数理解析研究所講究録
第 1710 巻 2010 年 180-191

p-adic logarithmic functions and applications

Noriko Hirata-Kohno
平田典子（日大理工）

Department of Mathematics,
College of Science and Technology, Nihon University, Tokyo
hirata @ math.cst.nihon-u.ac.jp

Abstract We explain how we define p-adic logarithmic functions to provide a new lower bound for linear forms in two p-adic elliptic logarithms proven in [11] . We adapt the argument that relies on the interpolation method on the variable change introduced by G. Chudnovsky, and on Faà-di-Bruno's formula adapted to matrices whose elements are p-adic elliptic logarithmic functions.

1 Introduction

Let K be a number field of finite degree D over $\mathbb{Q}$. Denote the ring of integers by $\mathfrak{O}$. Let $A, B \in K$, $\Delta := 4A^3 - 27B^2 \neq 0$ and $\mathcal{E}$ be an elliptic curve defined by

$$Y^2 = X^3 - AX - B.$$

We may assume $A, B \in \mathfrak{O}$ (for; if A or $B \notin \mathfrak{O}$, then there exists a suitable $c \in \mathfrak{O}$ such that the elliptic curve $Y^2 = X^3 - A'X - B'$ with $A' = c^4 A \in \mathfrak{O}$, $B' = c^6 B \in \mathfrak{O}$ and with the discriminant $\Delta' = c^{12}\Delta$, is isomorphic to $\mathcal{E}$ since the j-invariant remains equal under these multiplications).
Let us denote by $\overline{\mathbb{Q}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let p be a rational prime $\in \mathbb{Q}$ and $|\cdot|_\infty$ be an Archimedean valuation on K. For a place v of K over p, we write the valuation $|\cdot|_v$ normalized such that $|x|_v = p^{-ord_p(x)}$ for $x \in \mathbb{Q}$. Denote K_v the completion of K by v, and write $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ by p. The field K_v is a finite extension of $\mathbb{Q}_p$ of local degree $n_v = [K_v : \mathbb{Q}_p]$ with $\sum_{v|p} n_v = D$. Put $\mathbb{C}_p$ the completion of the

algebraic closure of K_v. We note that the algebraic closure of K_v is not complete itself. It is well-known that $\mathbb{C}_p$ is algebraically closed complete field of characteristic 0, in which the algebraic closure of K_v is dense and that there are D distinct embeddings of K into $\mathbb{C}_p$. Denote again by $|x|_v$ the extension of $|x|_v$ on $\mathbb{C}_p$.
For $\underline{x} \in \mathbb{P}_N(\overline{\mathbb{Q}})$ having coordinates $\underline{x} = (x_0, \dots, x_N) \in \mathbb{P}_N(K)$, define *the absolute logarithmic height* of $\underline{x}$ by

$$h(\underline{x}) = \frac{1}{[K:\mathbb{Q}]} \sum_v n_v \log(\max\{|x_0|_v, \dots, |x_N|_v\})$$

where the sum runs over all the normalized places of K. This definition is independent of the choice of the projective coordinates and the choice of the field containing $x_0, \dots, x_N$.

Let $a \in \overline{\mathbb{Q}}$ and put $h(a) := h(1:a)$, the absolute logarithmic height of the algebraic number a. We may write $h(a) = h_\infty(a) + h_f(a)$ where the sum in $h_\infty(a)$ runs over all the infinite places and the sum in $h_f(a)$ runs over all the finite places:

$$h_\infty(a) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \text{ infinite}} n_v \log(\max\{1, |a|_v\}),$$

$$h_f(a) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \text{ finite}} n_v \log(\max\{1, |a|_v\}).$$

Now we fix a place v over p and denote $|\cdot| = |\cdot|_v$. For a formal power series $f(z) = \sum_{k=0}^{\infty} a_k z^k \in \mathbb{C}_p[[z]]$, $f(z)$ converges at $z \in \mathbb{C}_p$ if and only if $|a_k z^k| \to 0$. It is known that the radius of convergence is also given by Hadamard's formula.

Let us recall the Lutz-Weil p-adic elliptic function which corresponds to the p-adic version of the Weierstraß elliptic function $\wp$. Consider $\mathcal{E}$ be an elliptic curve $\subset \mathbb{P}^2(\mathbb{C}_p)$:

$$ZY^2 = X^3 - AXZ^2 - BZ^3 \quad (A, B \in \mathfrak{O},\ 4A^3 \neq 27B^2).$$

Write $\lambda_p = \dfrac{1}{p-1}$ if $p \neq 2$, $\lambda_2 = 3$, $\mathcal{C}_p := \{z \in \mathbb{C}_p : |z| < p^{-\lambda_p}\}$ and $\mathcal{C}_v := \mathcal{C}_p \cap K_v$.

It is known that there exist two solutions φ and $-\varphi$ to the differential equation $(\varphi')^2 = 1 - A\varphi^4 - B\varphi^6$ with $\varphi(0) = 0$, defined over $\mathcal{C}_v \to K_v$, analytic in $\mathcal{C}_v$, after [18] [26]. In fact putting $\varphi^2 = \dfrac{1}{\wp_\varphi}$ we have $\left(\dfrac{\wp'_\varphi}{2}\right)^2 = \wp_\varphi^3 - A\wp_\varphi - B$ and $\varphi'(0) = 1$. The function $\varphi(z)$ is called *the Lutz-Weil p-adic elliptic function.* The elliptic curve can be given the structure of the p-adic Lie-group $\mathcal{E}(\mathbb{C}_p) \subset \mathbb{P}^2(\mathbb{C}_p)$ as follows. We may enlarge the domain of the definition of the function φ to $\mathcal{C}_p$ (*see e. g.* the page 151 of [1] and [2], [23]).

Definition 1.1 *For the p-adic Lie-group $\mathcal{E}(\mathbb{C}_p) \subset \mathbb{P}^2(\mathbb{C}_p)$ we have the exponential map:*

$$\exp = \exp_{\mathcal{E}} : \mathcal{C}_p \to \mathcal{E}(\mathbb{C}_p) \subset \mathbb{P}^2(\mathbb{C}_p)$$

$$z \mapsto (\varphi(z), -\varphi'(z), \varphi^3(z))$$

The p-adic exponential map is locally analytic only. The function φ is odd and injective; indeed, $|\varphi(z)| = |z|, |\varphi'(z)| = 1$ for any $z \in \mathcal{C}_p$, hence $\exp_{\mathcal{E}}$ has no period [3]. There are corresponding addition formula and derivation formula, similar to those of $\wp$.
Let $\beta \in K$. Take u_1 and u_2 in $\mathcal{C}_p$. We assume $\varphi^2(u_i)$ and $\frac{\varphi}{\varphi'}(u_i) \in K$ $(i = 1, 2)$ *i. e.* $\exp(u_i) \in \mathcal{E}(K)$ $(i = 1, 2)$. Put $\Lambda = \beta u_1 - u_2$ which is a linear form in two p-adic elliptic logarithms u_1 and u_2. Write $\hat{h}(P) := \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$ the Néron-Tate height defined on $\mathcal{E}$ for a rational point $P \in \mathcal{E}(K)$.
We may suppose that none of these 3 numbers β, u_1, u_2 equals to 0, for, otherwise our statement trivially follows thanks to the Liouville inequality: $|\alpha| \geq e^{-[K:\mathbb{Q}]h(\alpha)}$ where $\alpha \in K, \alpha \neq 0$.

Denote non-negative real numbers $h_1, h_2, h_3, \rho, E, a_1, a_2, b$ and d by $h_i = \hat{h}(\exp(u_i))$ $(i = 1, 2)$, $h_3 = \max\Big(1, h(\beta)\Big)$, $\rho = p^{-\lambda_p}$, $E = \rho/\max(|u_1|, |u_2|)$, $a_1 = \max\Big(1, h_1\Big)$, $a_2 = \max\Big(1, h_2\Big)$, $d = \max\Big(1, \frac{[K:\mathbb{Q}]}{\log E}\Big)$, $g = \max\Big(1, h_4, \log(h_1), \log(h_2), \log(d)\Big)$. We denote further by $h = h_4 = h(\mathcal{E}) := \max\{1, h(1, A, B)\}$ the height of the elliptic curve $\mathcal{E}$.

Our proncipal result is as follows.

Theorem 1.1 *[with R. Takada] Under the assumptions above, if we have*

$$|\Lambda| \leq \exp(-1.16 \times 10^{35} \times a_1 \cdot a_2 \cdot h_3 \cdot g^3 \cdot d^6 \cdot \log E),$$

then we obtain

$$\Lambda = 0$$

and $\beta = \frac{u_2}{u_1}$ is an algebraic number of degree at most 2 over $\mathbb{Q}$ with

$$h(\beta) \leq \log\Big(5.89 \times 10^{17} \times g^2 d^3 \times \max(a_1, \sqrt{a_1 a_2})\Big).$$

Corollary 1.1 *Whenever we have $\Lambda \neq 0$, then we obtain*

$$|\Lambda| > \exp(-1.16 \times 10^{35} \times a_1 \cdot a_2 \cdot h_3 \cdot g^3 \cdot d^6 \cdot \log E).$$

We compare our result with that of G. Rémond and F. Urfels.
Put $b = \max\Big(h_3, h_4, h_1, h_2, d\Big)$ and $c = \max(1, h_4, \log b)$. The result in [20] shows, if

$$|\Lambda| \leq \exp(-5.7 \times 10^{26} \times a_1 \cdot a_2 \cdot b \cdot c^3 \cdot d^6 \cdot \log E),$$

then

$$\Lambda = 0$$

and $\beta = \dfrac{u_2}{u_1}$ is an algebraic number of degree at most 2 over $\mathbb{Q}$ of height

$$\log(4.29 \times 10^{14} \times c^2\, d^3 \times \max(a_1, \sqrt{a_1\, a_2})).$$

We refine this result so as to obtain the best possible approximation concening with the height of algebraic coefficients of the linear forms since our bound does not contain $\log h_3$. Our constant is expressed in an explicit manner and the part of h_3 is separately written from other data. However, our numerical constant is larger than that of the statement of [20].

2 p-adic elliptic logarithmic function

We define the p-adic logarithmic function in elliptic case as a reversed function of the $\exp_{\mathcal{E}}$ with an expression of Formal group over $\mathfrak{O}$, following [15] [24] (see also [6][7]).

Let $P = (X, Y, 1) \in \mathcal{E}(K)$. Put $t = t(P) = -X/Y$, $\omega(t) = -1/Y$. We have $P = (X, Y, 1) = (t, -1, \omega(t)) = \left(\dfrac{\varphi(z)}{\varphi'(z)}, -1, \dfrac{\varphi^3(z)}{\varphi'(z)}\right)$. Let r be a positive real number. We put $\mathcal{E}(r)$ the set of points P in $\mathcal{E}(K)$ with $|t(P)| \leq p^{-r}$. We include the origin in $\mathcal{E}(r)$ by convention, and then $\mathcal{E}(r)$ is a subgroup of $\mathcal{E}(K)$. Denote by $\mathfrak{p}_r$ the set of elements $t \in K$ with $|t| \leq p^{-r}$. The map $P \to t(P)$ establishes a bijection between $\mathcal{E}(r)$ and $\mathfrak{p}_r$ (Theorem 3.2, Chapter III, [15]). There is a power series expansion of $\omega(t)$ in t where the coefficients are polynomials in A, B with coefficients in $\mathbb{Z}$ (Theorem 3.1, Chapter III, [15]). This power series expansion is studied in [7]. Below we rewrite estimates obtained in [7].

Lemma 2.1 *Under the notations above, we have* $\omega(t) = \sum_{n \geq 3} A_n t^n$ *where* $A_n \in \mathbb{Z}[A, B]$

is homogeneous of degree $n-3$ (of weights 4,6 on A, B) of form $A_3 = 1$ and

$$A_n = \sum_{\substack{4\lambda+6\mu=n-3,\\ \lambda,\mu\geq 0}} a_{\lambda,\mu}^{(n)} A^\lambda B^\mu \ ,$$

where $a_{\lambda,\mu}^{(n)} \in \mathbb{Z}$ with

$$|a_{\lambda,\mu}^{(n)}|_\infty \leq \frac{3^3 \cdot 8^{n-3}}{n^3(\lambda+1)^3(\mu+1)^3} \quad (n \geq 3, \lambda \geq 0, \mu \geq 0) \ .$$

Moreover, we have

$$h(A_n) \leq 3n + (n-3)h \ .$$

This lemma yields the estimate of the height of Taylor coefficients for the functions

$$\varphi^2(z) = \frac{\omega(t)}{t} = \sum_{n\geq 3} A_n t^{n-1},$$

$$\frac{\omega(t)}{t^2} = \sum_{n\geq 3} A_n t^{n-2}.$$

Since $\exp_{\mathcal{E}}(z) = \left(\frac{1}{\varphi^2(z)}, \frac{-\varphi'(z)}{\varphi^3(z)}, 1\right) = (t, -1, \omega(t))$, the function $z = z(t)$ corresponds to the logarithmic function which is introduced in [15] (*see* [7] [24]). By writing X, Y in terms of t and $\omega(t)$, the differential form $\Omega(t) = \frac{dX}{2Y}$ is viewed as a formal power series in t, and we define as in [15][24] the formal integral $\log_{\mathcal{E}}(t) = \int \Omega(t)$. With this formal integral we have;

$$\int \Omega(t) = \int \frac{dX}{2Y} = \int \frac{d\left(\frac{1}{\varphi^2}\right)z(t)}{\left(\frac{-2\varphi'}{\varphi^3}\right)z(t)}dt = \int \frac{\left(\frac{-2\varphi'}{\varphi^3}\right)z(t)}{\left(\frac{-2\varphi'}{\varphi^3}\right)z(t)}z'(t)dt = z(t)$$

which is indeed the local reversed function around the origin, of the function $t = t(P) = -\frac{X}{Y} = \frac{\varphi(z)}{\varphi'(z)}$.

Definition 2.1 *Put* $\log_{\mathcal{E}}(t) = z(t)$. *We call the function an elliptic p-adic logarithmic function associate to $\mathcal{E}$.*

We rewrite the statement in [7] for convenience in explicit calculations below, by using $h = h(\mathcal{E})$:

Lemma 2.2 *The Taylor expansion of* $\log_{\mathcal{E}}(t)$ *is given by*

$$\log_{\mathcal{E}}(t) = z(t) = \sum_{n\geq 1} B_n t^n$$

where $B_1 = 1, B_n = \dfrac{C_n}{2n}, C_n = \displaystyle\sum_{\substack{4\lambda+6\mu=n-1,\\ \lambda,\mu\geq 0}} b_{\lambda,\mu}^{(n)} A^\lambda B^\mu \quad (n\geq 1)$ *with* $b_{\lambda,\mu}^{(n)} \in \mathbb{Z}$ *and*

$$|b_{\lambda,\mu}^{(n)}|_\infty \leq \frac{(2^5\cdot 3\cdot 5^2)^n}{(n+2)^3(\lambda+1)^3(\mu+1)^3} \quad (n\geq 1, \lambda\geq 0, \mu\geq 0).$$

Concerning the height, we have

$$h(C_n) \leq 9n + (n-1)h \ .$$

Moreover, the domain of convergence of $\log_{\mathcal{E}}(t)$ *is* $\{z \in \mathbb{C}_p \ : \ |z| < 1\}$.

3 Differential operator

Consider a point $u = (0, u_1, u_2) \in \mathbb{C}_p \times \mathcal{C}_p^2$ and the hyperplane W defined by $z_0 = \beta z_1 - z_2$. To prove our theorem, with respect to the fixed non-Archimedean valuation $|\cdot| = |\cdot|_v$, we note that there is no restriction to suppose $|\beta| \leq 1$, otherwise we may consider $\frac{1}{\beta}u_2 - u_1$ instead of Λ.
We are going to look at (Λ, u_1, u_2). We choose as in [10] a basis of W: $(\beta, 1, 0)$ and $(-1, 0, 1)$. Put $\sigma = (\sigma_1, \sigma_2) \in \mathbb{Z}^2$, $\sigma_1, \sigma_2 \geq 0$, and a differential operator over ${\mathbb{C}_p}^3$ along W;

$$D_z^\sigma = \Big(\beta\frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_1}\Big)^{\sigma_1} \circ \Big(-\frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_2}\Big)^{\sigma_2}.$$

Introduce also a "divided differential operator" along W as in [8];

$$\Delta_z^\sigma := \frac{D_z^\sigma}{\sigma!} = \frac{D_z^\sigma}{\sigma_1!\sigma_2!} = \frac{1}{\sigma_1!\sigma_2!}\Big(\beta\frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_1}\Big)^{\sigma_1} \circ \Big(-\frac{\partial}{\partial z_0} + \frac{\partial}{\partial z_2}\Big)^{\sigma_2}.$$

Put $\tau = (\tau_0, \tau_1, \tau_2) \in \mathbb{Z}^3, \tau_0, \tau_1, \tau_2 \geq 0$ and define with $\psi = \varphi^2$;

$$f_\tau : \mathbb{C}_p \times \mathcal{C}_p^2 \to \mathbb{C}_p$$

$$(z_0, z_1, z_2) \to {z_0}^{\tau_0}\psi(z_1)^{\tau_1}\psi(z_2)^{\tau_2}.$$

For T_0, T_1, T_2, S_0, S_1 which are parameters ≥ 0 in $\mathbb{Z}$ with $S_0 \geq 5$, define a matrix

$$\mathcal{M} = (\Delta_z^\sigma f_\tau(su))_{\tau;(\sigma,s)} = (m_{\tau,\sigma,s}) \tag{1}$$

where the lines are indexed by $\mathcal{T} = \{\tau \in \mathbb{Z}^3 | 0 \leq \tau_i \leq T_i\}$, the columns by $\mathcal{S} = \{(\sigma, s) = (\sigma_1, \sigma_2, s) \in \mathbb{Z}^3 | \sigma_1 \geq 0, \sigma_2 \geq 0, |\sigma| := \sigma_1 + \sigma_2 < S_0, 0 \leq s \leq S_1\}$. The number of lines is $L := (T_0 + 1)(T_1 + 1)(T_2 + 1)$. The elements of the matrix are "divided derivatives" instead of the ordinary derivatives in [20].

4 Interpolation matrix

Lemma 4.1 *Let $D = [K : \mathbb{Q}]$. For any $L \times L$ minor determinant Δ of $\mathcal{M}$, we suppose;*

$$|\Delta| \leq \exp\Big(-D(\log(L!) - DL\Big(T_0(h_3 + 6) + 3.4S_0 \log(T_0 + 1) + (S_0 + 1)(18 + h_4)$$
$$+8S_1^2(T_1h_1 + T_2h_2) + (T_1 + T_2)(16h_4 + 60\log 2 + 12)\Big)\Big).$$

Then the rank of $\mathcal{M}$ is strictly less than L.

We remove $S_0 \log S_0$ in Proposition 6.1 of [20], that is essential for our improvement. For this, we carry out the variable change from z to t.

Now we assume that the rank of $\mathcal{M}$ equals to L. We shall show that there exists an $L \times L$ minor determinant $\Delta \neq 0$ of $\mathcal{M}$ and give a lower bound for $|\Delta|$ which contradicts the assumption of Lemma 4.1.

Recall that our matrix (1) is defined by $\mathcal{M} = (\Delta^\sigma f_\tau(su))_{\tau;(\sigma,s)}$ where

$$f_\tau = {z_0}^{\tau_0}\psi(z_1)^{\tau_1}\psi(z_2)^{\tau_2}, \quad \psi(z) = \varphi(z)^2.$$

Definition 4.1 *We order the set of the indices $(\sigma, s) = (\sigma_1, \sigma_2, s)$ of columns of $\mathcal{M}$ as follows. We order the set of $\sigma := (\sigma_1, \sigma_2)$ by the quantity $|\sigma| = \sigma_1 + \sigma_2$, namely if $|\sigma| < |\sigma'|$ then define $\sigma < \sigma'$. If $|\sigma| = |\sigma'|$ then we order lexicographically (σ_1, σ_2). We define an order for $(\sigma, s) = (\sigma_1, \sigma_2, s)$ firstly by the order defined above for σ and secondly by the order for s. Since the rank of $\mathcal{M}$ equals to L, then there exist L-tuple of the indices of columns such that the corresponding $L \times L$ minor determinant is non-zero. Choose the minimal L-tuple among such ones by the order defined now. We denote the minimal L-tuple by $(\sigma_\mu, s_\mu)_{1 \leq \mu \leq L}$. We put the corresponding square minimal matrix $\mathcal{N} = \left(m_{\tau,\sigma_\mu,s_\mu}\right)$ and denote $\Delta = \det \mathcal{N}$.*

We present some properties as follows [11].

Lemma 4.2 *For a fixed μ_0, every column of index $< (\sigma_{\mu_0}, s_{\mu_0})$ is contained in the subspace generated by the columns of index (σ_μ, s_μ) with $1 \leq \mu < \mu_0$.*

Lemma 4.3 *We have* $\det \mathcal{A} = \det \mathcal{N} = \Delta \neq 0$.

We are now going to give an upper bound for the height of the number $a_{\tau,\mu}$ by doing variable change of the functions "from z to t".

Lemma 4.4 *If $s = 0$, then we have*

$$a_{\tau,\mu} = m_{\tau,\sigma_\mu,0} = \Delta_z^{\sigma_\mu} f_\tau(0)$$
$$= \Delta_z^{\sigma_\mu}({z_0}^{\tau_0}\psi(z_1)^{\tau_1}\psi(z_2)^{\tau_2})(0) = b_{\tau,\sigma_\mu,0} + c_{\tau,\sigma_\mu,0}$$

with

$$b_{\tau,\sigma_\mu,0} = \frac{1}{\sigma_{\mu,1}!\sigma_{\mu,2}!}\left(\frac{\partial}{\partial t_1}\right)^{\sigma_{\mu,1}} \circ \left(\frac{\partial}{\partial t_2}\right)^{\sigma_{\mu,2}} (\beta z(t_1) - z(t_2))^{\tau_0}\left(\frac{\omega(t_1)}{t_1}\right)^{\tau_1}\left(\frac{\omega(t_2)}{t_2}\right)^{\tau_2}(0,0)$$

with exact order $|\sigma_\mu| = \sigma_{\mu,1} + \sigma_{\mu,2}$ for $b_{\tau,\sigma_\mu,0}$. The term $c_{\tau,\sigma_\mu,0}$ is a sum of the derivatives in $(t_1,t_2)$of order strictly inferior to $|\sigma_\mu|$.

Lemma 4.5 *If $s \neq 0$, then we have*

$$n_{\tau,\sigma_\mu,s_\mu} = \frac{1}{\sigma_{\mu,1}!\sigma_{\mu,2}!\psi(s_\mu u_1)^{T_1}\psi(s_\mu u_2)^{T_2}}\left(\frac{\partial}{\partial t_1}\right)^{\sigma_{\mu,1}} \circ \left(\frac{\partial}{\partial t_2}\right)^{\sigma_{\mu,2}} (F(z(t_1), z(t_2)))\,|_{t=0}$$
$$= d_{\tau,\sigma_\mu,s_\mu} + e_{\tau,\sigma_\mu,s_\mu}$$

with

$$F(z(t_1), z(t_2)) = (\beta z(t_1) - z(t_2))^{\tau_0}\left(\psi(z(t_1) - \psi(s_\mu u_1)\right)^{2\tau_1}$$
$$\times \left(\psi(z(t_2)) - \psi(s_\mu u_2)\right)^{2\tau_2} T(z(t_1), s_\mu u_1)^{T_1-\tau_1} T(z(t_2), s_\mu u_2)^{T_2-\tau_2}$$

and

$$d_{\tau,\sigma_\mu,s_\mu} = \frac{1}{\sigma_{\mu,1}!\sigma_{\mu,2}!\psi(s_\mu u_1)^{T_1}\psi(s_\mu u_2)^{T_2}}\left(\frac{\partial}{\partial t_1}\right)^{\sigma_{\mu,1}} \circ \left(\frac{\partial}{\partial t_2}\right)^{\sigma_{\mu,2}} (F(z(t_1), z(t_2)))\,|_{t=0}$$

with exact order $|\sigma_\mu| = \sigma_{\mu,1} + \sigma_{\mu,2}$ for $d_{\tau,\sigma_\mu,s_\mu}$. The term $e_{\tau,\sigma_\mu,s_\mu}$ is a sum of the derivatives in $(t_1,t_2)$of order strictly inferior to $|\sigma_\mu|$.

Lemma 4.6 *Put further*

$$\ell_{\tau,\sigma_\mu,s_\mu} = \begin{cases} b_{\tau,\sigma_\mu,0} & (\text{if } s_\mu = 0) \\ d_{\tau,\sigma_\mu,s_\mu} & (\text{if } s_\mu \neq 0) \end{cases} \tag{2}$$

and the new matrix

$$\mathcal{B} := (\gamma_{\tau,\mu}) := (\ell_{\tau,\sigma_\mu,s_\mu}).$$

Then we have $\det \mathcal{B} = \det \mathcal{A} = \det \mathcal{N} = \Delta$.

Now we are going to give a lower bound for the height of $\Delta = \det(\gamma_{\tau,\mu}) = \det(a_{\tau,\mu}) \neq 0$. We do not use the differential equation, as is done in [20]. We have then next Lemma to estimate the height of each $\gamma_{\tau,\mu}$.

Lemma 4.7 *Consider* $\gamma_{\tau,\mu}$ *namely either* $b_{\tau,\sigma_\mu,0}$ *or* $d_{\tau,\sigma_\mu,s_\mu}$. *Then we have*

$$h(\gamma_{\tau,\mu}) = \begin{cases} h(b_{\tau,\sigma_\mu,0}) \leq 3.4S_0 \log(T_0+1) + T_0 h_3 + 6T_0 + (S_0+1)(18+h_4) \\ \qquad +3(T_1+T_2), \\ h(d_{\tau,\sigma,s}) \leq 3.4S_0 \log(T_0+1) + T_0 h_3 + 6T_0 + (S_0+1)(18+h_4) \\ \qquad +(T_1+T_2)(16h_4 + 60\log 2 + 12) + 8S_1^2(T_1h_1 + T_2h_2). \end{cases} \tag{3}$$

Lemma 4.8 *We have*

$$h(\Delta) \leq \log(L!) + L\Big(T_0(h_3+6) + 3.4S_0\log(T_0+1) + (S_0+1)(18+h_4)$$
$$+8S_1^2(T_1h_1+T_2h_2) + (T_1+T_2)(16h_4 + 60\log 2 + 12)\Big).$$

By means of the Liouville inequality, we can complete the proof of Lemma 4.1.

5 Extrapolation

It is possible to prove;

Lemma 5.1 *Let* Δ *be an* $L \times L$ *minor determinant of* $\mathcal{M}$. *Suppose*

$$|\Lambda| \leq \exp\left(-\frac{L}{S_0}\log E\right) = E^{-L/S_0}.$$

Then we have

$$|\Delta| \leq \exp\left(-\frac{L}{2}\left(\frac{L}{S_0} - 2S_0 + 1\right)\log E\right). \tag{4}$$

Lemma 5.2 *Assume that there exist* $T_0, T_1, T_2, S_0, S_1 \in \mathbb{Z} \geq 0$ *with the following conditions.* $S_0 \geq 5$, $S_0 - 1 \in 3\mathbb{Z}$, $S_1 \in 3\mathbb{Z}$, $(S_0+2)(S_0+5)(S_1+3) > 2916T_0T_1T_2$, $(S_0+2)(S_0+5)(T_1+T_2) > 324T_0T_1T_2$, $(S_0+2)(S_1+3) > 81\max\{T_1, T_2\}$, $(S_0+2)(T_1+T_2) > 27T_1T_2$, $S_0+2 > 9T_0$. *Assume further* $\frac{L}{S_0} > \frac{D}{\log E} \times (2Q) + 2S_0 - 1$, $\frac{L}{S_0} > \frac{D}{\log E} \times R$ *with* $Q = \frac{\log(L!)}{L} + T_0(h_3+6) + 3.4S_0\log(T_0+1) + (S_0+1)(18+h_4) + 8S_1^2(T_1h_1 + T_2h_2) + (T_1+T_2)(16h_4 + 60\log 2 + 12)$ *and with* $R = 2\Omega_0^2 T_2(\frac{T_1h_1}{4} + T_2h_2) + \frac{13}{2}h_4 + \frac{53}{2}\log 2)$.
Now suppose

$$|\Lambda| \leq \exp\left(-\frac{L}{S_0}\log E\right).$$

Then we have $\Lambda = 0$.

We have to choose parameters to achieve the proof of the main theorem. We have $L \leq (T_0+1)(T_1+1)(T_2+1)$.
Put $T_0 = [c_0a_1a_2g^3d^5]$, $T_1 = [c_1a_2bgd^3]$, $T_2 = [c_2a_1bgd^3]$, $S_0 = 1 + 3[c_3a_1a_2bg^2d^5]$, $S_1 = 3[c_4gd]$, with absolute constants c_0, c_1, c_2, c_3, c_4.
Since the quantity Q only differs from the assumptions in [20], thanks to the calculations due in [20], it is sufficient to choose;

$c_0 = 2.13 \times 10^{28}$, $c_1 = c_2 = 9.85 \times 10^{16}$, $c_3 = 6.09 \times 10^{28}$, $c_4 = 5.50 \times 10^6$.
Thus we complete the proof of our main theorem since

$$\frac{(1+c_0)(1+c_1)(1+c_2)}{3c_3 - 2} \leq 1.16 \times 10^{35}$$

and

$$\frac{18c_0}{3c_3}\sqrt{c_2\max\left(\frac{c_1}{4}, c_2\right)} \leq 5.89 \times 10^{17}.$$

References

[1] D. Bertrand, *Algebraic Values of p-adic Elliptic Functions*, in: Transcendence theory: advances and applications, (eds. A. Baker and D.W. Masser), Academic Press, 1977, 149–159.

[2] D. Bertrand, *Problèmes locaux*, Appendix to *Nombres transcendants et groupes algébriques by M. Waldschmidt*, Astérisque, **69/70**, Soc. Math. de France, 1987.

[3] D. Bertrand, *Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe*, Compositio Math. **37**, 1978, 21–50.

[4] G. V. Chudnovsky, *Contributions to the theory of transcendental numbers*, Math. Soc. Math. Surveys Monographs, **19**, 1984.

[5] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mémoires, Nouvelle série 62, Supplément au Bulletin de la Soc. Math. de France, Tome **123**, Fascicule **3**, 1995.

[6] S. David and N. Hirata-Kohno, *Recent progress on linear forms in elliptic logarithms*, in: A Panorama of Number Theory, (ed. G. Wüstholz), Cambridge University Press, 2002, 26–37.

[7] S. David and N. Hirata-Kohno, *Logarithmic Functions and Formal Groups of Elliptic Curves*, In : Diophantine Equations, Tata Institute of Fundamental Research, Studies in Mathematics, Narosa Publishing House, 2008, 243–256.

[8] S. David and N. Hirata-Kohno, *Linear Forms in Elliptic Logarithms*, J. für die reine angew. Math., **628**, 2009, 37–89.

[9] N. I. Fel'dman and Yu. V. Nesterenko, *Number Theory IV*, (eds. A. N. Parshin and I. R. Schfarevich), Encyclopaedia of Mathematical Sciences **44**, Springer, 1998.

[10] N. Hirata-Kohno, *Formes linéaires de logarithmes de points algébriques sur les groupes algébriques*, Inventiones Math., **104**, 1991, 401–433.

[11] N. Hirata-Kohno and R. Takada, *Linear forms in two elliptic logarithms in the p-adic case*, accepted for publication in the Kyushu Journal of Mathematics, 2010.

[12] N. Hirata-Kohno, *Linear forms in p-adic elliptic logarithms*, preprint.

[13] K. Iwasawa, *Lectures on p-adic L-functions*, Ann. Math. Studies, **74**, Princeton, 1972.

[14] S. Lang, *Diophantine approximation on toruses*, Amer. J. Math., **86**, 1964, 521–533.

[15] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Math. Wissenschaften, **231**, Springer, 1978.

[16] M. Laurent, *Sur quelques résultats récents de transcendance*, Astérisque, **198/199/200**, Soc. Math. de France, 1991, 209-230.

[17] M. Laurent and D. Roy *Sur l'approximation algébrique en degré de transcendance un*, Ann. de l'institut Fourier Univ. Grenoble, **49-1**, 1999, 27–55.

[18] E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps p-adiques*, J. für die reine angew. Math., **177**, 1937, 237–247.

[19] K. Mahler, *p-adic numbers and their functions*, Cambridge University Press, Second edition, 1965.

[20] G. Rémond and F. Urfels, *Approximation diophantienne de logarithmes elliptiques p-adiques*, Journal of Number Theory, **57**, 1996, 133–169.

[21] J. B. Roser and L. Schönfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6**, 1962, 64–94.

[22] W. H. Schikhof, *Ultrametric calculus*, Cambridge Studies in Advanced Mathematics, **4**, Cambridge University Press, 1984.

[23] J. -P. Serre, *Quelques propriétés des groupes algébriques commutatifs*, Appendix to *Nombres transcendants et groupes algébriques by M. Waldschmidt*, Astérisque, **69/70**, Soc. Math. de France, 1987.

[24] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Text in Math., **106**, Springer, 1986.

[25] M. Waldschmidt, *Nombres transcendants*, Lecture Notes in Math. **402**, Springer, 1974.

[26] A. Weil, *Sur les fonctions elliptiques p-adiques*, C. R. Acad. Sc. Paris, t. **203**, 1936, 22–24.

[27] G. Wüstholz, *A Panorama of Number Theory*, Cambridge University Press, 2002.

[28] Kunrui Yu, *P-adic logarithmic forms and group varieties I*, J. für die reine angew. Math., **502**, 1998, 29–92.

[29] Kunrui Yu, *Report on p-adic logarithmic forms*, in: A Panorama of Number Theory, (ed. G. Wüstholz), Cambridge University Press, 2002, 11–25.