Bull. Aust. Math. Soc. **105** (2022), 31–36
doi:10.1017/S0004972721000320

ELLIPTIC CURVES AND p-ADIC ELLIPTIC TRANSCENDENCE

DUC HIEP PHAM

(Received 1 March 2021; accepted 31 March 2021; first published online 21 May 2021)

Abstract

We prove a necessary and sufficient condition for isogenous elliptic curves based on the algebraic dependence of p-adic elliptic functions. As a consequence, we give a short proof of the p-adic analogue of Schneider's theorem on the linear independence of p-adic elliptic logarithms of algebraic points on two nonisogenous elliptic curves defined over the field of algebraic numbers.

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

Keywords and phrases: elliptic curve, elliptic function, p-adic transcendence.

1. Introduction

Let $K \subset \mathbb{C}$ be a subfield of the field of complex numbers. Let E be an elliptic curve defined over K (that is, an abelian variety of dimension one defined over K). We can characterise E by the Weierstrass form

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

with $g_2, g_3 \in K$, called *the invariants of* E, such that $g_2^3 - 27g_3^2 \neq 0$. There is a unique lattice Λ in $\mathbb{C}$, that is, a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$, satisfying

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-4}, \quad g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-6},$$

and a unique function $\wp$ which is meromorphic on $\mathbb{C}$ and analytic on $\mathbb{C} \setminus \Lambda$ such that

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3.$$

Furthermore, the function $\wp$ is (doubly) periodic on Λ, that is, $\wp(z + \omega) = \wp(z)$ for all $\omega \in \Lambda$. We call $\wp$ the *Weierstrass elliptic function* associated with the elliptic curve E.

Let E^* be another elliptic curve defined over K. We say that E and E^* are *isogenous over* K if there is a nonconstant morphism from E to E^* defined over K which maps the point at infinity of E to that of E^*. It is known that E and E^* are isogenous over the field of algebraic numbers $\overline{\mathbb{Q}}$ if and only if $\wp$ and $\wp^*$ are algebraically dependent over $\overline{\mathbb{Q}}$, where $\wp^*$ is the Weierstrass elliptic function associated with E^*. Indeed, if there

is an isogeny $\phi : E \to E^*$ defined over $\overline{\mathbb{Q}}$, then it induces an analytic homomorphism of complex Lie groups $E(\mathbb{C})$ and $E^*(\mathbb{C})$, which is still denoted by ϕ. Furthermore, the diagram

$$\begin{array}{ccc} E(\mathbb{C}) & \xrightarrow{\phi} & E^*(\mathbb{C}) \\ {\scriptstyle \exp_{E(\mathbb{C})}}\uparrow & & \uparrow{\scriptstyle \exp_{E^*(\mathbb{C})}} \\ \mathrm{Lie}(E(\mathbb{C})) & \xrightarrow{d\phi} & \mathrm{Lie}(E^*(\mathbb{C})) \end{array}$$

commutes, where $\exp_{E(\mathbb{C})}$ and $\exp_{E^*(\mathbb{C})}$ are the exponential maps of E and E^*, respectively (see [11, Section 1]). There exist natural bases ∂_E and ∂_E^* for the Lie algebras of E and E^*, respectively, such that $\exp_{E(\mathbb{C})}(z\partial_E) = [\wp(z) : \wp'(z) : 1]$ and $\exp_{E^*(\mathbb{C})}(z\partial_E^*) = [\wp^*(z) : \wp^{*\prime}(z) : 1]$ (see [1, Section 6]). Since the isogeny ϕ is defined over $\overline{\mathbb{Q}}$, it follows that $\wp^*$ can be expressed as a rational function with coefficients in $\overline{\mathbb{Q}}$ with respect to $\wp$. This means that $\wp$ and $\wp^*$ are algebraically dependent over $\overline{\mathbb{Q}}$. Conversely, if $\wp$ and $\wp^*$ are algebraically dependent over $\overline{\mathbb{Q}}$, then it follows from [7, Ch. 15] that $m\Lambda \subset \Lambda^*$ for some positive integer m, where Λ^* is the lattice of periods of $\wp^*$. In particular, this gives an isogeny from $E(\mathbb{C})$ to $E^*(\mathbb{C})$ (defined over $\mathbb{C}$) which maps $[\wp(z) : \wp'(z) : 1]$ to $[\wp^*(mz) : \wp^{*\prime}(mz) : 1]$. But using the fact that $\wp^*(mz)$ is a rational function with coefficients in $\overline{\mathbb{Q}}$ in terms of $\wp^*(z)$ together with the algebraic dependence of $\wp(z)$ and $\wp^*(z)$, we see that the set of complex numbers λ such that $\wp(\lambda)$ and $\wp^*(m\lambda)$ are both in $\overline{\mathbb{Q}}$ is infinite. This allows us to deduce that $\wp^*(mz)$ is a rational function with coefficients in $\overline{\mathbb{Q}}$ in terms of $\wp(z)$, and from this we are able to conclude that E and E^* are isogenous over $\overline{\mathbb{Q}}$.

The main purpose of this paper is to prove such a result in the p-adic setting. To present this result, we recall the Lutz–Weil p-adic elliptic functions which can be seen as the p-adic analogue of the Weierstrass elliptic functions. Let $\mathbb{C}_p$ denote the completion of $\overline{\mathbb{Q}_p}$ with respect to the p-adic absolute value $|\cdot|_p$, as usual. We also denote by $B(r_p)$ the set of all p-adic numbers x in $\mathbb{C}_p$ such that $|x|_p < r_p$ with $r_p := p^{-1/(p-1)}$. Now, let E be an elliptic curve defined over $\mathbb{C}_p$, that is, the invariants g_2 and g_3 in the Weierstrass form of E are in $\mathbb{C}_p$. One can show that the differential equation

$$y'(z) = \left(1 - \frac{g_2}{4}y^4(z) - \frac{g_3}{4}y^6(z)\right)^{1/2}, \quad y(0) = 0$$

admits the solutions $\varphi(z)$ and $-\varphi(z)$ which are analytic on the disk

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

The disk $\mathscr{D}_p$ is called the *p-adic domain of E*. We put $\wp_p := \varphi^{-2}$ so that

$$\wp_p'^2 = 4\wp_p^3 - g_2\wp_p - g_3.$$

https://doi.org/10.1017/S0004972721000320 Published online by Cambridge University Press

Then $\wp_p$ is called the *(Lutz–Weil) p-adic elliptic function* associated with the elliptic curve E (see [6, 10]). Let E^* be another elliptic curve defined over $\mathbb{C}_p$. Let $\mathscr{D}_p^*$ be the p-adic domain of E^*. For each nonzero algebraic number α in $\overline{\mathbb{Q}}$, denote by $\mathscr{D}_{p,\alpha}$ the set of all nonzero p-adic numbers z in $\mathscr{D}_p$ with $\alpha z \in \mathscr{D}_p^*$. We also define the function $\wp_{p,\alpha}^*$ on $\mathscr{D}_{p,\alpha}$ by $\wp_{p,\alpha}^*(z) = \wp_p^*(\alpha z)$. Now, our main theorem reads as follows.

THEOREM 1.1. *Let E and E^* be elliptic curves defined over $\overline{\mathbb{Q}}$. Let α be a nonzero algebraic number in $\overline{\mathbb{Q}}$. Then E and E^* are isogenous over $\overline{\mathbb{Q}}$ if and only if $\wp_p$ and $\wp_{p,\alpha}^*$ are algebraically dependent over $\overline{\mathbb{Q}}$.*

The following corollaries can be immediately deduced from the main theorem.

COROLLARY 1.2. *Let E and E^* be elliptic curves defined over $\overline{\mathbb{Q}}$. The p-adic elliptic functions $\wp_p$ and $\wp_p^*$ associated with E and E^*, respectively, are algebraically dependent over $\overline{\mathbb{Q}}$ if and only if $\wp_p$ and $\wp_{p,\alpha}^*$ are algebraically dependent over $\overline{\mathbb{Q}}$ for any nonzero algebraic number α.*

COROLLARY 1.3. *Let E and E^* be elliptic curves defined over $\overline{\mathbb{Q}}$. The following statements are equivalent.*

(i) *The elliptic curves E and E^* are isogenous over $\overline{\mathbb{Q}}$.*
(ii) *The Weierstrass elliptic functions $\wp$ and $\wp^*$ associated with E and E^*, respectively, are algebraically dependent over $\overline{\mathbb{Q}}$.*
(iii) *The p-adic elliptic functions $\wp_p$ and $\wp_p^*$ associated with E and E^*, respectively, are algebraically dependent over $\overline{\mathbb{Q}}$.*

In 1936, Schneider proved that if two elliptic curves E and E^* are defined over $\overline{\mathbb{Q}}$ such that their corresponding associated Weierstrass elliptic functions $\wp$ and $\wp^*$ are algebraically independent over $\overline{\mathbb{Q}}$ (equivalently, E and E^* are not isogenous over $\overline{\mathbb{Q}}$), then either $\wp(u)$ or $\wp^*(u)$ is transcendental for any complex number u neither in the lattice of periods of E nor of E^* (see [8, 9]). The p-adic analogue of this result was obtained by Bertrand in 1977. Namely, he proved that if two elliptic curves E and E^* are defined over $\overline{\mathbb{Q}}$ with their corresponding p-adic elliptic functions $\wp_p$ and $\wp_p^*$, and if there is a nonzero p-adic number u in the p-adic domains of E and E^* such that $\wp_p(u)$ and $\wp_p^*(u)$ are both algebraic, then E and E^* are isogenous over $\overline{\mathbb{Q}}$ (see [2]). By using the main theorem and the p-adic analytic subgroup theorem (see Section 2), we are able to slightly extend Bertrand's result.

THEOREM 1.4. *Let E and E^* be elliptic curves defined over $\overline{\mathbb{Q}}$. Let α be a nonzero algebraic number in $\overline{\mathbb{Q}}$. If there is a nonzero p-adic number u in $\mathscr{D}_{p,\alpha}$ such that $\wp_p(u)$ and $\wp_p^*(\alpha u)$ are both algebraic, then E and E^* are isogenous over $\overline{\mathbb{Q}}$.*

It is worth noticing that Theorem 1.4 can be deduced from [5, Theorem 2.1]. Nevertheless, the situation in this theorem is much simpler than that in [5, Theorem 2.1] and we give a short proof of Theorem 1.4 in Section 3.

https://doi.org/10.1017/S0004972721000320 Published online by Cambridge University Press

2. The *p*-adic analytic subgroup theorem

The analytic subgroup theorem is one of the most significant results in modern (complex) transcendence theory with many applications. It was formulated and proved by Wüstholz in the 1980s (see [1, 11]). This theorem has a p-adic analogue that we will now discuss. Let G be a commutative algebraic group defined over a subfield K of $\mathbb{C}_p$. Then the set $G(\mathbb{C}_p)$ of $\mathbb{C}_p$-points of G is a Lie group over $\mathbb{C}_p$ whose Lie algebra is denoted by $\mathrm{Lie}(G(\mathbb{C}_p))$. According to [3, Ch. III, 7.6]), there is a p-adic analytic homomorphism, the so-called *the p-adic logarithm map of G*,

$$\log_{G(\mathbb{C}_p)} : G(\mathbb{C}_p)_f \to \mathrm{Lie}(G(\mathbb{C}_p)),$$

where $G(\mathbb{C}_p)_f$ is the set of $x \in G(\mathbb{C}_p)$ for which there exists a strictly increasing sequence (n_i) of integers such that x^{n_i} tends to the unity element of $G(\mathbb{C}_p)$ as i tends to infinity. If H is another commutative algebraic group defined over K, then $(G \times H)(\mathbb{C}_p)_f = G(\mathbb{C}_p)_f \times H(\mathbb{C}_p)_f$. Furthermore, $\mathrm{Lie}((G \times H)(\mathbb{C}_p)) = \mathrm{Lie}(G(\mathbb{C}_p)) \times \mathrm{Lie}(H(\mathbb{C}_p))$ and $\log_{(G\times H)(\mathbb{C}_p)}$ is the map $(\log_{G(\mathbb{C}_p)}, \log_{H(\mathbb{C}_p)})$.

If G is an abelian variety, one has $G(\mathbb{C}_p)_f = G(\mathbb{C}_p)$ (see [12]). In particular, in the case when G is an elliptic curve, one can express the p-adic logarithm map of G explicitly through the p-adic elliptic function associated with G. In more detail, let E be an elliptic curve defined over K. Denote by $\wp_p$ and $\mathscr{D}_p$ the p-adic elliptic function and the p-adic domain of E, as in Section 1. The Lie algebra of $E(\mathbb{C}_p)$ is canonically isomorphic to $\mathbb{C}_p$, and the p-adic exponential map is given by

$$\exp_{E(\mathbb{C}_p)} : \mathscr{D}_p \to E(\mathbb{C}_p) \subseteq \mathbb{P}^2(\mathbb{C}_p), \quad z \mapsto (\wp_p(z) : \wp_p'(z) : 1).$$

This map gives an isomorphism between $\mathscr{D}_p$ and $\exp_{E(\mathbb{C}_p)}(\mathscr{D}_p) \subseteq E(\mathbb{C}_p)$, and the restriction to $\exp_{E(\mathbb{C}_p)}(\mathscr{D}_p)$ of the p-adic logarithmic map $\log_{E(\mathbb{C}_p)} : E(\mathbb{C}_p) \to \mathbb{C}_p$ is the inverse of the p-adic exponential map $\exp_{E(\mathbb{C}_p)}$. In this language, Theorem 1.4 means that if two elliptic curves E and E^* are defined and not isogenous over $\overline{\mathbb{Q}}$, then the p-adic elliptic logarithms $\log_{E(\mathbb{C}_p)}(\omega)$ and $\log_{E(\mathbb{C}_p)}(\omega^*)$ are linearly independent over $\overline{\mathbb{Q}}$ for any algebraic points $\omega \in \exp_{E(\mathbb{C}_p)}(\mathscr{D}_p)$ and $\omega^* \in \exp_{E^*(\mathbb{C}_p)}(\mathscr{D}_p^*)$.

We end this section by quoting the following theorem which is called *the p-adic analytic subgroup theorem* (see [4]).

THEOREM 2.1. *Let G be a commutative algebraic group of positive dimension defined over $\overline{\mathbb{Q}}$ and let $\mathrm{Lie}(G)$ denote the Lie algebra of G. Let $V \subseteq \mathrm{Lie}(G)$ be a nontrivial $\overline{\mathbb{Q}}$-linear subspace. For any $\gamma \in G(\mathbb{C}_p)_f \cap G(\overline{\mathbb{Q}})$, the set of algebraic points of G in $G(\mathbb{C}_p)_f$, such that $0 \neq \log_{G(\mathbb{C}_p)}(\gamma) \in V_{\mathbb{C}_p} := V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$, there exists an algebraic subgroup $H \subseteq G$ of positive dimension defined over $\overline{\mathbb{Q}}$ such that the Lie algebra $\mathrm{Lie}(H)$ of H is contained in V and $\gamma \in H(\overline{\mathbb{Q}})$.*

3. Proofs

3.1. Proof of Theorem 1.1. We first prove the necessity of the condition in the theorem. Assume that there is an isogeny $\phi : E \to E^*$ defined over $\overline{\mathbb{Q}}$. Clearly, the

https://doi.org/10.1017/S0004972721000320 Published online by Cambridge University Press

graph of ϕ in $E \times E^*$ provides an algebraic relation between the maps $\exp_{E(\mathbb{C}_p)}(z)$ and $\exp_{E^*(\mathbb{C}_p)}(\beta z)$ (with $z \in \mathscr{D}_{p,\beta}$), where $\beta \in \overline{\mathbb{Q}}^*$ is the representation of the differential of ϕ at zero in a chosen basis of $\mathrm{Lie}(E(\mathbb{C}_p))$ and $\mathrm{Lie}(E^*(\mathbb{C}_p))$. Notice that $\mathrm{Lie}(E(\mathbb{C}_p))$ and $\mathrm{Lie}(E^*(\mathbb{C}_p))$ are $\mathbb{C}_p$-vector spaces (defined over $\overline{\mathbb{Q}}$) of dimension one. Therefore one can fix these bases so that $\beta = \alpha$. In particular, this shows that the functions $\wp_p$ and $\wp^*_{p,\alpha}$ are algebraically dependent over $\overline{\mathbb{Q}}$.

To prove the sufficiency of the condition, consider the one-parameter subgroup $\{(\exp_{E(\mathbb{C}_p)}(z), \exp_{E^*(\mathbb{C}_p)}(\alpha z)) : z \in \mathscr{D}_{p,\alpha}\} \subset E(\mathbb{C}_p) \times E^*(\mathbb{C}_p)$. By hypothesis, its Zariski closure H is an algebraic subgroup of $E \times E^*$ of dimension one. One can assume that H is connected, so H is an elliptic curve contained in $E \times E^*$. This implies that the projections from H to E and to E^* are surjections. In particular, E and E^* are isogenous since a surjection between elliptic curves is an isogeny. □

3.2. Proof of Theorem 1.4. Put $G := E \times E^*$. Then G is an abelian variety defined over $\overline{\mathbb{Q}}$. The Lie algebra $\mathrm{Lie}(G) = \mathrm{Lie}(E) \times \mathrm{Lie}(E^*)$ can be identified with $\overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$, and therefore

$$\mathrm{Lie}(G(\mathbb{C}_p)) = \mathrm{Lie}(G) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = \mathbb{C}_p \times \mathbb{C}_p.$$

One has $G(\mathbb{C}_p)_f = G(\mathbb{C}_p) = E(\mathbb{C}_p) \times E^*(\mathbb{C}_p)$ and the p-adic logarithm map of G is given by

$$\log_{G(\mathbb{C}_p)} = (\log_{E(\mathbb{C}_p)}, \log_{E^*(\mathbb{C}_p)}).$$

Let V be the $\overline{\mathbb{Q}}$-vector space defined by

$$V = \{(x, y) \in \overline{\mathbb{Q}}^2 : \alpha x - y = 0\}.$$

Then

$$V_{\mathbb{C}_p} = V \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p = \{(x, y) \in \mathbb{C}_p^2 : \alpha x - y = 0\}.$$

Consider the point

$$\begin{aligned}\gamma &:= (\exp_{E(\mathbb{C}_p)}(u), \exp_{E^*(\mathbb{C}_p)}(\alpha u)) \\ &= ((\wp_p(u) : \wp_p'(u) : 1), (\wp_p^*(\alpha u) : \wp_p^{*\prime}(\alpha u) : 1)) \in G(\mathbb{C}_p).\end{aligned}$$

By assumption, $\wp_p(u)$ and $\wp_p^*(\alpha u)$ are algebraic, and so are $\wp_p'(u)$ and $\wp_p^{*\prime}(\alpha u)$. It follows that γ is an algebraic point of $G(\mathbb{C}_p)$, that is, $\gamma \in G(\overline{\mathbb{Q}})$. Moreover,

$$\log_{G(\mathbb{C}_p)}(\gamma) = (\log_{E(\mathbb{C}_p)}(\exp_{E(\mathbb{C}_p)}(u)), \log_{E^*(\mathbb{C}_p)}(\exp_{E^*(\mathbb{C}_p)}(\alpha u))) = (u, \alpha u)$$

is a nonzero point in $V_{\mathbb{C}_p}$. Thanks to Theorem 2.1, there is an algebraic subgroup H of G of positive dimension defined over $\overline{\mathbb{Q}}$ such that the point γ belongs to $H(\overline{\mathbb{Q}})$ and the Lie algebra $\mathrm{Lie}(H)$ is contained in V. Obviously, the dimension of H must be one since the dimension of V over $\overline{\mathbb{Q}}$ is one. Therefore, $\mathrm{Lie}(H)$ must be V. In particular, this shows that the set $\{(\exp_{E(\mathbb{C}_p)}(z), \exp_{E^*(\mathbb{C}_p)}(\alpha z)) : z \in \mathscr{D}_{p,\alpha}\}$ is contained in $H(\mathbb{C}_p)$. This, together with the algebraic relations $\wp_p'^2 = 4\wp_p^3 - g_2\wp_p - g_3$

https://doi.org/10.1017/S0004972721000320 Published online by Cambridge University Press

and $\wp_p^{*\prime 2} = 4\wp_p^{*3} - g_2^*\wp_p^* - g_3^*$, gives rise to a nonzero two-variable polynomial P with coefficients in $\overline{\mathbb{Q}}$ satisfying $P(\wp_p(z), \wp_p^*(\alpha z)) = 0$ for all $z \in \mathscr{D}_{p,\alpha}$. In other words, $\wp_p$ and $\wp_{p,\alpha}^*$ are algebraically dependent over $\overline{\mathbb{Q}}$. This shows that E and E^* are isogenous over $\overline{\mathbb{Q}}$ by Theorem 1.1. □

Acknowledgement

The author would like to thank the anonymous referee for careful reading of this manuscript and useful comments.

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* (Hermann, Paris, 1975).
[4] C. Fuchs and D. H. Pham, 'The p-adic analytic subgroup theorem revisited', *p-Adic Numbers Ultrametric Anal. Appl.* **7** (2015), 143–156.
[5] C. Fuchs and D. H. Pham, 'Some applications of the p-adic analytic subgroup theorem', *Glas. Mat.* **51** (2016), 335–343.
[6] E. Lutz, 'Sur l'équation $Y^2 = AX^3 - AX - B$ dans les corps p-adiques', *J. reine angew. Math.* **177** (1937), 238–247.
[7] M. R. Murty and P. Rath, *Transcendental Numbers* (Springer, New York, 2014).
[8] T. Schneider, 'Arithmetische Untersuchungen elliptischer Integrale', *Math. Ann.* **113** (1936), 1–13.
[9] T. Schneider, *Einführung in die Transzendenten Zahlen* (Springer-Verlag, Berlin, 1957).
[10] A. Weil, 'Sur les fonctions elliptiques p-adiques', *Note aux C. R. Acad. Sci. Paris* **203** (1936), 22–24.
[11] G. Wüstholz, 'Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen', *Ann. of Math.* **129** (1989), 501–517.
[12] Y. G. Zarhin, 'p-adic abelian integrals and commutative Lie groups', *J. Math. Sci.* **81**(3) (1996), 2744–2750.

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/S0004972721000320 Published online by Cambridge University Press