TORSION POINTS AND ISOGENIES ON CM ELLIPTIC CURVES

ABBEY BOURDON AND PETE L. CLARK

Abstract. Let $\mathcal{O}$ be an order in the imaginary quadratic field K. For positive integers $M \mid N$, we determine the least degree of an $\mathcal{O}$-CM point on the modular curve $X(M,N)_{/K(\zeta_M)}$, and for a prime power ℓ^a, we determine the least degree of an $\mathcal{O}$-CM point on the modular curve $X_1(\ell^a)_{/\mathbb{Q}}$. To prove these results we establish several new theorems on rational cyclic isogenies of CM elliptic curves. In particular, we extend a result of Kwon [Kw99] that determines the set of positive integers N for which there is an $\mathcal{O}$-CM elliptic curve E admitting a cyclic, $\mathbb{Q}(j(E))$-rational N-isogeny.

Contents

1. Introduction 2
2. Background 3
2.1. The morphism $X_1(N) \to X_1(M)$ 3
2.2. Orders in imaginary quadratic fields and complex multiplication. 5
2.3. Galois representations of elliptic curves. 6
2.4. Weber functions and fields of moduli. 6
2.5. Isogenies of CM elliptic curves. 6
2.6. Classification of $K(\mathfrak{f})$-rational cyclic isogenies 7
3. The dual isogeny 7
3.1. Inert case 8
3.2. Split case 8
3.3. Ramified case 8
4. Degrees of CM points on $X(M,N)_{/K(\zeta_M)}$ 9
4.1. Statement of the theorem 9
4.2. Prime power case 10
4.3. Compiling across prime powers 14
5. A generalization of Kwon's theorem 15
5.1. Kwon's theorem 15
5.2. Statement of the generalization of Kwon's theorem 16
5.3. A preliminary lemma 16
5.4. Classification of primitive, proper real ideals 17
5.5. Proof of Theorem 5.3 17
5.6. Supplements to Kwon's theorem 18
6. Least degrees of CM points on $X_1(\ell^a)_{/\mathbb{Q}}$ 20
6.1. Inert case 20
6.2. Split case 20
6.3. Ramified case 21
6.4. An example 24
References 25

1. Introduction

We study torsion subgroups of elliptic curves defined over number fields with complex multiplication (CM), a field pionereed by A. Silverberg [Si88], [Si92]. This paper is a sequel to [BC], by the same authors. In that prior work we studied the mod N Galois representations attached to a CM elliptic curve defined over a number field containing the CM field K, with applications to the structure of torsion subgroups over such fields. Crucially, we considered elliptic curves with CM by any imaginary quadratic order $\mathcal{O}$.

We also called for work on the following general problem: given a modular curve $X = X(\Gamma)$ attached to a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$[1], for each imaginary quadratic order $\mathcal{O}$, determine the degrees of $\mathcal{O}$-CM points on X. The case $X = X(N)_{/\mathbb{Q}(\zeta_N)} = X(\Gamma(N))$, was treated in [St01] and [BC, Thm. 1.1], yielding a generalization of the first main theorem of CM to arbitrary quadratic orders. We also treated the case $X = X_1(N)_{/\mathbb{Q}} = X(\Gamma_1(N))$ under the hypothesis that the ground field contains the CM field K.[2]

The first main result of the present paper, Theorem 4.1, is a simultaneous generalization of the previous results to $X = X(M,N)_{/\mathbb{Q}(\zeta_M)} = X(\Gamma(M) \cap \Gamma_1(N))$: namely, for an imaginary quadratic order $\mathcal{O} \subset K$ of conductor $\mathfrak{f}$ and positive integers $M \mid N$, let $K(\mathfrak{f})$ be the ring class field of conductor $\mathfrak{f}$, and let $T(\mathcal{O}, M, N)$ be the least degree of a field extension $F/K(\mathfrak{f})$ such that there is an $\mathcal{O}$-CM elliptic curve $E_{/F}$ and an injection $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)[\mathrm{tors}]$. We explicitly compute $T(\mathcal{O}, M, N)$ in all cases and moreover show that if $F \supset K$ is any number field over which there is an $\mathcal{O}$-CM elliptic curve $E_{/F}$ and an injection $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$, then $T(\mathcal{O}, M, N) \mid [F : K(\mathfrak{f})]$: i.e., all such degrees are multiples of the minimal degree.

Next we return to the case of $X = X_1(N)$ but without the assumption that the ground field contains the CM field K. Write $\mathbb{Q}(\mathfrak{f})$ for $\mathbb{Q}(j(E))$ for E an elliptic curve with CM by the order of conductor $\mathfrak{f}$ in the imaginary quadratic field K. Then, for every prime power ℓ^a we compute the least degree over $\mathbb{Q}(\mathfrak{f})$ of an $\mathcal{O}$-CM point on $X_1(\ell^a)$. Since we know the answer over $K(\mathfrak{f})$, the least degree over $\mathbb{Q}(\mathfrak{f})$ is either $T(\mathcal{O}, 1, \ell^a)$ or $2T(\mathcal{O}, 1, \ell^a)$, so it is a matter of whether we can save the factor of 2. It turns out that we always save the factor of 2 when ℓ is inert in $\mathcal{O}$, we never save the factor of 2 when ℓ is split in $\mathcal{O}$ unless $\ell^a = 2$, and in the ramified case whether we can save the factor of 2 depends on a subtle interplay between b and $\mathrm{ord}_\ell(\mathfrak{f})$. See Theorems 6.1, 6.2, and 6.6.

We also show that the least such degree *need not* divide all such degrees, in contrast to the case where the ground field contains K: Example 6.7. This implies that a key result that we use to compile across prime powers in the $X(M,N)_{/K}$ case, Proposition 4.9, breaks down when the ground field does not contain K, and it is for this reason that we treat prime powers only.

Our remaining results concern isogenies, in two different ways.

First, there is a close relationship between rational cyclic N-isogenies and rational points of order N in minimal degree. Part of this relationship is easy to see: if $A_{/F}$ is an abelian variety defined over a number field and $C \subset A$ is an order N cyclic étale F-subgroup scheme, then the Galois action on $C(\overline{F})$ is given by a character $\chi : \mathfrak{g}_F \to (\mathbb{Z}/N\mathbb{Z})^\times$, and thus a generator of C becomes rational over an abelian extension of degree dividing $\varphi(N)$. With a bit more care, one sees that one can make an abelian extension L/F of degree dividing $\frac{\varphi(N)}{2}$ and then a quadratic twist A^D of $A_{/L}$ to get a point of order N on $A^D(L)$ [BCS17, Thm. 5.5]. Moreover, by [BC, Thm. 6.2], if $\mathcal{O}$ is an imaginary quadratic order of discriminant $\Delta < -4$ and there is an $\mathcal{O}$-CM elliptic curve E defined over a number field $F \supset K(\mathfrak{f})$

[1] To be precise, following [DR73, §4] and [Ma77, §2] we begin with $N \in \mathbb{Z}^+$ and a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then we take Γ to be the complete preimage of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ under the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Let ζ_N be a primitive Nth root of unity, so $(\mathbb{Z}/N\mathbb{Z})^\times = \mathrm{Aut}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Then the field of definition of $X(\Gamma)$ is $\mathbb{Q}(\zeta_N)^{\det H}$.

[2] For all $N \geq 3$, if a CM elliptic curve $E_{/F}$ has $(\mathbb{Z}/N\mathbb{Z})^2 \subset E(F)$ then necessarily $F \supset K$, so the previous result essentially falls into this regime as well.

with an F-rational point of order N, then $\frac{\varphi(N)}{2} \mid [F : K(\mathfrak{f})]$. From this it follows immediately that if there is an $\mathcal{O}$-CM elliptic curve defined over any number field F, then $\frac{\varphi(N)}{2} \mid [F : \mathbb{Q}(\mathfrak{f})]$. So we see that working over either $\mathbb{Q}(\mathfrak{f})$ or $K(\mathfrak{f})$, the existence of a rational cyclic N-isogeny yields an $\mathcal{O}$-CM point of order N in the lowest possible degree extension of $\mathbb{Q}(\mathfrak{f})$ or $K(\mathfrak{f})$. Strikingly, when $N = \ell^a$ is a prime power the converse turns out to be true: for $F_0 = \mathbb{Q}(\mathfrak{f})$ or $K(\mathfrak{f})$, if we have an $\mathcal{O}$-CM elliptic curve defined over an extension F/F_0 of degree $\frac{\varphi(\ell^a)}{2}$ with an F-rational point of order N, then we have an F_0-rational cyclic ℓ^a-isogeny. Moreover, in the case where ℓ is ramified in $\mathcal{O}$, the least degree over $\mathbb{Q}(\mathfrak{f})$ in which an $\mathcal{O}$-CM elliptic curve can have a point of order ℓ^a is computed in terms of the maximum m over all a such that there is a $\mathbb{Q}(\mathfrak{f})$-rational cyclic ℓ^a-iosgeny and the supremum M over all a such that there is a $K(\mathfrak{f})$-rational cyclic ℓ^a-isogeny. (See Theorem 6.5.) When ℓ splits in $\mathcal{O}$ we always have $m = 0$ and $M = \infty$, and these parameters yield the minimal degree as well, provided $\ell^a \neq 2$. (When ℓ is inert in $\mathcal{O}$ we always have $m = M = 0$, so isogenies do not intervene. But in fact, when $\Delta < -4$, in this case the least degree over $\mathbb{Q}(\mathfrak{f})$ matches an upper bound attainable for any elliptic curve over any extension of a number field, so we feel that this case is "not really about CM": cf. Lemma 2.3.)

Thus our analysis of least degrees over $\mathbb{Q}(\mathfrak{f})$ is heavily informed by the classification of rational cyclic isogenies over both $\mathbb{Q}(\mathfrak{f})$ and $K(\mathfrak{f})$. The classification over $\mathbb{Q}(\mathfrak{f})$ is due to S. Kwon [Kw99] unless $K = \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. In fact his work holds verbatim as long as the discriminant of the CM order is not -4 or -3 (in other words, it holds for all orders in these two fields except the maximal ones). Here we complete Kwon's classification for these last two discriminants: Corollary 5.11. Moreover we generalize half of Kwon's theorem, as follows: we show that when F is any number field containing neither K nor $\mathbb{Q}(\ell\mathfrak{f})$ for any $\ell \mid N$, if no $\mathcal{O}$-CM elliptic curve admits a $\mathbb{Q}(\mathfrak{f})$-rational cyclic N-isogeny, then no $\mathcal{O}$-CM elliptic curve admits an F-rational cyclic N-isogeny: Theorem 5.3.

This result is a crucial ingredient in showing that we cannot save the factor of 2 in the case of Theorem 6.6 in which we have a $K(\mathfrak{f})$-rational cyclic ℓ^a-isogeny but no $\mathbb{Q}(\mathfrak{f})$-rational cyclic ℓ^a-isogeny.

Working with non-maximal imaginary quadratic orders brings various complications: for instance, if $\mathcal{O}$ is maximal then every fractional $\mathcal{O}$-ideal is proper, and every finite $\mathcal{O}$-submodule of $K/\mathcal{O}$ is of the form $E[I] \cong \mathcal{O}/I$ for an $\mathcal{O}$-ideal I. Both of these can fail for non-maximal orders. For these and other reasons, the study of Galois representations and torsion subgroups is distinctly easier for $\mathcal{O}_K$-CM elliptic curves. When $\mathcal{O}$ has conductor $\mathfrak{f} > 1$, if $E_{/F}$ is any $\mathcal{O}$-CM elliptic curve defined over a number field, there is a canonical F-rational cyclic $\mathfrak{f}$-isogeny $\iota : E \to E'$ with $\operatorname{End} E' = \mathcal{O}_K$, and one can try to use E' to study E. For instance, if $F \supset K$, then $\#E(F)[\text{tors}] \mid \#E'(F)[\text{tors}]$ [BC, Thm. 1.7]. In Theorem 3.1, we analyze the dual isogeny $\iota^\vee : E' \to E$, computing the intersection of its kernel $\mathcal{K}$ with any finite $\mathcal{O}_K$-submodule of E'. This result is used in the proof of Theorem 4.1. It also has the following consequence:

Let $\iota : E \to E'$ be as above, defined over a number field F containing K, and write

$$E(F) \cong \mathbb{Z}/s\mathbb{Z} \times Z/e\mathbb{Z},\ E'(F) \cong \mathbb{Z}/s'\mathbb{Z} \times \mathbb{Z}/e'\mathbb{Z},\ s \mid e,\ s' \mid e'.$$

In [BC, Lemma 6.7] we showed that $s \mid s'$: in other words, if E has full s-torsion over F, then so does E'. Here we apply the analysis of $\iota^\vee$ to show that $e' \mid e$: that is, the exponent of $E'(F)$ divides the exponent of $E(F)$. This gives a contribution to the problem of how the torsion subgroup of an elliptic curve over a number field varies within a rational isogeny class, as studied e.g. in [FN07].

2. Background

2.1. **The morphism $X_1(N) \to X_1(M)$.** For positive integers $M \mid N$, we have a map of modular curves $X_1(N) \to X_1(M)$ defined over $\mathbb{Q}$.

The following result is quite well known, but for completeness we give the proof.

Lemma 2.1. *Let $N \geq 2$. We have*

$$\deg(X_1(N) \to X(1)) = \begin{cases} \frac{N^2 \prod_{p|N}\left(1-\frac{1}{p^2}\right)}{2} & N \geq 3 \\ 2 & N = 2 \end{cases}. \tag{1}$$

Proof. For $N \in \mathbb{Z}^+$, put

$$\Gamma_1(N) \coloneqq \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z},\ a-1, b \equiv 0 \pmod{N} \right\} \subset \mathrm{SL}_2(\mathbb{Z})$$

and

$$\overline{\Gamma_1(N)} \coloneqq \Gamma_1(N)\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{Z}) \coloneqq \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}.$$

For integers $M \mid N$, we have

$$\deg(X_1(N) \to X_1(M)) = \deg(\overline{\Gamma_1(N)}\backslash\mathcal{H} \to \overline{\Gamma_1(N)}\backslash\mathcal{H}) = [\overline{\Gamma_1(M)} : \overline{\Gamma_1(N)}]. \tag{2}$$

Moreover we have

$$[\Gamma_1(1) : \Gamma_1(N)] = N^2 \prod_{p|N}\left(1 - \frac{1}{p^2}\right) \tag{3}$$

and

$$[\overline{\Gamma_1(N)} : \Gamma_1(N)] = \begin{cases} 1 & N \leq 2 \\ 2 & N \geq 3 \end{cases}. \tag{4}$$

From (2), (3) and (4), the desired result (1) follows. □

We apply Lemma 2.1 to give "worst case scenarios" on lifting torsion points on elliptic curves.

Lemma 2.2. *Let ℓ be a prime number, and let $1 \leq a < b$ be integers. Let F be a field of characteristic 0, let $E_{/F}$ be an elliptic curve, and let $P \in E(F)$ be a point of order ℓ^a.*
a) There is a field extension L/F with $[L:F] \leq \ell^{2(b-a)}$ and a point $Q \in E(L)$ such that $\ell^{b-a}Q = P$ (and thus Q has order ℓ^b).
b) If $\ell^a = 2$, then there is a field extension L/F with $[L:F] \leq 2^{2b-3}$ and a point $Q \in E(L)$ such that $2^{b-1}Q = P$ (and thus Q has order 2^b).

Proof. It follows from (1) that we have

$$\deg(Y_1(\ell^b)) \to Y_1(\ell^a)) = \begin{cases} 2^{2b-3} & \ell^a = 2 \\ \ell^{2(b-a)} & \ell^a \geq 3 \end{cases}. \tag{5}$$

Since $\ell^b \geq 4$, the curve $Y_1(\ell^b)_{/\mathbb{Q}}$ is a fine moduli space, and the result follows from (5). □

Lemma 2.3. *Let $N \geq 3$, let F be a field of characteristic 0, and let $E_{/F}$ be an elliptic curve. Then there is a field extension L/F of degree at most $\frac{N^2 \prod_{p|N}\left(1-\frac{1}{p^2}\right)}{\#\operatorname{Aut} E}$ and a twist E' of $E_{/L}$ such that $E'(L)$ has a point of order N.*

Proof. Consider the natural modular map $\pi : X_1(N) \to X(1)$, viewed as a morphsim of curves defined over F. The elliptic curve $E_{/F}$ induces a degree 1 divisor $[x]$ on $X(1)_{/F}$, so its pullback $D \coloneqq \pi^*[x]$ is an effective divisor on $X_1(N)_{/F}$ of degree

$$\deg(X_1(N) \to X(1)) = \frac{N^2 \prod_{p|N}\left(1 - \frac{1}{p^2}\right)}{2}.$$

Case 1: Suppose $j(E) \neq 0, 1728$, so $\#\operatorname{Aut} E = 2$. Then there is some closed point y in the support of D of degree at most $\frac{N^2 \prod_{p|N}\left(1-\frac{1}{p^2}\right)}{\#\operatorname{Aut} E}$. Let $L = F(y)$. By [DR73, Prop. VI.3.2] there is an elliptic curve $E'_{/L}$ and an L-rational point P of order N on E' such that the pair $(E', P)_{/L}$ induces the point y on $X_1(N)$. Since $\pi(y) = \pi([E', P]) = x = [E]$, we have $j(E') = j(E)$ and thus $E'_{/L}$ is a twist of $E_{/L}$.

Case 2: Suppose $j(E) = 1728$, so $\operatorname{Aut} E = 4$. The map $X_1(N) \to X(1)$ is ramified over $j = 1728$: more precisely because $\overline{\Gamma_1(N)}$ has no nontrivial elements of finite order and $\overline{\Gamma(1)}$ has an element of order 2, we have $D = 2[y] + D'$ for a closed point y and an effective divisor D'. Again we take $L = F(y)$. Then everything is as in Case 1 except we have the improved upper bound

$$[L : F] = [F(y) : F] \leq \frac{\deg D}{2} = \frac{N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)}{4},$$

establishing the result in this case.
Case 3: Suppose $j(E) = 0$, so $\operatorname{Aut} E = 0$. The map $X_1(N) \to X(1)$ is ramified over $j = 0$: more precisely because $\overline{\Gamma_1(N)}$ has no nontrivial elements of finite order and $\overline{\Gamma(1)}$ has an element of order 3, we have $D = 3[y] + D'$ for a closed point y and an effective divisor D'. Again we take $L = F(y)$, getting the improved upper bound

$$[L : F] = [F(y) : F] \leq \frac{\deg D}{3} = \frac{N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)}{6}. \qquad \square$$

2.2. **Orders in imaginary quadratic fields and complex multiplication.** Let K be an imaginary quadratic field, with ring of integers $\mathcal{O}_K$. Throughout this paper, $\mathcal{O}$ denotes an arbitrary $\mathbb{Z}$-order in K, i.e., a subring of K that is free of rank 2 as a $\mathbb{Z}$-module such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = K$. For such an order $\mathcal{O}$, we define the **conductor**

$$\mathfrak{f} = [\mathcal{O}_K : \mathcal{O}].$$

For each positive integer $\mathfrak{f}$, there is a unique order $\mathcal{O}$ in K of conductor $\mathfrak{f}$, namely

$$\mathbb{Z} + \mathfrak{f}\mathcal{O}_K.$$

We let $\Delta = \Delta(\mathcal{O})$ be the discriminant of $\mathcal{O}$ (defined e.g. as the discriminant of the trace form, as for any $\mathbb{Z}$-algebra that is finitely generated and free as a $\mathbb{Z}$-module). Put $\Delta_K = \Delta(\mathcal{O}_K)$; then

$$\Delta(\mathcal{O}) = \mathfrak{f}^2 \Delta_K.$$

We let

$$w \coloneqq w(\mathcal{O}) = \#\mathcal{O}^\times, \ w_K \coloneqq \#\mathcal{O}_K^\times.$$

In particular, we have

$$w = \begin{cases} 6 & \text{if } \Delta = -3 \\ 4 & \text{if } \Delta = -4 \\ 2 & \text{if } \Delta < -4 \end{cases}.$$

An elliptic curve E defined over a field F of characteristic 0 has complex multiplication (CM) if $\operatorname{End} E_{/\overline{F}}$ is strictly larger than $\mathbb{Z}$, in which case it is necessarily an imaginary quadratic order $\mathcal{O}$. We denote by $\mathbb{Q}(\mathfrak{f})$ the field $\mathbb{Q}(j(E))$. Then $[\mathbb{Q}(\mathfrak{f}) : \mathbb{Q}] = \#\operatorname{Pic}\mathcal{O}$. We put $K(\mathfrak{f}) = K(j(E))$; this is the $\mathfrak{f}$-ring class field of K.[3] We have [Co89, Cor. 7.24]

$$[K(N) : K^{(1)}] = \frac{2}{w_K} N \prod_{p|N} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right). \tag{6}$$

[3]The field $K(\mathfrak{f})$ is always Galois over $\mathbb{Q}$, but the field $\mathbb{Q}(j(E))$ is Galois over $\mathbb{Q}$ iff $\operatorname{Pic}\mathcal{O}$ is a 2-torsion group, which holds only in finitely many cases. Thus the notation $\mathbb{Q}(\mathfrak{f})$ is slightly abusive because, as a subfield of $\mathbb{C}$, $\mathbb{Q}(\mathfrak{f})$ depends upon the chosen $\mathcal{O}$-CM elliptic curve. However, up to Galois conjugacy it does not, so no harm comes from this.

2.3. **Galois representations of elliptic curves.** For a field F of characteristic 0, let F^{sep} be a separable closure of F and let $\mathfrak{g}_F = \mathrm{Aut}(F^{\mathrm{sep}}/F)$ be the absolute Galois group of F. For an elliptic curve E defined over F and $N \in \mathbb{Z}^+$, let

$$\rho_N : \mathfrak{g}_F \to \mathrm{Aut}\, E[N] \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

be the mod N Galois representation, and let

$$\overline{\rho_N} : \mathfrak{g}_F \to \mathrm{Aut}\, E[N]/\mathrm{Aut}(E) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\mathrm{Aut}(E)$$

be the reduced mod N Galois representation. The advantage of the reduced Galois representation is that it is independent of the chosen F-rational model of E; it depends only on $j(E)$.

For $N \in \mathbb{Z}^+$, we put

$$C_N(\mathcal{O}) = (\mathcal{O}/N\mathcal{O})^\times,$$

the mod N Cartan subgroup. Let $q_N : \mathcal{O} \to \mathcal{O}/N\mathcal{O}$ be the natural map. The **reduced Cartan subgroup** is

$$\overline{C_N(\mathcal{O})} = C_N(\mathcal{O})/q_N(\mathcal{O}^\times).$$

If $E_{/F}$ has CM by the order $\mathcal{O}$ in K and if $F \supset K$, then the Galois action commutes with the $\mathcal{O}$-action and thus

$$\rho_N : \mathfrak{g}_F \to (\mathcal{O}/N\mathcal{O})^\times, \overline{\rho_N} : \mathfrak{g}_F \to \overline{C_N(\mathcal{O})}.$$

If $F = K(\mathfrak{f})$, work of Stevenhagen implies $\overline{\rho_N}(\mathfrak{g}_F) = \overline{C_N(\mathcal{O})}$. See [St01, §4] and [BC, Cor. 1.2].

2.4. **Weber functions and fields of moduli.** If E is an elliptic curve defined over a field F of characteristic 0, we define a Weber function $\mathfrak{h}$ to be the composition of the quotient map $E \to E/\mathrm{Aut}(E)$ with an F-isomorphism $E/\mathrm{Aut}(E) \cong \mathbb{P}^1$: thus a Weber function is uniquely specified up to an element of $\mathrm{PGL}_2(\mathrm{F}) = \mathrm{Aut}\, \mathbb{P}^1_{/F}$. If $E_{/F}$ is given by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in F$, then for $P = (x, y) \in E(\overline{F})$, we may take [Si94, Ex. II.5.5.1]

$$\mathfrak{h}(P) = \begin{cases} x & AB \neq 0 \\ x^2 & B = 0 \\ x^3 & A = 0 \end{cases}.$$

We have $B = 0$ iff $j(E) = 1728$ iff $\mathrm{End}\, E$ is the imaginary quadratic order of discriminant -4, and $A = 0$ iff $j(E) = 0$ iff $\mathrm{End}\, E$ is the imaginary quadratic order of discriminant -3.

For $P \in E(\overline{F})$, the Weber function field $F(\mathfrak{h}(P))$ is model-independent in the following sense: let $E'_{/F}$ be an elliptic curve such that there is an isomorphism $\psi : E_{/\overline{F}} \to E'_{/\overline{F}}$. Then $F(\mathfrak{h}(P)) = F(\mathfrak{h}(\psi(P)))$. This can be seen either because $E'_{/F}$ is obtained by twisting $E_{/F}$ by a cocycle $\eta \in Z^1(\mathfrak{g}_F, \mathrm{Aut}\, E)$ or by use of Weierstrass equations as above: cf. [Sh94, p. 107].

For $E_{/F}$ and $P \in E(\overline{F})$ of order N, we have $\mathbb{Q}(j(E), \mathfrak{h}(P)) \subset F(P)$. In fact $\mathbb{Q}(j(E), \mathfrak{h}(P))$ is the residue field $\mathbb{Q}(x)$ of the closed point $x = [(E, P)]$ on the modular curve $X_1(N)_{/\mathbb{Q}}$. Moreover, there is a model of $E_{/\mathbb{Q}(j(E),(\mathfrak{h}(P))}$ such that $P \in E(\mathbb{Q}(j(E), \mathfrak{h}(P))$ [DR73, Prop. VI.3.2].

2.5. **Isogenies of CM elliptic curves.** Let $\varphi : E \to E'$ be an isogeny of K-CM elliptic curves over $\mathbb{C}$. Let $\mathcal{O} = \mathcal{O}(\mathfrak{f}) = \mathrm{End}\, E$, $\mathcal{O}' = \mathcal{O}(\mathfrak{f}') = \mathrm{End}\, E'$, and suppose that $\mathfrak{f}' \mid \mathfrak{f}$. We may represent E as $\mathbb{C}/\mathfrak{a}$ for a proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$ and then $E' = \mathbb{C}/\Lambda$ for a proper fractional $\mathcal{O}'$-ideal $\Lambda \supset \mathfrak{a}$. Thus also $\mathfrak{a}\mathcal{O}' \subset \mathcal{O}'$. Putting $E'' = \mathbb{C}/\mathfrak{a}\mathcal{O}'$, the isogeny φ factors as

$$E \stackrel{\iota_{\mathfrak{f},\mathfrak{f}'}}{\to} E'' \stackrel{\varphi'}{\to} E'.$$

Recall that for an imaginary quadratic order $\mathcal{O}$, a fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is proper iff it is projective [BCS17, Lemma 3.1]. Thus $\mathfrak{a}$ is a projective $\mathcal{O}$-module, so $\mathfrak{a}\mathcal{O}' = \mathfrak{a} \otimes_{\mathcal{O}} \mathcal{O}'$ is a projective $\mathcal{O}'$-module, hence $\mathfrak{a}\mathcal{O}'$ is a proper fractional $\mathcal{O}'$-ideal, i.e., $\mathrm{End}\, E'' = \mathcal{O}'$. This shows that $\iota_{\mathfrak{f},\mathfrak{f}'}$ is the universal isogeny from an $\mathcal{O}(\mathfrak{f})$-CM elliptic curve to an $\mathcal{O}(\mathfrak{f}')$-CM elliptic curve. Moreover we have

$$\ker \iota_{\mathfrak{f},\mathfrak{f}'} = \mathfrak{a}\mathcal{O}'/\mathfrak{a} \cong \mathbb{Z}/\frac{\mathfrak{f}}{\mathfrak{f}'}\mathbb{Z}.$$

(This is easy when $\mathfrak{a} = \mathcal{O}$, but by [BCS17, Lemma 3.1], for all primes p we have $\mathfrak{a} \otimes \mathbb{Z}_p \cong \mathcal{O} \otimes \mathbb{Z}_p$, so the general case reduces to this.) This shows that there is only one possible kernel for a $\frac{\mathfrak{f}}{\mathfrak{f}'}$-isogeny from an $\mathcal{O}$-CM elliptic curve to an $\mathcal{O}'$-CM elliptic curve, and thus $\iota_{\mathfrak{f},\mathfrak{f}'}$ must be $\mathbb{Q}(\mathfrak{f})$-rational. (This is a well known result. For other treatments, see [Kw99, §2] and [BP17, Prop. 2.2].)

Now suppose that $\varphi : E \to E'$ is an isogeny of K-CM elliptic curves over $\mathbb{C}$ with $\operatorname{End} E = \operatorname{End} E' = \mathcal{O} = \mathcal{O}(\mathfrak{f})$. We may represent φ as $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ where $\Lambda' \supset \Lambda$ are proper (thus invertible) fractional $\mathcal{O}$-ideals. Taking $\mathfrak{b} = (\Lambda')^{-1}\Lambda$, we have $\Lambda' = \Lambda\mathfrak{b}^{-1}$, so

$$\ker \varphi = \Lambda\mathfrak{b}^{-1}/\Lambda = E[\mathfrak{b}].$$

It follows by [BCS17, §3.3] that φ is defined over a field $F \supset \mathbb{Q}(\mathfrak{f})$ iff $F \supset K$ or $\mathfrak{b}$ is real.

2.6. Classification of $K(\mathfrak{f})$-rational cyclic isogenies.

Theorem 2.4. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant Δ, and suppose that $\Delta < -4$. Let $N \in \mathbb{Z}^+$. The following are equivalent:*
(i) There is an $\mathcal{O}$-CM elliptic curve E and a $K(\mathfrak{f})$-rational cyclic N-isogeny $\varphi : E \to E'$.
(ii) There is a point $P \in \mathcal{O}/N\mathcal{O}$ of order N with $C_N(\mathcal{O})$-orbit of size $\varphi(N)$.
(iii) We have that Δ is a square in $\mathbb{Z}/4N\mathbb{Z}$.

Proof. Combine [BC, Thm. 6.18a)] with [BC, Thm. 6.15]. □

3. The dual isogeny

Let $\iota : E \to E'$ be the canonical cyclic $\mathfrak{f}$-isogeny to an $\mathcal{O}_K$-CM elliptic curve, and let $\iota^\vee$ be the dual isogeny. There is an embedding $K(\mathfrak{f}) \hookrightarrow \mathbb{C}$ such that $E_{/\mathbb{C}} \cong \mathbb{C}/\mathcal{O}$, $E'_{/C} \cong \mathbb{C}/\mathcal{O}_K$, ι is the quotient map and $\iota^\vee$ is $P + \mathcal{O}_K \mapsto \mathfrak{f}P + \mathcal{O}$.

In this section, we will compute $\iota^\vee(T')$ for any finite $\mathcal{O}_K$-submodule $T' \subset E'[\mathrm{tors}]$.

The following result will be proved in the next section.

Theorem 3.1. *Put $\mathcal{K} \coloneqq \ker \iota^\vee : E' \to E$ and $c \coloneqq \operatorname{ord}_\ell(\mathfrak{f})$.*
a) Suppose $\left(\frac{\Delta_K}{\ell}\right) = 1$, and let $\mathfrak{p}_1, \mathfrak{p}_2$ be the two primes[4] of $\mathcal{O}_K$ lying over ℓ. For $0 \le a \le b$ we have

$$\mathcal{K} \cap E'[\mathfrak{p}_1^a\mathfrak{p}_2^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\min(a,c)}\mathbb{Z}$$

and

$$\iota^\vee E'[\mathfrak{p}_1^a\mathfrak{p}_2^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\max(a-c,0)}\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

b) Suppose $\left(\frac{\Delta_K}{\ell}\right) = 0$, and let $\mathfrak{p}$ be the prime of $\mathcal{O}_K$ lying over ℓ. For all $d \in \mathbb{Z}^+$ we have

$$\mathcal{K} \cap E'[\mathfrak{p}^d] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\min(c,\lfloor \frac{d}{2} \rfloor)}\mathbb{Z}$$

and

$$\iota^\vee E'[\mathfrak{p}^d] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\max(\lfloor \frac{d}{2} \rfloor - c,0)}\mathbb{Z} \times \mathbb{Z}/\ell^{\lceil \frac{d}{2} \rceil}\mathbb{Z}.$$

c) Suppose $\left(\frac{\Delta_K}{\ell}\right) = -1$. For all $b \in \mathbb{Z}^+$ we have

$$\mathcal{K} \cap E[\ell^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\min(b,c)}\mathbb{Z}$$

and

$$\iota^\vee E'[\ell^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\max(b-c,0)}\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

From Theorem 3.1 we deduce the following result.

[4]The statement is not symmetric in $\mathfrak{p}_1$ and $\mathfrak{p}_2$, but it still holds after interchanging $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

Theorem 3.2. *Let $F \supset K(\mathfrak{f})$ be a number field, and let $\iota : E \to E'$ be the canonical $K(\mathfrak{f})$-rational cyclic $\mathfrak{f}$-isogeny to an $\mathcal{O}_K$-CM elliptic curve E'. Write*

$$E(F)[\mathrm{tors}] \cong \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/e\mathbb{Z}, \ E'(F)[\mathrm{tors}] \cong \mathbb{Z}/s'\mathbb{Z} \times \mathbb{Z}/e'\mathbb{Z}$$

with $s \mid e$ and $s' \mid e'$. Then $e' \mid e$.

Proof. It is enough to show that for all primes ℓ we have $\exp E'(F)[\ell^\infty] \mid \exp E(F)[\ell^\infty]$. Since $E'(F)[\ell^\infty]$ is a finite ℓ-primary $\mathcal{O}_K$-submodule of $E'[\mathrm{tors}]$, it is isomorphic to $E[I]$ for an ideal I of $\mathcal{O}_K$ that is divisible only by prime ideals lying over ℓ. Recalling that when ℓ ramifies in $\mathcal{O}_K$ we have

$$E'[\mathfrak{p}^d] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\lceil \frac{d}{2} \rceil}\mathbb{Z} \times \mathbb{Z}/\ell^{\lfloor \frac{d}{2} \rfloor}\mathbb{Z},$$

we see that Theorem 3.1 implies that in all cases

$$\exp E'(F)[\ell^\infty] = \exp E'[I] \mid \exp \iota^\vee E'[I] \mid \exp E(F)[\ell^\infty]. \qquad \square$$

Remark 3.3. *In* [BC, Lemma 6.7] *it was shown that in the setting of Theorem 3.2 we have $s \mid s'$. Theorem 3.2 is in some sense the "dual divisibility."*

3.1. **Inert case.** We suppose that $\left(\frac{\Delta_K}{\ell}\right) = -1$. Put $c \coloneqq \mathrm{ord}_\ell(\mathfrak{f})$. In this case the only finite $\mathcal{O}_K$-modules of $E'[\ell^\infty]$ are $E'[\ell^b]$ for $b \in \mathbb{Z}^+$. This is an easy case: if $\mathcal{K} = \ker \iota^\vee$ then $\mathcal{K} \cap E[\ell^b]$ is cyclic of order $\ell^{\min(b,c)}$ and $\iota^\vee(E[\ell^b])$ is the subgroup of $\mathbb{C}/\mathcal{O}$ generated by $\ell^c \cdot \frac{1}{\ell^b}$ and $\ell^{\mathfrak{a}} \cdot \frac{\tau_K}{\ell^b}$, and thus

$$\iota^\vee E'[\ell^b] \cong \mathbb{Z}/\ell^{\max(b-c,0)}\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

3.2. **Split case.** We suppose that $\left(\frac{\Delta_K}{\ell}\right) = 1$ and $\ell \mid \mathfrak{f}$. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the two primes of $\mathcal{O}_K$ lying over ℓ. We have

$$E'[\mathfrak{p}_1^a\mathfrak{p}_2^b] \cong E'[\mathfrak{p}_1^a] \oplus E'[\mathfrak{p}_2^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

We have $\mathcal{K} = \ker \iota^\vee$ is cyclic of order $\mathfrak{f}$, generated by $\frac{1}{\mathfrak{f}} + \mathcal{O}_K$. If $P \in \mathcal{K} \cap E'[\mathfrak{p}_1^a\mathfrak{p}_2^b]$ has order d, then $d \mid \ell^b$ and $d \mid \mathfrak{f}$, so $d \mid \ell^c$. Also the $\mathcal{O}_K$-submodule $\langle\langle P \rangle\rangle$ generated by P is $E'[d]$; since the largest d such that $E'[d] \subset [\mathfrak{p}_1^a\mathfrak{p}_2^b]$ is ℓ^a, we get $d \mid \ell^a$ and thus $d \mid \ell^{\min(a,c)}$. On the other hand, the unique cyclic subgroup of $\mathcal{K}$ of order $\ell^{\min(a,c)}$ is also contained in $E'[\mathfrak{p}_1^a\mathfrak{p}_2^b]$, so

$$\mathcal{K} \cap E'[\mathfrak{p}_1^a\mathfrak{p}_2^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\min(a,c)}\mathbb{Z}.$$

In particular it follows that $\mathcal{K} \cap E'[\mathfrak{p}_2^b]$ is the trivial group, so

$$\iota^{vee}(E'[\mathfrak{p}_2^b]) \cong_{\mathbb{Z}} E'[\mathfrak{p}_2^b] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^b\mathbb{Z},$$

and it follows that $\exp \iota^\vee E[\mathfrak{p}_1^a\mathfrak{p}_2^b] = \ell^b$. Since

$$\#\iota^\vee E[\mathfrak{p}_1^a\mathfrak{p}_2^b] = \frac{\#E[\mathfrak{p}_1^a\mathfrak{p}_2^b]}{\ell^{\min(a,c)}} = a + b - \min(a,c),$$

it follows that

$$\iota^\vee E[\mathfrak{p}_1^a\mathfrak{p}_2^b] \cong \mathbb{Z}/\ell^{\max(a-c,0)}\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

3.3. **Ramified case.** We suppose that $\left(\frac{\Delta_K}{\ell}\right) = 0$ and $\ell \mid \mathfrak{f}$.

Step 1: Let $\underline{a} = \min(a,c)$. Let $\mathfrak{p}$ be the unique prime of $\mathcal{O}_K$ lying over ℓ. Let $\iota : E \to E'$ be the canonical $K(\mathfrak{f})$-rational cyclic $\mathfrak{f}$-isogeny to an $\mathcal{O}_K$-CM elliptic curve $E'_{/K(\mathfrak{f})}$. Let $\mathcal{K} = \ker \iota^\vee$. For $d \in \mathbb{Z}^+$, we compute $E[\mathfrak{p}^d] \cap K$. This intersection is generated by $\frac{x}{\ell^c}$ for some $x \in \mathbb{Z}$, while $E[\mathfrak{p}^d] \cong \mathfrak{p}^{-d}/\mathcal{O}_K$. We have

$$\frac{x}{\ell^c} \in \mathfrak{p}^{-d} \iff x \in \ell^c\mathfrak{p}^{-d} = \mathfrak{p}^{2c-d}.$$

• If d is even, then

$$x \in (\ell)^{c-\frac{d}{2}},$$

so $\mathrm{ord}_\ell(x) \geq c - \frac{d}{2}$. If $c - \frac{d}{2} \leq 0$, this condition is vacuous and $E'[\mathfrak{p}^d] \cap \mathcal{K}$ is generated by $\frac{1}{\ell^c}$ and thus is cyclic of order ℓ^c. If $c - \frac{d}{2} \geq 0$ then $E[\mathfrak{p}^d] \cap \mathcal{K}$ is cyclic of order $\ell^{d/2}$. Compiling the two cases, we get that $E[\mathfrak{p}^d] \cap \mathcal{K}$ is cyclic of order $\ell^{\min(c,d/2)}$.

• If d is odd, then since $\mathrm{ord}_{\mathfrak{p}}(x)$ is even, the above gives $\mathrm{ord}_{\mathfrak{p}}(x) \geq 2c - (d-1)$, and running through the argument as above, we get that $E[\mathfrak{p}^d] \cap \mathcal{K}$ is cyclic of order $\ell^{\min(c, \frac{d-1}{2})}$.
• Thus in general we have

$$\#E'[\mathfrak{p}^d] \cap \mathcal{K} = \ell^{\min(c, \lfloor \frac{d}{2} \rfloor)}.$$

By [BC, §7.3], we have

$$E'[\mathfrak{p}^{2b-1}] \cong \mathbb{Z}/\ell^b\mathbb{Z} \times \mathbb{Z}/\ell^{b-1}\mathbb{Z}, \ E'[\mathfrak{p}^{2b}] = E'[\ell^b] \cong \mathbb{Z}/\ell^b\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

We claim that in the first case we can take $\frac{1}{\ell^{b-1}}$ as a generator for the second invariant factor, and the second case we can take $\frac{1}{\ell^b}$ as a generator for the second invariant factor. In the latter case this is clear: any element of order ℓ^b can be taken as a generator for the second invariant factor. In the former case, the elements that can be taken as a generator of the second invariant factor are precisely those elements x of order ℓ^{b-1} that generate a **pure** subgroup of $E'[\mathfrak{p}^{2b-1}]$: for all $m, i \in \mathbb{Z}^+$, if there is $y \in E'[\mathfrak{p}^{2b-1}]$ such that $mx = \ell^i y$, then $mx = \ell^i nx$ for some $n \in \mathbb{Z}$. (For in a commutative group G with $G = G[\ell^b]$ for some $b \in \mathbb{Z}^+$, every pure subgroup is a direct summand [Ro96, §4.3].) We apply this with $x = \frac{1}{\ell^{b-1}}$: if $mx = \ell^i y$ for $y \in \mathfrak{p}^{-(2b-1)}$, then $m\ell^{-b-i+1} \in \mathfrak{p}^{-(2b+1)}$, so

$$m \in \ell^{b+i-1}\mathfrak{p}^{-(2b-1)} = \mathfrak{p}^{2b+2i-2}\mathfrak{p}^{-2b+1} = \mathfrak{p}^{2i-1},$$

so $\mathrm{ord}_{\mathfrak{p}}(m) \geq 2i-1$. Since $m \in \mathbb{Z}$, $\mathrm{ord}_{\mathfrak{p}}(m)$ is even, so $\mathrm{ord}_{\mathfrak{p}}(m) \geq 2i$ and thus $\ell^i \mid m$ and we may take $n = \frac{m}{\ell^i}$. It follows that

$$\exp \iota^\vee(E[\mathfrak{p}^{2b-1}]) = \exp \iota^\vee(E[\mathfrak{p}^{2b}]) = \ell^b$$

and thus

$$\exp \iota^\vee(E[\mathfrak{p}^d]) = \ell^{\lceil \frac{d}{2} \rceil}.$$

Since

$$\#\iota^\vee E[\mathfrak{p}^d] = \frac{\#E[\mathfrak{p}^d]}{\ell^{\min(c, \lfloor \frac{d}{2} \rfloor)}} = \ell^{d - \min(c, \lfloor \frac{d}{2} \rfloor)},$$

it follows that

$$\iota^\vee E'[\mathfrak{p}^d] \cong_{\mathbb{Z}} \mathbb{Z}/\ell^{\max(\lfloor \frac{d}{2} \rfloor - c, 0)}\mathbb{Z} \times \mathbb{Z}/\ell^{\lceil \frac{d}{2} \rceil}\mathbb{Z}.$$

4. Degrees of CM points on $X(M,N)_{/K(\zeta_M)}$

4.1. **Statement of the theorem.**

Theorem 4.1. *Let $\mathcal{O}$ be an imaginary quadratic order of conductor $\mathfrak{f}$, and let $M = \ell_1^{a_1} \cdots \ell_r^{a_r} \mid N = \ell_1^{b_1} \cdots \ell_r^{b_r}$ be positive integers. Put $c := \mathrm{ord}_\ell(\mathfrak{f})$.*
a) There is $T(\mathcal{O}, M, N) \in \mathbb{Z}^+$ such that: for all $d \in \mathbb{Z}^+$, there is a number field $F \supset K(\mathfrak{f})$ such that $[F : K(\mathfrak{f})] = d$ and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$ iff $T(\mathcal{O}, M, N) \mid d$.
b) If $N = 2$ or 3, then $T(\mathcal{O}, M, N)$ is as follows:

$$T(\mathcal{O}, 1, 2) = \begin{cases} 3 & \left(\frac{\Delta}{2}\right) = -1 \text{ and } \Delta \neq -3 \\ 1 & \text{otherwise} \end{cases},$$

$$T(\mathcal{O}, 1, 3) = \begin{cases} 8/w & \left(\frac{\Delta}{3}\right) = -1 \text{ and } \Delta \neq -3 \\ 1 & \text{otherwise} \end{cases},$$

$$T(\mathcal{O}, 2, 2) = \frac{2(2 - \left(\frac{\Delta}{2}\right))}{w},$$

$$T(\mathcal{O}, 3, 3) = \frac{2(3 - \left(\frac{\Delta}{3}\right))}{w}.$$

c) Suppose $N \geq 4$ and $r = 1$, and write $M = \ell^a$, $N = \ell^b$ for $0 \leq a \leq b$. Then:
(i) If $\left(\frac{\Delta}{\ell}\right) = -1$, then

$$\widetilde{T}(\mathcal{O}, \ell^a, \ell^b) = \ell^{2b-2}(\ell^2 - 1).$$

(ii) If $\left(\frac{\Delta}{\ell}\right) = 1$*, then*

$$\widetilde{T}(\mathcal{O}, \ell^a, \ell^b) = \begin{cases} \ell^{b-1}(\ell-1) & a = 0 \\ \ell^{a+b-2}(\ell-1)^2 & a \geq 1 \end{cases}.$$

(iii) If $\ell \mid \mathfrak{f}$ *and* $\left(\frac{\Delta_K}{\ell}\right) = 1$*, then*

$$\widetilde{T}(\mathcal{O}, \ell^a, \ell^b) = \ell^{a+b-1}(\ell-1).$$

(iv) If $\left(\frac{\Delta_K}{\ell}\right) = 0$*, then*

$$\widetilde{T}(\mathcal{O}, \ell^a, \ell^b) = \begin{cases} \ell^{a+b-1}(\ell-1) & b \leq 2c+1 \\ \ell^{\max(a+b-1, 2b-2c-2)}(\ell-1) & b > 2c+1 \end{cases}.$$

(v) If $\ell \mid \mathfrak{f}$ *and* $\left(\frac{\Delta_K}{\ell}\right) = -1$*, then*

$$\widetilde{T}(\mathcal{O}, \ell^a, \ell^b) = \begin{cases} \ell^{a+b-1}(\ell-1) & b \leq 2c \\ \ell^{\max(a+b-1, 2b-2c-1)}(\ell-1) & b > 2c \end{cases}.$$

d) Suppose $N \geq 4$*. Then we have*

$$T(\mathcal{O}, M, N) = \frac{\prod_{i=1}^r \widetilde{T}(\mathcal{O}, \ell_i^{a_i}, \ell_i^{b_i})}{w}.$$

4.2. **Prime power case.**

f Let ℓ be a prime number. Let $0 \leq a \leq b$ be natural numbers. We assume that $b \geq 1$ and that $\ell^b \geq 4$.

Let $\mathcal{O}$ be the order in the imaginary quadratic field K of conductor $\mathfrak{f}$. Let E be an $\mathcal{O}$-CM elliptic curve defined over a number field F that contains K. Let $w = \#\mathcal{O}^\times$ and $w_K = \#\mathcal{O}_K^\times$.

The following preliminary result is a strengthening of [BCP17, Lemma 2.3].

Proposition 4.2. *Let* E *be an* $\mathcal{O}$*-CM elliptic curve defined over a number field* $F \supset K$*, and suppose*

$$\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F).$$

a) If $\left(\frac{\Delta}{\ell}\right) = -1$*, then* $a = b$ *and* $\ell^{2b-2}(\ell^2-1) \mid w[F : K(\mathfrak{f})]$*.*
b) If $\left(\frac{\Delta}{\ell}\right) = 1$ *and* $a = 0$*, then* $\ell^{b-1}(\ell-1) \mid w[F : K(\mathfrak{f})]$*.*
c) If $\left(\frac{\Delta}{\ell}\right) = 1$ *and* $a \geq 1$*, then* $\ell^{a+b-2}(\ell-1)^2 \mid w[F : K(\mathfrak{f})]$*.*
d) If $\left(\frac{\Delta}{\ell}\right) = 0$*, then* $\ell^{a+b-1}(\ell-1) \mid w[F : K(\mathfrak{f})]$*.*

Proof. By the results of [BC, Thm. 1.1], we have $F(E[\ell^b]) \supset K^{(\ell^b)}K(\mathfrak{f}\ell^b)$, so

$$\#\overline{C_{\ell^b}(\mathcal{O})} = [K^{(\ell^b)}K(\mathfrak{f}\ell^b) : K(\mathfrak{f})] \mid [F(E[\ell^b]) : K(\mathfrak{f})] = [F(E[\ell^b]) : F][F : K(\mathfrak{f})].$$

a) If $\left(\frac{\Delta}{\ell}\right) = -1$, then $C_{\ell^b}(\mathcal{O})$ acts transitively on points of order ℓ^b, so $a = b$ and $F = F(E[\ell^b])$, so

$$\frac{\ell^{2b-2}(\ell^2-1)}{w} = \#\overline{C_{\ell^b}(\mathcal{O})} \mid [F : K(\mathfrak{f})].$$

b) In this case, by [BCP17, Lemma 2.2], we have $[F(E[\ell^b]) : F] \mid \ell^{b-1}(\ell-1)$, so

$$\frac{\ell^{2b-2}(\ell-1)^2}{w} = \#\overline{C_{\ell^b}(\mathcal{O})} \mid [F(E[\ell^b]) : F][F : K(\mathfrak{f})] \mid \ell^{b-1}(\ell-1)[F : K(\mathfrak{f})],$$

and the result follows.
c),d) In both of these cases, by [BCP17, Lemma 2.2] we have $[F(E[\ell^b]) : F] \mid \ell^{b-a}$, so

$$\frac{\#\overline{C_{\ell^b}(\mathcal{O})}}{\ell^{b-a}} \mid [F : K(\mathfrak{f})].$$

Since

$$\#\overline{C_{\ell^b}(\mathcal{O})} = \begin{cases} \ell^{2b-2}(\ell-1)^2 & \left(\frac{\Delta}{\ell}\right) = 1 \\ \ell^{2b-1}(\ell-1) & \left(\frac{\Delta}{\ell}\right) = 0 \end{cases}$$

the result follows. □

Theorem 4.3. *Suppose* $\left(\frac{\Delta}{\ell}\right) = -1$*, and let* $b \in \mathbb{Z}^+$.
a) We have

$$w[K^{(\ell^b)}K(\mathfrak{f}\ell^b) : K(\mathfrak{f})] = \ell^{2b-2}(\ell^2-1).$$

b) There is an elliptic curve $E_{/K^{(\ell^b)}K(\mathfrak{f}\ell^b)}$ *such that*

$$E(K^{(\ell^b)}K(\mathfrak{f}\ell^b))[\ell^\infty] \cong \mathbb{Z}/\ell^b\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

Proof. By [BC, Thm. 1.1] we have

$$[K^{(\ell^b)}K(\mathfrak{f}\ell^b) : K(\mathfrak{f})] = \#\overline{C_{\ell^b}(\mathcal{O})} = \frac{\#C_{\ell^b}(\mathcal{O})}{w} = \frac{\ell^{2b-2}(\ell^2-1)}{w},$$

establishing part a). By [BC, Cor. 1.4] there is an $\mathcal{O}$-CM elliptic curve $E_{/K^{(\ell^b)}K(\mathfrak{f}\ell^b)}$ with $\mathbb{Z}/\ell^b\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(K^{(\ell^b)}K(\mathfrak{f}\ell^b))$. If the ℓ-primary torsion subgroup were any larger, then there would be full ℓ^{b+1}-torsion, which would imply that $K^{(\ell^b)}K(\mathfrak{f}\ell^b) \supset K^{(\ell^{b+1})}K(\mathfrak{f}\ell^{b+1})$. But since $[K^{(\ell^b)}K(\mathfrak{f}\ell^b) : K(\mathfrak{f})] = \frac{\ell^{2b-2}(\ell^2-1)}{w}$ is an increasing function of b, this is absurd. □

Theorem 4.4. *Suppose* $\left(\frac{\Delta}{\ell}\right) = 1$*. Let* $\mathfrak{p}_1, \mathfrak{p}_2$ *be the two primes of* $\mathcal{O}_K$ *lying over* ℓ*. Let* $a, b \in \mathbb{N}$ *with* $a \leq b$ *and* $\ell^b \geq 4$.
a) There is a number field $F \supset K(\mathfrak{f})$ *with*

$$w[F : K(\mathfrak{f})] = \begin{cases} \ell^{b-1}(\ell-1) & a = 0 \\ \ell^{a+b-2}(\ell-1)^2 & a \geq 1 \end{cases}$$

and an $\mathcal{O}$*-CM elliptic curve* $E_{/F}$ *such that* $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$.
b) If $\Delta_K \notin \{-4, -3\}$ *or if* $\mathfrak{f} = 1$*, then we may take* $F = K^{\mathfrak{p}_1^a\mathfrak{p}_2^b}K(\mathfrak{f})$.
c) If $\mathfrak{f} \neq 1$ *and* $\Delta_K \in \{-4, -3\}$*, then we may take* F *to be an extension of* $K^{\mathfrak{p}_1^a\mathfrak{p}_2^b}$ *of degree* $\frac{w_K}{2}$.

Proof. First suppose $\mathfrak{f} = 1$, i.e., $\mathcal{O} = \mathcal{O}_K$. By the results of [BC, §7.3], there is an $\mathcal{O}_K$-CM elliptic curve $E_{/K^{\mathfrak{p}_1^a\mathfrak{p}_2^b}}$ with $\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(K^{\mathfrak{p}_1^a\mathfrak{p}_2^a})$. By [BC, Lemma 2.10] we have

$$w_K[K^{\mathfrak{p}_1^a\mathfrak{p}_2^b} : K^{(1)}] = \begin{cases} \ell^{b-1}(\ell-1) & a = 0 \\ \ell^{a+b-2}(\ell-1)^2 & a \geq 1 \end{cases}. \tag{7}$$

By Proposition 4.2 we must have $E(K^{\mathfrak{p}_1^a\mathfrak{p}_2^b})[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, completing the proof in this case.

Next suppose $\mathfrak{f} > 1$ and $\Delta_K \notin \{-4, -3\}$. Let $E_{/K(\mathfrak{f})}$ be an $\mathcal{O}$-CM elliptic curve, and let $\iota : E \to E'$ be the canonical $K(\mathfrak{f})$-rational cyclic $\mathfrak{f}$-isogeny to an $\mathcal{O}_K$-CM elliptic curve E'. Then $T' \coloneqq E'[\mathfrak{p}_1^a\mathfrak{p}_2^b] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, and $K^{(1)}(\mathfrak{h}(E'[\mathfrak{p}_1^a\mathfrak{p}_2^b])) = K^{\mathfrak{p}_1^a\mathfrak{p}_2^b}$. Since $w_K = 2$, it follows that for all $\sigma \in \mathfrak{g}_F$ there is $\epsilon(\sigma) \in \pm 1$ such that for all $P' \in T'$ we have $\sigma P' = \epsilon(\sigma)P'$. Let $\iota^\vee_{/K(\mathfrak{f})} : E' \to E$ be the dual isogeny, also cyclic of order $\mathfrak{f}$. Put $T \coloneqq \iota^\vee(T')$. Since $\gcd(\mathfrak{f}, \ell) = 1$, the map $\iota^\vee : T' \to T$ is an isomorphism of $\mathfrak{g}_F$-modules, and thus for all $P \in T$, we have $\sigma P = \epsilon(\sigma)P$. Thus ϵ is a (possibly trivial) quadratic character on $\mathfrak{g}_F$, and twisting E by ϵ we get an elliptic curve $E_{/F}$ such that

$$\mathbb{Z}\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \cong T \subset E(F).$$

Since $w_K = 2$, (7) implies

$$[F : K(\mathfrak{f})] \leq \begin{cases} \frac{\ell^{b-1}(\ell-1)}{2} & a = 0 \\ \frac{\ell^{a+b-2}(\ell-1)}{2} & a \geq 1 \end{cases}.$$

By Proposition 4.2 we must have equality. Similarly, we must have $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, because if the ℓ-primary torsion subgroup were any larger, it would contradict Proposition 4.2.

Finally suppose $\mathfrak{f} > 1$ and $\Delta_K \in \{-4, -3\}$: thus w_K is 4 or 6 while $w = 2$. Then over the field $F_0 \coloneqq K^{\mathfrak{p}_1^a \mathfrak{p}_2^b K(\mathfrak{f})}$ the action of $\mathfrak{g}_{F_0}$ on T' is now by a character with values in $\mathcal{O}_K^\times$. There is thus a field extension F/F_0 of degree $\frac{w_K}{2}$ over which the action of $\mathfrak{g}_F$ on T' is given by a quadratic character, and the argument proceeds as above with this choice of F. Notice in particular that $[F_0 : K(\mathfrak{f})]$ is smaller than $[F : K(\mathfrak{f})]$ in the previous case by a factor of $\frac{w_K}{2}$; since $[F : F_0] = \frac{w_K}{2}$, these factors cancel out and $[F : K(\mathfrak{f})]$ is unchanged. □

Theorem 4.5. *Suppose $\ell \mid \mathfrak{f}$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, and let $\mathfrak{p}_1, \mathfrak{p}_2$ be the two primes of $\mathcal{O}_K$ lying over ℓ. Let $a, b \in \mathbb{N}$ with $0 \leq a \leq b$ and $\ell^b \geq 4$.*
a) There is a number field $F \supset K(\mathfrak{f})$ with

$$[F : K(\mathfrak{f})] = \frac{\ell^{a+b-1}(\ell - 1)}{2}$$

and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ such that $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$.
b) We may take F to be an extension of $K^{\mathfrak{p}_2^b}K(\ell^a\mathfrak{f})$ of degree $\frac{w_K}{2}$.

Proof. Let $\iota : E \to E'$ be the canonical $K(\mathfrak{f})$-rational cyclic $\mathfrak{f}$-isogeny to an $\mathcal{O}_K$-CM elliptic curve E'. We put $T' \coloneqq E'[\mathfrak{p}_1^a\mathfrak{p}_2^b]$ and $T \coloneqq \iota^\vee(T')$. Let us first assume that $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, so $w_K = 2$.
Case 1: Suppose $a = 0$. In this case, by Theorem 3.1 the map $\iota^\vee : T' \to T$ is an isomorphism of $\mathfrak{g}_F$-modules, so after twisting E by a unique quadratic character ϵ we get an elliptic curve $E_{/F}$ with $T \cong \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F)$, and combining with Proposition 4.2 we get $w[F : K] = \ell^{b-1}(\ell - 1)$ and $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^b\mathbb{Z}$, completing the proof in this case.
Case 2: Suppose $a \geq 1$, and let $F_0 \coloneqq K(\mathfrak{f})K^{\mathfrak{p}_2^b}$. By Case 1 there is an $\mathcal{O}$-CM elliptic curve $E_{/F_0}$ with an F_0-rational point of order ℓ^b. By [BC, Thm. 4.1], after base extension to $K^{\mathfrak{p}_2^b}K(\ell^a\mathfrak{f})$ the mod ℓ^a Galois representation is given by scalar matrices, but since we also have a rational point of order ℓ^b, the mod ℓ^a Galois representation is trivial. Since $[K(\ell^a\mathfrak{f}) : K(\mathfrak{f})] = \ell^a$ we must have

$$2[K^{\mathfrak{p}_2^b}K(\ell^a\mathfrak{f}) : K(\mathfrak{f})] \leq \ell^{a+b-1}(\ell - 1).$$

By Proposition 4.2 we must have

$$[K^{\mathfrak{p}_2^b}K(\ell^a\mathfrak{f}) : K(\mathfrak{f})] = \frac{\ell^{a+b-1}(\ell - 1)}{2}.$$

Taking $F = K^{\mathfrak{p}_2^b}K(\ell^a\mathfrak{f})$ completes the proof in this case.
If $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ then we modify the above argument as in the proof of Theorem 4.4: namely we make an extension of $K^{\mathfrak{p}_2^b}$ of degree $\frac{w_K}{2}$ so as to ensure that that Galois action on T' is given by a *quadratic* character. Once again, the degree comes out the same. □

Theorem 4.6. *Suppose $\left(\frac{\Delta_K}{\ell}\right) = 0$. Let $c \coloneqq \mathrm{ord}_\ell(\mathfrak{f})$. Let $a, b \in \mathbb{N}$ with $a \leq b$ and $\ell^b \geq 4$.*
a) Suppose $b \leq 2c + 1$. Then there is a number field $F \supset K(\mathfrak{f})$ with

$$[F : K(\mathfrak{f})] = \frac{\ell^{a+b-1}(\ell - 1)}{w}$$

and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ such that $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$.
b) Suppose $b > 2c + 1$. Then:
(i) If for a number field $F \supset K(\mathfrak{f})$ we have $\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F)$, then $a \geq b - 2c - 1$.
(ii) If $a \geq b - 2c - 1$, there is a number field $F \supset K(\mathfrak{f})$ with $[F : K(\mathfrak{f})] = \frac{\ell^{a+b-1}(\ell-1)}{w}$ and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ with $E(F)[\ell^\infty] = \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$.

Proof. Let $\mathfrak{p}$ be the unique prime of $\mathcal{O}_K$ lying over ℓ.
First suppose that $\mathfrak{f} = 1$, so $c = 0$. In this case, for any number field $F \supset K^{(1)}$ and any $\mathcal{O}_K$-CM elliptic curve $E_{/F}$, the subgroup $E(F)[\ell^\infty]$ is an $\mathcal{O}_K$-submodule of $E(F)$ and thus is isomorphic to $E[\mathfrak{p}^d]$ for some $d \in \mathbb{N}$. By the First Main Theorem of Complex Multiplication, we have

$$K^{(1)}(\mathfrak{h}(E[\mathfrak{p}^d])) = K^{\mathfrak{p}^d},$$

and by [BC, Thm. 1.1, Cor. 1.4] there is an $\mathcal{O}_K$-CM elliptic curve $E_{/K^{\mathfrak{p}^d}}$ with $E[\mathfrak{p}^d] \subset E(K^{\mathfrak{p}^d})$, so

$$\frac{\ell^{d-1}(\ell-1)}{w} = [K^{\mathfrak{p}^d} : K^{(1)}].$$

Moreover, as recalled above, we have

$$E[\mathfrak{p}^d] \cong \mathbb{Z}/\ell^{\lceil \frac{d}{2} \rceil}\mathbb{Z} \times \mathbb{Z}/\ell^{\lfloor \frac{d}{2} \rfloor}\mathbb{Z},$$

which implies that if $a \leq b$ are the natural numbers such that $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$, then either $a = b-1$ or $a = b$. If $a = b-1$ then $d = 2a+1$, while if $a = b$ then $d = 2a$. Either way we have

$$\frac{\ell^{a+b-1}(\ell-1)}{w} = \frac{\ell^{d-1}(\ell-1)}{w} = [K^{\mathfrak{p}^d} : K^{(1)}],$$

completing the result in this case. Henceforth we suppose that $\mathfrak{f} > 1$, so $w = 2$.

a) Suppose $b \leq 2c+1$. We claim that there is an $\mathcal{O}$-CM elliptic curve $E_{/K(\mathfrak{f})}$ with a $K(\mathfrak{f})$-rationally cyclic ℓ^b-isogeny: by [BC, Thm. 6.15], for this we must show that Δ is a square in $\mathbb{Z}/4\ell^b\mathbb{Z}$. First suppose $\ell > 2$: then Δ is a square in $\mathbb{Z}/4\ell^b\mathbb{Z}$ iff Δ is a square in $\mathbb{Z}/\ell^b\mathbb{Z}$, and since $\ell \mid \Delta_K$ and $\ell^c \mid \mathfrak{f}$, $\ell^b \mid \ell^{2c+1} \mid \mathfrak{f}^2\Delta_K = \Delta$. Now suppose $\ell = 2$. Then $4 \mid \Delta_K$, so $\Delta_K \equiv 0, 4 \pmod 8$. Either way, there is $x \in \mathbb{Z}$ such that $\Delta_K \equiv x^2 \pmod{2^3}$. Since $\mathrm{ord}_2(\mathfrak{f}) = c$, it follows that

$$\Delta = \mathfrak{f}^2\Delta_K \equiv (\mathfrak{f}x)^2 \pmod{2^{2c+3}}$$

so Δ is a square modulo $4 \cdot 2^b$. By [BCS17, Thm. 5.5], we get a point of order ℓ^b on some $\mathcal{O}$-CM elliptic curve $E_{/F_0}$ with $[F_0 : K(\mathfrak{f})] = \frac{\ell^{b-1}(\ell-1)}{2}$. By [CP15, Thm. 7] and its proof, there is an extension F/F_0 with $[F : F_0] \mid \ell^a$ such that $E_{/F}$ has full ℓ^a-torsion. Thus

$$\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F)[\ell^\infty]$$

and by Proposition 4.2 we must have equality.

b) Suppose $b > 2c+1$, let $F \supset K$, and suppose $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$. Let $\iota : E \to E'$ be the usual canonical isogeny to an $\mathcal{O}_K$-CM elliptic curve. If $E(F)$ has a point of order ℓ^b then $E'(F)$ has a point of order ℓ^{b-c} and thus there is a subgroup $T' \subset E'(F)$ with $T' \cong \mathbb{Z}/\ell^{b-c-1}\mathbb{Z} \times \mathbb{Z}/\ell^{b-c}\mathbb{Z}$. Let $T = \iota^\vee(T')$, and write $T \cong \mathbb{Z}/\ell^A\mathbb{Z} \times \mathbb{Z}/\ell^B\mathbb{Z}$ with $0 \leq A \leq B$. Since $\#T \geq \frac{\#T'}{\ell^c}$ and $B \leq b-c$, we must have $A \geq b-c-1-c = b-2c-1$, so $a \geq A \geq b-2c-1$. Now Proposition 4.2 implies

$$\ell^{2b-2c-2}(\ell-1) \mid 2[F : K(\mathfrak{f})].$$

Finally, as above there is a field extension $F_0/K(\mathfrak{f})$ of degree $\frac{\ell^{2c}(\ell-1)}{2}$ and an $\mathcal{O}$-CM elliptic curve $E_{/F_0}$ with an F_0-rational point of order ℓ^{2c+1}. In general, if $E_{/F}$ is an elliptic curve defined over a number field and $P \in E(F)$ has order ℓ^n, let $\tilde{P} \in E[\mathrm{tors}]$ be such that $\ell\tilde{P} = P$. Then for all $\sigma \in \mathfrak{g}_F$ we have

$$\ell(\sigma\tilde{P}) = \sigma(\ell\tilde{P}) = \sigma P = P,$$

so the $\mathfrak{g}_F$-orbit on $\tilde{P}$ is contained in $\{Q \in E[\mathrm{tors}] \mid \ell Q = P\} = \tilde{P} + E[\ell]$, so has size at most ℓ^2. It follows that there is a "lift" of P to a point of order ℓ^b in a field extension F_1/F_0 with $[F_1 : F_0] \leq \ell^{2(b-2c-1)}$, hence $[F_1 : K(\mathfrak{f})] \leq \frac{\ell^{2b-2c-2}(\ell-1)}{2}$. As above, this forces $\mathbb{Z}/\ell^{b-2c-1}\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F_1)[\ell^\infty]$, and then Proposition 4.2 forces

$$[F_1 : K(\mathfrak{f})] = \frac{\ell^{2b-2c-2}(\ell-1)}{2}$$

and

$$E(F_1)[\ell^\infty] \cong \mathbb{Z}/\ell^{2b-2c-1}\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}.$$

Finally, suppose $b-2c-1 \leq a \leq b$. By [CP15, Thm. 7] there is a field extension F/F_1 of degree dividing $\ell^{a-b+2c+1}$ over which E has full ℓ^a-torsion. Thus

$$[F : K(\mathfrak{f})] \mid \frac{\ell^{a-b+2c+1+2b-2c-2}(\ell-1)}{2} = \frac{\ell^{a+b-1}(\ell-1)}{2}$$

and

$$\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F)[\ell^\infty].$$

Once again, by Proposition 4.2 the degree divisibility and the group inclusion are each equalities. □

Theorem 4.7. *Suppose $\ell \mid \mathfrak{f}$ and $\left(\frac{\Delta_K}{\ell}\right) = -1$. Let $a, b \in \mathbb{N}$ with $a \leq b$ and $\ell^b \geq 4$.*
a) Suppose $b \leq 2c$. Then there is a number field $F \supset K(\mathfrak{f})$ with

$$[F : K(\mathfrak{f})] = \frac{\ell^{a+b-1}(\ell-1)}{2}$$

and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ such that $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$.
b) Suppose $b > 2c$. Then:
(i) If for a number field $F \supset K(\mathfrak{f})$ we have $\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(F)$, then $a \geq b - 2c$.
(ii) If $a \geq b - 2c$, there is a number field $F \supset K(\mathfrak{f})$ with $[F : K(\mathfrak{f})] = \frac{\ell^{a+b-1}(\ell-1)}{2}$ and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ with $E(F)[\ell^\infty] = \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$.

Proof. a) Suppose that $b \leq 2c$. We will show that there is an $\mathcal{O}$-CM elliptic curve $E_{/K(\mathfrak{f})}$ with an $K(\mathfrak{f})$-rational cyclic ℓ^b-isogeny. Given this, the remainder of the proof of part a) is identical to the proof of part a) of Theorem 4.6. First suppose that $\ell > 2$. Then $\Delta = \mathfrak{f}^2\Delta_K$ is divisible by ℓ^{2c} hence is a square modulo ℓ^b hence also modulo $4\ell^b$, so Theorem 2.4 gives the ℓ^b-isogeny. Now suppose that $\ell = 2$. Since 2 is inert in K, we have $\Delta_K \equiv 1 \pmod 4$; since $\ell^c \mid \mathfrak{f}$, we have

$$\Delta = \mathfrak{f}^2\Delta_K \equiv \mathfrak{f}^2 \pmod{4\ell^{2c}}.$$

Thus Δ is a square modulo $4\ell^b$, so Theorem 2.4 gives the ℓ^b-isogeny, completing the proof of part a).
b) Suppose $b > 2c$, let $F \supset K$, and suppose $E(F)[\ell^\infty] \cong \mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z}$. Let $\iota : E \to E'$ be the usual canonical isogeny to an $\mathcal{O}_K$-CM elliptic curve. If $E(F)$ has a point of order ℓ^b then $E'(F)$ has a point of order ℓ^{b-c} and thus – since $\left(\frac{\Delta_K}{\ell}\right) = -1$ – we have $E'[\ell^{b-c}] \subset E'(F)$. As in the proof of part b) of Theorem 4.6, it follows that $E[\ell^{b-2c}] \subset \iota^\vee(E'(F))$, so $a \geq b - 2c$. Now Proposition 4.2 implies

$$\ell^{2b-2c-1}(\ell-1) \mid 2[F : K(\mathfrak{f})].$$

The argument now proceeds exactly as in the proof of part b) of Theorem 4.6. □

4.3. **Compiling across prime powers.**

Let $\mathcal{O}$ be an imaginary quadratic order, and let $M \mid N$ be positive integers. By an **(M,N)-pair** we mean a pair (P, Q) with $P \in \mathcal{O}/N\mathcal{O}$ of order M and $Q \in \mathcal{O}/N\mathcal{O}$ of order N such that the $\mathbb{Z}$-module generated by P and Q is isomorphic to $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. We denote by $\widetilde{T}(\mathcal{O}, M, N)$ the least size of a $C_N(\mathcal{O})$-orbit on the set of (M, N)-pairs. The Cartan subgroup $C_N(\mathcal{O}) = (\mathcal{O}/N\mathcal{O})^\times$ has a natural action on (M, N) pairs:

$$g \cdot (P, Q) = (gP, gQ).$$

A **reduced (M,N)-pair** is an orbit of an (M, N)-pair (P, Q) under the image of $\mathcal{O}^\times$ in $\mathcal{O}/N\mathcal{O}$. Unless $\Delta = -4, -3$, this simply identifies (P, Q) with $(-P, -Q)$. The reduced Cartan subgroup $\overline{C_N(\mathcal{O})} = C_N(\mathcal{O})/q_N(\mathcal{O}^\times)$ has a natural action on the set of reduced (M, N)-pairs. We denote by $T(\mathcal{O}, M, N)$ the least size of a $\overline{C_N(\mathcal{O})}$-orbit on the set of reduced (M, N)-pairs.

Lemma 4.8. *For all $N \in \mathbb{Z}^+$, we have $\widetilde{T}(\mathcal{O}, N, N) = \#C_N(\mathcal{O})$.*

Proof. The action of $C_N(\mathcal{O})$ on (N, N)-pairs is free: if $gP = P$ and $gQ = Q$ then g fixes all of $\mathcal{O}/N\mathcal{O}$ and thus $g = 1$. It follows that *every* $C_N(\mathcal{O})$-orbit on the set of (N, N)-pairs has size $\#C_N(\mathcal{O})$. □

The following result explains the relevance of the latter definition to the problem at hand.

Proposition 4.9. *For an imaginary quadratic order $\mathcal{O}$, positive integers $M \mid N$, and a positive integer d, the following are equivalent:*
(i) There is a field $F \supset K(\mathfrak{f})$ with $[F : K(\mathfrak{f})] = d$, an $\mathcal{O}$-CM elliptic curve $E_{/F}$ and an injection

$$\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)[\text{tors}].$$

(ii) The integer d is divisible by the size of some $\overline{C_N(\mathcal{O})}$-orbit on the set of reduced (M, N)-pairs.

Proof. This is a direct consequence of the surjectivity of the reduced Galois representation

$$\overline{\rho_N} : \mathfrak{g}_{K(\mathfrak{f})} \to \overline{C_N(\mathcal{O})}.$$

Indeed, it follows that for an (M,N)-pair $(P,Q) \in E(\overline{K(\mathfrak{f})})$, the size of the $\overline{C_N(\mathcal{O})}$-orbit on the reduced pair is the unique minimal degree of a field extension $F/K(\mathfrak{f})$ over which there exists a single character $\chi : \mathfrak{g}_F :\to \mathcal{O}^\times$ such that for all $\sigma \in \mathfrak{g}_F$ we have $\sigma(P) = \chi(\sigma)P$ and $\sigma(Q) = \chi(\sigma)Q$, and thus (P,Q) both become rational on some twist of $E_{/F}$. □

Thus we wish to find, for all $\mathcal{O}$ and $M \mid N$, the set of all multiples of sizes of $\overline{C_N(\mathcal{O})}$-orbits on reduced (M,N)-pairs. Let $T(\mathcal{O},M,N)$ be the least size of a $\overline{C_N(\mathcal{O})}$-orbit on the set of reduced (M,N)-pairs. The results of the previous section determine $T(\mathcal{O},M,N)$ when $N \geq 4$ is a prime power and show that in this case every $\overline{C_N(\mathcal{O})}$-orbit has size a multiple of $T(\mathcal{O},M,N)$. We will show that this is true in the general case, with the consequence that condition (ii) in Proposition 4.9 will simplify to: d is a multiple of $T(\mathcal{O},M,N)$.

Although Proposition 4.9 gives us the answer in terms of orbits on reduced (M,N)-pairs, it is more natural to work with orbits on (M,N)-pairs, especially with regard to the process of compiling across prime powers. The following result allows us to pass back and forth between them.

Lemma 4.10. *Let $N \geq 4$ and let $M \mid N$. Let (P,Q) be an (M,N)-pair in $\mathcal{O}/N\mathcal{O}$, and let $\overline{(P,Q)}$ be the corresponding reduced (M,N)-pair.*
a) The size of the $C_N(\mathcal{O})$-orbit on (P,Q) is w times the size of the $\overline{C_N(\mathcal{O})}$-orbit on $\overline{(P,Q)}$.
It follows that:
b) $\widetilde{T}(\mathcal{O},M,N) = wT(\mathcal{O},M,N)$.
c) Every $C_N(\mathcal{O})$-orbit on an (M,N)-pair has size a multiple of $\widetilde{T}(\mathcal{O},M,N)$ iff every $\overline{C_N(\mathcal{O})}$-orbit on a reduced (M,N)-pair has size a multiple of $T(\mathcal{O},M,N)$.

Proof. a) The assertion is equivalent to: $\mathcal{O}^\times$ acts freely on (M,N)-pairs.[5] When $M = 1$, this follows from [BC, Lemma 7.6]. The general case follows.
b), c) These follow immediately. □

Proposition 4.11. *Let $M \mid N$ be positive integers. Write*

$$M = \ell_1^{a_1} \cdots \ell_r^{a_r},\ N = \ell_1^{b_1} \cdots \ell_r^{b_r}.$$

Let (P,Q) be an (M,N)-pair in $\mathcal{O}/N\mathcal{O}$. For $1 \leq i \leq r$, let P_i (resp. Q_i) be the image of P (resp. Q) in $\mathcal{O}/\ell_i^b\mathcal{O}$. Then:
a) For all $1 \leq i \leq r$, we have that (P_i,Q_i) is an $(\ell_i^{a_i},\ell_i^{b_i})$-pair in $\mathcal{O}/\ell_i^{b_i}\mathcal{O}$.
b) The $C_N(\mathcal{O})$-orbit on the pair (P,Q) is isomorphic as a $C_N(\mathcal{O})$-set to the direct product of the $C_{\ell_i^{b_i}}$-orbits on the pairs (P_i,Q_i).

Proof. This is an immediate consequence of the canonical CRT decompositions

$$C_N(\mathcal{O}) = \prod_{i=1}^r C_{\ell_i^{b_i}}(\mathcal{O}),\ \mathcal{O}/N\mathcal{O} = \prod_{i=1}^r \mathcal{O}/\ell_i^{b_i}(\mathcal{O}).$$ □

5. A generalization of Kwon's theorem

5.1. **Kwon's theorem.** For an imaginary quadratic order $\mathcal{O} = \mathcal{O}(\mathfrak{f})$ and a positive integer N, we consider the following condition:

• $I(\mathcal{O},N)$: there is a $\mathbb{Q}(\mathfrak{f})$-rational cyclic N-isogeny $\varphi : E \to E'$ between elliptic curves with $\operatorname{End} E = \mathcal{O}$.

[5]When $\Delta < -4$, we have $\mathcal{O}^\times = \{\pm 1\}$, and since $N > 2$ we have $-Q \neq Q$, so $-(P,Q) \neq (P,Q)$ and this is clear. So most of the fight is over the cases $\Delta \in \{-4,-3\}$.

Theorem 5.1. *(Kwon* [Kw99, Cor. 4.2]*) Let $\mathcal{O} = \mathcal{O}(\mathfrak{f})$ be an order in an imaginary quadratic field $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$. Let $N \in \mathbb{Z}^+$.*

(1) *Suppose one of the following holds:*
   (a) *$2 \mid \mathfrak{f}$ and 2 is ramified in K or*
   (b) *$4 \mid \mathfrak{f}$.*
   Then $I(\mathcal{O}, N)$ holds iff $N \mid \frac{\Delta}{4} = \frac{\mathfrak{f}^2 \Delta_K}{4}$.

(2) *Suppose one of the following holds:*
   (a) *$\mathfrak{f} \equiv 2 \pmod 4$ and 2 is unramified in K or*
   (b) *$\mathfrak{f}$ is odd and $\left(\frac{\Delta_K}{2}\right) \neq -1$.*
   Then $I(\mathcal{O}, N)$ holds iff either N or $\frac{N}{2}$ is an odd integer dividing $\Delta = \mathfrak{f}^2 \Delta_K$.

(3) *Suppose $2 \nmid \mathfrak{f}$ and $\left(\frac{\Delta_K}{2}\right) = -1$. Then $I(\mathcal{O}, N)$ holds iff $N \mid \Delta = \mathfrak{f}^2 \Delta_K$.*

Remark 5.2. *Let $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$.*

Suppose that $\mathfrak{f} > 1$. Then it follows from Theorem 5.3 and Proposition 5.8 that if $I(\mathcal{O}, N)$ holds then N must satisfy the same numerical conditions as in Theorem 5.1. The arguments of [Kw99, pp. 954-955] *hold verbatim to show that if N satisfies these numerical conditions then $I(\mathcal{O}, N)$ holds. Thus in fact Theorem 5.1 holds verbatim for every imaginary quadratic order of discriminant $\Delta < -4$.*

In Corollary 5.11 we will complete Kwon's theorem by determining all $N \in \mathbb{Z}^+$ such that $I(\mathcal{O}, N)$ holds when $\Delta = -4$ or $\Delta = -3$.

5.2. **Statement of the generalization of Kwon's theorem.** Half of Theorem 5.1 gives necessary conditions on N for the existence of a $\mathbb{Q}(\mathfrak{f})$-rational cyclic N-isogeny on an $\mathcal{O}$-CM elliptic curve. The following result generalizes this half of the result by showing that the conclusions continue to hold over a more general field.

Theorem 5.3. *Let $N, \mathfrak{f} \in \mathbb{Z}^+$. Let $F/\mathbb{Q}(\mathfrak{f})$ be a number field. We suppose that there is an $\mathcal{O}(\mathfrak{f})$-CM elliptic curve E/F admitting an F-rational cyclic N-isogeny. We also suppose:*
• *F does not contain K, and for all primes $\ell \mid N$, F does not contain $\mathbb{Q}(\ell\mathfrak{f})$.*
a) There is a positive integer $d \mid \gcd(\mathfrak{f}, N)$ and a primitive, proper, real $\mathcal{O}(\frac{\mathfrak{f}}{d})$-ideal of index $\frac{N}{d}$.
b) It follows that $N \mid \Delta = \mathfrak{f}^2 \Delta_K$. Moreover:
(i) Suppose that $16 \mid \Delta$. Then $N \mid \frac{\Delta}{4}$.
(ii) Suppose $\mathfrak{f} \equiv 2 \pmod 4$ and 2 is unramified in K. Then either N or $\frac{N}{2}$ is an odd divisor of Δ.
(iii) Suppose $2 \nmid \mathfrak{f}$ and 2 is ramified in K. Then either N or $\frac{N}{2}$ is an odd divisor of Δ.

Remark 5.4. *The hypotheses on F are natural. On the one hand,* [BC, Thm. 6.18] *gives the classification of $N \in \mathbb{Z}^+$ such that some $\mathcal{O}$-CM elliptic curve admits a $K(\mathfrak{f})$-rational cyclic N-isogeny. On the other: suppose that F is a number field containing $\mathbb{Q}(N\mathfrak{f})$. Let $\tilde{\mathcal{O}}$ be the order in K of conductor $N\mathfrak{f}$. Then there is a $\tilde{\mathcal{O}}$-CM elliptic curve $\tilde{E}_{/F}$ and a canonical F-rational cyclic N-isogeny $\iota_{N\mathfrak{f},\mathfrak{f}} : \tilde{E} \to E$ with $\operatorname{End} E = \mathcal{O}$, and thus $\iota_{N\mathfrak{f},\mathfrak{f}}^\vee : E \to \tilde{E}$ is a cyclic N-isogeny.*

5.3. **A preliminary lemma.**

Lemma 5.5. *Let $N \in \mathbb{Z}^+$.*
a) Let $\varphi : E \to E'$ be a degree N isogeny of K-CM elliptic curves, with $\operatorname{End} E$ an order of conductor $\mathfrak{f}$ and $\operatorname{End} E'$ an order of conductor $\mathfrak{f}'$. Then

$$\mathfrak{f} \mid N\mathfrak{f}', \ \mathfrak{f}' \mid N\mathfrak{f}.$$

b) Let $\mathcal{O}$ be an imaginary quadratic order of conductor $\mathfrak{f}$, let F be a number field that does not contain $\mathbb{Q}(\ell\mathfrak{f})$ for any $\ell \mid N$, let $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve, and let $\varphi : E \to E'$ be an F-rational N-isogeny. Then the conductor $\mathfrak{f}'$ of $\operatorname{End} E'$ divides $\mathfrak{f}$.

Proof. Every N-isogeny factors as a product of ℓ-isogenies, so is enough to treat the case $N = \ell$. Over $\mathbb{C}$ we may view φ as $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ where $\Lambda' \supset \Lambda$ and $\Lambda'/\Lambda \cong \mathbb{Z}/\ell\mathbb{Z}$. Let $\alpha \in \mathcal{O}$. For $\lambda' \in \Lambda'$ we have

$$(\ell\alpha)\lambda' = \alpha(\ell\lambda'),$$

but $\ell\lambda' \in \Lambda$, so

$$\alpha(\ell\lambda') \in \alpha\Lambda \subset \Lambda \subset \Lambda'.$$

Thus $\ell\alpha \in (\Lambda' : \Lambda') = \mathcal{O}'$. Applying this with $\alpha = \mathfrak{f}\tau_K$, we get that $\mathfrak{f}\ell\tau_K \in \mathcal{O}'$, so $\mathfrak{f}' \mid \ell\mathfrak{f}$. The same argument applied to the dual isogeny $\varphi^\vee : E' \to E$ shows that $\mathfrak{f} \mid \ell\mathfrak{f}'$ and thus $\frac{\mathfrak{f}}{\mathfrak{f}'} \in \{\ell^{-1}, 1, \ell\}$.
b) By part a), if $\mathfrak{f}'$ does not divide $\mathfrak{f}$, then there is some prime $\ell \mid N$ such that $\mathrm{ord}_\ell(\mathfrak{f}') > \mathrm{ord}_\ell(\mathfrak{f})$; seeking a contradiction, we fix such a prime. We may factor φ over F as $\varphi_2 \circ \varphi_1$, where $\deg \varphi_1 = \ell^{\mathrm{ord}_\ell(N)}$ and $\deg \varphi_2 = \frac{N}{\ell^{\mathrm{ord}_\ell(N)}}$. By part a), the ℓ-primary part of the conductor is unchanged under φ_2, so if $\mathfrak{f}_1$ is the conductor of $E/\ker\varphi_1$ then we must have $\mathfrak{f}\ell \mid \mathfrak{f}_1$ and thus $F \supset \mathbb{Q}(\mathfrak{f}\ell)$, contradicting our hypothesis. □

5.4. **Classification of primitive, proper real ideals.**

Lemma 5.6. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $\Delta = \mathfrak{f}^2\Delta_K$.*
a) If there is a primitive, proper real $\mathcal{O}$-ideal of index N, then $N \mid \Delta$.
b) Let $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. There is a primitive, proper real $\mathcal{O}$ ideal I such that $[\mathcal{O} : I] = N$ iff for all $1 \le i \le r$, there is a primitive, proper real $\mathcal{O}$ ideal I_i such that $[\mathcal{O} : I_i] = \ell_i^{a_i}$.
b) Let $\ell > 2$, and let $a \in \mathbb{N}$. There is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = \ell^a$ iff $a = \mathrm{ord}_\ell(\Delta)$.
c) Let $\ell = 2$, and let $a \in \mathbb{Z}^+$.
(i) Suppose $16 \mid \Delta$. Then there is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = 2^a$ iff $a = 2$ or $a = \mathrm{ord}_2(\Delta) - 2$.
(ii) Suppose $2 \mid \Delta$ and $16 \nmid \Delta$. Then there is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = 2^a$ iff $a = 1$.

Proof. a) See [Kw99, §3] or [BCS17, Cor. 3.8]. b) This is an easy primary decomposition argument. c) This is [Kw99, Prop. 3.1]. □

5.5. **Proof of Theorem 5.3.** a) Let F be a number field, let $E_{/F}$ be an $\mathcal{O} = \mathcal{O}(\mathfrak{f})$-CM elliptic curve, and let $\varphi : E \to E'$ be a cyclic N-isogeny. We assume that F contains neither K nor $\mathbb{Q}(\ell\mathfrak{f})$ for any $\ell \mid N$. By Lemma 5.5b), the conductor $\mathfrak{f}'$ of $\mathcal{O}' \coloneqq \mathrm{End}\, E'$ divides $\mathfrak{f}$. As above, we may factor φ as

$$E \overset{\iota_{\mathfrak{f},\mathfrak{f}'}}{\to} E'' \overset{\varphi'}{\to} E'.$$

Thus φ' is a cyclic $\frac{N}{\mathfrak{f}/\mathfrak{f}'}$-isogeny of $\mathcal{O}'$-CM elliptic curves, so $\ker\varphi' = E[\mathfrak{b}]$ for a primitive (since φ' is cyclic) proper $\mathcal{O}'$-ideal $\mathfrak{b}$. Let

$$\mathcal{K} \coloneqq \ker\varphi,\ \mathcal{K}'' \coloneqq \ker\iota_{\mathfrak{f},\mathfrak{f}'},\ \mathcal{K}' \coloneqq \ker\varphi'.$$

Since $\mathcal{K}$ and $\mathcal{K}''$ are both F-rational group schemes and

$$\mathcal{K}' = \mathcal{K}/\mathcal{K}'',$$

we have that $\mathcal{K}'$ is F-rational; equivalently, φ' is defined over F. Since F does not contain K, the F-rationality of $E[\mathfrak{b}]$ implies that $\mathfrak{b}$ is a real ideal, and $\#\mathcal{O}/\mathfrak{b} = \#E[\mathfrak{b}] = \frac{N}{\mathfrak{f}/\mathfrak{f}'}$.
b) Suppose that there is an $\mathcal{O} = \mathcal{O}(\mathfrak{f})$-CM elliptic curve E_F admitting an F-rational cyclic N-isogeny. By part a) there is there is some $\mathfrak{f}' \mid \gcd(\mathfrak{f}, N)$ such that $N = \frac{\mathfrak{f}}{\mathfrak{f}'} \cdot i$, where i is the index of a primitive, proper real $\mathcal{O}(\mathfrak{f}')$-ideal. By Lemma 5.6a) we have $i \mid \Delta(\mathcal{O}(\mathfrak{f}')) = \mathfrak{f}'^2\Delta_K$, so

$$N = \frac{\mathfrak{f}}{\mathfrak{f}'}i \mid \frac{\mathfrak{f}}{\mathfrak{f}'}\mathfrak{f}'^2\Delta_K = \mathfrak{f}\mathfrak{f}'\Delta_K \mid \mathfrak{f}^2\Delta_K. \tag{8}$$

• Suppose that $2 \mid \mathfrak{f}$ and $16 \mid \Delta$. We wish to show that $N \mid \frac{\mathfrak{f}^2\Delta_K}{4}$. In view of what we have already shown it is enough to show that if $N = 2^a$ then $a \le \mathrm{ord}_2(\mathfrak{f}^2\Delta_K) - 2$, and this follows easily from Lmma 5.6c).
• Suppose that $\mathfrak{f} \equiv 2 \pmod 4$ and 2 is unramified in K. We wish to show that if $2^a \mid N$ then $a \le 1$. This follows easily from Lemma 5.6.
• Suppose that $2 \nmid \mathfrak{f}$ and 2 ramifies in K. We wish to show that if $2^a \mid N$ then $a \le 1$. This follows easily from Lemma 5.6.

5.6. **Supplements to Kwon's theorem.** The hypotheses of Theorem 5.3 are never satisfied in the presence of "ring class field coincidences": namely, when $\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}(\ell\mathfrak{f})$ for some prime $\ell \mid N$. Using (6), one sees that the instances of $\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}(\ell\mathfrak{f})$ are precisely as follows:

(C1) If $\left(\frac{\Delta_K}{2}\right) = 1$ and $\mathfrak{f}$ is odd, then $\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}(2\mathfrak{f})$.
(C2) If $K = \mathbb{Q}(\sqrt{-1})$, then $\mathbb{Q}(1) = \mathbb{Q}(2)$.
(C3) If $K = \mathbb{Q}(\sqrt{-3})$, then $\mathbb{Q}(1) = \mathbb{Q}(2) = \mathbb{Q}(3)$.
In particular we must have $\ell \in \{2, 3\}$.

Concerning (C1):

Lemma 5.7. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $\Delta < -4$, and let $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve. For a positive integer N, if the image $\rho_N(\mathfrak{g}_F)$ of the mod N Galois representation on E consists only of scalar matrices, then $\mathbb{Q}(N\mathfrak{f}) \subset F$.*

Proof. This is really the observation that part of the proof of [BC, Thm. 4.1] goes through over $\mathbb{Q}(\mathfrak{f})$ rather than $K(\mathfrak{f})$, but for the convenience of the reader we will recap the argument.

There is a field embedding $F \hookrightarrow \mathbb{C}$ such that $E_{/\mathbb{C}} \cong \mathbb{C}/\mathcal{O}(\mathfrak{f})$. The map $z \mapsto Nz$ induces a cyclic N-isogeny $\varphi : \mathbb{C}/\mathcal{O}(\mathfrak{f}) \to \mathbb{C}/\mathcal{O}(N\mathfrak{f})$. Let $C = \ker\varphi = \langle P \rangle$ for some point $P \in E(\overline{F})$ of order N. Our assumption on $\mathfrak{g}_F$ implies that Galois acts by scaling P and thus C is F-rational. So $E \to E/C$ is an F-rational isogeny and $\operatorname{End} E/C = \mathcal{O}(N\mathfrak{f})$, so $\mathbb{Q}(N\mathfrak{f}) \subset F$. □

Proposition 5.8. *Let K be an imaginary quadratic field in which 2 splits. Let $\mathfrak{f}$ be an odd integer, and put $\mathcal{O} = \mathcal{O}(\mathfrak{f})$. Let F be a number field that does not contain K. The following are equivalent:*
(i) Every $\mathcal{O}$-CM elliptic curve defined over F admits an F-rational 4-isogeny.
(ii) There is an $\mathcal{O}$-CM elliptic curve defined over F admits an F-rational 4-isogeny.
(iii) The field F contains $\mathbb{Q}(4\mathfrak{f})$.

Proof. The hypotheses prevent K from being $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, so for any $\mathcal{O}$-CM elliptic curve E we have $\operatorname{Aut} E = \{\pm 1\}$, and thus the existence of rational isogenies is independent of the chosen F-rational model: (i) $\iff$ (ii).
(ii) $\implies$ (iii): Let $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve, and let $\varphi : E \to E'$ be an F-rational cyclic 4-isogeny. Seeking a contradiction, we suppose that F does not contain $\mathbb{Q}(4\mathfrak{f})$.

The isogeny φ factors as $E \xrightarrow{\iota} E'' \xrightarrow{\varphi'} E'$, where ι and φ' are both F-rational 2-isogenies, i.e., they are obtained by modding out by the subgroup generated by an F-rational point of order 2. By [BCS17, Thm. 4.2] E has an F-rational point P of order 2 and $F(E[2]) = K$, and thus P is the only order 2 element of $E(F)$. Because 2 splits in K and $2 \nmid \mathfrak{f}$, we have $2\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$ with $\overline{\mathfrak{p}_1} = \mathfrak{p}_2$, and the other two nontrivial points of $E[2]$ generate the subgroups $E[\mathfrak{p}_1]$ and $E[\mathfrak{p}_2]$. Let $\tilde{\mathcal{O}} = \mathcal{O}(2\mathfrak{f})$. It is easy to see that over $\mathbb{C}$ (hence over $\overline{\mathbb{Q}}$) there is a 2-isogeny $\iota_{2\mathfrak{f},\mathfrak{f}} : \tilde{E} \to E$ (for instance, we can embed $\mathbb{Q}(j(E)) \hookrightarrow \mathbb{C}$ such that $E_{/\mathbb{C}} \cong \mathbb{C}/\mathcal{O}$ and then the isogeny is $\mathbb{C}/\tilde{\mathcal{O}} \to \mathbb{C}/\mathcal{O}$), so it follows that if

$$\tilde{E} \coloneqq E/C,$$

then

$$\operatorname{End} \tilde{E} = \tilde{\mathcal{O}}.$$

Writing $\ker \iota^\vee = \langle Q \rangle$, we have that $Q \in \tilde{E}(F)$ has order 2. But $\tilde{E}(F)$ has no other rational point of order 2: if so, it would have full 2-torsion, hence $\mathbb{Q}(4\mathfrak{f}) \subset F$ by Lemma 5.7, a contradiction. It follows that, up to an isomorphism on the target, $\varphi' = \iota_{2\mathfrak{f},\mathfrak{f}}$, but then $\varphi = \iota_{2\mathfrak{f},\mathfrak{f}} \circ \iota_{2\mathfrak{f},\mathfrak{f}}^\vee = [2]$ is not cyclic.
(iii) $\implies$ (ii): If F contains $\mathbb{Q}(4\mathfrak{f})$ then there is an $\mathcal{O}(4\mathfrak{f})$-CM elliptic curve $\tilde{E}_{/F}$ and a cyclic 4-isogeny $\iota_{4\mathfrak{f},\mathfrak{f}}$ with target an $\mathcal{O}(\mathfrak{f})$-CM elliptic curve. □

Concerning (C2):

Proposition 5.9. *Let $K = \mathbb{Q}(\sqrt{-1})$, and let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of K, so $\Delta = \Delta_K = -4$, $\mathfrak{f} = 1$ and $\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}$. For $a \in \mathbb{Z}^+$, we have that $I(\mathcal{O}, 2^a)$ holds iff $a \leq 2$.*

Proof. Step 1: We show that there is an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}}$ admitting a $\mathbb{Q}$-rational cyclic 4-isogeny. Since $\varphi(4)/2 = 1$, by [BCS17, Thm. 5.5], this holds iff there is an $\mathcal{O}$-CM elliptic curve such that $E(\mathbb{Q})$ has an element of order 4. That the latter holds is well known [Ol74, p. 196]. However, we will give a "principled" proof. Namely, let $\mathcal{O}'$ be the order of conductor 2 in K. Since $\mathbb{Q}(2) = \mathbb{Q}(1) = \mathbb{Q}$, there is an $\mathcal{O}'$-CM elliptic curve $E'_{/\mathbb{Q}}$ and thus a $\mathbb{Q}$-rational 2-isogeny $\iota : E' \to E$ where $\operatorname{End} E = \mathcal{O}$. Let $\mathfrak{p}$ be the unique prime ideal of norm 2 in $\mathcal{O}$; by uniqueness, $\mathfrak{p}$ is real, so we have a $\mathbb{Q}$-rational 2-isogeny $\psi : E \to E/E[\mathfrak{p}]$. Since $\mathfrak{p}$ is a proper $\mathcal{O}$-ideal, we have $\operatorname{End}(E/E[\mathfrak{p}]) = \mathcal{O}$. Let $\varphi = (\psi \circ \iota)^\vee : E/E[\mathfrak{p}] \to E'$. Then φ is a $\mathbb{Q}$-rational 4-isogeny; if it were not cyclic, then it would be (up to an isomorphism on the target) [2], but this is impossible as $\operatorname{End} E/E[\mathfrak{p}] \neq \operatorname{End} E'$.
Step 2: By [BC, Thm. 6.18], no $\mathcal{O}$-CM elliptic curve has a K-rational cyclic 8-isogeny, so certainly no $\mathcal{O}$-CM elliptic curve has a $\mathbb{Q}$-rational cyclic 8-isogeny. □

Concerning (C3):

Proposition 5.10. *Let $K = \mathbb{Q}(\sqrt{-3})$, and let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers of K, so $\Delta = \Delta_K = -3$, $\mathfrak{f} = 1$ and $\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}$.*
a) For $a \in \mathbb{Z}^+$, we have that $I(\mathcal{O}, 2^a)$ holds iff $a = 1$.
b) For $a \in \mathbb{Z}^+$, we have that $I(\mathcal{O}, 3^a)$ holds iff $a \leq 2$.

Proof. a) Let $\mathcal{O}'$ be the order in K of conductor 2. Because $\mathbb{Q}(2) = \mathbb{Q}(1)$, there is an $\mathcal{O}'$-CM elliptic curve $E'_{/\mathbb{Q}}$ and thus a canonical $\mathbb{Q}$-rational 2-isogeny $\iota : E' \to E$ with $\operatorname{End} E = \mathcal{O}$. Then $\iota^\vee : E \to E'$ is a $\mathbb{Q}$-rational cyclic 2-isogeny. By [BC, Thm. 6.18], no $\mathcal{O}$-CM elliptic curve has even a K-rational cyclic 4-isogeny. (Alternately: if there were an $\mathcal{O}$-CM elliptic curve with a $\mathbb{Q}$-rational cyclic 4-isogeny, then since $\frac{\varphi(4)}{2} = 1$, by [BCS17, Thm. 5.5] there would be an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}}$ with a $\mathbb{Q}$-rational point of order 4, which is not the case: see [Ol74, p. 196], [Ao95, Cor. 9.4] or [BCS17, Thm. 5.1c)].)
b) Step 1: We construct a $\mathbb{Q}$-rational cyclic 9-isogeny $\varphi : E \to E'$ with $\operatorname{End} E = \mathcal{O}$ in exactly the same way as in the proof of Proposition 5.9: $\mathbb{Q}(3) = \mathbb{Q}(1) = \mathbb{Q}$, and there is a unique ideal $\mathfrak{p}$ of $\mathcal{O}$ of norm 3.
Step 2: By [BC, Thm. 6.18], no $\mathcal{O}$-CM elliptic curve has a K-rational cyclic 27-isogeny, so certainly no $\mathcal{O}$-CM elliptic curve has a $\mathbb{Q}$-rational cyclic 27-isogeny. □

The following result completes Kwon's theorem by determining all $N \in \mathbb{Z}^+$ such that $I(\mathcal{O}, N)$ holds for the orders $\mathcal{O}$ of discriminants -3 and -4.

Corollary 5.11.
a) Let $\mathcal{O}$ be the imaginary quadratic order of discriminant -4. Then $I(\mathcal{O}, N)$ holds iff $N \in \{1, 2, 4\}$.
b) Let $\mathcal{O}$ be the imginary quadratic order of discriminant -3. Then $I(\mathcal{O}, N)$ holds iff $N \in \{1, 2, 3, 6, 9\}$.

Proof. a) By Theorem 5.3, $I(\mathcal{O}, \ell)$ does not hold for any odd prime ℓ. The result now follows from Proposition 5.9.
b) By Theorem 5.3, $I(\mathcal{O}, \ell)$ does not hold for any prime $\ell \geq 5$, so by Proposition 5.10, if $I(\mathcal{O}, N)$ holds then $N \in \{1, 2, 3, 6, 9, 18\}$. Proposition 5.10 also shows that $I(\mathcal{O}, N)$ holds for $N \in \{1, 2, 3, 9\}$. In particular there is an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}}$ admitting a $\mathbb{Q}$-rational 2-isogeny; let C_2 be its kernel. Let $\mathfrak{p}$ be the unique $\mathcal{O}$-ideal of norm 3. Then $E \to E/(C_2 \times E[\mathfrak{p}])$ is a $\mathbb{Q}$-rational 6-isogeny, so $I(\mathcal{O}, 6)$ holds. Finally, by [BC, Thm. 6.18], no $\mathcal{O}$-CM elliptic curve has even a K-rational cyclic 18-isogeny. □

Remark 5.12. *a) As seen in the proof of Proposition 5.8, for an order $\mathcal{O}$ of discriminant $\Delta < -4$, whether an $\mathcal{O}$-CM elliptic curve $E_{/F}$ admits an F-rational cyclic N-isogeny is independent of the F-model, so if $\gcd(M, N) = 1$, then $I(\mathcal{O}, MN)$ holds iff $I(\mathcal{O}, M)$ holds and $I(\mathcal{O}, N)$ holds. However Corollary 5.11 shows that when $\Delta = -3$, $I(\mathcal{O}, 2)$ holds and $I(\mathcal{O}, 9)$ holds but $I(\mathcal{O}, 18)$ does not hold.*
b) It would be interesting to know whether Proposition 5.9 continues to hold over any number field F containing neither K nor $\mathbb{Q}(4)$, and similarly for Proposition 5.10.
c) Combining Proposition 5.10 with [BCS17, Thm. 5.5]*, we find that if $\mathcal{O}$ is the imaginary quadratic order of discriminant -3, there is an $\mathcal{O}$-CM elliptic curve defined over a cubic number field F with an F-rational point of order 9. In fact* [BCS17, Table II] *gives an explicit such curve: we may take*

$F = \mathbb{Q}[b]/(b^3 - 15b^2 - 9b - 1)$,

$$E_{/F} : y^2 + (1 - (\frac{b^2}{4} + \frac{5b}{2} + \frac{1}{4}))xy - (\frac{b^2}{4} + \frac{5b}{2} + \frac{1}{4})y = x^3 - bx^2, P = (0, 0).$$

6. Least degrees of CM points on $X_1(\ell^a)_{/\mathbb{Q}}$

6.1. Inert case.

Theorem 6.1. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant Δ, let ℓ be a prime that is inert in $\mathcal{O}$, and let $b \in \mathbb{Z}^+$. Then:*

(1) *Suppose $\ell^b \geq 3$.*
   (a) *If $E_{/L}$ is an $\mathcal{O}$-CM elliptic curve defined over a number field such that $E(L)$ has a point of order ℓ^b, then $\frac{\ell^{2b-2}(\ell^2-1)}{w} \mid [L : \mathbb{Q}(\mathfrak{f})]$.*
   (b) *Conversely, there is an extension $L \supset \mathbb{Q}(\mathfrak{f})$ with $[L : \mathbb{Q}(\mathfrak{f})] = \frac{\ell^{2b-2}(\ell^2-1)}{w}$ and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ such that $E(L)$ has a point of order ℓ^b.*

(2) *Suppose $\ell^b = 2$ and $\Delta \neq -3$.*
   (a) *If $E_{/L}$ is an $\mathcal{O}$-CM elliptic curve defined over a number field such that $E(L)$ has a point of order 2, then $3 \mid [L : \mathbb{Q}(\mathfrak{f})]$*
   (b) *Conversely, there is an extension $L \supset \mathbb{Q}(\mathfrak{f})$ with $[L : \mathbb{Q}(\mathfrak{f})] = 3$ and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ such that $E(L)$ has a point of order 2.*

(3) *If $\Delta = -3$, there is an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}}$ such that $E(\mathbb{Q})$ has a point of order 2.*

Proof. (1) Suppose $\ell^b \geq 3$. Then part (a) follows from [BC, Thm. 7.2] and part (b) follows from Lemma 2.3.

(2) Suppose $\ell^b = 2$ and $\Delta \neq -3$. Then part (a) follows from [BC, Remark 7.3], whereas part b) is clear in this case: for any elliptic curve E over a field F of characteristic 0 and any point P of order 2 on E, we have $[F(P) : F] \leq 3$ because there are precisely 3 points of order 2.
(3) Suppose $\ell^b = 2$ and $\Delta = -3$. Then [Ol74, p. 196] shows there is an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}}$ with a rational point of order 2. □

6.2. Split case.

Theorem 6.2. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant Δ, and let ℓ be a prime that splits in $\mathcal{O}$. For any $b \in \mathbb{Z}^+$ we have the following:*

(1) *Suppose $\ell^b \geq 3$.*
   (a) *If E is an $\mathcal{O}$-CM elliptic curve defined over a number field L such that $E(L)$ has a point of order ℓ^b, then $\frac{2\ell^{b-1}(\ell-1)}{w} \mid [L : \mathbb{Q}(\mathfrak{f})]$.*
   (b) *Conversely, there is an extension $L \supset \mathbb{Q}(\mathfrak{f})$ with $[L : \mathbb{Q}(\mathfrak{f})] = \frac{2\ell^{b-1}(\ell-1)}{w}$ and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ such that $E(L)$ has a point of order ℓ^b.*

(2) *Suppose $\ell^b = 2$. Then there exists an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}(\mathfrak{f})}$ with a point of order 2 in $E(\mathbb{Q}(\mathfrak{f}))$.*

Proof. If $\ell^b = 2$, then the result follows from Theorem 5.1 and Remark 5.2 (or from [BCS17, Thm. 4.2b)]), so suppose $\ell^b \geq 3$. If $L \supset K$, then Theorem 4.4 implies $\frac{\ell^{b-1}(\ell-1)}{w} \mid [L : K(\mathfrak{f})]$ and so $\frac{2\ell^{b-1}(\ell-1)}{w} \mid [L : \mathbb{Q}(\mathfrak{f})]$.

Now suppose that we have an $\mathcal{O}$-CM elliptic curve E defined over a number field L not containing K and such that $E(L)$ has a point of order ℓ^b. By [BCS17, Thm. 4.8], this implies that $\mathbb{Z}/\ell^b\mathbb{Z} \times \mathbb{Z}/\ell^b\mathbb{Z} \hookrightarrow E(KL)$, and thus by [BC, Cor. 1.2, Lemma 2.2] that

$$\frac{2\ell^{b-1}(\ell-1)}{w} \mid \ell^{b-1}(\ell-1)\left(\frac{\ell^{b-1}(\ell-1)}{w}\right) = \#\overline{C_{\ell^b}(\mathcal{O})} \mid [KL : K(\mathfrak{f})] = [L : \mathbb{Q}(\mathfrak{f})].$$

For the existence part of 1(b): by [BC, Thm. 7.2] there is an $\mathcal{O}$-CM elliptic curve defined over an extension $L/K(\mathfrak{f})$ with $[L : \mathbb{Q}(\mathfrak{f})] = 2[L : K(\mathfrak{f})] = \frac{2\ell^{b-1}(\ell-1)}{w}$ such that $E(L)$ has a point of order ℓ^b. □

In fact, [BCS17, Thm. 4.8] has the following additional consequence:

Proposition 6.3. *Suppose that ℓ splits in $\mathcal{O}$ and let $\ell^b \geq 3$. For $d \in \mathbb{Z}^+$, suppose there is an $\mathcal{O}$-CM elliptic curve E defined over an extension field $F/\mathbb{Q}(\mathfrak{f})$ of degree d.*
a) If F does not contain K, then

$$\frac{\varphi(\ell^b)^2}{w} \mid d.$$

b) Suppose $[F : \mathbb{Q}(\mathfrak{f})] = \varphi(\ell^d)$.
(i) If $\Delta < -4$ and $\ell^b \geq 5$ then $F \supset K$.
(ii) If $\Delta = -4$ and $\ell^b \geq 9$ then $F \supset K$.
(iii) If $\Delta = -3$ and $\ell^b \geq 11$ then $F \supset K$.

Proof. a) By [BCS17, Thm. 4.8] we have $E[\ell^b] \subset E(FK)$, so by [BC, Thm. 1.1] we have

$$\frac{\varphi(\ell^b)^2}{w} = \frac{\#C_{\ell^b}(\mathcal{O})}{w} = \#\overline{C_{\ell^b}(\mathcal{O})} \mid [FK : K(\mathfrak{f})] \mid [F : \mathbb{Q}(\mathfrak{f})] = d.$$

b) Taking $d = \varphi(\ell^b)$ in part a), we get that if $F \supset K$ then $\varphi(\ell^b) \mid w$. If $\Delta < -4$ then $w = 2$ and $\varphi(\ell^b) \mid 2 \implies \ell^b \leq 4$. If $\Delta = -4$ then $w = 4$ and $\varphi(\ell^b) \leq 4 \implies \ell^b \leq 8$. If $\Delta = -3$ then $w = 6$ and $\varphi(\ell^b) \leq 6$ implies $\ell^b \leq 9$. □

6.3. **Ramified case.** Let $\mathcal{O}$ be an order of conductor $\mathfrak{f}$ in the imaginary quadratic field K. Let ℓ be a prime ramified in $\mathcal{O}$ and put $c \coloneqq \mathrm{ord}_\ell(\mathfrak{f})$.

The least degree in which an $\mathcal{O}$-CM elliptic curve has a rational point of order ℓ^a is tied to the existence of rational isogenies over $\mathbb{Q}(\mathfrak{f})$ and $K(\mathfrak{f})$, both of which have been classified. Work of Kwon concerns isogenies over $\mathbb{Q}(\mathfrak{f})$ (see Theorem 5.1 and Remark 5.2), and the following result determines isogenies over $K(\mathfrak{f})$.

Let m be the maximum of all $a \in \mathbb{Z}^+$ such that there is an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}(\mathfrak{f})}$ with a $\mathbb{Q}(\mathfrak{f})$-rational cyclic ℓ^a-isogeny. Let M be the supremum over all $a \in \mathbb{Z}^+$ such that there is an $\mathcal{O}$-CM elliptic curve $E_{/K(\mathfrak{f})}$ with a $K(\mathfrak{f})$-rational cyclic ℓ^a-isogeny.

Proposition 6.4. *Suppose that $\ell \mid \Delta$. Recall that $c \coloneqq \mathrm{ord}_\ell(\mathfrak{f})$.*

(1) *Suppose $\ell \mid \mathfrak{f}$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$. Then we have:*

$$m = \begin{cases} 1 & \ell = 2, c = 1 \\ 2c-2 & \ell = 2, c \geq 2 \\ 2c & \ell \text{ is odd} \end{cases}$$
$$M = \infty$$

(2) *Suppose $\ell \mid \mathfrak{f}$ and $\left(\frac{\Delta_K}{\ell}\right) = -1$. Then we have:*

$$m = \begin{cases} 1 & \ell = 2, c = 1 \\ 2c-2 & \ell = 2, c \geq 2 \\ 2c & \ell \text{ is odd} \end{cases}$$
$$M = 2c$$

(3) *Suppose $\Delta \neq -3, -4$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$. Then we have:*

$$m = \begin{cases} 1 & \ell = 2, c = 0 \\ 2c & \ell = 2, c \geq 1, \mathrm{ord}_2(\Delta_K) = 2 \\ 2c+1 & \ell = 2, c \geq 1, \mathrm{ord}_2(\Delta_K) = 3 \\ 2c+1 & \ell \text{ is odd} \end{cases}$$
$$M = 2c+1$$

(4) *Suppose $\Delta = -3$ and $\ell = 3$. Then we have $m = M = 2$.*

(5) *Suppose* $\Delta = -4$ *and* $\ell = 2$. *Then we have* $m = M = 2$.

Proof. Suppose $\Delta \neq -3, -4$. Theorem 5.1 and Remark 5.2 gives the value of m in all cases. By Theorem 2.4, M is the maximum of all $a \in \mathbb{Z}^+$ such that Δ is a square modulo $\mathbb{Z}/4\ell^a\mathbb{Z}$. The explicit determination of M in terms of c and ℓ is given in [BC, §7.4]. (In that section we have the running hypothesis that $\mathrm{ord}_\ell(\mathfrak{f}) \geq 1$, but the calculation done in Case 3 is valid even when $\mathrm{ord}_\ell(\mathfrak{f}) = 0$.) For $\Delta = -3, -4$, see Propositions 5.9 and 5.10 and their proofs. □

Theorem 6.5. *Suppose that* $\ell \mid \Delta$. *The least degree over* $\mathbb{Q}(\mathfrak{f})$ *in which there is an* $\mathcal{O}$*-CM elliptic curve with a rational point of order* ℓ^a *for* $a \in \mathbb{Z}^+$ *is as follows:*

(1) *If* $a \leq m$, *then the least degree is* $\begin{cases} 1 & \ell^a = 2, \\ \varphi(\ell^a)/2 & \ell^a > 2. \end{cases}$

(2) *If* $m < a \leq M$, *then* $\ell^a > 2$ *and the least degree is* $\varphi(\ell^a)$.

(3) *If* $a > M = m \geq 1$, *then the least degree is* $\ell^{2(a-m)} \cdot \varphi(\ell^m)/2$.

(4) *If* $a > M > m \geq 1$, *then* $\ell = 2$ *and the least degree is* 2^{2a-M-1}.

Proof. We will consider each case separately:

(1) Suppose $a \leq m$.

• Suppose $\Delta \neq -3, -4$. If $\ell^a = 2$, then by Proposition 6.4 there is a $\mathbb{Q}(\mathfrak{f})$-rational 2-isogeny, hence a $\mathbb{Q}(\mathfrak{f})$-rational point of order 2. If $\ell^a > 2$, then by [BCS17, Thm. 5.5], there is an extension $L/\mathbb{Q}(\mathfrak{f})$ of degree $\varphi(\ell^a)/2$ and a twist E' of $E_{/L}$ such that $E'(L)$ has a rational point of order ℓ^a. This is the least possible degree by [BC, Thm. 6.2].

• Suppose $\Delta = -3$. Then $\ell = 3$ and $m = 2$ and the claim follows as above.

• Suppose $\Delta = -4$. Then $\ell = 2$ and $m = 2$, anad again the claim follows as above.

(2) Suppose $m < a \leq M$.

By Proposition 6.4, we may assume $\Delta \neq -3, -4$. As above, we have $\ell^a > 2$, and by [BCS17, Thm. 5.5], there is an extension $L/K(\mathfrak{f})$ of degree $\varphi(\ell^a)/2$ and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ with a rational point of order ℓ^a. Furthermore, by [BC, Thm. 6.2] if $E_{/L}$ is an $\mathcal{O}$-CM elliptic curve with an L-rational point of order ℓ^a, then

$$\varphi(\ell^a)/2 \mid [KL : K(\mathfrak{f})],$$

so the least degree over $\mathbb{Q}(\mathfrak{f})$ in which there is an $\mathcal{O}$-CM elliptic curve with a rational point of order ℓ^a is either $\varphi(\ell^a)/2$ or $\varphi(\ell^a)$.

Suppose for the sake of contradiction that there exists a number field $L/\mathbb{Q}(\mathfrak{f})$ of degree $\varphi(\ell^a)/2$ and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ such that $E(L)$ contains a rational point P of order ℓ^a. Since $\varphi(\ell^a)/2 \mid [KL : K(\mathfrak{f})]$, it follows that $[KL : K(\mathfrak{f})] = \varphi(\ell^a)/2$ and $K \not\subset L$. Since $a > m$, Theorem 5.3 implies $\mathbb{Q}(\ell\mathfrak{f}) \subset L$, and so $K(\ell\mathfrak{f}) \subset KL$. Recall that $K(\ell\mathfrak{f})$ is the projective ℓ-torsion point field of an $\mathcal{O}$-CM elliptic curve (see [Pa89, Prop.3] and [BC, Thm. 4.1]). Thus the image of the mod ℓ Galois representation of $E_{/KL}$ consists of scalar matrices. Since $E(KL)$ has a point of order ℓ, it therefore has full ℓ-torsion, so $\mathbb{Z}/\ell^a\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E(KL)$, contradicting Theorem 4.1.

(3) Suppose $a > M = m \geq 1$.

First suppose that ℓ is odd. By (1), there is an extension $F/\mathbb{Q}(\mathfrak{f})$ of degree $\frac{\varphi(\ell^m)}{2}$ and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ with an F-rational point P of order ℓ^m. By Lemma 2.2a), there is a field extension L/F of degree at most $\ell^{2(a-m)}$ and $Q \in E(L)$ of order ℓ^a, and thus

$$[L : \mathbb{Q}(\mathfrak{f})] = [L : F][F : \mathbb{Q}(\mathfrak{f})] \leq \ell^{2(a-m)} \frac{\varphi(\ell^m)}{2}.$$

It follows from [BC, Thm. 7.2] that this is the least possible degree for an $\mathcal{O}$-CM elliptic curve to have a rational point of order ℓ^a.

Now suppose that $\ell = 2$. Then the assumptions hold in two cases: (i) $\left(\frac{\Delta_K}{2}\right) = 0$ and $c = 0$; or (ii) $\left(\frac{\Delta_K}{2}\right) = 0$, $c \geq 1$, and $\mathrm{ord}_2(\Delta_K) = 3$. In both cases, it follows from [BC, Thm. 7.2] that $2^{2(a-m)} \cdot \varphi(2^m)/2$ is the least possible degree, and we shall construct a point of at most this degree.

Suppose (i): $\left(\frac{\Delta_K}{2}\right) = 0$ and $c = 0$. Let us first assume that $\Delta \neq -4$. Then $m = M = 1$, so by (1) there is an $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{Q}(\mathfrak{f})}$ with a $\mathbb{Q}(\mathfrak{f})$-rational point of order 2, and by Lemma 2.2b)

there is a field extension $L/\mathbb{Q}(\mathfrak{f})$ of degree at most $2^{2a-3} = 2^{2(a-m)\frac{\varphi(\ell^m)}{2}}$ and $Q \in E(L)$ of order 2^a. If $\Delta = -4$, then $m = M = 2$. By (1) there is an $\mathcal{O}_K$-CM elliptic curve $E_{/\mathbb{Q}}$ with a $\mathbb{Q}$-rational point of order 4. By Lemma 2.2a) there is a field extension $L/\mathbb{Q}(\mathfrak{f})$ of degree at most $2^{2a-4} = 2^{2(a-m)\frac{\varphi(\ell^m)}{2}}$ and $Q \in E(L)$ of order 2^a.

Suppose (ii): $\left(\frac{\Delta_K}{2}\right) = 0$, $c \geq 1$, and $\mathrm{ord}_2(\Delta_K) = 3$. By (1), there is an extension $F/\mathbb{Q}(\mathfrak{f})$ of degree $\frac{\varphi(2^m)}{2}$ and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ with an F-rational point of order 2^m. By Lemma 2.2a) there is a field extension L/F of degree at most $2^{2(a-m)}$ and $Q \in E(L)$ of order 2^a, so

$$[L : \mathbb{Q}(\mathfrak{f})] = [L : F][F : \mathbb{Q}(\mathfrak{f})] \leq 2^{2(a-m)}\frac{\varphi(2^m)}{2}.$$

(4) Suppose $a > M > m \geq 1$. This case is only possible when $\ell = 2$ and $2 \mid \mathfrak{f}$. By [BC, Thm. 7.2], the least degree of a field extension $F/K(\mathfrak{f})$ for which there is an $\mathcal{O}$-CM elliptic curve $E_{/F}$ with an F-rational point of order 2^a is 2^{2a-M-2}, so the least degree in which there exists an $\mathcal{O}$-CM elliptic curve with a rational point of order 2^a is either 2^{2a-M-2} or 2^{2a-M-1}.

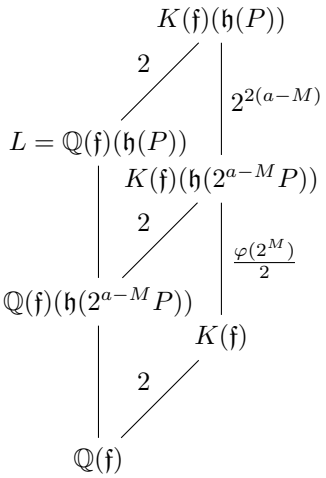
Suppose for the sake of contradiction that there is a number field $L/\mathbb{Q}(\mathfrak{f})$ of degree 2^{2a-M-2} and an $\mathcal{O}$-CM elliptic curve $E_{/L}$ such that $E(L)$ contains a rational point P of order 2^a. Then we must have $L = \mathbb{Q}(\mathfrak{f})(\mathfrak{h}(P))$. Since $2^{2a-M-2} \mid [K(\mathfrak{f})(P) : K(\mathfrak{f})]$, it follows that

$$[K(\mathfrak{f})(P) : K(\mathfrak{f})] = [K(\mathfrak{f})(\mathfrak{h}(P)) : K(\mathfrak{f})] = 2^{2a-M-2}$$

and $K \not\subset L$. The point $2^{a-M}P$ has order 2^M. Suppose for the sake of contradiction that the orbit of $C_{2^M}(\mathcal{O})$ on $2^{a-M}P$ has more than $\varphi(2^M)$ elements. By [BC, §7.4], the $C_{2^a}(\mathcal{O})$-orbit on P has size larger than

$$2^{2(a-M)}\varphi(2^M) = 2^{2a-M-1}.$$

This implies $[K(\mathfrak{f})(\mathfrak{h}(P)) : K(\mathfrak{f})] > 2^{2a-M-2}$, which is a contradiction. Thus the orbit of $C_{2^M}(\mathcal{O})$ on $2^{a-M}P$ has $\varphi(2^M)$ elements, and $[K(\mathfrak{f})(\mathfrak{h}(2^{a-M}P)) : K(\mathfrak{f})] = \frac{\varphi(2^M)}{2}$. We have the following diagram of fields:



It follows that $[L : \mathbb{Q}(\mathfrak{f})(\mathfrak{h}(2^{a-M}P))] = 2^{2a-M}$, and thus

$$[\mathbb{Q}(\mathfrak{f})(\mathfrak{h}(2^{a-M}P)) : \mathbb{Q}(\mathfrak{f})] = 2^{M-2}.$$

But then we have a point of order 2^M in an extension of $\mathbb{Q}(\mathfrak{f})$ of degree 2^{M-2}, contradicting (2). □

From Proposition 6.4 and Theorem 6.5 we deduce the following theorem:

Theorem 6.6. *Let ℓ be a prime with $\ell \mid \Delta$. Then the least degree over $\mathbb{Q}(\mathfrak{f})$ in which there is an $\mathcal{O}$-CM elliptic curve with a rational point of order ℓ^a for $a \in \mathbb{Z}^+$ is as follows:*

(1) *Suppose $\ell \mid \mathfrak{f}$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$.*

(a) *If* $\ell = 2$ *and* $c = 1$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{a-1} & a > 1. \end{cases}$

(b) *If* $\ell = 2$ *and* $c \geq 2$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{a-2} & 1 < a \leq 2c-2, \\ 2^{a-1} & a > 2c-2. \end{cases}$

(c) *If* ℓ *is odd, the least degree is* $\begin{cases} \ell^{a-1}(\ell-1)/2 & a \leq 2c, \\ \ell^{a-1}(\ell-1) & a > 2c. \end{cases}$

(2) *Suppose* $\ell \mid \mathfrak{f}$ *and* $\left(\frac{\Delta_K}{\ell}\right) = -1$.

(a) *If* $\ell = 2$ *and* $c = 1$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{2a-3} & a \geq 2. \end{cases}$

(b) *If* $\ell = 2$ *and* $c \geq 2$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{a-2} & 1 < a \leq 2c-2, \\ 2^{a-1} & 2c-2 < a \leq 2c, \\ 2^{2a-2c-1} & a > 2c. \end{cases}$

(c) *If* ℓ *is odd, the least degree is* $\begin{cases} \ell^{a-1}(\ell-1)/2 & a \leq 2c, \\ \ell^{2a-2c-1}(\ell-1)/2 & a > 2c. \end{cases}$

(3) *Let* $\Delta \neq -3, -4$, *and suppose* $\left(\frac{\Delta_K}{\ell}\right) = 0$.

(a) *If* $\ell = 2$ *and* $c = 0$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{2a-3} & a > 1. \end{cases}$

(b) *If* $\ell = 2$, $c \geq 1$, *and* $\mathrm{ord}_2(\Delta_K) = 2$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{a-2} & 1 < a \leq 2c, \\ 2^{2a-2c-2} & a \geq 2c+1. \end{cases}$

(c) *If* $\ell = 2$, $c \geq 1$, *and* $\mathrm{ord}_2(\Delta_K) = 3$, *the least degree is* $\begin{cases} 1 & a = 1, \\ 2^{a-2} & 1 < a \leq 2c+1, \\ 2^{2a-2c-3} & a > 2c+1. \end{cases}$

(d) *If* ℓ *is odd, the least degree is* $\begin{cases} \ell^{a-1}(\ell-1)/2 & a \leq 2c+1, \\ \ell^{2a-2c-2}(\ell-1)/2 & a > 2c+1. \end{cases}$

(4) *Suppose* $\Delta = -3$ *and* $\ell = 3$. *Then the least degree is* $\begin{cases} 3^{a-1} & a \leq 2, \\ 3^{2a-3} & a > 2. \end{cases}$

(5) *Suppose* $\Delta = -4$ *and* $\ell = 2$. *Then the least degree is* $\begin{cases} 1 & a \leq 2, \\ 2^{2a-4} & a > 2. \end{cases}$

6.4. **An example.**

Example 6.7. *We place ourselves in the setting of Theorem 6.6(1) with a prime* $\ell > 2$. *Then there is a number field* $F \supset \mathbb{Q}(\mathfrak{f})$ *of degree* $\frac{\ell-1}{2}$ *and an* $\mathcal{O}$*-CM elliptic curve* $E_{/F}$ *with an* F*-rational point* P *of order* ℓ. *We observe that for any* $a \in \mathbb{Z}^+$, *there is an extension* L/F *such that* $[L : F]$ *is odd and* $E(L)$ *has a point of order* ℓ^a*: indeed, the* $\mathfrak{g}_F$*-set* $\{Q \in E(\overline{F}) \mid \ell^{a-1}Q = P\}$ *has odd order* ℓ^{2a-2}, *and thus contains at least one* $\mathfrak{g}_F$*-orbit of odd cardinality. Overall we get a point of order* ℓ^a *over an extension* L/F *with* $\mathrm{ord}_2[L : F] = \mathrm{ord}_2 \frac{\ell-1}{2}$. *On the other hand, when* $a > 2c$ *the* least *degree of an extension field* $F/\mathbb{Q}(\mathfrak{f})$ *for which there is an* $\mathcal{O}$*-CM elliptic curve with an* F*-rational point of order* ℓ^a *is* $\ell^{a-1}(\ell-1)$. *Since* $\mathrm{ord}_2(\ell^{a-1}(\ell-1)) = \mathrm{ord}_2([L : F]) + 1$, *it is not the case that every degree of an extension field* F *of* $\mathbb{Q}(\mathfrak{f})$ *for which some* $\mathcal{O}$*-CM elliptic curve admits an* F*-rational point of* ℓ^a *is a multiple of the least such degree. This is in distinct contrast to Theorem 4.1, which works over* $K(\mathfrak{f})$.

References

[Ao95] N. Aoki, *Torsion points on abelian varieties with complex multiplication.* Algebraic cycles and related topics (Kitasakado, 1994), 1–22, World Sci. Publ., River Edge, NJ, 1995.

[BC] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves*, submitted.

[BCP17] A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case.* Math. Z. 285 (2017), 795–820.

[BCS17] 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.

[Co89] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* John Wiley & Sons, New York, 1989.

[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.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques.* Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[FN07] Y. Fujita and T. Nakamura, *Torsion on elliptic curves in isogeny classes.* Trans. Amer. Math. Soc. 359 (2007), 5505-5515.

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

[Ol74] L. Olson, *Points of finite order on elliptic curves with complex multiplication.* Manuscripta math. 14 (1974), 195–205.

[Ma77] B. Mazur, *Rational points on modular curves.* Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107-148. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

[Pa89] J.L. Parish, *Rational Torsion in Complex-Multiplication Elliptic Curves.* Journal of Number Theory 33 (1989), 257–265.

[Ro96] D.J.S. Robinson, *A course in the theory of groups.* Second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[Sh94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[Si88] A. Silverberg, *Torsion points on abelian varieties of CM-type.* Compositio Math. 68 (1988), no. 3, 241–249.

[Si92] A. Silverberg, *Points of finite order on abelian varieties.* In *p-adic methods in number theory and algebraic geometry*, 175–193, Contemp. Math. 133, Amer. Math. Soc., Providence, RI, 1992.

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

[St01] P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity.* Class field theory – its centenary and prospect (Tokyo, 1998), 161-176, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.