ACYCLOTOMY OF TORSION IN THE CM CASE

MICHAEL CHOU, PETE L. CLARK, AND MARKO MILOSEVIC

Abstract. Let F be a number field, and let F^{cyc} be obtained by adjoining to F all the roots of unity. We show that as E ranges over all elliptic curves defined over F^{cyc} with complex multiplication, the torsion subgroups $E(F^{\mathrm{cyc}})$ are finite and uniformly bounded in size.

–

1. Introduction

1.1. **Notation and terminology.** For a field F, we write $\overline{F}$ for a separable algebraic closure and $\mathfrak{g}_F$ for $\mathrm{Aut}(\overline{F}/F)$. We identify étale group schemes $G_{/F}$ with their associated $\mathfrak{g}_F$-modules $G(\overline{F})$. For a commutative group A we denote the torsion subgroup by $A[\mathrm{tors}]$.

Here, a number field is a subfield of F of $\mathbb{C}$ with $[F:\mathbb{Q}]$ finite. For a field F of characteristic 0, we put $F^{\mathrm{cyc}} := \bigcup_{n\geq 1} F(\zeta_n)$, the field obtained by adjoining to F all the roots of unity. Let F^{ab} be the maximal abelian extension of F. We have $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$ – the Kronecker-Weber Theorem.

A complex number j is a **singular modulus** if there is an elliptic curve $E_{/\mathbb{C}}$ with $j(E) = j$ and complex multiplication (CM); otherwise we say j is a **nonsingular modulus**. If $j \in \mathbb{C}$ is a singular modulus, then $j \in \overline{\mathbb{Q}}$.

1.2. **Results.** Here is our main result.

Theorem 1.1. *Let $F \subset \mathbb{C}$ be a number field. There is a positive integer $B = B(F)$ such that: for all elliptic curves $E_{/F^{\mathrm{cyc}}}$ with complex multiplication, we have*

$$\#E(F^{\mathrm{cyc}})[\mathrm{tors}] \leq B.$$

Theorem 1.1 follows immediately from the following more precise results.

Theorem 1.2. *For any number field $F \subset \mathbb{C}$, the field F^{cyc} contains only finitely many singular moduli.*

Theorem 1.3. *Let $F \subset \mathbb{C}$ be a number field, let K be an imaginary quadratic field, let $\mathcal{O}$ be an order in K, let $\mathcal{O}_K$ be the ring of integers of K and let $h_2(\mathcal{O}_K) = \#(\mathrm{Pic}\,\mathcal{O}_K)[2]$ be the 2-part of the class number of K.*
a) For any $\mathcal{O}$-CM elliptic curve $E_{/F^{\mathrm{cyc}}}$, there is an $\mathcal{O}_K$-CM elliptic curve $E'_{/F^{\mathrm{cyc}}}$ such that

$$\#E(F^{\mathrm{cyc}})[\mathrm{tors}] \leq \#E'(F^{\mathrm{cyc}})[\mathrm{tors}].$$

b) Let $E_{/F^{\mathrm{cyc}}}$ be an $\mathcal{O}_K$-CM elliptic curve. Then:
(i) If $E(F^{\mathrm{cyc}})$ has a point of order ℓ, then ℓ ramifies in K or

$$\ell \leq 12h_2(\mathcal{O}_K)[F:\mathbb{Q}] + 1.$$

Date: October 22, 2019.

(ii) If ℓ does not ramify in K and $E(F^{\mathrm{cyc}})$ has a point of order ℓ^a, then

$$\varphi(\ell^a) \leq 12h_2(\mathcal{O}_K)[F:\mathbb{Q}].$$

(iii) If ℓ ramifies in K and $E(F^{\mathrm{cyc}})$ has a point of order ℓ^a, then

$$\varphi(\ell^{a-1}) \leq 12h_2(\mathcal{O}_K)[F:\mathbb{Q}].$$

c) Assume the Generalized Riemann Hypothesis. Then:
(i) There is a CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with a $\mathbb{Q}^{\mathrm{ab}}$-rational point of prime order ℓ iff $\ell \in \{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,89,163\}$.
(ii) There are 101 imaginary quadratic orders $\mathcal{O}$ such that there is an elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with $\operatorname{End} E \cong \mathcal{O}$. The fraction fields of these orders yield 65 different imaginary quadratic fields. For each such imaginary quadratic field K, we determine[1] the positive integer $T(K)$ that is the least common multiple of $\#E(\mathbb{Q}^{ab})[\mathrm{tors}]$ as E ranges over all K-CM elliptic curves defined over $\mathbb{Q}^{\mathrm{ab}}$.

Our definition of $T(K)$ is natural but also somewhat self-serving: to compute $T(K)$ it suffices to calculate (maximal) ℓ-primary torsion subgroups of $\mathcal{O}_K$-CM elliptic curves $E_{/\mathbb{Q}^{\mathrm{ab}}}$, and that is what we do.

We also have the following result in the non-CM case.

Theorem 1.4. *Let $j \in \overline{\mathbb{Q}}$ be a nonsingular modulus, and let F be a number field containing j. Then there is a positive integer $T = T(F,j)$ such that for every elliptic curve $E_{/F^{\mathrm{ab}}}$ with $j(E) = j$, we have $\#E(F^{\mathrm{ab}})[\mathrm{tors}] \leq T$.*

Theorem 1.4 should be compared to Theorem 1.3: in the CM case, fixing the j-invariant is (up to Galois conjugacy, which is harmless) the same as fixing the endomorphism ring, so after Theorem 1.2 the matter of the CM case is to deal with a fixed j-invariant. It is interesting that Theorem 1.4, though less quantitatively precise than Theorem 1.3, is stronger in that we work over F^{ab} rather than just F^{cyc}: these coincide when $F = \mathbb{Q}$ but in general $F^{\mathrm{ab}}/F^{\mathrm{cyc}}$ has infinite degree. On the other hand, there is certainly no analogue of Theorem 1.2 in the non-CM case!

This also raises the prospect of a strengthened version of Theorem 1.1 to F^{ab} in place of F^{cyc}. We take this up in §6, extending Theorem 1.1 from F^{cyc} to F^{ab} for "most" number fields F.

1.3. **Acknowledgments.** We thank John Voight for the question that inspired this note and Abbey Bourdon and James H. Stankewicz for helpful comments.

2. Comments on related work

2.1. **Najman.** The second named author first proved Theorem 1.1 in the case $F = \mathbb{Q}$, prompted by a conversation with John Voight in 2015. Voight suggested to give special consideration to torsion points of CM elliptic curves over cyclotomic fields. In this regard, he was motivated by the following result of Najman, which gives one of very few known non-CM sporadic points on modular curves.

Theorem 2.1 (Najman [Na16])**.** *There is exactly one pair (E,F) where $E_{/\mathbb{Q}}$ is an elliptic curve, $F/\mathbb{Q}$ is a cubic number field, and $E(F)$ has a point of order 21:*

$$E_{/\mathbb{Q}} : y^2 + xy + y = x^3 - x^2 - 5x + 5,\ F = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}).$$

[1]Please see the table at the end of the document.

Najman also found [Na16, §6] an abelian sextic number field F and an elliptic curve $E_{/F}$ such that $E(F)$ has a point of order 37. In each case, the corresponding closed point P on $X_1(N)$ – i.e., the degree 3 point on $X_1(21)$ and the degree 6 point on $X_1(37)$ – is **sporadic** in the sense that there are only finitely many closed points of degree at most the degree of P. Let us also call a closed point P on a nice curve $X_{/\mathbb{Q}}$ **of low degree** if its degree is less than the least degree of a nonconstant $\mathbb{Q}$-morphism $f : X \to \mathbb{P}^1$. Sporadic points have low degree, but the converse does not always hold.

It seems interesting to ask whether there are further low degree non-cuspidal points on $X_1(N)$ with abelian field of moduli.

2.2. **Ribet and Zarhin.** Since F^{cyc} has infinite degree over $\mathbb{Q}$, for a CM elliptic curve $E_{/F^{\mathrm{cyc}}}$ it is not even obvious that $E(F^{\mathrm{cyc}})[\mathrm{tors}]$ is finite. However this result and more was already known.

Theorem 2.2 (Ribet [KL81])**.** *Let $A_{/F}$ be an abelian variety over a number field. Then $A(F^{\mathrm{cyc}})[\mathrm{tors}]$ is finite.*

In an earlier draft we used Theorem 2.2 to prove the boundedness of torsion on CM elliptic curves over $\mathbb{Q}^{\mathrm{ab}}$. Our current proof does not make use of Theorem 2.2, but our proof of Theorem 1.4 makes use of the following related result.

Theorem 2.3 (Zarhin [Za87])**.** *Let $A_{/F}$ be an abelian variety over a number field. Then A is isogenous over F to $\prod_{i=1}^n A_i$ with each A_i an F-simple abelian variety. Then $A(F^{\mathrm{ab}})[\mathrm{tors}]$ is finite iff no A_i is of CM-type: more precisely, for all $1 \leq i \leq n$, the ring $\mathrm{End}_F A_i$ is* not *an order in a number field of degree $2 \dim A_i$.*

2.3. **Chou.** Work of the first named author [Ch17] studies the groups $E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}]$ as E ranges over all elliptic curves defined over $\mathbb{Q}$. For this family Chou obtains a complete, finite classification of the torsion subgroups.

The largest torsion subgroup that appears in Chou's classification is $\mathbb{Z}/163\mathbb{Z}$. This group arises from an elliptic curve $E_{/\mathbb{Q}}$ with CM by the imaginary quadratic order $\mathcal{O}$ of discriminant -163: Let $\mathfrak{p}$ be the prime ideal of the $\mathcal{O}$ of norm 163; then $E \to E/E[\mathfrak{p}]$ is a $\mathbb{Q}$-rational cyclic 163-isogeny. The isogeny character trivializes over an abelian extension of $\mathbb{Q}$, yielding a point of order 163 over $\mathbb{Q}^{\mathrm{ab}}$. We will see in Proposition 4.2a) that for any imaginary quadratic field K such that the Hilbert class field $K^{(1)}$ is abelian over $\mathbb{Q}$ and any prime ℓ that ramifies in K, there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with a $\mathbb{Q}^{\mathrm{ab}}$-rational point of order ℓ.

The largest value of $\#E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty]$ for any CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ and any prime number ℓ is 163, again coming from an elliptic curve $E_{/\mathbb{Q}}$ with CM by the order of discriminant -163. This seems somewhat coincidental, since there are values of $\#E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty]$ that are only attained for elliptic curves E with $j(E) \notin \mathbb{Q}$, e.g. 89. While $T(\mathbb{Q}(\sqrt{-163})) = 163$, there are imaginary quadratic fields K with $K^{(1)}/\mathbb{Q}$ abelian such that $T(K) > 163$: the largest such value is

$$T(\mathbb{Q}(\sqrt{-3})) = 529200.$$

We leave to a later work an analysis of the extent to which different ℓ-primary torsion subgroups can be simultaneously realized over $\mathbb{Q}^{\mathrm{ab}}$. But we do not know of any CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ such that $\#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}]$ is divisible by two distinct odd primes, and we find it plausible that the largest value of $\#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}]$ is 163.

3. The Proofs

3.1. **The Basic Strategy.**

Let $\{(A_i)_{/F_i}\}_{i\in I}$ be a family of abelian varieties of uniformly bounded dimension defined over a family of fields $\{F_i\}_{i\in I}$. Then $\sup_{i\in I} \#A_i(F_i)[\mathrm{tors}] < \infty$ iff both of the following hold:

(B1) The set of primes ℓ dividing some $\#A_i(F_i)[\mathrm{tors}]$ is finite;
(B2) For all primes ℓ, there is $a \in \mathbb{Z}^+$ such that no $A_i(F_i)$ has a point of order ℓ^a.

3.2. **Ring class fields.** Let $\mathcal{O}$ be an order in an imaginary quadratic field K, of conductor $\mathfrak{f} \in \mathbb{Z}^+$ and discriminant $\Delta \in \mathbb{Z}^-$. Let $H_\Delta \in \mathbb{Q}[t]$ be the Hilbert class polynomial of Δ: it is the squarefree polynomial whose roots are the j-invariants of $\mathcal{O}$-CM elliptic curves, and it is irreducible over K. We put

$$\mathbb{Q}(\mathfrak{f}) \coloneqq \mathbb{Q}[t]/(H_\Delta),\ K(\mathfrak{f}) \coloneqq K[t]/(H_\Delta).$$

The field $K(\mathfrak{f})$ is the **ring class field of** $\mathcal{O}$; when $\mathfrak{f} = 1$ this is the **Hilbert class field** of K. The extension $K(\mathfrak{f})/K$ is abelian with $\mathrm{Aut}(K(\mathfrak{f})/K)$ canonically isomorphic to the class group $\operatorname{Pic}\mathcal{O}$ of $\mathcal{O}$. The extension $K(\mathfrak{f})/\mathbb{Q}$ is Galois, and complex conjugation c gives a splitting of the short exact sequence

$$1 \to \mathrm{Aut}(K(\mathfrak{f})/K) \to \mathrm{Aut}(K(\mathfrak{f})/\mathbb{Q}) \to \mathrm{Aut}(K/\mathbb{Q}) \to 1,$$

so

$$\mathrm{Aut}(K(\mathfrak{f})/\mathbb{Q}) \cong \operatorname{Pic}\mathcal{O} \rtimes \mathbb{Z}/2\mathbb{Z},$$

where the action of the nontrivial element c of $\mathbb{Z}/2\mathbb{Z}$ on $\operatorname{Pic}\mathcal{O}$ is by $x \mapsto x^{-1}$. Put

$$h(\mathcal{O}) \coloneqq \#\operatorname{Pic}\mathcal{O},\ h_2(\mathcal{O}) \coloneqq \#(\operatorname{Pic}\mathcal{O})[2],\ \overline{h}(\mathcal{O}) \coloneqq \frac{h(\mathcal{O})}{h_2(\mathcal{O})}.$$

The quantity $h_2(\mathcal{O})$ is completely known: see e.g. [Cx, Prop. 3.11]. In particular, if r is the number of odd prime divisors of D, then $h_2(\mathcal{O}) = 2^{r+\epsilon(\mathcal{O})}$ for $\epsilon(\mathcal{O}) \in \{0,1,2\}$. It is a deep result of Heilbronn [He34] that for any $M \in \mathbb{Z}^+$, there are only finitely many imaginary quadratic fields K such that $\overline{h}(\mathcal{O}_K) \le M$.

Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders in the same imaginary quadratic field K, of conductors $\mathfrak{f}$ and $\mathfrak{f}'$. Then we have $\mathcal{O}' \subset \mathcal{O} \iff \mathfrak{f} \mid \mathfrak{f}'$. Let us assume that these conditions hold. Then we have $K(\mathfrak{f}) \subset K(\mathfrak{f}')$, and the corresponding surjection $\operatorname{Pic}\mathcal{O}' \to \operatorname{Pic}\mathcal{O}$ is the natural pushforward $I \mapsto I\mathcal{O}$ of fractional ideals. For any surjection $A \to B$ of commutative groups, there is an induced surjection $A/A[2] \to B/B[2]$, hence $\overline{h}(\mathcal{O}) \mid \overline{h}(\mathcal{O}')$. (Since $\operatorname{Pic}\mathcal{O}' \to \operatorname{Pic}\mathcal{O}$ is a surjection, so is $\operatorname{Pic}\mathcal{O}'/(2\operatorname{Pic}\mathcal{O}') \to \operatorname{Pic}\mathcal{O}/(2\operatorname{Pic}\mathcal{O})$, and since $\operatorname{Pic}\mathcal{O}$ is finite we have $h_2(\mathcal{O}) = \#\operatorname{Pic}\mathcal{O}/(2\operatorname{Pic}\mathcal{O})$, which shows that also $h_2(\mathcal{O}) \mid h_2(\mathcal{O}')$.) Moreover:

$$\frac{h(\mathcal{O}(a\mathfrak{f}))}{h(\mathcal{O}(\mathfrak{f}))} = \frac{a}{[\mathcal{O}(\mathfrak{f})^\times : \mathcal{O}(a\mathfrak{f})^\times]} \prod_{p \mid a} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right) \in \mathbb{Z}^+. \tag{1}$$

Put $w_K \coloneqq \mathcal{O}_K^\times$, so $w_K = 6$ if $K = \mathbb{Q}(\sqrt{-3})$, $w_K = 4$ if $K = \mathbb{Q}(\sqrt{-1})$ and $w_K = 2$ otherwise. Thus we get

$$\frac{h(\mathcal{O}(\mathfrak{f}))}{h(\mathcal{O}_K)} \ge \frac{\varphi(\mathfrak{f})}{w_K} \ge \frac{\varphi(\mathfrak{f})}{6} \gg \frac{\mathfrak{f}}{\log\log\mathfrak{f}}, \tag{2}$$

the last inequality by a result of Mertens [HW, Thm. 429]. In particular, for each fixed K, there are only finitely many orders in K of bounded class number. Thus Heilbronn's result implies the following one.

Lemma 3.1. *For every $M \in \mathbb{Z}^+$, there are only finitely many imaginary quadratic orders $\mathcal{O}$ such that $\overline{h}(\mathcal{O}) \leq M$.*

Again we fix an imaginary quadratic order $\mathcal{O}$ of conductor $\mathfrak{f}$ and discriminant Δ. We define the **genus field**

$$G(\mathfrak{f}) \coloneqq K(\mathfrak{f}) \cap \mathbb{Q}^{\mathrm{ab}},$$

i.e., the maximal subextension of $K(\mathfrak{f})$ that is abelian over $\mathbb{Q}$. The group $\mathrm{Aut}(G(\mathfrak{f})/\mathbb{Q})$ is the abelianization of $\mathrm{Aut}(K(\mathfrak{f})/\mathbb{Q})$. It follows that

$$\mathrm{Aut}(G(\mathfrak{f})/\mathbb{Q}) \cong (\mathrm{Pic}\,\mathcal{O})[2] \times \mathbb{Z}/2\mathbb{Z}$$

and thus

$$[K(\mathfrak{f}) : G(\mathfrak{f})] = \overline{h}(\mathcal{O}),\ [G(\mathfrak{f}) : \mathbb{Q}] = 2h_2(\mathcal{O}).$$

Since $\mathbb{Q}^{\mathrm{ab}}$ and $K(\mathfrak{f})$ are linearly disjoint over $G(\mathfrak{f})$, we have

$$[K(\mathfrak{f})\mathbb{Q}^{\mathrm{ab}} : \mathbb{Q}^{\mathrm{ab}}] = [K(\mathfrak{f}) : K(\mathfrak{f}) \cap \mathbb{Q}^{\mathrm{ab}}] = \overline{h}(\mathcal{O}).$$

From this we deduce the following key result.

Lemma 3.2. *For an imaginary quadratic order $\mathcal{O}$ and a number field F, we have*

$$[K(\mathfrak{f})F^{\mathrm{cyc}} : F^{\mathrm{cyc}}] \geq \frac{[K(\mathfrak{f})\mathbb{Q}^{\mathrm{ab}} : \mathbb{Q}^{\mathrm{ab}}]}{[F : \mathbb{Q}]} = \frac{\overline{h}(\mathcal{O})}{[F : \mathbb{Q}]}.$$

Proof. Since $[F^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{ab}}] = [F\mathbb{Q}^{\mathrm{ab}} : \mathbb{Q}^{\mathrm{ab}}] \leq [F : \mathbb{Q}]$, we have

$$[K(\mathfrak{f})F^{\mathrm{cyc}} : F^{\mathrm{cyc}}] = \frac{[K(\mathfrak{f})F^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{ab}}]}{[F^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{ab}}]} = \frac{[K(\mathfrak{f})F^{\mathrm{cyc}} : K(\mathfrak{f})\mathbb{Q}^{\mathrm{ab}}][K(\mathfrak{f})\mathbb{Q}^{\mathrm{ab}} : \mathbb{Q}^{\mathrm{ab}}]}{[F^{\mathrm{cyc}} : \mathbb{Q}^{\mathrm{ab}}]}$$

$$\geq \frac{[K(\mathfrak{f})\mathbb{Q}^{\mathrm{ab}} : \mathbb{Q}^{\mathrm{ab}}]}{[F : \mathbb{Q}]} = \frac{\overline{h}(\mathcal{O})}{[F : \mathbb{Q}]}. \qquad \square$$

3.3. **Proof of Theorem 1.2.** Let F be a number field. In order to establish that only finitely many singular moduli lie in F^{cyc} it is no loss of generality to assume that $F/\mathbb{Q}$ is Galois. This is not crucial, but it simplifies matters: under that assumption, for each imaginary quadratic order $\mathcal{O}$, either we have $j(E) \in F$ for every $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{C}}$ or for no $\mathcal{O}$-CM elliptic curve. So let $\mathcal{O}$ be an imaginary quadratic order, with conductor $\mathfrak{f}$, such that $j(\mathbb{C}/\mathcal{O}) \in F^{\mathrm{cyc}}$. Since $F^{\mathrm{cyc}} \supset \mathbb{Q}^{\mathrm{ab}} \supset K$, this implies that $K(\mathfrak{f}) \subset F^{\mathrm{cyc}}$, and now Lemma 3.2 gives

$$\overline{h}(\mathcal{O}) \leq [F : \mathbb{Q}].$$

By Lemma 3.1 there are only finitely many such orders $\mathcal{O}$, and since each $\mathcal{O}$ gives rise to $\mathrm{Pic}\,\mathcal{O}$ singular moduli, only finitely many singular moduli lie in F^{cyc}.

3.4. **Proof of Theorem 1.3a).** Let $\mathcal{O}$ be an order of conductor $\mathfrak{f}$ in the imaginary quadratic field K, and let $\mathcal{O}_K$ be the maximal order. Let F be a field of characteristic 0, and let $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve. Then (e.g. [Kw99, §2], [BP17, Prop. 2.2] or [BC2, §2.5]) there is an $\mathcal{O}_K$-CM elliptic curve $(E')_{/F}$ and an F-rational cyclic $\mathfrak{f}$-isogeny $\iota : E \to E'$. The existence of ι and the dual isogeny $\iota^\vee : E' \to E$ shows

$$\#E(F)[\mathrm{tors}] \mid \mathfrak{f}\#E'(F)[\mathrm{tors}] \mid \mathfrak{f}^2\#E(F)[\mathrm{tors}].$$

This bound is sufficient to prove Theorem 1.1, since Theorem 1.2 reduces us to the case of fixed $\mathcal{O}$, which we can then replace by $\mathcal{O}_K$ at a cost of introducing a factor of $\mathfrak{f}$. However, one can do better: in the above setup if F is moreover a number field containing the CM field K, then by [BC, Thm. 1.7] we have

$$\#E(F)[\mathrm{tors}] \mid \#E'(F)[\mathrm{tors}].$$

From this it follows that for every $\mathcal{O}$-CM elliptic curve $E_{/F^{\mathrm{cyc}}}$ there is an $\mathcal{O}_K$-CM elliptic curve $(E')_{/F^{\mathrm{cyc}}}$ with

$$\#E(F^{\mathrm{cyc}})[\mathrm{tors}] \mid \#E'(F^{\mathrm{cyc}})[\mathrm{tors}].$$

3.5. **Torsion points and ray class containments.** We begin by recalling the following classical result.

Theorem 3.3. *(First Main Theorem of Complex Multiplication) Let $E_{/\mathbb{C}}$ be an $\mathcal{O}_K$-CM elliptic curve, and let I be a nonzero ideal of $\mathcal{O}_K$. Let $\mathfrak{h} : E \to \mathbb{P}^1$ be a Weber function. Then:*

$$K^{(1)}(\mathfrak{h}(E[I])) = K^I.$$

Proof. See e.g. [Si94, Thm. II.5.6]. □

In light of Theorem 3.3 it is useful to know the degree $[K^I : K^{(1)}]$, which is a standard result (see [Ch, Cor. 3.2.4] and [BC, Lemma 2.10]):

Lemma 3.4. *Let I be a nonzero ideal of K, and let K^I be the I-**ray class field**. We put $U(K) \coloneqq \mathcal{O}_K^\times$, $U_I(K) \coloneqq \{x \in U(K) \mid x - 1 \in I\}$ and*

$$\varphi_K(I) \coloneqq \#(\mathcal{O}_K/I)^\times = |I| \prod_{\mathfrak{p} \mid I} \left(1 - \frac{1}{|\mathfrak{p}|}\right).$$

a) We have

$$[K^I : K^{(1)}] = \frac{\varphi_K(I)}{[U(K) : U_I(K)]}.$$

b) If $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then

$$[K^I : K^{(1)}] = \begin{cases} \varphi_K(I) & I \mid (2) \\ \frac{\varphi_K(I)}{2} & I \nmid (2) \end{cases}.$$

c) If $K = \mathbb{Q}(\sqrt{-1})$, then

$$[K^I : K^{(1)}] = \begin{cases} \varphi_K(I) & I \mid (1+i) \\ \frac{\varphi_K(I)}{2} & I \nmid (1+i) \text{ and } I \mid (2) \\ \frac{\varphi_K(I)}{4} & I \nmid (2) \end{cases}.$$

d) If $K = \mathbb{Q}(\sqrt{-3})$, then

$$[K^I : K^{(1)}] = \begin{cases} 1 & I = (1) \\ \frac{\varphi_K(I)}{2} & I \neq (1) \text{ and } I \mid (\zeta_3 - 1) \\ \frac{\varphi_K(I)}{3} & I = (2) \\ \frac{\varphi_K(I)}{6} & \text{otherwise} \end{cases}.$$

Let $N \geq 2$. Applying Theorem 3.3 with $I = (N)$, we get that if for an $\mathcal{O}_K$-CM elliptic curve $E_{/F^{\mathrm{cyc}}}$ we have $(\mathbb{Z}/N\mathbb{Z})^2 \hookrightarrow E(F^{\mathrm{cyc}})$, then $F^{\mathrm{cyc}} \supset K^{(N)} \supset K(N)$. As we've seen, for each fixed F this containment can hold for only finitely many integers N. However, this only bounds the possibilities for full N-torsion. In order to check Conditions (B1) and (B2) we need the following refinement.

Proposition 3.5. *Let K be an imaginary field, ℓ a prime number, and $a \in \mathbb{Z}^+$. Let $F \subset \mathbb{C}$ be a field containing K and a primitive ℓ^ath root of unity. Let $E_{/F}$ be an $\mathcal{O}_K$-CM elliptic curve with an F-rational point of order ℓ^a.*
a) If $\ell \nmid \Delta_K$, then F contains the ray class field $K^{(\ell^a)}$.
b) If $\ell \mid \Delta_K$, let $\mathfrak{p}$ be the unique prime of $\mathcal{O}_K$ lying over (ℓ). Then F contains the ray class field $K^{\mathfrak{p}^{2a-1}}$.

Proof. Let $P \in E(F)$ be a point of order ℓ^a. Since F contains the CM field K, the endomorphisms are F-rationally defined, so P also contains the $\mathcal{O}_K$-module $\langle\langle P \rangle\rangle$ generated by P. Such $\mathcal{O}_K$-submodules are classified in [BC, §7.3]. In particular, each is of the form $E[I]$ for an ideal I of $\mathcal{O}_K$ [BC, Thm. 2.6].
Split Case: Suppose that $\ell\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Then (cf. [BC, §7.3]) $\langle\langle P \rangle\rangle = E[\mathfrak{p}_1^i\mathfrak{p}_2^j]$ with $0 \leq i, j \leq a$ and $\max(i, j) = a$. Since for ideals I, J of $\mathcal{O}_K$ we have $E[I] \subset E[J] \iff I \supset J$, we get that $E(F)$ contains either $E[\mathfrak{p}_1^a]$ or $E[\mathfrak{p}_2^a]$; interchanging $\mathfrak{p}_1$ and $\mathfrak{p}_2$ if necessary, we may assume

$$E(F) \supset E[\mathfrak{p}_1^a].$$

Moreover we have an internal $\mathcal{O}_K$-module decomposition

$$E[\ell^a] = E[\mathfrak{p}_1^a] \oplus E[\mathfrak{p}_2^a],$$

whereas as $\mathbb{Z}$-modules we have

$$E[\mathfrak{p}_1^a] \cong_{\mathbb{Z}} E[\mathfrak{p}_2^a] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^a\mathbb{Z}.$$

So for $i = 1, 2$ let P_i be a generator for $E[\mathfrak{p}_i^a]$ (here a $\mathbb{Z}$-module generator is also an $\mathcal{O}_K$-module generator). Then P_1, P_2 is a $\mathbb{Z}/\ell^a\mathbb{Z}$-basis for $E[\ell^a]$, and since $P_1 \in E(F)$ and $\langle P_2 \rangle$ is $\mathfrak{g}_F$-stable, the image of the Galois representation $\rho_{\ell^a} : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/\ell^a\mathbb{Z})$ on E consists of matrices of the form $\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$. But moreover $\det \rho_{\ell^a} = \chi_{\ell^a}$ is the modulo ℓ^a cyclotomic character, which is trivial, since F contains a primitive ℓ^ath root of unity. Thus ρ_{ℓ^a} is trivial, so

$$F \supset K(E[\ell^a]) \supset K(\mathfrak{h}(E[\ell^a])) = K^{(\ell^a)}.$$

Inert Case: Suppose that $\ell\mathcal{O}_K$ is a prime ideal. Then (cf. [BC, §7.3]) $\langle\langle P \rangle\rangle = E[\ell^a]$, so as above we get $F \supset K^{(\ell^a)}$.
Ramified Case: suppose that $\ell\mathcal{O}_K = \mathfrak{p}^2$. Then (cf. [BC, §7.3]) $\langle\langle P \rangle\rangle$ is either $E[\mathfrak{p}^{2a-1}]$ or $E[\mathfrak{p}^{2a}] = E[\ell^a]$. Either way we get

$$F \supset K(E[\mathfrak{p}^{2a-1}]) \supset K(\mathfrak{h}(E[\mathfrak{p}^{2a-1}])) = K^{\mathfrak{p}^{2a-1}}. \qquad \square$$

3.6. **Proof of Theorem 1.3b).** Let F be a number field, and let $E_{F^{\mathrm{cyc}}}$ be an $\mathcal{O}_K$-CM elliptic curve. Let ℓ be a prime number and let $a \in \mathbb{Z}^+$. Suppose that $E(F^{\mathrm{cyc}})$ contains a point of order ℓ^a. Then since $F^{\mathrm{cyc}} \supset \mathbb{Q}^{\mathrm{ab}} \supset K$, the hypotheses of Proposition 3.5 apply.

Step 1: Put $\overline{a} = \begin{cases} a & \left(\frac{\Delta_K}{\ell}\right) \neq 0 \\ a-1 & \left(\frac{\Delta_K}{\ell}\right) = 0 \end{cases}$, and let $\mathcal{O}$ be the imaginary quadratic order of conductor $\ell^{\overline{a}}$. We claim that $F \supset K(\ell^{\overline{a}})$. Indeed, if ℓ does not ramify in K, then using Proposition 3.5 we get

$$F \supset K^{(\ell^a)} \supset K(\ell^a) = K(\ell^{\overline{a}}).$$

If ℓ ramifies in K then using Proposition 3.5 we get

$$F \supset K^{\mathfrak{p}^{2a-1}} \supset K^{\mathfrak{p}^{2a-2}} = K^{(\ell^{a-1})} \supset K(\ell^{a-1}) = K(\ell^{\overline{a}}).$$

Step 2: Applying Lemma 3.2 we get

$$\frac{h(\mathcal{O})}{h_2(\mathcal{O})} = \overline{h}(\mathcal{O}) \leq [F : \mathbb{Q}].$$

By [Cx, Prop. 3.11] we have

$$h_2(\mathcal{O}) \leq 2h_2(\mathcal{O}_K),$$

so

$$h(\mathcal{O}) \leq 2h_2(\mathcal{O}_K)[F : \mathbb{Q}].$$

By (2) we have $h(\mathcal{O}) \geq \frac{\varphi(\ell^{\overline{a}})}{6}$, and thus

$$\varphi(\ell^{\overline{a}}) \leq 12h_2(\mathcal{O}_K)[F : \mathbb{Q}].$$

4. The Case $F = \mathbb{Q}$

4.1. **When $K^{(1)}/\mathbb{Q}$ is abelian.** We now concentrate on the case $F = \mathbb{Q}$, in which we are considering torsion points on CM elliptic curves over $\mathbb{Q}^{\mathrm{ab}}$. Since $\mathbb{Q}^{\mathrm{ab}}$ is Galois over $\mathbb{Q}$, for an imaginary quadratic order $\mathcal{O}$ there is an $\mathcal{O}$-CM elliptic curve defined over $\mathbb{Q}^{\mathrm{ab}}$ iff $j(\mathbb{C}/\mathcal{O}) \in \mathbb{Q}^{\mathrm{ab}}$ iff $\overline{h}(\mathcal{O}) = 1$. By the above reults there are only finitely many such $\mathcal{O}$. Unfortunately Heilbronn's work is fundamentally ineffective. However, in [Vo07], Voight lists 101 imaginary quadratic orders $\mathcal{O}$ with $\overline{h}(\mathcal{O}) = 1$ and shows that this list is complete conditionally on the Generalized Riemann Hypothesis. We list these orders, sorted by imaginary quadratic field K and then by conductor:

$\Delta_K = -3$, $\mathfrak{f} \in \{1, 2, 3, 4, 5, 7, 8\}$
$\Delta_K = -4$, $\mathfrak{f} \in \{1, 2, 3, 4, 5\}$
$\Delta_K = -7$, $\mathfrak{f} \in \{1, 2, 4, 8\}$
$\Delta_K = -8 = -2^3$, $\mathfrak{f} \in \{1, 2, 3, 6\}$
$\Delta_K = -11$, $\mathfrak{f} \in \{1, 3\}$
$\Delta_K = -15 = -3 \cdot 5$, $\mathfrak{f} \in \{1, 2, 4, 8\}$
$\Delta_K = -19$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -20 = -2^2 \cdot 5$, $\mathfrak{f} \in \{1, 3\}$
$\Delta_K = -24 = -2^3 \cdot 3$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -35 = -5 \cdot 7$, $\mathfrak{f} \in \{1, 3\}$
$\Delta_K = -40 = -2^3 \cdot 5$, $\mathfrak{f} \in \{1, 2\}$

$\Delta_K = -43$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -51 = -3 \cdot 17$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -52 = -2^2 \cdot 13$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -67$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -84 = -2^2 \cdot 3 \cdot 7$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -88 = -2^3 \cdot 11$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -91 = -7 \cdot 13$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -115 = -5 \cdot 23$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -120 = -2^3 \cdot 3 \cdot 5$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -123 = -3 \cdot 41$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -132 = -2^2 \cdot 3 \cdot 11$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -148 = -2^2 \cdot 37$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -163$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -168 = -2^3 \cdot 3 \cdot 7$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -187 = -11 \cdot 17$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -195 = -3 \cdot 5 \cdot 13$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -228 = -2^2 \cdot 3 \cdot 19$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -232 = -2^3 \cdot 29$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -235 = -5 \cdot 47$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -267 = -3 \cdot 89$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -280 = -2^3 \cdot 5 \cdot 7$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -312 = -2^3 \cdot 3 \cdot 13$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -340 = -2^2 \cdot 5 \cdot 17$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -372 = -2^2 \cdot 3 \cdot 31$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -403 = -13 \cdot 31$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -408 = -2^3 \cdot 3 \cdot 17$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -420 = -2^3 \cdot 3 \cdot 5 \cdot 7$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -427 = -7 \cdot 61$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -435 = -3 \cdot 5 \cdot 29$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -483 = -3 \cdot 7 \cdot 23$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -520 = -2^3 \cdot 5 \cdot 13$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -532 = -2^2 \cdot 7 \cdot 19$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -555 = -3 \cdot 5 \cdot 37$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -595 = -5 \cdot 7 \cdot 17$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -627 = -3 \cdot 11 \cdot 19$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -660 = -2^2 \cdot 3 \cdot 5 \cdot 11$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -708 = -2^3 \cdot 3 \cdot 59$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -715 = -5 \cdot 11 \cdot 13$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -760 = -2^3 \cdot 5 \cdot 19$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -795 = -3 \cdot 5 \cdot 53$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -840 = -2^3 \cdot 3 \cdot 5 \cdot 7$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -1012 = -2^2 \cdot 11 \cdot 23$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -1092 = -2^2 \cdot 3 \cdot 7 \cdot 13$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -1155 = -3 \cdot 5 \cdot 7 \cdot 11$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -1320 = -2^3 \cdot 3 \cdot 5 \cdot 11$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -1380 = -2^2 \cdot 3 \cdot 5 \cdot 23$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -1428 = -2^2 \cdot 3 \cdot 7 \cdot 17$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -1435 = -5 \cdot 7 \cdot 41$, $\mathfrak{f} \in \{1\}$

$\Delta_K = -1540 = -2^2 \cdot 5 \cdot 7 \cdot 11$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -1848 = 2^3 \cdot 3 \cdot 7 \cdot 11$, $\mathfrak{f} \in \{1, 2\}$
$\Delta_K = -1995 = -3 \cdot 5 \cdot 7 \cdot 19$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -3003 = 3 \cdot 7 \cdot 11 \cdot 13$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -3315 = -3 \cdot 5 \cdot 13 \cdot 17$, $\mathfrak{f} \in \{1\}$
$\Delta_K = -5460 = -2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$, $\mathfrak{f} \in \{1\}$

For the rest of the section, K is an imaginary quadratic field with $\overline{h}(\mathcal{O}_K) = 1$. We also assume GRH, so that K is one of the 65 fields listed above.

4.2. **Split primes.** Let ℓ be a prime that splits in K, and let $a \in \mathbb{Z}^+$. Suppose there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ such that $E(\mathbb{Q}^{\mathrm{ab}})$ contains a point of order ℓ^a. As in the proof of Proposition 3.5, there is some labelling $\mathfrak{p}_1$, $\mathfrak{p}_2$ of the primes of $\mathcal{O}_K$ lying over ℓ such that $\mathbb{Q}^{\mathrm{ab}} \supset K^{\mathfrak{p}_1^a}$. Since $\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ is abelian, every subextension F must be Galois over $\mathbb{Q}$. Complex conjugation carries $K^{\mathfrak{p}_1^a}$ to $K^{\mathfrak{p}_2^a}$, so if $K^{\mathfrak{p}_1^a}$ is Galois over $\mathbb{Q}$ then $K^{\mathfrak{p}_1^a} = K^{\mathfrak{p}_2^a}$ which then forces $K^{\mathfrak{p}_1^a} = K^{(1)} = K^{\mathfrak{p}_2^a}$. Using Lemma 3.4 we see that this occurs precisely in the following cases:
• $\Delta_K < -4$:
(i) $\ell^a = 2, 4$ and $\Delta_K \equiv \pm 1 \pmod 8$, or
(ii) $\ell^a = 3$ and $\Delta_K \equiv 1 \pmod 3$.
• $\Delta_K = -4$, $\ell^a = 5$.
• $\Delta_K = -3$, $\ell^a = 7$.

Proposition 4.1. *Let K be an imaginary quadratic field in which the prime 2 splits, and let $\mathfrak{p}$, $\overline{\mathfrak{p}}$ be the prime ideals lying over 2. Let ζ_4 be a primitive 4th root of unity.*
a) For all $a \in \mathbb{Z}^+$, we have $K^{\mathfrak{p}^a}(\zeta_{2^a}) = K^{(2^a)}$.
b) We have $K^{(4)} = K^{(1)}(\zeta_4)$.

Proof. a) Certainly $K^{\mathfrak{p}^a}(\zeta_{2^a}) \subset K^{(2^a)}$. Moreover, there is an elliptic curve E defined over $F := K^{\mathfrak{p}^a}(\zeta_{2^a})$ such that $E[\mathfrak{p}^a] = E[\mathfrak{p}^a](F)$. If $F = K^{\mathfrak{p}^a}(\zeta_{2^a})$ then by Theorem 3.3 every $\mathcal{O}_K$-CM elliptic curve $E_{/F}$ has $K(\mathbf{h}(E[\mathfrak{p}^a])) \subset F$, and then some twist E^χ has $K(E^\chi[\mathfrak{p}^a]) \subset F$. The proof of Proposition 3.5 then shows that $K(E^\chi[2^a]) \subset F$, and applying Theorem 3.3 again we get $K^{(2^a)} \subset F$.
b) By Lemma 3.4 we have $K^{\mathfrak{p}^2} = K^{(1)}$, so this follows from part a). □

Combining Proposition 4.1 with Theorem 3.3, we find: when $K^{(1)}/\mathbb{Q}$ is abelian and 2 splits in K, there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \hookrightarrow E(\mathbb{Q}^{\mathrm{ab}})$.

4.3. **Inert primes.** Let ℓ be a prime that splits in K, and let $a \in \mathbb{Z}^+$. By Proposition 3.5, if an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ has a $\mathbb{Q}^{\mathrm{ab}}$-rational point of order ℓ^a then the ray class field $K^{(\ell^a)}$ is abelian over $\mathbb{Q}$ and thus so is the ring class field $K(\ell^a)$. This means that ℓ^a appears in the list of conductors in the corresponding entry in Table 1. In all cases we have $\ell^a \leq 8$, so $\ell \in \{2, 3, 5, 7\}$.

It turns out that that for $\Delta < -4$ there is no prime ℓ that is inert in K such that $K(\ell)/\mathbb{Q}$ is abelian. The cases $\Delta_K \in \{-3, -4\}$ are handled by direct computation in §4.4 below.

4.4. **Ramified Primes.**

Proposition 4.2. *Let K be an imaginary quadratic field, let ℓ be a prime that ramifies in K, and let $\mathfrak{p}_\ell$ be the unique prime of $\mathcal{O}_K$ lying over ℓ.*
a) We have

$$K^{\mathfrak{p}_\ell} = K^{(1)}(\zeta_\ell). \tag{3}$$

b) Let $A \in \mathbb{Z}^+$. If the ring class field $K(\ell^A)$ is not *abelian over $\mathbb{Q}$, then for any $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ we have $E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty] \subset E[\mathfrak{p}_\ell^{2A-1}]$.*
c) If $\ell = 2$ then we have

$$K^{\mathfrak{p}_2^3} = K^{(2)} = K(2).$$

Proof. a) If either $\ell = 2$ or $\Delta_K \in \{-3, -4\}$, then we have $K^{\mathfrak{p}_\ell} = K^{(1)} = K(\zeta_\ell)$. So we may assume $\ell > 2$ and $\Delta_K < -4$. Now we have

$$K^{(1)}(\zeta_\ell) \subset K^{(\ell)},$$

and

$$[K^{(\ell)} : K^{\mathfrak{p}_\ell}] = \ell.$$

We CLAIM that $K^{(1)}(\zeta_\ell) \subset K^{\mathfrak{p}_\ell}$. For if not, then we have $K^{(1)}(\zeta_\ell) = K^{(\ell)}$, but

$$[K^{(\ell)} : K^{(1)}] = \frac{\ell^2 - \ell}{2} > \ell - 1 \geq [K^{(1)}(\zeta_\ell) : K^{(1)}],$$

a contradiction. Therefore to show (3) it is enough to show that

$$[K^{(1)}(\zeta_\ell) : K^{(1)}] \geq [K^{\mathfrak{p}_\ell} : K^{(1)}] = \frac{\ell - 1}{2}.$$

Since $K^{(1)} \cap \mathbb{Q}^{\mathrm{ab}}$ is a multi-quadratic field and $\mathbb{Q}(\zeta_p)$ contains a unique quadratic field, we have $[K^{(1)} \cap \mathbb{Q}(\zeta_\ell) : \mathbb{Q}] \leq 2$, and thus $[K^{(1)}(\zeta_\ell) : K^{(1)}] \geq \frac{\ell-1}{2}$.
b) The group $E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty]$ is also finite $\mathcal{O}_K$-submodule of $E(\mathbb{C})$ of ℓ-power order, and all such submodules are of the form $E[\mathfrak{p}_\ell^a]$ for some $a \in \mathbb{Z}^+$, so they are linearly ordered under inclusion. Thus if $E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty]$ is not contained in $E[\mathfrak{p}_\ell^{2A-1}]$ then it contains $E[\mathfrak{p}_\ell^{2A}] = E[\ell^A]$, but then by Theorem 3.3 we have $\mathbb{Q}^{\mathrm{ab}} \supset K^{(\ell^A)} \supset K(\ell^A)$, a contradiction.
c) Since $K^{(1)} \subset K(2) \subset K^{(2)} \subset K^{\mathfrak{p}_2^3}$, it suffices to show that

$$[K(2) : K^{(1)}] = [K^{\mathfrak{p}_2^3} : K^{(1)}].$$

It follows from (1) and Lemma 3.4 that both degrees above are 1 if $\Delta_K = -4$ and both degrees above are 2 if $\Delta_K < -4$. □

For an imaginary quadratic field K such that $K^{(1)}/\mathbb{Q}$ is abelian and a prime ℓ that ramifies in K, Proposition 4.2 has the following consequences:

• Since $K^{\mathfrak{p}_\ell} = K^{(1)}(\zeta_\ell)$ is abelian over $\mathbb{Q}$, by Theorem 3.3 there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with a $\mathbb{Q}^{\mathrm{ab}}$-rational point of order ℓ.
• If $K(2)/\mathbb{Q}$ is not abelian then for any $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ we have $\#E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty] \mid \ell$.
• If $K(2)/\mathbb{Q}$ is abelian, then there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with $E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty] = E[\mathfrak{p}_2^3] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
• If $K(4)/\mathbb{Q}$ is not abelian, then for any $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ we have $\#E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty] \mid \ell^3$.

4.5. **Computing $T(K)$.** We now determine all the possibilities for $E(\mathbb{Q}^{\mathrm{ab}})[\ell^\infty]$ for an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ and a prime number ℓ. It turns out that when $\Delta_K < -4$, from the list of 101 ring class fields that are abelian over $\mathbb{Q}$ and the work of the previous sections, for each K such that $K^{(1)}/\mathbb{Q}$ is abelian, we need no further calculations to determine the complete set of prime power ideals I of $\mathcal{O}_K$ such that $K^I/\mathbb{Q}$ is abelian.

When $\Delta_K = -3$ then 2 is inert in K and $K(8)/\mathbb{Q}$ is abelian, so we compute that $K^{(2)}$ and $K^{(4)}$ are abelian over $\mathbb{Q}$ but $K^{(8)}$ is not.

When $\Delta_K = -4$ then 2 ramifies in K and $K(4)/\mathbb{Q}$ is abelian, so we compute that $K^{(4)}/\mathbb{Q}$ is abelian but $K^{\mathfrak{p}_2^5}/\mathbb{Q}$ is not. Also 3 is inert in K and $K(3)/\mathbb{Q}$ is abelian, so we compute that $K^{(3)}/\mathbb{Q}$ is abelian.

4.6. **What remains to be done.** Above we computed, for each imaginary quadratic field K such that the Hilbert class field $K^{(1)}$ is abelian over $\mathbb{Q}$, the maximal ℓ-primary torsion subgroups of $\mathcal{O}_K$-CM elliptic curves $E_{/\mathbb{Q}^{\mathrm{ab}}}$. To extend these results to give a complete classification, one must address the following issues.

First: when E is $\mathcal{O}_K$-CM, we must investigate the extent to which different ℓ-pimary torsion structures can jointly occur over $\mathbb{Q}^{\mathrm{ab}}$. Let ℓ_1 and ℓ_2 be distinct primes, and for $i = 1, 2$ let I_i be an ℓ_i-primary $\mathcal{O}_K$-ideal. Then by Lemma 3.4, the compositum $K^{I_1}K^{I_2}$ of the ray class fields has index $w_K := \#\mathcal{O}_K^\times \in \{2, 4, 6\}$ in the composite ray class field $K^{I_1 I_2}$. Otherwise put, if $K^{I_1}, K^{I_2} \subset \mathbb{Q}^{\mathrm{ab}}$, then there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ for which $E[I_1] \subset E(\mathbb{Q}^{\mathrm{ab}})$ and $\mathfrak{h}(E[I_2]) \subset \mathbb{Q}^{\mathrm{ab}}$ (here $\mathfrak{h} : E \to E/\operatorname{Aut}(E) \xrightarrow{\sim} \mathbb{P}^1$ is a Weber function; when $\Delta < -4$ we can take $\mathfrak{h}((x, y)) = x$), but in order to rationalize $E[I_2]$ we need to extract a w_Kth root, and this will usually (in some sense!) not give an abelian extension of $\mathbb{Q}$.

In principle this can be resolved by computing all "composite" ray class fields $K^{I_1 I_2}$ (and, if necessary, $K^{I_1 \cdots I_r}$) and checking whether they are abelian over $\mathbb{Q}$. In practice, in many cases the degrees of these ray class fields are too large for MAGMA to compute them and/or to check whether they are abelian over $\mathbb{Q}$. It would be preferable to have a more conceptual understanding of abelianness over $\mathbb{Q}$ of ray class fields of imaginary quadratic fields.

Second: we must deal with the cases in which for some $\mathfrak{f} > 1$ the ring class field $K(\mathfrak{f})$ is abelian over $\mathbb{Q}$ and thus we have elliptic curves $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with CM by the non-maximal order $\mathcal{O}$ in K of conductor $\mathfrak{f}$. In this case the finite $\mathcal{O}$-submodules M of $E(\mathbb{C})$ have a more complicated structure: cf. [BC, Remark 2.7]. In particular, in some cases we do not know as explicit a description of the abelian extension $K(\mathfrak{h}(M))/K$ as in the $\mathcal{O}_K$-CM case. As mentioned above, there is a canonical $\mathbb{Q}(\mathfrak{f})$-rational isogeny $\iota : E \to E'$ with $\operatorname{End} E' \cong \mathcal{O}_K$, and the induced maps

$$\iota : E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}] \to E'(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}],$$

$$\iota^\vee : E'(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}] \to E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}]$$

have kernel cyclic of order dividing $\mathfrak{f}$. Thus there is a tightly bounded discrepancy between the two torsion subgroups, so in theory a brute force computation would suffice, but in practice we are looking for a more principled approach.

Let us consider the following case: $8 \mid \Delta_K$ and $\mathfrak{f} = 2$. Let $\mathcal{O}$ be the order in K with conductor 2. Thus $K(2)$ is abelian over $\mathbb{Q}$ but $K(4)$ is not, so by [BC, Thm.

1.1] there is no $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ with $E[2] \subset \mathbb{Q}^{\mathrm{ab}}$. So for all $\ell > 2$, the maximal ℓ-primary torsion on an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$ is the same as for an $\mathcal{O}_K$-CM elliptic curve, while for $\ell = 2$ the maximal such 2-primary torsion is either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/8\mathbb{Z}$. By [Kw99, Cor. 4.2] some (equivalently, since $\Delta_K < -4$, every) $\mathcal{O}$-CM elliptic curve has a $\mathbb{Q}(\mathfrak{f})$-rational cyclic 8-isogeny. The isogeny character

$$\chi_8 : \mathfrak{g}_{\mathbb{Q}(\mathfrak{f})} \to (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

is well-defined up to a quadratic twist, so the *reduced* isogeny characer

$$\overline{\chi_8} : \mathfrak{g}_{\mathbb{Q}(\mathfrak{f})} \to (\mathbb{Z}/8\mathbb{Z})^\times/\{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$

is canonical; it cuts out a quadratic extension $\mathbb{Q}(\mathfrak{f})(\sqrt{d})/\mathbb{Q}(\mathfrak{f})$ over which some quadratic twist has a rational point of order 8. Therefore if the extension $\mathbb{Q}(\mathfrak{f})(\sqrt{d})/\mathbb{Q}$ is abelian, then we get a point of order 8 on an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}^{\mathrm{ab}}}$. It seems likely that the converse is also true. In general, explicitly computing reduced isogeny characters of CM elliptic curves is an interesting problem; notice that Proposition 4.2a) can be viewed as a result of this type.

Remark 4.3. *Let $N \geq 3$. For any number field F, let $E_{/F}$ be an elliptic curve admitting an F-rational cyclic N-isogeny. Let $\chi_N : \mathfrak{g}_F \to (\mathbb{Z}/N\mathbb{Z})^\times$ be the associated isogeny character. As above, composing with the quotient map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$ gives a reduced isogeny character*

$$\overline{\chi_N} : \mathfrak{g}_F \to (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}.$$

The spliting field of $\overline{\chi_N}$ is an abelian extension L/F of degree dividing $\frac{\varphi(N)}{2}$, and there is a quadratic twist E^D of $E_{/M}$ that admits an M-rational point of order M.

Najman's non-CM sporadic points on $X_1(27)$ and $X_1(37)$ with abelian field of moduli arise in this way starting from elliptic curves $E_{/\mathbb{Q}}$ with rational 21 and 37-isogenies. In these cases the reduced isogeny character is not surjective, and thus the points on $X_1(N)$ have degree properly dividing $\frac{\varphi(N)}{2}$.

5. Proof of Theorem 1.4

5.1. **Condition (B1).** Suppose j is a nonsingular modulus. Let F be a number field containing j, and let $E_{/F}$ be an elliptic curve with $j(E) = j$. By Serre's Open Image Theorem [S72, Thm. 3], there is $L = L(E, F)$ such that for all primes $\ell \geq \max(L, 5)$, the mod ℓ Galois representation

$$\rho_\ell : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

is surjective. We will show that for all such ℓ, for any elliptic curve $E'_{/F^{\mathrm{ab}}}$ with $j(E') = j$, we have $E'(F^{\mathrm{ab}})[\ell] = 0$. Indeed, suppose not: then E' is a quadratic twist of E by some $t \in (F^{\mathrm{ab}})^\times$, so E has a point of order ℓ rational over $F^{\mathrm{ab}}(\sqrt{t})$. Consider the following tower of fields:

$$F \subset F^{\mathrm{ab}} \subset F^{\mathrm{ab}}(\sqrt{t}) \subset F^{\mathrm{ab}}(\sqrt{t}, E[\ell]).$$

At each step in the tower we have a solvable extension; this is immediate for all steps except the last. For that: since we have a point of order ℓ defined over $F^{\mathrm{ab}}(\sqrt{t})$, the image of the mod ℓ Galois representation on E when restricted to this field lies in $\{\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \mid b \in \mathbb{Z}/\ell\mathbb{Z}, d \in (\mathbb{Z}/\ell\mathbb{Z})^\times\}$, which is a solvable group. Thus $F^{\mathrm{ab}}(\sqrt{t}, E[\ell])/F$ is solvable, hence its subextension $F(E[\ell])/F$ is solvable.

But the latter extension is Galois with group $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $\ell \geq 5$, which has the nonabelian simple group $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as a Jordan-Hölder factor: contradiction.

5.2. **Condition (B2).**

Lemma 5.1. *Let F be a field. Let $N > 2$ be indivisible by the characteristic of F.*
a) Let $E_{/F}$ be an elliptic curve and suppose that $E(F)$ has a point of order N. Then at most one nontrivial quadratic twist $E^t_{/F}$ of E has a point of order N.
b) Let $A_{/F}$ be an abelian variety, and suppose that $E(F)$ has a point of order N. Then at most finitely many quadratic twists $A^t_{/F}$ have points of order N.

Proof. a) Without loss of generality we may assume that either N is an odd prime or $N = 4$. Either way, let P_1 be a point of order N in $E(F)$. Let $t \in F^\times \setminus F^{\times 2}$ be such that there is $P_2 \in E^t(F)$ of order N. Let $\epsilon_t : \mathfrak{g}_F \to \{\pm 1\}$ be the character on the corresponding to the quadratic extension $F(\sqrt{t})/F$. The mod N Galois representations on E and E^t are related as follows:

$$\rho_{N,E} = \rho_{N,E^t} \otimes \epsilon_t.$$

Since P_2 is fixed under the action of ρ_{N,E^t}, ρ_N stabilizes the subgroup $\langle P_2 \rangle$ and acts on it via the isogeny character ϵ_t, which is nontrivial since $N > 2$.

• Suppose $N = \ell$ is an odd prime. Then $\langle P_1, P_2 \rangle = E[\ell](\overline{F})$ and it follows that upon restriction to $F(\sqrt{t})$ the mod N Galois representation is trivial. This rules out a second quadratic twist t' – i.e., such that $t', \frac{t'}{t} \notin F^{\times 2}$ – such that $E^{t'}(F)$ has a point of order N, because that would lead to a nontrivial quadratic isogeny character $\epsilon_{t'} \neq \epsilon_t$, which then cannot trivialize upon restriction to $F(\sqrt{t})$.

• Suppose $N = 4$. Let $T = E[4](\overline{F})$ and by choosing a basis P_1, Q, identify T with $(\mathbb{Z}/4\mathbb{Z})^2$. If $\langle P_1, P_2 \rangle = T$, we argue as above. However, it may be that $\langle P_1, P_2 \rangle \subsetneq T$: this happens when $\langle P_1 \rangle$ and $\langle P_2 \rangle$ lie in the same fiber of the map $\mathbb{P}^1(\mathbb{Z}/4\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/2\mathbb{Z})$. But all fibers of this map have 2 elements, so if there is t' such that $t', \frac{t'}{t} \notin F^{\times 2}$ such that $A^{t'}$ has an F-rational point P_3 of order 4, then either $\langle P_1, P_2 \rangle = T$ or $\langle P_1, P_3 \rangle = T$. Thus, by taking P_3 in place of P_2 if necessary, we may argue as above.
b) Replacing "one nontrivial twist" with "finitely many twists," the above argument easily adapts to the case of abelian varieties. □

We immediately deduce the following result.

Proposition 5.2. *Let F be a field, and let $A_{/F}$ be an abelian variety. Let ℓ be a prime number which is indivisible by the characteristic of F. Suppose $A^t(F)[\ell^\infty]$ is finite for all quadratic twists $A^t_{/F}$ of A, including the "trivial twist" $A^t = A$. Then*

$$\sup_{t \in F^\times/F^{\times 2}} \#A^t(F)[\ell^\infty] < \infty.$$

Let $E_{/F}$ be an elliptic curve over a number field. Suppose $j(E) \neq 0, 1728$, so that every twist of E is a quadratic twist. Then combining Proposition 5.2 with Theorem 2.2a) we get that for each prime ℓ, there is $a \in \mathbb{Z}^+$ such that for any elliptic curve $E'_{/F^{\mathrm{cyc}}}$ with $j(E') = j(E)$, we have $E'(F^{\mathrm{cyc}})[\ell^\infty] = E'(F^{\mathrm{cyc}})[\ell^a]$ is a finite group. Similarly, if $j(E)$ is a nonsingular modulus then using Theorem 2.2b) instead we get that for each prime ℓ, there is $a \in \mathbb{Z}^+$ such that for any elliptic curve $E'_{/F^{\mathrm{ab}}}$ with $j(E') = j(E)$, we have $E'(F^{\mathrm{ab}})[\ell^\infty] = E'(F^{\mathrm{ab}})[\ell^a]$ is a finite group. The same holds when $j(E)$ is a singular modulus and F does not contain the CM field.

5.3. **A variant.** The following is a variant of Lemma 5.1 that can also be used to deduce Condition (B2). It is stronger in that it applies to all twists (so can be applied when $j \in \{0, 1728\}$, though these cases are already covered by the results of the previous section) but weaker in that the bound obtained on the number of twists that can have a point of order N depends on N.

Proposition 5.3. *Let F be a field of characteristic 0, and let $N \geq 4$. For any $j \in F$, there are only finitely many F-isomorphism classes of elliptic curves $E_{/F}$ with $j(E) = j$ such that $E(F)$ has a point of order N.*

Proof. This follows from the fact that $Y_1(N)_{/F}$ is a fine moduli scheme for $N \geq 4$. Namely, j induces a closed point on $Y(1)$. The fiber of $Y_1(N) \to Y(1)$ over j contains only finitely many points, which correspond to all F-rational isomorphism classes of pairs (E_i, P_i). with $P_i \in E_i(F)$ of order N. Any elliptic curve over F with $j(E) = j$ and an F-point of order N must be one of these finitely many E_i's. □

6. Open Questions

We begin by asking for an abelian variety version of Theorem 1.4.

Question 6.1. *Let F be a number field, and let $A_{/F}$ be an abelian variety. Let $\mathcal{T}(A)$ be the class of all abelian varieties $A'_{/F}$ such that $A'_{/\overline{F}} \cong A_{/\overline{F}}$.*
a) Do we have $\sup_{A' \in \mathcal{T}(A)} \#A'(F^{\mathrm{cyc}})[\mathrm{tors}] < \infty$?
b) Suppose A has no F-simple isogeny factor B of F-rational CM type, i.e., such that $\mathrm{End}_F(B)$ is an order in a number field of degree $2 \dim B$. Do we then have $\sup_{A' \in \mathcal{T}(A)} \#A'(F^{\mathrm{ab}})[\mathrm{tors}] < \infty$?

The proof given for the one-dimensional case does not adapt immediately since when $\dim A = g \geq 2$ it is no longer true that a rational point of order ℓ forces the modulo ℓ Galois representation $\rho_\ell : \mathfrak{g}_F \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ to have solvable image. However, we believe a less crude group-theoretic analysis would carry over the argument under the assumption that for all sufficiently large primes ℓ, the image of ρ_ℓ is isomorphic to $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$. This is the most stringent reasonable interpretation of "no complex multiplication" whereas the hypothesis in Zarhin's theorem is the most lax. There are intermediate cases, even when $g = 1$.

Indeed: in the setting of Theorem 1.4, suppose instead that $j \in \overline{\mathbb{Q}}$ is a singular modulus, with corresponding CM field K. Then the conclusion of Theorem 1.4 is false if F is a number field containing an imaginary quadratic field K: for every imaginary quadratic order $\mathcal{O}$ we have $K(\mathfrak{f}) \subset K^{\mathrm{ab}}$ so there is an $\mathcal{O}$-CM elliptic curve $E_{/K^{\mathrm{ab}}}$. Moereover for any $\mathcal{O}$-CM elliptic curve we have $K^{(1)}(\mathfrak{h}(E[\mathrm{tors}]) = K^{\mathrm{ab}}$, and via an easy twisting argument it follows that for all $N \in \mathbb{Z}^+$ there is an $\mathcal{O}$-CM elliptic curve $E_{/K^{\mathrm{ab}}}$ with $E[N] \subset E(K^{\mathrm{ab}})$.[2] This motivates:

Question 6.2. *Let F be a number field that does not contain any imaginary quadratic field. Is there a positive integer $B = B(F)$ such that: for all elliptic curves $E_{/F^{\mathrm{ab}}}$ with complex multiplication, we have*

$$\#E(F^{\mathrm{ab}})[\mathrm{tors}] \leq B?$$

[2]In this case Theorem 2.3 implies (only) that $E(K(\mathfrak{f})^{\mathrm{ab}})[\mathrm{tors}]$ is infinite. A more careful analysis of twists shows that there is an $\mathcal{O}$-CM elliptic curve $E_{/K^{\mathrm{ab}}}$ with $E(K^{\mathrm{ab}})[\mathrm{tors}]$ infinite.

Consider the following condition on a number field F:

(F) The field F^{ab} contains only finitely many singular moduli.

Theorem 6.3. a) *Let $n \geq 4$, and let F be an S_n-number field – i.e., $[F : \mathbb{Q}] = n$, and if M is the Galois closure of $F/\mathbb{Q}$ then $\mathrm{Aut}(M/\mathbb{Q}) \cong S_n$. Then F satisfies Condition (F).*

b) *If F satisfies Condition (F), then Question 6.2 has an affirmative answer.*

Proof. a) It will suffice to show that for every ring class field $K(\mathfrak{f})$, the fields $K(\mathfrak{f})$ and F are linearly disjoint over $\mathbb{Q}$: for if so, $\mathrm{Aut}(FK(\mathfrak{f})/F) = \mathrm{Aut}(K(\mathfrak{f})/\mathbb{Q})$, so by §3.2 there are only finitely many orders $\mathcal{O}$ such that $\mathrm{Aut}(FK(\mathfrak{f})/F)$ is abelian, and Condition (F) follows. Since $K(\mathfrak{f})/\mathbb{Q}$ is Galois, failure of linear disjointness means that $F \cap K(\mathfrak{f}) \supsetneq \mathbb{Q}$, and since an S_n-number field has no nontrivial proper subfields, this gives $F \subset K(\mathfrak{f})$. Since again $K(\mathfrak{f})/\mathbb{Q}$ is Galois, if M is the Galois closure of $F/\mathbb{Q}$, we have $M \subset K(\mathfrak{f})$ and thus that S_n is a quotient of $\mathrm{Aut}(K(\mathfrak{f})/\mathbb{Q})$. So S_n has a commutative subgroup of index at most 2, which holds iff $n \leq 3$.
b) If F satisfies Condition (F), only finitely many singular moduli lie in F^{ab}, so it suffices to work with a fixed imaginary quadratic order. By §3.4 we are reduced to the maximal order $\mathcal{O}_K$. Proposition 3.5 and the containments $K^{(\ell^a)} \supset K(\ell^a)$ and – when $\ell\mathcal{O}_K = \mathfrak{p}^2$ – $K^{\mathfrak{p}^{2a-1}} \supset K$ then give the boundedness of torsion over F^{ab}. □

Proposition 6.3a) shows that Condition (F) holds for "most" number fields. Clearly it does not hold when F contains an imaginary quadratic field! The proof of Theorem 6.3a) shows that being linearly disjoint over $\mathbb{Q}$ from all ring class fields of imaginary quadratic fields is sufficient for Condition (F). Real quadratic fields do not satisfy this sufficient condition but may yet satisfy Condition (F). It seems conceivable that a number field satisfies Condition (F) iff it does not contain an imaginary quadratic field; if true, this would give a complete answer to Question 6.2.

Finally we ask for a common generalization of Theorem 1.1 and the work of [Ch17].

Question 6.4. *As $E_{/\mathbb{Q}^{\mathrm{ab}}}$ ranges over all elliptic curves, is $\sup \#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}] < \infty$?*

For a fixed number F, if one assumes that there is $L = L(F) \in \mathbb{Z}^+$ such that for all primes $\ell > L$ and all non-CM elliptic curves $E_{/F}$, the modulo ℓ Galois representation $\rho_\ell : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is surjective ("Serre's uniformity over F") one can show that there is a uniform bound on $\#E(\mathbb{Q}^{\mathrm{ab}})[\mathrm{tors}]$ as $E_{/\mathbb{Q}^{\mathrm{ab}}}$ ranges over all ellptic curves with j-invariant in F. Notice though that when $F = \mathbb{Q}$, the work [Ch17] establishes this unconditionally. The argument makes use of the classification of $\mathbb{Q}$-points on the modular curves $X_0(N)$ and also on work of González-Jiménez and Lozano-Robledo on abelian division fields of elliptic curves over $\mathbb{Q}$ [GJLR16]. If the latter work could be generalized – in the form of a finiteness result rather than a complete classification – then it should be possible to prove the above uniform bound assuming only that there is $L = L(F) \in \mathbb{Z}^+$ such that for all primes $\ell > L$ no non-CM elliptic curve $E_{/F}$ has an F-rational cyclic ℓ-isogeny.

References

[BC] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves*. http://alpha.math.uga.edu/~pete/Bourdon_Clark_arxiv_v5.pdf

[BC2] A. Bourdon and P.L. Clark, *Torsion points and isogenies on CM elliptic curves*. `http://alpha.math.uga.edu/~pete/BCII.pdf`

[BCS14] A. Bourdon, P.L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*. Trans. Amer. Math. Soc. 369 (2017), 8457–8496.

[BP17] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*. Int. Math. Res. Not. IMRN 2017, 4923–4961.

[Ch] H. Cohen, *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics 193, Springer-Verlag, 2000.

[Ch17] M. Chou, *Torsion of rational elliptic curves over the maximal abelian extension of* $\mathbb{Q}$. `https://arxiv.org/abs/1711.00412`

[CCRS13] P.L. Clark, B. Cook and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*. International Journal of Number Theory 9 (2013), 447–479.

[CP15] P.L. Clark and P. Pollack, *The truth about torsion in the CM case*. C. R. Math. Acad. Sci. Paris 353 (2015), 683–688.

[Cx] D. Cox, *Primes of the form* $x^2 + ny^2$*. Fermat, class field theory and complex multiplication.* John Wiley & Sons, New York, 1989.

[GJLR16] E. González-Jiménez and Á. Lozano-Robledo, *Elliptic curves with abelian division fields*. Math. Z. 283 (2016), 835–859.

[He34] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields*. Quart. J. Math. Oxford Ser. 25 (1934), 150–160.

[HW] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*. Sixth edition. Oxford University Press, Oxford, 2008.

[KL81] N.M. Katz and S. Lang, *Finiteness theorems in geometric classfield theory*. With an appendix by Kenneth A. Ribet. Enseign. Math. (2) 27 (1981), no. 3–4, 285–319 (1982).

[Kw99] S. Kwon, *Degree of isogenies of elliptic curves with complex multiplication*. J. Korean Math. Soc. 36 (1999), 945–958.

[Na16] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$. Math. Res. Lett. 23 (2016), 245–272.

[S72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), no. 4, 259–331.

[Si94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, 1994.

[Vo07] J. Voight, *Quadratic forms that represent almost the same primes*. Math. Comp. 76 (2007), 1589–1617.

[Za87] Yu. G. Zarhin, *Endomorphisms and torsion of abelian varieties*. Duke Math. J. 54 (1987), 131–145.

K	Primary $I \trianglelefteq \mathcal{O}_K$ such that $K^I/\mathbb{Q}$ is abelian	$T(K)$
$\mathbb{Q}(\sqrt{-3})$	(2), (4), $\mathfrak{p}_3$, $\mathfrak{p}_3^2 = (3)$, (5), $\mathfrak{p}_7$, $\overline{\mathfrak{p}_7}$, (7)	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7^2 = 529200$
$\mathbb{Q}(\sqrt{-4})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_2^4 = (4)$, (3), $\mathfrak{p}_5$, $\overline{\mathfrak{p}_5}$, (5)	$2^4 \cdot 3^2 \cdot 5^2 = 3600$
$\mathbb{Q}(\sqrt{-7})$	$\mathfrak{p}_2$, $\overline{\mathfrak{p}_2}$, $\mathfrak{p}_2^2$, $\overline{\mathfrak{p}_2^2}$, (2), (4), $\mathfrak{p}_7$	$2^4 \cdot 7 = 112$
$\mathbb{Q}(\sqrt{-8})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$, $\overline{\mathfrak{p}_3}$, (3)	$2^3 \cdot 3^2 = 72$
$\mathbb{Q}(\sqrt{-11})$	$\mathfrak{p}_3$, $\overline{\mathfrak{p}_3}$, (3), $\mathfrak{p}_{11}$	$3^2 \cdot 11 = 99$
$\mathbb{Q}(\sqrt{-15})$	$\mathfrak{p}_2$, $\overline{\mathfrak{p}_2}$, $\mathfrak{p}_2^2$, $\overline{\mathfrak{p}_2^2}$, (2), (4), $\mathfrak{p}_3$, $\mathfrak{p}_5$	$2^4 \cdot 3 \cdot 5 = 240$
$\mathbb{Q}(\sqrt{-19})$	$\mathfrak{p}_{19}$	19
$\mathbb{Q}(\sqrt{-20})$	$\mathfrak{p}_3$, $\overline{\mathfrak{p}_3}$, (3), $\mathfrak{p}_2$	$2 \cdot 3^2 = 18$
$\mathbb{Q}(\sqrt{-24})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$	$2^3 \cdot 3 = 24$
$\mathbb{Q}(\sqrt{-35})$	$\mathfrak{p}_3$, $\overline{\mathfrak{p}_3}$, (3), $\mathfrak{p}_5$, $\mathfrak{p}_7$	$3^2 \cdot 5 \cdot 7 = 315$
$\mathbb{Q}(\sqrt{-40})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_5$	$2^3 \cdot 5 = 40$
$\mathbb{Q}(\sqrt{-43})$	$\mathfrak{p}_{43}$	43
$\mathbb{Q}(\sqrt{-51})$	$\mathfrak{p}_3$, $\mathfrak{p}_{17}$	$3 \cdot 17 = 51$
$\mathbb{Q}(\sqrt{-52})$	$\mathfrak{p}_2$, $\mathfrak{p}_{13}$	$2 \cdot 13 = 26$
$\mathbb{Q}(\sqrt{-67})$	$\mathfrak{p}_{67}$	67
$\mathbb{Q}(\sqrt{-84})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_7$	$2 \cdot 3 \cdot 7 = 42$
$\mathbb{Q}(\sqrt{-88})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_{11}$	$2^3 \cdot 11 = 88$
$\mathbb{Q}(\sqrt{-91})$	$\mathfrak{p}_7$, $\mathfrak{p}_{13}$	$7 \cdot 13 = 91$
$\mathbb{Q}(\sqrt{-115})$	$\mathfrak{p}_5$, $\mathfrak{p}_{23}$	$5 \cdot 23 = 115$
$\mathbb{Q}(\sqrt{-120})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$, $\mathfrak{p}_5$	$2^3 \cdot 3 \cdot 5 = 120$
$\mathbb{Q}(\sqrt{-123})$	$\mathfrak{p}_3$, $\mathfrak{p}_{41}$	$3 \cdot 41 = 123$
$\mathbb{Q}(\sqrt{-132})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_{11}$	$2 \cdot 3 \cdot 11 = 66$
$\mathbb{Q}(\sqrt{-148})$	$\mathfrak{p}_2$, $\mathfrak{p}_{37}$	$2 \cdot 37 = 74$
$\mathbb{Q}(\sqrt{-163})$	$\mathfrak{p}_{163}$	163
$\mathbb{Q}(\sqrt{-168})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$, $\mathfrak{p}_7$	$2^3 \cdot 3 \cdot 7 = 168$
$\mathbb{Q}(\sqrt{-187})$	$\mathfrak{p}_{11}$, $\mathfrak{p}_{17}$	$11 \cdot 17 = 187$
$\mathbb{Q}(\sqrt{-195})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{13}$	$3 \cdot 5 \cdot 13 = 195$
$\mathbb{Q}(\sqrt{-228})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_{19}$	$2 \cdot 3 \cdot 19 = 114$
$\mathbb{Q}(\sqrt{-232})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_{29}$	$2^3 \cdot 29 = 232$
$\mathbb{Q}(\sqrt{-235})$	$\mathfrak{p}_5$, $\mathfrak{p}_{47}$	$5 \cdot 47 = 235$
$\mathbb{Q}(\sqrt{-267})$	$\mathfrak{p}_3$, $\mathfrak{p}_{89}$	$3 \cdot 89 = 267$
$\mathbb{Q}(\sqrt{-280})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$	$2^3 \cdot 5 \cdot 7 = 280$
$\mathbb{Q}(\sqrt{-312})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$, $\mathfrak{p}_{13}$	$2^3 \cdot 3 \cdot 13 = 312$
$\mathbb{Q}(\sqrt{-340})$	$\mathfrak{p}_2$, $\mathfrak{p}_5$, $\mathfrak{p}_{17}$	$2 \cdot 5 \cdot 17 = 170$
$\mathbb{Q}(\sqrt{-372})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_{31}$	$2 \cdot 3 \cdot 31 = 186$
$\mathbb{Q}(\sqrt{-403})$	$\mathfrak{p}_{13}$, $\mathfrak{p}_{31}$	$13 \cdot 31 = 403$
$\mathbb{Q}(\sqrt{-408})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$, $\mathfrak{p}_{17}$	$2^3 \cdot 3 \cdot 17 = 408$
$\mathbb{Q}(\sqrt{-420})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$	$2 \cdot 3 \cdot 5 \cdot 7 = 210$
$\mathbb{Q}(\sqrt{-427})$	$\mathfrak{p}_7$, $\mathfrak{p}_{61}$	$7 \cdot 61 = 427$
$\mathbb{Q}(\sqrt{-435})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{29}$	$3 \cdot 5 \cdot 29 = 435$
$\mathbb{Q}(\sqrt{-483})$	$\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p} - 23$	$3 \cdot 7 \cdot 23 = 483$
$\mathbb{Q}(\sqrt{-520})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_5$, $\mathfrak{p}_{13}$	$2^3 \cdot 5 \cdot 13 = 520$
$\mathbb{Q}(\sqrt{-532})$	$\mathfrak{p}_2$, $\mathfrak{p}_7$, $\mathfrak{p}_{19}$	$2 \cdot 7 \cdot 19 = 266$
$\mathbb{Q}(\sqrt{-555})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{37}$	$3 \cdot 5 \cdot 37 = 555$
$\mathbb{Q}(\sqrt{-595})$	$\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_{17}$	$5 \cdot 7 \cdot 17 = 595$
$\mathbb{Q}(\sqrt{-627})$	$\mathfrak{p}_3$, $\mathfrak{p}_{11}$, $\mathfrak{p}_{19}$	$3 \cdot 11 \cdot 19 = 627$
$\mathbb{Q}(\sqrt{-660})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{11}$	$2 \cdot 3 \cdot 5 \cdot 11 = 330$
$\mathbb{Q}(\sqrt{-708})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_{59}$	$2 \cdot 3 \cdot 59 = 354$
$\mathbb{Q}(\sqrt{-715})$	$\mathfrak{p}_5$, $\mathfrak{p}_{11}$, $\mathfrak{p}_{13}$	$5 \cdot 11 \cdot 13 = 715$
$\mathbb{Q}(\sqrt{-760})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_5$, $\mathfrak{p}_{19}$	$2^3 \cdot 5 \cdot 19 = 760$
$\mathbb{Q}(\sqrt{-795})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{53}$	$3 \cdot 5 \cdot 53 = 795$
$\mathbb{Q}(\sqrt{-840})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2$, $\mathfrak{p}_5$, $\mathfrak{p}_7$	$2^3 \cdot 3 \cdot 5 \cdot 7 = 840$
$\mathbb{Q}(\sqrt{-1012})$	$\mathfrak{p}_2$, $\mathfrak{p}_{11}$, $\mathfrak{p}_{23}$	$2 \cdot 11 \cdot 23 = 506$
$\mathbb{Q}(\sqrt{-1092})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_{13}$	$2 * 3 * 7 * 13 = 546$
$\mathbb{Q}(\sqrt{-1155})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_{11}$	$3 \cdot 5 \cdot 7 \cdot 11 = 1155$
$\mathbb{Q}(\sqrt{-1320})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_2^3$, $\mathfrak{p}_5$, $\mathfrak{p}_{11}$	$2^3 \cdot 3 \cdot 11 = 1320$
$\mathbb{Q}(\sqrt{-1380})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{23}$	$2 \cdot 3 \cdot 5 \cdot 23 = 690$
$\mathbb{Q}(\sqrt{-1428})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_{17}$	$2 \cdot 3 \cdot 7 \cdot 17 = 714$
$\mathbb{Q}(\sqrt{-1435})$	$\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_{41}$	$5 \cdot 7 \cdot 41 = 1435$
$\mathbb{Q}(\sqrt{-1540})$	$\mathfrak{p}_2$, $\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_1$	$2 \cdot 5 \cdot 7 \cdot 11 = 770$
$\mathbb{Q}(\sqrt{-1848})$	$\mathfrak{p}_2$, $\mathfrak{p}_2^2$, $\mathfrak{p}_2^3$, $\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_{11}$	$2^3 \cdot 3 \cdot 7 \cdot 11 = 1848$
$\mathbb{Q}(\sqrt{-1995})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_{19}$	$3 \cdot 5 \cdot 7 \cdot 19 = 1995$
$\mathbb{Q}(\sqrt{-3003})$	$\mathfrak{p}_3$, $\mathfrak{p}_7$, $\mathfrak{p}_{11}$, $\mathfrak{p}_{13}$	$3 \cdot 7 \cdot 11 \cdot 13 = 3003$
$\mathbb{Q}(\sqrt{-3315})$	$\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_{13}$, $\mathfrak{p}_{17}$	$3 \cdot 5 \cdot 13 \cdot 17 = 3315$
$\mathbb{Q}(\sqrt{-5460})$	$\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_5$, $\mathfrak{p}_7$, $\mathfrak{p}_{13}$	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$