*Bull. Aust. Math. Soc.* **110** (2024), 234–243
doi:10.1017/S0004972724000091

# WEIERSTRASS ZETA FUNCTIONS AND *p*-ADIC LINEAR RELATIONS

**DUC HIEP PHAM**

(Received 13 October 2023; accepted 27 January 2024; first published online 11 March 2024)

**Abstract**

We discuss the $p$-adic Weierstrass zeta functions associated with elliptic curves defined over the field of algebraic numbers and linear relations for their values in the $p$-adic domain. These results are extensions of the $p$-adic analogues of results given by Wüstholz in the complex domain [see A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, New Mathematical Monographs, 9 (Cambridge University Press, Cambridge, 2007), Theorem 6.3] and also generalise a result of Bertrand to higher dimensions ['Sous-groupes à un paramètre $p$-adique de variétés de groupe', *Invent. Math.* **40**(2) (1977), 171–193].

2020 *Mathematics subject classification*: primary 11J89; secondary 11G07, 11S99.

*Keywords and phrases*: elliptic curve, Weierstrass zeta function, $p$-adic transcendence.

## 1. Introduction

Let $K$ be a subfield of the field of complex numbers $\mathbb{C}$. Let $E$ be an elliptic curve defined over $K$ by the Weierstrass form

$$Y^2Z - 4X^3 + g_2XZ^2 + g_3Z^3 = 0,$$

where $g_2, g_3$ are elements in $K$ satisfying $g_2^3 - 27g_3^2 \neq 0$. Let $e_1$ and $e_2$ be two roots among the three (distinct) complex roots of the polynomial $4X^3 - g_2X - g_3$. Put $\Lambda = \mathbb{Z}\omega_1^* + \mathbb{Z}\omega_2^*$ with

$$\omega_1^* = \int_{e_1}^{\infty} \frac{dx}{\sqrt{4x^3 - g_2x - g_3}} \quad \text{and} \quad \omega_2^* = \int_{e_2}^{\infty} \frac{dx}{\sqrt{4x^3 - g_2x - g_3}}.$$

Then $\Lambda$ is a lattice in $\mathbb{C}$. The elliptic function $\wp : \mathbb{C} \setminus \Lambda \to \mathbb{C}$ relative to $\Lambda$ is defined by

$$\wp(z) = \wp(z; \Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

This research has been done under the research project QG.23.48 'Some selected topics in number theory' of Vietnam National University, Hanoi.

This function is called the *Weierstrass elliptic function* associated with the elliptic curve $E$ and $\Lambda$ is called the *lattice of periods* of $\wp$ (or the lattice associated with $E$). The *Weierstrass zeta function* associated with $E$ (or relative to $\Lambda$) is the function $\zeta : \mathbb{C} \setminus \Lambda \to \mathbb{C}$ defined by

$$\zeta(z) = \zeta(z; \Lambda) := \frac{1}{z} + \sum_{\omega \in \Lambda \setminus \{0\}} \Big( \frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \Big).$$

The Weierstrass zeta function is related to the Weierstrass elliptic function by $\zeta' = -\wp$ and one can write the Laurent expansion at zero of $\zeta$ as

$$\zeta(z) = \frac{1}{z} - \sum_{k \geq 1} \mathcal{G}_{2k+2}(\Lambda) z^{2k+1},$$

where $\mathcal{G}_{2k+2}(\Lambda)$ is the Eisenstein series of weight $2k+2$ (with respect to the lattice $\Lambda$). By induction, $\mathcal{G}_{2k+2}(\Lambda)$ can be represented as a polynomial in $g_2, g_3$ with rational coefficients (see [5, Ch. IV]). In other words,

$$\zeta(z) = \frac{1}{z} + \sum_{k \geq 1} \alpha_k z^{2k+1}$$

with $\alpha_k \in \mathbb{Q}[g_2, g_3]$ for all positive integers $k$.

Since $\wp$ is a periodic function, it follows that $\zeta$ is a quasiperiodic function, that is, for each $\omega \in \Lambda$, there exists a complex number $\eta = \eta(\omega)$ satisfying $\zeta(z+\omega) = \zeta(z) + \eta$ for all $z \in \mathbb{C} \setminus \Lambda$. The number $\eta$ is called a *quasiperiod* of the elliptic curve $E$. If $(\omega_1, \omega_2)$ is a pair of fundamental periods of $\Lambda$ (that is, $\omega_1$ and $\omega_2$ are complex numbers generating $\Lambda$ over $\mathbb{Z}$), one can show that $\eta(a\omega_1 + b\omega_2) = a\eta_1 + b\eta_2$ for any integers $a, b$, where $\eta_1 = \eta(\omega_1)$ and $\eta_2 = \eta(\omega_2)$. Furthermore, in the case when the ratio $\omega_2/\omega_1$ has positive imaginary part, we obtain the *Legendre relation* between the periods and the quasiperiods:

$$\omega_2\eta_1 - \omega_1\eta_2 = 2\pi i.$$

Schneider was the first to give a transcendence result concerning linear relations between periods and quasiperiods, by showing that any nonvanishing linear combination of $\omega$ and $\eta$ over $\overline{\mathbb{Q}}$ is transcendental (see [12]). The result was extended by Coates to pairs of fundamental periods. He obtained a similar result for the numbers $2\pi i, \omega_1, \omega_2, \eta_1, \eta_2$, where $(\omega_1, \omega_2)$ is a pair of fundamental periods (see [6]). Masser established the dimension of the vector space generated by $1, 2\pi i, \omega_1, \omega_2, \eta_1, \eta_2$ over $\overline{\mathbb{Q}}$, proving that this dimension is either 4 if the elliptic curve $E$ has complex multiplication, or 6 otherwise.

In the 1980s, Wüstholz formulated and proved a celebrated theorem in complex transcendental number theory which is called *the analytic subgroup theorem* (see [1] or [15]). The theorem states that an analytic subgroup defined over $\overline{\mathbb{Q}}$ of a commutative algebraic group defined over $\overline{\mathbb{Q}}$ contains a nontrivial algebraic point if and only if it contains a nontrivial algebraic subgroup defined over $\overline{\mathbb{Q}}$. The analytic subgroup theorem has many significant consequences, some of which concern elliptic curves.

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

In particular, Wüstholz himself used the theorem to deduce a result on linear relations for the values of the Weierstrass zeta function $\zeta$ at algebraic points of the Weierstrass elliptic function $\wp$. Here, a complex number $u \in \mathbb{C} \setminus \Lambda$ is called an *algebraic point of* $\wp$ if $\wp(u) \in \overline{\mathbb{Q}}$. Let $\mathrm{End}(E)$ denote the ring of endomorphisms of $E$. Then it is known that $K := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ (*the field of endomorphisms of* $E$) is either $\mathbb{Q}$ or an imaginary quadratic field. The following theorem was given by Wüstholz (see [1, Theorem 6.3]).

THEOREM 1.1. *Let $E$ be an elliptic curve defined over $\overline{\mathbb{Q}}$ and $\gamma_1, \ldots, \gamma_n$ algebraic points of $\wp$. Denote by $W$ the vector space generated by $\gamma_1, \ldots, \gamma_n$ over $K$ and by $V$ the vector space generated by $1, 2\pi i, \gamma_1, \ldots, \gamma_n, \zeta(\gamma_1), \ldots, \zeta(\gamma_n)$ over $\overline{\mathbb{Q}}$. Then*

$$\dim_{\overline{\mathbb{Q}}} V = 2 \dim_K W + 2.$$

It is natural to extend this result to the $p$-adic case and the main goal of this paper is to establish an extension of the $p$-adic analogue of Theorem 1.1. To state it, let $E$ be an elliptic curve given by

$$Y^2 Z - 4X^3 + g_2 X Z^2 + g_3 Z^3 = 0,$$

now defined over $\mathbb{C}_p$ (that is, $g_2, g_3 \in \mathbb{C}_p$). Here, $\mathbb{C}_p$ denotes the completion of $\overline{\mathbb{Q}_p}$ with respect to the $p$-adic absolute value $|\cdot|_p$ as usual. Let $\wp_p$ be the *(Lutz–Weil) $p$-adic elliptic function* associated with the elliptic curve $E$ (see [9, 14]). The function $\wp_p$ is analytic on the set $\mathscr{D}_p \setminus \{0\}$, where $\mathscr{D}_p$ is the *$p$-adic domain of $E$* defined by

$$\mathscr{D}_p := \{z \in \mathbb{C}_p : |1/4|_p \max\{|g_2|_p^{1/4}, |g_3|_p^{1/6}\} z \in B(r_p)\}$$

with $B(r_p)$ the set of all $p$-adic numbers $x$ in $\mathbb{C}_p$ such that $|x|_p < r_p := p^{-1/(p-1)}$. As in the complex case, we say that a nonzero $p$-adic number $u \in \mathscr{D}_p$ is an *algebraic point of* $\wp_p$ if $\wp_p(u) \in \overline{\mathbb{Q}}$. Let $\zeta_p$ be the $p$-adic Weierstrass zeta function ($p$-adic analogue of the Weierstrass zeta function $\zeta$) associated with $E$ which is, by definition, the (unique) odd $p$-adic meromorphic function on $\mathscr{D}_p$ satisfying $\zeta_p' = -\wp_p$. Let $\mathrm{Log}_p : \mathbb{C}_p \setminus \{0\} \to \mathbb{C}_p$ be the Iwasawa logarithm (see [11, Ch. 5, Section 4.5]). We now state our main theorem.

THEOREM 1.2. *Let $E$ be an elliptic curve defined over $\overline{\mathbb{Q}}$. Let $u_1, \ldots, u_l$ be nonzero algebraic numbers and $v_1, \ldots, v_n$ algebraic points of $\wp_p$. Denote by $U$ the vector space generated by $\mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_l)$ over $\mathbb{Q}$ and by $V$ the vector space generated by $v_1, \ldots, v_n$ over the field $K$ of endomorphisms of $E$. Then the dimension of the vector space $W$ generated by $1, \mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_l), v_1, \ldots, v_n, \zeta_p(v_1), \ldots, \zeta_p(v_n)$ over $\overline{\mathbb{Q}}$ is determined by*

$$\dim_{\overline{\mathbb{Q}}} W = 1 + \dim_{\mathbb{Q}} U + 2 \dim_K V.$$

In the case when $l = n = 1$, we deduce at once from Theorem 1.2 the following result which is an extension of a result given by Bertrand in 1977 (see [2, Proposition 1]).

COROLLARY 1.3. *Let $E$ be an elliptic curve defined over $\overline{\mathbb{Q}}$. Let $u$ be a nonzero algebraic number with $\mathrm{Log}_p(u) \neq 0$ and $v$ an algebraic point of $\wp_p$. Let $\alpha$, $\beta$ and $\gamma$ be algebraic numbers not all zero. Then the number $\alpha \mathrm{Log}_p(u) + \beta v + \gamma \zeta_p(v)$ is transcendental.*

## 2. Extensions of commutative algebraic groups

In this section, let $K$ be a fixed algebraically closed field of characteristic 0. Let $A$ and $B$ be commutative algebraic groups defined over $K$. A commutative algebraic group $C$ defined over $K$ is called an *extension* of $A$ by $B$ if there is an exact sequence of commutative algebraic groups

$$0 \longrightarrow B \xrightarrow{i} C \xrightarrow{\pi} A \longrightarrow 0.$$

To give an extension $C$ of $A$ by $B$ is equivalent to giving a pair $(i, \pi) \in \mathrm{Hom}(B, C) \times \mathrm{Hom}(C, A)$ for which the above sequence is exact. Let

$$0 \longrightarrow B \xrightarrow{i} C \xrightarrow{\pi} A \longrightarrow 0$$

and

$$0 \longrightarrow B' \xrightarrow{i'} C' \xrightarrow{\pi'} A' \longrightarrow 0$$

be extensions of commutative algebraic groups. A homomorphism between the above two extensions is a triple of homomorphisms $\varphi : C \to C', \alpha : A \to A', \beta : B \to B'$ of algebraic groups such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \xrightarrow{i} & C & \xrightarrow{\pi} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\alpha} & & \\ 0 & \longrightarrow & B' & \xrightarrow{i'} & C' & \xrightarrow{\pi'} & A' & \longrightarrow & 0 \end{array}$$

commutes. Clearly, $\varphi$ is an isomorphism if and only if $\alpha$ and $\beta$ are isomorphisms. In the case $A = A', B = B'$ and $\alpha = \mathrm{id}_A, \beta = \mathrm{id}_B$, we say that the two extensions $C$ and $C'$ are *equivalent* if there is a homomorphism between them. The set of equivalence classes $[C]$ of extensions forms a commutative group $\mathrm{Ext}^1(A, B)$ with the neutral element $[A \times B]$ (via the Baer sum). We write $C$ for its equivalence class $[C]$ by abuse of notation. The bi-functor $\mathrm{Ext}^1$ which assigns to the pair $(A, B)$ the group $\mathrm{Ext}^1(A, B)$ is contravariant in the first variable and covariant in the second one. This means that if $\alpha : A' \to A$ and $\beta : B \to B'$ are homomorphisms between commutative algebraic groups, then they induce homomorphisms $\alpha^* : \mathrm{Ext}^1(A, B) \to \mathrm{Ext}^1(A', B)$ and $\beta_* : \mathrm{Ext}^1(A, B) \to \mathrm{Ext}^1(A, B')$. The two homomorphisms $\alpha^*$ and $\beta_*$ make the diagram

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

$$\begin{array}{ccc} \mathrm{Ext}^1(A,B) & \xrightarrow{\alpha^*} & \mathrm{Ext}^1(A',B) \\ \downarrow{\beta_*} & & \downarrow{\beta_*} \\ \mathrm{Ext}^1(A,B') & \xrightarrow{\alpha^*} & \mathrm{Ext}^1(A',B') \end{array}$$

commute. Furthermore, $\mathrm{Ext}^1$ is additive in both variables, which implies that

$$\mathrm{Ext}^1(A_1 \times A_2, B) = \mathrm{Ext}^1(A_1, B) \times \mathrm{Ext}^1(A_2, B)$$

and

$$\mathrm{Ext}^1(A, B_1 \times B_2) = \mathrm{Ext}^1(A, B_1) \times \mathrm{Ext}^1(A, B_2).$$

For example, we describe the exponential map of $G$ in the case where $G$ is an extension of an elliptic curve by the additive group $\mathbb{G}_a$ defined over $\overline{\mathbb{Q}}$ as given in [4]. (We refer the reader to [7] for the general case.) Let $E$ be an elliptic curve defined over $\overline{\mathbb{Q}}$ and let $G$ be an extension of $E$ by $\mathbb{G}_a$. By compactification,

$$0 \longrightarrow \mathbb{P}_1 \xrightarrow{\ i\ } \overline{G} \xrightarrow{\ \pi\ } E \longrightarrow 0.$$

Denote by 0 the identity element in $E$. The divisor $D = (\overline{G} - G) + 3\pi^*(0)$ is very ample for $\overline{G}$ and $l(D) = 6$. Hence, there is an embedding of $\overline{G}$ into $\mathbb{P}_5$, and one can express the exponential map of $G$ in terms of the Weierstrass elliptic and zeta functions $\wp(z), \zeta(z)$ associated with $E$. One can identify the Lie algebra $\mathrm{Lie}(G(\mathbb{C}))$ with $\mathbb{C}^2$ and the exponential map of $G$ is expressed by

$$\exp_{G(\mathbb{C})}(z,t) = (1 : \wp(z) : \wp'(z) : f_1(z,t) : f_2(z,t) : f_3(z,t)) \quad \text{for } z \notin \Lambda$$

and $\exp(z,t) = (0 : 0 : 1 : 0 : 0 : t + b\eta(z))$ for $z \in \Lambda$, where

$$f_1(z,t) = t + b\zeta(z), f_2(z,t) = \wp(z)f_1(z,t) + \frac{b}{2}\wp'(z), f_3(z,t) = \wp'(z)f_1(z,t) + 2b\wp^2(z)$$

for some algebraic number $b$.

## 3. Analytic representation of exponential maps

In this section, we discuss the analytic representation of the complex and $p$-adic exponential maps of a commutative algebraic group defined over $\overline{\mathbb{Q}}$ (with respect to a fixed basis for its Lie algebra). Let $G$ be a commutative algebraic group defined over $\overline{\mathbb{Q}}$ of positive dimension $n$. It is known that, by a compactification constructed by Serre, there is an embedding defined over $\overline{\mathbb{Q}}$ from $G$ into the projective space $\mathbb{P}^N$ with projective coordinates $X_0, \ldots, X_N$ for some positive integer $N$ (see [13]). One can now describe the exponential maps of $G$ (over $\mathbb{C}$ and $\mathbb{C}_p$) by analytic functions as follows. Let $\overline{G}$ denote the Zariski closure of $G$ in $\mathbb{P}^N$ and let $G_0$ be the open affine subset defined by $\overline{G} \cap \{X_0 \neq 0\}$. Then the affine algebra $\Gamma(G_0, O_{\overline{G}})$ of $G_0$ is generated over $\overline{\mathbb{Q}}$ by $\xi_i = X_i/X_0$ (the affine coordinates on $G_0$) for $i = 1, \ldots, N$, and we write it as $\overline{\mathbb{Q}}[\xi_1, \ldots, \xi_N]$. It is known that any element in the Lie algebra $\mathrm{Lie}(G)$ of $G$ maps

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

$\overline{\mathbb{Q}}[\xi_1, \ldots, \xi_N]$ into itself. In particular, for each $D \in \mathrm{Lie}(G)$, there exist polynomials $P_{1,D}, \ldots, P_{N,D}$ in $N$ variables with algebraic coefficients such that

$$D\xi_i = P_{i,D}(\xi_1, \ldots, \xi_N) \quad \text{for } i = 1, \ldots, N.$$

Let $v$ be a place of $\overline{\mathbb{Q}}$. Then there is a natural embedding from $\overline{\mathbb{Q}}$ into $C_v$, where $C_v = \mathbb{C}$ if $v$ is infinite, and $C_v = \mathbb{C}_p$ if $v$ is finite and lies above $p$. The set $G(C_v)$ is a $v$-adic Lie group whose Lie algebra $\mathrm{Lie}(G(C_v)) = \mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} C_v$, and it is known that the *v-adic exponential map* $\exp_{G(C_v)}$ of the Lie group $G(C_v)$ is a local diffeomorphism defined on a subgroup $G_v$ of $\mathrm{Lie}(G(C_v))$ (see [3]). From now on, we fix a basis $D_1, \ldots, D_n$ for the $\overline{\mathbb{Q}}$-vector space $\mathrm{Lie}(G)$ which is also a basis for the $C_v$-vector space $\mathrm{Lie}(G(C_v))$ (by the identifications $D_i = D_i \otimes 1$ for $i = 1, \ldots, N$). Let $\delta_1, \ldots, \delta_n$ denote the canonical basis of $\mathrm{Lie}(C_v^n)$, that is, $\partial_i x_j = \delta_{ij}$ for $i = 1, \ldots, n$ and for $j = 1, \ldots, N$, where $\delta_{ij}$ is Kronecker's delta and $x_1, \ldots, x_n$ are the coordinate functions of $C_v^n$. There exists an isomorphism $\phi : C_v^n \to \mathrm{Lie}(G(C_v))$ with the property that the differential of the composition map $\exp_{G(C_v)} \circ \phi$ satisfies

$$d(\exp_{G(C_v)} \circ \phi)(\partial_i) = D_i \quad \text{for } i = 1, \ldots, n.$$

Put $f_{i,v} = \xi_i \circ \exp_{G(C_v)} \circ \phi$ for $i = 1, \ldots, N$. The functions $f_{1,v}, \ldots, f_{N,v}$ are analytic on a neighbourhood $\mathcal{C}_v$ of the origin in $C_v^n$, and the system $\{f_{1,v}, \ldots, f_{N,v}\}$ is called the *(normalised) analytic representation of the exponential map* $\exp_{G(C_v)}$ (with respect to $D$). By convention, for each $i \in \{1, \ldots, N\}$, we write $f_{i,p}$ for $f_{i,v}$ and $\mathcal{C}_p$ for $\mathcal{C}_v$ if $C_v = \mathbb{C}_p$, and we write $f_i$ for $f_{i,v}$ and $\mathcal{C}$ for $\mathcal{C}_v$ if $C_v = \mathbb{C}$. (Note that in the complex case, the functions $f_1, \ldots, f_N$ can be extended as meromorphic functions on the whole space $\mathbb{C}^n$.) For $i = 1, \ldots, N$ and $j = 1, \ldots, n$,

$$\begin{aligned}\partial_j(f_{i,v}) &= \partial_j(\xi_i \circ \exp_{G(C_v)} \circ \phi) = (d(\exp_{G(C_v)} \circ \phi)(\partial_i)\xi_i) \circ \exp_{G(C_v)} \circ \phi \\ &= (D_j\xi_i) \circ \exp_{G(C_v)} \circ \phi = P_{i,D_j}(\xi_1, \ldots, \xi_N) \circ \exp_{G(C_v)} \circ \phi = P_{i,D_j}(f_{1,v}, \ldots, f_{N,v}).\end{aligned}$$

By induction, one can show that for $j = 1, \ldots, N$ and for nonnegative integers $i_1, \ldots, i_n$, there exists a polynomial $P_{i_1,\ldots,i_n,j}$ in $N$ variables with coefficients in $\overline{\mathbb{Q}}$ such that

$$(\partial_1^{i_1} \cdots \partial_n^{i_n}) f_{j,v} = P_{i_1,\ldots,i_n,j}(f_{1,v}, \ldots, f_{N,v}).$$

Since $\exp_{G(C_v)}(0) = e \in G(\overline{\mathbb{Q}})$ (where $e$ denotes the identity element of $G$), it follows that $f_i(0) = f_{i,p}(0) \in \overline{\mathbb{Q}}$ for $i = 1, \ldots, N$. Using the Taylor expansions of $f_{1,v}, \ldots, f_{N,v}$ at 0, we get the following proposition.

PROPOSITION 3.1. *There exist formal power series* $F_1, \ldots, F_N \in \overline{\mathbb{Q}}[[X_1, \ldots, X_N]]$ *converging both in* $\mathcal{C}$ *and* $\mathcal{C}_p$ *such that*

$$f_1(x) = F_1(x), \ldots, f_N(x) = F_N(x) \quad \textit{for all } x \in \mathcal{C}$$

*and*

$$f_{1,p}(x) = F_1(x), \ldots, f_{N,p}(x) = F_N(x) \quad \textit{for all } x \in \mathcal{C}_p.$$

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

## 4. Proof of the main theorem

This section is devoted to the proof of Theorem 1.2 which follows that of Theorem 1.1 with some extensions.

PROOF OF THEOREM 1.2. Without loss of generality, we may assume that the elements $\mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_l)$ are linearly independent over $\mathbb{Q}$ and the elements $v_1, \ldots, v_n$ are linearly independent over $K$, that is, $\dim_{\mathbb{Q}} U = l$ and $\dim_K V = n$. It is clear that there exists a positive integer $r$ sufficiently large for which $w_i := u_i^{p^r} \in B(r_p)$ for all $i = 1, \ldots, l$. Let $\log_p$ denote the $p$-adic logarithm function. Then

$$\log_p(w_i) = \mathrm{Log}_p(w_i) = \mathrm{Log}_p(u_i^{p^r}) = p^r \mathrm{Log}_p(u_i) \quad \text{for } i = 1, \ldots, l.$$

We have to show that the elements

$$1, \log_p(w_1), \ldots, \log_p(w_l), v_1, \ldots, v_n, \zeta_p(v_1), \ldots, \zeta_p(v_n)$$

are linearly independent over $\overline{\mathbb{Q}}$. Suppose that this is not true. Then there exists a nonzero linear form $L$ in $l + 2n + 1$ variables $T_0, T_1, \ldots, T_l, T'_1, \ldots, T'_n, T''_1, \ldots, T''_n$ with coefficients in $\overline{\mathbb{Q}}$ such that $L$ vanishes on $1, \log_p(w_1), \ldots, \log_p(w_l), v_1, \ldots, v_n, \zeta_p(v_1), \ldots, \zeta_p(v_n)$. We write $L$ in the form $L = L_0 + L' + L''$, where $L_0 = \alpha T_0 + \beta_1 T_1 + \cdots + \beta_l T_l$ with $\alpha, \beta_1, \ldots, \beta_l \in \overline{\mathbb{Q}}$ and where $L', L''$ are linear forms in $T'_1, \ldots, T'_n$ and $T''_1, \ldots, T''_n$, respectively. Let $G \in \mathrm{Ext}^1(\mathbb{G}_m^l \times E^n, \mathbb{G}_a)$ be the extension of $\mathbb{G}_m^l \times E^n$ by $\mathbb{G}_a$ determined by $L''$. The components of the complex exponential map $\exp_{G(\mathbb{C})}$ of $G$ are give by the functions

$$x_0 + L''(\zeta(y_1), \ldots, \zeta(y_n)), e^{x_1}, \ldots, e^{x_l}, \wp(y_1), \wp'(y_1), \ldots, \wp(y_n), \wp'(y_n)$$

for complex variables $x_0, x_1, \ldots, x_l, y_1, \ldots, y_n$. By Proposition 3.1, the corresponding components of the $p$-adic exponential map $\exp_{G(\mathbb{C}_p)}$ are given by the functions

$$z_0 + L''(\zeta_p(t_1), \ldots, \zeta_p(t_n)), e_p(z_1), \ldots, e_p(z_l), \wp_p(t_1), \wp'(t_1), \ldots, \wp_p(t_n), \wp'_p(t_n)$$

for $p$-adic variables $z_0, z_1, \ldots, z_l, t_1, \ldots, t_n$, where $e_p$ denotes the $p$-adic exponential function. Consider the point

$$\epsilon = (\beta_1 \log_p(w_1) + \cdots + \beta_l \log_p(w_l) + L'(v_1, \ldots, v_n), \log_p(w_1), \ldots, \log_p(w_l), v_1, \ldots, v_n).$$

Then the point $\gamma := \exp_{G(\mathbb{C}_p)}(\epsilon)$ is

$$(\beta_1 \log_p(w_1) + \cdots + \beta_l \log_p(w_l) + L'(v_1, \ldots, v_n) + L''(\zeta_p(v_1), \ldots, \zeta_p(v_n)),$$
$$w_1, \ldots, w_l, \wp_p(v_1), \wp'_p(v_1), \ldots, \wp_p(v_n), \wp'_p(v_n)).$$

Since

$$L(1, \log_p(w_1), \ldots, \log_p(w_l), v_1, \ldots, v_n, \zeta_p(v_1), \ldots, \zeta_p(v_n)) = 0,$$

it follows that

$$\beta_1 \log_p(w_1) + \cdots + \beta_l \log_p(w_l) + L'(v_1, \ldots, v_n) + L''(\zeta_p(v_1), \ldots, \zeta_p(v_n)) = -\alpha \in \overline{\mathbb{Q}}.$$

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

In particular, this means that the point $\gamma$ is an algebraic point of $G$. Let $\log_{G(\mathbb{C}_p)}$ be the $p$-adic logarithm map of $G$ and let $S$ be the $\overline{\mathbb{Q}}$-vector subspace of $\mathrm{Lie}(G)$ (which is identified with $\overline{\mathbb{Q}}^{l+n+1}$) given by

$$S = \{(s_0, s_1, \ldots, s_{l+n}) \in \overline{\mathbb{Q}}^{l+n+1} : s_0 - \beta_1 s_1 - \cdots - \beta_l s_l - L'(s_{l+1}, \ldots, s_{l+n}) = 0\}.$$

We see that

$$\log_{G(\mathbb{C}_p)}(\gamma) = \log_{G(\mathbb{C}_p)}(\exp_{G(\mathbb{C}_p)}(\epsilon)) = \epsilon \in S \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p.$$

Thanks to the $p$-adic analytic subgroup theorem (see [8] or [10]), there exists a nontrivial connected algebraic subgroup $H$ of $G$ defined over $\overline{\mathbb{Q}}$ such that $\gamma \in H(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H) \subseteq S$. Let $\pi$ be the composition of the homomorphism $G \to \mathbb{G}_m^l \times E^n$ and the canonical projection $\mathbb{G}_m^l \times E^n \to E^n$. Then the algebraic subgroup $\mathcal{E} := \pi(H)$ is isogenous (over $\overline{\mathbb{Q}}$) to $E^m$ with $m \leq n$. This gives a corresponding element $p : E^n \to \mathcal{E} \hookrightarrow E^n$ in $\mathrm{End}(E^n)$. Note that $\pi : G \to E^n$ induces the differential $d\pi$ from the Lie algebra of $G$ to that of $E^n$ and the algebra of endomorphisms $\mathrm{End}(E^n) \otimes_{\mathbb{Z}} \mathbb{Q}$ is identified with the matrix algebra $M_n(K)$. This means that the endomorphism $\mathrm{id}_{E^n} - p$ can be written as an $n \times n$ matrix with entries in $K$. Furthermore, since $\gamma \in H$, one has

$$\epsilon = \log_{G(\mathbb{C}_p)}(\gamma) = \log_{H(\mathbb{C}_p)}(\gamma) \in \mathrm{Lie}(H) \otimes_{\mathbb{Q}} \mathbb{C}_p.$$

It follows that the point $(v_1, \ldots, v_n) = d\pi(\epsilon) \in \mathrm{Lie}(\mathcal{E})$ which turns out to be the kernel of the endomorphism given by the above matrix. However, the elements $v_1, \ldots, v_n$ are linearly independent over $K$, so that this matrix must be trivial. In other words, $p = \mathrm{id}_{E^n}$, that is, $\mathcal{E} = E^n$.

Next, we see that $G \cong \mathbb{G}_m^l \times G_0$, where $G_0 \in \mathrm{Ext}^1(E^n, \mathbb{G}_a)$ since $\mathrm{Ext}^1(\mathbb{G}_m, \mathbb{G}_a)$ is trivial (in fact, it is known more generally that the group extension of linear algebraic groups is trivial). Hence, without loss of generality, we may assume that the algebraic numbers $\beta_1, \ldots, \beta_l$ are not all zero (since, if not, one can take the quotient of $G$ by the multiplicative group $\mathbb{G}_m$, and we are in a simpler case with $G_0$). The intersection of $H$ with $\mathbb{G}_a \times \mathbb{G}_m^l$ is an algebraic subgroup of $\mathbb{G}_a \times \mathbb{G}_m^l$, and therefore has the form $H_a \times H_m$, where $H_a$ and $H_m$ are (connected) algebraic subgroups of $\mathbb{G}_a$ and $\mathbb{G}_m^l$, respectively (see [1, Proposition 4.3]). This leads to

$$\begin{aligned}\mathrm{Lie}(H_a) \times \mathrm{Lie}(H_m) &= \mathrm{Lie}(H_a \times H_m) \\ &= \mathrm{Lie}(H) \cap (\mathrm{Lie}(\mathbb{G}_a) \times \mathrm{Lie}(\mathbb{G}_m^l)) = \mathrm{Lie}(H) \cap (\overline{\mathbb{Q}} \times \overline{\mathbb{Q}}^l).\end{aligned}$$

If $H_m$ is a proper algebraic subgroup of the torus $\mathbb{G}_m^l$, it follows from [1, Lemma 4.4] that the Lie algebra $\mathrm{Lie}(H_m)$ is given by $L_1 = \cdots = L_d = 0$, where $d = l - \dim H_m \geq 1$ and $L_1, \ldots, L_d$ are nonzero linear forms in $n$ variables with integer coefficients. In particular, this means that $\log_p(w_1), \ldots, \log_p(w_l)$ are linearly dependent over $\mathbb{Q}$, or equivalently, $\mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_l)$ are linearly dependent over $\mathbb{Q}$. This contradiction shows that $H_m = \mathbb{G}_m^l$ and then $H_a$ must be trivial (since $\dim H \leq \dim_{\overline{\mathbb{Q}}} S = n + l$). This

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

enables us to conclude that $\beta_1 s_1 + \cdots + \beta_l s_l = 0$ for all $s_1, \ldots, s_l \in \overline{\mathbb{Q}}$ and this happens if and only if $\beta_1 = \cdots = \beta_l = 0$, which is a contradiction. The theorem is proved. □

As in the complex case, it is also possible to slightly extend the main theorem to the case of several $p$-adic Weierstrass zeta functions as follows. Let $E_1, \ldots, E_n$ be elliptic curves defined over $\overline{\mathbb{Q}}$. For each $i \in \{1, \ldots, n\}$, denote by $\wp_{p,i}$ and $\zeta_{p,i}$ the $p$-adic elliptic function and the $p$-adic Weierstrass zeta function associated with the elliptic curve $E_i$, respectively. Let $v_i$ be an algebraic point of $\wp_{p,i}$ for $i = 1, \ldots, n$. Let $I_\nu$ $(\nu = 1, \ldots, k)$ be maximal sets of indices such that $E_i$ are pairwise isogenous (over $\overline{\mathbb{Q}}$) for all $i \in I_\nu$. Fix an element $E^{(\nu)}$ in the set $\{E_j : j \in I_\nu\}$. The field of endomorphisms of $E^{(\nu)}$ is the same as that of $E_j$ for any $j \in I_\nu$, and we denote it by $K_\nu$. Let $V_\nu$ be the vector space generated by the set $\{v_j : j \in I_\nu\}$ over $K_\nu$. Then we obtain the following theorem which is an extension of the $p$-adic analogue of [1, Theorem 6.4].

THEOREM 4.1. *Let $u_1, \ldots, u_l$ be nonzero algebraic numbers and $U$ the vector space generated by* $\mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_l)$ *over* $\mathbb{Q}$. *Then the dimension of the vector space $W$ generated by* $1, \mathrm{Log}_p(u_1), \ldots, \mathrm{Log}_p(u_l), v_1, \ldots, v_n, \zeta_{p,1}(v_1), \ldots, \zeta_{p,n}(v_n)$ *over* $\overline{\mathbb{Q}}$ *is determined by*

$$\dim_{\overline{\mathbb{Q}}} W = 1 + \dim_{\mathbb{Q}} U + 2(\dim_{K_1} V_1 + \cdots + \dim_{K_k} V_k).$$

## References

[1] A. Baker and G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, New Mathematical Monographs, 9 (Cambridge University Press, Cambridge, 2007).

[2] D. Bertrand, 'Sous-groupes à un paramètre $p$-adique de variétés de groupe', *Invent. Math.* **40**(2) (1977), 171–193.

[3] N. Bourbaki, *Elements of Mathematics. Lie groups and Lie algebras. Part I: Chapters 1–3*, Actualities scientifiques et industrielles (Herman, Paris, 1975); English translantion.

[4] D. Caveny and R. Tubbs, 'Well-approximated points on linear extensions of elliptic curves', *Proc. Amer. Math. Soc.* **138** (2010), 2745–2754.

[5] K. Chandrasekharan, *Elliptic Functions*, Grundlehren der mathematischen Wissenschaften, 281 (Springer-Verlag, Berlin, 1985).

[6] J. Coates, 'The transcendence of linear forms in $\omega_1, \omega_2, \eta_1, \eta_2, 2\pi i$', *Amer. J. Math.* **93** (1971), 385–397.

[7] G. Faltings and G. Wüstholz, 'Einbettungen kommutativer algebraischer Gruppen und einige ihrer Eigenschaften', *J. reine angew. Math.* **354** (1984), 175–205.

[8] C. Fuchs and D. H. Pham, 'The $p$-adic analytic subgroup theorem revisited', *p-Adic Numbers Ultrametric Anal. Appl.* **7** (2015), 143–156.

[9] E. Lutz, 'Sur l'équation $Y^2 = AX^3 - AX - B$ dans les corps $p$-adiques', *J. reine angew. Math.* **177** (1937), 238–247.

[10] T. Matev, 'The $p$-adic analytic subgroup theorem and applications', Preprint, 2010, arXiv:1010.3156v1.

[11] A. M. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics, 198 (Springer-Verlag, New York, 2000).

[12] T. Schneider, 'Transzendenzuntersuchungen periodischer Funktionen: I Transzendenz von Potenzen; II Transzendenzeigenschaften elliptischer Funktionen', *J. reine angew. Math.* **172** (1934), 65–74.

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press

[13] J. P. Serre, ‘Quelques propriétés des groupes algébriques commutatifs’, *Astérisque* **69–70** (1979), 191–202.
[14] A. Weil, ‘Sur les fonctions elliptiques $\mathfrak{p}$-adiques’, *C. R. Hebdomadaires Séances L’Acad. Sci.* **203**(1) (1936), 22–24.
[15] G. Wüstholz, ‘Algebraische Punkte auf Analytischen Untergruppen algebraischer Gruppen’, *Ann. of Math. (2)* **129** (1989), 501–517.

DUC HIEP PHAM, University of Education,
Vietnam National University, Hanoi, 144 Xuan Thuy, Cau Giay, Hanoi, Vietnam
e-mail: phamduchiep@vnu.edu.vn

https://doi.org/10.1017/S0004972724000091 Published online by Cambridge University Press