 |_v, \cdots, | p_N |_v\}^{N_v}$$

where $N_v = [K_v : \mathbf{Q}_v]$.
Let $h(P)$ be logarithmic absolute height defined by

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

(cf. [Si] Chap. 8)

Now we state a result on transcendence measures of elliptic logarithms which are not periods. This refines some previous transcendence measures concerning with height of the coefficients of linear forms.

Theorem.

There exists a constant $C_1 > 0$ which is effectively calculable which depends on the fixed data with the following properties.

Let $L(\mathbf{z}) = \beta_1 z_1 + \cdots + \beta_d z_d$ be a linear form on $\mathbf{C}^d$ with coefficients $\beta_i \in K - \{0\}$ $(1 \leq i \leq d)$.

For each $2 \leq i \leq d$ let $u_i \in \mathbf{C}$ satisfying $\gamma_i := (1, \wp_i(u_i), \wp_i'(u_i)) \in E_i(K)$.

Let $\mathbf{u}_1 = (u_1, u_2) \in \mathbf{C}^2$ such that $\gamma_1 := \exp_{G_1}(\mathbf{u}_1) \in G_1(K)$.

Let $B, E, V_1, V_3, \cdots, V_d, V$ be positive real numbers which satisfy

$$\log\ B \geq \max\left(h(\beta_i),\, e\right) \quad (1 \leq i \leq d)$$

$$\log\ V_i \geq \max\left(h(\gamma_i),\, \| u_i \|^2 /D, 1/D\right) \quad (3 \leq i \leq d)$$

$$\log\ V_1 \geq \max\left(h(\gamma_1),\, \| u_1 \|^2 /D, 1/D\right)$$

$$V = \max\ V_i \quad (i = 1, 3, \cdots, d)$$

$$e \leq E \leq \min\{e \cdot (D \log V_i)^{1/2} / \| u_i \|,\ e \cdot (D \log V_1)^{1/2} / \| u_1 \| \quad (3 \leq i \leq d)\}.$$

If $\Lambda := \beta_1 u_1 + \cdots + \beta_d u_d \neq 0$, then we have

$$\begin{aligned}\log |\, \Lambda \,| > & -C_1 D^{2d+2}(\log(BE) + (\log D)^2 + \log V(\log\log V)^2) \\ & \times \{\frac{\log\log B + \log(DE) + \log\log V}{\log E}\}^d \\ & \times \prod_{i=3}^{d}(\log V_i) \times (\log V_1) \times (\log E)^{-d+1}.\end{aligned}$$

When $d = 2$, our theorem gives a transcendence measure, same as (4) of [R] concerning with the height of $\beta' s$.

Corollary.

Let $\beta \in K - \{0\}$ and $u \in \mathbf{C}$ such that $\gamma := (1, \wp_2(u), \wp_2'(u)) \in E_2(K)$.

Let B be a positive real number with

$$\log\ B \geq \max(h(\beta),\, e).$$

There exists a constant $C_2 > 0$ which is effectively calculable, independent of B satisfying that, if $u - \beta\zeta_2(u) \neq 0$, then

$$\log |\, u - \beta\zeta_2(u) \,| > -C_2 \log B(\log\log B)^2.$$

2. Outline of the proof

We now turn to give an outline of the proof. The idea is as follows:the exponential map of our group G is polynomial in terms of z_1, then we can use the idea of Fel'dman which is based on the fact that the t-times derivative of $\exp_G$ by z_1 vanishes if t is greater than the degree of z_1. In general, to use this trick, we have to add one factor $\mathbf{G}_a$ to the algebraic group as in [H1] and [H2]. However, in our case, the group G already inculdes one $\mathbf{G}_a$, therefore we can improve one factor of $\log\log B$ in the lower bound. For this, we need a new zero estimate on G_1 due to P. Philippon [P] which allows us to treat separately the part over $z_1 + a\zeta_2(z_2)$ and the other part over $\wp_2(z_2)$, although G_1 is not a direct product of $\mathbf{G}_a$ and E_2. Our statement spoils the factor V, E and D. This is because the new zero estimate requires us that the degree for the part over $z_1 + a\zeta_2(z_2)$ should be greater than the degree for the part over $\wp_2(z_2)$ in our auxiliary function.

Choice of parameters

We choose a constant $c_0 > 0$ which depends on $d, g_{2,i}, g_{3,i} (2 \le i \le d), a$, the fixed idendification of a tangent space and a complex plane, the fixed embedding of G into a projective space, but independent of the parameters $B, V_1, V_3, \cdots, V_d, E, D$. We suppose that this constant c_0 is sufficiently large, much larger than other constants. Denoting by $[x]$ the largest integer part of a real number x, we define parameters $S, S_0, T, T_0, U, U_0, L_1, \cdots, L_d$ as follows.

$$S = \left[\frac{c_0^5 D(\log\log B + \log(DE) + \log\log V)}{\log E}\right]$$

$$S_0 = [S/(c_0)^2]$$

$$\begin{aligned} U_0 = {} & c_0^{9d} D^{2d}(\log(BE) + (\log D)^2 + \log V(\log\log V)^2) \\ & \left\{\frac{\log\log B + \log(DE) + \log\log V}{\log E}\right\}^d \\ & \cdot \log V_1 \cdot \prod_{i=3}^{d}(\log V_i) \cdot (\log E)^{-d+1}. \end{aligned}$$

Let $U > 0$ be a real number. We put also

$$L_1' = \frac{U}{c_0^5 D^3(\log B + (\log(DE))^2 + \log V(\log\log V)^2)}$$

$$L_1 = [L_1']$$

$$L_2' = \frac{U}{DS^2(\log V_1)}$$

$$L_2 = [L_2']$$

$$L_i' = \frac{U}{DS^2 \log V_i} \quad (3 \le i \le d)$$

$$L_i = [L_i'] \quad (3 \le i \le d).$$

For $U' = \max(U, U_0)$, put

$$T' = \frac{U'}{c_0 D(\log\log B + \log(DE) + \log\log V)}$$

$$T = [T']$$

$$T_0 = [T/(c_0)^2].$$

These parameters are different from those in [H1] [H2], in fact, U_0 has one less factor $\log\log B$ because of Fel'dman's idea. However, this has one more $\log(DE)$ and one more $\log V \log\log V$, which come from the condition for new zero estimete.

Base of hyperplane

For $L(\mathbf{z}) = \beta_1 z_1 + \cdots + \beta_d z_d$ the linear form on $\mathbf{C}^d$, put $W = \ker L$. Thanks to Liouville's inequality, we may suppose that W is defined by $W = \ker L_1$ for $L_1(\mathbf{z}) = -z_1 + \beta_2' z_2 + \cdots + \beta_d' z_d$ with $\beta_i' = \beta_i/\beta_1 \quad (2 \le i \le d)$. Then we can associate two systems of basis $\mathbf{E}$ and $\mathbf{W}$ to W :

$$\mathbf{E} = (\mathbf{e}_1, \cdots, \mathbf{e}_{d-1})$$

$$\mathbf{W} = (\mathbf{e}_1, \cdots, \mathbf{e}_{d-2}, \mathbf{w},)$$

with $\mathbf{e}_i = (\beta_i', 0, \cdots, 1, 0, \cdots, 0)$ where 1 is the $(i+1)$-th coordinate in $\mathbf{C}^d$, and $\mathbf{w} = (\beta_2' u_2 + \cdots + \beta_d' u_d, u_2, \cdots, u_d)$. For $\mathbf{u} = (u_1, \cdots, u_d)$, we have $\| \mathbf{w} - \mathbf{u} \| = | \Lambda |$.

We prove the theorem as the main theorem in [H1], but with lower dimensional space $\mathbf{C}^d$ than [H1]. The step in Liouville's inequality goes well as in [H1] because our auxiliary function is also polynomial in z_1. The last essential step of the proof is the zero estimate of Philippon, which can be stated in a simple manner as follows in our case, for, any proper algebraic subgroup of G is 0 under our assumptions.

Zero estimate

We state the following lemme under our notations and assumptions, derived from a special case of Philippon's zero estimates (Theorem 8 and Theorem 9 in [P]).

Lemma.

If there exists a non-zero polynomial P of multi-degrees $\leq L_1, L_2, \cdots, L_d$ on the group $G = G_1 \times E_2 \times \cdots \times E_d$, which vanishes at the points

$$\Gamma(S) := \{\exp_G(s\mathbf{u}); s \in \mathbf{Z}, 0 \leq s < S\}$$

with multiplicity $\geq T$ along the hyperplane W, then there exists a constant $C_3 > 0$ which is effectively calculable, independent of the parameters, satisfying

$$T^{d-1} \cdot \sharp(\Gamma(S/d)) < C_3 L_1 \cdot L_2 \cdots L_d.$$

We remark that this lemme can be used when the condition on the degree : $L_1 \leq L_2$, is verified. Our choice of parameters satisfies this condition, therefore the lemma allows us to give a contradiction in the last step of usual transcendence proof.

In our previous situations, the zero estimate could only derive

$$T^{d-1} \cdot \sharp(\Gamma(S/d)) < C_3 (M_1)^2 \cdot L_3 \cdots L_d$$

where $M_1 = \max(L_1, L_2)$, because we could not separate the degree parts on one algebraic group G_1.

With this previous estimate, we do not benefit the fact that the degree L_1 is much less than de degree L_2, then get no refinements. The new estimate is obtained by combining Theorem 8 and Theorem 9 in [P], indeed, the degree of the subgroup in Theorem 8 is written separately in two parts, say, in linear part and in elliptic part, by Theorem 9. By using the same idea, we are able to treat abelian case, not only elliptic case, and also with extra factors of multiplicative groups.

REFERENCES

[B] A. Baker, *Transcendental Number Theorey (Cambridge Math. Library series)*, Cambridge Univ. Press, Cambridge New York (1975).

[H 1] N. Hirata-Kohno, *Formes linéaires de logarithmes de points algébriques sur les groupes algébriques*, Invent. Math., 104 (1991), 401-433.

[H 2] N. Hirata-Kohno, *Approximations simultanées sur les groupes algébriques commutatifs*, Compositio Math., 86 (1993), 69-96.

[P] P. Philippon, *Nouveaux lemmes de zéros dans les groupes algébriques commutatifs*, preprint.

[R] E. Reyssat, *Approximation algébrique de nombres liés aux fonctions elliptiques et exponentielle*, Bull. Soc. Math. France 108 (1980), 47-79.

[Si] J. H. Silverman,, *The arithmetic of elliptic curves*, GTM 106, Springer, Berlin Heidelberg New York (1986).