GROWTH OF p-PARTS OF IDEAL CLASS GROUPS AND FINE SELMER GROUPS IN $\mathbb{Z}_q$-EXTENSIONS WITH $p \neq q$

DEBANJANA KUNDU AND ANTONIO LEI

Abstract. Fix two distinct odd primes p and q. We study "$p \neq q$" Iwasawa theory in two different settings.
(1) Let K be an imaginary quadratic field of class number 1 such that both p and q split in K. We show that under appropriate hypotheses, the p-part of the ideal class groups is bounded over finite subextensions of an anticyclotomic $\mathbb{Z}_q$-extension of K.
(2) Let F be a number field and let $A_{/F}$ be an abelian variety with $A[p] \subseteq A(F)$. We give sufficient conditions for the p-part of the fine Selmer groups of A over finite subextensions of a $\mathbb{Z}_q$-extension of F to stabilize.

1. Introduction

Let $F/\mathbb{Q}$ be an algebraic number field and F_∞/F be a Galois extension with Galois group isomorphic to the additive group $\mathbb{Z}_q$ of q-adic integers. For each integer $n \geq 0$, there is a unique subfield F_n/F of degree q^n. Let $h(F_n)$ be the class number of F_n. K. Iwasawa showed that if q^{e_n} is the highest power of q dividing $h(F_n)$, then there exist integers λ, μ, ν independent of n, such that $e_n = \mu q^n + \lambda n + \nu$ for $n \gg 0$. On the other hand, in [Was75, Was78], L. C. Washington proved that for distinct primes p and q, the p-part of the class number stabilizes in the *cyclotomic* $\mathbb{Z}_q$-extension of an abelian number field. Washington's results have been extended to other $\mathbb{Z}_q$-extensions where primes are finitely decomposed. In particular, J. Lamplugh proved the following in [Lam15]: if p, q are distinct primes ≥ 5 that split in an imaginary quadratic field K of class number 1 and F/K is a prime-to-p abelian extension which is also unramified at p, then the p-class group stabilizes in the $\mathbb{Z}_q$-extension of F which is unramified outside precisely one of the primes above q.

Throughout this article, p and q will denote two distinct odd primes and K is an imaginary quadratic field of class number 1 in which both p and q split. We write $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and $q\mathcal{O}_K = \mathfrak{q}\bar{\mathfrak{q}}$.

Given an ideal $\mathfrak{h}$ of $\mathcal{O}_K$, we write $\mathscr{R}(\mathfrak{h})$ for the ray class field of K of conductor $\mathfrak{h}$. Consider the infinite extension $\mathscr{R}(\mathfrak{g}q^\infty) = \bigcup_{n\geq 1} \mathscr{R}(\mathfrak{g}q^n)$, where $\mathfrak{g}$ is a fixed ideal of $\mathcal{O}_K$ coprime to q. We have the isomorphism

$$\mathrm{Gal}(\mathscr{R}(\mathfrak{g}q^\infty)/K) \cong \Delta \times \mathbb{Z}_q^2,$$

where $\Delta = \mathrm{Gal}(\mathscr{R}(\mathfrak{g}q)/K)$. We consider the anticyclotomic $\mathbb{Z}_q$-extension $\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}/\mathscr{R}(\mathfrak{g}q)$, i.e., the subextension of $\mathscr{R}(\mathfrak{g}q^\infty)/\mathscr{R}(\mathfrak{g}q)$ corresponding to the -1-eigensubspace of the complex conjugation in $\mathrm{Gal}(\mathscr{R}(\mathfrak{g}q^\infty)/\mathscr{R}(\mathfrak{g}q))$. We set $F = \mathscr{R}(\mathfrak{g}q)$ and write F_n to denote the unique subextension of $\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}$ such that $\mathrm{Gal}(F_n/\mathscr{R}(\mathfrak{g}q)) \cong \mathbb{Z}/q^n\mathbb{Z}$.

Date: July 12, 2022.
2020 *Mathematics Subject Classification.* Primary 11R23, 11R29; Secondary 11R20, 11J95.
Key words and phrases. Ideal class groups, fine Selmer groups, $p \neq q$ Iwasawa theory.

In the first half of this article, we study the growth of the p-part of the ideal class group of F_n as $n \to \infty$. This generalizes [Lam15, Theorem 1.3], where the stability of the p-part of the class numbers $\mathscr{R}(\mathfrak{g}\mathfrak{q}^n)$ is studied. More precisely, we prove the following result.

Theorem A. *Let K be an imaginary quadratic field of class number 1. Let p and q be distinct primes (≥ 5) which split in K. Let $\mathfrak{g}$ be a fixed ideal of $\mathcal{O}_K$ coprime to pq such that $\mathfrak{g}$ is a product of split primes*[1] *and $w_{\mathfrak{g}} = 1$, where $w_{\mathfrak{g}}$ denotes the number of roots of unity in K that are congruent to 1 modulo $\mathfrak{g}$. Let $F = \mathscr{R}(\mathfrak{g}q)$ be a prime-to-p extension of K and $\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}/F$ be the anticyclotomic $\mathbb{Z}_q$-extension. Then, there exists an integer N such that for all $n \geq N$,*

$$\mathrm{ord}_p(h(F_n)) = \mathrm{ord}_p(h(F_N)).$$

To prove this theorem, we will make use of a special case of a theorem of H. Hida, which guarantees the non-vanishing modulo p of certain algebraic L-functions (see Theorem 2.2). Using a result of Lamplugh (see Theorem 3.1), we show in Theorem 3.2 that certain p-primary Galois modules stabilize in the said anticyclotomic $\mathbb{Z}_q$-extension. Finally, Theorem A follows by an application of the Iwasawa Main Conjecture, which is known in this setting by the work of K. Rubin [Rub91].

In the second half of the article, we prove a general statement (see Theorem 4.3) which shows that in certain $\mathbb{Z}_q$-extensions of a number field F, the growth of the p-part of the class group is closely related to that of the p-primary *fine* Selmer group of an abelian variety $A_{/F}$. This subgroup of the classical p-primary Selmer group is denoted by $\mathrm{Sel}_0(A/F)$, and is obtained by imposing stronger vanishing conditions at primes above p (the precise definition is reviewed in §4.1). The following result is an application of the aforementioned theorem to the growth of the p-part of fine Selmer group of a fixed abelian variety A over a $\mathbb{Z}_q$-tower (which is not necessarily anticyclotomic).

Theorem B. *Let p and q be distinct odd primes. Let F be any number field and $A_{/F}$ be an abelian variety such that $A[p] \subseteq A(F)$. Let F_∞/F be a $\mathbb{Z}_q$-extension where the primes above q and the primes of bad reduction of A are finitely decomposed. If there exists $N \gg 0$ such that for all $n \geq N$,*

$$\mathrm{ord}_p(h(F_n)) = \mathrm{ord}_p(h(F_N)),$$

then

$$\mathrm{Sel}_0(A/F_n) = \mathrm{Sel}_0(A/F_N).$$

In particular, Theorem B applies to the setting studied by Washington [Was75, Was78].

Acknowledgement. We thank Ming-Lun Hsieh, Filippo A. E. Nuccio Mortarino Majno di Capriglio, and Lawrence Washington for answering our questions during the preparation of this article. DK acknowledges the support of the PIMS Postdoctoral Fellowship. AL is supported by the NSERC Discovery Grants Program RGPIN-2020-04259 and RGPAS-2020-00096.

2. A result of Hida on L-values of anticyclotomic Hecke characters

Throughout this section, K is a fixed imaginary quadratic field of class number one. We review a special case of a result of Hida from [Hid07] that will play a crucial role in our proof of Theorem A.

Let $\mathfrak{f}$ be an ideal of $\mathcal{O}_K$ that is a product of split primes of K coprime to pq with $w_{\mathfrak{f}} = 1$. Let $E_{/K}$ be an elliptic curve with CM by $\mathcal{O}_K$ such that its corresponding Hecke character ψ is of conductor $\mathfrak{f}$ (such an E exists by [dS87, Lemma on p. 41]; see also Appendix A).

[1] In this article, a split prime of K refers to a prime ideal of $\mathcal{O}_K$ that lies above a rational prime that splits in K.

Definition 2.1. Let $\mathfrak{h}$ be any integral ideal of K. Let ϵ be any Hecke character of K. The *imprimitive L-function* of ϵ modulo $\mathfrak{h}$ is defined as follows

$$\begin{aligned} L_{\mathfrak{h}}(\epsilon, s) &= \prod_{\gcd(\nu,\mathfrak{h})=1} \left(1 - \frac{\epsilon(\nu)}{(N\nu)^s}\right)^{-1} \\ &= \sum_{\gcd(\mathfrak{a},\mathfrak{h})=1} \frac{\epsilon(\mathfrak{a})}{(N\mathfrak{a})^s}, \end{aligned}$$

where the product runs over *prime ideals* of K coprime to $\mathfrak{h}$, and sum is taken over *integral ideals* coprime to $\mathfrak{h}$.

Fix an integral ideal $\mathfrak{g}$ of K, which is divisible by $\mathfrak{f}$, relatively prime to pq, and such that only split primes of K divide $\mathfrak{g}$. Note that we have $w_{\mathfrak{g}} = 1$ since $\mathfrak{f}|\mathfrak{g}$ and $w_{\mathfrak{f}} = 1$. Let $F = \mathscr{R}(\mathfrak{g}q)$ be the *ray class field* of K of conductor $\mathfrak{g}q$ and write $\Delta = \mathrm{Gal}(F/K)$. Set $F_\infty = \bigcup_{n\geq 1} \mathscr{R}(\mathfrak{g}q^n)$; this is a $\mathbb{Z}_q^2$-extension of F. We fix an isomorphism

$$\mathrm{Gal}(F_\infty/K) \simeq \mathrm{Gal}(F/K) \times \mathrm{Gal}(K_\infty/K) = \Delta \times \mathbb{Z}_q^2.$$

Let ϵ be a character of $\mathrm{Gal}(F_\infty/K)$. For our purpose, ϵ will be of the form $\overline{\varphi\psi^k}$, where φ is a finite-order character and k is an integer between 1 and $p-1$. Denote by $L(\epsilon, s)$ the *primitive Hecke L-function* of ϵ. Recall that the imprimitive (or partial) L-function differs from the primitive (or classical) L-function by a finite number of Euler factors. We can further define the *primitive algebraic Hecke L-function*,

$$L^{\mathrm{alg}}(\overline{\varphi\psi^k}) = L^{\mathrm{alg}}_{\mathfrak{h}}(\epsilon) := \frac{L(\epsilon, k)}{\Omega_\infty^k} = \frac{L\left(\overline{\varphi\psi^k}N^{-k}, 0\right)}{\Omega_\infty^k}.$$

Here, Ω_∞ denotes a complex period for $E_{/\mathbb{C}}$. Similarly, given an integral ideal $\mathfrak{h}$ of K, we define the *imprimitive algebraic Hecke L-function*,

$$L^{\mathrm{alg}}_{\mathfrak{h}}(\overline{\varphi\psi^k}) = L^{\mathrm{alg}}(\epsilon) := \frac{L_{\mathfrak{h}}(\epsilon, k)}{\Omega_\infty^k} = \frac{L_{\mathfrak{h}}\left(\overline{\varphi\psi^k}N^{-k}, 0\right)}{\Omega_\infty^k}.$$

In what follows, we say that a Hecke character ϵ of K is of *infinity type* (a, b) if its infinity component sends x to $x^a\overline{x}^b$. Under this convention, ψ has infinity type $(-1, 0)$, whereas the norm map N is of infinity type $(-1, -1)$. Thus, the Hecke character $\overline{\psi^k}N^{-k}$ is of infinity type $(k, 0)$.

Henceforth, we fix a prime $v|\mathfrak{p}$ of F and an embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}_p}$ so that v is sent into the maximal ideal of $\mathcal{O}_{\overline{\mathbb{Q}_p}}$. This allows us to consider $L^{\mathrm{alg}}_{\mathfrak{h}}(\overline{\varphi\psi^k})$ as elements of $\overline{\mathbb{Q}_p}$. Throughout, π will be a fixed uniformizer of F_v and we write ord_π for the valuation on $\overline{\mathbb{Q}_p}$ normalized so that $\mathrm{ord}_\pi(\pi) = 1$.

Theorem 2.2 (Hida)**.** *For all but finitely many characters φ that factor through $\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}$, we have*

$$\mathrm{ord}_\pi\left(L^{\mathrm{alg}}_{(q)}(\overline{\varphi\psi^k})\right) = 0.$$

Proof. For each φ, we have $\overline{\varphi} = \phi\eta$, where ϕ is a character of Δ and η is a character of $\mathrm{Gal}(\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}/F)$. We may further decompose ϕ into $\phi'\nu^{-1}$, where ν is a character of $\mathrm{Gal}(F/\mathscr{R}(\mathfrak{g}))$ and ϕ' is a character of $\mathrm{Gal}(\mathscr{R}(\mathfrak{g})/K)$. We have the field diagram:

$$\begin{tikzcd}
\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}} \arrow[dd, dash] \arrow[dd, dash, bend right, "\mathbb{Z}_q"'] & & & \\
{} \arrow[rrr, dashed, dash] & & & \eta \\
\mathscr{R}(\mathfrak{g}q) = F \arrow[dddd, dash] \arrow[dddd, dash, bend right, "\Delta"'] \arrow[dr, dash] & & & \\
& {} \arrow[rr, dashed, dash] & & \nu^{-1} \\
& \mathscr{R}(\mathfrak{g}) \arrow[dd, dash] & & \\
& {} \arrow[rr, dashed, dash] & & \phi' \\
K \arrow[d, dash] & & & \\
\mathbb{Q} & & &
\end{tikzcd}$$

We take the CM field M in [Hid07] to be the imaginary quadratic field K. We take the CM type Σ there to be the one that corresponds to the infinity type $(1,0)$ and $\kappa = 0$. Then the infinity type of the character λ in *op. cit.* becomes

$$k\Sigma + 0(1-c) = k(1,0) + (0,0) - (0,0) = (k,0).$$

The condition (M1) in [Hid07, Theorem 4.3] does not hold since $K/\mathbb{Q}$ is not unramified. Hence, we can apply the aforementioned theorem with λ and χ^{-1} taken to be $\overline{\psi^k} N^{-k}\phi'$ and η, respectively. $\square$

Remark 2.3 ([Lam14, proof of Theorem 3.1.9]). Let $\mathfrak{g}$ be a fixed ideal as before. Fix an ideal $\mathfrak{h}$ of $\mathcal{O}_K$ which is coprime to $\mathfrak{p}$ and divisible by $\mathfrak{g}q$. Recall that the algebraic L-function of $\overline{\varphi\psi^k}$ modulo $\mathfrak{h}$ is given by

$$L_{\mathfrak{h}}^{(\mathrm{alg})}(\overline{\varphi\psi^k}) = \frac{L_{\mathfrak{h}}(\overline{\varphi\psi^k}, k)}{\Omega_\infty^k}.$$

Then, for almost all characters of $\mathrm{Gal}\left(\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}/F\right) \cong \mathbb{Z}_q$, we have that

$$\mathrm{ord}_\pi\left(L_{(q)}^{(\mathrm{alg})}(\overline{\varphi\psi^k})\right) = \mathrm{ord}_\pi\left(L_{\mathfrak{h}}^{(\mathrm{alg})}(\overline{\varphi\psi^k})\right).$$

This follows from the observation that for a given prime ideal $\mathfrak{a}$ of K that is coprime to q, for almost all characters η,

$$\mathrm{ord}_\pi\left(1 - \frac{\overline{\varphi\psi^k}(\mathfrak{a})}{(N\mathfrak{a})^k}\right) = 0$$

since η sends $\mathfrak{a}$ to a q-power roots of unity, which are distinct modulo π.

3. Consequences on class groups

In this section, we will make use of Theorem 2.2 to study the growth of the p-part of the class group in an anticyclotomic $\mathbb{Z}_q$-extension. Let us introduce the necessary notation. Throughout, $p \nmid 6q$ is a fixed prime that is split in K and $E_{/K}$ is a fixed CM elliptic curve as in the previous section (with Hecke character ψ whose conductor is $\mathfrak{f}$). Let K_0 be a finite abelian extension of K such that p is unramified in K_0 and $p \nmid [K_0 : K]$. Fix a prime $\mathfrak{p}$ of K lying above p. Set $L = K_0(E_{\mathfrak{p}})$

and $L_\infty = L(E_{\mathfrak{p}^\infty})$. Let $\Delta = \mathrm{Gal}(L/K)$ and $\Gamma = \mathrm{Gal}(L_\infty/L) \simeq \mathbb{Z}_p$. Let $\mathcal{G} = \mathrm{Gal}(L_\infty/K) \cong \Delta \times \Gamma$ and $\Lambda = \mathbb{Z}_p[\![\mathcal{G}]\!]$.

Following [Rub91], we write $\overline{\mathcal{C}}(L_\infty)$ (resp. $U(L_\infty)$) for the inverse limits over all finite sub-extensions inside L_∞ of the completion of the elliptic units (resp. local principal units) at $\mathfrak{p}$.

Fix an ideal $\mathfrak{h}$ of $\mathcal{O}_K$ which is coprime to $\mathfrak{p}$, is divisible by $\mathfrak{f}$, and is such that $K_0 \subset K(E_{\mathfrak{h}})$. Let μ_K be the group of roots of unity of K and $\lambda \in \mathcal{O}_K \setminus \mu_K$ such that $\lambda \equiv 1 \mod \mathfrak{h}$ with $(\lambda, 6\mathfrak{h}\mathfrak{p}) = 1$. We let $\sigma_{(\lambda)} \in \mathrm{Gal}(K_0/K)$ denote the Artin symbol associated to λ.

We further decompose Δ as $H \times I$, where $H = \mathrm{Gal}(K_0/K)$ and $I = \mathrm{Gal}(K(E_{\mathfrak{p}})/K)$. Here, I is the inertia subgroup at $\mathfrak{p}$ inside Δ. Let $\theta_{\mathfrak{p}}$ denote the canonical character given by the Galois action on $E_{\mathfrak{p}^\infty}$ restricted to I. Given a character χ of Δ, we write it as $\varphi\theta_{\mathfrak{p}}^k$, where φ is a character of H and $1 \leq k \leq p-1$. We have the following diagram:

$$\begin{tikzcd}
L_\infty = L(E_{\mathfrak{p}^\infty}) \arrow[dd, dash] \arrow[dd, dash, bend right, "\mathbb{Z}_p"'] & & \\
& & \\
L = K_0(E_{\mathfrak{p}}) \arrow[dr, dash] \arrow[dd, dash] \arrow[dd, dash, bend right, "\Delta"'] & & \theta_{\mathfrak{p}}^k \\
& K_0 & \\
K \arrow[ur, dash] \arrow[d, dash] & & \varphi \\
\mathbb{Q} & &
\end{tikzcd}$$

Let $\mathcal{Z}$ denote the decomposition subgroup at $\mathfrak{p}$ inside $\mathcal{G}$. Recall that π is the uniformizer of $\mathcal{O}_{K_{\mathfrak{p}}}$. Before proceeding, we need to introduce the notion of an *anomalous prime.* In the sense of Mazur (see [Maz72, p. 186]), a prime $v|p$ is called *anomalous* if $\widetilde{E}(\kappa_v)[p] \neq 0$, where κ_v is the residue field. In our current setting, this can be related to counting the p-power roots of unity in the residue field (see [Lam14, pp. 70–71]). Indeed, if $v|p$ is a prime above p in L_∞ then

$$\#\widetilde{E}(\kappa_v) = \left(\pi^f - 1\right)\left(\overline{\pi}^f - 1\right)$$

where f is the residue degree of the extension K_0/K. It follows that

$$M := \mathrm{ord}_p\left(\#\widetilde{E}(\kappa_v)\right) = \mathrm{ord}_p\left(\left(\pi^f - 1\right)\left(\overline{\pi}^f - 1\right)\right) = \mathrm{ord}_\pi\left(\left(\pi^f - 1\right)\left(\overline{\pi}^f - 1\right)\right) = \mathrm{ord}_\pi\left(\overline{\pi}^f - 1\right).$$

Therefore, an equivalent definition of a prime being anomalous is $M = \mathrm{ord}_\pi\left(\overline{\pi}^f - 1\right) \geq 1$. Since $\gcd(p, |\Delta|) = 1$, the action of $\Delta \cap \mathcal{Z}$ on $\mu_{p^\infty}(L_{\infty,v}) = \mu_{p^M}$ gives a $\mathbb{Z}_p$-valued character which we denote by $\chi_{\mathrm{cyc}} : \Delta \cap \mathcal{Z} \to \mu_{p-1} \subseteq \mathbb{Z}_p^\times$. We have the following theorem.

Theorem 3.1. *Let $\chi = \varphi\theta_{\mathfrak{p}}^k$ be a character of Δ. When E/K_0 is anomalous at $\mathfrak{p}$, we assume that $\chi|_{\Delta\cap\mathcal{Z}}$ is not the cyclotomic character. Let $\mathfrak{h}$ and λ be as above. If*

$$\mathrm{ord}_\pi\left(\left(N(\lambda) - \lambda^k\varphi(\sigma_{(\lambda)})\right) \cdot L_{\mathfrak{h}}^{(\mathrm{alg})}(\overline{\varphi\psi^k})\right) = 0,$$

then $\overline{\mathcal{C}}(L_\infty)^\chi = U(L_\infty)^\chi$*. Here,* M^χ *denotes the* χ*-isotypic component of a* Λ*-module* M*.*

Proof. See [Lam15, Theorem 7.7]. □

3.1. **Variations of class groups.** Let $F \subset K(E_{\mathfrak{g}})$ for some ideal $\mathfrak{g}$ of $\mathcal{O}_K$ such that p is unramified in F/K, $p \nmid [F : K]$, and $\mathfrak{g}$ is divisible by $\mathfrak{f}$ and is coprime to $\mathfrak{p}q$. Furthermore, we assume that both $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ are tamely ramified in F. Then $\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}$ is a $\mathbb{Z}_q$-extension of F, and for integers $n \geq 0$, let F_n/F be the n-th layer of this $\mathbb{Z}_q$-extension. Note that only primes above q ramify in F_n/F, $p \nmid [F_n : K]$ (since $q \neq p$), and $F_n \subset K(E_{\mathfrak{g}q^{n+1}})$. Therefore, we may take K_0 and $\mathfrak{h}$ in the previous section to be F_n and $\mathfrak{h}_n := \mathfrak{g}q^{n+1}$, respectively.

For $n \geq 1$, just as before we define $L_n = F_n(E_\mathfrak{p})$, $L_{n,\infty} = F_n(E_{\mathfrak{p}^\infty})$, $\Delta_n = H_n \times I$, $\mathcal{G}_n = \Delta_n \times \Gamma$, $U_{n,\infty} = U(L_{n,\infty})$, etc. Note that $I = \mathrm{Gal}(K_0(E_\mathfrak{p})/K_0) \cong \mathrm{Gal}(L_n/F_n)$. Define $X_{n,\infty}$ to be the Galois group of the maximal abelian p-extension of $L_{n,\infty}$ which is unramified outside $\mathfrak{p}$. By global class field theory we have the following four-term exact sequence

$$0 \to \overline{\mathcal{E}}_{n,\infty}/\overline{\mathcal{C}}_{n,\infty} \to U_{n,\infty}/\overline{\mathcal{C}}_{n,\infty} \to X_{n,\infty} \to A_{n,\infty} \to 0. \tag{1}$$

Here, $\overline{\mathcal{E}}_{n,\infty} = \overline{\mathcal{E}}(L_{n,\infty})$ is used to denote the global units of $L_{n,\infty}$. Finally, $A_{n,\infty} = A(L_{n,\infty})$ is the inverse limit of the p-part of the class group for each finite extension of F_n contained inside $L_{n,\infty}$. In other words, $A_{n,\infty}$ can be identified with the Galois group of the maximal abelian unramified p-extension of $L_{n,\infty}$. We now prove the key result which will be required in proving Theorem A.

Theorem 3.2. *There exists an integer* $N \geq 0$ *such that* $X^I_{n,\infty} = X^I_{N,\infty}$ *for all* $n \geq N$*, where* M^I *denotes the isotypic component of* M *corresponding to the trivial character of* I*.*

Proof. To prove the theorem, it suffices to show that for $N \gg 0$,

$$\mathrm{char}_\Lambda(X^I_{n,\infty}) = \mathrm{char}_\Lambda(X^I_{N,\infty})$$

for all $n \geq N$. Consider the restriction map

$$\pi_{n,N} : X^I_{n,\infty} \twoheadrightarrow X^I_{N,\infty}.$$

Since characteristic ideals are multiplicative in short exact sequences, the kernel of the above surjective map must be finite. However, a theorem of R. Greenberg (see [Gre78, Theorem §1]) ensures that there are no non-trivial finite submodules inside $X^I_{n,\infty}$. This forces the kernel to be trivial, i.e.,

$$X^I_{n,\infty} = X^I_{N,\infty}.$$

Via the main conjecture of Iwasawa theory for imaginary quadratic fields [Rub91, Theorem 4.1(i)], it is enough to show that

$$U^I_{n,\infty}/\overline{\mathcal{C}}^I_{n,\infty} = U^I_{N,\infty}/\overline{\mathcal{C}}^I_{N,\infty}.$$

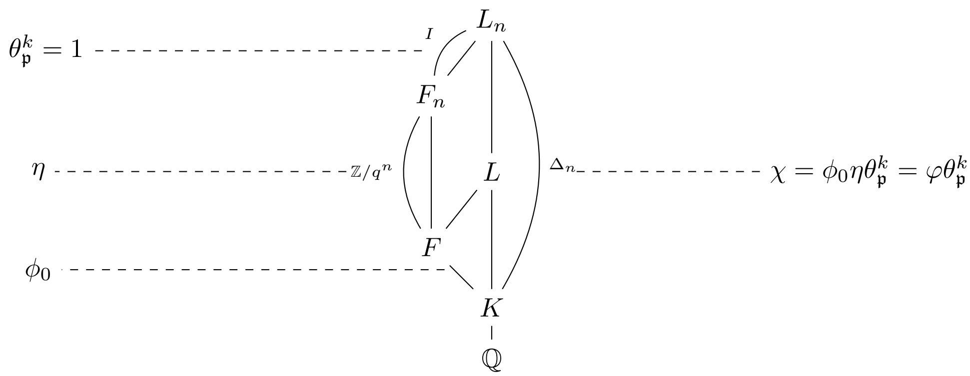
This in turn would follow from

$$U^\chi_{n,\infty} = \overline{\mathcal{C}}^\chi_{n,\infty}$$

for all characters χ of Δ_n that do not factor through Δ_N with $\chi|_I = 1$. Taking $\mathfrak{h}_n$ and applying Theorem 3.1 with K_0 taken to be F_n, it is now enough to show that for all such χ, there exists $\lambda \in \mathcal{O}_K \setminus \mu_K$ such that $\lambda \equiv 1 \mod \mathfrak{f}$ and $(\lambda, 6q\mathfrak{p}) = 1$ satisfying

$$\mathrm{ord}_\pi\left(\left(N(\lambda) - \lambda^k \varphi(\sigma_{(\lambda)})\right) \cdot L^{(\mathrm{alg})}_{\mathfrak{h}}(\overline{\varphi\psi^k})\right) = 0, \tag{2}$$

where $\chi = \varphi\theta_{\mathfrak{p}}^k$, with φ being a character of H_n and $k = p-1$ (so that its restriction to I is trivial). In particular, the condition on E/K_0 being anomalous is irrelevant. We draw another field diagram for convenience of the reader



Note that (2) is equivalent to saying that

$$\left(\lambda\overline{\lambda} - \lambda^k\varphi(\sigma_{(\lambda)})\right) \cdot L_{\mathfrak{h}}^{(\mathrm{alg})}(\overline{\varphi\psi^k}) \not\equiv 0 \pmod{\pi\mathcal{O}}.$$

Now, observe that

$$\begin{aligned}\left(\lambda\overline{\lambda} - \lambda^k\varphi(\sigma_{(\lambda)})\right) \equiv 0 \pmod{\pi\mathcal{O}} &\Leftrightarrow \varphi(\sigma_{(\lambda)}) \equiv \overline{\lambda}\lambda^{1-k} \pmod{\pi\mathcal{O}}\\ &\Leftrightarrow \eta\phi_0(\sigma_{(\lambda)}) \equiv \overline{\lambda}\lambda^{1-k} \pmod{\pi\mathcal{O}}\\ &\Leftrightarrow \eta(\sigma_{(\lambda)}) \equiv \overline{\lambda}\lambda^{1-k}\phi_0^{-1}(\sigma_{(\lambda)}) \pmod{\pi\mathcal{O}}.\end{aligned}$$

Here, we have written $\varphi = \eta\phi_0$, where η is a character of $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/q^n$. Note that η has exact order q^m for some $m \geq 1$. Therefore, $\eta(\sigma_{(\lambda)})$ is a primitive q^m-th root of unity. But, modulo π, the q-power roots of unity are distinct. Therefore, for almost all η,

$$\mathrm{ord}_\pi\left(N(\lambda) - \lambda^k\varphi(\sigma_{(\lambda)})\right) = 0.$$

By Theorem 2.2 and Remark 2.3, one can choose $N \gg 0$ such that $\mathrm{ord}_\pi\left(L_{\mathfrak{h}}^{(\mathrm{alg})}(\overline{\varphi\psi^k})\right) = 0$ holds for all characters χ of Δ_n with $n \geq N$, which do not factor through Δ_N. This establishes (2) and the proof of the theorem is now complete. □

We are now in a position to prove Theorem A from the Introduction. We repeat the statement below for the convenience of the reader.

Theorem. *Let K be an imaginary quadratic field of class number 1. Let p and q be distinct primes (≥ 5) which split in K. Let $\mathfrak{g}$ be a fixed ideal of $\mathcal{O}_K$ coprime to pq such that $\mathfrak{g}$ is a product of split primes and that $w_{\mathfrak{g}} = 1$. Let $F = \mathscr{R}(\mathfrak{g}q)$ be a prime-to-p extension of K and $\mathscr{R}(\mathfrak{g}q^\infty)^{\mathrm{ac}}/F$ be the anticyclotomic $\mathbb{Z}_q$-extension. Then, there exists an integer N such that for all $n \geq N$,*

$$\mathrm{ord}_p(h(F_n)) = \mathrm{ord}_p(h(F_N)).$$

Proof. Let the p-class group of F_n (resp. F_N) be denoted by $A(F_n)$ (resp. $A(F_N)$). Since p does not divide $[F_n : F_N]$, we have an injection

$$A(F_N) \hookrightarrow A(F_n). \tag{3}$$

It follows from global class field theory that for all $n \geq 0$, we have the identification

$$A_{n,\infty} \simeq \mathrm{Gal}(M_{n,\infty}/L_{n,\infty}),$$

where $M_{n,\infty}$ is the maximal abelian unramified p-extension of $L_{n,\infty}$. Recall the four-term exact sequence introduced in (1). It follows from Theorem 3.2 that $A_{n,\infty} = A_{N,\infty}$. Now, consider the following diagram

$$\begin{tikzcd} 0 \arrow[r] & A_{N,\infty} \arrow[r] \arrow[d] & A_{n,\infty} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A(F_N) \arrow[r] & A(F_n) & \end{tikzcd}$$

where the vertical maps are given by restriction and are surjective because the extension $L_{n,\infty}/F_n$ and $L_{N,\infty}/F_N$ are totally ramified at primes above $\mathfrak{p}$. As explained above, the top horizontal row is an isomorphism. Therefore, the bottom row is a surjective map as well. When combined with (3), we see that the bottom row is in fact an isomorphism. This completes the proof of the theorem. □

4. Asymptotic growth of fine Selmer groups of abelian varieties

4.1. **Definition of fine Selmer groups.** Suppose F is a number field. Throughout, $A_{/F}$ is a fixed abelian variety. We fix a finite set S of primes of F containing p, the primes dividing the conductor of A, as well as the archimedean primes. Denote by F_S, the maximal algebraic extension of F unramified outside S. For every (possibly infinite) extension L of F contained in F_S, write $G_S(L) = \mathrm{Gal}(F_S/L)$. Write $S(L)$ for the set of primes of L above S. If L is a finite extension of F and w is a place of L, we write L_w for its completion at w; when L/F is infinite, it is the union of completions of all finite sub-extensions of L.

Definition 4.1. Let L/F be an algebraic extension. The *p-primary fine Selmer group of* A over L is defined as

$$\mathrm{Sel}_0(A/L) = \ker\left(H^1\left(G_S(L), A[p^\infty]\right) \to \bigoplus_{v \in S} H^1\left(L_v, A[p^\infty]\right)\right).$$

Similarly, the *p-fine Selmer group of* A over L is defined as

$$\mathrm{Sel}_0(A[p]/L) = \ker\left(H^1\left(G_S(L), A[p]\right) \to \bigoplus_{v \in S} H^1\left(L_v, A[p]\right)\right).$$

It is easy to observe that if F_∞/F is an infinite extension,

$$\mathrm{Sel}_0\left(A/F_\infty\right) = \varinjlim_L \mathrm{Sel}_0\left(A/L\right), \quad \mathrm{Sel}_0\left(A[p]/F_\infty\right) = \varinjlim_L \mathrm{Sel}_0\left(A[p]/L\right),$$

where the inductive limits are taken with respect to the restriction maps and L runs over all finite extensions of F contained in F_∞. Next, we define the notion of p-rank of an abelian group G.

Definition 4.2. Let G be an abelian group. Define the *p-rank* of G as

$$r_p(G) = r_p(G[p]) := \dim_{\mathbb{F}_p}\left(G[p]\right).$$

4.2. **Growth of fine Selmer groups in $\mathbb{Z}_q$-extensions.** In this section, we prove the following theorem which essentially says that the p-part of the class group and the p-primary fine Selmer group have similar growth behaviour in $\mathbb{Z}_q$-extensions.

Theorem 4.3. *Let A be a d-dimensional abelian variety defined over any number field F. Let $S(F)$ be a finite set of primes in F consisting precisely of the primes above q, the primes of bad reduction of A, and the Archimedean primes. Let F_∞/F be a fixed $\mathbb{Z}_q$ extension such that primes in $S(F)$ are finitely decomposed in F_∞/F and suppose $[F_n : F] = q^n$. Further suppose that $A[p] \subseteq A(F)$. Then*

$$\left| r_p \left(\mathrm{Sel}_0 \left(A/F_n \right) \right) - 2d r_p \left(\mathrm{Cl}(F_n) \right) \right| = O(1).$$

If $A[p] \subseteq A(F)$, then the action of G_F on $A[p]$ is trivial. Let $A^\vee$ be the dual abelian variety. The action on the dual representation, $A^\vee[p]$ is also trivial. This tells us that $A^\vee[p] \subseteq A^\vee(F)$. Therefore, Theorem 4.3 allows us to deduce the following result.

Corollary 4.4. *With the same hypothesis as in Theorem 4.3*

$$\left| r_p \left(\mathrm{Sel}_0 \left(A/F_n \right) \right) - r_p \left(\mathrm{Sel}_0 \left(A^\vee/F_n \right) \right) \right| = O(1).$$

To prove Theorem 4.3, we need a few lemmas.

Lemma 4.5. *Consider the following short exact sequence of of co-finitely generated abelian groups*

$$P \to Q \to R \to S.$$

Then,

$$\left| r_p(Q) - r_p(R) \right| \leq 2 r_p(P) + r_p(S).$$

Proof. See [LM16, Lemma 3.2]. □

Lemma 4.6. *Let F_∞ be any $\mathbb{Z}_q$-extension of F such that all the primes in $S(F)$ are finitely decomposed. Let F_n be the subfield of F_∞ such that $[F_n : F] = q^n$. Then*

$$\left| r_p \left(\mathrm{Cl}(F_n) \right) - r_p \left(\mathrm{Cl}_S(F_n) \right) \right| = O(1).$$

Proof. For each F_n, we write $S_f(F_n)$ for the set of finite primes of F_n above S_f. For each n, we have the following exact sequence

$$\mathbb{Z}^{\left| S_f(F_n) \right|} \longrightarrow \mathrm{Cl}(F_n) \xrightarrow{\alpha_n} \mathrm{Cl}_S(F_n) \longrightarrow 0$$

(see [NSW08, Lemma 10.3.12]). Since the class group is always finite, it follows that $\ker(\alpha_n)$ is finite. Also, $r_p \left(\ker(\alpha_n) \right) \leq \left| S_f(F_n) \right|$ and $r_p \left(\ker(\alpha_n)/p \right) \leq \left| S_f(F_n) \right|$. By Lemma 4.5,

$$\left| r_p \left(\mathrm{Cl}(F_n) \right) - r_p \left(\mathrm{Cl}_S(F_n) \right) \right| \leq 2 \left| S_f(F_n) \right| = O(1).$$

□

Lemma 4.7. *Let F_∞/F be a $\mathbb{Z}_q$-extension and let F_n be the subfield of F_∞ such that $[F_n : F] = q^n$. Let A be an abelian variety defined over F. Suppose that all primes of $S(F)$ are finitely decomposed in F_∞/F. Then*

$$\left| r_p \left(\mathrm{Sel}_0(A[p]/F_n) \right) - r_p \left(\mathrm{Sel}_0(A/F_n) \right) \right| = O(1).$$

Proof. Consider the commutative diagram below.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_0(A[p]/F_n) \arrow[r] \arrow[d, "s_n"] & H^1(G_S(F_n), A[p]) \arrow[r] \arrow[d, "f_n"] & \bigoplus_{v\in S(F_n)} H^1(F_{n,v_n}, A[p]) \arrow[d, "\gamma_n"] \\
0 \arrow[r] & \mathrm{Sel}_0(A/F_n)[p] \arrow[r] & H^1(G_S(F_n),\ A[p^\infty])[p] \arrow[r] & \bigoplus_{v_n\in S(F_n)} H^1(F_{n,v_n},\ A[p^\infty])[p]
\end{tikzcd}$$

Both f_n and γ_n are surjective. The kernel of these maps are given by

$$\ker(f_n) = A(F_n)[p^\infty]/p,$$
$$\ker(\gamma_n) = \bigoplus_{v_n\in S(F_n)} A(F_{n,v_n})[p^\infty]/p.$$

Observe that $r_p\left(\ker(s_n)\right) \leq r_p\left(\ker(f_n)\right) \leq 2d$ and that $r_p\left(\ker(\gamma_n)\right) \leq 2d\left|S_f(F_n)\right|$. By hypothesis, $S_f(F_n)$ is bounded as n varies. It follows from the snake lemma that both $r_p\left(\ker(s_n)\right)$ and $r_p\left(\mathrm{coker}(s_n)\right)$ are finite and bounded. Applying Lemma 4.5 to the following exact sequence

$$0 \to \ker(s_n) \to \mathrm{Sel}_0(A[p]/F_n) \to \mathrm{Sel}_0(A/F_n)[p] \to \mathrm{coker}(s_n) \to 0$$

completes the proof. □

Proof of Theorem 4.3. By hypothesis, $A[p] \subseteq A(F)$. Therefore, $A[p] \simeq (\mathbb{Z}/p)^{2d}$. We have

$$H^1\left(G_S(F_n),\ A[p]\right) = \mathrm{Hom}\left(G_S(F_n),\ A[p]\right).$$

There are similar identifications for the local cohomology groups. Thus,

$$\mathrm{Sel}_0\left(A[p]/F_n\right) \simeq \mathrm{Hom}\left(\mathrm{Cl}_S(F_n), A[p]\right) \simeq \mathrm{Cl}_S(F_n)[p]^{2d}$$

as abelian groups. Therefore,

$$r_p\left(\mathrm{Sel}_0\left(A[p]/F_n\right)\right) = 2d r_p\left(\mathrm{Cl}_S(F_n)\right).$$

The theorem now follows from Lemmas 4.6 and 4.7. □

Let p^{e_n} be the largest power of p that divides the class number of F_n. If e_n is bounded then it follows (trivially) that the p-rank is bounded. Thus, the following corollary is immediate.

Corollary 4.8. *Let $p \neq q$. Let $F/\mathbb{Q}$ be any finite extension of $\mathbb{Q}$ and F_∞/F be any $\mathbb{Z}_q$-extension of F. Let p^{e_n} be the exact power of p dividing the class number of the n-th intermediate field F_n. Let $A_{/F}$ be an abelian variety such that $A[p] \subseteq A(F)$. If e_n is bounded as $n \to \infty$, then $r_p\left(\mathrm{Sel}_0\left(A/F_n\right)\right)$ is bounded independently of n.*

In addition to Theorem A, there are some other results in the literature where it is known that the p-part of the class group stabilizes in a $\mathbb{Z}_q$-extension (when p, q are distinct primes). These were discussed briefly in the Introduction and are recorded here more precisely.

(1) ([Was78, Theorem]) Let $F/\mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ and F_∞/F be the cyclotomic $\mathbb{Z}_q$-extension of F. If p^{e_n} be the exact power of p dividing the class number of the n-th intermediate field F_n, then e_n is bounded as $n \to \infty$.

(2) ([Lam15, Theorem 7.10]) Let p, q be fixed odd distinct primes both ≥ 5, K be an imaginary quadratic field of class number 1 where p and q split, and $E_{/K}$ be an elliptic curves with CM by $\mathcal{O}_K$ and good reduction at p, q. Let K_∞ be the $\mathbb{Z}_q$ extensions of K which is unramified outside $\mathfrak{q}$ (resp. $\overline{\mathfrak{q}}$). Let $\mathfrak{g}$ be a fixed ideal of $\mathcal{O}_K$ such that it is coprime to pq and $F = \mathscr{R}(\mathfrak{g}\mathfrak{q})$ is of degree prime-to-p over F. Then, the p-part of the class number

stabilizes in $FK_\infty = \mathscr{R}(\mathfrak{g}\mathfrak{q}^\infty)$. However, since p is assumed to be unramified in F in *loc. cit.*, the hypothesis $A[p] \subseteq A(F)$ in Theorem 4.3 is unlikely to hold. The same can be said regarding the setting studied in Theorem A.

Theorem 4.9. *With notation as above, suppose that the p-rank of the fine Selmer group, $r_p\left(\mathrm{Sel}_0(A/F_n)\right)$ stabilizes in a $\mathbb{Z}_q$-extension of F. Then there exists $n \gg 0$, such that for all $m \geq n$*

$$\mathrm{Sel}_0(A/F_n) = \mathrm{Sel}_0(A/F_m).$$

Proof. The following argument is similar to the one presented in [Lam14, p. 15], where instead of classical Selmer groups, we consider fine Selmer groups. Consider the extension F_m/F_n. Then $[F_m : F_n] = q^{m-n} = t$ (say). The restriction map

$$\mathrm{Gal}\left(\overline{F}/F_n\right) \longrightarrow \mathrm{Gal}\left(\overline{F}/F_m\right)$$

induces the restriction homomorphism

$$\mathrm{res} : \mathrm{Sel}_0(A/F_n) \longrightarrow \mathrm{Sel}_0(A/F_m).$$

Since $\gcd(q,p) = 1$, this maps is an injection. Moreover, we have

$$\mathrm{Sel}_0(A/F_n) \xrightarrow{\mathrm{res}} \mathrm{Sel}_0(A/F_m) \xrightarrow{\mathrm{cores}} \mathrm{Sel}_0(A/F_n) \xrightarrow{t^{-1}} \mathrm{Sel}_0(A/F_n)$$

where $\mathrm{cores} \circ \mathrm{res} = \mathrm{t}$. Since the composition $\mathrm{res} \circ \mathrm{cores} \circ \mathrm{t}^{-1}$ is the identity map, the exact sequence

$$0 \longrightarrow \mathrm{Sel}_0(A/F_n) \longrightarrow \mathrm{Sel}_0(A/F_m) \longrightarrow \mathrm{Sel}_0(A/F_m)\big/ \mathrm{Sel}_0(A/F_n) \longrightarrow 0$$

is split exact.

Let us write $\mathrm{Sel}_0(A/F_n) = (\mathbb{Q}_p/\mathbb{Z}_p)^{s_n} \oplus T_n$, where $s_n \geq 0$ and T_n is a finite p-group. Then,

$$r_p\left(\mathrm{Sel}_0(A/F_n)\right) = s_n + r_p(T_n).$$

The injection $\mathrm{Sel}_0(A/F_n) \hookrightarrow \mathrm{Sel}_0(A/F_m)$ tells us that $s_m \geq s_n$. If the p-rank $r_p\left(\mathrm{Sel}_0(A/F_n)\right)$ eventually stabilizes it follows that s_n also stabilizes. In particular, the cokernel of the injection, which we denote by $C_{m,n}$, is finite when $n \gg 0$. By duality, we have the short exact sequence

$$0 \to C_{m,n}^\vee \to \mathbb{Z}_p^{s_m} \oplus T_m \to \mathbb{Z}_p^{s_n} \oplus T_n \to 0.$$

When $s_m = s_n$, $C_{m,n}$ has to be finite. Consequently, the image of $C_{m,n}^\vee$ in $\mathrm{Sel}_0(A/F_n)^\vee$ is contained inside T_m. Furthermore, since the short exact sequence splits, we deduce the isomorphism

$$T_m = T_n \oplus C_{m,n}^\vee.$$

As s_n stabilizes, $r_p(T_n)$ also stabilizes. Therefore, $C_{m,n}^\vee$ has to be 0 eventually. $\square$

Theorem B is now an immediate corollary of Theorems 4.3 and 4.9.

Corollary 4.10. *Let p, q be distinct odd primes. Let F be any number field and $A_{/F}$ be an abelian variety such that $A[p] \subseteq A(F)$. Let F_∞/F be a $\mathbb{Z}_q$-extension where the primes above q, the primes of bad reduction of A, and the archimedean primes are finitely decomposed. If the p-part of the class group stabilizes, i.e., there exists $N \gg 0$ such that for all $n \geq N$,*

$$\mathrm{ord}_p(h(F_n)) = \mathrm{ord}_p(h(F_N)),$$

then the growth of the p-primary fine Selmer group stabilizes in the $\mathbb{Z}_q$-extension as well, i.e., for all $n \geq N$,

$$\mathrm{Sel}_0(A/F_n) = \mathrm{Sel}_0(A/F_N).$$

Appendix A. Existence of CM elliptic curves with only split primes in the conductor

In this appendix, we give an elementary proof that given any imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ of class number 1, there exists a CM elliptic curve (over K) such that it has conductor divisible only by split primes of K. The imaginary quadratic fields of class number 1 are precisely the following

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{-11}),\ \mathbb{Q}(\sqrt{-19}),\ \mathbb{Q}(\sqrt{-43}),\mathbb{Q}(\sqrt{-67}),\ \mathbb{Q}(\sqrt{-167}).$$

When $d = 1, 2,$ and 3, we produce explicit examples. For $d \geq 7$, we can prove a general result.

Let K denote one of the nine imaginary quadratic fields with class number 1. Suppose that $E_{/K}$ is an elliptic curve with CM by an order $\mathcal{O}$ in K. We know that the j-invariant $j(E)$ is an integer in this case, so E must be a twist of the base extension of an elliptic curve defined over $\mathbb{Q}$. For $d > 3$, the base curve is uniquely determined (up to isomorphism over K) by the condition that it has CM by $\mathcal{O}_K$ and bad reduction at the ramified prime $\mathfrak{p} = (\sqrt{-d})$. For $d = 1, 2,$ and 3 there are several choices for the elliptic curve over $\mathbb{Q}$ (see [CP19, Remark 3.1]).

(i) Case $K = \mathbb{Q}(\sqrt{-1})$.
The discriminant of K is $D_K = -4$. Consider the elliptic curve $E =$ 25.1-CMa1. This elliptic curve is a twist of 256.1-CMa1 which is a base change of 64.a4. It has bad reduction only at $2 + \sqrt{-1}$ which is a split prime above 5 since

$$5 = (2 + \sqrt{-1})(2 - \sqrt{-1}).$$

(ii) Case $K = \mathbb{Q}(\sqrt{-2})$.
The discriminant of K is $D_K = -8$. Consider the elliptic curve 256.d1 over $\mathbb{Q}$ and its base change to K is the elliptic curve 1024.1-CMb1. A twist of this latter curve is $E =$ 9.3-CMa1 which has bad reduction only at $1 - \sqrt{-2}$, which is a split prime above 3 since

$$3 = (1 + \sqrt{-2})(1 - \sqrt{-2}).$$

(iii) Case $K = \mathbb{Q}(\sqrt{-3})$.
The discriminant of K is $D_K = -3$. Consider the elliptic curve $E =$ 2401.3-CMa1 which arises as a twist of 81.1-CMa1. This latter curve is obtained by base extension of 27.a4 over $\mathbb{Q}$. The primes of bad reduction of E are both primes in K above 7, which admits the splitting

$$7 = (2 + \sqrt{-3})(2 - \sqrt{-3}).$$

(iv) Other cases.
When K is one of the remaining imaginary quadratic fields, the discriminant $D_K = -d \equiv 1 \pmod 4$. In the following proposition, we show that in this case as well there always exist CM elliptic curves with bad reduction only at split primes.

Proposition A.1. *Let $d > 3$ and $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with class number 1. There exists an elliptic curve over K with CM by $\mathcal{O}_K$ whose conductor is divisible only by primes that split in K.*

Proof. For $d = 7, 11, 19, 43, 67,$ and 167, fix the following elliptic curves $A_{/\mathbb{Q}}$: 49.a4, 121.b2, 361.a2, 1849.b2, 4489.b2, and 26569.a2, respectively. As explained above, any elliptic curve over K with CM by $\mathcal{O}_K$ is obtained as a quadratic twist of the respective $A_{/K}$.

Henceforth, set $\mathfrak{P} = \sqrt{-d}$. It follows from [CP19, Theorem 3.3] that if we twist $A_{/K}$ by a character corresponding to $K(\sqrt{\alpha})$ where $\alpha = \mathfrak{P}\mathfrak{Q}$ such that $\mathfrak{Q}$ is a prime of K distinct from $\mathfrak{P}$

satisfying $\mathfrak{Q} \equiv u^2\sqrt{-d} \mod 4\mathcal{O}_K$ for some $u \in \mathcal{O}_K$, then the twisted elliptic curve (over K) has good reduction everywhere except at $\mathfrak{Q}$. Therefore, it is enough to show that we may choose $\mathfrak{Q}$ to be a split prime in K.

Let $r \in \mathbb{Z}$ such that $(4r + \sqrt{-d})(4r - \sqrt{-d}) = 16r^2 + d$ is an odd rational prime. Such r exists for all possible values of d. For example, we may take r to be 1 when $d = 7, 43, 67$, $r = 2$ when $d = 19$, $r = 3$ when $d = 167$ and $r = 6$ when $d = 11$. Then $4r + \sqrt{-d}$ is a split prime of K and $4r + \sqrt{-d} \equiv 1^2\sqrt{-d} \mod 4\mathcal{O}_K$. In particular, we may apply [CP19, Theorem 3.3] with $\mathfrak{q} = 4r + \sqrt{-d}$ and $u = 1$. This completes the proof of the proposition. □

References

[CP19] John Cremona and Ariel Pacetti, *On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1*, Proc. London Math. Soc. **118** (2019), no. 5, 1245–1276.

[dS87] Ehud de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3, Academic Press, Orlando, 1987.

[Gre78] Ralph Greenberg, *On the structure of certain Galois groups*, Invent. math. **47** (1978), no. 1, 85–99.

[Hid07] Haruzo Hida, *Non-vanishing modulo p of Hecke L-values and application*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 207–269.

[Lam14] Jack Lamplugh, *Class numbers and Selmer groups in $\mathbb{Z}_S$-extensions of imaginary quadratic fields*, 2014, Thesis (PhD), University of Cambridge.

[Lam15] ———, *An analogue of the Washington–Sinnott theorem for elliptic curves with complex multiplication I*, J. London Math. Soc. **91** (2015), no. 3, 609–642.

[LM16] Meng Fai Lim and V Kumar Murty, *The growth of fine Selmer groups*, J. Ramanujan Math. Soc. 31, no. 1, 79–94 (2016).

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), no. 3-4, 183–266.

[NSW08] Jurgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, vol. 323 of Fundamental Principles of Mathematical Sciences, Springer-Verlag, Berlin, 2008.

[Rub91] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.

[Was75] Lawrence C Washington, *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. **214** (1975), no. 2, 177–193.

[Was78] ———, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math. **49** (1978), no. 1, 87–97.

(Kundu) Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada

Email address: dkundu@math.ubc.ca

(Lei) Département de Mathématiques et de Statistique, Université Laval, Pavillion Alexandre-Vachon, 1045 Avenue de la Médecine, Québec, QC, Canada G1V 0A6

Email address: antonio.lei@mat.ulaval.ca