



Title	BF PATH INTEGRALS FOR ELLIPTIC CURVES AND p -ADIC L -FUNCTIONS
Author(s)	Park, Jeehoon; Park, Junyeong
Citation	Osaka Journal of Mathematics. 2026, 63(3), p. 397-408
Version Type	VoR
URL	https://doi.org/10.18910/106083
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

BF PATH INTEGRALS FOR ELLIPTIC CURVES AND p -ADIC L -FUNCTIONS

JEEHOON PARK and JUNYEONG PARK

(Received August 23, 2024, revised September 25, 2024)

Abstract

We prove an arithmetic path integral formula for the inverse p -adic absolute values of the p -adic L -functions of elliptic curves over the rational numbers with good ordinary reduction at an odd prime p based on the Iwasawa main conjecture and Mazur’s control theorem. This is an elliptic curve analogue of [2].

Contents

1. Introduction	397
1.1. The statement of the main theorem	398
1.2. Open question	400
2. The BF-functional for elliptic curves	401
3. Isotypic components of the BF-functional	402
4. The proof of the main theorem	405
References	407

1. Introduction

The arithmetic BF theory for number fields and abelian varieties was introduced in [3] to show the philosophy of arithmetic gauge theory which indicates that the path integral of the physical theory is closely related to the L -function of the relevant number theory. The arithmetic BF theory for cyclotomic fields led to [2], which proves an arithmetic path integral formula for the inverse p -adic absolute values of Kubota-Leopoldt p -adic L -functions at roots of unity (a precise connection between Kubota-Leopoldt p -adic L -function and the arithmetic BF path integral of cyclotomic fields up to p -adic units); the formula in [2] adds a small step toward such philosophy. Then a natural question is to prove a similar path integral formula for the p -adic L -function of elliptic curves with ordinary good reduction at p ; the aim of this article is to resolve this question.

1.1. The statement of the main theorem. Let $E/\mathbb{Q}$ be an elliptic curve with semistable reduction at all places. Let p be an odd prime where E has good ordinary reduction. For $n \geq 0$, denote

$$K_n := \mathbb{Q}(\zeta_{p^{n+1}}), \quad X_n := \operatorname{Spec} \mathbb{Z}[\zeta_{p^{n+1}}],$$

where $\zeta_{p^{n+1}}$ is a primitive p^{n+1} -th root of unity. Also, we simply denote $K := K_0$ so that

$$\Gamma := \operatorname{Gal}(K_\infty/K) \cong \mathbb{Z}_p.$$

Denote $\Gamma_n \subseteq \Gamma$ the subgroup of index p^n . On the other hand, let

$$\omega : \operatorname{Gal}(K/\mathbb{Q}) \longrightarrow \mathbb{Z}_p^\times (\cong \operatorname{Gal}(K_\infty/\mathbb{Q}))$$

be the Teichmüller character and let $(\cdot)_r$ be the ω^r -isotypic component of a Γ -module with $\operatorname{Gal}(K/\mathbb{Q}) \cong \mathbb{F}_p^\times$ -action. Then $\mathbb{Q}_n := K_{n,0} \subseteq K_n$ is the subfield fixed under ω so that we have the following diagram of field extensions:

$$(1.1) \quad \begin{array}{ccc} & & K_n \\ & \nearrow \mathbb{F}_p^\times & \downarrow \Gamma/\Gamma_n \\ \mathbb{Q}_n = K_{n,0} & & K \\ & \nwarrow \mathbb{F}_p^\times & \downarrow \Gamma/\Gamma_n \\ & & \mathbb{Q} \end{array} .$$

Note that $\Gamma/\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$. We also denote

$$Y_n := \operatorname{Spec} \mathcal{O}_{\mathbb{Q}_n}.$$

Denote $\mathcal{E}$ the Néron model of E over $\mathbb{Z}$. For $m \geq 1$ we use the following notation:

$$\mathcal{F}^m(\operatorname{Spec} \mathcal{O}) := H_{\text{fppf}}^1(\operatorname{Spec} \mathcal{O}, \mathcal{E}[p^m]) \times H_{\text{fppf}}^1(\operatorname{Spec} \mathcal{O}, \mathcal{E}[p^m]),$$

where $\mathcal{O}$ is the ring of integers of a number field and we view $\mathcal{E}[p^m]$ as sheaves in the flat topology. Denote $\mathcal{E}^0 \subseteq \mathcal{E}$ the identity component and $\Phi_{\mathcal{E}}$ the group of connected components. Then, as in [3, p. 1305], we have an exact sequence of fppf sheaves:

$$0 \longrightarrow \mathcal{E}^0 \longrightarrow \mathcal{E} \longrightarrow \Phi_{\mathcal{E}} \longrightarrow 0 .$$

Note that if $\mathbb{Z} \hookrightarrow \mathcal{O}$ is ramified only at $p \in \mathbb{Z}$, then $\mathcal{E} \otimes_{\mathbb{Z}} \mathcal{O}$ is the Néron model of E over $\mathcal{O}$ and the order¹ of $\Phi_{\mathcal{E} \otimes_{\mathbb{Z}} \mathcal{O}}$ is the same as the order of $\Phi_{\mathcal{E}}$ (Lemma 2.1).

We briefly recall the definition of the Tate-Shafarevich group $\text{III}(K_n, E)$ for each $n \in \mathbb{N} \cup \{\infty\}$:

¹Given a Néron model $\mathcal{A}$ over $\mathcal{O}$ of an abelian variety A over $\operatorname{Frac}(\mathcal{O})$, we have

$$\Phi_{\mathcal{A}} = \bigoplus_{s \in \operatorname{Spec} \mathcal{O}} i_{s*} \Phi_{\mathcal{A}_s},$$

where each $\Phi_{\mathcal{A}_s}$ is a finite étale group of connected component of $\mathcal{A}_s$ over the residue field $\kappa(s)$ (see [4, Proposition B.2] for example). Then the order of $\Phi_{\mathcal{A}}$ is defined to be the sum of orders of $\Phi_{\mathcal{A}_s}$.

$$\text{III}(K_n, E) := \ker \left(H^1(K_n, E(\overline{K}_n)) \longrightarrow \prod_v H^1(K_{n,v}, E(\overline{K}_{n,v})) \right),$$

where v runs over all primes of K_n . The Selmer group for each $n \in \mathbb{N} \cup \{\infty\}$ is defined so that it fits into the following exact sequence:

$$0 \longrightarrow E(K_n) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \longrightarrow \text{Sel}(K_n, E) \longrightarrow \text{III}(K_n, E) \longrightarrow 0.$$

We refer to [6, chapter 2] for detailed definition. Then we make the following assumptions:

- the Selmer group $\text{Sel}(K_n, E)$ is finite,
- the order of Φ_E is relatively prime to p , and
- $E[p]$ is irreducible as a $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -representation.

Note that by the first assumption, $\text{III}(K_n, E)$ becomes finite (Lemma 2.2) and hence

$$\text{III}(K_n, E)[p^m] = \text{III}(K_n, E)[p^{2m}] \quad \text{for all sufficiently large } m.$$

The second assumption is needed to prove a correspondence between the flat cohomology and the Selmer group (Lemma 2.1). The third assumption is needed for the integrality of the p -adic L -function of E (i.e. $g_E(t) \in \mathbb{Z}_p[[t]]$; see (1.2)).

With the first two assumptions, one can define a 3-dimensional arithmetic BF theory [3]. The input data of such theory consists of

- (spacetime) the scheme $Y_n = \text{Spec}(\mathcal{O}_{\mathbb{Q}_n})$.
- (space of fields) the space $\mathcal{F}^m(Y_n)$.
- (action functional) an arithmetic BF-functional (see (2.1) and (3.1)):

$$\text{BF} : \mathcal{F}^m(Y_n) \longrightarrow \frac{1}{p^m} \mathbb{Z}/\mathbb{Z}$$

for each $n \geq 0$ and $m \geq 1$.

Then the output of the theory is the following arithmetic path integral:

$$\sum_{(a,b) \in \mathcal{F}^m(Y_n)} \exp(2\pi i \text{BF}(a, b)).$$

For the reason that the above sum is called an ‘arithmetic path integral’, we refer to [2, Section 1.3]. By Lemma 2.1, this sum becomes finite if we assume that $\text{Sel}(\mathbb{Q}_n, E[p^\infty])$ is finite. This follows from our finite assumption on $\text{Sel}(K_n, E)$ by Lemma 2.2. Since we will define and use the BF-functional over X_n , we have assumed that $\text{Sel}(K_n, E)$ is finite. In section 3, we will explain how to get the path integral over Y_n from the path integral over X_n .

Now we briefly review the p -adic L -function of E . Since E has good ordinary reduction at p , there exists a power series

$$(1.2) \quad g_E(t) \in \mathbb{Z}_p[[t]] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

which represents the p -adic L -function $L_p(E/\mathbb{Q}, s)$ of an elliptic curve (see [8] and [6, p. 459]). Under the assumption that $E[p]$ is an irreducible $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -module, $g_E(t) \in \mathbb{Z}_p[[t]]$ holds. Let $\alpha_p, \beta_p \in \overline{\mathbb{Q}}$ be defined by $\alpha_p + \beta_p = a_p$ and $\alpha_p \beta_p = p$, where $a_p = 1 + p - \tilde{E}(\mathbb{F}_p)$. Then p does not divide a_p , which means p splits in $\mathbb{Q}(\alpha_p, \beta_p)$. Let $\tau(\chi) \in \overline{\mathbb{Q}}$ be the

Gauss sum for a Dirichlet character χ . By the modularity of $E/\mathbb{Q}$, the L -value $L(E/\mathbb{Q}, \chi, 1)$ is defined and $L(E/\mathbb{Q}, \chi, 1)/\Omega_E$ is known to be algebraic by a theorem of Shimura, where $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{y}$. Let us fix a topological generator $\gamma_0 \in \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. If χ is viewed as a faithful character of $\text{Gal}(\mathbb{Q}_n/\mathbb{Q})$ with $n \geq 1$, then the conductor of χ is p^{n+1} and $\zeta = \chi(\gamma_0)$ is a p^n -th root of unity. Now the interpolation property of $g_E(t)$ is given by

$$g_E(0) = \frac{(1 - \beta_p p^{-1})^2 L(E/\mathbb{Q}, 1)}{\Omega_E},$$

$$g_E(\zeta - 1) = \frac{(\beta_p)^{n+1} L(E/\mathbb{Q}, \chi, 1)}{\tau(\chi) \Omega_E}$$

for $n \geq 1$. Sometimes $g_E(t)$ is called an analytic p -adic L -function of E , while there is the notion of an algebraic p -adic L -function of E defined by the generator of the characteristic ideal of the Pontrygin dual of the Selmer group $\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])$ which is a torsion $\mathbb{Z}_p[[t]]$ -module.² The Iwasawa main conjecture [6, Conjecture 4.16], which is now a theorem by Skinner-Urban [13], asserts that they are the same.

Let $|\cdot|_p$ be the p -adic absolute value on the algebraic closure $\overline{\mathbb{Q}}_p$ normalized by $|p|_p = p^{-1}$. Now we can state our main theorem.

Theorem 1.1. *For each $v \in Y_n$, let $c_v^{(p)}(E)$ be the highest power of p dividing the Tamagawa factor $c_v(E)$ for E at v . Then the following arithmetic path integral formula holds.*

$$\left| \prod_{\zeta^{p^n}=1} g_E(\zeta - 1) \right|_p^{-1} = \frac{|\widetilde{E}(\mathbb{F}_p)[p^\infty]|^2}{|E(\mathbb{Q}_n)[p^\infty]|} \cdot \prod_{\substack{v \in Y_n \\ v \nmid p, v \nmid N_E}} c_v^{(p)}(E) \cdot \lim_{m \rightarrow \infty} \sum_{(a,b) \in \mathcal{F}^m(Y_n)} \exp(2\pi i \text{BF}(a, b)),$$

where $\widetilde{E}$ is the reduction of E at p , and N_E is the conductor of E .

We prove this theorem in section 4. For the proof, we first derive a path integral formula (Lemma 4.1) in a more general context, using Mazur's control theorem [6, Theorem 4.1] and the Iwasawa main conjecture. Then we analyze the "error term" of Mazur's control theorem following the method of [5].

1.2. Open question. An interesting open question is to enlarge the space of fields $\mathcal{F}^m(Y_n)$ or modify the BF-functional so that we can obtain a path integral formula for the L -value $\prod_{\zeta^{p^n}=1} g_E(\zeta - 1)$ itself, which amounts to remove the p -adic absolute value from the formula in Theorem 1.1 incorporating p -adic unit information.

²The Selmer groups for each $n \in \mathbb{N} \cup \{\infty\}$ fit into the following exact sequences:

$$0 \longrightarrow E(\mathbb{Q}_n)[p^\infty] \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \text{Sel}(\mathbb{Q}_n, E[p^\infty]) \longrightarrow \text{III}(\mathbb{Q}_n, E)[p^\infty] \longrightarrow 0.$$

We refer to [6, chapter 2] for detailed definition.

2. The BF-functional for elliptic curves

We now recall the definition of the BF-functional in [3, p. 1303]. By [11, Corollary 3.4], we have a perfect pairing³:

$$\cup : H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m]) \times H_{\text{fppf}}^2(X_n, \mathcal{E}[p^m]) \longrightarrow H_{\text{fppf}}^3(X_n, \mathbb{G}_m)[p^m] ,$$

together with an isomorphism as in [11, p. 252]:

$$\text{inv} : H_{\text{fppf}}^3(X_n, \mathbb{G}_m) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} ,$$

which restricts to

$$\text{inv} : H_{\text{fppf}}^3(X_n, \mathbb{G}_m)[p^m] \xrightarrow{\sim} \frac{1}{p^m} \mathbb{Z}/\mathbb{Z} .$$

Finally, let

$$\delta : H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m]) \longrightarrow H_{\text{fppf}}^2(X_n, \mathcal{E}[p^m])$$

be the Bockstein map coming from the exact sequence:

$$0 \longrightarrow \mathcal{E}[p^m] \longrightarrow \mathcal{E}[p^{2m}] \xrightarrow{p^m} \mathcal{E}[p^m] \longrightarrow 0 .$$

Combining all these, we define the arithmetic BF-functional as follows:

$$(2.1) \quad \text{BF} : \mathcal{F}^m(X_n) \longrightarrow \frac{1}{p^m} \mathbb{Z}/\mathbb{Z}, \quad (a, b) \longmapsto \text{inv}(a \cup \delta b).$$

Lemma 2.1. *Let $\mathcal{O}$ be the ring of integers of a number field such that $\mathbb{Z} \hookrightarrow \mathcal{O}$ is ramified only at $p \in \mathbb{Z}$. Assume that the order of $\Phi_{\mathcal{E}}$ is relatively prime to p .*

- (1) $\mathcal{E} \otimes_{\mathbb{Z}} \mathcal{O}$ is the Néron model of E over $\mathcal{O}$.
- (2) The order of $\Phi_{\mathcal{E} \otimes_{\mathbb{Z}} \mathcal{O}}$ is the same as the order of $\Phi_{\mathcal{E}}$.
- (3) We have the following isomorphisms:

$$H_{\text{fppf}}^1(\text{Spec } \mathcal{O}, \mathcal{E}[p^m]) \cong \text{Sel}(\text{Frac}(\mathcal{O}), E[p^m])$$

$$H_{\text{fppf}}^1(\text{Spec } \mathcal{O}, \mathcal{E})[p^m] \cong \text{III}(\text{Frac}(\mathcal{O}), E)[p^m]$$

where $\text{Frac}(\mathcal{O})$ is the field of fractions of $\mathcal{O}$.

Proof. (1) follows because the étale base change of a Néron model is still a Néron model and our E has good ordinary reduction at p .

(2) Since $\mathbb{Z} \hookrightarrow \mathcal{O}$ is ramified only at $p \in \mathbb{Z}$, the number of connected component may vary at the primes in $\mathcal{O}$ lying over p . Since E has good ordinary reduction at p , our $\mathcal{E}$ is always connected at these primes.

(3) By (1) and (2), the first isomorphism comes from [3, Lemma A.2] and the second from [3, Lemma A.3]. $\square$

³By [11, p. 220], we have $H_{\text{fppf},c}^{\bullet}(X_n, -) \cong H_{\text{fppf}}^{\bullet}(X_n, -)$.

Lemma 2.2. *With the assumptions so far, the following holds.*

- (1) $E(K_n)$ and $\text{III}(K_n, E)$ are finite.
- (2) $\text{Sel}(\mathbb{Q}_n, E)$ is finite. Hence $E(\mathbb{Q}_n)$, $\text{III}(\mathbb{Q}_n, E)$, and $\text{Sel}(\mathbb{Q}_n, E[p^\infty])$ become finite.

Proof. For a number field F we have the following exact sequence ([6, chapter 2]):

$$(2.2) \quad 0 \longrightarrow E(F) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} \longrightarrow \text{Sel}(F, E) \longrightarrow \text{III}(F, E) \longrightarrow 0.$$

(1) Taking $F = K_n$ in (2.2), we immediately conclude that $\text{III}(K_n, E)$ is finite and $E(K_n) \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$, i.e., $E(K_n)$ is a torsion abelian group. Since $E(K_n)$ is a finitely generated abelian group by the Mordell-Weil theorem, we conclude that $E(K_n)$ is finite.

(2) From the inflation-restriction sequence for group cohomology, we get

$$\ker \left(\text{Sel}(\mathbb{Q}_n, E) \longrightarrow \text{Sel}(K_n, E)^{\text{Gal}(K_n/\mathbb{Q}_n)} \right) \subseteq H^1(\text{Gal}(K_n/\mathbb{Q}_n), E(K_n)).$$

Note that $E(K_n)_{\text{tors}} = E(K_n)$ by (1). Therefore, $\text{Sel}(\mathbb{Q}_n, E)$ is finite, which immediately says that $\text{Sel}(\mathbb{Q}_n, E[p^\infty])$ is finite. By the same argument as in the proof (1), we conclude that $E(\mathbb{Q}_n)$ and $\text{III}(\mathbb{Q}_n, E)$ are finite. $\square$

Proposition 2.3. *For every n and every sufficiently large m , we have*

$$\sum_{(a,b) \in \mathcal{F}^m(X_n)} \exp(2\pi i \text{BF}(a, b)) = |\text{Sel}(K_n, E[p^m])| \left| \frac{E(K_n)}{p^m E(K_n)} \right|.$$

Proof. The assertion follows from [3, Section 3] by noting that E is self-dual. $\square$

3. Isotypic components of the BF-functional

The $\text{Gal}(K_\infty/\mathbb{Q})$ -action on X_n induces by functoriality a $\text{Gal}(K_\infty/\mathbb{Q})$ -module structure on $H_{\text{fppf}}^\bullet(X_n, \mathcal{E}[p^m])$. Since $p-1$ is relatively prime to p , the $\text{Gal}(K/\mathbb{Q})$ -action on $H_{\text{fppf}}^\bullet(X_n, \mathcal{E}[p^m])$ is semisimple. Denote

$$(3.1) \quad \mathcal{F}_r^m(X_n) := H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_r \times H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_{-r},$$

so that we have

$$\mathcal{F}^m(X_n) = \bigoplus_{r=0}^{p-2} \mathcal{F}_r^m(X_n).$$

We will show that $\mathcal{F}_0^m(X_n) = \mathcal{F}^m(Y_n)$.

By functoriality, $\cup$ and δ are ω^r -equivariant. Hence they restrict to

$$\cup : H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_r \times H_{\text{fppf}}^2(X_n, \mathcal{E}[p^m])_s \longrightarrow H_{\text{fppf}}^3(X_n, \mathbb{G}_m)_{r+s},$$

$$\delta : H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_r \longrightarrow H_{\text{fppf}}^2(X_n, \mathcal{E}[p^m])_r.$$

Since the $\text{Gal}(K/\mathbb{Q})$ -action on

$$\text{inv} : H_{\text{fppf}}^3(X_n, \mathbb{G}_m) \xrightarrow{\sim} \frac{1}{p^m} \mathbb{Z} / \mathbb{Z}$$

is trivial, $H_{\text{fppf}}^3(X_n, \mathbb{G}_m)_{r+s} \neq 0$ if and only if $r + s \equiv 0 \pmod{p-1}$ so the BF-functional (2.1) splits into

$$\sum_{r=0}^{p-2} \text{BF}_r : \bigoplus_{r=0}^{p-2} \mathcal{F}_r^m(X_n) \longrightarrow \frac{1}{p^m} \mathbb{Z} / \mathbb{Z} .$$

Therefore, we have

$$\sum_{(a,b) \in \mathcal{F}^m(X_n)} \exp(2\pi i \text{BF}(a,b)) = \prod_{r=0}^{p-2} \sum_{(a,b) \in \mathcal{F}_r^m(X_n)} \exp(2\pi i \text{BF}(a,b)).$$

Proposition 3.1. *For every n and every sufficiently large m , we have*

$$\sum_{(a,b) \in \mathcal{F}_r^m(X_n)} \exp(2\pi i \text{BF}(a,b)) = |\text{Sel}(K_n, E[p^m])_r| \left| \left(\frac{E(K_n)}{p^m E(K_n)} \right)_{-r} \right|.$$

Proof. If $\delta b \neq 0$, then the sum over $a \in H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_{-r}$ becomes

$$\sum_a \exp(2\pi i \text{BF}(a,b)) = \sum_a \exp(2\pi i \cdot \text{inv}(a \cup \delta b)) = 0.$$

On the other hand, if $\delta b = 0$, then $\exp(2\pi i \text{BF}(a,b)) = 1$. Since δ is ω -equivariant,

$$(\ker \delta)_{-r} = H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_{-r} \cap \ker \delta.$$

Combining these, we get

$$\sum_{(a,b) \in \mathcal{F}_r^m(X_n)} \exp(2\pi i \text{BF}(a,b)) = |H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m])_r| |(\ker \delta)_{-r}|.$$

For each n and sufficiently large m , we have a factorization coming from [3, p. 1304]:

$$\begin{array}{ccc} H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m]) & \xrightarrow{\delta} & H_{\text{fppf}}^2(X_n, \mathcal{E}[p^m]) \\ & \searrow & \nearrow \\ & H_{\text{fppf}}^1(X_n, \mathcal{E})[p^m] & \end{array} ,$$

where the surjection fits into the Kummer sequence:

$$0 \longrightarrow \frac{E(K_n)}{p^m E(K_n)} \longrightarrow H_{\text{fppf}}^1(X_n, \mathcal{E}[p^m]) \longrightarrow H_{\text{fppf}}^1(X_n, \mathcal{E})[p^m] \longrightarrow 0 .$$

Consequently,

$$(\ker \delta)_{-r} = \left| \left(\frac{E(K_n)}{p^m E(K_n)} \right)_{-r} \right|.$$

The other factor is determined from (3) of Lemma 2.1. □

We conclude this section by realizing Proposition 3.1 as an arithmetic path integral on Y_n . For the reader's convenience, we begin with a lemma.

Lemma 3.2. *Let m be a positive integer.*

(1) *For each scheme S , the canonical map is an isomorphism:*

$$H_{\text{ét}}^{\bullet}(S, \mathcal{E}[p^m]_S) \xrightarrow{\sim} H_{\text{fppf}}^{\bullet}(S, \mathcal{E}[p^m]_S).$$

(2) *For each $n \geq 0$, the canonical map is an isomorphism:*

$$H_{\text{fppf}}^{\bullet}(Y_n, \text{Res}_{X_n/Y_n}(\mathcal{E}[p^m]_{X_n})) \xrightarrow{\sim} H_{\text{fppf}}^{\bullet}(X_n, \mathcal{E}[p^m]_{X_n}),$$

where Res denotes the Weil restriction.

Proof. (1) By [10, Theorem III.3.9], the canonical map for $\mathcal{E}$:

$$H_{\text{ét}}^{\bullet}(S, \mathcal{E}_S) \xrightarrow{\sim} H_{\text{fppf}}^{\bullet}(S, \mathcal{E}_S)$$

is an isomorphism. Hence the assertion follows from applying the five lemma to the long exact sequence associated to the following exact sequence of fppf sheaves:

$$0 \longrightarrow \mathcal{E}[p^m]_S \longrightarrow \mathcal{E}_S \xrightarrow{p^m} \mathcal{E}_S \longrightarrow 0.$$

(2) By Lemma 2.1 and [1, Proposition 7.6.6], the Weil restriction $\text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n})$ is a Néron model of its generic fiber:

$$(\text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n}))_{\mathbb{Q}_n} \cong \text{Res}_{K_n/\mathbb{Q}_n}(E_{K_n}).$$

Since $K_n/\mathbb{Q}_n$ is separable, the right hand side is an abelian variety over $\mathbb{Q}_n$ (cf. [9, p. 178]). Hence we have the following commutative square of abelian groups:

$$\begin{array}{ccc} H_{\text{ét}}^{\bullet}(Y_n, \text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n})) & \xrightarrow{\sim} & H_{\text{fppf}}^{\bullet}(Y_n, \text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n})) \\ \downarrow \wr & & \downarrow \\ H_{\text{ét}}^{\bullet}(X_n, \mathcal{E}_{X_n}) & \xrightarrow{\sim} & H_{\text{fppf}}^{\bullet}(X_n, \mathcal{E}_{X_n}) \end{array}$$

where the rows are isomorphisms by [11, Proposition III.0.4d] again, and the left column is an isomorphism by [14, Tag 03QP] because $X_n \rightarrow Y_n$ is finite.

On the other hand, by [7, Proposition 3.19], we have

$$|\Phi_{\text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n})}| = |\Phi_{\mathcal{E}_{X_n}}|,$$

which are relatively prime to p by assumption. Hence the following sequence of fppf sheaves is exact (note that the Weil restriction is left exact):

$$0 \longrightarrow \text{Res}_{X_n/Y_n}(\mathcal{E}[p^m]_{X_n}) \longrightarrow \text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n}) \xrightarrow{p^m} \text{Res}_{X_n/Y_n}(\mathcal{E}_{X_n}) \longrightarrow 0.$$

Therefore the assertion follows from applying the five lemma to the associated cohomology long exact sequence. $\square$

Since $(\mathcal{O}_{K_n})_0 = \mathcal{O}_{\mathbb{Q}_n}$, the ω^r -isotypic decomposition of $\mathcal{O}_{K_n}$ becomes

$$\mathcal{O}_{K_n} = \mathcal{O}_{\mathbb{Q}_n} \oplus \bigoplus_{r=1}^{p-2} (\mathcal{O}_{K_n})_r,$$

where each factor is canonically an $\mathcal{O}_{\mathbb{Q}_n}$ -module. Hence, from Lemma 3.2, we get

$$\begin{aligned} H_{\text{fppf}}^\bullet(X_n, \mathcal{E}[p^m]) &\cong H_{\text{fppf}}^\bullet(X_n, \mathcal{E}[p^m] \otimes_{\mathbb{Z}} \mathcal{O}_{K_n}) \\ &\cong H_{\text{fppf}}^\bullet(Y_n, \text{Res}_{X_n/Y_n}(\mathcal{E}[p^m] \otimes_{\mathbb{Z}} \mathcal{O}_{K_n})) \\ &\cong H_{\text{fppf}}^\bullet(Y_n, \mathcal{E}[p^m]) \oplus \bigoplus_{r=1}^{p-2} H_{\text{fppf}}^\bullet(Y_n, \mathcal{E}[p^m] \otimes_{\mathbb{Z}} (\mathcal{O}_{K_n})_r) \end{aligned}$$

because taking the $\text{Gal}(K/\mathbb{Q})$ -invariant of abelian p -groups is an exact functor. Consequently, (3.1) can be rewritten as

$$\mathcal{F}_r^m(X_n) \cong H_{\text{fppf}}^1(Y_n, \mathcal{E}[p^m] \otimes_{\mathbb{Z}} (\mathcal{O}_{K_n})_r) \times H_{\text{fppf}}^1(Y_n, \mathcal{E}[p^m] \otimes_{\mathbb{Z}} (\mathcal{O}_{K_n})_{-r}).$$

Moreover, we have the corresponding Bockstein map:

$$\delta : H_{\text{fppf}}^1(Y_n, \mathcal{E}[p^m] \otimes_{\mathbb{Z}} (\mathcal{O}_{K_n})_{-r}) \longrightarrow H_{\text{fppf}}^2(Y_n, \mathcal{E}[p^m] \otimes_{\mathbb{Z}} (\mathcal{O}_{K_n})_{-r}).$$

Therefore, Proposition 3.1 can be rewritten as an arithmetic path integral on Y_n as desired. In particular, we have $\mathcal{F}_0^m(X_n) = \mathcal{F}^m(Y_n)$ and hence (for sufficiently large m)

$$(3.2) \quad \sum_{(a,b) \in \mathcal{F}^m(Y_n)} \exp(2\pi i \text{BF}(a,b)) = |\text{Sel}(\mathbb{Q}_n, E[p^m])| \left| \frac{E(\mathbb{Q}_n)}{p^m E(\mathbb{Q}_n)} \right|.$$

4. The proof of the main theorem

In this section, we prove Theorem 1.1. We begin with a lemma. Define abelian groups A_n and B_n via the following exact sequence:

$$0 \longrightarrow A_n \longrightarrow \text{Sel}(\mathbb{Q}_n, E[p^\infty]) \longrightarrow \text{Sel}(\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n} \longrightarrow B_n \longrightarrow 0,$$

where $\text{Sel}(F, E[p^\infty])$ is the Selmer group over F associated to $E[p^\infty]$. By Mazur's control theorem [6, Theorem 4.1], A_n and B_n are finite p -groups whose orders are bounded as $n \rightarrow \infty$.

Lemma 4.1. *For each $n \geq 0$, the BF functional satisfies the following formula:*

$$\left| \prod_{\zeta^{p^n}=1} g_E(\zeta-1) \right|_p^{-1} = \frac{1}{|E(\mathbb{Q}_n)[p^\infty]|} \frac{|B_n|}{|A_n|} \lim_{m \rightarrow \infty} \sum_{(a,b) \in \mathcal{F}^m(Y_n)} \exp(2\pi i \text{BF}(a,b)).$$

Proof. The proof is based on the Iwasawa main conjecture [6, Conjecture 4.16] and Mazur's control theorem.

Since $E(\mathbb{Q}_n)$ is finite by Lemma 2.2, the following composition is an isomorphism for every sufficiently large m :

$$E(\mathbb{Q}_n)[p^\infty] = E(\mathbb{Q}_n)[p^m] \hookrightarrow E(\mathbb{Q}_n) \longrightarrow \frac{E(\mathbb{Q}_n)}{p^m E(\mathbb{Q}_n)}.$$

Consequently, for sufficiently large m ,

$$\left| \frac{E(\mathbb{Q}_n)}{p^m E(\mathbb{Q}_n)} \right| = |E(\mathbb{Q}_n)[p^\infty]|.$$

Hence (3.2) can be rewritten as

$$\sum_{(a,b) \in \mathcal{F}^m(Y_n)} \exp(2\pi i \text{BF}(a,b)) = |\text{Sel}(\mathbb{Q}_n, E[p^m])| \cdot |E(\mathbb{Q}_n)[p^\infty]|.$$

Denote $(\cdot)^\vee$ the Pontryagin dual of abelian groups and let

$$V_n := \text{Sel}(\mathbb{Q}_n, E[p^\infty])^\vee.$$

Choose a topological generator $\gamma \in \Gamma$, which gives a topological ring isomorphism

$$\Lambda := \mathbb{Z}_p[[t]] \xrightarrow{\sim} \mathbb{Z}_p[[\Gamma]], \quad t \longmapsto \gamma - 1.$$

Along this isomorphism, we can write

$$(\text{Sel}(\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n})^\vee \cong \frac{V_\infty}{((t+1)^{p^n} - 1)V_\infty}.$$

Note that V_∞ is a torsion Λ -module by [5, Theorem 1.5]. Moreover, $g_E(t) \in \Lambda$ by [6, p. 459], and V_∞ has no nonzero pseudo-null Λ -submodule by [5, Proposition 4.15]. Applying the structure theorem for Λ -modules [6, Theorem 3.1] to V_∞ (cf. [12, Lemma 4]) and using [6, Exercise 3.7], we get

$$\left| \frac{V_\infty}{((t+1)^{p^n} - 1)V_\infty} \right| = \left| \frac{\Lambda}{(g_E(t), (t+1)^p - 1)} \right| = u \cdot \prod_{\zeta^{p^n}=1} g_E(\zeta - 1), \quad u \in \mathbb{Z}_p^\times.$$

This in turn gives the following equalities:

$$\begin{aligned} |\text{Sel}(\mathbb{Q}_n, E[p^\infty])| &= |V_n| \\ &= \frac{|A_n^\vee|}{|B_n^\vee|} \left| \frac{V_\infty}{((t+1)^{p^n} - 1)V_\infty} \right| = \frac{|A_n|}{|B_n|} \cdot u \cdot \prod_{\zeta^{p^n}=1} g_E(\zeta - 1). \end{aligned}$$

Since $\text{Sel}(\mathbb{Q}_n, E[p^\infty])$, A_n , and B_n are abelian p -groups, we conclude that

$$\frac{|B_n|}{|A_n|} |\text{Sel}(\mathbb{Q}_n, E[p^\infty])| = \left| \prod_{\zeta^{p^n}=1} g_E(\zeta - 1) \right|_p^{-1},$$

which finishes the proof. $\square$

Let us return to the proof of Theorem 1.1. It remains to determine $|A_n|$ and $|B_n|$ in Lemma 4.1. We begin with the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Sel}(\mathbb{Q}_n, E[p^\infty]) & \longrightarrow & H^1(\mathbb{Q}_n, E[p^\infty]) & \longrightarrow & \mathcal{G}_E(\mathbb{Q}_n) \longrightarrow 0 \\ & & \downarrow s_n & & \downarrow h_n & & \downarrow g_n \\ 0 & \longrightarrow & \text{Sel}(\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & H^1(\mathbb{Q}_\infty, E[p^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}_E(\mathbb{Q}_\infty) \end{array},$$

where $\mathcal{G}_E$ is essentially defined to be the cokernel of $\mathrm{Sel}(-, E[p^\infty]) \hookrightarrow H^1(-, E[p^\infty])$. See [5, pp. 451–452] for the precise description of this diagram. By our assumptions and the proof of [5, Lemma 3.1], we have

$$|\ker h_n| = |E(\mathbb{Q}_n)[p^\infty]|.$$

From the snake lemma together with [5, Lemma 3.2], we get

$$\frac{|B_n|}{|A_n|} = \frac{|\mathrm{coker} s_n|}{|\ker s_n|} = \frac{|\ker g_n|}{|\ker h_n|} = \frac{|\ker g_n|}{|E(\mathbb{Q}_n)[p^\infty]|}.$$

Since $\Gamma_n \cong \mathbb{Z}_p$, we may apply [5, Lemma 4.7] to the above diagram. Using [5, Lemma 3.3], [5, Lemma 3.4], and [5, Proposition 4.8], we get

$$|\ker g_n| = |\widetilde{E}(\mathbb{F}_p)[p^\infty]|^2 \cdot \prod_{\substack{v \in Y_n \\ v \nmid p, v \nmid N_E}} c_v^{(p)}(E).$$

Note that $\mathbb{Q}_n/\mathbb{Q}$ is totally ramified at p so the unique prime in Y_n lying over p has the residue field $\mathbb{F}_p$. This concludes the proof of Theorem 1.1.

ACKNOWLEDGEMENTS. Jeehoon Park was supported by the National Research Foundation of Korea (NRF-2021R1A2C1006696) and the National Research Foundation of Korea grant (NRF-2020R1A5A1016126) funded by the Korea government (MSIT). Junyeong Park was supported by Samsung Science and Technology Foundation under Project Number SSTF-BA2001-02, the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2024-00341372), and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2024-00449679).

References

- [1] S. Bosch, W. Lütkebohmert and M. Raynaud: *Néron models*, Springer-Verlag (1990).
- [2] M. Carlson, C. Hee-Joong, D. Kim, M. Kim, J. Park and H. Yoo: *Path integrals and p -adic L -functions*, Bull. London Math. Soc., **56** (2024), 1951–1966.
- [3] M. Carlson and M. Kim: *A note on abelian arithmetic BF-theory*, Bull. London Math. Soc., **54** (2022), 1299–1307.
- [4] K. Česnavičius: *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31** (2016), 31–61.
- [5] R. Greenberg: *Iwasawa theory for elliptic curves*; in Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., **1716** (1999), 51–144.
- [6] R. Greenberg: *Introduction to Iwasawa theory for elliptic curves*; in Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., **9** (2001), 407–464.
- [7] D. Lorenzini: *Torsion and Tamagawa numbers*, Ann. Inst. Fourier **61** (2011), 1995–2037.
- [8] B. Mazur, J. Tate and J. Teitelbaum: *On p -adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.
- [9] J.S. Milne: *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.
- [10] J.S. Milne: *Étale cohomology*, Princeton University Press (1980).
- [11] J. S. Milne: *Arithmetic duality theorems*, BookSurge, LLC, Charleston, SC, 2nd ed. (2006).
- [12] C. Skinner: *Lectures on the Iwasawa theory of elliptic curves*, Lecture notes for the Arizona Winter school, <https://swc-math.github.io/aws/2018/2018SkinnerNotes.pdf>
- [13] C. Skinner and E. Urban: *The Iwasawa Main Conjectures for GL_2* , Invent. math. **195** (2014), 1–277.

[14] The stacks project authors: Stacks project, <https://stacks.math.columbia.edu> (2018).

Jeehoon Park
QSMS, Seoul National University
1 Gwanak-ro, Gwanak-gu, Seoul 08826
Korea
e-mail: jpark.math@gmail.com

Junyeong Park
Department of Mathematics Education, Chonnam National University
77, Yongbong-ro, Buk-gu, Gwangju 61186
Korea
e-mail: junyeongp@gmail.com