ON THE BIRCH-SWINNERTON-DYER CONJECTURE FOR RATIONAL ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION AND ANALYTIC RANK ONE

YONGXIONG LI, YE TIAN, XIAOJUN YAN, XIUWU ZHU

ABSTRACT. Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field K, and let p be a prime that splits in K. Let $L(E,s)$ denote the complex L-series of E over $\mathbb{Q}$, which is a holomorphic function of s on the whole complex plane, according to a theorem of Deuring. In this paper, we assume that $L(E,s)$ has a simple zero at $s=1$, and that E has good ordinary reduction at p when $p=2$. We show that the p-part of the refined Birch-Swinnerton-Dyer formula for E holds. We present two applications of this result: (1) Based on recent progress on the 2-converse theorem for rational elliptic curves, we show that if the $\mathbb{Z}_2$-corank of the 2-power Selmer group of E is one, and E has good ordinary reduction at 2, then the 2-part of the refined Birch-Swinnerton-Dyer formula for E holds; (2) By combining earlier works of one of us on the congruent number problem, we prove that there are infinitely many rational elliptic curves with both algebraic and analytic ranks one, whose conductors can have any prescribed number of prime factors, for which the full Birch-Swinnerton-Dyer conjecture holds.

1. INTRODUCTION

1.1. **The main result.** Let E be an elliptic curve defined over $\mathbb{Q}$. We assume that E has complex multiplication, i.e., $\mathrm{End}_{\overline{\mathbb{Q}}}(E)\otimes_{\mathbb{Z}}\mathbb{Q}$ is an imaginary quadratic number field. Denote by $E(\mathbb{Q})$ (resp. $Ш(E/\mathbb{Q})$) the Mordell–Weil (resp. the Shafarevich-Tate group) of E. Let $L(E,s)$ be the complex L-series of E, which, by a theorem of Deuring, is a holomorphic function on the entire complex s-plane. Let p be a prime at which E has potentially good ordinary reduction, i.e., E has good ordinary reduction at all primes above p in some finite extension of $\mathbb{Q}$.

The primary goal of this paper is to prove the following result:

Theorem 1.1. *Assume that $L(E,s)$ has a simple zero at $s=1$.*

(i) *The Mordell-Weil group $E(\mathbb{Q})$ has rank one and the Shafarevich-Tate group $Ш(E/\mathbb{Q})$ is finite;*
(ii) *Assume further that E has good ordinary reduction at p if $p=2$. Then the p-part of the refined Birch-Swinnerton-Dyer formula for E holds.*

1.2. **Historical Background and Our Approach.** We now provide some historical background for Theorem 1.1. Part (i) follows from the theorems of Gross-Zagier and Kolyvagin. For part (ii), when p is an odd good ordinary prime, the p-part of the refined Birch-Swinnerton-Dyer formula was established by Perrin-Riou [40], using the following three ingredients:

- The complex and p-adic Gross-Zagier formulae [31], [40];
- Schneider's algebraic descent methods [47];
- The Iwasawa main conjecture over imaginary quadratic fields [45].

Therefore, Theorem 1.1 essentially covers two distinct cases:

- **Odd bad case**: p is an odd potentially good ordinary prime;
- **Even case:** $p=2$.

Our approach generalizes Perrin-Riou's proof, leveraging recent advances on the complex and p-adic Gross-Zagier formulae ([53], [18], [19]), the Iwasawa main conjecture over imaginary quadratic fields ([32]), and an extension of Yager's theorem to $p=2$ ([35]). The main challenge arises in the even case. Schneider's algebraic descent methods fail in this case for two reasons:

2010 *Mathematics Subject Classification.* 11G40 (primary), 11G05, 11R23 (secondary).

- Since the Tamagawa numbers are even, the Mazur module defined via global flat cohomology cannot coincide with the classical Selmer group when E has a bad prime (see [36, Appendix] and [46, Lemma 6.6]).
- Schneider's proof depends on Mazur's theorem, which asserts the non-existence of certain non-zero finite submodules. However, this result holds only for $p \neq 2$ (see [47, Pages 338 and 340] and [36, Corollary 5.12]).

We assume that the elliptic curve E has complex multiplication (CM) by an imaginary quadratic field K. To address the aforementioned obstacles, we consider a base change of E to certain quadratic extension F over K, such that E has good reduction everywhere over F, and the analytic rank of E/F is equal to that of E/K. The first assumption allows us to reduce the study of Mazur modules to the study of Selmer groups. Based on the recent development of the rank zero Birch-Swinnerton-Dyer formula for CM elliptic curves [4], the second assumption ensures that once we can prove the algebraic analogue of the Birch-Swinnerton-Dyer formula for E/F we get the formula for E/K.

We apply the following two approaches:

(1) We generalize the work of Perrin-Riou and Schneider (see [41], [48]) on the isogeny invariance of the product of algebraic p-adic L-function and complex period of an abelian variety to the case where $p = 2$. Using the isogeny invariance theorem for the Birch-Swinnerton-Dyer conjecture ([37]), we can prove the even case, provided that F/K is unramified at 2.

(2) We draw upon recent works by Coates (see [9], [13]) regarding Iwasawa theory for elliptic curves with complex multiplication at $p = 2$. These works involve both finite-level descent and infinite descent along the Coates-Wiles $\mathbb{Z}_2$-extension. We can then identify a field F that satisfies the conditions mentioned above and link the descent of E/F to E/K using Coates's method.

To handle the descent for E/F, we employ methods from Greenberg (see [27], [29] and [28]), and from this, we establish the non-existence of non-zero finite submodules.

1.3. **Outline of the Proof of the Main Theorem.** We now give a brief overview of the proof of Theorem 1.1. Assume that E has CM by the ring $\mathcal{O}_K$ of integers in K. The potentially good ordinary assumption on p implies that p splits in K, i.e., $p\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{p}^*$. The crucial part is to establish the p-adic Birch-Swinnerton-Dyer conjecture for E over K, or more precisely, the $\mathfrak{p}$-adic Birch-Swinnerton-Dyer conjecture for φ, where φ is the Hecke character over K associated with E. The proof proceeds by considering the following two cases:

(I) If p is an odd potentially good ordinary prime, we can find a finite Galois extension F over K such that: (1) E has good ordinary reduction at all primes above p in F; (2) the Galois group $\Delta = \mathrm{Gal}(F/K)$ is cyclic, with order dividing $w_K = |\mathcal{O}_K^\times|$, thus prime to p. Since the algebraic descent methods in [47] are Galois-equivariant, we can apply these methods to the elliptic curve E/F and consider the Δ-invariant part of the descent diagrams. This enables us to establish an algebraic analogue of the Birch-Swinnerton-Dyer conjecture for E/K. The p-adic Birch-Swinnerton-Dyer conjecture then follows from the Iwasawa main conjecture [45] and Yager's theorem [52]. Let E^F denote the quadratic twist of E by the extension F/K. The proof involves comparing the periods and descent data between E and E^F.

(II) If $p = 2$, we can assume that E is a quadratic twist of $X_0(49)$ by $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, where $D \equiv 1 \bmod 4$ is a square-free integer. We use the same notation as in (I). For $\alpha \in \mathcal{O}_K$, let E_α denote the group of α-division points of $E(\overline{K})$. For any integral ideal $\mathfrak{b}$ in $\mathcal{O}_K$, we define $E_\mathfrak{b} = \cap_{\alpha \in \mathfrak{b}} E_\alpha$. Let $F = K(E_{\mathfrak{p}^2})$. A fundamental result of Coates-Wiles guarantees that E has good reduction everywhere over F, eliminating the connected component problem between Mazur modules and Selmer groups. However, the twisted curve E^F depends on the behavior of E along the extension F/K. In this context, Choi and Coates ([9], [13], see also [23]) demonstrated that the algebraic and analytic ranks of E^F are zero, the 2-part of $Ш(E^F/K)$ is trivial, and the 2-part of the refined Birch-Swinnerton-Dyer formula for E^F holds. Consequently, the arithmetic of E/K is equivalent to that of E/F in the sense of the 2-part Birch-Swinnerton-Dyer conjecture. Let F_{cyc} be the cyclotomic $\mathbb{Z}_2$-extension over F, and let $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$ denote the p-power Selmer group of E over F_{cyc}. Define $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$. Using a variation of Greenberg's methods, we can prove the non-existence of non-zero finite Γ-submodules in the Pontryagin dual of $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$. Therefore, Schneider's descent methods are applicable to E/F, enabling us to establish an algebraic analogue 2-adic Birch-Swinnerton-Dyer formula for E/K. The 2-adic Birch-Swinnerton-Dyer conjecture follows by the Iwasawa main conjecture [32] and an extension of Yager's theorem to $p = 2$ [35].

Once the p-adic Birch-Swinnerton-Dyer formula has been established, Theorem 1.1 follows in the standard manner, utilizing both the complex and p-adic Gross-Zagier formulae ([7], [53]).

It is worth noting that, using our first approach–specifically, the isogeny invariance of the product for the algebraic 2-adic L-functions and complex periods of abelian varieties–we can establish a more general case for the algebraic analogue of the 2-adic Birch-Swinnerton-Dyer formula for CM elliptic curve E over a finite abelian extension F_0 over K satisfying Shimura's conditions, when E has good ordinary reduction at all primes above 2. This result holds provided we can find a quadratic extension F/F_0 such that E/F has good reduction everywhere, E^F has analytic rank zero, and F/F_0 is unramified at all primes above 2. In a forthcoming paper [34], we will generalize Yager's theorem to all primes that split in a general imaginary quadratic field K. We will also employ a method introduced by Perrin-Riou [42], which uses universal norms to handle the algebraic descent formula, thereby resolving the issue of finite submodules

1.4. **Applications and Concrete Examples.** Let $\mathrm{Sel}_E(\mathbb{Q})_2$ denote the 2-power Selmer group of E over $\mathbb{Q}$, and let $\mathrm{corank}_{\mathbb{Z}_2}\mathrm{Sel}_E(\mathbb{Q})_2$ be the $\mathbb{Z}_2$-rank of the Pontryagin dual of $\mathrm{Sel}_E(\mathbb{Q})_2$. Combining with the 2-converse theorem (proven in [5], [3], see also [6], [50]), Theorem 1.1 implies the following:

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. Assume that E has good ordinary reduction at 2. If $\mathrm{corank}_{\mathbb{Z}_2}\mathrm{Sel}_E(\mathbb{Q})_2 = 1$, then $E(\mathbb{Q})$ has rank 1 and $Ш(E/\mathbb{Q})$ is finite. Moreover, the 2-part of the refined Birch-Swinnerton-Dyer formula of E holds.*

In practice, using 2-descent method, computing the root number $\epsilon(E/\mathbb{Q})$, and applying the 2-parity theorem of Dokchitser brothers (see [20]), one can easily verify the corank condition in the above theorem. As a result, Theorem 1.2 also implies several earlier results in [14].

Next, we present several examples. The following theorem establishes that there are infinitely many elliptic curves over $\mathbb{Q}$ of rank one, whose conductors possess arbitrarily many prime factors, for which the full Birch-Swinnerton-Dyer conjecture holds.

Theorem 1.3. *Let $n \equiv 5 \bmod 8$ be a square-free positive integer, whose prime factors are all congruent to 1 modulo 4. Assume that $\mathbb{Q}(\sqrt{-n})$ has no ideal class of order 4. Then the full Birch-Swinnerton-Dyer conjecture holds for the elliptic curve $y^2 = x^3 - n^2x$ over $\mathbb{Q}$. In particular, for any prime $p \equiv 5 \bmod 8$, the full Birch-Swinnerton-Dyer conjecture holds for $y^2 = x^3 - p^2x$.*

Proof. An induction argument (see [49] and [51]) shows the Heegner point associated to $y^2 = x^3 - x$ and $\mathbb{Q}(\sqrt{-n})$ has infinite order. Moreover, by applying the Gross-Zagier formula [7], the 2-part of the refined Birch-Swinnerton-Dyer formula for the curve $y^2 = x^3 - n^2x$ is also verified. As a result, both the analytic rank and Mordell-Weil rank of $y^2 = x^3 - n^2x$ over $\mathbb{Q}$ are equal to one, and the Shafarevich-Tate group of $y^2 = x^3 - n^2x$ is finite.

By the theorems of Perrin-Riou [40] and Kobayashi [33], the p-part of the refined Birch-Swinnerton-Dyer formula holds for all primes $p \nmid 2n$. Additionally, by Theorem 1.1, the p-part of the refined Birch-Swinnerton-Dyer formula holds for all primes p dividing n, since all primes $p \equiv 1 \bmod 4$ are potentially good ordinary primes for the curve $y^2 = x^3 - n^2x$. □

Example 1.4. *The number $p = 1493$ is the smallest prime congruent to 5 modulo 8 such that the elliptic curve $y^2 = x^3 - p^2x$ has rank one and a non-trivial Shafarevich-Tate group. Specifically, the associated Heegner point (x, y) has coordinates*

$$x = \frac{24561535499147214939689754594226969327289514983716301314 53}{29585011828542075719444686875619200646812053585105 29},$$
$$y = \frac{12172578066826359687361812381055798397237566018418043946536533570990618109872158526010 0}{16091910960547986287175324647321077268221974568783910945697471178779686889283 3}.$$

It can be shown that the free part of the Mordell-Weil group of the elliptic curve $y^2 = x^3 - p^2x$ over $\mathbb{Q}$ is generated by

$$\left[\frac{1674371133}{744769}, -\frac{51224214734700}{642735647}\right].$$

By Theorem 1.3, it follows that the Shafarevich-Tate group of $y^2 = x^3 - p^2x$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$.

The remainder of this paper is organized as follows. In Section 2, we establish the notation and conventions. Sections 3 through 7 are dedicated to proving the p-adic Birch-Swinnerton-Dyer conjecture for E/K. In Section 8, we introduce both the complex and p-adic Gross-Zagier formulae, and in Section 9, we complete the proof of Theorem 1.1. The first appendix (Section 10) provides a detailed proof

for the non-existence of certain non-trivial finite submodules using Greenberg's methods. In the second appendix, we employ variants of the algebraic p-adic L-functions and periods under isogeny, as developed by Perrin-Riou and Schneider, to offer an alternative proof of the algebraic analogue of the p-adic Birch-Swinnerton-Dyer conjecture for $p = 2$.

Acknowledgement We dedicate this paper to the memory of John Coates, whose unwavering encouragement and support have been instrumental in our exploration of Iwasawa theory for elliptic curves with complex multiplication, particularly in the case of the prime $p = 2$ and its applications to analytic rank one. It was John's insight that highlighted the role of the finite submodule issue in the CM Iwasawa theory at $p = 2$. In this paper, we pay tribute to his pioneering contributions, recognizing the profound and lasting impact his groundbreaking research has had on our own.

2. Notation and conventions

2.1. General Notation.

- For a field k, we denote by $\overline{k}$ an algebraic closure of k.
- For a finite set S, we denote by $|S|$ the cardinality of S.
- For an abelian group $\mathfrak{A}$ and a ring R, we define $\mathfrak{A}_R := \mathfrak{A} \otimes_{\mathbb{Z}} R$ as an R-module. For two abelian groups $\mathfrak{A}_1$ and $\mathfrak{A}_2$ such that $\mathfrak{A}_1 \subset \mathfrak{A}_2$ with finite index, we denote by $[\mathfrak{A}_2 : \mathfrak{A}_1]$ the index of $\mathfrak{A}_1$ in $\mathfrak{A}_2$.
- For an abelian group $\mathfrak{A}$ and a positive integer n, we define $\mathfrak{A}_n := \ker(\mathfrak{A} \xrightarrow{n} \mathfrak{A})$. For a prime p, we set $\mathfrak{A}(p) = \cup_{n\geq 1}\mathfrak{A}_{p^n}$.
- For an abelian group $\mathfrak{A}$, we denote by $\mathfrak{A}_{\mathrm{tor}}$ the torsion subgroup of $\mathfrak{A}$. We set $\mathfrak{A}_{/\mathrm{tor}} = \mathfrak{A}/\mathfrak{A}_{\mathrm{tor}}$. Additionally, we define $\mathfrak{A}_{\mathrm{div}}$ to be the divisible part of $\mathfrak{A}$, and set $\mathfrak{A}_{/\mathrm{div}} = \mathfrak{A}/\mathfrak{A}_{\mathrm{div}}$.
- For a commutative ring R, we denote by $R^\times$ the group of units in R.

2.2. Notation in Number theory.

- For any number field (resp. local field) $\mathfrak{F}$, we denote by $\mathcal{O}_{\mathfrak{F}}$ the ring of integers in $\mathfrak{F}$. For a prime ideal $\mathfrak{p}$ in a number field $\mathfrak{F}$, we write $\mathfrak{F}_{\mathfrak{p}}$ for the completion of $\mathfrak{F}$ at $\mathfrak{p}$. We denote by $\mathbb{C}_p$ the completion of $\overline{\mathbb{Q}}_p$. As usual, we set $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$.
- Fix embeddings
$$\iota_\infty : \overline{\mathbb{Q}} \to \mathbb{C} \quad \text{and} \quad \iota_p : \overline{\mathbb{Q}} \to \mathbb{C}_p$$
such that $\iota_p = \iota \circ \iota_\infty$ for an isomorphism $\iota : \mathbb{C} \xrightarrow{\sim} \mathbb{C}_p$.
- Let $\mathrm{ord}_p(\cdot)$ denote the additive valuation on $\mathbb{C}_p$, normalized by $\mathrm{ord}_p(p) = 1$.
- Fix a nontrivial additive character $\psi : \mathbb{Q}_p \to \mathbb{C}_p^\times$ of conductor $\mathbb{Z}_p$. For a character $\chi : \mathbb{Q}_p^\times \to \mathbb{C}_p^\times$ of conductor p^n with $n \geq 0$, define the root number
$$\tau(\chi, \psi) = p^{-n} \int_{v_p(t)=-n} \chi^{-1}(t)\psi(t)dt,$$
where dt is the Haar measure on $\mathbb{Q}_p$ normalized so that $\mathrm{Vol}(\mathbb{Z}_p, dt) = 1$.
- Let E be an elliptic curve defined over a number field $\mathfrak{K}$, and let p be a potentially good ordinary prime for E. Denote by $(\cdot,\cdot)_\infty$ the normalized Néron -Tate height pairing, and by $(\cdot,\cdot)_p$ the p-adic height pairing associated with the cyclotomic character over $\mathfrak{K}$. Suppose $P_1, \cdots, P_r \in E(\mathfrak{K})$ form a $\mathbb{Q}$-basis of $E(\mathfrak{K})_{\mathbb{Q}}$. Then the (real) regulator and the p-adic regulator of $E(\mathfrak{K})$ are defined by
$$R_\infty(E/\mathfrak{K}) = \frac{\det((P_i, P_j)_\infty)_{r\times r}}{[E(\mathfrak{K}) : \sum_i \mathbb{Z}P_i]^2} \quad \left(\text{resp.} \quad R_p(E/\mathfrak{K}) = \frac{\det((P_i, P_j)_p)_{r\times r}}{[E(\mathfrak{K}) : \sum_i \mathbb{Z}P_i]^2}\right).$$
- Let K be an imaginary quadratic number field. For a character χ of $\widehat{K}^\times$, denote its conductor by $\mathfrak{f}_\chi \subset \mathcal{O}_K$. For an elliptic curve E over K with complex multiplication by $\mathcal{O}_K$, let $\mathfrak{f}_E$ denote its conductor, i.e., the conductor of the associated Hecke character $\varphi_E = \varphi$. For nonzero integral ideals $\mathfrak{g}$ and $\mathfrak{a}$ of $\mathcal{O}_K$, let $\mathfrak{g}^{(\mathfrak{a})}$ denote the part of $\mathfrak{g}$ relatively prime to $\mathfrak{a}$. Let $\mathbb{D}$ be the completion of the maximal unramified extension of $\mathbb{Z}_p$, and let $\mathbb{D}_\chi$ be the finite extension of $\mathbb{D}$ generated by the values of χ. Let L/K be an abelian extension with Galois group $\mathcal{G} = \mathrm{Gal}(L/K) \cong \Delta' \times \Gamma$, where Δ' a finite group and $\Gamma \cong \mathbb{Z}_p^d$ for some nonnegative integer $d \leq 2$. For any $\mathbb{D}[[\mathcal{G}]]$-module $\mathfrak{M}$ and character χ of Δ', define the χ-isotypic component of $\mathfrak{M}$ as
$$\mathfrak{M}_\chi := \mathfrak{M} \otimes_{\mathbb{D}[[\mathcal{G}]],\chi} \mathbb{D}_\chi[[\Gamma]],$$

where the tensor product is taken via the character $\chi : \Delta' \to \mathbb{D}_\chi^\times$, extended to $\mathbb{D}[[\mathcal{G}]] \to \mathbb{D}_\chi[[\Gamma]]$.

3. Descent theory over the fields K and F

Throughout this section, we assume $p = 2$. Let $A = X_0(49)$, and let $E = A^{(D)}$ denote the quadratic twist of A by the quadratic extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, where D is a square-free integer satisfying $D \equiv 1(\text{ mod } 4)$. Recall that $2\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{p}^*$, and let $F = K(E_{\mathfrak{p}^2})$. In the following, we always consider E as defined over K.

For any element $\alpha \in \mathcal{O}_K$, we denote by E_α the group of α-torsion points of $E(\overline{K})$. For any integral ideal $\mathfrak{b}$ in $\mathcal{O}_K$, we define $E_\mathfrak{b} := \cap_{\alpha \in \mathfrak{b}} E_\alpha$, $E(\mathfrak{b}) := \cup_{n \geq 1} E_{\mathfrak{b}^n}$.

Let M/K be any algebraic extension. The $\mathfrak{p}$-power Selmer group of E over M is defined via the exact sequence

$$0 \to \mathrm{Sel}_E(M)_\mathfrak{p} \to H^1(M, E(\mathfrak{p})) \to \prod_v H^1(M_v, E)$$

where the product is taken over all finite places v of M. Let S be a finite set of finite places of M. The relaxed Selmer group at S is defined by the exact sequence:

$$0 \to \mathrm{Sel}_E^S(M)_\mathfrak{p} \to H^1(M, E(\mathfrak{p})) \to \prod_{v \notin S} H^1(M_v, E)$$

where the product ranges over all finite places v of M not lying above any place in S.

Let $\mathcal{P}$ denote the set of the primes lying above $\mathfrak{p}$, and let $\mathcal{B}$ denote the set of the primes where E has bad reduction. Set $\mathcal{W} = \mathcal{P} \cup \mathcal{B}$. With these definitions, we obtain an exact sequence

$$0 \to \mathrm{Sel}_E(K)_\mathfrak{p} \to \mathrm{Sel}_E^\mathcal{W}(K)_\mathfrak{p} \xrightarrow{\mathfrak{r}} \prod_{v \in \mathcal{W}} H^1(K_v, E)_{\mathfrak{p}^\infty} \to \mathrm{coker}(\mathfrak{r}) \to 0. \tag{3.1}$$

Let φ denote the Hecke character associated to E over K.

Lemma 3.1.

(1) *If $v \in \mathcal{B}$ then $H^1(K_v, E)(\mathfrak{p})$ is finite of order 2.*
(2) *The module $H^1(K_\mathfrak{p}, E)(\mathfrak{p})$ is finite of order equal to $|1 - \varphi(\mathfrak{p})/2|_\mathfrak{p}^{-1}$, where $|\cdot|_\mathfrak{p}$ denotes the $\mathfrak{p}$-adic absolute value on $K_\mathfrak{p}$, normalized such that $|\varpi|_\mathfrak{p}^{-1} = 2$ for a uniformizer ϖ of $K_\mathfrak{p}$.*

Proof. The first result follows from Tate local duality and the fact that E has purely additive reduction at all bad primes $v \in \mathcal{B}$, with the exponent of the component group of the Néron model of E at each such v equal to 2 (see [30, Proposition 4.5]). The second statement follows by the same argument as in [10, Lemma 1]. □

Let $\mathcal{O}_\mathfrak{p} = \mathcal{O}_{K_\mathfrak{p}}$, and let $\mathfrak{M}$ be a discrete $\mathcal{O}_\mathfrak{p}$-module. We denote by $\mathfrak{M}^\wedge$ the Pontryagin dual of $\mathfrak{M}$ with coefficients in $\mathcal{O}_\mathfrak{p}$, defined by

$$\mathfrak{M}^\wedge := \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(\mathfrak{M}, K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}).$$

We define the ($\mathcal{O}_\mathfrak{p}$-)corank of $\mathfrak{M}$ as the $\mathcal{O}_\mathfrak{p}$-rank of $\mathfrak{M}^\wedge$.

Corollary 3.2. *The divisible parts of the Selmer groups $\mathrm{Sel}_E(K)_\mathfrak{p}$ and $\mathrm{Sel}_E^\mathcal{W}(K)_\mathfrak{p}$ are isomorphic. Assuming that $Ш(E/F)(\mathfrak{p})$ is finite, the coranks of these modules are both equal to the $\mathcal{O}_\mathfrak{p}$-rank of $E(K) \otimes_{\mathcal{O}_K} \mathcal{O}_\mathfrak{p}$.*

For a discrete $\mathcal{O}_\mathfrak{p}$-module $\mathfrak{M}$, recall that we define $\mathfrak{M}_{/\mathrm{div}}$ to be the quotient of $\mathfrak{M}$ by its divisible part. If $\mathfrak{M}^\wedge$ is a finitely generated $\mathcal{O}_\mathfrak{p}$-module, then $\mathfrak{M}_{/\mathrm{div}}$ is finite.

Since E has good ordinary reduction at $\mathfrak{p}$, from [10, Lemma 1], we have the isomorphism:

$$E(K_\mathfrak{p}) \otimes \mathcal{O}_{\mathfrak{p}^*} \simeq \widetilde{E}(\kappa_\mathfrak{p})(2),$$

where $\kappa_\mathfrak{p}$ is the residue field of $K_\mathfrak{p}$, $\widetilde{E}$ is the reduction of E modulo $\mathfrak{p}$ and the isomorphism is given by the reduction modulo $\mathfrak{p}$. Let $\mathcal{C}$ denote the quotient of the image of $E(K)_{/\mathrm{tor}}$ in $\widetilde{E}(\kappa_\mathfrak{p})(2)$ under the reduction map, modulo the image of $E(K)(\mathfrak{p}^*)$.

Proposition 3.3. *Assume that E has good reduction at all primes of K lying above 2. If $Ш(E/K)(p)$ is finite, then we have*

$$\left| \left(\mathrm{Sel}_E^\mathcal{W}(K)_\mathfrak{p} \right)_{/\mathrm{div}} \right| = |Ш(E/K)(\mathfrak{p})| \cdot |(1 - \varphi(\mathfrak{p})/2) \cdot |\mathcal{C}||_\mathfrak{p}^{-1} \cdot 2^{(|\mathcal{B}|-1)}. \tag{3.2}$$

Proof. Write π for a generator of $\mathfrak{p}$, thus $\overline{\pi}$ is a generator of $\mathfrak{p}^*$. For each integer $n \geq 1$, we have the short exact sequence

$$0 \to \mathrm{Sel}_E(K)[\pi^n] \to \mathrm{Sel}_E^{\mathcal{W}}(K)[\pi^n] \to \prod_{v \in \mathcal{W}} H^1(K_v, E)_{\pi^n}, \tag{3.3}$$

and we write u_n for the right-hand homomorphism in this sequence. Here we write $\mathrm{Sel}_E(K)[\pi^n]$ (resp. $\mathrm{Sel}_E^{\mathcal{W}}(K)[\pi^n]$) for the Selmer group defined using the Galois module E_{π^n}. On the other hand, by the definition of the Selmer group $\mathrm{Sel}_E(K)[\overline{\pi}^n]$, we have the following natural homomorphism

$$s_n : \mathrm{Sel}_E(K)[\overline{\pi}^n] \to \prod_{v \in \mathcal{W}} E(K_v)/\overline{\pi}^n E(K_v). \tag{3.4}$$

Note that the right hand groups in (3.3) and (3.4) are dual to each other by Tate local duality. By the modified Poitou–Tate sequence (see, for example, the Appendix of [39] or [1]), we conclude that, for all $n \geq 1$, $\mathrm{Coker}(u_n)$ is equal to the Pontryagin dual of $\mathrm{Im}(s_n)$. Hence, noting that $\mathfrak{r}$ is the inductive limit of the maps u_n as $n \to \infty$, it follows that $\mathrm{Coker}(\mathfrak{r})$ is dual to the image of the map $\mathfrak{s}_\infty = \varprojlim_n s_n$, where

$$\mathfrak{s}_\infty : \varprojlim_n \mathrm{Sel}_E(K)[\overline{\pi}^n] \to \prod_{v \in \mathcal{W}} E(K_v) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}. \tag{3.5}$$

Since $Ш(E/K)(\mathfrak{p}^*)$ is finite, it follows that $\varprojlim_n \mathrm{Sel}_E(K)[\overline{\pi}^n] = E(K) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathfrak{p}^*}$. Applying the proof of Lemma 3.1, we obtain the isomorphism

$$\prod_{v \in \mathcal{W}} E(K_v) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*} \simeq \prod_{v \in \mathcal{W}} E(K_v)(\mathfrak{p}^*).$$

Noting that $\mathfrak{p}^*$ is not contained in $\mathcal{W}$, E has additive reduction at $v \in \mathcal{B}$, we can show that the non-torsion points in $E(K)$ maps to zero in $\prod_{v \in \mathcal{B}} E(K_v) \otimes_{\mathcal{O}} \mathcal{O}_{\mathfrak{p}^*}$. By [10, Lemma 1], the only contribution of the non-torsion points in $E(K)$ is given by the image of $E(K)_{/\mathrm{tor}}$ in $\widetilde{E}(\kappa_{\mathfrak{p}})(2)$ under the reduction map. Since $\mathfrak{s}_\infty$ is injective on torsion part of $E(K) \otimes \mathcal{O}_{\mathfrak{p}^*}$, we conclude that the image of $\mathfrak{s}_\infty$ is equal to the group generated by $E(K)(\mathfrak{p}^*)$ and $\mathcal{C}$. From the Lemma 3.4 below, we obtain that $E(K)(\mathfrak{p}^*) = E(K)_{\mathfrak{p}^*}$. Now the proposition follows by a simple diagram chasing in the exact sequence (3.1). □

We recall that

$$F = K(E_{\mathfrak{p}^2}) \quad \text{and} \quad \Delta = \mathrm{Gal}(F/K).$$

Lemma 3.4. *The elliptic curve E has good reduction everywhere over F.*

Proof. A detailed proof can be found in [9, Lemma 2.1]. □

We write

$$\alpha_F : H^1(K, E(\mathfrak{p})) \to H^1(F, E(\mathfrak{p}))^\Delta$$

for the restriction map.

Proposition 3.5. *The map α_F induces an exact sequence*

$$0 \to H^1(\Delta, E_{\mathfrak{p}^2}) \to \mathrm{Sel}_E^{\mathcal{W}}(K)_{\mathfrak{p}} \xrightarrow{\alpha} \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^\Delta \to 0. \tag{3.6}$$

In particular, both groups $\mathrm{Sel}_E^{\mathcal{W}}(K)_{\mathfrak{p}}$ and $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^\Delta$ have the same corank.

Proof. Consider the following exact commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_E^{\mathcal{W}}(K)_{\mathfrak{p}} & \longrightarrow & H^1(K, E(\mathfrak{p})) & \longrightarrow & \prod_{v \notin \mathcal{W}} H^1(K_v, E)_{\mathfrak{p}^\infty} \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \downarrow{\scriptstyle j} \\ 0 & \longrightarrow & \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^\Delta & \longrightarrow & H^1(F, E(\mathfrak{p}))^\Delta & \longrightarrow & (\prod_{w \notin \mathcal{P}} H^1(F_w, E)_{\mathfrak{p}^\infty})^\Delta. \end{array} \tag{3.7}$$

For $v \notin \mathcal{W}$, classical theorems of unramified cohomology (see [36, Proposition 4.3]) give us

$$H^1(\mathrm{Gal}(F_w/K_v), E(F_w)) = 0.$$

Thus, the vertical map j on the right hand side of (3.7) is injective. For each prime $v \in \mathcal{B}$, from the Tate local duality, the fact that E has additive reduction at each v and v is totally ramified in F, we can show that the restriction map

$$H^1(K_v, E)_{\mathfrak{p}^\infty} \to H^1(F_w, E)_{\mathfrak{p}^\infty}$$

is zero, and thus, the image of α is contained in $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}$. By applying the snake lemma to the commutative diagram (3.7), we obtain the desired exact sequence except for the surjectivity of α. The surjectivity follows by the same method as [23, Lemma 3.7]. Therefore the proposition follows. □

Proposition 3.6. *Assume that E has good reduction at all primes of K above 2. Let $F = K(E_{\mathfrak{p}^2})$. Assume that $Ш(E/K)(2)$ is finite, then the coranks of the three modules $\mathrm{Sel}_E(K)_{\mathfrak{p}}$, $\mathrm{Sel}_E^{\mathcal{W}}(K)_{\mathfrak{p}}$ and $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^{\Delta}$ are the same and are equal to $\mathrm{rank}_{\mathcal{O}_K} E(K)$, and we have*

$$\left|\left(\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^{\Delta}\right)_{/\mathrm{div}}\right| = |Ш(E/K)(\mathfrak{p})| \cdot 2^{(|\mathcal{B}|-2)} \cdot |(1-\varphi(\mathfrak{p})/2) \cdot |\mathcal{C}||_{\mathfrak{p}}^{-1}. \tag{3.8}$$

Proof. One simply combines Propositions 3.3 and 3.5, noting that, we have $E(K)(\mathfrak{p}^*) = \mathbb{Z}/2\mathbb{Z}$, and $H^1(\Delta, E(F)(\mathfrak{p})) = \mathbb{Z}/2\mathbb{Z}$. □

The above proposition demonstrates that $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^{\Delta}$ is closely related to the arithmetic information of E/K. Let δ be a generator of Δ. By considering the exact sequence

$$0 \to \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^{\Delta} \to \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}} \to (1-\delta)\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}} \to 0,$$

it follows that, in general, $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^{\Delta}$ is not equal to the entire Selmer group $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}$. However, as noted in [9], by applying the 2-adic Iwasawa theory to the Coates-Wiles $\mathbb{Z}_2$-extension over F, one can show that the error term $(1-\delta)\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}$ vanishes. This important result is recorded in the following lemma.

Lemma 3.7. *We have*

$$\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}^{\Delta} = \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}.$$

Proof. One can refer to [9, Corollary 2.12] for a detailed proof. □

Define $Ш^{\mathcal{P}}(E/F)(\mathfrak{p})$ as the kernel of the map

$$H^1(F,E)(\mathfrak{p}) \to \prod_{v \notin \mathcal{P}} H^1(F_v, E)(\mathfrak{p}).$$

Then, the Selmer group $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}$ fits into the middle of the exact sequence

$$0 \to E(F) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}} \to Ш^{\mathcal{P}}(E/F)(\mathfrak{p}) \to 0. \tag{3.9}$$

Let E^F be the twist of E by the quadratic extension F/K, let $L(E^F/K, s)$ be the L-series of E^F over K.

Theorem 3.8. *We have*

1. $\mathrm{ord}_{s=1} L(E^F/K, s) = 0$, *and* $\mathrm{rank}_{\mathbb{Z}} E^F(K) = 0$.
2. $Ш(E^F/K)$ *is finite, and the refined Birch-Swinnerton-Dyer formula for E^F holds. Moreover, $Ш(E^F/K)(2)$ is trivial.*

The non-vanishing of $L(E^F/K, 1)$ and the triviality of $Ш(E^F/K)(2)$ were established in [9], [13] or [23]. The full Birch-Swinnerton-Dyer formula was proven in [23] extending Rubin's results [45] (see also [4]).

From Theorem 3.8, Proposition 3.6, Lemma 3.7 and the exact sequence (3.9), we obtain the following corollary:

Corollary 3.9. *Keeping the same assumptions as Proposition 3.6, we have*

$$\left|Ш^{\mathcal{P}}(E/F)(\mathfrak{p})\right| = |Ш(E/K)(\mathfrak{p})| \cdot 2^{(|\mathcal{B}|-2)} \cdot |(1-\varphi(\mathfrak{p})/2) \cdot |\mathcal{C}||_{\mathfrak{p}}^{-1}.$$

Proposition 3.10. *The index of $Ш(E/F)(\mathfrak{p})$ in $Ш^{\mathcal{P}}(E/F)(\mathfrak{p})$ is finite. Moreover, we have*

$$[Ш^{\mathcal{P}}(E/F)(\mathfrak{p}) : Ш(E/F)(\mathfrak{p})] = \left||E(K)(\mathfrak{p}^*)|^{-1} \cdot (1-\varphi(\mathfrak{p})/2) \cdot |\mathcal{C}|\right|_{\mathfrak{p}}^{-1}.$$

Proof. The descent sequence

$$0 \to E(F) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to \mathrm{Sel}_E(F)_{\mathfrak{p}} \to Ш(E/F)(\mathfrak{p}) \to 0$$

and exact sequence (3.9) imply the following exact commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(F) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) & \longrightarrow & \mathrm{Sel}_E(F)_{\mathfrak{p}} & \longrightarrow & Ш(E/F)(\mathfrak{p}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{j}_1} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(F) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) & \longrightarrow & \mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}} & \longrightarrow & Ш_E^{\mathcal{P}}(F)(\mathfrak{p}) & \longrightarrow & 0. \end{array} \tag{3.10}$$

Since E has good reduction everywhere over F, the same proof as in Proposition 3.3 shows that the index of $\mathrm{Sel}_E(F)_{\mathfrak{p}}$ in $\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}}$ is finite. Moreover, we have

$$[\mathrm{Sel}_E^{\mathcal{P}}(F)_{\mathfrak{p}} : \mathrm{Sel}_E(F)_{\mathfrak{p}}] = \left| |E(K)(\mathfrak{p}^*)|^{-1} \cdot (1 - \varphi(\mathfrak{p})/2) \cdot |\mathcal{C}| \right|_{\mathfrak{p}}^{-1}. \tag{3.11}$$

The following facts are used to derive the above equality:

- Since E has good reduction at $\mathfrak{p}$, the formal group associated to E over $K_{\mathfrak{p}}$ is the Lubin-Tate formal group. Therefore $F = K(E_{\mathfrak{p}^2})$ is a totally ramified extension over K at $\mathfrak{p}$. So that the residue field of F at $\mathfrak{p}$ is equal to that of $K_{\mathfrak{p}}$.
- Let $\varphi_{E/F}$ denote the Hecke character of E/F. Then $\varphi_{E/F} = \varphi \circ N_{F/K}$.
- Since $\mathfrak{p}^*$ is unramified in F/K, $E(F)(\mathfrak{p}) = E_{\mathfrak{p}^2}$ and the Weil pairing, we obtain
$$E(F)(\mathfrak{p}^*) = E(K)(\mathfrak{p}^*) = \mathbb{Z}/2\mathbb{Z}.$$
- From Lemma 3.7, the non-torsion points of $E(F)$ comes exactly from the non-torsion points of $E(K)$, so $\mathcal{C}$ remains unchanged for E/F.

In the diagram (3.10), since the map j_1 is the identity map and the middle vertical map is injective, the index of $Ш(E/F)(\mathfrak{p})$ in $Ш^{\mathcal{P}}(E/F)(\mathfrak{p})$ is finite. Thus, from (3.11), the equation in the proposition follows. □

Corollary 3.11. *Under the same assumptions as Proposition 3.6, we have*

$$|Ш(E/F)(\mathfrak{p})| = |Ш(E/K)(\mathfrak{p})| \cdot 2^{(|\mathcal{B}|-1)}. \tag{3.12}$$

The proof of this corollary follows directly from Proposition 3.10 and Corollary 3.9.

4. Iwasawa theory for E over cyclotomic $\mathbb{Z}_p$-extensions

Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}_K$. Assume p is a prime which splits in K. We assume either E has potentially good ordinary at p when $p \neq 2$ or is the same as Section 3 when $p = 2$. Let F be a finite cyclic extension over K such that E has good ordinary reduction over F at all primes above p. One can refer to [43] for the existence of such F.

For any number field $\mathfrak{F}$, we let $\mathfrak{F}_{\mathrm{cyc}}$ denote the cyclotomic $\mathbb{Z}_p$-extension over $\mathfrak{F}$. Let $\mathfrak{F}_n$ be the unique subfield in $\mathfrak{F}_{\mathrm{cyc}}$ such that $\mathrm{Gal}(\mathfrak{F}_n/\mathfrak{F})$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. Assume $\mathfrak{F}$ contains K, we define

$$\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p = \varinjlim_n \mathrm{Sel}_E(\mathfrak{F}_n)_p$$

where the inductive limit is taken with respect to the restriction maps.

Let $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$ and let Λ_Γ be the Iwasawa algebra defined as $\Lambda_\Gamma = \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n]$, where Γ_n is the unique subgroup in Γ with index p^n. For a discrete Λ_Γ-module $\mathfrak{M}$, we set $\mathfrak{M}^\wedge$ to be the Pontryagin dual of $\mathfrak{M}$, i.e., $\mathfrak{M}^\wedge = \mathrm{Hom}_{\mathbb{Z}_p}(\mathfrak{M}, \mathbb{Q}_p/\mathbb{Z}_p)$. The module $\mathfrak{M}$ is cofinitely generated over Λ_Γ (resp. $\mathbb{Z}_p$) if $\mathfrak{M}^\wedge$ is a finitely generated Λ_Γ (resp. $\mathbb{Z}_p$)-module. We say that $\mathfrak{M}$ is a cotorsion Λ_Γ-module if $\mathfrak{M}^\wedge$ is a torsion Λ_Γ-module. It is well-known that $\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p$ is a cofinitely generated Λ_Γ-module. Throughout this section we assume that $\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p$ is a cotorsion Λ_Γ-module.

Let $\Delta = \mathrm{Gal}(F/K)$. We know $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$ is also a Δ-module. For each character η of Δ, we define $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p^\eta$ to be the η-part of $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$. If η is the trivial character, $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p^\eta$ is equal to $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p^\Delta$, which is the submodule consisting of elements in $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$ fixed under the action of Δ. For each η the module $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p^\eta$ is a finitely generated cotorsion Λ_Γ-module. From the structure theorem for finitely generated modules over Λ_Γ, we define c_F^η to be a generator of the characteristic ideal of $\left(\mathrm{Sel}_E(F_{\mathrm{cyc}})_p^\eta\right)^\wedge$. We denote by c_F a generator of the characteristic ideal of $(\mathrm{Sel}_E(F_{\mathrm{cyc}})_p)^\wedge$. Both c_F^η and c_F are well-defined up to units in the Iwasawa algebra Λ_Γ. We make the following convention: for a discrete Λ_Γ-module $\mathfrak{M}$, the characteristic ideal of $\mathfrak{M}$ means the characteristic ideal of $\mathfrak{M}^\wedge$; for a $\mathcal{O}_{\mathfrak{p}}$-(resp. $\mathbb{Z}_p$-) module $\mathfrak{M}$, we write the same notation $\mathfrak{M}^\wedge$ to denote the $\mathcal{O}_{\mathfrak{p}}$-(resp. $\mathbb{Z}_p$-)Pontryagin dual of $\mathfrak{M}$.

Proposition 4.1. *Assume that*

- *if $p \neq 2$, the order of Δ is prime to p;*
- *if $p = 2$, let $F = K(E_{\mathfrak{p}^2})$.*

Then we have $c_K = c_F^1$ and

$$c_F = c_K \times \prod_{\eta \neq 1} c_F^\eta$$

where the product runs over all nontrivial characters of Δ. In the above equations, the equalities mean up to units in Λ_Γ.

We omit the proof for the case $p \neq 2$, since it follows directly from the fact that the action of Δ on $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$ is semi-simple. In the follows we assume that $p = 2$. The first equality follows from the below lemma.

Lemma 4.2. *The characteristic ideals of both $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p^\Delta$ and $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$ are equal.*

Proof. We consider the following exact commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_E(K_{\mathrm{cyc}})_p & \longrightarrow & H^1(K_{\mathrm{cyc}}, E(p)) & \longrightarrow & \prod_v H^1(K_{\mathrm{cyc},v}, E)(p) \\ & & \downarrow{\scriptstyle \mathrm{j}_1} & & \downarrow{\scriptstyle \mathrm{j}_2} & & \downarrow{\scriptstyle \mathrm{j}_3} \\ 0 & \longrightarrow & (\mathrm{Sel}_E(F_{\mathrm{cyc}})_p)^\Delta & \longrightarrow & H^1(F_{\mathrm{cyc}}, E(p))^\Delta & \longrightarrow & \left(\prod_w H^1(F_{\mathrm{cyc},w}, E)(p)\right)^\Delta. \end{array}$$

It is obvious that both kernel and cokernel of j_2 are finite. In fact, by a Theorem of Mazur ([36]), we know $E(F_{\mathrm{cyc}})(p)$ is finite. Write j_3 as a product $(j_v)_v$ where v runs over all primes of K_{cyc}. If v is a prime not lying above p or at which E has good reduction, from [36, Proposition 4.3] j_v is injective. As every non-archimedean prime is finitely decomposed in K_{cyc} and the kernel of each j_v at either a bad prime v or a prime v above p is finite, we know the kernel of j_3 is finite. Thus both the kernel and cokernel of j_1 are finite, the lemma then follows.

□

Recall that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$ and note the relation

$$\mathrm{Sel}_E(F_{\mathrm{cyc}})_p = \mathrm{Sel}_E(F_{\mathrm{cyc}})_\mathfrak{p} \oplus \mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}^*},$$

as $\mathrm{Gal}(F_{\mathrm{cyc}}/K)$-modules. Let $c_{F,\mathfrak{p}}^\eta$ (resp. $c_{F,\mathfrak{p}^*}^\eta$) denote a generator of the corresponding characteristic ideals of $\mathrm{Sel}_E(F_{\mathrm{cyc}})_\mathfrak{p}^\eta$ (resp. $\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}^*}^\eta$). We write $c_{F,\mathfrak{p}}$ (resp. $c_{F,\mathfrak{p}^*}$) in the similar meaning for $\mathrm{Sel}_E(F_{\mathrm{cyc}})_\mathfrak{p}$ (resp. $\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}^*}$). Then the proof of the second equation in Proposition 4.1 reduces to showing the below equality

$$c_{F,\mathfrak{p}} = \prod_\eta c_{F,\mathfrak{p}}^\eta. \tag{4.1}$$

To prove the above equation, we now introduce a $\mathbb{Z}_2^2$-extension over F. Let $\mathcal{F} = F_{\mathrm{cyc}}(E(\mathfrak{p}))$ and put Γ_- for $\mathrm{Gal}(\mathcal{F}/F_{\mathrm{cyc}})$. Let $\Gamma_\mathcal{F} = \mathrm{Gal}(\mathcal{F}/F)$ and $\Lambda_\mathcal{F}$ the Iwasawa algebra of $\Gamma_\mathcal{F}$. It is easy to see that $\Gamma_\mathcal{F}$ is isomorphic to $\Gamma_- \times \Gamma$ which is also isomorphic to $\mathbb{Z}_2^2$. We can define the Selmer group $\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}$ in a similar way as $\mathrm{Sel}_E(F_{\mathrm{cyc}})_\mathfrak{p}$. The group $\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}$ is a $\Lambda_\mathcal{F}$-module. Let $\mathfrak{K}$ be the unique $\mathbb{Z}_2^2$-extension over K. We identify Δ with $\mathrm{Gal}(\mathcal{F}/\mathfrak{K})$. Then $\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}$ is also a $\mathbb{Z}_p[\Delta]$-module. For each character η of Δ we let $\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}^\eta$ denote the η-part of $\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}$.

Lemma 4.3. *For each character η of Δ, we have*

$$\mathrm{Sel}_E(F_{\mathrm{cyc}})_\mathfrak{p}^\eta = \left(\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}^\eta\right)^{\Gamma_-}.$$

Proof. Let e_η be a $\mathcal{O}_\mathfrak{p}$-basis of the rank one $\mathcal{O}_\mathfrak{p}$-module corresponding to η. Then

$$\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}^\eta \simeq (\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p} \otimes e_\eta)^\Delta.$$

Since Γ_- lies in the kernel of η and the actions of Δ and Γ_- are commutative, we obtain

$$\left(\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}^\eta\right)^{\Gamma_-} \simeq \left(\mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}^{\Gamma_-}\right)^\eta.$$

Then we reduce to show that $\mathrm{Sel}_E(F_{\mathrm{cyc}})_\mathfrak{p} \simeq \mathrm{Sel}_E(\mathcal{F})_\mathfrak{p}^{\Gamma_-}$. This follows from a similar proof as in Lemma 4.2 by noting $H^1(\Gamma_-, E(\mathfrak{p})) = 0$ and that E has good reduction everywhere over F_{cyc}. □

We come back to the proof of Proposition 4.1.

Proof of Proposition 4.1. Let $M_{\mathcal{F}}$ be the maximal abelian pro-2 extension over $\mathcal{F}$ which is ramified only at the primes above $\mathfrak{p}$ and put $X(\mathcal{F}) = \mathrm{Gal}(M_{\mathcal{F}}/\mathcal{F})$. From [39] (or an extension of [10] to this two variable setting) we obtain the isomorphism

$$\mathrm{Sel}_E(\mathcal{F})_{\mathfrak{p}} \simeq \mathrm{Hom}(X(\mathcal{F}), E_{\mathfrak{p}^\infty}).$$

A similar proof as Lemma 4.3 implies an invariant of the above Selmer group is isomorphic to the Selmer group of E over the Coates-Wiles $\mathbb{Z}_2$-extension over F which is ramified only at primes above $\mathfrak{p}$. From the works on μ-invariants (see [8], [38] and [16]), this Selmer group is a cofinitely generated $\mathbb{Z}_2$-module. Thus $\mathrm{Sel}_E(\mathcal{F})_{\mathfrak{p}}$ is cotorsion over $\Lambda_{\mathcal{F}}$ and has characteristic ideal which is prime to 2. Write $C_{\mathcal{F}}$, resp. $C_{\mathcal{F}}^{\eta}$ for a generator of the characteristic ideals of the Pontryagin dual of $\mathrm{Sel}_E(\mathcal{F})_{\mathfrak{p}}$, resp. $\mathrm{Sel}_E(\mathcal{F})_{\mathfrak{p}}^{\eta}$. Here η is any character of Δ. Since the characteristic ideal is prime to 2 all these elements are the same after taking tensor product with $\mathbb{Q}_2$, therefore we obtain

$$C_{\mathcal{F}} = \prod_{\eta} C_{\mathcal{F}}^{\eta}.$$

Noting Lemma 4.3, we know that the equation (4.1) is the image of the above equation under the natural map $\Lambda_{\mathcal{F}} \to \Lambda_\Gamma$. Since we have shown $c_K = c_F^1$, the Proposition 4.1 now follows. □

To lighten the notation we let $E' = E^F$.

Lemma 4.4. *We have*

$$\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}}^{\eta} \simeq \mathrm{Sel}_{E'}(F_{\mathrm{cyc}})_{\mathfrak{p}}^{\Delta}.$$

Proof. Recall e_η in the proof of Lemma 4.3. From the definition on twist of elliptic curves we know

$$E(\mathfrak{p}) \otimes e_\eta \simeq E'(\mathfrak{p}).$$

(As G_K-modules.) Therefore we obtain

$$H^1(F_{\mathrm{cyc}}, E'(\mathfrak{p}))^{\Delta} \simeq (H^1(F_{\mathrm{cyc}}, E(\mathfrak{p})) \otimes e_\eta)^{\Delta} \simeq H^1(F_{\mathrm{cyc}}, E(\mathfrak{p}))^{\eta}.$$

This isomorphism also holds locally for all non-archimedean primes of F_{cyc}, thus the lemma follows by the definition of Selmer groups. □

Corollary 4.5. *Write $c_{F,E}$ for c_F. Let $c_{K,E'}$ (resp. $c_{K,E}$) be a generator of the characteristic ideal of $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_p$ (resp. $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$). Then $c_{F,E} = c_{K,E'} \cdot c_{K,E}$. (up to p-adic units.)*

This corollary follows from Proposition 4.1, Lemmas 4.2, 4.4 and the fact that the Pontryagin dual of $\mathrm{Sel}_{E'}(F_{\mathrm{cyc}})_p^{\Delta}$ and $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_p$ are quasi-isomorphic.

5. Algebraic analogue of a Birch-Swinnerton-Dyer formula of E′ over K.

We keep the notation and setting as in Section 3 throughout this section. As usual, we let χ_{cyc} denote the cyclotomic character over K. Because of Theorem 3.8, $\mathrm{Sel}_{E'}(K)_2$ is finite. From Mazur's control theorem (see [36] or [26]) and the structure theorem of finitely generated modules over Λ_Γ, $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_2$ is a finitely generated cotorsion Λ_Γ-module. Let $c_{K,E'}$ be a generator of the characteristic ideal of $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_2$. We define the Iwasawa L-function of E' with respect to χ_{cyc} as follows:

$$f_{E'}(s) = \chi_{\mathrm{cyc}}^{1-s}(c_{K,E'}) \qquad (s \in \mathbb{Z}_2).$$

By Theorem 3.8, $f_{E'}(s)$ is nonzero at $s = 1$. In this section, we will compute the leading term, i.e., the constant term of $f_{E'}(s)$ at $s = 1$. Recall that $\varphi\eta$ is the Hecke character associated to E' over K.

Proposition 5.1. *Up to a 2-adic unit, we have*

$$f_{E'}(1) = \frac{1}{16} \cdot \left(1 - \frac{\overline{\varphi\eta(\mathfrak{p}^*)}}{2}\right)^2. \tag{5.1}$$

In the following part of this section, we use the Birch-Swinnerton-Dyer formula of E' and the Iwasawa main conjecture to prove the proposition. Consider the decomposition

$$\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_p = \mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}} \oplus \mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}^*}$$

The $\mathbb{Z}_2$-modules $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}}$ and $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}^*}$ are finitely generated cotorsion Λ_Γ-modules. Let $c_{K,E',\mathfrak{p}}$ (resp. $c_{K,E',\mathfrak{p}^*}$) be a generator of the characteristic ideal of $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}}$ (resp. $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}^*}$). We define

$$f_{E',\mathfrak{p}}(s) = \chi_{\mathrm{cyc}}^{1-s}(c_{K,E',\mathfrak{p}}) \quad \text{and} \quad f_{E',\mathfrak{p}^*}(s) = \chi_{\mathrm{cyc}}^{1-s}(c_{K,E',\mathfrak{p}^*}) \qquad (s \in \mathbb{Z}_2).$$

Then $f_{E'}(s) = f_{E',\mathfrak{p}}(s) \cdot f_{E',\mathfrak{p}^*}(s)$. (Up to a unit in the Iwasawa algebra.)

Proof of Proposition 5.1. Restricting the two variable Iwasawa main conjecture (see [32]) and Yager's theorem (see [52], [35]) to K_{cyc}, $f_{E',\mathfrak{p}}(s)$ (resp. $f_{E',\mathfrak{p}^*}(s)$) is equal to the Katz measure in [17, Theorem II 4.14] evaluating at $\varphi_{E'}\chi_{\mathrm{cyc}}^{1-s}$ (resp. $\overline{\varphi}_{E'}\chi_{\mathrm{cyc}}^{1-s}$). Write $\Omega_{E'}$ for the period associated to E'. Denote by $\varphi_{E'}=\varphi\eta$ the Hecke character associated to E' over K. By the interpolation formula in [17, Theorem II 4.14] we obtain (up to 2-adic units)

$$f_{E',\mathfrak{p}}(1)=\left(1-\frac{\overline{\varphi_{E'}(\mathfrak{p}^*)}}{2}\right)\cdot\frac{L(\overline{\varphi}_{E'},1)}{\Omega_{E'}}.$$

To handle the Selmer group $\mathrm{Sel}_{E'}(K_{\mathrm{cyc}})_{\mathfrak{p}^*}$, we apply the complex conjugation on E' to get an elliptic curve $\mathcal{E}$. Write K'_{cyc} the conjugated field of K_{cyc} under complex conjugation. Here we should note that since E' is defined over K, the field K'_{cyc} is not equal to K_{cyc}. Then we reduce to calculating the Iwasawa function $f_{\mathcal{E},\mathfrak{p}}$ associated to $\mathrm{Sel}_{\mathcal{E}}(K'_{\mathrm{cyc}})_{\mathfrak{p}}$. Note that $\mathcal{E}$ has only bad reduction at $\mathfrak{p}^*$, and that the period $\Omega_{\mathcal{E}}=\overline{\Omega}_{E'}$. Applying the same argument as above, we obtain (up to 2-adic units)

$$f_{E',\mathfrak{p}^*}(1)=\left(1-\frac{\overline{\varphi_{E'}(\mathfrak{p}^*)}}{2}\right)\cdot\frac{L(\varphi_{E'},1)}{\overline{\Omega}_{E'}}.$$

Notice that the 2-part of refined Birch Swinnerton-Dyer formula of E' is given as

$$\frac{L(E'/K,1)}{\Omega_{E'}\cdot\overline{\Omega}_{E'}}=\frac{|Ш(E'/K)(2)|\cdot t_{\mathfrak{p}}(E'/K)}{|E'(K)(2)|^2}$$

(up to 2-adic units.). From [9] or [23], we know the above equation is valid. Here $t_{\mathfrak{p}}(E'/K)$ denotes the Tamagawa number of E' at $\mathfrak{p}$. Thus the proposition follows from the facts that $Ш(E'/K)(2)=0$, $t_{\mathfrak{p}}(E'/K)=4$ (see [23]), $|E'(K)(2)|=8$ and $\varphi_{E'}=\varphi\eta$. □

6. Algebraic p-adic height formula for E over K

Let E be an elliptic curve over K with complex multiplication by $\mathcal{O}_K$. Let p be a potentially good ordinary prime for E. We assume that E has good ordinary reduction at p when $p=2$, i.e., E has good ordinary reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$. For any finite field extension $\mathfrak{F}/K$, we define $\mathfrak{F}_{\mathrm{cyc}}$ to be the cyclotomic $\mathbb{Z}_p$-extension over $\mathfrak{F}$. Put $\Gamma_{\mathfrak{F}}=\mathrm{Gal}(\mathfrak{F}_{\mathrm{cyc}}/\mathfrak{F})$ and denote $\Lambda(\Gamma_{\mathfrak{F}})$ by the Iwasawa algebra of $\Gamma_{\mathfrak{F}}$. When $\mathfrak{F}=K$, we simply write Γ (resp. Λ_Γ) for $\Gamma_{\mathfrak{F}}$ (resp. $\Lambda(\Gamma_{\mathfrak{F}})$). Let $\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p$ be the p-power Selmer group of E over $\mathfrak{F}_{\mathrm{cyc}}$. It is clear that $\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p$ is a cofinitely generated $\Lambda(\Gamma_{\mathfrak{F}})$-module. We assume further that $\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p$ is cotorsion over $\Lambda(\Gamma_{\mathfrak{F}})$. Write $c_{\mathfrak{F}}$ for a generator of the characteristic ideal of $\mathrm{Sel}_E(\mathfrak{F}_{\mathrm{cyc}})_p$. Let $\chi_{\mathrm{cyc},\mathfrak{F}}$ be the cyclotomic character of $\mathrm{Gal}(\mathfrak{F}_{\mathrm{cyc}}/\mathfrak{F})$. We define

$$f_{E/\mathfrak{F}}(s)=\chi_{\mathrm{cyc},\mathfrak{F}}^{1-s}(c_{\mathfrak{F}})\qquad(s\in\mathbb{Z}_p)$$

to be the Iwasawa L-function of E over $\mathfrak{F}$ with respect to $\chi_{\mathrm{cyc},\mathfrak{F}}$. When $\mathfrak{F}=K$, we omit $\mathfrak{F}$ in the subscripts of $f_{E/\mathfrak{F}}$ and $\chi_{\mathrm{cyc},\mathfrak{F}}$. Recall that φ is the Hecke character over K associated to E. The aim of this section is to prove the following

Theorem 6.1. *Assume that $E(K)\otimes_{\mathcal{O}_K}K$ has dimension one over K and $Ш(E/K)(p)$ is finite. Then $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$ is a cotorsion Λ_Γ-module and the vanishing order of $f_E(s)$ at $s=1$ is equal to 2. Moreover, denote by $f_E^*(1)$ the coefficient of the leading term of $f_E(s)$ at $s=1$, we have*

$$f_E^*(1)=\mathscr{C}_p\cdot|Ш(E/K)(p)|\cdot R_p(E/K)\cdot(1-\varphi(\mathfrak{p}))^4(1-\varphi(\mathfrak{p}^*))^4. \tag{6.1}$$

(The equality holds up to p-adic units.) Here $\mathscr{C}_p$ is equal to $4^{|\mathcal{B}|}$ or 1 according as $p=2$ or p is odd. Recall that $\mathcal{B}$ denotes the set of bad primes for E over K.

We postpone the proof of the odd case. From now on, we assume $p=2$, thus E is a twist of $A=X_0(49)$ by the extension $\mathbb{Q}(\sqrt{D})$ over $\mathbb{Q}$. As always we assume the integer $D\equiv 1 \bmod 4$. Recall that $2\mathcal{O}_K=\mathfrak{p}\cdot\mathfrak{p}^*$ and $F=K(E_{\mathfrak{p}^2})$. From Lemma 3.4, the elliptic curve E has good reduction everywhere over F. By the assumption that $E(K)$ has $\mathcal{O}_K$-rank one and $Ш(E/K)(2)$ is finite, from Theorem 3.8 we know $\dim_K E(F)\otimes_{\mathcal{O}_K}K=1$ and $Ш(E/F)(2)$ is finite.

Proposition 6.2. *Keep the above notation. The Selmer group* $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$ *is a cotorsion* $\Lambda(\Gamma_F)$*-module and the vanishing order of* $f_{E/F}(s)$ *at* $s=1$ *is two. Moreover, denote by* $f^*_{E/F}(1)$ *the coefficient of the leading term of* $f_{E/F}(s)$ *at* $s=1$*, we have*

$$f^*_{E/F}(1) = |Ш(E/F)(2)| \cdot R_p(E/F) \cdot \prod_{v|p} |\widetilde{E}(\kappa_v)|^2. \tag{6.2}$$

Here the equality is up to 2*-adic units. The curve* $\widetilde{E}$ *is the reduction curve of* E *at* v *and* κ_v *is the residue field of* F_v*.*

Proof. Since E has complex multiplication, the p-adic height of the $\mathcal{O}_K$-generator of $E(F)$ is nonzero (see [2]). Therefore, by the same proof as [47, Theorems (1.1), (2.2′)], $\mathrm{Sel}_E(F_{\mathrm{cyc}})_p$ is a cotorsion $\Lambda(\Gamma_F)$-module and the vanishing order of $f_{E/F}(s)$ at $s=1$ is equal to two. To show the formula (6.2), Schneider's proof works only when F is totally imaginary, and we can show $(\mathrm{Sel}_E(F_{\mathrm{cyc}})_p)^\wedge$ has no nonzero finite sub Λ_Γ-modules (see [47, Pages 338 and 340]). We will prove this last statement in the appendix using methods due to Greenberg. Here, we should also note that the proof of Schneider on comparison between the algebraic and analytic p-adic heights (see [47, §6 and 7, especially Proposition (6.2)]) still works for $p=2$. From these reasons, the proposition follows from the equality in [47, Theorem 2.2′] using the fact that E has good reduction everywhere over F. □

Since $Ш(E/F)(2)$ is finite, Cassels's pairing on $Ш(E/F)(2)$ implies that $|Ш(E/F)(\mathfrak{p}^*)| = |Ш(E/F)(\mathfrak{p})|$. From Corollary 3.11 and

$$Ш(E/F)(2) = Ш(E/F)(\mathfrak{p}) \oplus Ш(E/F)(\mathfrak{p}^*),$$

we have

$$|Ш(E/F)(2)| = |Ш(E/K)(2)| \cdot 4^{|\mathcal{B}|-1}. \tag{6.3}$$

Recall that the torsion free part of $E(F)$ (resp. $E(K)$) is an $\mathcal{O}_K$-module of rank one.

Lemma 6.3. *Any* $\mathcal{O}_K$*-generator of* $E(F)$ *comes from an* $\mathcal{O}_K$*-generator of* $E(K)$*.*

Proof. Denote by δ a generator of $\Delta = \mathrm{Gal}(F/K)$. Noting the exact sequence

$$0 \to E(F) \otimes_{\mathcal{O}_K} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to \mathrm{Sel}^{\mathcal{P}}_E(F)_{\mathfrak{p}} \to Ш^{\mathcal{P}}(E/F)(\mathfrak{p}) \to 0$$

and Lemma 3.7, we obtain

$$(E(F) \otimes_{\mathcal{O}_K} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}))^{\Delta} = E(F) \otimes_{\mathcal{O}_K} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}).$$

Let P_1 be an $\mathcal{O}_K$ generator of $E(F)$ and put π to be a generator of $\mathfrak{p}$. Since $\delta(P_1 \otimes (1/\pi^m)) = P_1 \otimes (1/\pi^m)$ we obtain

$$\delta(P_1) - P_1 \in \pi^m E(F)$$

for all $m \in \mathbb{Z}_+$. As any nonzero point in $E(F)$ is finitely divisible, we must have $\delta(P_1) = P_1$. Therefore, the lemma follows. □

Lemma 6.4. *Recall that* E *is defined over* $\mathbb{Q}$ *and we view* E *defined over* K*. We can choose a point* $P_0 \in E(\mathbb{Q})$ *such that* $[E(K)_{/\mathrm{tor}} : \mathcal{O}_K P_0]$ *is prime to* 2*. In particular, up to* 2*-adic units, an* $\mathcal{O}_K$*-generator of* $E(K)$ *can be taken from a point in* $E(\mathbb{Q})$*.*

Proof. Let $E(K) = \mathcal{O}_K \cdot P_2$ and put σ to be a generator of $\mathrm{Gal}(K/\mathbb{Q})$. Since σP_2 is still a generator of $E(K)$ we obtain

$$\sigma P_2 = sP_2 + T \qquad (s \in \{\pm 1\}, T \in E(K)_{\mathrm{tor}}).$$

We can assume that $s=1$ by changing P_2 to $\sqrt{-7}P_2$. Here we recall $K = \mathbb{Q}(\sqrt{-7})$ and that $\sqrt{-7}P_2$ is given by the action of complex multiplication. Thus $\sigma P_2 = P_2 + T$ with $T \in E(K)_2$. Note that $E(K)_2 = E_{\mathfrak{p}^*} \times E_{\mathfrak{p}}$ we denote by $t_{\mathfrak{p}}$, resp. $t_{\mathfrak{p}^*}$ the generator of $E_{\mathfrak{p}}$, resp. $E_{\mathfrak{p}^*}$. We claim that either $T=0$ or $T = t_{\mathfrak{p}} + t_{\mathfrak{p}^*}$. Admitting the claim, if $\sigma P_2 = P_2 + t_{\mathfrak{p}} + t_{\mathfrak{p}^*}$, changing P_2 to $P_2 + t_{\mathfrak{p}^*}$ we know that P_2 is invariant under σ. Thus the claim implies the lemma. Now we prove the claim. Otherwise, we may assume $\sigma P_2 = P_2 + t_{\mathfrak{p}}$. By applying σ to both sides of the equation we obtain $P_2 = \sigma(P_2) + t_{\mathfrak{p}^*} = P_2 + t_{\mathfrak{p}} + t_{\mathfrak{p}^*}$, thus $t_{\mathfrak{p}} + t_{\mathfrak{p}^*} = 0$ which is a contradiction. The case $\sigma P_2 = P_2 + t_{\mathfrak{p}^*}$ can be proven in a similar way, therefore the claim follows. □

Proof of Theorem 6.1 when $p = 2$. In the following proof, we write $\sim$ to denote the equality of the quantity is up to 2-adic units. From [10] (see [39]), we know that $|\widetilde{E}'(\kappa_{\mathfrak{p}^*})| \sim (1 - \overline{\varphi\eta(\mathfrak{p}^*)}/2)$. Note that $\mathfrak{p}$ is totally ramified in E/K, $\mathfrak{p}^*$ is unramified in F/K, we can easily show that

$$\frac{\prod_{w|p} |\widetilde{E}(\kappa_w)|}{|\widetilde{E}'(\kappa_{\mathfrak{p}})||\widetilde{E}'(\kappa_{\mathfrak{p}^*})|} = (1 - \varphi(\mathfrak{p}))^2(1 - \varphi(\mathfrak{p}^*))^2.$$

Here, the product in the left hand side runs over all primes of F lying above p. Now, from equations (6.2), (5.1), (6.3) and Corollary 4.5, we obtain

$$f_E^*(1) \sim \frac{|Ш(E/K)(2)| \cdot 4^{|\mathcal{B}|} \cdot \det(\cdot,\cdot)_{p,F}}{|E(K)_{\mathrm{tor}}|^2} \cdot (1 - \varphi(\mathfrak{p}))^4(1 - \varphi(\mathfrak{p}^*))^4, \tag{6.4}$$

where $\det(\cdot,\cdot)_{p,F}$ is the determinant associated to p-adic height pairing on $E(F)_{/\mathrm{tor}} \times E(F)_{/\mathrm{tor}}$, and we have used the fact that $R_p(E/F) = \frac{\det(\cdot,\cdot)_{p,F}}{|E(F)_{\mathrm{tor}}|^2}$. From Lemma 6.3, using a $\mathbb{Z}$-basis for $\mathcal{O}_K$ and applying the relation between p-adic height pairing and p-adic height, we obtain $\det(\cdot,\cdot)_{p,F} \sim ht_{p,K}(P)^2$. Here $ht_{p,K}(\cdot)$ denotes the p-adic height over K. Noting the compatibility of p-adic height under complex multiplication (see [39]), and the analogues between refined p-adic regulator and usual p-adic regulator (for the complex case, see [30]), from Lemma 6.4 we obtain $ht_{p,K}(P)^2 \sim \det(\cdot,\cdot)_{p,K}$. Thus the formula (6.4) becomes

$$f_E^*(1) \sim |Ш(E/K)(2)| \cdot 4^{|\mathcal{B}|} \cdot R_p(E/K) \cdot (1 - \varphi(\mathfrak{p}))^4(1 - \varphi(\mathfrak{p}^*))^4,$$

where we used the relation $R_p(E/K) = \frac{\det(\cdot,\cdot)_{p,K}}{|E(K)_{\mathrm{tor}}|^2}$. The case $p = 2$ of Theorem 6.1 now follows. □

In the final part of this section, we deal with the case of $p \neq 2$. Recall that E is an elliptic curve over K with complex multiplication by $\mathcal{O}_K$ and E has potentially good ordinary reduction at p. Write $p\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{p}^*$. Recall also that φ is the Hecke character over K associated to E. Let ϵ be a Galois character over K taking values in $\mathcal{O}_K^\times$ such that $\varphi' = \varphi\epsilon$ is unramified at both $\mathfrak{p}$ and $\mathfrak{p}^*$. Let F be the cyclic extension over K cut out by ϵ, thus $[F : K]$ divides $w_K := |\mathcal{O}_K^\times|$. Let E' be the twist of E by the field extension F/K. Then φ' is the Hecke character associated to E'. Since φ' is unramified at both $\mathfrak{p}$ and $\mathfrak{p}^*$, E' has good reduction at p. The curves E and E' are isomorphic over F, $E'(F)^\epsilon \simeq E(K)$, and $Ш(E'/F)(p)^\epsilon \simeq Ш(E/K)(p)$. Here, for a $\mathrm{Gal}(F/K)$-module $\mathfrak{M}$, we write $\mathfrak{M}^\epsilon$ for the ϵ-part of $\mathfrak{M}$.

Proof of Theorem 6.1 when p is odd. Put $\Delta = \mathrm{Gal(F/K)}$. Since $|\Delta|$ is prime to p, for any exact commutative diagram, taking Δ-invariant of each term still gives an exact commutative diagram. In particular, we have $Ш(E/F)(p)^\Delta = Ш(E/K)(p)$ and $\mathrm{Sel}_E(F)_p^\Delta = \mathrm{Sel}_E(K)_p$. Note also that since the Tamagawa numbers are prime to p, the Mazur module associated to $E(p)$ is equal to the corresponding Selmer group.

The case when E has good ordinary reduction at all primes above p was proven in [47]. Our case follows by a variant of the same proof. Since E has good ordinary reduction at all primes of F above p, we can adopt the same descent arguments as [47] for E/F. Noting that the descent diagram in [47, Page 332] for E over F is Δ-equivariant, after taking Δ-invariant part in every module in the diagram, we can get a descent diagram with exact rows and columns. We can also apply the similar method to the diagram [47, Page 335] to get the algebraic p-adic height pairing for E over K, which is equal to the analytic p-adic height by [47, Section B]. Using the same proof as [47, Theorem 2′], we obtain

$$f_E^*(1) \sim |Ш(E/K)(p)| \cdot R_p(E/K) \cdot \prod_{v|p} \left|H^1(F_{\mathrm{cyc}}/F, E(F_{\mathrm{cyc}} \otimes_K K_v))^\Delta\right|. \tag{6.5}$$

As in the proof for $p = 2$, we write $\sim$ to mean the equality is up to p-adic units. The below lemma will complete the proof of Theorem 6.1.

Lemma 6.5. *Let $v_0 = \mathfrak{p}$ or $\mathfrak{p}^*$. Assume that if $w_K = 4$ or 6 then E has bad reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$ or good reduction at both $\mathfrak{p}$ and $\mathfrak{p}^*$. Then*

$$\left|H^1(\mathrm{Gal}(F_{\mathrm{cyc}}/F), E(F_{\mathrm{cyc}} \otimes_K K_{v_0}))^\Delta\right| \sim (1 - \varphi(v_0))^2(1 - \varphi(v_0^*))^2.$$

Note that [46] handled the case where E has good reduction above p. We now assume that E has bad reduction either at $\mathfrak{p}$ or at $\mathfrak{p}^*$. The isomorphism between E and E' over F gives rise to an isomorphism

$$H^1\left(F_{\mathrm{cyc}}/F, E(F_{\mathrm{cyc}} \otimes_K K_{v_0})\right)^\Delta \xrightarrow{\sim} H^1\left(F_{\mathrm{cyc}}/F, E'(F_{\mathrm{cyc}} \otimes_K K_{v_0})\right)^\epsilon.$$

We will use a fact in [46, Proposition (7.2)] saying that for any elliptic curve $\mathcal{A}$ over a local field f with good ordinary reduction and let $\widetilde{\mathcal{A}}$ denote its reduction over the residue field κ of f, we have

$$|H^1\left(f_{\mathrm{cyc}}/f, \mathcal{A}(f_{\mathrm{cyc}})\right) = |\widetilde{\mathcal{A}}(\kappa)(p)|^2.$$

Here f_{cyc} is the unique cyclotomic $\mathbb{Z}_p$-extension contained in $f(\mu_{p^\infty})$.

Let $w|v_0$ be a place of F above v_0 and κ_w/κ_{v_0} be the residue fields of F_w and K_{v_0} respectively, we have

$$|E'(\kappa_w)| \sim \left(1-\varphi'(v_0)^{[\kappa_w:\kappa_{v_0}]}\right)\left(1-\varphi'(v_0^*)^{[\kappa_w:\kappa_{v_0}]}\right).$$

If $w_K = 2$, then F/K is a quadratic extension. If E had bad reduction at v_0, then F/K is ramified at v_0 and let w be the unique place of F above v_0, we have $\kappa_w = \kappa_{v_0}$ and thus

$$\left|H^1\left(F_{\mathrm{cyc}}/F, E'(F_{\mathrm{cyc}} \otimes_K K_{v_0})^\epsilon\right|\right| = \frac{|H^1\left(F_{\mathrm{cyc},w}/F_w, E'(F_{\mathrm{cyc},w})\right)|}{|H^1\left(K_{\mathrm{cyc},v_0}/K_{v_0}, E'(K_{\mathrm{cyc},v_0})\right)|} = \frac{|\widetilde{E'}(\kappa_w)|^2}{|\widetilde{E'}(\kappa_{v_0})|^2} = 1.$$

If E has good reduction at v_0, then F/K is unramified at v_0. If v_0 is split over F, then $F\otimes_K K_{v_0} \cong K_{v_0}^2$ and $\epsilon_{v_0} = 1$. It is easy to see that

$$\left|H^1\left(F_{\mathrm{cyc}}/F, E'(F_{\mathrm{cyc}} \otimes_K K_{v_0})^\epsilon\right|\right| \sim (1-\varphi(v_0))^2(1-\varphi(v_0^*))^2.$$

If v_0 is inert in F, let w be the unique prime of F above v_0. Note that $\varphi'_{v_0} = \varphi_{v_0}\epsilon_{v_0}$ and $\epsilon(v_0) = -1$. Then we have

$$\begin{aligned}\left|H^1\left(F_{\mathrm{cyc}}/F, E'(F_{\mathrm{cyc}} \otimes_K K_{v_0})^\epsilon\right|\right| &= \frac{|H^1\left(F_{\mathrm{cyc},w}/F_w, E'(F_{\mathrm{cyc},w})\right)|}{|H^1\left(K_{\mathrm{cyc},v_0}/K_{v_0}, E'(K_{\mathrm{cyc},v_0})\right)|} = \frac{|\widetilde{E'}(\kappa_w)|^2}{|\widetilde{E'}(\kappa_{v_0})|^2} \\ &\sim \left(\frac{(1-(\varphi\epsilon)(v_0)^2)(1-\varphi\epsilon(v_0^*)^2)}{(1-(\varphi\epsilon)(v_0))(1-\varphi\epsilon(v_0^*))}\right)^2 = (1-\varphi(v_0))^2(1-\varphi(v_0^*))^2.\end{aligned}$$

If $w_K = 4$ or 6, by our assumption, v_0 must be ramified over F and ϵ is non-trivial on the inertia subgroup. The proof is similar to the previous ramified case. We omit the details. □

7. Iwasawa main conjecture and p-adic Birch-Swinnerton-dyer conjecture for E

Let K be an imaginary quadratic field. Denote by p a prime which splits in K, i.e., $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. We make the assumption that $\mathfrak{p}$ is induced by the embedding ι_p. In particular, $K_{\mathfrak{p}} = \mathbb{Q}_p$ in $\mathbb{C}_p$ and let $\psi_{\mathfrak{p}} = \psi_p$ on $K_{\mathfrak{p}}$ under this identification. Let E be an elliptic curve defined over K with complex multiplication by $\mathcal{O}_K$. Let Ω_E be a $\mathfrak{p}$-minimal period of E over K. We assume that E has potentially good (resp. good) ordinary reduction at p for p odd (resp. $p = 2$). Write φ for the associated Hecke character of E and $\mathfrak{f}_E$ for the conductor of φ. Denote by $\varphi_{\mathfrak{p}}$ the $\mathfrak{p}$-component of φ.

For any two non-zero integral ideals $\mathfrak{a}, \mathfrak{b}$ in K, we denote by $K(\mathfrak{a})$ the ray class field over K modulo $\mathfrak{a}$ and put $K(\mathfrak{a}\mathfrak{b}^\infty) = \cup_{n\geq 1}K(\mathfrak{a}\mathfrak{b}^n)$.

Theorem 7.1 (Two variable p-adic L-function)**.** *Let $\mathfrak{g}$ be any prime-to-p non-zero integral ideal of K. Assume that $\mathfrak{f}_E^{(p)}|\mathfrak{g}$. There exists a unique measure $\mu_{\mathfrak{g}} = \mu_{\mathfrak{g},\mathfrak{p}}$ on the group $\mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)$ such that for any character ρ of $\mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)$ of type $(1,0)$, we have*

$$\rho(\mu_{\mathfrak{g}}) = \frac{\tau(\rho_{\mathfrak{p}}, \psi_{\mathfrak{p}})}{\tau(\varphi_{\mathfrak{p}}, \psi_{\mathfrak{p}})} \cdot \frac{1-\rho(\mathfrak{p})p^{-1}}{1-\overline{\rho(\mathfrak{p})}p^{-1}} \cdot \frac{L^{(\mathfrak{g}p)}(\overline{\rho}, 1)}{\Omega_E}.$$

Here, $L^{(\mathfrak{g}p)}(\overline{\rho}, s)$ is the imprimitive L-series of $\overline{\rho}$ with Euler factors at the places dividing $\mathfrak{g}p$ removed.

We remark that, for any continuous character $\rho : \mathrm{Gal}(K(\mathfrak{g}p^\infty)/K) \to \mathbb{C}_p^\times$, by linear extension, we obtain a continuous algebra homomorphism $\rho : \mathbb{D}[[\mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)]] \to \mathbb{C}_p$. Since we can view $\mu_{\mathfrak{g}}$ as an element in $\mathbb{D}[[\mathrm{Gal}(K(\mathfrak{g}p^\infty)/K)]]$, $\rho(\mu_{\mathfrak{g}})$ is defined to be the image of $\mu_{\mathfrak{g}}$ under the homomorphism ρ. For the definition of the type of ρ, one can refer to [17, Chap II §1].

Proof. The result follows from the lemma 7.3 below and the construction of Katz's two variable p-adic measure. One can refer to [17, Theorem4.14], [52] for details. □

Let F be a finite abelian extension over K with Galois group $\Delta = \mathrm{Gal}(F/K)$. Assume that $|\Delta|$ is prime to p. Set $\mathcal{G} = \mathrm{Gal}(F(E(p))/K)$. Then $\mathcal{G} = \mathcal{G}_{\mathrm{tor}} \times \Gamma_K$ with $\Gamma_K = \mathrm{Gal}(F(E(p))/F(E_q))$, where the integer $q = p$ or 4 according as p is odd or even. Let $\Lambda_{\mathcal{G}} = \mathbb{Z}_p[[\mathcal{G}]]$ be the Iwasawa algebra of $\mathcal{G}$. Let U_∞ (resp. C_∞) denote the $\Lambda_{\mathcal{G}}$-module of the principal local units at the primes above $\mathfrak{p}$ (resp. the closure of the elliptic units for $F(E(p))/K$ under the $\mathfrak{p}$-adic topology). One can refer to [45, §4] for a precise

definition for these modules. Since $p \nmid |\Delta|$ and the group $\mathrm{Gal}(F(E_4)/F)$ has exponent 2, every character χ of $\mathcal{G}_{\mathrm{tor}}$ takes values in $\mathbb{D}$. It is well-known (see [52], [45], [35]) that $(U_\infty/C_\infty)_\chi$ is a finitely generated torsion $\mathbb{D}[[\Gamma_K]]$-module. We define $\mathrm{char}_{\Gamma_K}(U_\infty/C_\infty)_\chi$ to be the characteristic ideal of $(U_\infty/C_\infty)_\chi$.

Theorem 7.2 (Yager)**.** *Assume that $F = K$ if $p = 2$. For any character χ of $\mathcal{G}_{\mathrm{tor}}$, let $\mathfrak{f} = \mathfrak{f}_\chi^{(p)}$. Assume that $\mathfrak{f}_E^{(p)}$ divides $\mathfrak{f}$. Define*

$$\mu_{\mathfrak{f}}^\chi := \chi(\mu_{\mathfrak{f}}) \in \mathbb{D}[[\Gamma_K]],$$

then

$$\mathrm{char}_{\Gamma_K}(U_\infty/C_\infty)_\chi \cdot \mathbb{D}[[\Gamma_K]] = \left(\mu_{\mathfrak{f}}^\chi\right).$$

Here the measure $\mu_{\mathfrak{f}}$ is defined as in Theorem 7.1.

Proof. For p is an odd prime, this is a theorem of Yager [52]. The case for $p = 2$ can be proven in a similar way using a two variable generalisation of de Shalit's observation (in [17, Chap I]) that the one variable structure theorem for principal local units can vary very well under unramified extensions. A detailed proof can be found in [35]. □

Lemma 7.3. *Let E/K be an elliptic curve associated with a Hecke character φ, assume that $p \neq 2$ splits in K and write $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. Let φ_0 be a Hecke character over K unramified at $\mathfrak{p}$. Let Ω_E and Ω_0 be $\mathfrak{p}$-minimal periods of E and φ_0, respectively. Then*

$$\mathrm{ord}_p\left(\frac{\Omega_E \cdot \tau(\varphi_{\mathfrak{p}}, \psi_p)}{\Omega_0}\right) = 0.$$

Proof. The method for the proof is via Stickelberger's theorem on prime ideal decomposition of Gauss sum. In fact, for $\mathfrak{p} \nmid w = w_K$, E has $\mathfrak{p}$-minimal Weierstrass equation of form

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6, \qquad a_2, a_4, a_6 \in K^\times \cap \mathcal{O}_{\mathfrak{p}}.$$

Note that for $w = 4, 6$, we can take form $y^2 = x^3 + a_4x$, $y^2 = x^3 + a_6$, respectively. Then there is an elliptic curve E'' over K which has good reduction at $\mathfrak{p}$. Let φ'' be its associated Hecke character. Then $\epsilon = \varphi\varphi''^{-1} : \mathbb{A}_K^\times/K^\times \to \mathcal{O}_K^\times$ (also viewed as a Galois character via class field theory) is of the form $\chi(\sigma) = \sigma(d^{1/w})/d^{1/w}$ for an element $d \in K^\times/K^{\times w}$. Then the twist E'' has $\mathfrak{p}$-good model

$$E'' : \begin{cases} y^2 = x^3 + da_2x^2 + d^2a_4x + d^3a_6, & \text{if } w = 2, \\ y^2 = x^3 + da_4x, & \text{if } w = 4, \\ y^2 = x^3 + da_6, & \text{if } w = 6. \end{cases}$$

It is easy to check that $\Omega_{E''} = d^{1/w} \cdot \Omega_E$. Let $\omega : \mathcal{O}_{\mathfrak{p}}^\times \longrightarrow \mu_w \subset K$ be the character characterized by $\omega(a) \equiv a \bmod \mathfrak{p}$ and let $\chi = \omega^{-(p-1)/w}$. Then $\epsilon_{\mathfrak{p}} = \chi^k$ for some $k \in \mathbb{Z}/w\mathbb{Z}$. Let $\kappa_{\mathfrak{p}} \cong \mathbb{F}_p$ be the residue field of $K_{\mathfrak{p}}$. By Stickelberger's theorem, the Gauss sum $g(\epsilon_{\mathfrak{p}}, \psi) := -\sum_{a \in \kappa_{\mathfrak{p}}^\times} \epsilon_{\mathfrak{p}}(a)\psi(a)$ has $\mathfrak{p}$-valuation $\{k/w\}$. Notice that $\tau(\varphi_{\mathfrak{p}}, \psi_p)$ and $g(\epsilon_{\mathfrak{p}}, \psi)$ are up to $\mathfrak{p}$-adic units. It remains to show that $k = \mathrm{ord}_{\mathfrak{p}}(d)$. Note that for any $u \in \mathcal{O}_{\mathfrak{p}}^\times$, $K_{\mathfrak{p}}(u^{1/w})$ is unramified over $K_{\mathfrak{p}}$. Thus it is equivalent to show that for any uniformizer π of $K_{\mathfrak{p}}$,

$$\sigma_u(\pi^{1/w})/\pi^{1/w} \equiv u^{-(p-1)/w} \bmod \mathfrak{p}, \qquad \forall u \in \mathcal{O}_{\mathfrak{p}}^\times.$$

But it is easy to see this by using local class field theory for formal group associated to $x^p - \pi x$.

For general Hecke character φ_0 over K unramified at $\mathfrak{p}$ (not necessarily K-valued) and Ω_0 its $\mathfrak{p}$-minimal period, it is easy to see that $\mathrm{ord}_p(\Omega_0/\Omega_{E''}) = 0$.

□

Let $\chi_{\mathrm{cyc},K} : \mathcal{G} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character defined by the following composition

$$\mathcal{G} \to \mathrm{Gal}(K_{\mathrm{cyc}}/K) \to \mathbb{Z}_p^\times.$$

Here the first map is the natural quotient map and the second map is given by the restriction of the cyclotomic character of $\mathrm{Gal}(K(\mu(p))/K)$ to $\mathrm{Gal}(K_{\mathrm{cyc}}/K)$. We define

$$\mathscr{L}_{\varphi_E}(s) := \varphi_E\chi_{\mathrm{cyc},K}^{1-s}(\mu_{\mathfrak{f}_E^{(\mathfrak{p})}}) \qquad (s \in \mathbb{Z}_p).$$

Recall that we have defined the Selmer group $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$, $\Gamma = \mathrm{Gal}(K_{\mathrm{cyc}}/K)$ and the Iwasawa algebra $\Lambda = \Lambda_\Gamma$.

Proposition 7.4. *The Selmer group $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$ is a finitely generated cotorsion Λ-module.*

Proof. For p odd this is a main result in [44]. For $p=2$, since Rubin's main conjecture at $p=2$ was proven in [32], by a similar argument in the below proposition which links the Selmer group over K_{cyc} to the Selmer group over $K(E(p))$, the proposition follows by the same argument as in [44] using Rohrlich's theorem on generic non-vanishing of the cyclotomic twists of L-values of E. □

Let $c_{E,K}$ denote a generator of the characteristic ideal of $(\mathrm{Sel}_E(K_{\mathrm{cyc}})_p)^\wedge$. As in the previous sections, we define $f_E(s)=\chi_{\mathrm{cyc}}^{1-s}(c_{E,K})$ for $s\in\mathbb{Z}_p$.

Proposition 7.5. *There exists a function $u(s)$ on $\mathbb{Z}_p$ taking values in $\mathbb{D}^\times$ such that*

$$f_E(s)=u(s)\mathscr{L}_\varphi(s)\mathscr{L}_{\overline{\varphi}}(s)\qquad s\in\mathbb{Z}_p.$$

Proof. This is the p-adic cyclotomic main conjecture for E over K. The idea is via the two variable Iwasawa main conjecture for E ([45], [32]) and Yager's theorem ([52], [17], [35]).

If $p\neq 2$, recall that ϵ is a Galois character over K taking values in $\mathcal{O}_K^\times$ such that $\varphi'=\varphi\epsilon$ is unramified at both $\mathfrak{p}$ and $\mathfrak{p}^*$. Then we have defined F to be the cyclic extension cut out by ϵ over K with degree $[F:K]$ prime to p. The curve E/F has good reduction at primes above p, and the p-power Selmer group of E/K is equal to the $\Delta=\mathrm{Gal}(E/K)$-invariant of the p-power Selmer group of E/F. If $p=2$, we write $F=K$. Write $F_0=F(E_q)$, here $q=p$ or 4 according as p is odd or $p=2$. Let $\chi:\mathrm{Gal}(F_0/K)\to\mathcal{O}_{\mathfrak{p}}^\times$ be the character giving the action of $\mathrm{Gal}(F_0/K)$ on E_q.

Let $F_\infty=F(E(p))$. Then $\mathrm{Gal}(F_\infty/F_0)$ is isomorphic to $\mathbb{Z}_p^2$. Let $M_{\infty,\mathfrak{p}}$ be the maximal abelian p-extension over F_∞ which is unramified outside the primes above $\mathfrak{p}$. Set $X_{\infty,\mathfrak{p}}=\mathrm{Gal}(M_{\infty,\mathfrak{p}}/F_\infty)$. A well-known theorem due to Coates and Perrin-Riou shows that $(X_{\infty,\mathfrak{p}})_\chi$ is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]]$-module. We write $\mathrm{Char}(X_{\infty,\mathfrak{p}})_\chi$ for the characteristic ideal of $(X_{\infty,\mathfrak{p}})_\chi$. Rubin's two variable main conjecture (see [45] for p odd and [32] combined with the vanishing of μ-invariant [38], [16], [8] for $p=2$), and Yager's theorem (see [52] [35]) imply that

$$\mathrm{Char}(X_{\infty,\mathfrak{p}})_\chi\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]]=\left(\mu^\chi_{f_E^{(p)},\mathfrak{p}}\right),\tag{7.1}$$

where for an integral ideal $\mathfrak{g}$ of K prime to p, the measure $\mu_{\mathfrak{g}}$ is given as in Theorem 7.1. Here, we write $\mu_{\mathfrak{g},\mathfrak{p}}=\mu_{\mathfrak{g}}$ to emphasize that we embed K under ι_p via the prime $\mathfrak{p}$.

Recall that $\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}}$ is the $\mathfrak{p}$-power Selmer group of E over F_∞. Let $\mathfrak{K}_\infty$ be the unique $\mathbb{Z}_p^2$-extension over K, and we identify $\mathrm{Gal}(F_0/K)$ with $\mathrm{Gal}(F_\infty/\mathfrak{K}_\infty)$. Set $\Upsilon=\mathrm{Gal}(F_\infty/\mathfrak{K}_\infty)$. Note that

$$\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}}^\Upsilon=\mathrm{Hom}((X_{\infty,\mathfrak{p}})_\chi,E(\mathfrak{p}))\tag{7.2}$$

and $(X_{\infty,\mathfrak{p}})_\chi$ is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]]$-module, we know $(\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}})^\wedge_\Upsilon$ is a finitely generated torsion $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]]$-module. Write $\mathrm{Char}((\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}})^\wedge_\Upsilon)$ for its characteristic ideal in $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]]$. Observe that

$$\mathrm{Char}((\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}})^\wedge_\Upsilon)=\iota_{\mathfrak{p}}\mathrm{Char}((X_{\infty,\mathfrak{p}})_\chi),\tag{7.3}$$

where $\iota_{\mathfrak{p}}:\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]]\to\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/F_0)]],\gamma\mapsto\varrho_{\mathfrak{p}}(\gamma)\gamma$ for any $\gamma\in\mathrm{Gal}(F_\infty/F_0)$ and $\varrho_{\mathfrak{p}}$ is the character of $\mathrm{Gal}(F_\infty/F_0)$ giving the action on $E(\mathfrak{p})$. The equations (7.1) and (7.3) show that

$$\mathrm{Char}((\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}})^\wedge_\Upsilon)\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]]=(\iota_{\mathfrak{p}}\mu^\chi_{f_E^{(p)},\mathfrak{p}}).\tag{7.4}$$

Similarly, by changing the role of $\mathfrak{p}$ and $\mathfrak{p}^*$, we obtain

$$\mathrm{Char}((\mathrm{Sel}_E(F_\infty)_{\mathfrak{p}^*})^\wedge_\Upsilon)\mathbb{D}[[\mathrm{Gal}(F_\infty/F_0)]]=(\iota_{\mathfrak{p}^*}\mu^\chi_{f_E^{(p)},\mathfrak{p}^*}).\tag{7.5}$$

Put $\Gamma_-=\mathrm{Gal}(\mathfrak{K}_\infty/K_{\mathrm{cyc}})$. Recall the decomposition

$$\mathrm{Sel}_E(K_{\mathrm{cyc}})_p=\mathrm{Sel}_E(K_{\mathrm{cyc}})_{\mathfrak{p}}\oplus\mathrm{Sel}_E(K_{\mathrm{cyc}})_{\mathfrak{p}^*}.$$

The same proof as Lemmas 4.2, 4.3 shows that $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$ is quasi-isomorphic to

$$\mathrm{Hom}((X_{\infty,\mathfrak{p}})_\chi,E(\mathfrak{p}))^{\Gamma_-}\oplus\mathrm{Hom}((X_{\infty,\mathfrak{p}^*})_\chi,E(\mathfrak{p}^*))^{\Gamma_-}.$$

Noting Proposition 7.4, from equations (7.2), (7.4) and (7.5), we obtain

$$c_{E,K}\cdot\Lambda_{\mathbb{D}}=\left(\iota_{\mathfrak{p}}\mu^\chi_{f_E^{(p)},\mathfrak{p}}\iota_{\mathfrak{p}^*}\mu^\chi_{f_E^{(p)},\mathfrak{p}^*}\right).$$

Here, $c_{E,K}$ denotes the characteristic ideal of $(\mathrm{Sel}_E(K_{\mathrm{cyc}})_p)^\wedge$ and $\Lambda_{\mathbb{D}}=\Lambda\widehat{\otimes}\mathbb{D}$. Now applying $\chi_{\mathrm{cyc},K}^{1-s}$ to both sides of the above equality, we know the proposition follows. □

Now we come back to consider the p-adic Birch and Swinnerton-Dyer conjecture of E. If $p=2$, we keep the assumption that E is a quadratic twist of $X_0(49)$ by the extension $\mathbb{Q}(\sqrt{D})$ over $\mathbb{Q}$ for some square-free integer $D \equiv 1 \bmod 4$.

Theorem 7.6. *Assume that $E(K)\otimes_{\mathcal{O}_K} K$ has dimension one over K and $Ш(E/K)(p)$ is finite. Then $\mathrm{Sel}_E(K_{\mathrm{cyc}})_p$ is a cotorsion Λ_Γ-module and the vanishing order of $\mathscr{L}_\varphi(s)$ (resp. $\mathscr{L}_{\overline{\varphi}}(s)$) at $s=1$ is equal to 1. Denote by $\mathscr{L}^*_\varphi(1)$ (resp. $\mathscr{L}^*_{\overline{\varphi}}(1)$) the coefficient of the leading term of $\mathscr{L}_\varphi(s)$ (resp. $\mathscr{L}_{\overline{\varphi}}(s)$) at $s=1$, we have*

$$\mathrm{ord}_p\left(\mathscr{L}^*_\varphi(1)\cdot\mathscr{L}^*_{\overline{\varphi}}(1)\right)=\mathrm{ord}_p\left(\mathscr{C}_p\cdot|Ш(E/K)(p)|\cdot R_p(E/K)\cdot(1-\varphi(\mathfrak{p}))^4(1-\varphi(\mathfrak{p}^*))^4\right). \tag{7.6}$$

Here $\mathscr{C}_p$ is equal to $4^{|\mathcal{B}|}$ or 1 according as $p=2$ or p is odd. Recall that $\mathcal{B}$ denotes the set of bad primes for E over K. Moreover, if E is defined over $\mathbb{Q}$, then we have

$$\mathrm{ord}_p\left(\mathscr{L}^*_\varphi(1)\right)=\mathrm{ord}_p\left(\prod_\ell m_\ell(E/\mathbb{Q})\cdot|Ш(E/\mathbb{Q})(p)|\cdot R_p(E/\mathbb{Q})\cdot(1-\varphi(\mathfrak{p}))^2(1-\varphi(\mathfrak{p}^*))^2\right). \tag{7.7}$$

Here $m_\ell(E/\mathbb{Q})$ denotes the Tamagawa number of E at a prime ℓ, and the first product in (7.7) runs over all bad primes of E over $\mathbb{Q}$.

Proof. Since the complex conjugation changes $\mathscr{L}_\varphi(s)$ to $\mathscr{L}_{\overline{\varphi}}(s)$, we know both p-adic L-functions have the same vanishing order at $s=1$. All assertions in the theorem except (7.7) follow from Theorem 6.1 and Proposition 7.5. In the following we show how to derive (7.7) from (7.6).

Let us first consider the case when p is odd. In this case, the equation (7.6) becomes

$$2\mathrm{ord}_p\left(\mathscr{L}^*_\varphi(1)\right)=\mathrm{ord}_p\left(|Ш(E/K)(p)|\cdot R_p(E/K)\cdot(1-\varphi(\mathfrak{p}))^4(1-\varphi(\mathfrak{p}^*))^4\right).$$

Write N_E for the conductor of E. Since E is defined over $\mathbb{Q}$, the conductor formula of $E/\mathbb{Q}$ shows that the discriminant of K must divide N_E. Noting that p splits in K, from Coates-Wiles theorem (see [15]), we know $E(K)_p=0$. Similar proof as Lemma 6.4 implies that an $\mathcal{O}_K$ generator of $E(K)$ can be taken from $E(\mathbb{Q})$ without changing the p-adic valuation of $R_p(E/K)$. A direct computation using a $\mathbb{Z}$-basis of $\mathcal{O}_K$ shows that

$$\mathrm{ord}_p(R_p(E/K))=2\cdot\mathrm{ord}_p(R_p(E/\mathbb{Q})).$$

Write E^K for the twist of E by $K/\mathbb{Q}$. Since $\mathrm{Gal}(K/\mathbb{Q})$ has order prime to p, its action on $Ш(E/K)(p)$ is semi-simple. We denote by $Ш(E/K)(p)^+$, resp. $Ш(E/K)(p)^-$ the eigenspace with eigenvalue 1, resp. -1 under this action. Then

$$Ш(E/K)(p)=Ш(E/K)(p)^+\oplus Ш(E/K)(p)^-.$$

Similar proof as Lemma 4.4 shows that $Ш(E^K/\mathbb{Q})(p)\simeq Ш(E/K)(p)^-$. We also have $Ш(E/K)(p)^+\simeq Ш(E/\mathbb{Q})(p)$. Since E has complex multiplication by $\mathcal{O}_K$ and p is unramified in K, by [37, Proposition 6(a)] we have that there exists an isogeny between E and E^K whose degree is prime to p. Therefore we know the isogeny induces an isomorphism between $Ш(E/\mathbb{Q})(p)$ and $Ш(E^K/\mathbb{Q})(p)$. We obtain $|Ш(E/K)(p)|=|Ш(E/\mathbb{Q})(p)|^2$. It is clear that (7.7) follows.

Next we consider the case $p=2$, the equation (7.7) turns to be

$$2\mathrm{ord}_p\left(\mathscr{L}^*_\varphi(1)\right)=\mathrm{ord}_p\left(4^{|\mathcal{B}|}\cdot|Ш(E/K)(p)|\cdot R_p(E/K)\cdot(1-\varphi(\mathfrak{p}))^4(1-\varphi(\mathfrak{p}^*))^4\right).$$

Since E has good reduction at 2, the bad primes must be odd. For a bad prime ℓ, viewing E defined over a local field $\mathfrak{L}$ over $\mathbb{Q}_\ell$, from [30, Proposition 4.9], we know $t_\ell(E/\mathfrak{L})=|E(\mathfrak{L})_2|$. Here $t_\ell(E/\mathfrak{L})$ denotes the Tamagawa number of $E/\mathfrak{L}$ at ℓ. Since E is defined over $\mathbb{Q}$, considering the behavior of the bad primes under the extension $K/\mathbb{Q}$, using the fact that $E(K)_2=(\mathbb{Z}/2\mathbb{Z})^2$ and $E(\mathbb{Q})_2=\mathbb{Z}/2\mathbb{Z}$, we obtain

$$\prod_\ell m_\ell(E/\mathbb{Q})=2^{|\mathcal{B}|}.$$

Applying Lemma 6.4 and noting that $|E(K)(2)|=|E(\mathbb{Q})(2)|^2$, we have

$$\mathrm{ord}_p(R_p(E/K))=2\cdot\mathrm{ord}_p(R_p(E/\mathbb{Q})).$$

We conclude the proof by showing that $|Ш(E/K)(2)|=|Ш(E/\mathbb{Q})(2)|^2$. Note that

$$\mathrm{ord}_p\left(R_\infty(E/K)/R_\infty(E/\mathbb{Q})^2\right)=0.$$

By the equivalence of the Birch-Swinnerton-Dyer conjecture for $E/\mathbb{Q}$ and E/K (see [37, Corollary after Theorem 3]), observing all terms except $|Ш(E/K)|$ involving in the Birch-Swinnerton-Dyer formula over

K are square of the corresponding terms over $\mathbb{Q}$, we see immediately that $|Ш(E/K)(2)| = |Ш(E/\mathbb{Q})(2)|^2$. For another proof of this last fact, one can refer to [23, equation (13) on Page 4197]. □

8. Complex and p-adic Gross-Zagier Formulae

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, write ϕ for the newform associated to E. Let p be a prime where E has potentially ordinary reduction, i.e., E has either potentially good ordinary or potentially semistable reduction at p. Let $\alpha : \mathbb{Q}_p^\times \to \mathbb{Z}_p^\times$ be the character contained in the representation $(V_pE)^{ss}$ of $G_{\mathbb{Q}_p}$ such that $\alpha|_{\mathbb{Z}_p^\times}$ is of finite order.

Let $\mathcal{K}$ be an imaginary quadratic field such that $\epsilon(E/\mathcal{K}) = -1$ and p splits in $\mathcal{K}$. Let $\Gamma_\mathcal{K}$ be the Galois group of the $\mathbb{Z}_p^2$-extension over $\mathcal{K}$. Recall that, in [18], there exists a p-adic measure $\mu_{E/\mathcal{K}}$ on $\Gamma_\mathcal{K}$ such that for any finite order character χ of $\Gamma_\mathcal{K}$, we have

$$\chi(\mu_{E/\mathcal{K}}) = \frac{L^{(p)}(1,\phi,\chi)}{8\pi^2(\phi,\phi)} \cdot \prod_{w|p} Z_w(\chi_w, \psi_w),$$

where (ϕ,ϕ) is the Petersson norm of ϕ:

$$(\phi,\phi) = \iint_{\Gamma_0(N)\backslash\mathcal{H}} |\phi(z)|^2 dxdy, \qquad z = x+iy,$$

and for each prime $w|p$ of $\mathcal{K}$, let $\alpha_w = \alpha \circ \mathrm{N}_{\mathcal{K}_w/\mathbb{Q}_p}$ and $\psi_w = \psi_p \circ \mathrm{Tr}_{\mathcal{K}_w/\mathbb{Q}_p}$, and let ϖ_w be a uniformizer of $\mathcal{K}_w$, then

$$Z_w(\chi_w,\psi_w) = \begin{cases} (1-\alpha_w\chi_w(\varpi_w)^{-1})(1-\alpha_w\chi_w(\varpi_w)p^{-1})^{-1}, & \text{if } \alpha_w\chi_w \text{ is unramified;} \\ p^n\tau((\alpha_w\chi_w)^{-1},\psi_w), & \text{if } \alpha_w\chi_w \text{ is of conductor } \varpi^n \ (n\geq 1). \end{cases}$$

From now on, we assume that E has complex multiplication by an imaginary quadratic field K. Since E has potentially good ordinary reduction, the prime p splits in K, say $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. Let φ be the Hecke character over K associated to E. The following lemma will be used to prove our main theorem.

Lemma 8.1. *Assume that $\mathfrak{p}$ is induced by ι_p, i.e., we can identify $K_\mathfrak{p}$ with $\mathbb{Q}_p$. The non-trivial element $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ induces an isomorphism on $\mathbb{A}_K$ so that $\tau : K_{\mathfrak{p}^*} \xrightarrow{\sim} K_\mathfrak{p} = \mathbb{Q}_p$. Then $\alpha = \varphi_{\mathfrak{p}^*} \circ \tau^{-1}$ and $(\alpha^{-1}\chi_{\mathrm{cyc}})(x) = \varphi_\mathfrak{p}(x)x^{-1}$ for any $x \in \mathbb{Q}_p^\times$. Moreover, for any place $w|p$ of $\mathcal{K}$, any finite order character $\nu : \widehat{\mathbb{Q}}^\times/\mathbb{Q}^\times\widehat{\mathbb{Z}}^{\times(p)}\mathbb{Z}_{p,\mathrm{tor}}^\times \to \mu_{p^\infty}$ viewed as a character on $\Gamma_\mathcal{K}$ by composing with the norm map, we have*

$$Z_w(\nu_w,\psi_w) = \tau(\varphi_\mathfrak{p}\nu_\mathfrak{p}^{-1},\psi_w) \cdot \frac{1-(\varphi_\mathfrak{p}\nu_\mathfrak{p}^{-1})(p)p^{-1}}{1-\overline{(\varphi_\mathfrak{p}\nu_\mathfrak{p}^{-1})}(p)p^{-1}}.$$

Proof. The assertions follow from the equalities $\varphi\overline{\varphi} = |\ |_{\mathbb{A}_K^{(\infty)}}^{-1}$ and $\varphi^\tau = \overline{\varphi}$. □

Let $\chi_{\mathrm{cyc},\mathcal{K}} : \Gamma_\mathcal{K} \to \mathbb{Z}_p^\times$ denote the p-adic cyclotomic character of $\Gamma_\mathcal{K}$. Let χ be a finite order anticyclotomic character. Define $\mathscr{L}_{E/\mathcal{K},\chi}$ to be the p-adic L-function

$$\mathscr{L}_{E/\mathcal{K},\chi}(s) = \chi\chi_{\mathrm{cyc},\mathcal{K}}^{1-s}(\mu_{E/\mathcal{K}}), \quad s \in \mathbb{Z}_p.$$

For the trivial character χ, we simply write $\mathscr{L}_{E/\mathcal{K}}$ for $\mathscr{L}_{E/\mathcal{K},\chi}$. Similar to $R_p(E/\mathcal{K})$ and $R_\infty(E/\mathcal{K})$ we define $R_p(E/\mathcal{K},\chi)$, $R_\infty(E/\mathcal{K},\chi)$ to be the complex χ-regulator, the p-adic χ-regulator, respectively.

Theorem 8.2 (See [53] and [18])**.** *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication, let p be a prime where E has potentially good ordinary reduction. Let $\mathcal{K}$ be an imaginary quadratic field such that p splits in $\mathcal{K}$ and $\epsilon(E/\mathcal{K}) = -1$. Then*

$$\frac{\mathscr{L}'_{E/\mathcal{K},\chi}(1)}{R_p(E/\mathcal{K},\chi)} \cdot \frac{L_p(E/\mathcal{K},\chi,1)}{\prod_{w|p} Z_w(\chi_w,\psi_w)} = \frac{L'(E/\mathcal{K},\chi,1)}{R_\infty(E/\mathcal{K},\chi)\cdot 8\pi^2(\phi,\phi)}. \tag{8.1}$$

Here $L_p(E/\mathcal{K},\chi,s)$ denotes the Euler factor of $L(E/\mathcal{K},\chi,s)$ at p. In particular, $\mathscr{L}'_{E/\mathcal{K}}(1) = 0$ if and only if $L'(E/\mathcal{K},1) = 0$.

Proof. Write $\eta_{\mathcal{K}/\mathbb{Q}}$ for the quadratic character associated to $\mathcal{K}/\mathbb{Q}$. For each place v of $\mathbb{Q}$, we denote by η_v the v-component of $\eta_{\mathcal{K}/\mathbb{Q}}$. Let B be an indefinite quaternion algebra over $\mathbb{Q}$ ramified exactly at the places v where $\epsilon_v(E/\mathcal{K},\chi)\eta_v(-1) = -1$. It is well-known that there exists a Shimura curve X over $\mathbb{Q}$ (with suitable level) and a non-constant morphism $f : X \to E$ over $\mathbb{Q}$ mapping a divisor in the Hodge class to the identity of E such that the corresponding Heegner point $P_\chi(f)$ is non-torsion if and only if

$L'(E/\mathcal{K},\chi,1)\neq 0$ by [53, Theorem 1.2]. Note that the p-adic height is non-vanishing when E has complex multiplication (see [2]). From [18, Theorem B], $P_\chi(f)$ is non-torsion if and only if $\mathscr{L}'_{E/\mathcal{K},\chi}(1)\neq 0$. Thus $L'(E/\mathcal{K},\chi,1)=0$ if and only if $\mathscr{L}'_{E/\mathcal{K},\chi}(1)=0$.

Now we assume that $L'(E/\mathcal{K},\chi,1)\neq 0$. Write $\mathcal{K}_\chi$ for the field cut out by χ. Put $\mathcal{O}_\chi$ to be the ring generated by values of χ over $\mathbb{Z}$. By the Euler system method due to Kolyvagin, we know that $(E(\mathcal{K}_\chi)\otimes\mathcal{O}_\chi)^\chi$ is of $\mathcal{O}_\chi$-rank one and

$$\frac{\widehat{h}_\infty(P_\chi(f))}{R_\infty(E/\mathcal{K},\chi)}=\frac{\widehat{h}_p(P_\chi(f))}{R_p(E/\mathcal{K},\chi)}\in\overline{\mathbb{Q}}^\times.$$

Here $\widehat{h}_\infty$ (resp. $\widehat{h}_p$) denotes the Néron -Tate (resp. p-adic) height on $E/\mathcal{K}$.

By [53, Theorem 1.2], we obtain

$$\frac{L'(E/\mathcal{K},\chi,1)}{R_\infty(E/\mathcal{K},\chi)\cdot 8\pi^2(\phi,\phi)}=\frac{h_\infty(P_\chi(f))}{R_\infty(E/\mathcal{K},\chi)}\cdot\frac{4L(1,\eta)}{\pi c_\mathcal{K}}\cdot\frac{L(1,\pi,\mathrm{ad})}{8\pi^3(\phi,\phi)}\cdot\alpha^{-1}(f,\chi).$$

From [18, Theorem B] and [19, Appendix B] (with our definition of $\mathscr{L}_{E/\mathcal{K},\chi}$), we obtain

$$\frac{\mathscr{L}'_{E/\mathcal{K},\chi}(1)}{R_p(E/\mathcal{K},\chi)}=\frac{h_p(P_\chi(f))}{R_p(E/\mathcal{K},\chi)}\cdot\frac{4L(1,\eta)}{\pi c_\mathcal{K}}\cdot\frac{\prod_{w|p}Z_w(\chi_w,\psi_w)}{L_p(E/\mathcal{K},\chi,1)}\cdot\frac{L(1,\pi,\mathrm{ad})}{8\pi^3(\phi,\phi)}\cdot\alpha^{-1}(f,\chi),$$

where the $\alpha(f,\chi)\in\overline{\mathbb{Q}}^\times$. One can refer to [18, equation (1.1.4)] for the definition of $c_\mathcal{K}$. The theorem follows.

□

Now we give an explicit form of p-adic Gross-Zagier formula as an application. Let c be the conductor of χ and D the discriminant of $\mathcal{K}$. Recall that $\phi=\sum_n a_nq^n$ is the newform associated to E. Assume the following Heegner hypothesis holds:

(1) $(c,N)=1$, and no prime divisor q of N is inert in $\mathcal{K}$, and also q must be split in $\mathcal{K}$ if $q^2|N$.
(2) $\chi([\mathfrak{q}])\neq a_q$ for any prime $q|(N,D)$, where $\mathfrak{q}$ is the unique prime ideal of $\mathcal{O}_\mathcal{K}$ above q and $[\mathfrak{q}]$ is its class in $\mathrm{Pic}(\mathcal{O}_c)$.

Let $X_0(N)$ be the modular curve over $\mathbb{Q}$, whose $\mathbb{C}$-points parametrize isogenies $E_1\to E_2$ between elliptic curves over $\mathbb{C}$ whose kernel is cyclic of order N. Let $\mathcal{O}_c=\mathbb{Z}+c\mathcal{O}_\mathcal{K}$ be an order in $\mathcal{K}$. From the above Heegner hypothesis, there exists a proper ideal $\mathcal{N}$ of $\mathcal{O}_c$ such that $\mathcal{O}_c/\mathcal{N}\cong\mathbb{Z}/N\mathbb{Z}$. For any proper ideal $\mathfrak{a}$ of $\mathcal{O}_c$, let $P_\mathfrak{a}\in X_0(N)$ be the point representing the isogeny $\mathbb{C}/\mathfrak{a}\to\mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$, which is defined over the ring class field H_c over $\mathcal{K}$ of conductor c, and only depends on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_c)$. Let $f:X_0(N)\to E$ be a modular parametrization mapping the cusp at infinity to the identity in E. Denote by $\deg f$ the degree of the morphism f. Define the Heegner point to be

$$P_\chi(f):=\sum_{[\mathfrak{a}]\in\mathrm{Pic}(\mathcal{O}_c)}f(P_\mathfrak{a})\otimes\chi([\mathfrak{a}])\in E(H_c)_{\overline{\mathbb{Q}}}.$$

Theorem 8.3. *Let E,χ be as above satisfying the Heegner conditions (1) and (2). Then*

$$L'(E/\mathcal{K},\chi,1)=2^{-\mu(N,D)}\cdot\frac{8\pi^2(\phi,\phi)}{u^2\sqrt{|Dc^2|}}\cdot\frac{\widehat{h}_\infty(P_\chi(f))}{\deg f},$$

where $\mu(N,D)$ is the number of prime factors of the greatest common divisor of N and D, $u=[\mathcal{O}_c^\times:\mathbb{Z}^\times]$ is half of the number of roots of unity in $\mathcal{O}_c$, and $\widehat{h}_\infty$ is the Néron -Tate height on E over $\mathcal{K}$.

Moreover, let p be a prime split in $\mathcal{K}$ and assume that E has potentially ordinary reduction at p, then we have

$$\mathscr{L}'_{E/\mathcal{K},\chi}(1)=\frac{\prod_{w|p}Z_w(\chi_w,\psi_w)}{L_p(E/\mathcal{K},\chi,1)}\cdot\frac{2^{-\mu(N,D)}}{u^2\sqrt{|Dc^2|}}\cdot\frac{\widehat{h}_p(P_\chi(f))}{\deg f},$$

where $\widehat{h}_p$ is the p-adic height on E over $\mathcal{K}$.

Proof. The explicit form of the complex Gross-Zagier formula is proved in [7]. The explicit form of the p-adic Gross-Zagier formula then follows from the equation (8.1) in Theorem 8.2. □

9. Proof of the main theorem

In this section, let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by K, let $\Omega(E/\mathbb{Q})$ be the minimal real period of E over $\mathbb{Q}$. Denote by p a prime which splits in K. As always we assume that E has potentially good ordinary reduction at p, and good ordinary reduction at p when $p = 2$. Recall that we have defined Ω_E to be the $\mathfrak{p}$-minimal period for E over K in §7.

Lemma 9.1. *Let $\mathcal{K}$ be an imaginary quadratic field where p splits, $\eta_{\mathcal{K}/\mathbb{Q}}$ the associated quadratic character, and η_K the base extension of $\eta_{\mathcal{K}/\mathbb{Q}}$ to K. Assume that $\epsilon(E/\mathcal{K}) = -1$. Then there exists a p-adic unit u such that*

$$\mathscr{L}_{E/\mathcal{K}} = u \cdot \frac{\tau(\varphi_{\mathfrak{p}}, \psi_{\mathfrak{p}})^2 \cdot \Omega_E^2}{8\pi^2(\phi, \phi)} \cdot \mathscr{L}_{\varphi}\mathscr{L}_{\varphi\eta_K}.$$

Proof. Let $\mathfrak{f}_0 = \mathfrak{f}_E^{(p)}$. It's enough to show that for any finite order character

$$\nu : \widehat{\mathbb{Q}}/\mathbb{Q}^\times \widehat{\mathbb{Z}}^{\times(p)} \mathbb{Z}_{p,\mathrm{tor}}^\times \to \mathbb{C}^\times,$$

we have

$$\nu_{\mathcal{K}}(\mu_{E/K}) = \tau(\varphi_{\mathfrak{p}}, \psi_{\mathfrak{p}})^2 \cdot \frac{\Omega_E^2}{8\pi^2(\phi, \phi)} \cdot \mu_{\mathfrak{f}_0}(\varphi\nu_K^{-1})\mu_{\mathfrak{f}_0}(\varphi\eta_K\nu_K^{-1}). \tag{9.1}$$

Here $\nu_{\mathcal{K}} = \nu \circ \mathrm{N}_{\mathcal{K}/\mathbb{Q}}$ and $\nu_K = \nu \circ \mathrm{N}_{K/\mathbb{Q}}$. By interpolation property, $\nu_{\mathcal{K}}(\mu_{E/K})$ is equal to

$$\frac{L^{(p)}(1, \phi, \nu_{\mathcal{K}}^{-1})}{8\pi^2(\phi, \phi)} \prod_{w|p} Z_w(\nu_w, \psi_w).$$

Note that p splits in $\mathcal{K}$, η_K is trivial at primes above p. From Theorem 7.1, $\mu_{\mathfrak{f}_0}(\varphi\nu_K^{-1})\mu_{\mathfrak{f}_0}(\varphi\eta_K\nu_K^{-1})$ is equal to

$$\frac{\tau(\varphi_{\mathfrak{p}}\nu_{\mathfrak{p}}^{-1}, \psi_{\mathfrak{p}})^2}{\tau(\varphi_{\mathfrak{p}}, \psi_{\mathfrak{p}})^2} \cdot \left(\frac{1 - \varphi\nu^{-1}(\mathfrak{p})p^{-1}}{1 - \overline{\varphi\nu^{-1}}(\mathfrak{p})p^{-1}}\right)^2 \cdot \frac{L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu_K^{-1}}, 1)}{\Omega_E} \cdot \frac{L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu_K^{-1}\eta_K}, 1)}{\Omega_E}.$$

Then the equality (9.1) follows from the identity

$$L^{(p)}(1, \phi, \nu_{\mathcal{K}}^{-1}) = L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu_K^{-1}}, 1) \cdot L^{(p\mathfrak{f}_0)}(\overline{\varphi\nu_K^{-1}\eta_K}, 1)$$

and Lemma 8.1. □

We are ready to prove Theorem 1.1. Assume that $L(E, s)$ has a simple zero at $s = 1$. Let p be a prime satisfying either E has bad but potentially good ordinary reduction at $p \neq 2$ (odd case) or E has good ordinary reduction at $p = 2$ (even case). Let φ be the Hecke character over K associated to E and recall that $\mathfrak{f}_0 = \mathfrak{f}_E^{(p)}$. We choose an imaginary quadratic field $\mathcal{K}$ such that

- $L(E/\mathcal{K}, s)$ has a simple zero at $s = 1$.
- p splits in $\mathcal{K}$.
- The discriminant D of $\mathcal{K}$ is prime to $\mathfrak{f}_0$.

Let $E^{\mathcal{K}}$ denote the twist of E by the field extension $\mathcal{K}$ over $\mathbb{Q}$.

Proof of Theorem 1.1 for the odd case. Note that related Euler factors are trivial in this case, we then have

- $\mathscr{L}_{\varphi\eta_K}(1) = \dfrac{L(E^{\mathcal{K}}, 1)}{\Omega_E}$,
- $\dfrac{\mathscr{L}'_{E/\mathcal{K}}(1)}{R_p(E/\mathbb{Q}) \cdot \tau(\varphi_{\mathfrak{p}}, \psi_{\mathfrak{p}})^2} = \dfrac{L'(E/\mathcal{K}, 1)}{R_\infty(E/\mathbb{Q}) \cdot 8\pi^2(\phi, \phi)}$.
- $\mathrm{ord}_p(|Ш(E/\mathbb{Q})|) = \mathrm{ord}_p\left(\dfrac{\mathscr{L}'_{\varphi}(1)}{R_p(E/\mathbb{Q})}\right)$,
- $\mathrm{ord}_p\left(\dfrac{\mathscr{L}'_{E/K}(1)}{\mathscr{L}'_{\varphi}(1)\mathscr{L}_{\varphi\eta_K}(1)}\right) = \mathrm{ord}_p\left(\dfrac{\tau(\varphi_{\mathfrak{p}}, \psi_{\mathfrak{p}})^2 \cdot \Omega_E^2}{8\pi^2 \cdot (\phi, \phi)}\right)$,
- $\mathrm{ord}_p\left(\dfrac{\Omega(E/\mathbb{Q})}{\Omega_E}\right) = 0$.

It follows that

$$\mathrm{ord}_p(|Ш(E/\mathbb{Q})|) = \mathrm{ord}_p\left(\frac{L'(E/\mathbb{Q},1)}{\Omega(E/\mathbb{Q})\cdot R_\infty(E/\mathbb{Q})}\right).$$

This proves Theorem 1.1 when p is odd.

□

Proof of Theorem 1.1 for the even case. Note that all related root numbers (or Gauss sums) are trivial in this case. We then have

- $\mathscr{L}_{\varphi\eta_K}(1) = \left(1-\frac{\varphi(\mathfrak{p})}{p}\right)^2\cdot\frac{L(E^{\mathcal{K}},1)}{\Omega_E}$,
- $\frac{\mathscr{L}'_{E/\mathcal{K}}(1)}{R_p(E/\mathbb{Q})}\cdot\left(1-\frac{\varphi(\mathfrak{p})}{p}\right)^{-4} = \frac{L'(E/\mathcal{K},1)}{R_\infty(E/\mathbb{Q})\cdot 8\pi^2(\phi,\phi)}$.
- $\mathrm{ord}_p\left(\left(1-\frac{\varphi(\mathfrak{p})}{p}\right)^{-2}\cdot\frac{\mathscr{L}'_\varphi(1)}{R_p(E/\mathbb{Q})}\right) = \mathrm{ord}_p\left(\prod_\ell m_\ell(E/\mathbb{Q})\cdot|Ш(E/\mathbb{Q})|\right)$,
- $\mathrm{ord}_p\left(\frac{\mathscr{L}'_{E/K}(1)}{\mathscr{L}'_\varphi(1)\mathscr{L}_{\varphi\eta_K}(1)}\right) = \mathrm{ord}_p\left(\frac{\Omega_E^2}{8\pi^2\cdot(\phi,\phi)}\right)$,
- $\mathrm{ord}_p\left(\frac{\Omega(E/\mathbb{Q})}{\Omega_E}\right) = 0$.

Therefore we obtain

$$\mathrm{ord}_p\left(\prod_\ell m_\ell(E/\mathbb{Q})\cdot|Ш(E/\mathbb{Q}|)\right) = \mathrm{ord}_p\left(\frac{L'(E/\mathbb{Q},1)}{\Omega(E/\mathbb{Q})\cdot R_\infty(E/\mathbb{Q})}\right).$$

The even case of Theorem 1.1 follows.

□

10. Appendix (I): Non-existence of certain non-zero finite submodules

Let K be an imaginary quadratic field and F a finite abelian extension over K. Let E be an elliptic curve over F with complex multiplication by $\mathcal{O}_K$. Let p be a prime such that p splits in K, i.e., $p\mathcal{O}_K = \mathfrak{p}\cdot\mathfrak{p}^*$. We assume E has good ordinary reduction at all primes of F above p.

Let $\mathcal{P}$ be the set of primes in F above $\mathfrak{p}$ and $\mathcal{B}$ the set of primes in F where E has bad reduction. Put $\mathcal{W} = \mathcal{P}\cup\mathcal{B}$. We make the convention that for an algebraic extension over F and a set $\mathcal{S}$ of primes in F, we use the same notation to denote the set of primes lying above the ones in $\mathcal{S}$. Let F_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension over F, let $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F)$ and denote by $\Lambda = \Lambda_\Gamma$ the Iwasawa algebra of Γ. For any set $\mathcal{S}$ of primes in F, we define $\mathrm{Sel}_E^{\mathcal{S}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ to be the relaxed at $\mathcal{S}$ $\mathfrak{p}$-power Selmer group of E over F_{cyc}. The Selmer group $\mathrm{Sel}_E^{\mathcal{S}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ is a Λ-module.

The aim of the appendix is to prove the following theorem.

Theorem 10.1. *Assume that $\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}}$ is a cotorsion Λ-module. If each prime of F above p is totally ramified in F_{cyc}, then the Pontryagin dual of $\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ has no non-zero finite Λ-submodules.*

We remark that Theorem 10.1 implies the non-existence of non-zero Λ-modules used in the proof for Proposition 6.2. Either by the assumption $E(F)$ has $\mathcal{O}_K$-rank one, $Ш(E/F)(p)$ is finite in the proposition and Schneider's proof, or applying a similar proof of Rubin [44] using Iwasawa main conjecture and Rohrlich's theorem, we know $\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}}$ is a cotorsion Λ-module. It is also easy to see each prime above p is totally ramified in F_{cyc}/F. Since the curve E in Proposition 6.2 has good reduction everywhere over F, Theorem 10.1 shows that $(\mathrm{Sel}_E^{\mathcal{P}}(F_{\mathrm{cyc}})_{\mathfrak{p}})^\wedge$ has no non-zero finite Λ-submodules. An easy argument using Tate local duality implies that $H^1(F_{\mathrm{cyc},w},E)(\mathfrak{p}) = 0$ for every prime w of F_{cyc} above $\mathfrak{p}$. Therefore, $\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}} = \mathrm{Sel}_E^{\mathcal{P}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ and $(\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}})^\wedge$ has no non-zero finite Λ-submodules. Notice the decomposition

$$\mathrm{Sel}_E(F_{\mathrm{cyc}})_p = \mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}}\oplus\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}^*}.$$

Since E in Proposition 6.2 is defined over $\mathbb{Q}$, E is invariant under complex conjugation. The same proof as Theorem 10.1 applying to the prime $\mathfrak{p}^*$ implies that $(\mathrm{Sel}_E(F_{\mathrm{cyc}})_p)^\wedge$ has no non-zero finite Λ-submodules.

The rest of this section is devoted to giving a proof of Theorem 10.1. The idea of showing that the dual of $\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ has no non-trivial finite Λ-submodules is due to Greenberg. In fact, we know from [27,

Proposition 2.4] that the Λ-module $(\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}})^\wedge$ having no non-zero finite Λ-submodules is equivalent to the discrete Λ-module $\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ being almost (Λ-)divisible, that is, for all but finitely many height one elements $\lambda \in \Lambda$, i.e., $\lambda\Lambda$ is a height one prime ideal in Λ, we have

$$\lambda \,\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}} = \mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}.$$

To show the almost divisibility of $\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$, we show that the sequence

$$0 \to \mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}} \to H^1(F_{\mathrm{cyc}}, E(\mathfrak{p})) \to \prod_{v\nmid\mathcal{W}} H^1(F_{\mathrm{cyc},v}, E)(\mathfrak{p}) \to 0 \tag{10.1}$$

is exact (the difficult part is showing the surjectivity of the localization map). Since this is an exact sequence of Λ-modules, we can consider the multiplication-by-λ map on each term for any element $\lambda \in \Lambda$. Then the snake lemma gives us the exact sequence

$$H^1(F_{\mathrm{cyc}}, E(\mathfrak{p}))[\lambda] \xrightarrow{\alpha_\lambda} \left(\prod_{v\nmid\mathcal{W}} H^1(F_{\mathrm{cyc},v}, E)(\mathfrak{p})\right)[\lambda] \to \frac{\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}}{\lambda\,\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}} \to \frac{H^1(F_{\mathrm{cyc}}, E(\mathfrak{p}))}{\lambda\, H^1(F_{\mathrm{cyc}}, E(\mathfrak{p}))}, \tag{10.2}$$

where for a Λ-module $\mathfrak{M}$, we denote $\mathfrak{M}[\lambda]$ by the submodule consisting of elements which are annihilated by λ. Thus, the almost divisibility of $\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}}$ follows from the almost divisibility of $H^1(F_{\mathrm{cyc}}, E(\mathfrak{p}))$ and the surjectivity of the map α_λ for all but finitely many λ. We will give this argument in the language of Selmer group for p-adic Galois representations [24]. For this purpose, let us introduce more notation. Denote by Σ the set of primes of F which either lie above p or are bad for E. We denote by F_Σ the maximal algebraic extension over F which is unramified outside the set of primes of F lying above those in Σ.

Lemma 10.2. *We have*

$$\mathrm{Sel}_E^{\mathcal{W}}(F_{\mathrm{cyc}})_{\mathfrak{p}} = \mathrm{Ker}\left(H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p})) \to \prod_{v\mid\mathfrak{p}^*} H^1(F_{\mathrm{cyc},v}, E(\mathfrak{p}))\right). \tag{10.3}$$

Proof. This is a well-known fact. A similar proof as [11, Lemma 2.3] gives the result. □

Now, we introduce the Greenberg Selmer group. Identifying $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{K_{\mathfrak{p}}}$ with $\mathbb{Z}_p$, we have $\Lambda = \mathscr{O}_{\mathfrak{p}}[[\Gamma]]$. Recall that $\Lambda^\times$ is the group of units in Λ. Denote by $T_{\mathfrak{p}}E$ the $\mathfrak{p}$-adic Tate module of E, and we let

$$\rho_0 : \mathrm{Gal}(F_\Sigma/F) \to \mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(T_{\mathfrak{p}}E)$$

be the $\mathcal{O}_{\mathfrak{p}}$-linear representation of $\mathrm{Gal}(F_\Sigma/F)$ on $T_{\mathfrak{p}}E$. Let $\kappa : \Gamma \to \Lambda^\times$ be the natural inclusion. We write $\Lambda(\kappa)$ for the Iwasawa algebra Λ with the Galois action of $\mathrm{Gal}(F_\Sigma/F)$ given by the composition of the map κ with the quotient map $\mathrm{Gal}(F_\Sigma/F) \twoheadrightarrow \mathrm{Gal}(F_{\mathrm{cyc}}/F) = \Gamma$. Then we have a representation

$$\rho : \mathrm{Gal}(F_\Sigma/F) \to \Lambda^\times$$

with the representation space $\mathcal{T} = T_{\mathfrak{p}}E \otimes_{\mathcal{O}_{\mathfrak{p}}} \Lambda(\kappa)$, where the Galois group $\mathrm{Gal}(F_\Sigma/F)$ acts on $\mathcal{T}$ via $\rho_0 \otimes \kappa$.

Recall that $\Lambda^\wedge = \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(\Lambda, K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$ is the Pontryagin dual of Λ. We define $\mathcal{E} = \mathcal{T} \otimes_\Lambda \Lambda^\wedge$. Then the Greenberg Selmer group of E over F is defined to be

$$S_{\mathcal{E}}(F) := \bigcap_{v\in\Sigma} \ker\left(H^1(F_\Sigma/F, \mathcal{E}) \to \frac{H^1(F_v, \mathcal{E})}{L_v(\mathcal{E})}\right).$$

Here, the set of local conditions $\mathcal{L} = (L_v(\mathcal{E}))_{v\in\Sigma}$ is given by

$$L_v(\mathcal{E}) = \begin{cases} H^1(F_v, \mathcal{E}) & \text{if } v \nmid \mathfrak{p}^*, \\ 0 & \text{if } v \mid \mathfrak{p}^*. \end{cases} \tag{10.4}$$

Lemma 10.3. *As Λ-modules, we have $S_{\mathcal{E}}(F) \simeq (\mathrm{Sel}_E(F_{\mathrm{cyc}})_{\mathfrak{p}})^\iota$, where for a Λ-module $\mathfrak{M}$, $\mathfrak{M}^\iota$ means the abelian group $\mathfrak{M}$ with the Γ action given by the map $\gamma \mapsto \gamma^{-1}$ for $\gamma \in \Gamma$.*

Proof. The lemma is an application of Shapiro Lemma. A detailed proof can be found in [25, Proposition 3.2]. □

For any place v of F lying above $\mathfrak{p}$, our assumption implies that F_{cyc}/F is totally ramified at v. Thus, writing w for the unique place of F_{cyc} above v, the proof of the Lemma 10.3 (or [25, Proposition 3.2]) gives the isomorphism

$$H^1(F_v, \mathcal{E}) \simeq H^1(F_{\mathrm{cyc},w}, E(\mathfrak{p}))^\iota. \tag{10.5}$$

Now we show that $H^1(F_\Sigma/F, \mathcal{E})$ is an almost divisible Λ-module. For this purpose, we compute the Λ-corank of each term in the following exact sequence

$$0 \to S_{\mathcal{E}}(F) \to H^1(F_\Sigma/F, \mathcal{E}) \xrightarrow{\phi_{\mathcal{L}}} Q_{\mathcal{L}}(F, \mathcal{E}), \tag{10.6}$$

where $Q_{\mathcal{L}}(F, \mathcal{E}) = \prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E})}{L_v(\mathcal{E})}$, and $\phi_{\mathcal{L}} = (\phi_{L_v})_v$ is the natural localization map for $H^1(F_\Sigma/F, \mathcal{E})$ at each $v \in \Sigma$. Recall we have assumed that $S_{\mathcal{E}}(F)$ is a cofinitely generated Λ-torsion module.

Lemma 10.4. *The modules $H^1(F_\Sigma/F, \mathcal{E})$ and $Q_{\mathcal{L}}(F, \mathcal{E})$ are cofinitely generated Λ-modules and*

$$\mathrm{corank}_\Lambda(H^1(F_\Sigma/F, \mathcal{E})) = \mathrm{corank}_\Lambda(Q_{\mathcal{L}}(F, \mathcal{E})) = r_2(F) = [F : K].$$

Here $r_2(F)$ denotes the number of the complex places of F. In particular, we have $H^2(F_\Sigma/F, \mathcal{E}) = 0$.

Proof. The cofinitely generated property of these modules are well-known (see [27, Proposition 3.2]). For the assertion on the $\mathrm{corank}_\Lambda(Q_{\mathcal{L}}(F, \mathcal{E}))$, we refer the reader to [29, §2.3], or [27, section 4]. The method also works for $p = 2$ since F has no real places. Note the exact sequence

$$0 \to S_{\mathcal{E}}(F) \to H^1(F_\Sigma/F, \mathcal{E}) \to Q_{\mathcal{L}}(F, \mathcal{E})$$

and that $S_{\mathcal{E}}(F)^\vee$ is Λ-torsion, we have $\mathrm{corank}_\Lambda(H^1(F_\Sigma/F, \mathcal{E})) \le r_2(F)$. On the other hand, by the global Euler characteristic, we obtain

$$\mathrm{corank}_\Lambda(H^1(F_\Sigma/F, \mathcal{E})) = \mathrm{corank}_\Lambda(H^0(F_\Sigma/F, \mathcal{E})) + \mathrm{corank}_\Lambda(H^2(F_\Sigma/F, \mathcal{E})) + r_2(F).$$

Thus $\mathrm{corank}_\Lambda(H^1(F_\Sigma/F, \mathcal{E})) \ge r_2(F)$ and we obtain $\mathrm{corank}_\Lambda(H^1(F_\Sigma/F, \mathcal{E})) = r_2(F)$. So $H^2(F_\Sigma/F, \mathcal{E})$ is a cotorsion Λ-module. The second assertion follows from the fact that $H^2(F_\Sigma/F, \mathcal{E})$ is a divisible Λ-module (see [28, Proposition 2.1.1, Lemma 5.2.2]). □

Proposition 10.5. *The module $H^1(F_\Sigma/F, \mathcal{E})$ is an almost divisible Λ-module.*

Proof. By [27, Theorem 3], $H^i(F_\Sigma/F, \mathcal{E})$ is isomorphic to $H^i(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\iota$ for $i = 1, 2$. The Hochschild-Serre spectral sequence implies the exact sequence

$$0 \to H^1(\Gamma, H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))) \to H^2(F_\Sigma/F, E(\mathfrak{p})) \to H^2(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\Gamma \to 0.$$

Since Lemma 10.4 shows that $H^2(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p})) = 0$, we obtain

$$H^1(\Gamma, H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))) \simeq H^2(F_\Sigma/F, E(\mathfrak{p})).$$

From the proof of Lemma 10.4, we know that $H^2(F_\Sigma/F, \mathcal{E})$ is a divisible Λ-module. Therefore the module $(H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\vee)^\Gamma$ has no non-zero finite submodules. Now, by the equivalence of the notions of a module being almost Λ-divisible and its dual having no non-zero finite Λ-submodules, it remains to show that $H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\vee$ has no non-zero finite Λ-submodules. Indeed, suppose otherwise and let $\mathscr{F}' \neq 0$ be a maximal finite Λ-submodule of $H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\vee$. Let γ_0 be a topological generator of Γ. Given any integer $m \ge 1$, we may consider $\gamma_0^m - 1$ acting on the exact sequence

$$0 \to \mathscr{F}' \to H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\vee \to H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\vee/\mathscr{F}' \to 0.$$

Noting that $(H^1(F_\Sigma/F_{\mathrm{cyc}}, E(\mathfrak{p}))^\vee)^\Gamma$ is $\mathbb{Z}_p$-torsion free and applying the snake lemma, we see that $\gamma_0^m - 1$ is injective on $\mathscr{F}'$. On the other hand, γ_0 acts on $\mathscr{F}'$ continuously and $\mathscr{F}'$ is finite, and so $\mathscr{F}'$ is annihilated by $\gamma_0^m - 1$ when m is sufficiently large. Thus, $\mathscr{F}' = 0$, and the proposition follows. □

Next, we show that the map $\phi_{\mathcal{L}}$ in the sequence (10.6) is surjective. Let μ_{p^∞} be the group of all p-power roots of unity. We define $\mathcal{E}^* = \mathrm{Hom}(\mathcal{E}, \mu_{p^\infty})$.

Lemma 10.6. *For any place $v \in \Sigma$, we have $H^0(F_v, \mathcal{E}^*) = 0$.*

Proof. The result follows from the fact that each $v \in \Sigma$ does not split completely in the extension F_{cyc}/F and Burnside's finite basis theorem. For details, one can refer [28, Lemma 5.2.2]. □

Proposition 10.7. *The map $\phi_{\mathcal{L}}$ in (10.6) is surjective.*

Proof. Since $\Lambda \simeq \mathbb{Z}_p[[T]]$, the module $\mathcal{E}$ is a divisible Λ-module. Notice our assumption that $S_{\mathcal{E}}(F)$ is a cotorsion Λ-module, by the exact sequence

$$0 \to S_{\mathcal{E}}(F) \to H^1(F_\Sigma/F, \mathcal{E}) \to Q_{\mathcal{L}}(F, \mathcal{E}) \to \mathrm{coker}(\phi_{\mathcal{L}}) \to 0$$

and Lemma 10.4, $\mathrm{coker}(\phi_{\mathcal{L}})$ is a cotorsion Λ-module. Set

$$Ш^2(F, \Sigma, \mathcal{E}) = \ker\left(H^2(F_\Sigma/F, \mathcal{E}) \to \prod_{v\in\Sigma} H^2(F_v, \mathcal{E})\right).$$

From Lemma 10.6 and Tate local duality, we obtain $H^2(F_v, \mathcal{E}) = 0$ for each $v \in \Sigma$. By Lemma 10.4 we have

$$Ш^2(F, \Sigma, \mathcal{E}) = H^2(F_\Sigma/F, \mathcal{E}) = 0.$$

Therefore we have verified the assumptions in [28, Proposition 3.2.1]. We take any place $\varsigma \in \Sigma$ such that $\varsigma \nmid \mathfrak{p}^*$. This is possible since p splits in K and Σ contains the primes above p. From the local conditions (10.4), we have

$$\frac{H^1(F_\varsigma, \mathcal{E})}{L_\varsigma(\mathcal{E})} = 0.$$

By Lemma 10.6, $H^0(F_\varsigma, \mathcal{E}^*) = 0$. Therefore the condition (c) in [28, Proposition 3.2.1] is satisfied and $\phi_{\mathcal{L}}$ is surjective. □

In the final part of this section, we show that for all but finitely many height one $\lambda \in \Lambda$, the map on the λ-torsion submodules

$$\alpha_\lambda : H^1(F_\Sigma/F, \mathcal{E})[\lambda] \to \left(\prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E})}{L_v(\mathcal{E})}\right)[\lambda]$$

is surjective. From the exact sequence

$$0 \to \mathcal{E}[\lambda] \to \mathcal{E} \xrightarrow{\lambda} \mathcal{E} \to 0,$$

we obtain two natural surjective morphisms

$$h_\lambda : H^1(F_\Sigma/F, \mathcal{E}[\lambda]) \to H^1(F_\Sigma/F, \mathcal{E})[\lambda] \quad \text{and} \quad h_{\lambda,v} : H^1(F_v, \mathcal{E}[\lambda]) \to H^1(F_v, \mathcal{E})[\lambda]. \tag{10.7}$$

We consider these modules as (Λ/λ)-modules. We then define the local conditions $\mathcal{L}_\lambda = (L_v(\mathcal{E}[\lambda]))$ for $\mathcal{E}[\lambda]$ to be

$$L_v(\mathcal{E}[\lambda]) = h_{\lambda,v}^{-1}(L_v(\mathcal{E})[\lambda]).$$

Then we can define the Selmer group $S_{\mathcal{E}[\lambda]}(F)$ with respect to $\mathcal{E}[\lambda]$ and $\mathcal{L}_\lambda$ in the same way as we defined $S_{\mathcal{E}}(F)$. The product of the $h_{\lambda,v}$'s for $v \in \Sigma$ defines a surjective map $b_\lambda : \prod_{v\in\Sigma} H^1(F_v, \mathcal{E}[\lambda]) \to \left(\prod_v H^1(F_v, \mathcal{E})\right)[\lambda]$. Note that the image of $\mathcal{L}_\lambda$ is contained in $\mathcal{L}$, thus, we get a well-defined morphism

$$q_\lambda : \prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E}[\lambda])}{L_v(\mathcal{E}[\lambda])} \to \left(\prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E})}{L_v(\mathcal{E})}\right)[\lambda].$$

Lemma 10.8. *Assume that $\mathcal{E}$ and $L_v(\mathcal{E})$ at each $v \in \Sigma$ are divisible by λ. Then q_λ is an isomorphism.*

Proof. This is [29, Lemma 3.2.1]. □

From the definitions of the Selmer groups $S_{\mathcal{E}}(F)$ and $S_{\mathcal{E}[\lambda]}(F)$, we obtain the commutative diagram

$$\begin{array}{ccc} H^1(F_\Sigma/F, \mathcal{E}[\lambda]) & \xrightarrow{\phi_\lambda} & \prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E}[\lambda])}{L_v(\mathcal{E}[\lambda])} \\ \downarrow{\scriptstyle h_\lambda} & & \downarrow{\scriptstyle q_\lambda} \\ H^1(F_\Sigma/F, \mathcal{E})[\lambda] & \xrightarrow{\alpha_\lambda} & \left(\prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E})}{L_v(\mathcal{E})}\right)[\lambda]. \end{array}$$

Since $\mathcal{E}$ is Λ-divisible, it follows from Lemma 10.8 that q_λ is an isomorphism if $L_v(\mathcal{E})$ is λ-divisible. Furthermore, from (10.7) the left vertical map is surjective, we obtain $\mathrm{im}(\alpha_\lambda) \simeq \mathrm{im}(\phi_\lambda)$, and $\mathrm{coker}(\alpha_\lambda) \simeq \mathrm{coker}(\phi_\lambda)$. Therefore, showing the surjectivity of α_λ is reduced to showing the surjectivity of ϕ_λ.

Lemma 10.9. *For our local conditions $\mathcal{L} = (L_v(\mathcal{E}))_{v\in\Sigma}$, we have*

$$L_v(\mathcal{E}) = \begin{cases} 0 & \text{if } v \nmid \mathfrak{p} \\ E(F_{\mathrm{cyc},v}) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) & \text{if } v \mid \mathfrak{p}. \end{cases}$$

In particular, $\mathcal{L}$ is an almost divisible Λ-module. Here, for any prime v of F above $\mathfrak{p}$, we denote by $F_{\mathrm{cyc},v}$ the completion of F_{cyc} at the unique prime above v since we have assumed v is totally ramified in F_{cyc}/F.

Proof. For a prime $w \in \mathcal{B}$, since w not lying above p, the Kummer descent sequence shows that

$$H^1(F_{\mathrm{cyc},w}, E(\mathfrak{p})) \simeq H^1(F_{\mathrm{cyc},w}, E)(\mathfrak{p}).$$

We now show that $H^1(F_{\mathrm{cyc},w}, E)(p) = 0$, which implies the above two groups are zero. For p odd this is easy. We now assume that $p = 2$. In fact, since E has additive reduction at w and the formal group at w is not pro-p, using Tate local duality, for each integer $m \geq 0$, $H^1(F_{m,w}, E)(2)$ is dual to $E(F_{m,w})_2$. The latter group is of uniformly bounded order which is independent of m. Since $H^1(F_{\mathrm{cyc},w}, E)(2)$ is dual to the projective limit of $E(F_{m,w})_2$ with respect to m via the norm maps, we know that $H^1(F_{\mathrm{cyc},w}, E)(2) = 0$. Now, using Tate local duality and noting that $E(F_{\mathrm{cyc}})(\mathfrak{p}^*)$ is finite, for any $w \in \mathcal{P}$, we have $H^1(F_{\mathrm{cyc},w}, E)(\mathfrak{p}) = 0$. Thus, by the Kummer descent sequence, we obtain $H^1(F_{\mathrm{cyc},w}, E(\mathfrak{p})) \simeq E(F_{\mathrm{cyc},w}) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$. Then the first assertion follows. The almost Λ-divisibility of $\mathcal{L}$ follows from [27, Proposition 2.4] and the fact that the dual of $E(F_{\mathrm{cyc},w}) \otimes (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$ for $w \mid \mathfrak{p}$ has no non-zero finite Λ-submodules. □

We conclude this appendix with the following proposition, from which Theorem 10.1 follows.

Proposition 10.10. *For all but finitely many height one $\lambda \in \Lambda$, α_λ is surjective.*

Proof. By Lemma 10.9, the remark preceding it, and [27, Proposition 2.4], we can reduce to showing that

$$\phi_\lambda : H^1(F_\Sigma/F, \mathcal{E}[\lambda]) \to \prod_{v\in\Sigma} \frac{H^1(F_v, \mathcal{E}[\lambda])}{L_v(\mathcal{E}[\lambda])}$$

is surjective for almost all λ such that $(\lambda) = \lambda\Lambda$ is a height one prime ideal. Here, we just sketch the main ingredients for the proof, and the details can be found in [29, Proposition 4.1.1]. The key is that the module $\mathcal{E}$ is a coreflexive Λ-module (since Λ is a UFD, and it is reflexive by [27] or [29, Page 229]). This guarantees that

(a) the module $\mathcal{E}[\lambda]$ is a divisible (Λ/λ)-module for all height one $(\lambda) \in \mathrm{Spec}(\Lambda)$, see [27, Corollary 2.6.1];
(b) for each place $v \in \Sigma$, $H^0(F_v, \mathcal{E}^*) = 0$ if and only if $H^0(F_v, (\mathcal{E}[\lambda])^*) = 0$ for almost all height one $(\lambda) \in \mathrm{Spec}(\Lambda)$, where $(\mathcal{E}[\lambda])^* = \mathrm{Hom}(\mathcal{E}[\lambda], \mu_{p^\infty})$, see [29, Page 233];
(c) for almost all height one $(\lambda) \in \mathrm{Spec}(\Lambda)$, the corank relations still hold. For example, $S_{\mathcal{E}[\lambda]}(F)$ is a cotorsion module over (Λ/λ); see [29, Page 238].

Combining (a)–(c) with our local conditions, we know the method for the proof of Proposition 10.7 still applies for the Λ/λ-module $\mathcal{E}[\lambda]$ for almost all height one $(\lambda) \in \mathrm{Spec}(\Lambda)$. This completes the proof of the theorem. □

11. Appendix (II): Isogeny invariance of the product of algebraic p-adic L-function and complex period of an abelian variety

Let F be a number field, and let A and A' be two abelian varieties defined over F. Let p be a prime. We assume that $f : A \to A'$ is an isogeny defined over F with degree a power of p. For each prime w of F, we denote by $\kappa(w)$ (respectively, $\overline{\kappa(w)}$) the residue field at w (respectively, a separable algebraic closure of $\kappa(w)$). We assume that both A and A' have good ordinary reduction at all primes of F above p. Let $C = \ker f$ denote the kernel of f. For each prime v of F above p, we denote by $\widetilde{C}_v$ the reduction of C modulo v, which becomes a $\mathrm{Gal}(\overline{\kappa(v)}/\kappa(v))$-module. Finally, let $C_{1,v}$ denote the kernel of $C(F_v)$ modulo v.

Let F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension. We denote by $\mathrm{Sel}_A(F_{cyc})_p$ the Selmer group of A/F_{cyc} corresponding to the p^∞-division points of A. Let Λ be the Iwasawa algebra of $\mathrm{Gal}(F_{cyc}/F)$. We define

$X_p(A/F_{cyc})$ as the Pontryagin dual of $\mathrm{Sel}_A(F_{cyc})_p$. The characteristic ideal of $X_p(A/F_{cyc})$ is denoted by $C_{A/F}$. We assume that $C_{A/F} \neq 0$, which is equivalent to $X_p(A/F_{cyc})$ being a torsion Λ-module.

Theorem 11.1. *Assume that F is totally imaginary when $p = 2$. Then we have the following:*

$$\mathcal{C}_{A'/F} = p^{m(f)} \cdot \mathcal{C}_{A/F}$$

and

$$m(f) = \sum_{v|\infty} \mathrm{ord}_p(|C(F_v)|) - \sum_{v|p} [F_v : \mathbb{Q}_p] \cdot \mathrm{ord}_p(|C_{1,v}|).$$

Let us give a simple remark. For a compact, finitely generated torsion Λ-module M, we can express the characteristic ideal C_M of M as

$$C_M = p^{\mu(M)} \mathcal{R}_M$$

where $\mathcal{R}_M$ is not divisible by p and depends only on the structure of $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as a $\Lambda_{\mathbb{Q}_p}$-module. It is clear that the $\Lambda_{\mathbb{Q}_p}$-modules $X_p(A'/F_{cyc}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $X_p(A/F_{cyc}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ are isomorphic. Thus, we have

$$\mathcal{R}_{A/F} = \mathcal{R}_{A'/F}.$$

For simplicity, we denote $\mathcal{R}_{X_p(A/F_{cyc})}$ by $\mathcal{R}_{A/F}$. Furthermore, we define $\mu(M) = \mu(M^\wedge)$. Theorem 11.1 is equivalent to the following identity:

$$m(f) = \mu(\mathrm{Sel}_{A'}(F_{cyc})_p) - \mu(\mathrm{Sel}_A(F_{cyc})_p). \tag{11.1}$$

Proof. The proof is identical to [41, Théoreme on page 448]. Note that we assume F is totally imaginary, and the cohomology dimensions for the cohomology groups remain the same for odd p. The only distinction for $p = 2$ lies in the proof of [41, Lemme 3 on Page 451], where we utilize a fundamental result by Coates and Greenberg [12, Theorem 3.1] to obtain the same outcome as in [41, Lemme 3 on Page 451] for $p = 2$. □

Let A/F be an abelian variety with $\dim A = d$. We write $\mathcal{O}$ for $\mathcal{O}_F$.

Definition 11.2. *The periods $\Omega(A)$ of A is defined as follows: Let $\mathcal{A}/\mathcal{O}$ be the Néron model of A/F, and choose ω_A satisfies $\mathfrak{a}_{\omega_A} \cdot \omega_A = \wedge^d \Gamma(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}})^{\mathrm{inv}}$ for a fractional ideal $\mathfrak{a}_{\omega_A}$ of F, where $\Gamma(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}})^{\mathrm{inv}}$ denotes the global invariant differential on $\mathcal{A}/\mathcal{O}$, then*

$$\Omega(A) = \mathrm{N}(\mathfrak{a}_{\omega_A}) \mathrm{disc}(F/\mathbb{Q})^{-d/2} \int_{A(F \otimes_{\mathbb{Q}} \mathbb{R})} |\omega_A|_\infty.$$

Here, one can refer to [21, Lemma 18] *for the definition of $|\omega_A|_\infty$.*

Recall that $f : A \to A'$ is an isogeny of abelian varieties defined over F. Recall also that $C = \mathrm{Ker}(f)$. Assume that A has good ordinary reduction at all prime of F above p.

Theorem 11.3. *The quotient $\frac{\Omega(A')}{\Omega(A)}$ is a nonzero rational number and*

$$\mathrm{ord}_p\left(\Omega(A')/\Omega(A)\right) = -m(f).$$

From Theorems 11.1 and 11.3, we obtain the isogeny invariance of the product of algebraic p-adic L-function and complex period of an abelian variety.

To prove Theorem 11.3, let us recall some properties on differential on schemes. Let $t : G \to H$ be a morphism of S-schemes. There is an exact sequence of O_G-modules

$$t^* \Omega_{H/S} \to \Omega_{G/S} \to \Omega_{G/H} \to 0. \tag{11.2}$$

Let G, H be group schemes, and assume that t is a group homomorphism. Let $e_H : S \to H$ (resp. $e_G : S \to G$) be the zero section, $K := \mathrm{Ker}(t)$. Then we have $i : K = G \times_H S \to G$ satisfying

$$e_G = i \circ e_K, \text{ and } i^*(\Omega_{G/H}) \simeq \Omega_{K/S}.$$

We have

$$e_G^* \Omega_{G/H} \simeq e_K^* \Omega_{K/S}$$

Apply e_G^* to the exact sequence (11.2), note that pullback is right exact, we have an exact sequence

$$e_H^* \Omega_{H/S} \to e_G^* \Omega_{G/S} \to e_K^* \Omega_{K/S} \to 0. \tag{11.3}$$

Let $S = \mathrm{Spec}\mathcal{O}$, $f_{\mathcal{A}} : \mathcal{A} \to S, f_{\mathcal{A}'} : \mathcal{A}' \to S$ be Neron models of A/F and B/F over S, and $\mathfrak{F} : \mathcal{A} \to \mathcal{A}'$ be the morphism of group schemes over S extend $f : A/F \to A'/F$, $\mathcal{C} = \mathrm{Ker}\mathfrak{F}$. From the exact sequence (11.3), we have an exact sequence of O_S-module

$$e^*_{\mathcal{A}'}\Omega_{\mathcal{A}'/S} \to e^*_{\mathcal{A}}\Omega_{\mathcal{A}/S} \to e^*_{\mathcal{C}}\Omega_{\mathcal{C}/S} \to 0. \tag{11.4}$$

Let $I = \mathrm{Fitt}_{\mathcal{O}}(\Gamma(S, e^*_{\mathcal{C}}\Omega_{C/S})) \subset \mathcal{O}$ be the Fitting ideal. From the above exact sequence (11.4), we have

Lemma 11.4.

$$f^*(\wedge^d\Gamma(\mathcal{A}', \Omega_{\mathcal{A}'/S})^{\mathrm{inv}}) = I \cdot \wedge^d\Gamma(\mathcal{A}, \Omega_{\mathcal{A}/S})^{\mathrm{inv}}$$

in $\wedge^d\Gamma(\mathcal{A}, \Omega_{\mathcal{A}/S})^{\mathrm{inv}}$.

For an ideal $\mathfrak{b}$ in F, we write $\mathrm{N}(\mathfrak{b})$ for the norm of $\mathfrak{b}$.

Corollary 11.5. *We have*

$$\Omega(A)/\Omega(A') = \mathrm{N}(I)^{-1} \prod_{v|\infty} |C(F_v)|.$$

Proof. Choose $\omega_{A'}$ and $\mathfrak{a}_{\omega_{A'}}$ as in Definition 11.2. For an archimedean place v of F, we have

$$\int_{A'(F_v)} \omega_{A'} = |C(F_v)|^{-1} \int_{f_* A(F_v)} \omega_{A'} = |C(F_v)|^{-1} \int_{A(F_v)} f^*\omega_{A'}.$$

By Corollary 11.4, we can choose $(\omega_A = f^*\omega_{A'}, \mathfrak{a}_{\omega_A} = I^{-1}\mathfrak{a}_{\omega_{A'}})$ as in Definition 11.2. Then we have

$$\begin{aligned}
\Omega(A') &= \mathrm{N}(\mathfrak{a}_{\omega_{A'}})\mathrm{disc}(F/\mathbb{Q})^{-d/2} \int_{A'(F_\infty)} |\omega_{A'}|_\infty \\
&= \mathrm{N}(\mathfrak{a}_{\omega_{A'}})\mathrm{disc}(F/\mathbb{Q})^{-d/2} \prod_{v|\infty} |(C(F_v))|^{-1} \int_{A(F_\infty)} |\omega_A|_\infty \\
&= \mathrm{N}(I) \prod_{v|\infty} |(C(F_v))|^{-1} \mathrm{N}(\mathfrak{a}_{\omega_A})\mathrm{disc}(F/\mathbb{Q})^{-d/2} \int_{A(F_\infty)} |\omega_A|_\infty \\
&= \mathrm{N}(I) \cdot \prod_{v|\infty} |(C(F_v))|^{-1} \Omega(A),
\end{aligned}$$

which completes the proof. □

Let p be a prime. For any $\mathfrak{p}|p$ primes of F, let $S_{\mathfrak{p}} = \mathrm{Spec}\mathcal{O}_{\mathfrak{p}}$, $C_{\mathfrak{p}} := C \times_S S_{\mathfrak{p}}$. Assume that A has good reduction at $\mathfrak{p}$, then $C_{\mathfrak{p}}/S_{\mathfrak{p}}$ is a finite flat group scheme. It is well known that there is an exact sequence of group scheme

$$0 \to \mathcal{C}^0_{\mathfrak{p}} \to \mathcal{C}_{\mathfrak{p}} \to \mathcal{C}^{\text{ét}}_{\mathfrak{p}} \to 0,$$

where $\mathcal{C}^0_{\mathfrak{p}}$ is the connect component of $\mathcal{C}_{\mathfrak{p}}$, $\mathcal{C}^{\text{ét}}_{\mathfrak{p}}$ is etale over $S_{\mathfrak{p}}$. Similarly, we have an exact sequence

$$e^*_{\mathcal{C}^{\text{ét}}_{\mathfrak{p}}}\Omega_{\mathcal{C}^{\text{ét}}_{\mathfrak{p}}/S_{\mathfrak{p}}} \to e^*_{\mathcal{C}_{\mathfrak{p}}}\Omega_{\mathcal{C}_{\mathfrak{p}}/S_{\mathfrak{p}}} \to e^*_{\mathcal{C}^0_{\mathfrak{p}}}\Omega_{\mathcal{C}^0_{\mathfrak{p}}/S_{\mathfrak{p}}} \to 0.$$

However, since $\mathcal{C}^{\text{ét}}_{\mathfrak{p}}/S_{\mathfrak{p}}$ is etale, we have $\Omega_{\mathcal{C}^{\text{ét}}_{\mathfrak{p}}/S_{\mathfrak{p}}} = 0$, hence we have

Lemma 11.6. $e^*_{\mathcal{C}_{\mathfrak{p}}}\Omega_{\mathcal{C}_{\mathfrak{p}}/S_{\mathfrak{p}}} \simeq e^*_{\mathcal{C}^0_{\mathfrak{p}}}\Omega_{\mathcal{C}^0_{\mathfrak{p}}/S_{\mathfrak{p}}}$.

Lemma 11.7. *Assume that $\mathcal{A}$ is ordinary at $\mathfrak{p}$. Then*

$$|\Gamma(S_{\mathfrak{p}}, e^*_{\mathcal{C}^0_{\mathfrak{p}}}\Omega_{\mathcal{C}^0_{\mathfrak{p}}/S_{\mathfrak{p}}})| = |C^0_{1,\mathfrak{p}}|^{[F_{\mathfrak{p}}:\mathbb{Q}_p]}.$$

Proof. Since $\mathcal{A}$ is ordinary at $\mathfrak{p}$, $\mathcal{C}^0_{\mathfrak{p}}$ is of multiplicative type ([48, Page 169]). □

Now Theorem 11.3 comes from Corollary 11.5, and Lemmas 11.6, 11.7.

References

[1] Basmakov, M., *Cohomology of Abelian varieties over a number field.*, Uspehi Mat. Nauk **27** (1972), no. 6 (168), pp. 25–66.

[2] Bertrand, D., *Propriétés Arithmétiques de Fonctions Thêta à plusieurs variables*, Lect. Notes in Math., vol 1068, pp. 17-22. Berlin-Heidelberg-New York-Tokyo: Springer 1984.

[3] Burungale, A., Castella, F., Skinner, C. and Tian, Y., *p^∞-Selmer groups and rational points on CM elliptic curves.*, Ann. Math. Qué. 46 (2022), no. 2, 325–346

[4] Burungale, A. and Flach, M., *The conjecture of Birch and Swinnerton-Dyer for certain elliptic curves with complex multiplication*, Camb. J. Math. 12 (2024), no. 2, 357–415.

[5] Burungale, A. and Tian, Y., *p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin*, Invent. Math. 220 (2020), no. 1, 211–253.

[6] Burungale, A and Tian, Y., *The even parity Goldfeld conjecture: congruent number elliptic curves*, J. Number Theory 230 (2022), 161–195.

[7] Cai, L., Shu, J. and Tian, Y., *Explicit Gross-Zagier and Waldspurger formulae.* Algebra Number Theory 8 (2014), no. 10, 2523–2572.

[8] Choi. J., Kezuka. Y. and Li. Y., *Analogues of Iwasawa's $\mu = 0$ conjecture and weak Leopoldt theorem for certain non-cyclotomic $\mathbb{Z}_2$-extensions*, Asian J. Math. 23 (2019), no. 3, 383–400.

[9] Choi, J. and Coates, J., *Iwasawa theory of quadratic twists of $X_0(49)$.*, Acta Math. Sin. (Engl. Ser.) 34 (2018), no. 1, 19–28.

[10] Coates, J., *Infinite descent on elliptic curves with complex multiplication.*, Arithmetic and geometry, Vol. I, 107–137, Progr. Math., 35, Birkhauser Boston, Boston, MA, 1983.

[11] Coates, J., *Fragments of the GL_2 Iwasawa theory of elliptic curves without complex multiplication.*, Arithmetic theory of elliptic curves (Cetraro, 1997), 1-50, Lecture Notes in Math., 1716.

[12] Coates, J. and Greenberg, R., *Kummer theory for abelian varieties over local fields.*, Invent. Math. 124 (1996), no. 1-3, 129–174.

[13] Coates, J. and Li, Y., *Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication.*, Proc. Lond. Math. Soc. (3) 121 (2020), no. 6, 1531–1578.

[14] Coates, J., Li, Y., Tian, Y. and Zhai, S., *Quadratic twists of elliptic curves.*, Proc. Lond. Math. Soc. (3) 110 (2015), no. 2, 357–394.

[15] Coates, J. and Wiles, A., *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.

[16] Crişan. V. and Müller. K., *The vanishing of the μ-invariant for split prime $\mathbb{Z}_p$-extensions over imaginary quadratic fields*, Asian J. Math. 24 (2020), no. 2, 267–302.

[17] de Shalit. E., *The Iwasawa theory of elliptic curves with complex multiplication*, Perspect. Math. Vol. 3 (1987).

[18] Disegni, D., *The p-adic Gross-Zagier formula on Shimura curves.* , Compos. Math. 153 (2017), no. 10, 1987–2074.

[19] Disegni, D., *The p-adic Gross-Zagier formula on Shimura curves, II: nonsplit primes.* , J. Inst. Math. Jussieu 22 (2023), no. 5, 2199–2240.

[20] Dokchitser, T. and Dokchitser, V., *On the Birch-Swinnerton-Dyer quotients modulo squares.*, Ann. of Math. (2) 172 (2010), no. 1, 567–596.

[21] Flach, M. and Siebel, D., *Special values of the zeta function of an arithmetic surface.*, J. Inst. Math. Jussieu 21 (2022), no. 6, 2043–2091.

[22] Görtz, U. and Wedhorn, T., *Algebraic geometry II: cohomology of schemes. With examples and exercises*

[23] Gonzalez-Aviles, C., *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. 349 (1997), no. 10, 4181–4200.

[24] Greenberg, R., *Iwasawa theory for p-adic representations*, Algebraic number theory, 97–137, Adv. Stud. Pure Math, 17, Academic Press, Boston, MA, 1989.

[25] Greenberg, R., *Iwasawa theory and p-adic deformations of motives*, Motives (Seattle, WA, 1991), 193-223, Proc. Sympos. Pure Math., 55, Part 2, Amer. Math. Soc., Providence, RI, 1994.

[26] Greenberg, R., *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.

[27] Greenberg, R., *On the structure of certain Galois cohomology groups*, Doc. Math. 2006, Extra Vol., 335–391

[28] Greenberg, R., *Surjectivity of the global-to-local map defining a Selmer group*, Kyoto J. Math. 50 (2010), no. 4, 853–888

[29] Greenberg, R., *On the structure of Selmer groups*, Elliptic curves, modular forms and Iwasawa theory, 225-252, Springer Proc. Math. Stat, 188, Springer, Cham, 2016.

[30] Gross, B., *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, Number theory related to Fermat's last theorem (Cambridge, Mass., 1981), pp. 219–236, Progr. Math., 26, Birkhauser, Boston, 1982.

[31] Gross, B. and Zagier, D., *Heegner points and derivatives of L-series.*, Invent. Math. 84 (1986), no. 2, 225–320.

[32] Johnson-Leung, J. and Kings, G., *On the equivariant main conjecture for imaginary quadratic fields.* , J. Reine Angew. Math. 653 (2011), 75–114.

[33] Kobayashi, S., *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes.* Invent. Math. 191 (2013), no. 3, 527 -629.

[34] Li, Y., Tian, Y., Yan, X., Zhu, X., *On the Birch-Swinnerton-Dyer Conjecture for Elliptic Curves with Complex Multiplication and Analytic Rank One*, In preparation.

[35] Li, Y., *On the μ-invariant of two-variable 2-adic L-functions*, To appear in Glasgow Mathematical Journal.

[36] Mazur, B., *Rational points of abelian varieties with values in towers of number fields.*, Invent. Math. 18 (1972), 183–266.

[37] Milne, J., *On the arithmetic of abelian varieties.*, Invent. Math. 17 (1972), 177–190.

[38] Oukhaba. H. and Viguié. S., *On the μ-invariant of Katz p-adic L-functions attached to imaginary quadratic fields*, Forum Math. 28 (2016), no. 3, 507–525.
[39] Perrin-Riou, B., *Arithmetique des courbes elliptiques et theorie d'Iwasawa*, Memoires Soc. Math. de France, fascicule 4, 112 (1984).
[40] Perrin-Riou, B., *Points de Heegner et dérivées de fonctions L p-adiques.*, Invent. Math. 89 (1987), no. 3, 455–510.
[41] Perrin-Riou, B., *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner.*, Invent. Math. 89 (1987), Bull. Soc. Math. France 115 (1987), no. 4, 399–456.
[42] Perrin-Riou, B., *Théorie d'Iwasawa et hauteurs p-adiques.*, Invent. Math. 109 (1992), no. 1, 137–185.
[43] Rubin, K., *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication.*, Invent. Math. 89 (1987), no. 3, 527–559.
[44] Rubin, K., *On the main conjecture of Iwasawa theory for imaginary quadratic fields.* , Invent. Math. 93 (1988), no. 3, 701–713.
[45] Rubin, K., *The ″main conjectures″ of Iwasawa theory for imaginary quadratic fields.*, Invent. Math. 103 (1991), no. 1, 25–68.
[46] Schneider, P., *Iwasawa L -functions of varieties over algebraic number fields. A first approach*, Invent. Math. 71 (1983), no. 2, 251–293.
[47] Schneider, P., *p-adic height pairings. II.*, Invent. Math. 79 (1985), no. 2, 329–374.
[48] Schneider, P., *The μ-invariant of isogenies.*, J. Indian Math. Soc. (N.S.) 52 (1987), 159–170 (1988).
[49] Tian, Y., *Congruent Numbers and Heegner Points*, Camb. J. Math. 2 (2014), no. 1, 117–161.
[50] Tian, Y., *The congruent number problem and elliptic curves*, ICM—International Congress of Mathematicians. Vol. 3. Sections 1-4, 1990–2010, EMS Press, Berlin.
[51] Tian, Y., Yuan, X and Zhang, S., *Genus Periods, Genus Points and Congruent Number Problem*, Asian J. Math. 21 (2017), no. 4, 721–773.
[52] Yager, R., *On two variable p-adic L-functions.*, Ann. of Math. (2) 115 (1982), no. 2, 411–449.
[53] Yuan, X., Zhang, S. and Zhang, W., *The Gross-Zagier Formula on Shimura Curves*, Annals of Mathematics Studies Number 184, 2013.

Yongxiong Li: Beijing Institute of Mathematical Sciences and Applications, No. 544, Hefangkou Village Huaibei Town, Huairou District Beijing 101408.
Email address: yongxiongli@gmail.com

Ye Tian: Academy of Mathematics and Systems Science, Morningside center of Mathematics, Chinese Academy of Sciences, Beijing 100190.
Email address: ytian@math.ac.cn

Xiaojun Yan: Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190.
Email address: xjyan95@amss.ac.cn

Xiuwu Zhu: Beijing Institute of Mathematical Sciences and Applications, No. 544, Hefangkou Village Huaibei Town, Huairou District Beijing 101408.
Email address: xwzhu@bimsa.cn