NON-VANISHING OF CENTRAL L-VALUES OF THE GROSS FAMILY OF ELLIPTIC CURVES

YUKAKO KEZUKA AND YONG-XIONG LI

Abstract. We prove non-vanishing theorems for the central values of L-series of quadratic twists of the Gross elliptic curve with complex multiplication by the imaginary quadratic field $\mathbb{Q}(\sqrt{-q})$, where q is any prime congruent to 7 modulo 8. This completes the non-vanishing theorems proven by Coates and the second author in which the primes q were taken to be congruent to 7 modulo 16. From this, we obtain the finiteness of the Mordell–Weil group and the Tate–Shafarevich group for these curves. For a prime $\mathfrak{P}$ lying above the prime 2, we also prove a converse theorem in the rank 0 case and the $\mathfrak{P}$-part of the Birch–Swinnerton-Dyer conjecture for the higher-dimensional abelian varieties obtained by restriction of scalars.

1. Introduction

We let q be a prime number congruent to 7 modulo 8. We define K to be the imaginary quadratic field $\mathbb{Q}(\sqrt{-q})$, viewed as a subfield of $\mathbb{C}$, with ring of integers $\mathcal{O}_K$ and class number h. Let $H = K(j(\mathcal{O}_K))$ be the Hilbert class field of K, where $j(\mathcal{O}_K)$ denotes the j-invariant of the complex lattice $\mathcal{O}_K$. The prime 2 then splits in K, say $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$, and since $q \equiv 3 \bmod 4$ is a prime, h is odd by genus theory due to Gauss.

Amongst the elliptic curves with complex multiplication by K, Gross has introduced in [10] an elliptic curve A with particularly nice properties (in fact, the Gross curve can be defined for any prime $q \equiv 3 \bmod 4$). The Gross elliptic curve A is the unique elliptic curve which is defined over $\mathbb{Q}(j(\mathcal{O}_K))$ with complex multiplication by $\mathcal{O}_K$, minimal discriminant $(-q^3)$ (so that A has bad reduction only at the prime q), and which is a $\mathbb{Q}$-curve, in the sense that it is H-isogeneous to all its conjugates A^σ, where σ is any element of the automorphism group of H. In addition, Gross has shown that A has a global minimal model over $\mathcal{O}_H$, and we write Ω_∞ for the corresponding complex period.

The study of the arithmetic of A has attracted many mathematicians since it was developed in [10]. In particular, Gross has shown in [10] by a 2-descent argument that A has Mordell–Weil rank zero over H. Motivated by this, Rohrlich showed in [19] that the L-function $L(A/H, s)$ of A over H does not vanish at $s = 1$. Following this, Rodriguez Villegas gave another proof in [18] for the fact that $L(A/H, 1) \neq 0$ using a factorisation formula, parallel to the work of Waldspurger.

Let $A^{(D)}$ be a quadratic twist of A by the extension $H(\sqrt{D})/H$ for a square-free integer D. We note that this is a non-trivial extension since the class number h is odd. The arithmetic of $A^{(D)}$ has also received a lot of attention. For example, using theta liftings and analytic methods, Yang [22, 23] showed that $L(A^{(D)}/H, 1) \neq 0$ when D is small compared to q, roughly, $D < q^{\frac{1}{4}}$.

We now introduce some notation to state our main theorem. Let $\mathfrak{R}$ denote the set of all square-free positive integers R of the form $R = r_1 \cdots r_k$, where $k \geq 0$

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

The first author is supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 101026826.

($k = 0$ means $R = 1$) and $r_1, \ldots, r_k$ are distinct primes such that (i) $r_i \equiv 1 \bmod 4$, and (ii) r_i is inert in K, for $i = 1, \ldots, k$. For $R \in \mathfrak{R}$ with $R \neq 1$, we write $A^{(R)}$ for the twist of A by the quadratic extension $H(\sqrt{R})/H$. We write $L(A^{(R)}/H, s)$ for the complex L-series of $A^{(R)}/H$. By Deuring's theorem, $L(A^{(R)}/H, s)$ is a product of Hecke L-functions coming from the Hecke character ψ_R associated to $A^{(R)}/H$. This can in turn be written as a product of Hecke characters associated to $\mathrm{Res}_{H/K} A^{(R)} = B^{(R)}$ obtained from $A^{(R)}$ by restriction of scalars from H to K. In view of the relations discussed in Section 2, it suffices to show $L(\overline{\phi}_R, 1) \neq 0$ for a Hecke character of $B^{(R)}$ to conclude $L(A^{(R)}/H, 1) \neq 0$. We write T for the CM field of B, and we write $\mathfrak{P}$ for the special prime of T lying above 2 whose existence is given in Proposition 2.1, where without loss of generality we assume that it also lies above the prime $\mathfrak{p}$ of K. We shall prove the following result.

Theorem 1.1. *For any $R = r_1 \cdots r_k \in \mathfrak{R}$. Then $\frac{L(\overline{\phi}_R, 1)\sqrt{R}}{\Omega_\infty} \in TH$, and for any prime $\mathcal{P}$ of TH lying above $\mathfrak{P}$, we have*

$$\mathrm{ord}_{\mathcal{P}} \left(\frac{L(\overline{\phi}_R, 1)\sqrt{R}}{\Omega_\infty} \right) = k - 1.$$

In particular, $L(A^{(R)}/H, 1) \neq 0$. Moreover, the Mordell–Weil group $A^{(R)}(H)$ and and the Tate–Shafarevich group $Ш(A^{(R)}/H)$ of $A^{(R)}$ are finite.

The implication that $L(A^{(R)}/H, 1) \neq 0$, then $A^{(R)}(H)$ is finite, is a theorem of Coates–Wiles [8] and its extensions due to Arthaud [1] and Rubin [20]. In the case of the congruent number curves, such an implication was used by Tunnell [21] to provide a method of verifying a given positive integer is not congruent, and the 2-adic valuation of the algebraic part of their L-values was analysed by Zhao [24, 25].

The implication that $L(A^{(R)}/H, 1) \neq 0$, then both $A^{(R)}(H)$ and $Ш(A^{(R)}/H)$ are finite, follows either from an Euler system argument due to Kolyvagin [16] and Gross–Zagier [13], or its extension due to Kato [14] for twists of eigen cusp forms f. We recall that A is a $\mathbb{Q}$-curve and its restriction of scalars is modular, and the relation (2.2) satisfied by the Hecke characters can be used to show that the curves we deal with appear as quotients of the Jacobian $J_0(N)$ (see [3]). We also note that in the case f has complex multiplication, the proof of Kato is based on the work of Rubin on the main conjecture for imaginary quadratic field [20].

Letting $R = 1$ in Theorem 1.1, we obtain $L(A/H, 1) \neq 0$, reproving the result of Rohrlich in [19]. The key difference is that our result gives the exact valuation at the primes above $\mathfrak{P}$ of the L-value for the base curve, *which provides the crucial initial step in the induction on which the proof of Theorem 1.1 relies.*

We remark that when $q \equiv 7 \bmod 16$, the above result was proven by John Coates and the second author in [6]. The new part of the theorem thus concerns the case when $q \equiv 15 \bmod 16$. We stress that this case could not be covered in [6], and this is due to the fact that the a corresponding Iwasawa module $X(F_\infty)$ introduced in Section 5 is trivial in the case $q \equiv 7 \bmod 16$, but it was proven to be always non-trivial in the case $q \equiv 15 \bmod 16$ [17]. It is thus essential to obtain a better understanding of this Iwasawa module.

The module $X(F_\infty)$ is the Pontryagin dual of a certain Selmer group (see Theorem 5.1). A key method used to prove Theorem 1.1 is thus a combination of various descents at finite levels and an infinite descent in the setting of Iwasawa theory.

In proving Theorem 1.1, we will first study the abelian variety $B = \mathrm{Res}_{H/K}(A)$ over K. Another key ingredient is the Iwasawa main conjecture at the special

prime $\mathfrak{P}$, following [6]. Indeed, the field F_∞ above is given by $K(B_{\mathfrak{P}^\infty})$, obtained by adjoining to K all $\mathfrak{P}$-power division points on B. In order to treat the case $p = 2$, we also need to show that $X(F_\infty)$ is a finitely generated $\mathbb{Z}_2$-module. This will follow from our earlier work [4], in which we show that the Iwasawa module $X(H(A_{\mathfrak{p}^\infty}))$ corresponding to the field $H(A_{\mathfrak{p}^\infty})$ is a finitely generated $\mathbb{Z}_2$-module. Combined with the descent arguments, this gives us a non-vanishing result for the base curve A and a rank zero $\mathfrak{P}$-converse theorem for B. Furthermore, we prove the $\mathfrak{P}$-part of the Birch–Swinnerton-Dyer conjecture for B over K, a refinement due to Buhler and Gross [3]. Using this as the base case, we apply an induction argument on the number of prime divisors of $R \in \mathfrak{R}$, a generalisation of Zhao's method to abelian varieties, to extend the non-vanishing result to the twists $A^{(R)}$ as in Theorem 1.1. We stress that knowing the non-vanishing result for the base curve A is not sufficient for obtaining the non-vanishing result for the twisted curve $A^{(R)}$, and we crucially use the exact $\mathfrak{P}$-adic valuation for the base curve in our argument.

In a subsequent paper [15], we will study the exact Birch–Swinnerton-Dyer formula for $A^{(R)}$ by proving the refined Birch–Swinnerton-Dyer conjecture at all primes of the CM field lying above 2.

We remark that, as a consequence of Theorem 1.1, we obtain the following density result. Let $D \geq 1$ denote a fundamental discriminant, and let

$$N(X) = \#\{D < X : L(A^{(D)}/H, 1) \neq 0\}.$$

Then we have

Corollary 1.2.

$$N(X) \gg \frac{X}{\log^{\frac{3}{4}} X}.$$

This paper is structured as follows. In Section 2, we introduce some notation and preliminary results. We give a 2-descent argument in Section 3 showing that B has no first descent at the special prime $\mathfrak{P}$ of T lying above 2. In Sections 4 and 5, we prove a rank zero converse theorem for B at the prime $\mathfrak{P}$, and prove the $\mathfrak{P}$-part of the Birch–Swinnerton-Dyer conjecture. This uses Iwasawa theory for the prime $\mathfrak{P}$ and the descent results, giving the exact $\mathfrak{P}$-adic valuation of the algebraic part of the Hecke L-value associated to B/K at $s = 1$. In Section 6, we apply a generalisation of Zhao's induction method to obtain the non-vanishing result for the twisted curves, concluding the proof of Theorem 1.1. The proof of Corollary 1.2 can be found at the end of Section 6.

Acknowledgement This is one of the two papers we wish to dedicate to John Coates. John encouraged us to give a full detailed proof of the full Birch–Swinnerton-Dyer conjecture for these elliptic curves with complex multiplication based on classical approaches which he, Wiles and Rubin developed. He believed in the power of small primes in number theory, and he inspired us to pursue it. With this paper, we wish to tell him that what he predicted is indeed true.

2. Preliminaries

Since the minimal discriminant ideal $(-q^3)$ of A is a principal ideal, it raises the question as to whether there exists a global minimal Weierstrass equation for A over the ring of integers $\mathcal{O}_H$ of H. Gross has proven that this is indeed the case [11], and we fix one such equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

with $a_i \in \mathcal{O}_H$. We let B/K be the abelian variety which is the restriction of scalars from H to K of the Gross curve A/H. For each $R \in \mathfrak{R}$, we write $B^{(R)}$ for the twist

of B by the quadratic extension $K(\sqrt{R})/K$, and $A^{(R)}$ for the twist of A by the quadratic extension $H(\sqrt{R})/H$. It is easily seen that $B^{(R)}$ is in fact the restriction of scalars from H to K of $A^{(R)}$.

We write

$$\mathscr{T} = \mathrm{End}_K(B^{(R)}) = \mathrm{End}_K(B) \quad \text{and} \quad T = \mathscr{T} \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then T is a CM field of degree h over K, where h denotes the class number of K. Let $\alpha : T \hookrightarrow \mathbb{C}$ be an embedding of T into $\mathbb{C}$ which extends our embedding of K into $\mathbb{C}$. There are h such choices of α. We write ψ for the Hecke character of A/H and $\phi = \phi^\alpha$ for the Hecke character of B/K relative to α. We then have $\psi = \phi \circ N_{H/K}$, where $N_{H/K}$ denotes the norm map from H to K. Since $(R, q) = 1$, the Hecke character ϕ_R of $B^{(R)}/K$ is then given by $\phi_R = \phi\chi_R$, where χ_R denotes the abelian character of K defining the quadratic extension $K(\sqrt{R})/K$. Moreover, since H/K is unramified, the Hecke character ψ_R of $A^{(R)}/H$ is equal to

$$\psi_R = \phi_R \circ N_{H/K}. \tag{2.2}$$

Note that the Hecke characters ϕ and ϕ_R take values in T. In what follows, we shall write $\overline{\psi}$ and $\overline{\phi}$ for the complex conjugate characters of ψ and ϕ, respectively. Since A is a $\mathbb{Q}$-curve, we have $L(A/H, s) = L(\overline{\psi}, s)^2$ by a theorem of Deuring, and we have the relation between L-series [10, Section 18]

$$L(\overline{\psi}, s) = \prod_{\alpha \in \mathrm{Hom}_K(T, \mathbb{C})} L(\overline{\phi}^\alpha, s), \tag{2.3}$$

where the product runs over the h distinct embeddings of T lying above our fixed embedding of K. We will first show the non-vanishing of $L(\overline{\phi}, 1)$. Since the same arguments show that $L(\overline{\phi}^\alpha, 1) \neq 0$ for any α, we may conclude that $L(A/H, 1) \neq 0$. Similarly, in order to show $L(A^{(R)}/H, 1) \neq 0$, it is sufficient to show $L(\overline{\phi}_R, 1) \neq 0$.

We now choose a prime of T lying above 2, which is well suited for our purpose. Note that the index of $\mathscr{T}$ in the maximal order of T is prime to 2 (see Section 13 of [10]). As $q \equiv 7 \bmod 8$, the prime 2 splits in K into two distinct primes, which we will denote by $\mathfrak{p}$ and $\mathfrak{p}^*$. The following lemma (see [3] or Lemma 2.1 in [6]) gives the existence of a degree one prime $\mathfrak{P}$ of T above $\mathfrak{p}$, which is the special prime mentioned in the introduction and which will play a fundamental role throughout this paper.

Proposition 2.1. *There exists a unique, unramified degree one prime $\mathfrak{P}$ of T lying above $\mathfrak{p}$.*

Of course, since the index of $\mathscr{T}$ in the ring of integers of T is prime to 2, $\mathfrak{P} \cap \mathscr{T}$ will be a degree one prime ideal of $\mathscr{T}$, which for simplicity we shall again denote by $\mathfrak{P}$. We will also use the degree one prime $\mathfrak{P}^*$ of T lying above $\mathfrak{p}^*$, which is obtained by applying the complex conjugation to $\mathfrak{P}$.

3. The first 2-descent on B over K

Iwasawa theory of B for the prime $\mathfrak{P}$ shall deal with the extension F_∞/K, where $F_\infty = K(B_{\mathfrak{P}^\infty})$. Its Galois group is of the form $\Gamma \times \Delta$ where $\Gamma \simeq \mathbb{Z}_2$ and $\Delta \simeq \mathbb{Z}/2\mathbb{Z}$. The main conjecture of Iwasawa theory relates the corresponding Iwasawa module $X(F_\infty)$ to a $\mathfrak{P}$-adic L-function, which interpolates the Hecke L-value $L(\overline{\phi}, 1)$ (see Section 5). In the case $q \equiv 7 \bmod 16$ treated in [6], it could be shown that $X(F_\infty) = 0$. In the new case $q \equiv 15 \bmod 16$ treated here, we know that $X(F_\infty)$ is non-trivial [17]. We will get around this by studying its Pontryagin dual $\mathrm{Sel}_{\mathfrak{P}^\infty}(B/F_\infty)$. In particular, we will show that its Γ-invariant part $\mathrm{Sel}_{\mathfrak{P}^\infty}(B/F_\infty)^\Gamma$

is finite and compute the $\mathfrak{P}$-adic valuation of its order to relate it to the $\mathfrak{P}$-adic valuation of the Hecke L-value. This requires carrying out various descents, both at finite and inifinite levels, and proving exact relations between them. In this section, we will carry out a 2-descent on B over K.

We let $G = \mathrm{Gal}(H/K)$, which is a group of order h, an odd number by our choice of q. In this section, we will use a G-invariant 2-descent result on A/H due to Gross (see the proof of Proposition 3.1) to prove a 2-descent result on B/K. Recall that $\mathscr{T}$ is the ring of K-endomorphisms of the abelian variety B. For each integer $n \geq 1$, let $B_{\mathfrak{P}^n}$ be the Galois module of $\mathfrak{P}^n$-division points on B. We define the Selmer group $\mathrm{Sel}_{\mathfrak{P}^n}(B/K)$ by the exact sequence

$$\mathrm{Sel}_{\mathfrak{P}^n}(B/K) = \mathrm{Ker}\left(H^1(K, B_{\mathfrak{P}^n}) \to \prod_v H^1(K_v, B)_{\mathfrak{P}^n} \right),$$

where v runs over all finite places of K, and K_v is the completion at v of K.

Recall that $\mathfrak{P}$ lies above $\mathfrak{p}$, where $\mathfrak{p}$ is one of the primes of K lying above 2. Let $A_{\mathfrak{p}}$ be the Galois module of $\mathfrak{p}$-division points on A. We similarly define the Selmer group $\mathrm{Sel}_{\mathfrak{p}}(A/H)$ by the exact sequence

$$\mathrm{Sel}_{\mathfrak{p}}(A/H) = \mathrm{Ker}\left(H^1(H, A_{\mathfrak{p}}) \to \prod_w H^1(H_w, A)_{\mathfrak{p}} \right),$$

where w runs over all finite places of H, and H_w is the completion at w of H. This Selmer group is also a G-module, and we denote by $\mathrm{Sel}_{\mathfrak{p}}(A/H)^G$ the subgroup of $\mathrm{Sel}_{\mathfrak{p}}(A/H)$ consisting of elements fixed by G.

Proposition 3.1. *We have*

$$\mathrm{Sel}_{\mathfrak{p}}(A/H)^G \simeq \mathbb{Z}/2\mathbb{Z}.$$

Proof. Let $\mathrm{Sel}_2(A/H)$ be the 2-Selmer group of A/H using the Galois module A_2 of 2-torsion points on A defined in a similar way as above. This is also a G-module, and we denote by $\mathrm{Sel}_2(A/H)^G$ its Galois invariant subgroup. The G-invariant Selmer group is much easier to compute than the full Selmer group, and Gross shows in [10] that

$$\mathrm{Sel}_2(A/H)^G \simeq \mathcal{O}_K/2\mathcal{O}_K. \tag{3.1}$$

Note that $A_2 = A_{\mathfrak{p}} \times A_{\mathfrak{p}^*}$ as $\mathrm{Gal}(\overline{K}/H)$-modules, where $A_{\mathfrak{p}^*}$ the Galois module of $\mathfrak{p}^*$-torsion points on A, and A_2 is contained in $A(H)$. Thus, by the definitions of the Selmer groups, we have $\mathrm{Sel}_2(A/H) = \mathrm{Sel}_{\mathfrak{p}}(A/H) \times \mathrm{Sel}_{\mathfrak{p}^*}(A/H)$, where $\mathrm{Sel}_{\mathfrak{p}^*}(A/H)$ is defined in a similar way to $\mathrm{Sel}_{\mathfrak{p}}(A/H)$ given above. Since both $\mathrm{Sel}_{\mathfrak{p}}(A)$ and $\mathrm{Sel}_{\mathfrak{p}^*}(A)$ are G-modules and G is of odd order, we have

$$\mathrm{Sel}_2(A/H)^G = \mathrm{Sel}_{\mathfrak{p}}(A/H)^G \times \mathrm{Sel}_{\mathfrak{p}^*}(A/H)^G.$$

Note that $\mathrm{Sel}_{\mathfrak{p}}(A/H)^G$ is an $\mathcal{O}_{K_{\mathfrak{p}}}$-module where $\mathcal{O}_{K_{\mathfrak{p}}}$ is the ring of integers of $K_{\mathfrak{p}}$, and $\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}} \simeq \mathbb{Z}/2\mathbb{Z}$, The proposition follows on taking the tensor product on both sides of (3.1) with $\mathcal{O}_{K_{\mathfrak{p}}}$. □

Next, we calculate the $\mathfrak{P}$-Selmer group $\mathrm{Sel}_{\mathfrak{P}}(B/K)$ using standard exact sequences of Galois cohomology. We will also use the following isomorphism of Galois modules.

Lemma 3.2. *We have an isomorphism*

$$B_{\mathfrak{P}} \simeq A_{\mathfrak{p}}.$$

of $\mathrm{Gal}(\overline{K}/H)$*-modules.*

Proof. Since $B_{\mathfrak{P}}$ is a $\mathrm{Gal}(\overline{K}/K)$-module, we can naturally view it as a $\mathrm{Gal}(\overline{K}/H)$-module. Both modules are isomorphic to $\mathbb{Z}/2\mathbb{Z}$, and the action of $\mathrm{Gal}(\overline{K}/H)$ on both modules is trivial, so the result follows. □

Proposition 3.3. *We have*

$$\mathrm{Sel}_{\mathfrak{P}}(B/K) \simeq \mathbb{Z}/2\mathbb{Z}.$$

In particular, $B(K)$ is finite since $B_{\mathfrak{P}}(K)$ is non-trivial, and

$$Ш(B/K)(\mathfrak{P}) = 0.$$

Here, we denote by $Ш(B/K)(\mathfrak{P})$ the $\mathfrak{P}$-primary part of the Tate–Shafarevich group of B/K.

Proof. The proof crucially depends on the 2-descent result in Proposition 3.1. We recall the following definitions for $\mathrm{Sel}_{\mathfrak{P}}(B/K)$ and $\mathrm{Sel}_{\mathfrak{p}}(A/H)$ using the exact sequences

$$0 \to \mathrm{Sel}_{\mathfrak{P}}(B/K) \to H^1(K, B_{\mathfrak{P}}) \to \prod_v \frac{H^1(K_v, B_{\mathfrak{P}})}{\mathrm{Im}\kappa_v(B)}$$

and

$$0 \to \mathrm{Sel}_{\mathfrak{p}}(A/H) \to H^1(H, A_{\mathfrak{p}}) \to \prod_w \frac{H^1(H_w, A_{\mathfrak{p}})}{\mathrm{Im}\kappa_w(A)},$$

where, $\kappa_v(B)$ (resp. $\kappa_w(A)$) denotes the local Kummer map of B (resp. A) at v (resp. w). Recall that $G = \mathrm{Gal}(H/K)$. By taking the G-invariant part of the second exact sequence, we obtain the exact sequence

$$0 \to \mathrm{Sel}_{\mathfrak{p}}(A/H)^G \to H^1(H, A_{\mathfrak{p}})^G \to \left(\prod_w \frac{H^1(H_w, A_{\mathfrak{p}})}{\mathrm{Im}\kappa_w(A)}\right)^G.$$

Using Lemma 3.2 and noting that $\#(G)$ is odd, we see that the restriction map

$$i : H^1(K, B_{\mathfrak{P}}) \to H^1(H, A_{\mathfrak{p}})^G \tag{3.2}$$

is an isomorphism. Furthermore, locally at each prime v of K we can identify G with the group $\mathrm{Gal}((K_v \otimes_K H)/K_v)$. Thus, the restriction map also gives the isomorphism

$$j_0 : H^1(K_v, B_{\mathfrak{P}}) \to \left(\prod_{w|v} H^1(H_w, A_{\mathfrak{p}})\right)^G. \tag{3.3}$$

Now, since B is the restriction of scalars of A from H to K (or from [10]), we have

$$B(K_v) = A(K_v \otimes_K H) = \prod_{w|v} A(H_w).$$

Since $B(K_v)$ is fixed by $G = \mathrm{Gal}((K_v \otimes_K H)/K_v)$, given any point $(P_w) \in \prod_w A(H_w)$ and any $\sigma \in G$, we may identify (P_w) with $(P^{\sigma}_{\sigma w})$.

Note that we have $\mathcal{O}_{T_{\mathfrak{P}}}/\mathfrak{P} = \mathcal{O}_K/\mathfrak{p} = \mathbb{Z}/2\mathbb{Z}$, and thus

$$\left(\prod_{w|v} A(H_w)\right) \otimes (\mathcal{O}_K/\mathfrak{p}) = B(K_v) \otimes (\mathcal{O}_{T_{\mathfrak{P}}}/\mathfrak{P}).$$

Consider the maps

$$B(K_v) \otimes (\mathcal{O}_{T_{\mathfrak{P}}}/\mathfrak{P}) \overset{\kappa_v(B)}{\hookrightarrow} H^1(K_v, B_{\mathfrak{P}}) \xrightarrow{\simeq} \left(\prod_{w|v} H^1(H_w, A_{\mathfrak{p}})\right)^G,$$

where the last isomorphism is given by j_0 in (3.3). From our remark on the Galois action of G, we see that the composition of these maps coincides with $\prod_{w|v}\kappa_w(A)$. It then follows from the definition of the Selmer groups and the isomorphisms (3.2) and (3.3) that i sends $\mathrm{Sel}_{\mathfrak{P}}(B/K)$ isomorphically to $\mathrm{Sel}_{\mathfrak{p}}(A/H)^G$. The result now follows from Proposition 3.1. □

We define

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B/K) = \varinjlim \mathrm{Sel}_{\mathfrak{P}^n}(B/K)$$

to be the direct limit of the Selmer groups $\mathrm{Sel}_{\mathfrak{P}^n}(B/K)$ with respect to n. We then immediately obtain

Corollary 3.4. *We have*

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B/K) = 0.$$

We end this section with the following remark which will be used in Sections 4 and 5.

Remark 3.5. By replacing $\mathfrak{P}$ with $\mathfrak{P}^*$ (the degree one prime of T lying above $\mathfrak{p}^*$) above, we similarly obtain that $Ш(B/K)(\mathfrak{P}^*)$ and $\mathrm{Sel}_{\mathfrak{P}^{*\infty}}(B/K)$ are trivial. Thus, both $B(K)$ and $Ш(B/K)(\mathfrak{P}\mathfrak{P}^*)$ are finite.

4. Descent theory on B over the fields K and $F = K(B_{\mathfrak{P}^2})$

The elliptic curve A only has additive reduction at each place w of H lying above $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$. For each such w, we write $A_0(H_w)$ for the subgroup of $A(H_w)$ consisting of points with non-singular reduction modulo w, and put $\mathfrak{C}_w = A(H_w)/A_0(H_w)$. Of course, $\mathfrak{C}_w$ is a $\mathcal{O}_K$-module, and by the theory of the Néron model, the order of $\mathfrak{C}_w$ is at most 4.

Lemma 4.1. *Let w be a place of H lying above $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$. Then $\mathfrak{C}_w \simeq \mathcal{O}_K/2\mathcal{O}_K$ as a $\mathcal{O}_K$-module. In particular, $\mathfrak{C}_w$ is of order 4.*

Proof. Since w does not divide 2 and A has additive reduction at w, it follows that multiplication by 2 must be an automorphism of $A_0(H_w)$, whence the kernel of multiplication by 2 on $\mathfrak{C}_w$ must be isomorphic to $A(H_w)_2 = \mathcal{O}_K/2\mathcal{O}_K$, as required. □

Since $B = \mathrm{Res}_{H/K}A$, we know that

$$B(K_{\mathfrak{q}}) = \prod_{w|\mathfrak{q}} A(H_w). \tag{4.1}$$

We define

$$B_0(K_{\mathfrak{q}}) = \prod_{w|\mathfrak{q}} A_0(H_w), \tag{4.2}$$

where the two products are taken over all places w of H above $\mathfrak{q}$, and we set $C_{\mathfrak{q}} = \frac{B(K_{\mathfrak{q}})}{B_0(K_{\mathfrak{q}})}$.

Lemma 4.2. *We have*

(1) $C_{\mathfrak{q}} = \prod_{w|\mathfrak{q}} \mathfrak{C}_w$, and
(2) $C_{\mathfrak{q}}$ is a module over $\mathcal{O}_T \otimes_{\mathbb{Z}} \mathbb{Z}_2$, and $(C_{\mathfrak{q}})(\mathfrak{P}^*) \simeq \mathcal{O}_{T_{\mathfrak{P}^*}}/\mathfrak{P}^*\mathcal{O}_{T_{\mathfrak{P}^*}}$.

Proof. The first assertion follows from the restriction of scalar properties for Néron models. For the details, see Proposition 4.5 of [12]. The second assertion follows from the fact that $[T : K] = [H : K] = h$, combined with Lemma 4.1 and the structure theory for modules over principal ideal domains. □

It is known that B is a self dual abelian variety (see 4 lines below (3.1) in [12]). Thus, we have the following lemma.

Lemma 4.3. *We have*

(i) $H^1(K_\mathfrak{q}, B)(\mathfrak{P})$ *is finite of order* 2*, and*

(ii) $H^1(K_\mathfrak{p}, B)(\mathfrak{P})$ *is finite of order equal to* $|\ (1-\phi(\mathfrak{p})/2)\ |_\mathfrak{P}^{-1}$.

Here, $|\cdot|_\mathfrak{P}$ *is the multiplicative valuation on* $T_\mathfrak{P}$*, normalised so that* $|2|_\mathfrak{P} = 2^{-1}$.

Proof. Recall that $\mathscr{T}$ is the ring of K-endomorphisms of the abelian variety B. We fix any non-zero element π of $\mathscr{T}$ such that the ideal factorisation of π in the ring of integers of $\mathscr{T}$ is $\mathfrak{P}^r$ for some integer $r \geq 1$. Since B is self-dual, Tate local duality shows that, for all $n \geq 1$, $H^1(K_\mathfrak{q}, B)_{\pi^n}$ is dual to $B(K_\mathfrak{q})/\pi^{*n}B(K_\mathfrak{q})$, whence $H^1(K_\mathfrak{q}, B)(\mathfrak{P})$ is dual to $\varprojlim_n B(K_\mathfrak{q})/\pi^{*n}B(K_\mathfrak{q})$. Here, π^* is the non-zero element of $\mathscr{T}$ such that the ideal factorisation of π^* in the ring of integers of $\mathscr{T}$ is $\mathfrak{P}^{*r}$.

From the formulae (4.1) and (4.2), we have the exact sequence

$$0 \to B_0(K_\mathfrak{q}) \to B(K_\mathfrak{q}) \to C_\mathfrak{q} \to 0. \tag{4.3}$$

Now, for each w above $\mathfrak{q}$, we use the reduction modulo w exact sequence for $A_0(H_w)$. Noting that A has additive reduction at w and w is prime to 2, we see from (4.1) and (4.2) that π^{*n} is an automorphism of $B_0(K_\mathfrak{q})$. Then from the exact sequence (4.3), we obtain

$$B(K_\mathfrak{q})/\pi^{*n}B(K_\mathfrak{q}) = C_\mathfrak{q}/\pi^{*n}C_\mathfrak{q}.$$

The first assertion of the lemma now follows easily from Lemma 4.2.

For the second assertion, given a local field L_v, we write $k(L_v)$ for the residue field of L_v. Then we have $\tilde{B}(k(K_\mathfrak{p})) = \prod_{w|\mathfrak{p}} \tilde{A}(k(H_w))$, where $\tilde{A}$ is the reduction of A modulo w using the global model (2.1) and $\tilde{B}$ is the reduction of B modulo $\mathfrak{p}$. Since A has good reduction at $\mathfrak{p}$, we know that π^{*n} is an automorphism on $\prod_{w|\mathfrak{p}} \widehat{A}_w$, where $\widehat{A}_w$ denotes the formal group of A at w. Then by the same reasoning as in (i), we have that $H^1(K_\mathfrak{p}, B)(\mathfrak{P})$ is dual to

$$\varprojlim_n \frac{B(K_\mathfrak{p})}{\pi^{*n}B(K_\mathfrak{p})} = \varprojlim_n \frac{\tilde{B}(k(K_\mathfrak{p}))}{\pi^{*n}\tilde{B}(k(K_\mathfrak{p}))} = \tilde{B}(k(K_\mathfrak{p}))(\mathfrak{P}^*).$$

Now, by the theory of complex multiplication, $\phi(v)$ is the unique element of the ring of endomorphisms $\mathscr{T} = \mathrm{End}_K(B)$ whose reduction modulo $\mathfrak{p}$ is the Frobenius endomorphism of $\tilde{B}$ over the finite field $k(K_\mathfrak{p})$. Note that $\phi(\mathfrak{p})\overline{\phi}(\mathfrak{p}) = 2$ and $\phi(\mathfrak{p})-1$ is a $\mathfrak{P}$-unit. Thus,

$$\left|\#(\tilde{B}(k(K_\mathfrak{p}))(\mathfrak{P}^*))\right|_\mathfrak{P}^{-1} = |\ (\overline{\phi}(\mathfrak{p})-1)(\phi(\mathfrak{p})-1)\ |_\mathfrak{P}^{-1} = \left|\left(1-\frac{\phi(\mathfrak{p})}{2}\right)\right|_\mathfrak{P}^{-1}.$$

This completes the proof of the second assertion of the lemma. □

Let L/K be an algebraic extension over K, and let S be a finite set of primes of K. Then we define

$$\mathrm{Sel}^S_{\mathfrak{P}^\infty}(B/L) = \ker\left(H^1(L, B_{\mathfrak{P}^\infty}) \to \prod_{v\nmid S} H^1(L_v, B)(\mathfrak{P})\right),$$

where the product runs over all primes v of L not lying above the primes in S and L_v denotes the compositum field of all completions at v of finite extensions over K contained in L. In the following, we will simply write $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/L)$ for $\mathrm{Sel}'^{\{\mathfrak{p}\}}_{\mathfrak{P}^\infty}(B/L)$ and $\mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/L)$ for $\mathrm{Sel}^{\{\mathfrak{p},\mathfrak{q}\}}_{\mathfrak{P}^\infty}(B/L)$.

Proposition 4.4. *We have*

$$\left|\#\left(\mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K)\right)\right|^{-1}_{\mathfrak{P}} = \left|\left(1-\frac{\phi(\mathfrak{p})}{2}\right)\right|^{-1}_{\mathfrak{P}}.$$

Proof. We recall that π is a fixed element of $\mathscr{T}$ satisfying the factorisation $(\pi)=\mathfrak{P}^r$ in the ring of integers of $\mathscr{T}$ for some $r\geq 1$. For each integer $n\geq 1$, we have the short exact sequence

$$0\to \mathrm{Sel}_{\pi^n}(B/K)\to \mathrm{Sel}^{\mathcal{W}}_{\pi^n}(B/K)\xrightarrow{u_n}\prod_{v\in\mathcal{W}} H^1(K_v,B)_{\pi^n}, \tag{4.4}$$

where $\mathrm{Sel}^{\mathcal{W}}_{\pi^n}(B/K)$ is defined in a similar manner for B_{π^n}, and we write u_n for the right hand homomorphism in this sequence. On the other hand, by the definition of the Selmer group $\mathrm{Sel}_{\pi^{*n}}(B/K)$, we have the natural homomorphism

$$s_n : \mathrm{Sel}_{\pi^{*n}}(B/K)\to \prod_{v\in\mathcal{W}} B(K_v)/\pi^{*n}B(K_v). \tag{4.5}$$

Note that the groups on the right of (4.4) and (4.5) are dual to each other by Tate local duality and self-dualness of B. By the modified Poitou–Tate sequence (see, for example, [2, Section 3.3]), we conclude that $\mathrm{Coker}(u_n)$ is equal to the Pontryagin dual of $\mathrm{Im}(s_n)$ for all $n\geq 1$. Hence, writing u_∞ for the inductive limit of the maps u_n as $n\to\infty$, it follows that $\mathrm{Coker}(u_\infty)$ is dual to the image of the map $\mathfrak{s}_\infty=\varprojlim_n s_n$, where

$$\mathfrak{s}_\infty : \varprojlim_n \mathrm{Sel}_{\pi^{*n}}(B/K)\to \prod_{v\in\mathcal{W}} B(K_v)\otimes_{\mathscr{T}}\mathcal{O}_{T_{\mathfrak{P}^*}}.$$

But by Remark 3.5, $B(K)$ and $Ш(B/K)(\mathfrak{P}^*)$ are both finite. It follows that $\varprojlim_n \mathrm{Sel}_{\pi^{*n}}(B/K)$ is isormorphic to $B(K)(\mathfrak{P}^*)$, which is cyclic of order 2. Moreover, $\mathfrak{s}_\infty$ is injective because $\mathcal{W}$ is non-empty. Thus, the cokernel of u_∞ has order equal to $\#(B(K)(\mathfrak{P}^*))$. The result now follows on taking the inductive limit over all $n\geq 1$ of the exact sequences (4.4) and combining with Lemma 4.3 and Corollary 3.4. □

Let $F=K(B_{\mathfrak{P}^2})$. One can easily show that the degree of F over K is equal to 2. The next proposition is Theorem 2.4 of [6].

Proposition 4.5. *The abelian variety B has good reduction everywhere over F.*

Let K_∞ be the unique $\mathbb{Z}_2$-extension over K which is unramified outside of the prime $\mathfrak{p}$. Then we have $F_\infty=K(B_{\mathfrak{P}^\infty})=K_\infty(B_{\mathfrak{P}^2})$. We denote by

$$\mathscr{G}=\mathrm{Gal}(F_\infty/K)=\Gamma\times\Delta,$$

where $\Gamma\simeq\mathbb{Z}_2$ and $\Delta=\mathrm{Gal}(F_\infty/K_\infty)\simeq\mathrm{Gal}(F/K)$ is of order 2. We write δ for the generator of Δ, so that δ acts on $B_{\mathfrak{P}^\infty}$ by multiplication by -1. We refer the reader to [6] for more details on these fields and Galois groups.

Since $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)$ is a module over $\mathrm{Gal}(F/K)$, we may denote by $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta$ the subgroup of elements in $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)$ fixed by Δ.

Proposition 4.6. *We have the exact sequence*

$$0 \to H^1(F/K, B(F)_{\mathfrak{P}^\infty}) \to \mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K) \to \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta \to 0. \tag{4.6}$$

Proof. The assertion, except for the surjectivity, will follow from the commutative diagram

(4.7)

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K) & \longrightarrow & H^1(K, B_{\mathfrak{P}^\infty}) & \longrightarrow & \prod_{v\notin\mathcal{W}} H^1(K_v, B)(\mathfrak{P}) \\ & & \downarrow{\scriptstyle j_1} & & \downarrow{\scriptstyle j_2} & & \downarrow{\scriptstyle j_3} \\ 0 & \longrightarrow & \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta & \longrightarrow & (H^1(F, B_{\mathfrak{P}^\infty}))^\Delta & \longrightarrow & \left(\prod_{w\notin\{\mathfrak{p}\}} H^1(F_w, B)(\mathfrak{P})\right)^\Delta, \end{array}$$

where j_2 is the restriction map and j_1 is induced by the restriction of j_2 to $\mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K)$. We first show that

$$j_2\left(\mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K)\right) \subset (\mathrm{Sel}^{\mathcal{P}}_{\mathfrak{P}^\infty}(B/F))^\Delta. \tag{4.8}$$

To prove this, we note that since B has good reduction everywhere over F, the prime $\mathfrak{q}$ must ramify in F. We write w for the unique prime of F above $\mathfrak{q}$. We now claim that the local restriction map

$$r_{\mathfrak{q}} : H^1(K_{\mathfrak{q}}, B)(\mathfrak{P}) \to H^1(F_w, B)(\mathfrak{P})$$

must be the zero map, from which (4.8) follows easily. Indeed, we know from Lemma 4.3 that $H^1(K_{\mathfrak{q}}, B)(\mathfrak{P})$ is of order 2. Hence, it suffices to prove that the restriction map from $H^1(K_{\mathfrak{q}}, B)_2$ to $H^1(F_w, B)_2$ is the zero map, or equivalently, that the dual map from $B(F_w)/2B(F_w)$ to $B(K_{\mathfrak{q}})/2B(K_{\mathfrak{q}})$ given by the norm is the zero map. Since $\mathfrak{q}$ is prime to 2, multiplication by 2 is an automorphism of the formal group of B at w. Moreover, B has good reduction at w, and we write $\tilde{B}$ for the reduction of B modulo w. Thus, $\tilde{B}$ is an abelian variety over the residue field $k(F_w) = k(K_{\mathfrak{q}})$, and we have

$$B(F_w)/2B(F_w) = \tilde{B}(k(F_w))/2\tilde{B}(k(F_w)).$$

But since $k(F_w) = k(K_{\mathfrak{q}})$, the non-trivial element of Δ acts trivially on the group on the right hand side, and so the norm map will just be multiplication by 2 on this group, which clearly annihilates it, proving that $r_{\mathfrak{q}}$ is indeed the zero map. On the other hand, if $v \neq \mathfrak{q}$ is a place of K where B has good reduction, then v is unramified in F. Thus, writing Δ_v for the decomposition group of any prime w of F above v, a basic local property of abelian varieties with good reduction tells us that $H^1(\Delta_v, B(F_w)) = 0$. Thus, $r_v : H^1(K_v, B)(\mathfrak{P}) \to H^1(F_w, B)(\mathfrak{P})$ is injective in this case. A simple diagram chase in (4.7) then shows that the kernel of j_2 restricted to $\mathrm{Sel}^{\mathcal{W}}(E/H, E_{\mathfrak{p}^\infty})$ must be equal to the kernel of j_2, which is equal to $H^1(\Delta, E_{\mathfrak{p}^2})$. By applying the snake lemma to the diagram (4.7), we obtain the exact sequence

$$0 \to H^1(F/K, B(F)_{\mathfrak{P}^\infty}) \to \mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K) \xrightarrow{j_1} \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta.$$

We next show that j_1 is surjective. We simply write $v = \mathfrak{q}$ in $\mathcal{W}$, and let I_v be the inertia subgroup of some fixed prime of the algebraic closure of K above v. Since v is ramified in F/K, we can find an element θ of I_v whose restriction to F is $\delta\big|_F$. We now take ξ to be any element of $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta$. We must show that there exists a cohomology class ρ in $H^1(K, B_{\mathfrak{P}^\infty})$ such that $j_2(\rho) = \xi$. Note that any such ρ must automatically lie in $\mathrm{Sel}^{\mathcal{W}}_{\mathfrak{P}^\infty}(B/K)$ by the injectivity of j_3. Since B has good reduction everywhere over F, we can choose a cocycle representative g of ξ which is trivial on $I_v \cap \mathrm{Gal}(\overline{K}/F)$, whence $g(\theta^{2n}) = 0$ for all integers n, as

θ^{2n} lies in $I_v \cap \mathrm{Gal}(\overline{K}/F)$. For each z in $B_{\mathfrak{P}^\infty}$, let $d(z)$ denote the 1-coboundary on $\mathrm{Gal}(\overline{K}/F)$ defined by $d(z)(\sigma) = (\sigma - 1)z$. Note that

$$(\delta d)(z) = \theta(\theta^{-1}\sigma\theta - 1)z = (\sigma - 1)\delta(z) = -d(z).$$

Now, since the cohomology class ξ is fixed by Δ, we have $(1-\delta)g = d(z)$ for some $z \in B_{\mathfrak{P}^\infty}$. Let u be any element of $B_{\mathfrak{P}^\infty}$ such that $2u = z$. We claim that the equivalent cocycle f defined by $f = g - d(u)$ is then actually invariant under the action of Δ. Indeed, we have

$$(1-\delta)f = (1-\delta)g - (1-\delta)d(u) = d(z) - 2d(u) = 0.$$

Note also that we have $f(\theta^{2n}) = 0$ for all integers n. Now, every element τ in $\mathrm{Gal}(\overline{K}/K)$ can be written in the form $\tau = \sigma\theta^i$, where σ is in $\mathrm{Gal}(\overline{K}/F)$ and $i \in \{0, 1\}$. We define the map $h : \mathrm{Gal}(\overline{K}/K) \to B_{\mathfrak{P}^\infty}$ by $h(\tau) = f(\sigma)$. We claim that h is indeed a 1-cocycle, that is, taking $\tau_k = \sigma_k\theta^{i_k}$ for $k \in \{1, 2\}$, we must show that

$$h(\tau_1\tau_2) = h(\tau_1) + \tau_1 h(\tau_2). \tag{4.9}$$

Note first that, for any σ in $\mathrm{Gal}(\overline{K}/F)$ and any integer m, we have $h(\sigma\theta^m) = f(\sigma)$ since f vanishes on the even powers of θ. Now, we have $\tau_1\tau_2 = \sigma_1\sigma_2'\theta^{i_1+i_2}$, where $\sigma_2' = \theta^{i_1}\sigma_2\theta^{-i_1}$, whence it follows that

$$h(\tau_1\tau_2) = f(\sigma_1\sigma_2') = f(\sigma_1) + \sigma_1 f(\sigma_2').$$

But by construction, the cocycle f is fixed by Δ, and so we have $f(\sigma_2') = \theta^{i_1} f(\sigma_2)$, and the equality (4.9) follows. This completes the proof. □

Combining Propositions 4.4 and Proposition 4.6, and noting that

$$B(K)(\mathfrak{P}^*) \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad H^1(F/K, B(F)(\mathfrak{P})) \simeq B_{\mathfrak{P}^2}/B_{\mathfrak{P}},$$

we obtain the following corollary.

Corollary 4.7. *The Selmer group* $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta$ *is finite, and we have*

$$\left|\#\left(\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F)^\Delta\right)\right|_{\mathfrak{P}}^{-1} = \frac{1}{2}\left|\left(1 - \frac{\phi(\mathfrak{p})}{2}\right)\right|_{\mathfrak{P}}^{-1}.$$

5. Infinite descent over the field $F_\infty = K(B_{\mathfrak{P}^\infty})$ and a main conjecture for F_∞/K

In this section, we will use an infinite descent method due to Coates [5] and a main conjecture of Iwasawa theory in order to show that $L(\overline{\phi}, 1) \neq 0$, and to give the precise $\mathfrak{P}$-adic valuation for the algebraic part of the L-value $L(\overline{\phi}, 1)$. This precise $\mathfrak{P}$-adic valuation will play a key role as the base case of an induction argument in Section 6. We recall that $F_\infty = K(B_{\mathfrak{P}^\infty})$. A large part of this section, namely the construction of the $\mathfrak{P}$-adic L-function for B over F_∞/K and the proof of the main conjecture for B for the tower F_∞/F, has been established in [6]. We will just briefly recall these results and use the results from Sections 3 and 4 in order to obtain the desired $\mathfrak{P}$-adic valuation for the algebraic L-value of ϕ.

We define $M(F_\infty)$ to be the maximal abelian 2-extension of F_∞ which is unramified outside the primes lying above $\mathfrak{p}$, and we put

$$X(F_\infty) = \mathrm{Gal}(M(F_\infty)/F_\infty).$$

By maximality, $M(F_\infty)$ is Galois over K, and thus $\mathscr{G} = \mathrm{Gal}(F_\infty/K)$ acts on $X(F_\infty)$ in the usual manner via lifting of inner automorphisms. We list some results relating $X(F_\infty)$ to the Selmer groups in the following theorem.

Theorem 5.1. *We have*

(1) $\mathrm{Sel}_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Hom}(X(F_\infty), B_{\mathfrak{P}^\infty})$, *where all these modules are Galois modules over* $\mathscr{G}$.

(2) $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty) = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty)^\Delta$, *where* $\Delta = \mathrm{Gal}(F_\infty/K_\infty)$.

(3) The restriction map yields the isomorphism

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F) \simeq \mathrm{Sel}'_{\mathfrak{P}^\infty}(B/F_\infty)^\Gamma,$$

where $\Gamma = \mathrm{Gal}(F_\infty/F)$.

Proof. For a detailed proof, we refer to Theorem 3.9, Proposition 3.10 and Proposition 3.11 in [6]. □

Note that Γ is isomorphic to $\mathbb{Z}_p$, and we write $\Lambda(\Gamma)$ for the Iwasawa algebra of Γ with coefficients in $\mathbb{Z}_p$. For each choice of a topological generator γ of Γ, there is a unique isomorphism of compact $\mathbb{Z}_p$-algebras

$$i : \Lambda(\Gamma) \simeq \mathbb{Z}_p[[T]]$$

which maps γ to $1+T$, where $\mathbb{Z}_p[[T]]$ denotes the ring of formal power series in variable T with coefficients in $\mathbb{Z}_p$. Let $\mathfrak{M}$ be any finitely generated torsion $\Lambda(\Gamma)$-module. The structure theory of finitely generated $\Lambda(\Gamma)$-modules asserts that there is an exact sequence of $\Lambda(\Gamma)$-modules

$$0 \to \oplus_{k=1}^m \Lambda(\Gamma)/f_k\Lambda(\Gamma) \to \mathfrak{M} \to D \to 0,$$

where the f_k for $k = 1, \ldots, m$ are non-zero elements of $\Lambda(\Gamma)$ and D is some finite $\Lambda(\Gamma)$-module. Moreover, the ideal $\mathfrak{C}(\mathfrak{M}) = f_1 \cdots f_m \Lambda(\Gamma)$ is then uniquely determined by $\mathfrak{M}$, and is called the *characteristic ideal* of $\mathfrak{M}$. Any generator of this ideal is called a *characteristic element* of $\mathfrak{M}$, and the image of a characteristic element under the isomorphism i will be called a *characteristic power series* of $\mathfrak{M}$. The following elementary lemma is then classical [7, Appendix A.2].

Lemma 5.2. *Let* $\mathfrak{M}$ *be a finitely generated torsion* $\Lambda(\Gamma)$*-module, and let* $c_{\mathfrak{M}}(T)$ *be any characteristic power series of* $\mathfrak{M}$. *Then the following assertions are equivalent:* $(i) c_{\mathfrak{M}}(0) \neq 0$, *(ii)* $\mathfrak{M}_\Gamma$ *is finite, and (iii)* $\mathfrak{M}^\Gamma$ *is finite. Moreover, when these equivalent assertions hold, we have*

$$|c_{\mathfrak{M}}(0)|_p^{-1} = \#(\mathfrak{M}_\Gamma)/\#(\mathfrak{M}^\Gamma).$$

Here, $|\cdot|_p$ *is a fixed multiplicative valuation on* $\mathbb{C}_p$ *extending* $|\cdot|_{\mathfrak{P}}$. *We note here that we always fix an embedding of* T *into* $\mathbb{C}_p$ *via the prime* $\mathfrak{P}$.

In particular, if $\mathfrak{M}$ has no non-zero finite Γ-submodules, then the lemma shows that $\mathfrak{M}^\Gamma = 0$ when $c_{\mathfrak{M}}(0) \neq 0$. Finally, we write $\mathscr{I}$ for the ring of integers of the completion of the maximal unramified extension of $T_{\mathfrak{P}}$, and we define $\Lambda_{\mathscr{I}}(\Gamma) = \mathscr{I}[[\Gamma]]$ to be the Iwasawa algebra of Γ with coefficients in $\mathscr{I}$.

Another key input we need for treating the case $p = 2$ is that we need to show $X(F_\infty)$ is a finitely generated $\mathbb{Z}_2$-module. Fortunately, this follows easily from our earlier work [4].

Lemma 5.3. *The Iwasawa module* $X(F_\infty)$ *is a finitely generated* $\mathbb{Z}_2$*-module.*

Proof. We have the inclusions of fields

$$F_\infty \subset H(A_{\mathfrak{p}^\infty}) \subset M(F_\infty) \subset M(H(A_{\mathfrak{p}^\infty})),$$

where $M(H(A_{\mathfrak{p}^\infty}))$ denotes the maximal abelian 2-extension of $H(A_{\mathfrak{p}^\infty})$ which is unramified outside the primes lying above $\mathfrak{p}$. In [4], it was shown that $X(H(A_{\mathfrak{p}^\infty})) = \mathrm{Gal}(M(H(A_{\mathfrak{p}^\infty}))/H(A_{\mathfrak{p}^\infty}))$ is a finitely generated $\mathbb{Z}_2$-module. Thus, the quotient

$\mathrm{Gal}(M(F_\infty)/H(A_{\mathfrak{p}^2}))$ of $X(H(A_{\mathfrak{p}^\infty}))$ is also a finitely generated $\mathbb{Z}_2$-module. The lemma now follows since $X(F_\infty)$ consists of finite copies of $\mathrm{Gal}(M(F_\infty)/H(A_{\mathfrak{p}^2}))$. □

In particular, $X(F_\infty)$ is a finitely generated torsion Λ-module. We write $c_X(T)$ for a characteristic power series of $X(F_\infty)$. Let

$$\rho_{\mathfrak{P}} : \mathscr{G} \to \mathbb{Z}_2^\times$$

be the character giving the action of the Galois group $\mathscr{G}$ on $B_{\mathfrak{P}^\infty}$. We denote by $\mathrm{T}_{\mathfrak{P}}B$ the $\mathfrak{P}$-adic Tate module of B. Let $\mathrm{T}_{\mathfrak{P}}B^{\otimes(-1)} = \mathrm{Hom}(B_{\mathfrak{P}^\infty}, T_{\mathfrak{P}}/\mathcal{O}_{T_{\mathfrak{P}}})$ be the free $\mathcal{O}_{T_{\mathfrak{P}}}$-module of rank 1 on which Γ acts by the character $\rho_{\mathfrak{P},\Gamma}^{-1}$, where $\rho_{\mathfrak{P},\Gamma}$ denotes the restriction of $\rho_{\mathfrak{P}}$ to Γ. If $\mathfrak{M}$ is any finitely generated torsion $\Lambda(\Gamma)$-module, we define, as usual, $\mathfrak{M}(-1) = \mathfrak{M} \otimes_{\mathcal{O}_{\mathfrak{P}}} \mathrm{T}_{\mathfrak{P}}B^{\otimes(-1)}$, endowed with the diagonal action of Γ. Here, we note that $T_{\mathfrak{P}} \simeq \mathbb{Z}_2$. Then, writing $c_{\mathfrak{M}}(T)$ for a characteristic power series of $\mathfrak{M}$, a characteristic power series of the $\Lambda(\Gamma)$-module $\mathfrak{M}(-1)$ is given by $c_{\mathfrak{M}}(u(1+T)-1)$, where $u = \rho_{\mathfrak{P},\Gamma}(\gamma)$. We also note that if $\mathfrak{M}$ has no non-zero finite Γ-submodule, then the same is true for $\mathfrak{M}(-1)$.

Recall that γ is our fixed topological generator of Γ, and recall also that both $B(K)$ and $Ш(B/K)(\mathfrak{P}\mathfrak{P}^*)$ are finite by Remark 3.5. Using Theorem 5.1 and the theorem of Greenberg on the non-existence of finite submodules for $X(F_\infty)$ [9, p. 93], and noting that $\mathrm{Hom}(X(F_\infty), B_{\mathfrak{P}^\infty})$ is isormorphic to $\mathrm{Hom}(X(F_\infty)(-1), T_{\mathfrak{P}}/\mathcal{O}_{T_{\mathfrak{P}}})$ as Γ-modules, we can reformulate Corollary 4.7 as follows.

Proposition 5.4. *Let $c_X(T)$ be a characteristic power series of $X(F_\infty)$, and let $u = \rho_{\mathfrak{P},\Gamma}(\gamma)$. Then $c_X(u-1) \neq 0$. Moreover, we have*

$$|c_X(u-1)|_p^{-1} = \frac{1}{2}\left|\left(1 - \frac{\phi(\mathfrak{p})}{2}\right)\right|_{\mathfrak{P}}^{-1}. \tag{5.1}$$

We now introduce the $\mathfrak{P}$-adic L-function of B for the tower F_∞/K and a corresponding main conjecture of Iwasawa theory. Recall that we have chosen a global minimal generalised Weierstrass equation (2.1) for A/H. Moreover, since $H = K(j(\mathcal{O}_K))$ and we have fixed an embedding of K into $\mathbb{C}$, we also have an embedding of H into $\mathbb{C}$. The Néron differential $\omega = dx/(2y + a_1x + a_3)$ on A/H then has a complex period lattice of the form $\mathcal{L} = \Omega_\infty \mathcal{O}_K$, where Ω_∞ is a nonzero complex number which is uniquely determined up to sign.

We now fix an embedding of H into the fraction field of $\mathscr{I}$, which amounts to choosing a prime w of H lying above $\mathfrak{p}$. We write $\widehat{A}$ for the formal group of A under this embedding. Since $\widehat{A}$ has height 1 as a formal group, there exists an isomorphism

$$j_{\mathfrak{p}} : \widehat{\mathbb{G}}_m \xrightarrow{\sim} \widehat{A} \tag{5.2}$$

of formal groups over $\mathscr{I}$, where $\widehat{\mathbb{G}}_m$ denotes the formal multiplicative group. As usual, we take as a parameter for $\widehat{A}$ the local parameter $t = -\frac{x}{y}$ at infinity of the Weierstrass equation (2.1). The isomorphism $j_{\mathfrak{p}}$ is then given by a power series $t = j_{\mathfrak{p}}(w_0)$ with coefficients in $\mathscr{I}$, where w_0 is the parameter of $\widehat{\mathbb{G}}_m$. We then define the $\mathfrak{p}$-adic period $\Omega_{\mathfrak{p}}$ to be the coefficient of w_0 in the formal power series $t = j_{\mathfrak{p}}(w_0)$. Since $j_{\mathfrak{p}}$ is an isomorphism, $\Omega_{\mathfrak{p}}$ is a unit in $\mathscr{I}$.

We now fix an embedding of the field T into $\mathbb{C}$ which extends our fixed embedding of K into $\mathbb{C}$, so that we can consider the complex Hecke L-functions $L(\overline{\phi}^k, s)$ for all odd integers $k \geq 1$. Here, we note that the Hecke character $\overline{\phi}^k$ has conductor $\mathfrak{q}$, and by a theorem of Deuring, $L(\overline{\phi}^k, s)$ is an entire function. Finally, we fix an

embedding of the compositum HT into the fraction field of $\mathscr{I}$ which induces the prime w of H and the prime $\mathfrak{P}$ of T. This is possible because $H \cap T = K$.

By Theorem 5.4 in [6], for all odd integers $k \geq 1$, we have

$$\frac{L(\overline{\phi}^k, k)}{\Omega_\infty^k} \in HT.$$

We are now ready to introduce a $\mathfrak{P}$-adic L-function and to state a main conjecture.

Proposition 5.5. *There exists a unique measure μ_A in $\Lambda_{\mathscr{I}}(\Gamma)$ such that, for all odd positive integers $k = 1, 3, 5, \ldots$, we have*

$$\Omega_{\mathfrak{p}}^{-k} \int_\Gamma (\rho_{\mathfrak{P},\Gamma})^k d\mu_A = (k-1)! \Omega_\infty^{-k} L(\overline{\phi}^k, k)(1 - \phi^k(\mathfrak{p})/2). \tag{5.3}$$

Furthermore, μ_A satisfies the main conjecture

$$c_X \Lambda_{\mathscr{I}}(\Gamma) = \mu_A \Lambda_{\mathscr{I}}(\Gamma),$$

where c_X is a characteristic element for $X(F_\infty)$.

Proof. The details for the construction of μ_A and its relation to certain Iwasawa modules can be found in Sections 4–7 in [6]. For the proof of the main conjecture, we refer to Theorem 7.13 in [6]. □

Combined with Proposition 5.4, we thus obtain a new proof of the theorem of Rohrlich on the non-vanishing of $L(A, 1)$ on noting that $L(A, 1) \neq 0$ if and only if $L(\overline{\phi}, 1) \neq 0$. Furthermore, we obtain the precise 2-adic valuation of the algebraic part of the L-value $L(\overline{\phi}, 1)/\Omega_\infty$:

Corollary 5.6. *We have $L(\overline{\phi}, 1) \neq 0$. Moreover, we have*

$$\left| \frac{L(\overline{\phi}, 1)}{\Omega_\infty} \right|_2^{-1} = 2^{-1}. \tag{5.4}$$

Proof. This follows from Propositions 5.4 and 5.5. Indeed, given an element w in $\Lambda_{\mathscr{I}}(\Gamma)$, we write $w(T)$ for the corresponding power series under the isomorphism from $\Lambda_{\mathscr{I}}(\Gamma)$ to $\mathscr{I}[[T]]$ induced by mapping γ to $1 + T$. By Theorem 5.5, we have $c_X = \mu_A \beta$ for some unit β in $\Lambda_{\mathscr{I}}(\Gamma)$, whence

$$|c_X(u-1)|_2^{-1} = |\mu_A(u-1)|_2^{-1} = \left| \int_\Gamma \rho_{\mathfrak{p},\Gamma} d\mu_A \right|_2^{-1}.$$

In particular, we conclude from (5.3) for $k = 1$ that $c_X(u-1) \neq 0$ if and only if $L(\overline{\phi}, 1) \neq 0$. Thus, the first assertion of Corollary 5.6 follows from the first assertion of Proposition 5.4. Finally, since $\Omega_{\mathfrak{p}}$ is a unit in $\mathscr{I}$, the formula (5.4) follows immediately from (5.1) and (5.3) for $k = 1$. □

We end this section with some remarks on the algebraic L-value in Corollary 5.6. It was shown by Buhler and Gross (or in [6]) that $L(\overline{\phi}, 1)/\Omega_\infty$ is contained in HT, and that the fractional ideal $\frac{L(\overline{\phi},1)}{\Omega_\infty}\mathcal{O}_{HT}$ descends to a fractional ideal $\mathfrak{m}$ in T. Corollary 5.6 shows the $\mathfrak{P}$-adic valuation of $\mathfrak{m}$ is equal to -1. Thus, we have proved:

Theorem 5.7. *The $\mathfrak{P}$-part of the Birch–Swinnerton-Dyer conjecture holds for B.*

At present, we cannot give the precise $\mathfrak{P}'$-adic valuation of $\mathfrak{m}$ for other primes of T lying above 2 (except for $\mathfrak{P}^*$). A detailed study of these $\mathfrak{P}'$-valuations will be contained in our subsequence work [15].

6. Generalised Zhao's method and 2-adic valuation of central L-values

In this section, we will use an extension of Zhao's induction method [24, 25], modified for the abelian varieties, to obtain the exact valuation of central L-values for quadratic twists, using Corollary 5.6 as the base case.

As defined in the introduction, let $R \in \mathfrak{R}$ be of the form $R = r_1 \cdots r_k$, where $k \geq 0$ and $r_1, \ldots, r_k$ are distinct primes such that (i) $r_i \equiv 1 \bmod 4$, and (ii) r_i is inert in K for $i = 1, \ldots, k$. We recall that ϕ is the Hecke character of B/K. Then, since $(R, q) = 1$, for each positive integer $d \mid R$, the Hecke character ϕ_d of $B^{(d)}/K$ is given by $\phi_d = \phi\chi_d$, where χ_d denotes the abelian character of K defining the quadratic extension $K(\sqrt{d})/K$. Here, as usual, we denote by $B^{(d)}$ the twist of B by the extension $K(\sqrt{d})/K$. The remainder of this section will be dedicated to concluding the proof of the following main result stated in the introduction.

Theorem 6.1. *For any $R = r_1 \cdots r_k \in \mathfrak{R}$. Then $\frac{L(\overline{\phi}_R, 1)\sqrt{R}}{\Omega_\infty} \in TH$, and for any prime $\mathcal{P}$ of TH lying above $\mathfrak{P}$, we have*

$$\mathrm{ord}_{\mathcal{P}}\left(\frac{L(\overline{\phi}_R, 1)\sqrt{R}}{\Omega_\infty}\right) = k - 1.$$

In particular, $L(A^{(R)}/H, 1) \neq 0$. Moreover, the Mordell–Weil group $A^{(R)}(H)$ and and the Tate–Shafarevich group $Ш(A^{(R)}/H)$ of $A^{(R)}$ are finite.

We define the imprimitive Hecke L-series

$$L_R(\overline{\phi}_d, s) = \sum_{(\mathfrak{b}, R\mathfrak{q})=1} \frac{\overline{\phi}_d(\mathfrak{b})}{N(\mathfrak{b})^s},$$

where the sum on the right is taken over all integral ideals $\mathfrak{b}$ of K which are prime to $R\mathfrak{q}$. It is classical that the Dirichlet series on the right converges for $\mathrm{Re}(s) > 3/2$, and it has analytic continuation to the whole complex plane.

We define the fields

$$J_R = K(\sqrt{r_1}, \ldots, \sqrt{r_k}),\ H_R = H(\sqrt{r_1}, \ldots, \sqrt{r_k}), \tag{6.1}$$

and we recall that Ω_∞ is the complex period defined in Section 5. The proof of the following proposition can be found in Proposition 9.8 and Theorem 9.9 of [6].

Proposition 6.2. *There exists an element $V_R \in H_R$ which is integral at all places of H_R above 2, and which satisfies*

$$\sum_{d \mid R} L_R(\overline{\phi}_d, 1)/\Omega_\infty = 2^k V_R,$$

where the sum runs over all positive divisors d of R.

This will be a key identity in the induction argument to follow.

Lemma 6.3. *For each $R \in \mathfrak{R}$, the extension J_R/K defined by* (6.1) *is unramified at the primes of K lying above 2.*

Proof. It suffices to show that, for each prime divisor r of R, the extension $K(\sqrt{r})/K$ is unramified at the primes above 2. Put $m = (\sqrt{r} - 1)/2$, so that $V(m) = 0$, where $V(X) = X^2 + X - (r-1)/4$. But then $V'(m) = 2m + 1$ is a unit at $\mathfrak{p}$ and $\mathfrak{p}^*$, and so $K(m) = K(\sqrt{r})$ is unramified at the primes of K above 2. □

For each positive divisor d of R, we define

$$\mathscr{L}(d) = \sqrt{d}L(\overline{\phi}_d, 1)/\Omega_\infty,\ \mathscr{L} = \mathscr{L}(1).$$

Proposition 9.3 in [6] shows that $\mathscr{L}(d)$ always belongs to the field HT. However, the following stronger assertion is essential for our proof. Note that by Corollary 5.6, we have $\mathscr{L} \neq 0$ for all primes $q \equiv 7 \bmod 8$.

Proposition 6.4. *Assume $R \in \mathfrak{R}$, and let d be any positive divisor of R. Then $\mathscr{L}(d)/\mathscr{L}$ belongs to the field T.*

Proof. This is exactly Proposition 9.15 in [6], which uses Proposition 11.1 in [3] as a key input. □

Before we prove Theorem 6.1, we need the following lemma.

Lemma 6.5. *Let d be any positive divisor of R, and let r be any prime dividing R with $(r, d) = 1$. Then $\phi_d(r\mathcal{O}_K) = -r$.*

Proof. Let $\mathfrak{r} = r\mathcal{O}_K$. Noting that $-r$ is a square modulo $\mathfrak{q}$, the explicit formula for ϕ given at the beginning of §2 of [3] shows that $\phi(\mathfrak{r}) = -r$. On the other hand, since r is inert in K and the Galois group of $K(\sqrt{d})/\mathbb{Q}$ is not cyclic, the prime $\mathfrak{r}$ of K must split in $K(\sqrt{d})$, so that we have $\chi_d(\mathfrak{r}) = 1$. Hence $\phi_d(\mathfrak{r}) = -r$, as required. □

We can now conclude the proof of Theorem 6.1 using induction on the number k of prime factors of R. Assume first that $k = 1$, so that $R = r$, a prime number. Then Proposition 6.2 gives

$$\mathscr{L}(r)/\sqrt{r} + (1 - \overline{\phi}((r))/r^2)\mathscr{L} = 2V_r. \tag{6.2}$$

Let $\mathfrak{Q}$ be any prime of $HT(\sqrt{r})$ lying above the prime $\mathfrak{P}$ of T. We then have $\mathrm{ord}_{\mathfrak{Q}}(V_r) \geq 0$. Furthermore, by Lemma 6.5, we have $(1 - \overline{\phi}((r))/r^2) = (1 + 1/r)$. Since $r+1 \equiv 2 \bmod 4$, it follows from Corollary 5.6 that $\mathrm{ord}_{\mathfrak{Q}}((1 - \overline{\phi}((r))/r^2)\mathscr{L}) = 0$. As $\mathrm{ord}_{\mathfrak{Q}}(V_r) \geq 0$, we conclude from (6.2) that $\mathrm{ord}_{\mathfrak{Q}}(\mathscr{L}(r)/\sqrt{r}) = 0$, and so Theorem 6.1 holds when $k = 1$.

Suppose now that $R = r_1 \cdots r_k$ with $k \geq 2$. By Proposition 6.2, we have

$$\mathscr{L}(R)/\sqrt{R} + \sum_{d|R, d\neq 1, R} \Lambda(d, R)/\sqrt{d} + \mathscr{L}\prod_{i=1}^{k}(1 - \overline{\phi}((r_i))/r_i^2) = 2^k V_R, \tag{6.3}$$

where

$$\Lambda(d, R) = \mathscr{L}(d) \prod_{r|R/d} (1 - \overline{\phi}_d((r))/r^2).$$

The problem here is that the terms $\Lambda(d, R)$ lie in an extension of HT, where the prime $\mathfrak{P}$ of T is unramified but will usually have a large residue class field extension. This means that one cannot carry through the inductive argument in its naive form, and we must appeal to Proposition 6.4 to get around it. The key to overcoming this difficulty is to divide both side of (6.3) by the non-zero number $\mathscr{L}$. Then defining $\Phi(d, R) = \Lambda(d, R)/\mathscr{L}$ for each positive integer divisor d of R, we obtain the equation

$$\Phi(R)/\sqrt{R} + \sum_{d|R, d\neq 1, R} \Phi(d, R)/\sqrt{d} + \prod_{i=1}^{k}(1 - \overline{\phi}((r_i))/r_i^2) = 2^k V_R/\mathscr{L}, \tag{6.4}$$

where $\Phi(R) = \mathscr{L}(R)/\mathscr{L}$. Let H_R be the field defined in (6.1), and we now take $\mathfrak{Q}$ to be any prime of the compositum $H_R T$ lying above $\mathfrak{P}$ so that $\mathfrak{Q}/\mathfrak{P}$ is unramified.

By Proposition 6.2, we have $\mathrm{ord}_{\mathfrak{Q}}(V_R) \geq 0$. Thus we conclude from Corollary 5.6 that $\mathrm{ord}_{\mathfrak{Q}}(2^k V_R/\mathscr{L}) \geq k+1$. Thanks to Lemma 6.5, we have

$$\mathrm{ord}_{\mathfrak{Q}}(\prod_{i=1}^{k}(1-\overline{\phi}((r_i))/r_i^2)) = k. \tag{6.5}$$

On the other hand, our inductive hypothesis together with Corollary 5.6 and Lemma 6.5 shows that, for each positive divisor d of R with $d \neq 1, R$, we have

$$\mathrm{ord}_{\mathfrak{Q}}(\Phi(d,R)/\sqrt{d}) = k.$$

Of course, these estimates alone do not allow us to conclude that $\mathrm{ord}_{\mathfrak{Q}}(\Phi(R)/\sqrt{R}) = k$ when applied to (6.4). However, the argument is saved by Proposition 6.4, which tells us that $\Phi(d,R)$ belongs to the field T for every positive divisor d of R, and so it lies in the completion $T_{\mathfrak{P}}$ at $\mathfrak{P}$. Since $\mathfrak{P}$ has its residue degree of order 2, we can write for each divisor d of R with $1 < d < R$

$$\Phi(d,R)/\sqrt{d} = \sqrt{d}\pi_{\mathfrak{P}}^k(1+\pi_{\mathfrak{P}}b_d),$$

where $\pi_{\mathfrak{P}}$ is a local parameter at $\mathfrak{P}$ and $\mathrm{ord}_{\mathfrak{P}}(b_d) \geq 0$. Thus,

$$\sum_{d|R, d\neq 1,R} \Phi(d,R)/\sqrt{d} \equiv \pi_{\mathfrak{P}}^k D_R \bmod \mathfrak{Q}^{k+1}$$

with $D_R = \sum_{d|R.d\neq 1,R}\sqrt{d}$. But

$$D_R^2 \equiv \sum_{d|R.d\neq 1,R} d \bmod \mathfrak{Q}$$

and $\sum_{d|R.d\neq 1,R} d \equiv 2^k \bmod 2$, whence $\mathrm{ord}_{\mathfrak{Q}}(D_R) \geq 1$. Thus, we have shown that

$$\mathrm{ord}_{\mathfrak{Q}}\left(\sum_{d|R,d\neq 1,R}\Phi(d,R)/\sqrt{d}\right) \geq k+1.$$

It now follows from (6.4) and (6.5) that $\mathrm{ord}_{\mathfrak{Q}}(\Phi(R)) = k$. Thus, again applying Corollary 5.6, we have finally completed the proof of Theorem 6.1 by induction on the number of prime factors of $R \in \mathfrak{R}$.

We will conclude this paper the proof of the density result in Corollary 1.2, which we now recall.

Corollary 6.6 (Corollary 1.2)**.** *Let $D \geq 1$ denote a fundamental discriminant, and let $N(X) = \#\{D < X : L(A^{(D)}/H, 1) \neq 0\}$. Then we have*

$$N(X) \gg \frac{X}{\log^{\frac{3}{4}} X}.$$

Proof. The proof follows closely the ideas of Serre [**?**], which is based on generalisations of the Tauberian theorem of Ikehara due to Delange[**?**], Wintner[**?**] et al. and a method of Landau [**?**]. Such an argument has already appeared in, for example, the works of Ono [**?**] or Kriz–Li [**?**], but we write out the details for our particular case.

We define the set of primes $\mathcal{P}$ denote the set of primes which is the *complement* of the set of primes which are congruent to 1 modulo 4 and inert in K. Then $\mathcal{P}$ is *regular* of density $1 - \frac{1}{2}\cdot\frac{1}{2} = \frac{3}{4}$ in the sense of Delange [**?**], by the Chebotarev density theorem. Furthermore, $\mathcal{P}$ is *associated* to the set $E = \mathbb{N}_{>0}\backslash\mathfrak{R}$, in the sense that for any $p \in \mathcal{P}$ and any integer $m \geq 1$ not divisible by p, we have $pm \in E$. Given X, let $E(X) = \{D \leq X : D \in E\}$ and $\mathfrak{R}(X) = \{D \leq X : D \in \mathfrak{R}\}$, so that $E(X) + \mathfrak{R}(X) = X$.

Noting that now $\mathfrak{R}(X) = E'(X)$ in the notation of [**?**], we have from [**?**, Théorème 2.8], for any integer $k \geq 0$, real numbers $c_0, c_1, \ldots, c_k$ with $c_0 > 0$ such that

$$\mathfrak{R}(X) = \frac{X}{\log^{\frac{3}{4}} X}(c_0 + c_1/\log X + \cdots c_k \log^k X + O(1/\log^{k+1} X)).$$

In particular,

$$\mathfrak{R}(X) = c_0 \frac{X}{\log^{\frac{3}{4}} X} + O(X/\log^{\frac{7}{4}} X).$$

The result now follows, on noting that by Theorem 1.1 we have $L(A^{(D)}/H, 1) \neq 0$ for all $D \in \mathfrak{R}$. □

References

[1] *N. Arthaud*, On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication, I, Compos. Math. 37 (1978), pp. 209–232.

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

[3] *J. Buhler* and *B. Gross*, Arithmetic on elliptic curves with complex multiplication. II, Invent. Math. 79 (1985), pp. 11–29.

[4] *J. Choi*, *Y. Kezuka* and *Y-X. Li*, 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, pp. 383-400.

[5] *J. Coates*, Infinite Descent on Elliptic Curves with Complex Multiplication, Arithmetic and geometry, Progress in Mathematics **35**, M. Artin and J. Tate (eds) Birkhäuser Boston, Boston, MA (1983) pp. 107–137.

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

[7] *J. Coates* and *R. Sujatha*, Cyclotomic Fields and Zeta Values, Springer, first edition (2006).

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

[9] *R. Greenberg*, On the structure of certain Galois groups, Invent. Math. **47** (1978), no. 1, pp. 85–99.

[10] *B. Gross*, Arithmetic on elliptic curves with complex multiplication, Lecture Notes in Mathematics 776, Springer, Berlin, 1980.

[11] *B. Gross*, Minimal models for elliptic curves with complex multiplication, Compositio Math. **45** (1982), pp. 155–164.

[12] *B. Gross* 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, Mass., 1982.

[13] *B. Gross* and *D. Zagier* Heegner points and derivatives of L-series, Invent. Math. 84 (2), pp. 225–320 (1986)

[14] *K. Kato*, p-adic Hodge theory and values of zeta functions of modular forms, Asterisque **295** (2004) pp. 117–290.

[15] *Y. Kezuka* and *Y-X. Li*, On the Birch and Swinnerton-Dyer formula for quadratic twists of certain abelian varieties with complex multiplication at $p = 2$, in preparation.

[16] *V.A.Kolyvagin* Finitenessof $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. Izv. Akad. Nauk SSSR Ser. Mat. 52 (3) pp. 522–540, 670–671,1988.

[17] *J. Li*, On the 2-adic logarithm of units of pure imaginary quartic fields, Asian J. Math. **25** (2021) pp. 177–182.

[18] *F. Rodriguez Villegas*, On the square root of special values of certain L-series., Invent. Math. **106** (1991), no. 3, pp. 549–573.

[19] *D. Rohrlich*, The non-vanishing of certain Hecke L-functions at the center of the critical strip, Duke Math. J. **47** (1980), pp. 223–232.

[20] *K. Rubin* Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 64 (1981), pp. 455–470.

[21] *J. B. Tunnell*, A classical Diophantine problem and modular forms of weight 3/2, Invent. Math., 72 (2) (1983), pp. 323–334.

[22] *T. Yang*, Theta liftings and Hecke L-functions, J. reine angew. Math. **485** (1997), pp. 25–53.

[23] *T. Yang*, Nonvanishing of central Hecke L-values and rank of certain elliptic curves, Compositio Math. **117** (1999), no. 3, pp. 337–359.

[24] *C. Zhao*, A criterion for elliptic curves with lowest 2-power in $L(1)$, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 3, pp. 385-400.

[25] *C. Zhao*, A criterion for elliptic curves with second lowest 2-power in $L(1)$, Math. Proc. Cambridge Philos. Soc. **131** (2001), no. 3, pp. 385-404.

Yukako Kezuka
Institut de mathématiques de Jussieu
4 Pl. Jussieu
75005 Paris, France
yukako.kezuka@imj-prg.fr

Yong-Xiong Li
Yau Mathematical Sciences Center
Tsinghua University,
100084 Beijing, China
liyx_1029@tsinghua.edu.cn