On the λ-invariant of Selmer groups arising from certain quadratic twists of Gross curves

Jianing Li

Shandong University

Abstract. Let q be a prime with $q \equiv 7 \bmod 8$, and let $K = \mathbb{Q}(\sqrt{-q})$. Then 2 splits in K, and we write $\mathfrak{p}$ for either of the primes K above 2. Let K_∞ be the unique $\mathbb{Z}_2$-extension of K unramified outside $\mathfrak{p}$. For certain quadratic and biquadratic extensions $\mathfrak{F}/K$, we prove a simple exact formula for the λ-invariant of the Galois group of the maximal abelian 2-extension unramified outside $\mathfrak{p}$ of the field $\mathfrak{F}_\infty = \mathfrak{F}K_\infty$. Equivalently, our result determines the exact $\mathbb{Z}_2$-corank of certain Selmer groups over $\mathfrak{F}_\infty$ of a large family of quadratic twists of the higher dimensional abelian variety with complex multiplication, which is the restriction of scalars to K of the Gross curve with complex multiplication defined over the Hilbert class field of K. We also exhibit computations of the associated Selmer groups over K_n in the case when the λ-invariant is equal to 1; here K_n denotes the n-th layer of K_∞/K.

1. Introduction

The aim of the present paper is to prove a simple exact formula for the λ-invariant of a certain classical Iwasawa module at the prime $p = 2$. Our result can be viewed as an analogue of a result of Kida [9] and Ferrero [5]. However, there is a fundamental difference in that, unlike Kida's and Ferrero's work, the Iwasawa module we consider has a simple interpretation in terms of classical infinite descent theory on a family of abelian varieties with complex multiplication arising from certain quadratic twists of the Gross [8] family of elliptic curves with complex multiplication. We mention that, for odd primes, such formulas for elliptic curves with complex multiplication (usually called Kida formulas) have been obtained by Michel [12] and Wingberg [14].

We first explain our result in terms of classical Iwasawa theory. Let q be any prime with $q \equiv 7 \bmod 8$, and let $K = \mathbb{Q}(\sqrt{-q})$. Write $\mathcal{O}_K$ for the ring of integers of K. Then 2 splits in K, say $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. By class field theory, there is a unique $\mathbb{Z}_2$-extension K_∞/K which is unramified outside $\mathfrak{p}$, and we write K_n for the unique intermediate field with $[K_n : K] = 2^n$, and $\mathcal{O}_{K_n}$ for the ring of integers of K_n. Throughout, we assume that $\mathfrak{p}$ corresponds to the embedding $\iota_\mathfrak{p} : K \to \mathbb{Q}_2$ determined

2010 *Mathematics Subject Classification*: 11R23, 11G05.
Key words and phrases: Iwasawa theory, Selmer groups, elliptic curves.

by $\iota_{\mathfrak{p}}(\sqrt{-q}) \equiv 1 \bmod 4\mathbb{Z}_2$. For each prime $\mathfrak{w}$ of K, we write $\mathrm{ord}_{\mathfrak{w}}$ for the normalized additive valuation at $\mathfrak{w}$. Also, put $\mathfrak{q} = \sqrt{-q}\mathcal{O}_K$.

In all that follows, R will denote any element of $\mathcal{O}_K$, which will always be assumed to satisfy the following:

Twisting Hypothesis We have $R \equiv 1 \bmod 4\mathcal{O}_K$, $(\mathfrak{q}, R) = 1$, and $\mathrm{ord}_{\mathfrak{w}}(R)$ is odd for each prime $\mathfrak{w}$ of K dividing R.

We then define

$$F = K(\sqrt{-\sqrt{-q}R}), \quad F' = K(\sqrt{\sqrt{-q}R}), \quad D = K(\sqrt{-1}), \quad J = FF' = FD. \tag{1.1}$$

For any finite extension T/K, let

$$T_n = TK_n, \quad T_\infty = TK_\infty.$$

Further, let $M(T_\infty)$ be the maximal abelian 2-extension of T_∞, which is unramified outside the primes of T_∞ lying above $\mathfrak{p}$, and let

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

Then the main result of this paper is as follows.

THEOREM 1.1. *Let $s_\infty(R)$ be the number of primes of K_∞ dividing $\sqrt{-q}R$, where R satisfies the above Twisting Hypothesis. Then (i) $X(F_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module of exact rank $s_\infty(R) - 1$; and (ii) if $q \equiv 7 \bmod 16$, then $X(F'_\infty)$ (resp. $X(J_\infty)$) is a free finitely generated $\mathbb{Z}_2$-module of exact rank $s_\infty(R)$ (resp. $2s_\infty(R) - 1$).*

We point out that the number $s_\infty(R)$ is finite and can be computed explicitly as follows. Let h be the class number of K, which is odd. Suppose $\mathfrak{w}$ is a prime of K distinct from $\mathfrak{p}$. Then $\mathfrak{w}^h = (w)$ is principal. Adjust the sign of w so that $\iota_{\mathfrak{p}}(w) \equiv 1 \bmod 4\mathbb{Z}_2$. Then, by class field theory (see the proof of Lemma 2.3 of [4] or of Lemma 3.3 of [3]), the number of primes of K_∞ dividing $\mathfrak{w}$ is

$$2^{\mathrm{ord}_2(\iota_{\mathfrak{p}}(w)-1)-2}.$$

It follows that if $q \equiv 7 \bmod 16$ and $R = 1$, we have $s_\infty(R) = 1$ whence $X(J_\infty)$ is a free $\mathbb{Z}_2$-module of rank 1. This recovers [4, Theorem 1.1]. It was proven in [10] that $X(F_\infty) \neq 0$ when $q \equiv 15 \bmod 16$ and $R = 1$, but the methods there are different from those of the present paper. The fact that $X(F_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module of $\mathbb{Z}_2$-rank at most $s_\infty(R) - 1$ has been proven when $q = 7$ in [1], and the argument extends easily to the more general case considered here. In particular, it can be proved in this way that $X(D_\infty) = 0$ when $q \equiv 7 \bmod 16$ (see [4, Proposition 2.2] or Proposition 3.2 in the present paper).

As we shall explain in §4, Theorem 1.1 has an equivalent formulation in terms of a certain Selmer group arising from infinite descent on the h-dimensional abelian variety which is the twist by the quadratic extension $K(\sqrt{R})/K$ of the abelian variety B/K; here B/K is the restriction of scalars from the Hilbert class field H of K to K of the Gross elliptic curve A/H with complex multiplication by $\mathcal{O}_K$ [8]. It seems that no such clear cut result giving the exact $\mathbb{Z}_2$-corank of Selmer groups of a large family of quadratic twists of an abelian variety over a $\mathbb{Z}_2$-extension of the base field was known previously. In §5, we shall discuss more on the case $s_\infty(R) = 2$ where R is a square free rational integer satisfying the Twisting Hypothesis.

2. Prelimaries

For this section alone, we consider a more general situation than in the rest of the paper. Take p to be an arbitrary prime number, and take K to be any imaginary quadratic field in which p splits. We fix one of the primes $\mathfrak{p}$ of K above lying above p. By class field theory, there is a unique $\mathbb{Z}_p$-extension K_∞ of K which is unramified outside $\mathfrak{p}$. If W/K is any finite extension, we define $W_\infty = WK_\infty$. Let $M(W_\infty)$ be the maximal abelian p-extension of W_∞, which is unramified outside the primes lying above $\mathfrak{p}$, and put $X(W_\infty) = \mathrm{Gal}(M(W_\infty)/W_\infty)$. Again by class field theory, we have:

LEMMA 2.1. *There are only finitely many primes of W_∞ lying above each prime of W.*

For each finite extension $\mathfrak{W}/W$, we define $S_\infty(\mathfrak{W}/W)$ to be the set of primes of W_∞, which do not lie above $\mathfrak{p}$, and which are ramified in $\mathfrak{W}_\infty$. Of course, $S_\infty(\mathfrak{W}/W)$ is a finite set by Lemma 2.1. Put

$$s_\infty(\mathfrak{W}/W) = \#(S_\infty(\mathfrak{W}/W)). \tag{2.1}$$

Assume that $\mathfrak{W}/W$ is a cyclic extension of degree p with $\mathfrak{W} \not\subset W_\infty$. Thus $\mathfrak{W}_\infty/W_\infty$ is cyclic of degree p, and we put $\Delta = \mathrm{Gal}(\mathfrak{W}_\infty/W_\infty)$, As usual, $X(\mathfrak{W}_\infty)$ has its natural structure as a module over the group ring $\mathbb{Z}_p[\Delta]$. The maximal ideal of the local ring $\mathbb{Z}_p[\Delta]$ is $(p, \delta - 1)$, and its residue field is the finite field $\mathbb{F}_p$ with p elements; here δ is any generator of Δ. If X is a $\mathbb{Z}_p[\Delta]$-module, put $X_\Delta = X/(\delta - 1)X$.

LEMMA 2.2. *Let $\mathfrak{W}/W$ be a cyclic extension of degree p with $\mathfrak{W} \not\subset W_\infty$. Then (i) $X(\mathfrak{W}_\infty)$ is finitely generated as a $\mathbb{Z}_p$-module if and only if $X(W_\infty)$ is finitely generated as a $\mathbb{Z}_p$-module, (ii) if $X(W_\infty) = 0$, then $(X(\mathfrak{W}_\infty))_\Delta$ is an $\mathbb{F}_p$-vector space of dimension at most $s_\infty(\mathfrak{W}/W) - 1$, and (iii) the restriction map induces an isomorphism $(X(\mathfrak{W}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)_\Delta \cong X(W_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.*

PROOF. If $X(\mathfrak{W}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, so is its quotient $\mathrm{Gal}(\mathfrak{W}_\infty M(W_\infty)/\mathfrak{W}_\infty)$. Since $[\mathfrak{W}_\infty : W_\infty]$ is finite, it follows that the abelian group $\mathrm{Gal}(\mathfrak{W}_\infty M(W_\infty)/W_\infty)$ is finitely generated over $\mathbb{Z}_p$, and hence so is its quotient

$X(W_\infty)$. Conversely, assume that $X(W_\infty)$ is finitely generated over $\mathbb{Z}_p$, and let T denote the maximal abelian extension of W_∞ contained in $M(\mathfrak{W}_\infty)$. Then we have an isomorphism

$$X(\mathfrak{W}_\infty)_\Delta \cong \mathrm{Gal}(T/\mathfrak{W}_\infty). \tag{2.2}$$

Now $M(W_\infty)$ is a subfield of T, and $\mathrm{Gal}(T/M(W_\infty))$ is generated by the inertial subgroups of the primes in $S_\infty(\mathfrak{W}/W)$ in the extension T/W_∞. Such an inertial subgroup is of order p since we are assuming that $\mathfrak{W}_\infty/W_\infty$ is of degree p. Thus $\mathrm{Gal}(T/M(W_\infty))$ is an $\mathbb{F}_p$-vector space, and

$$\dim_{\mathbb{F}_p} \mathrm{Gal}(T/M(W_\infty)) \leq s_\infty(\mathfrak{W}/W). \tag{2.3}$$

Since we are assuming that $X(W_\infty)$ is finitely generated over $\mathbb{Z}_p$, and the set $S_\infty(\mathfrak{W}/W)$ is finite, it follows easily that $\mathrm{Gal}(T/\mathfrak{W}_\infty)$ is finitely generated over $\mathbb{Z}_p$. Thus, in view of (2.2), $X(\mathfrak{W}_\infty)/(p, \delta - 1)X(\mathfrak{W}_\infty)$ is a finite dimensional $\mathbb{F}_p$-vector space. Since $X(\mathfrak{W}_\infty)$ is a compact $\mathbb{Z}_p[\Delta]$-module, it follows from Nakayama's lemma that $X(\mathfrak{W}_\infty)$ is a finitely generated $\mathbb{Z}_p[\Delta]$-module, whence it is also finitely generated as a $\mathbb{Z}_p$-module. This completes the proof of (i). For (ii), when $X(W_\infty) = 0$, (2.3) becomes $\dim_{\mathbb{F}_p} \mathrm{Gal}(T/W_\infty) \leq s_\infty(\mathfrak{W}/W)$, whence $\dim_{\mathbb{F}_p} \mathrm{Gal}(T/\mathfrak{W}_\infty) \leq s_\infty(\mathfrak{W}/W) - 1$. Recalling (2.2), the assertion (ii) follows. To prove (iii), we first note that (2.2) implies that we have the exact sequence

$$1 \to X(\mathfrak{W}_\infty)_\Delta \to \mathrm{Gal}(T/W_\infty) \to \mathrm{Gal}(\mathfrak{W}_\infty/W_\infty) \to 1.$$

We also have the exact sequence

$$1 \to \mathrm{Gal}(T/M(W_\infty)) \to \mathrm{Gal}(T/W_\infty) \to X(W_\infty) \to 1.$$

Since $\mathrm{Gal}(\mathfrak{W}_\infty/W_\infty)$ and $\mathrm{Gal}(T/M(W_\infty))$ are both finite, it follows that

$$(X(\mathfrak{W}_\infty)_\Delta) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong X(W_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

This completes the proof. □

Corollary 2.3. *If $\mathfrak{W}/W$ is a finite Galois extension of p-power degree, then $X(\mathfrak{W}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module if and only if $X(W_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.*

This is immediate because any finite p-group is solvable.

Lemma 2.4. *Let Δ be a cyclic group of order p. Let Y be a free $\mathbb{Z}_p$-module of finite rank, which is also a Δ-module. Assume that $Y_\Delta = (\mathbb{Z}/p\mathbb{Z})^r$ for some integer $r \geq 0$. Then (i) $N_\Delta(Y) = 0$, where $N_\Delta = \sum_{\tau \in \Delta} \tau$, whence Y is a $\mathbb{Z}_p[\Delta]/(N_\Delta)$-module, and (ii) Y is a quotient of $\mathbb{Z}_p^{(p-1)r}$ for any prime p, and $Y \cong \mathbb{Z}_2^r$ when $p = 2$.*

Proof. The proof, which the authors attribute to Sharifi, is entirely similar to the case $p = 2$ given in [3, Lemma 2.8]. □

Combining Lemmas 2.2 and 2.4, we immediately obtain:

LEMMA 2.5. *Let $\mathfrak{W}/W$ be a cyclic extension of degree p. Assume that $X(W_\infty) = 0$, and that $X(\mathfrak{W}_\infty)$ is a torsion free $\mathbb{Z}_p$-module. Then $X(\mathfrak{W}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module of rank at most $(p-1)(s_\infty(\mathfrak{W}/W) - 1)$.*

For a finitely generated $\mathbb{Z}_p$-module Y, we write $t_p(Y)$ for its $\mathbb{Z}_p$-rank. In our applications, we only need the following lemma for the prime $p = 2$.

LEMMA 2.6. *Assume that $p = 2$, and let W be any finite extension of K such that $X(W_\infty)$ is a finitely generated $\mathbb{Z}_2$-module. Take $\mathfrak{M}$ to be any Galois extension of W with $\mathrm{Gal}(\mathfrak{M}/W) \cong \mathrm{Gal}(\mathfrak{M}_\infty/W_\infty) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Then*

$$t_2(X(\mathfrak{M}_\infty)) + 2t_2(X(W_\infty)) = \sum_{i=1}^{3} t_2(X(\mathfrak{W}_{i,\infty})),$$

where $\mathfrak{W}_1, \mathfrak{W}_2, \mathfrak{W}_3$ are the three quadratic extensions of W contained in $\mathfrak{M}$.

PROOF. Since we are assuming that $X(W_\infty)$ is a finitely generated $\mathbb{Z}_2$-module, the same is true for $X(\mathfrak{M}_\infty)$ because $\mathrm{Gal}(\mathfrak{M}/W)$ is a 2-group. Let $V = X(\mathfrak{M}_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$, so that the $\mathbb{Q}_2$-dimension of V is equal to $t_2(X(\mathfrak{M}_\infty))$. Put $\Omega = \mathrm{Gal}(\mathfrak{M}_\infty/W_\infty)$. Then

$$V = \oplus_\chi V^{e_\chi},$$

where the sum runs over the characters χ of Ω, and $e_\chi = \sum_{\sigma\in\Omega} \chi(\sigma)\sigma$. Thus we must compute the $\mathbb{Q}_2$-dimension of each V^{e_χ}. Note that if Y is any vector space over $\mathbb{Q}_2$ and g is the non-identity element of a group Δ of order 2 acting on Y, then plainly

$$Y = Y^{1+g} \oplus Y^{1-g},\ (Y)_\Delta = Y^{1+g}. \tag{2.4}$$

Suppose first that χ is the trivial character of Ω, so that $e_\chi = (1+\sigma)(1+\tau)$, where, of course, σ and τ are distinct elements Ω of exact order 2. By (2.4) and (iii) of Lemma 2.2 applied to the group $\langle\sigma\rangle$ of order 2, we conclude that $V^{1+\sigma} = X(T_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$, where T_∞ is the fixed field of σ. Thus

$$V^\chi = (X(T_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2)^{1+\tau} = X(W_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2;$$

here the second equality follows from applying the remark (2.4) and (iii) of Lemma 2.2 to the quadratic extension T_∞/W_∞. Hence in this case the $\mathbb{Q}_2$-dimension of V^χ is equal to the $\mathbb{Q}_2$-dimension of $X(W_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. Suppose next that χ is a nontrivial character of Ω, say with $\chi(\sigma) = 1$ and $\chi(\tau) = -1$, so that $e_\chi = (1+\sigma)(1-\tau)$. If T is now the fixed field of $\mathrm{Ker}(\chi) = \{1, \sigma\}$, we again conclude from the remark (2.4) and (iii) of Lemma 2.2 that $V^{1+\sigma} = X(T_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$, whence

$$V^{e_\chi} \cong (X(T_\infty) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2)^{1-\tau}.$$

But applying (iii) of Lemma 2.2 to the extension T_∞/W_∞, we conclude that

$$X(T_\infty)\otimes_{\mathbb{Z}_2}\mathbb{Q}_2/(X(T_\infty)\otimes_{\mathbb{Z}_2}\mathbb{Q}_2)^{1-\tau}=X(W_\infty)\otimes_{\mathbb{Z}_2}\mathbb{Q}_2,$$

whence it follows that the $\mathbb{Q}_2$-dimension of V^{e_χ} is equal to the $\mathbb{Q}_2$-dimension of $X(T_\infty)\otimes_{\mathbb{Z}_2}\mathbb{Q}_2$ minus the $\mathbb{Q}_2$-dimension of $X(W_\infty)\otimes_{\mathbb{Z}_2}\mathbb{Q}_2$. Since this holds for each of the three non-trivial characters of Ω, the proof of Lemma 2.6 is now complete. □

3. Proof of Theorem 1.1

We now return to the situation discussed in §1. Thus from now on $K=\mathbb{Q}(\sqrt{-q})$, where q is any prime with $q\equiv 7 \bmod 8$, and again the fields F, F', D, J are defined by (1.1). As always, $\mathfrak{p}$ will denote one of the primes of K lying above 2, and we again fix the sign of $\sqrt{-q}$ so that $\sqrt{-q}\equiv 1 \bmod \mathfrak{p}^2$. Recall that, for each finite extension W/K, the integer $s_\infty(W/K)$ is defined by (2.1) in §2. Again R will denote an arbitrary element of $\mathcal{O}_K$ satisfying the Twisting Hypothesis, and $s_\infty(R)$ will denote the number of primes of K_∞ dividing $\sqrt{-q}R$.

Lemma 3.1. *We have $s_\infty(F/K)=s_\infty(R)$ for all primes $q\equiv 7 \bmod 8$. Moreover, if $q\equiv 7 \bmod 16$, we also have $s_\infty(F'/K)=s_\infty(R)+1$ and $s_\infty(D/K)=1$.*

Proof. The first assertion is clear because the primes of K_∞, not lying above $\mathfrak{p}$, which ramify in F_∞ are precisely the primes dividing $\sqrt{-q}R$. Note that $\mathfrak{p}^*$ is ramified in F'/K and in D/K by our choice of sign. Then the second assertion follows from the fact that $\mathfrak{p}^*$ is inert in K_∞ when $q\equiv 7 \bmod 16$ (see [4, Proposition 2.4]). □

Proposition 3.2 (Choi-Coates[1]). *(i) $X(F_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module of rank at most $s_\infty(R)-1$, and (ii) if $q\equiv 7 \bmod 16$, then $X(D_\infty)=0$ and $X(F'_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module of rank at most $s_\infty(R)$.*

Proof. It is easy to see $X(K_\infty)=0$ (for example see [3, Lemma 3.2]). Then by Lemma 2.2 $X(F_\infty)$, $X(D_\infty)$ and $X(F'_\infty)$ are all finitely generated over $\mathbb{Z}_2$. Moreover, by Greenberg's theorem [7, p.94], they are torsion-free whence are free of finite rank. The assertions then follow from Lemma 3.1 and Lemma 2.5. □

Proposition 3.3. *Let $\mathfrak{C}_n$ be the ray class group of K_n modulo $(\mathfrak{p}^*)^2\mathcal{O}_{K_n}$. Then $\mathfrak{C}_n$ has odd order for all $n\geq 0$.*

Before giving the proof, we recall Chevalley's formula for ray class groups (see [6] or [11, §4], for example). Suppose that L/k is any cyclic extension of number fields with Galois group G, and write $\mathcal{O}_L$ (resp. $\mathcal{O}_k$) for the ring of integers of L (resp. k). For our application, we may assume that k has no real places. If $\mathfrak{m}$ is an integral ideal in k, let $\mathrm{Cl}_L^{\mathfrak{m}}$ (resp. $\mathrm{Cl}_k^{\mathfrak{m}}$) denote the ray class group of L (resp. k) modulo $\mathfrak{m}\mathcal{O}_L$ (resp. $\mathfrak{m}$). Clearly $\mathrm{Cl}_L^{\mathfrak{m}}$ is a G-module, and $(\mathrm{Cl}_L^{\mathfrak{m}})^G$ will denote, as always, its G-invariants. For a prime v (resp. w) of k (resp. L), write $\mathcal{O}_v$ (resp. $\mathcal{O}_w$) for the ring of integers

of the completion k_v (resp. L_w). Let $L^{\mathfrak{m}}$ denote the set of all $a \in L^\times$ such that $\mathrm{ord}_w(a-1) \geq \mathrm{ord}_w(\mathfrak{m})$ for all places w of L dividing $\mathfrak{m}$. Let $\mathcal{O}_{k,\mathfrak{m}}^\times$ be the subgroup of the unit group $\mathcal{O}_k^\times$ of k consisting of all units a with $\mathrm{ord}_v(a-1) \geq \mathrm{ord}_v(\mathfrak{m})$ at all places v of k dividing $\mathfrak{m}$. Then Chevalley's formula with respect to L/k and the ideal $\mathfrak{m}$ is as follows:

$$\frac{\#((\mathrm{Cl}_L^{\mathfrak{m}})^G)}{\#(\mathrm{Cl}_k^{\mathfrak{m}})} = \frac{\prod_{v|\mathfrak{m}} [1+\mathfrak{m}\mathcal{O}_v : N_{L_w/k_v}(1+\mathfrak{m}\mathcal{O}_w)] \cdot \prod_{v\nmid\mathfrak{m}} e_v}{[L:k][\mathcal{O}_{k,\mathfrak{m}}^\times : \mathcal{O}_{k,\mathfrak{m}}^\times \cap N_{L/k}(L^{\mathfrak{m}})]}; \tag{3.1}$$

here $N_{L/k}$ (resp. N_{L_w/k_v}) is the norm map for L/k (resp. L_w/k_v), and e_v is the ramification index of v in L. In the first product, w is an arbitrary place of L above v and the group $N_{L_w/k_v}(1+\mathfrak{m}\mathcal{O}_w)$ is independent of the choice of w. We have the following lemma on local units index:

LEMMA 3.4. *If k is a finite unramified extension of $\mathbb{Q}_2$, then for every $m \geq 2$ we have $N_{k/\mathbb{Q}_2}(1+2^m\mathcal{O}_k) = 1+2^m\mathbb{Z}_2$, where $\mathcal{O}_k$ is the ring of integers in k.*

PROOF. Let $\mathrm{Tr}_{k/\mathbb{Q}_2}$ be the trace map from k to $\mathbb{Q}_2$. Let log be the usual 2-adic logarithm map. It commutes with the Galois action. For $m \geq 2$, we then have a commutative diagram:

$$\begin{array}{ccc} 1+2^m\mathcal{O}_k & \xrightarrow{\log} & 2^m\mathcal{O}_k \\ {\scriptstyle N_{k/\mathbb{Q}_2}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{k/\mathbb{Q}_2}} \\ 1+2^m\mathbb{Z}_2 & \xrightarrow{\log} & 2^m\mathbb{Z}_2. \end{array}$$

The two horizontal maps are isomorphisms as $m \geq 2$. The right vertical map is a surjection because $k/\mathbb{Q}_2$ is unramified. The lemma then follows. □

PROOF OF PROPOSITION 3.3. We apply (3.1) with respect to the cyclic extension $(K_n/K, \mathfrak{m})$, with $\mathfrak{m} = (\mathfrak{p}^*)^2$. As $\mathcal{O}_{K,\mathfrak{m}}^\times = \{1\}$, then, if we write $v = \mathfrak{p}^*$, the formula gives

$$\#((\mathfrak{C}_n)^{\mathrm{Gal}(K_n/K)}) = \#(\mathfrak{C}_0) \cdot [1+\mathfrak{m}\mathcal{O}_v : N(1+\mathfrak{m}\mathcal{O}_w)] = \#(\mathfrak{C}_0).$$

The second equality follows from Lemma 3.4. Using the fact that the class number of K is odd, and that the units of K are $\{\pm 1\}$, it is readily verified that $\#(\mathfrak{C}_0)$ is odd. Therefore $\#(\mathfrak{C}_n)$ is odd by Nakayama's lemma, since $\mathrm{Gal}(K_n/K)$ is cyclic of order 2^n. □

Note: We sketch another proof of Proposition 3.3 which is pointed out to us by an anonymous referee. For each n, let L_n be the 2-ray class field modulo $(\mathfrak{p}^*)^2\mathcal{O}_{K_n}$, so that $Y_n := \mathrm{Gal}(L_n/K_n)$ is isomorphic to the 2-part of $\mathfrak{C}_n$ as $\mathrm{Gal}(K_n/K)$-modules. Since K_n/K_0 is unramified at $\mathfrak{p}^*$, by some local arguments (using Lemma 3.4 and the

functoriality in local class field theory), one can show that the conductor of L_0K_n/K_n is $(\mathfrak{p}^*)^2\mathcal{O}_{K_n}$. Then using the fact that K_n/K_0 unramified outside $\mathfrak{p}$ and is totally ramified at $\mathfrak{p}$, one can show that the restriction map $Y_n \to Y_0$ induces an isomorphism $(Y_n)_{\mathrm{Gal}(K_n/K_0)} \cong Y_0$ by a classical argument (see the proof of [4, Proposition 3.2] for example). As Y_0 is trivial, by Nakayama's lemma Y_n is trivial too.

Proof of Theorem 1.1. The part (i) is clear by Proposition 3.2. For part (ii), take n to be an integer which is sufficiently large to ensure that there are precisely $s_\infty(R)$ primes of K_n dividing $\sqrt{-q}R$. These primes are then all inert in K_∞. To simplify notation, we shall write $s = s_\infty(R)$ in the rest of this proof. We have

$$\sqrt{-q}R\mathcal{O}_{K_n} = \mathfrak{a}_1 \cdots \mathfrak{a}_s, \tag{3.2}$$

where each $\mathfrak{a}_i$ is the power of some prime ideal of K_n, and $(\mathfrak{a}_i, \mathfrak{a}_j) = 1$ when $i \neq j$. Note that the exponents to which these prime ideals occur in (3.2) are all odd by the definition of R and the fact $(\mathfrak{q}, R) = 1$. Write h' for the order of $\mathfrak{C}_n$, which is odd by Proposition 3.3. Thus there exist $\alpha_i \in \mathcal{O}_{K_n}$ such that

$$\mathfrak{a}_i^{h'} = (\alpha_i) \quad \text{and} \quad \alpha_i \equiv 1 \bmod (\mathfrak{p}^*)^2\mathcal{O}_{K_n} \quad \text{for } 1 \leq i \leq s-1.$$

We define

$$\alpha_s = \frac{(-\sqrt{-q}R)^{h'}}{\alpha_1 \cdots \alpha_{r-1}}. \tag{3.3}$$

Note that, thanks to the oddness of h' and our choice of the sign, we also have $\alpha_s \equiv 1 \bmod (\mathfrak{p}^*)^2\mathcal{O}_{K_n}$. Again because h' is odd, it follows that, for $1 \leq i \leq s$, the extension $K_n(\sqrt{\alpha_i})/K_n$ is quadratic and is ramified at the unique prime dividing α_i. Moreover, this extension is unramified at the primes above $\mathfrak{p}^*$, since it is obtained by adjoining a root of $x^2 - x + \frac{1-\alpha_i}{4}$ and this polynomial is separable modulo each prime of K_n above $\mathfrak{p}^*$. Define

$$T = K_\infty(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_s}). \tag{3.4}$$

Now $K_\infty(\sqrt{\alpha_i})/K_\infty$ is ramified at the unique prime dividing α_i, while it is unramified at the primes dividing α_j for $j \neq i$, whence it follows easily that $[T : K_\infty] = 2^s$, and

$$\mathrm{Gal}(T/K_\infty) \cong (\mathbb{Z}/2\mathbb{Z})^s.$$

Thanks again to the oddness of h', it follows from (3.3) that

$$F_\infty \subset T \quad \text{and} \quad \mathrm{Gal}(T/F_\infty) \cong (\mathbb{Z}/2\mathbb{Z})^{s-1}.$$

The extension T/F_∞ is unramified at primes not dividing $\mathfrak{p}\mathfrak{a}_1 \cdots \mathfrak{a}_s$, since T/K_∞ is. Moreover, T/F_∞ is also unramified at the prime dividing $\mathfrak{a}_i$ for $1 \leq i \leq s$, since from (3.4) the ramification index of this prime in T/K_∞ is clearly equal to 2, but F_∞/K_∞ is also ramified at this prime by Lemma 3.1. This proves $T \subset M(F_\infty)$.

Hence $X(F_\infty)$ has $(\mathbb{Z}/2\mathbb{Z})^{s-1}$ as a quotient, and so its $\mathbb{Z}_2$-rank must be at least $s-1$. Combining this with the upper bound given by Proposition 3.2, the proof of assertion (i) of Theorem 1.1 is complete.

Assume for the rest of the proof that $q \equiv 7 \bmod 16$. By Proposition 3.2, it suffices to construct $s+1$ independent quadratic extensions of F'_∞ contained in $M(F'_\infty)$. Define

$$T' = T(\sqrt{-1}) = K_\infty(\sqrt{-1}, \sqrt{\alpha_1}, \ldots, \sqrt{\alpha_s}).$$

Note that $T' \supset F'_\infty$. Since $F'(\sqrt{-1})/F'$ is unramified at $\mathfrak{p}$, we have $F'_\infty(\sqrt{-1}) \subset M(F'_\infty)$. Moreover, by the same argument as in the first paragraph, we have $T \subset M(F'_\infty)$. Thus $T' \subset M(F'_\infty)$, and so it remains to show that $[T' : F'_\infty] = 2^s$. Note that T/K_∞ is unramified at the unique prime above $\mathfrak{p}^*$, but $K_\infty(\sqrt{-1})/K_\infty$ is ramified at this prime. It follows that $T' \neq T$ whence $[T' : K_\infty] = 2^{s+1}$ and therefore $[T' : F'_\infty] = 2^s$. This proves $X(F'_\infty) \cong \mathbb{Z}_2^s$, as required.

Finally, since J/K is a biquadratic extension, with F, F' and D being the nontrivial intermediate fields, it follows from Lemma 2.6 and Proposition 3.2 that $X(J_\infty) \cong \mathbb{Z}_2^{2s-1}$. This completes the proof of Theorem 1.1. □

4. Equivalent formulation of Theorem 1.1 in terms of infinite descent on certain abelian varieties with complex multiplication

The aim of this section is to briefly explain an equivalent formulation of Theorem 1.1 in terms of infinite descent on a family of quadratic twists of a certain higher dimensional abelian variety with complex multiplication. We omit detailed proofs, and refer the reader to [3, 8] for further explanations of the background material. Fix an embedding of K in $\mathbb{C}$. Let $H = K(j(\mathcal{O}_K))$ be the Hilbert class field of K, where j is the classical modular function, and let $A/\mathbb{Q}(j(\mathcal{O}_K))$ be the Gross elliptic curve with complex multiplication by $\mathcal{O}_K$ (see [8], Chap. 5). Thus A has minimal discriminant $(-q^3)$, and A is isogenous over H to all of its conjugates. Let

$$B = \mathrm{Res}^H_K A$$

be the h-dimensional abelian variety over K which is the restriction of scalars of A from H to K. Let $\mathscr{B} = \mathrm{End}_K(B)$, and $\mathscr{T} = \mathscr{B} \otimes \mathbb{Q}$, so that $\mathscr{T}$ is a CM field of degree h over K. Then $\mathscr{B}$ is an order in $\mathscr{T}$, which is ramified over $\mathcal{O}_K$ at precisely the primes dividing h (see [8], Theorem 15.2.5). In particular, since h is odd, the primes $\mathfrak{p}$, and $\mathfrak{p}^*$ are both unramified in $\mathscr{T}$. Now the torsion subgroup of $B(K)$ is $\mathcal{O}_K/2\mathcal{O}_K$, and the action of $\mathscr{B}$ on this torsion subgroup gives an $\mathcal{O}_K$-algebra surjection from $\mathscr{B}$ onto $\mathcal{O}_K/2\mathcal{O}_K$, whose kernel is the product of two conjugate primes $\mathfrak{P}, \mathfrak{P}^*$ of $\mathscr{B}$ lying above $\mathfrak{p}, \mathfrak{p}^*$, respectively. These primes are both unramified in $\mathscr{B}$, and have residue fields equal to the field $\mathbb{F}_2$ with 2 elements. Our equivalent formulation of Theorem 1.1 will be in terms of the arithmetic of the abelian variety $B^{(R)}/K$, which is the twist

of B by the quadratic extension $K(\sqrt{R})/K$. For each $n \geq 1$, let $B^{(R)}_{\mathfrak{P}^n}$ be the Galois module of $\mathfrak{P}^n$-division points on $B^{(R)}$. Then we have the following interpretation of the fields defined in §1.

THEOREM 4.1. *We have*

$$F = K(B^{(R)}_{\mathfrak{P}^2}), \quad F' = K(B^{(R)}_{\mathfrak{P}^{*2}}), \quad J = FF' = K(B^{(R)}_{\mathfrak{P}^2}, \sqrt{-1}),$$
$$F_\infty = K(B^{(R)}_{\mathfrak{P}^\infty}), \quad J_\infty = K(B^{(R)}_{\mathfrak{P}^\infty}, \sqrt{-1}).$$

Moreover, $B^{(R)}$ has good reduction everywhere over F and F'.

We omit the detailed proofs, which are similar to those given in [3] for the abelian variety B (see [3, §2 and Lemma 7.11] and also see [1, Lemma 2.1, 2.2]).

We next recall the definition of the $\mathfrak{P}^\infty$-Selmer group of $B^{(R)}$ over an algebraic extension of K. Take any non-zero endomorphism π in $\mathscr{B}$ such that the ideal factorization of π in the ring of integers of $\mathscr{T}$ is equal to $\mathfrak{P}^r$ for some integer $r \geq 1$. Let L be any algebraic extension of K. Then for each integer $n \geq 1$, the group $\mathrm{Sel}_{\pi^n}(B^{(R)}/L)$ is defined by

$$\mathrm{Sel}_{\pi^n}(B^{(R)}/L) = \mathrm{Ker}(H^1(L, B^{(R)}_{\pi^n}) \to \prod_v H^1(L_v, B^{(R)})),$$

where v runs over all finite places of L, and L_v is the compositum of the completions at v of all finite extensions of K contained in L. Passing to the inductive limit over all $n \geq 1$, and noting that $B^{(R)}_{\pi^\infty} = B^{(R)}_{\mathfrak{P}^\infty}$ as Galois modules, we then define the Selmer group $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/L)$ to be the inductive limit of the $\mathrm{Sel}_{\pi^n}(B^{(R)}/L)$, so that:

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/L) = \mathrm{Ker}(H^1(L, B^{(R)}_{\mathfrak{P}^\infty}) \to \prod_v H^1(L_v, B^{(R)})).$$

Since $B^{(R)}$ has good reduction everywhere over F, and $F_\infty = K(B^{(R)}_{\mathfrak{P}^\infty})$, it is then easily seen that we have (see [3, Theorem 3.9] and [2]):

THEOREM 4.2. *As Galois modules, we have*

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty) = \mathrm{Hom}(X(F_\infty), B^{(R)}_{\mathfrak{P}^\infty}), \ \ \mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/J_\infty) = \mathrm{Hom}(X(J_\infty), B^{(R)}_{\mathfrak{P}^\infty}),$$

Noting that $B^{(R)}_{\mathfrak{P}^\infty} = \mathscr{T}_\mathfrak{P}/\mathscr{B}_\mathfrak{P} = \mathbb{Q}_2/\mathbb{Z}_2$ as abelian groups, we immediately obtain the following equivalent form of Theorem 1.1.

THEOREM 4.3. *As abelian groups, we have (i)* $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty) = (\mathbb{Q}_2/\mathbb{Z}_2)^{s_\infty(R)-1}$, *and (ii) if* $q \equiv 7 \bmod 16$, $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/J_\infty) = (\mathbb{Q}_2/\mathbb{Z}_2)^{2s_\infty(R)-1}$ *for all R satisfying the Twisting Hypothesis, and where $s_\infty(R)$ is the number of primes of K_∞ dividing $\sqrt{-q}R$.*

Let $\mathfrak{F}$ denote either of the fields F or J. We recall that the Tate-Shafarevich group $Ш(B^{(R)}/\mathfrak{F}_\infty)$ of $B^{(R)}/\mathfrak{F}_\infty$ is defined by

$$Ш(B^{(R)}/\mathfrak{F}_\infty) = \mathrm{Ker}(H^1(\mathfrak{F}_\infty, B^{(R)}) \to \prod_v H^1(\mathfrak{F}_{\infty,v}, B^{(R)})).$$

It is a $\mathscr{B}$-module and we write $Ш(B^{(R)}/\mathfrak{F}_\infty)(\mathfrak{P}^\infty)$ for its $\mathfrak{P}$-primary subgroup. Note also that the group $B^{(R)}(\mathfrak{F}_\infty)$ of $\mathfrak{F}_\infty$-rational points of $B^{(R)}$ has a natural structure as an $\mathscr{B}$-module, and we have the exact sequence

$$0 \to B^{(R)}(\mathfrak{F}_\infty) \otimes_{\mathscr{B}} (\mathscr{T}_\mathfrak{P}/\mathscr{B}_\mathfrak{P}) \to \mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/\mathfrak{F}_\infty) \to Ш(B^{(R)}/\mathfrak{F}_\infty)(\mathfrak{P}^\infty) \to 0. \quad (4.1)$$

Thus Theorem 4.3 can be reformulated as follows. Define $g_{\mathfrak{F}_\infty}(R)$ to be the $\mathscr{T}$-dimension of $B^{(R)}(\mathfrak{F}_\infty) \otimes_\mathbb{Z} \mathbb{Q}$. Now $Ш(B^{(R)}/\mathfrak{F}_\infty)(\mathfrak{P}^\infty)$ is a divisible group thanks to Theorem 4.2, the fact that $X(\mathfrak{F}_\infty)$ is a free finitely generated $\mathbb{Z}_2$-module, and the exact sequence (4.1), whence we define $e_{\mathfrak{F}_\infty}(R)$ to be its $\mathbb{Z}_2$-corank.

THEOREM 4.4. *For all R satisfying the Twisting Hypothesis, we have (i) $g_{F_\infty}(R) + e_{F_\infty}(R) = s_\infty(R) - 1$, and (ii) if $q \equiv 7 \bmod 16$, $g_{J_\infty}(R) + e_{J_\infty}(R) = 2s_\infty(R) - 1$, where we recall that $g_{\mathfrak{F}_\infty}(R)$ is the $\mathscr{T}$-dimension of $B^{(R)}(\mathfrak{F}_\infty) \otimes_\mathbb{Z} \mathbb{Q}$, $e_{\mathfrak{F}_\infty}(R)$ is the $\mathbb{Z}_2$-corank of $Ш(B^{(R)}/\mathfrak{F}_\infty)(\mathfrak{P}^\infty)$, and, as always, $s_\infty(R)$ is the number of primes of K_∞ dividing $\sqrt{-q}R$.*

Since $s_\infty(R)$ is very easy to calculate explicitly, it seems to us that no simple explicit general result like Theorems 4.3 and 4.4 was known previously in the Iwasawa theory of elliptic curves. As an illustration, at the end of the next section we apply these theorems to one numerical example taken from [1], with $s_\infty(R) = 4, g_{F_\infty}(R) = 2, e_{F_\infty}(R) = 1$.

5. Applications of Theorem 1.1

In this last section, we discuss the situation when R is a square free rational integer satisfying the Twisting Hypothesis, and having the property that $s_\infty(R) = 2$ (the case when $s_\infty(R) = 1$ is already discussed fully in [4]). We also discuss one numerical example with $s_\infty(R) = 4$. The following lemma is clear from the remarks made immediately after the statement of Theorem 1.1.

LEMMA 5.1. *Assume that R is a square free rational integer satisfying the Twisting Hypothesis. Then $s_\infty(R) = 2$ if and only if one of the following three cases hold: (i) we have $q \equiv 15 \bmod 32$ and $R = 1$, (ii) we have $q \equiv 7 \bmod 16$ and $R = r$, where r is a prime with $r \equiv 5 \bmod 8$, which is inert in K, or (iii) we have $q \equiv 7 \bmod 16$ and $R = -r$, where r is a prime with $r \equiv 3 \bmod 8$, which is inert in K.*

By Theorem 4.3, we know that, whenever $s_\infty(R) = 2$, we have $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty) = \mathbb{Q}_2/\mathbb{Z}_2$ as an abelian group. For each $n \geq 0$, recall that K_n is the

n-th layer of the $\mathbb{Z}_2$-extension K_∞/K. The cases $(i), (ii), (iii)$ of the next theorem refer to the three cases of Lemma 5.1.

THEOREM 5.2. *In cases (i) and (ii), we have* $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K)$ *is finite. Moreover, either* $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n)$ *is finite for all* $n \geq 1$*, or* $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n)$ *has* $\mathbb{Z}_2$*-corank equal to 1 for all* $n \geq 1$*, according as* $L(B^{(R)}/K_1) \neq 0$ *or* $L(B^{(R)}/K_1) = 0$*. In case (iii), we have* $L(B^{(R)}/K) = 0$ *and* $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n)$ *has* $\mathbb{Z}_2$*-corank equal to 1 for all* $n \geq 0$*.*

We now outline the proof of this theorem, again referring to [3] for similar detailed arguments. We begin by recalling an elementary purely algebraic lemma, which holds for any R in $\mathcal{O}_K$ satisfying the Twisting Hypothesis. Put $\Gamma = \mathrm{Gal}(F_\infty/F)$, $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$, and fix any topological generator γ of Γ. Let $\Lambda(\Gamma)$ be the Iwasawa algebra of Γ with coefficients in $\mathbb{Z}_2$. As usual, we identify $\Lambda(\Gamma)$ with the formal power series ring $\mathbb{Z}_2[[T]]$ by mapping γ to $1+T$. Since $X(F_\infty)$ is a finitely generated $\mathbb{Z}_2$-module, it is clearly a torsion $\Lambda(\Gamma)$-module, and we write $c_{F_\infty}(T)$ for its characteristic power series. By Theorem 4.1, we have a character $\kappa : \Gamma \to 1 + \mathfrak{P}^2\mathscr{B}_{\mathfrak{P}} = 1 + 4\mathbb{Z}_2$ giving the action of Γ on $B^{(R)}_{\mathfrak{P}^\infty}$ and we define $u = \kappa(\gamma)$.

LEMMA 5.3. *For each* R *in* $\mathcal{O}_K$ *satisfying the Twisting Hypothesis,* $(\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty))^{\Gamma_n}$ *is infinite for some integer* $n \geq 0$ *if and only if* $c_{F_\infty}(u\zeta - 1) = 0$ *for some* 2^n*-th power root of unity* ζ*. Assume further* $s_\infty(R) = 2$*; we have that if* $(\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty))^{\Gamma_n}$ *is finite for* $n = 0, 1$*, then it is finite for each* $n \geq 0$*.*

PROOF. Put $\gamma_n = \gamma^{2^n}$, so that γ_n is a topological generator of Γ_n, $\gamma_n = (1+T)^{2^n}$ and $\kappa(\gamma_n) = u^{2^n}$. Write $X = X(F_\infty)$ in this proof. By Theorem 4.2, we have

$$(\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty))^{\Gamma_n} = \mathrm{Hom}(X/(\gamma_n - \kappa(\gamma_n))X, B^{(R)}_{\mathfrak{P}^\infty}).$$

Thus, the left hand side is finite if and only if $X/(\gamma_n - \kappa(\gamma_n))X$ is finite. Note that

$$\gamma_n - \kappa(\gamma_n) = (1+T)^{2^n} - u^{2^n} = \prod_\zeta (T - (u\zeta - 1)),$$

where ζ runs over all the 2^n-th power of roots unity. Since $c_{F_\infty}(T)$ is the characteristic power series of X, it follows that $X/(\gamma_n - \kappa(\gamma_n))X$ is finite if and only if $c_{F_\infty}(T)$ is coprime to $T - (u\zeta - 1)$ for each ζ. This proves the first part of Lemma 5.3.

Now we turn to prove the second part. By the Weierstrass Preparation Theorem, we may assume that $c_{F_\infty}(T) \in \mathbb{Z}_2[T]$ is a polynomial of degree 1 as $X(F_\infty)$ is of rank 1 by Theorem 1.1. Suppose that the assertion does not hold. Take $n \geq 2$ be the smallest integer such that $(\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty))^{\Gamma_n}$ is infinite. It follows that $c_{F_\infty}(T)$ is divisible by $T - (u\zeta - 1)$ for some primitive 2^n-th root of unit ζ. Since $c_{F_\infty}(T) \in \mathbb{Z}_2[[T]]$, it is divisible by the 2^{n-1} conjugates of $T - (u\zeta - 1)$. Thus, we have $2^{n-1} \leq 1$, namely $n = 0$ or 1. This contradicts our assumption. □

In addition, we have the following arithmetic lemma. For each algebraic extension L/K, we define

$$\mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/L) = \mathrm{Ker}(H^1(L, B^{(R)}_{\mathfrak{P}^\infty}) \to \prod_{v \nmid \mathfrak{p}} H^1(L_v, B^{(R)})).$$

Recall that $F_n = FK_n$ for $n \geq 0$.

LEMMA 5.4. *For each R in $\mathcal{O}_K$ satisfying the Twisting Hypothesis, and for all $n \geq 0$, $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n)$ has the same $\mathbb{Z}_2$-corank as $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_n) = (\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty))^{\Gamma_n}$.*

PROOF. Since $B^{(R)}$ has good reduction everywhere over F, entirely similar arguments to those given in §3 of [3] show that

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty) = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty),$$

and that Δ acts trivially on $\mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty)$, where $\Delta = \mathrm{Gal}(F_\infty/K_\infty)$. Since $B^{(R)}$ has good reduction everywhere over F, the same argument as in the proof of Proposition 3.11 of [3] shows that

$$(\mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty))^{\Gamma_n} = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_n)$$

for all $n \geq 0$. Thus to complete the proof, it suffices to show that the natural map

$$\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n) \to (\mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_n))^{\Delta} = \mathrm{Sel}'_{\mathfrak{P}^\infty}(B^{(R)}/F_n)$$

has finite kernel and cokernel for all $n \geq 0$. But this follows easily from the fact that Δ is of order 2 by the inflation-restriction sequence. □

For each $n \geq 0$, let $L(B^{(R)}/F_n, s)$ (resp. $L(B^{(R)}/K_n, s)$) be the complex L-series of $B^{(R)}/F_n$ (resp. $B^{(R)}/K_n$). Let χ_n be the non-trivial character of $\mathrm{Gal}(F_n/K_n)$, and write $L(B^{(R)}/K_n, \chi_n, s)$ for the twist of $L(B^{(R)}/K_n, s)$ by χ_n. Then we have

$$L(B^{(R)}/F_n, s) = L(B^{(R)}/K_n, s)L(B^{(R)}/K_n, \chi_n, s).$$

THEOREM 5.5. *For all R in $\mathcal{O}_K$ satisfying the Twisting Hypothesis, and all $n \geq 0$, we have $L(B^{(R)}/K_n, \chi_n, 1) \neq 0$, and so $L(B^{(R)}/F_n, 1) \neq 0$ if and only if $L(B^{(R)}/K_n, 1) \neq 0$.*

PROOF. This theorem, which is valid for all primes $q \equiv 7 \bmod 8$ is an equivalent form of Theorem 1.5 of [3]. Put $\beta = \sqrt{-q}$. Now $L(B^{(R)}/K_n, \chi_n, s)$ is the complex L-series of the twist of $B^{(R)}$ by the quadratic extension F_n/K_n. As $F_n = K_n(\sqrt{-\beta R})$, it follows that the twist of $B^{(R)}$ by F_n/K_n is just $B^{(-\beta)}/K_n$. Put $H_n = HK_n$, where we recall that H is the Hilbert class field of K. Then the complex L-series of

$B^{(-\beta)}/K_n$ is the same as the complex L-series $L(A^{(-\beta)}/H_n, s)$ of $A^{(-\beta)}/H_n$, where A/H is the basic Gross $\mathbb{Q}$-curve defined over H. Since Theorem 1.5 of [3] asserts that $L(A^{(-\beta)}/H_n, 1) \neq 0$ for all $n \geq 0$, the proof is complete. □

The following deep theorem is a consequence of the main conjecture of Iwasawa theory for the $\mathbb{Z}_2$-extension F_∞/F. As above, $c_{F_\infty}(T)$ will denote a characteristic power series of the Γ-module $X(F_\infty)$.

THEOREM 5.6. *Let $n \geq 0$ be any non-negative integer, and let R in $\mathcal{O}_K$ satisfy the Twisting Hypothesis. Then $c_{F_\infty}(u\zeta - 1) \neq 0$ for all 2^n-th roots of unity ζ if and only if $L(B^{(R)}/F_n, 1) \neq 0$.*

Combining this result with Theorem 5.5 and Lemmas 5.3 and 5.4, we immediately obtain:

COROLLARY 5.7. *For all $n \geq 0$, we have $\mathrm{Sel}_{\mathfrak{p}^\infty}(B^{(R)}/K_n)$ is finite if and only if $L(B^{(R)}/K_n, 1) \neq 0$.*

Of course, this is not the place to give a detailed proof of this main conjecture. We simply say that similar methods, using the Euler system of elliptic units, to those used to prove Theorem 7.13 in §7 of [3], can be generalized to prove the desired main conjecture for $B^{(R)}/F_\infty$, from which the above theorem follows as an immediate corollary.

PROOF. We now prove Theorem 5.2. We first suppose we are in case (i), so that $q \equiv 15 \bmod 32$ and $R = 1$. By a theorem of Rohrlich [13], we have $L(B/K, 1) = L(A/H, 1) \neq 0$. Thus, by Corollary 5.7, $\mathrm{Sel}_{\mathfrak{p}^\infty}(B/K)$ is finite, and, for all $n \geq 1$, $\mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_n)$ is finite if and only if $L(B/K_n, 1) \neq 0$. Moreover, as $s_\infty(R) = 2$, it follows from Theorem 4.3 that $\mathrm{Sel}_{\mathfrak{p}^\infty}(B/F_\infty) = \mathbb{Q}_2/\mathbb{Z}_2$ as an abelian group, and so Lemma 5.4 implies that $\mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_n)$ has $\mathbb{Z}_2$-corank at most 1 for all $n \geq 1$. The assertion then follows from Lemma 5.3, completing the proof of case (i). Next suppose we are in the case (ii), so that $q \equiv 7 \bmod 16$ and $R = r$, with $r \equiv 5 \bmod 8$ and r inert in K. Then Theorem 1.3 of [3] shows that $L(B^{(R)}/K, 1) = L(A^{(R)}/H, 1) \neq 0$. Again invoking Corollary 5.7, it follows that $\mathrm{Sel}_{\mathfrak{p}^\infty}(B^{(R)}/K)$ is finite, and, for all $n \geq 1$, $\mathrm{Sel}_{\mathfrak{p}^\infty}(B^{(R)}/K_n)$ is finite if and only if $L(B^{(R)}/K_n, 1) \neq 0$. But $\mathrm{Sel}_{\mathfrak{p}^\infty}(B^{(R)}/F_\infty) = \mathbb{Q}_2/\mathbb{Z}_2$ as an abelian group, whence, again by Lemma 5.4, $\mathrm{Sel}_{\mathfrak{p}^\infty}(B^{(R)}/K_n)$ has $\mathbb{Z}_2$-corank at most 1 for all $n \geq 1$, and the proof of case (ii) is complete by Lemma 5.3. Finally, suppose we are in case (iii), so that $q \equiv 7 \bmod 16$ and $R = -r$, with $r \equiv 3 \bmod 8$ and r inert in K. Now $B^{(R)}$ is in fact defined over $\mathbb{Q}$, and $L(B^{(R)}/K, s) = L(B^{(R)}/\mathbb{Q}, s)^2$, where $L(B^{(R)}/\mathbb{Q}, s)$ is the complex L-series of $B^{(R)}/\mathbb{Q}$ (see §18 of [8]). Write

$$\Phi(B^{(R)}/\mathbb{Q}, s)) = (-qr/(2\pi))^{hs}\Gamma(s)^h L(B^{(R)}/\mathbb{Q}, s),$$

where we recall that h is the class number of K. Now, since h is odd and 2 splits in K, Theorem 19.1.1 of [8] shows that $\Phi(B^{(R)}/\mathbb{Q}, s)$ satisfies the functional equation

$$\Phi(B^{(R)}/\mathbb{Q}, s) = -\Phi(B^{(R)}/\mathbb{Q}, 2-s).$$

Hence $\Phi(B^{(R)}/\mathbb{Q}, s))$ must have a zero of odd order at $s = 1$, and so $L(B^{(R)}/\mathbb{Q}, 1) = 0$, whence also $L(B^{(R)}/K, 1) = 0$, which, in turn, clearly implies that $L(B^{(R)}/K_n, 1) = 0$ for each $n \geq 0$. By Corollary 5.7, $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n)$ has positive $\mathbb{Z}_2$-rank. On the other hand, by Lemma 5.4 this group has the same $\mathbb{Z}_2$-rank as a subgroup of $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/F_\infty)$, which is isomorphic to $\mathbb{Q}_2/\mathbb{Z}_2$ by Theorem 4.3. Therefore, the rank of $\mathrm{Sel}_{\mathfrak{P}^\infty}(B^{(R)}/K_n)$ must be equal to 1. This completes the proof of case (iii), and so of the whole theorem. □

We end by discussing one numerical example with $s_\infty(R) = 4$, which arose in [1]. Let $q = 7$, so that B is the elliptic curve $X_0(49)$, with equation

$$y^2 + xy = x^3 - x^2 - 2x - 1.$$

Take $R = 741 = 3 \times 13 \times 19$, and define $E = X_0(49)^{(R)}$, whence $s_\infty(R) = 4$. By Theorem 4.4, we then have $g_{F_\infty}(R) + e_{F_\infty}(R) = 3$. It is shown in [1] that $E(K) \otimes \mathbb{Q}$ has dimension 2 over K and $Ш(E/K)(2) = 0$. We shall prove the following result. We recall that in this case $F_\infty = K(E_{\mathfrak{p}^\infty})$, where $K = \mathbb{Q}(\sqrt{-7})$, and $F_n = K(E_{\mathfrak{p}^{n+2}})$ for all $n \geq 0$.

Proposition 5.8. *Let $E = X_0(49)^{(R)}$, with $R = 741$. Then $g_{F_\infty} = 2$, and $e_{F_\infty}(R) = 1$, so that $E(F_\infty) \otimes_{\mathbb{Z}} \mathbb{Q}$ has K-dimension equal to 2, and $Ш(E/F_\infty)(\mathfrak{p}^\infty) = \mathbb{Q}_2/\mathbb{Z}_2$. Moreover, for all integers $n \geq 0$, we have that $E(F_n) \otimes_{\mathbb{Z}} \mathbb{Q}$ has K-dimension equal to 2 and $Ш(E/F_n)(\mathfrak{p}^\infty)$ is finite.*

Proof. There are two ingredients to the proof. The first is a MAGMA calculation. Let C/K be the twist of E/K by the quadratic extension K_1/K. Then a MAGMA computation shows that $C(K) \otimes \mathbb{Q}$ has dimension 0 and $Ш(C/K)(2) = 0$. It follows easily that $E(K_1) \otimes \mathbb{Q}$ has K-dimension 2 and $Ш(E/K_1)(\mathfrak{p}^\infty)$ is finite, whence $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/K_n)$ has corank 2 for $n = 1$. We now recall that (see [1, Theorem 2.13]), for all $n \geq 0$ both the K-dimensions of $E(K_n) \otimes \mathbb{Q}$ and the corank of $Ш(E/K_n)(\mathfrak{p}^\infty)$ do not change if we replace K_n with F_n. Thus the MAGMA calculation proves that $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_1)$ as well as $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F_1)$ has $\mathbb{Z}_2$-corank equal to 2 by Lemma 5.4. The second ingredient in the the proof is a simple remark on the characteristic power series $c_{F_\infty}(T)$ of $X(F_\infty)$. By the Weierstrass Preparation Theorem, we may assume that $c_{F_\infty}(T)$ is a monic polynomial of degree 3, because $X(F_\infty)$ is a free $\mathbb{Z}_2$-module of rank 3. The characteristic power series of the Pontryagin dual of $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty) = \mathrm{Hom}(X(F_\infty), E_{\mathfrak{p}^\infty})$ is given by $c_{F_\infty}(u(1+T) - 1)$. Moreover, since $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F)$ has $\mathbb{Z}_2$-corank equal to 2, we conclude that $(T - (u-1))^2$ must divide

$c_{F_\infty}(T)$. Suppose now that there exists an integer $n > 0$ such that $\mathrm{Sel}'_{\mathfrak{p}^\infty}(E/F_n)$ has $\mathbb{Z}_2$-corank at least 3, and choose the smallest integer n with this property. Then it follows from Lemma 5.4 that $c_{F_\infty}(T)$ must also be divisible by $T-(u\zeta-1)$ for some primitive 2^n-th root of unity ζ. But, as $c_{F_\infty}(T)$ is a polynomial with coefficients in $\mathbb{Z}_2$, it would then be divisible by the product of all $T-(u\alpha-1)$, where α runs over all primitive 2^n-th roots of unity. Since this product is an irreducible polynomial of degree 2^{n-1} with coefficients in $\mathbb{Z}_2$, and $c_{F_\infty}(T)$ has degree 3, we must have $2^{n-1}=1$, or equivalently $n=1$. But our MAGMA calculation has already shown that $\mathrm{Sel}'(E/F_1)$ has $\mathbb{Z}_2$-corank 2, and the proof is complete. □

Acknowledgments. The author is deeply grateful to John Coates for discussing this problem and for his careful reading and polishing of the manuscript. Thanks also goes to Yongxiong Li for helpful discussions and to an anonymous referee for pointing out another proof of Proposition 3.3.

References

[1] J. Choi, J. Coates, Iwasawa theory of quadratic twists of $X_0(49)$, Acta Math. Sin. (Engl. Ser.) **34** (2018), 19–28.

[2] J. Coates, Infinite descent on elliptic curves with complex multiplication, Arithmetic and geometry, vol. I, Progress in Mathematics 35, eds. M. Artin and J. Tate; Birkhauser Boston, Boston, MA, 1983, 107–137.

[3] J. Coates, Y. Li, Non-vanishing theorems for central L-values of some elliptic curves with complex multiplication, Proc. Lond. Math. Soc. (3) **121** (2020), 1531–1578.

[4] J. Coates, J. Li, Y. Li, Classical Iwasawa theory and infinite descent on a family of abelian varieties, Selecta Math. (N.S.) **27** (2021), Paper No. 28, 36 pp.

[5] B. Ferrero, The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields, Amer. J. Math. **102** (1980), 447–459.

[6] G. Gras, Classes généralisées invariantes, J. Math. Soc. Japan **46** (1994), 467–476.

[7] R. Greenberg, On the structure of certain Galois groups, Invent. Math. **47** (1978), 85–99.

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

[9] Y. Kida, On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields, Tohoku Math. J. (2) **31** (1979), 91–96.

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

[11] J. Li, C. Yu, The Chevalley-Gras formula over global fields, J. Théor. Nombres Bordeaux. **32** (2020), 525–544.

[12] A. Michel, Une formule de Riemann-Hurwitz pour le groupe de Selmer d'une courbe elliptique, Ann. Inst. Fourier (Grenoble) **43** (1993), 57–84.

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

[14] K. Wingberg, A Riemann-Hurwitz formula for the Selmer group of an elliptic curve with complex multiplication, Comment. Math. Helv. **63** (1988), 587–592.

Present Address:
Jianing Li
Research Center for Mathematics and Interdisciplinary Sciences
Shandong University
Qingdao 266237, P. R. China.
e-mail: lijn@sdu.edu.cn