CM ELLIPTIC CURVES: VOLCANOES, REALITY AND APPLICATIONS, PART II

PETE L. CLARK AND FREDERICK SAIA

Abstract. Let $M \mid N$ be positive integers, and let Δ be the discriminant of an order in an imaginary quadratic field K. When $\Delta_K < -4$, the first author determined the fiber of the morphism $X_0(M,N) \to X(1)$ over the closed point J_Δ corresponding to Δ and showed that all fibers of the map $X_1(M,N) \to X_0(M,N)$ over J_Δ were connected. [Cl22a]. In the present work we complement the work of [Cl22a] by addressing the most difficult cases $\Delta_K \in \{-3,-4\}$. These works provide all the information needed to compute, for each positive integer d, all subgroups of $E(F)[\mathrm{tors}]$, where F is a number field of degree d and $E_{/F}$ is an elliptic curve with complex multiplication.

Contents

1. Introduction

1.1. **Main Results.** This paper is a direct continuation of [Cl22a], which determined the Δ-CM locus on the modular curves $X_0(M,N)_{/\mathbb{Q}}$ for Δ the discriminant of an order in an imaginary quadratic field K *different from* $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. This work also gave a completely explicit description of the *primitive* residue fields of Δ-CM closed points: i.e., the residue fields $\mathbb{Q}(P)$ of Δ-CM points $P \in X_0(M,N)$ for which there is no Δ-CM point $P' \in X_0(M,N)$ such that $\mathbb{Q}(P')$ embeds into $\mathbb{Q}(P)$ as a proper subfield. Finally, the work [Cl22a] also gave an inertness result for the fibers of $X_1(M,N) \to X_0(M,N)$ over Δ-CM points on $X_0(M,N)$, which yields a complete description of the multiset of degrees of Δ-CM closed points on $X_1(M,N)_{/\mathbb{Q}}$. Using only the knowledge of the degrees of primitive residue fields of Δ-CM points on $X_0(M,N)$ yields the corresponding knowledge of degrees of primitive residue fields of Δ-CM points on $X_1(M,N)$, which is precisely what is needed in order to classify torsion subgroups of Δ-CM elliptic curves over number fields of any fixed degree.

In the present work we treat the excluded fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. If $\Delta = \mathfrak{f}^2\Delta_K$ and $\Delta_K \in \{-3,-4\}$, then for all $M \mid N$ we determine the Δ-CM locus on $X_0(M,N)_{/\mathbb{Q}}$ and explicitly determine all primitive residue fields of Δ-CM points on $X_0(M,N)_{/\mathbb{Q}}$. Finally, we show that the fibers of $X_1(M,N) \to X_0(M,N)$ over Δ-CM points are connected.[1]

Taken together, the works [Cl22a] and the present work give a complete description of torsion subgroups of CM elliptic curves over number fields. In particular, we get an algorithm that takes as input a positive integer d and outputs the complete, finite list of groups isomorphic to $E(F)[\mathrm{tors}]$ where F is a number field of degree d and $E_{/F}$ is a CM elliptic curve, conditionally on knowing the finite list of imaginary quadratic orders of class number properly dividing d. With current knowledge about class numbers, this allows us to enumerate CM torsion in number field degree $d \leq 200$. If we are willing to assume the Generalized Riemann Hypothesis (GRH), then by [LLS15, Cor. 1.3] we can enumerate CM torsion in number field degree $d \leq 18104$. This enumeration will appear in a future work.

1.2. **Review of the $\Delta_K < -4$ case.** Let us outline the proof of the computation of the fiber of $X_0(M,N) \to X(1)$ over the closed Δ-CM point J_Δ on $X(1)$ given in [Cl22a] so that we can see what must be modified to treat the $\Delta_K \in \{-3,-4\}$ case.

Step 1: We handle the case $X_0(1,\ell^a) = X_0(\ell^a)$ for a prime power ℓ^a.

[1]The difference between "inertness" and "connectedness" is that the latter allows ramification. The map $X_0(M,N) \to X(1)$ can only ramify over 0, 1728 and ∞.

Step 1a: The ℓ-power isogeny graph corresponding to a Δ-CM elliptic curve with $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ (where $\gcd(\ell, \mathfrak{f}_0) = 1$) has the structure of an **ℓ-isogeny volcano**. This is an infinite graph that is very close to being a rooted tree and with vertex set stratified into levels indexed by $\mathbb{Z}^{\geq 0}$; the set of vertices at level L corresponds to the set of j-invariants of $(\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K)$-CM elliptic curves, which is a torsor under $\operatorname{Pic}\mathcal{O}(\Delta)$, the Picard group of the imaginary quadratic order $\mathcal{O}(\Delta)$ of discriminant Δ. Cyclic ℓ^a-isogenies with Δ-CM source elliptic curve correspond to paths of length a in this volcano with initial vertex at level L. From this it is easy to see that if $\varphi : E \to E'$ is such an isogeny and if the target elliptic curve has level L', then over K the field of moduli of φ is the ring class field $K(\mathfrak{f}_0\ell^{\max(L,L')})$, which is equal to $K(j(E), j(E'))$. It follows that

$$\mathbb{Q}(j(E), j(E')) \subseteq \mathbb{Q}(\varphi) \subseteq K(j(E), j(E')).$$

Step 1b: Thus the field of moduli $\mathbb{Q}(\varphi)$ of φ is determined when $\mathbb{Q}(j(E), j(E'))$ contains K: this happens if and only if $\mathbb{Q}(j(E), j(E'))$ has no real embedding ($j(E)$ and $j(E')$ are "not coreal"). Otherwise we are left to decide whether $\mathbb{Q}(\varphi)$ is $\mathbb{Q}(j(E), j(E'))$ or $K(j(E), j(E'))$. Both the coreality question and the dichotomy between the two possible fields can be answered in terms of the natural action of complex conjugation on the ℓ-isogeny volcano. Determining the explicit action of $\mathfrak{g}_{\mathbb{R}} = \{1, c\}$ on the ℓ-isogeny volcano is one of the main contributions of [Cl22a]. In the end, depending upon whether or not the path is fixed under complex conjugation or not,[2] we get that $\mathbb{Q}(\varphi)$ is isomorphic to $\mathbb{Q}(\mathfrak{f}_0\ell^{\max(L,L')}$ – that is, isomorphic to a *rational ring class field* – the field obtained by adjoining to $\mathbb{Q}$ the j-invariant of an elliptic curve with CM by the imaginary quadratic order of discriminant $(\mathfrak{f}_0\ell^{\max(L,L')})^2\Delta_K$ – or to the ring class field $K(\mathfrak{f}_0\ell^{\max(L,L')})$ – which is obtained by adjoining to K the same j-invariant.

Step 2: We pass from the prime power case $X_0(\ell^a)$ to the case $X_0(N)$.
Step 2a: For any closed point $p \notin \{0, 1728, \infty\}$ on the j-line $X(1)$, if $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$, let F be the fiber of $\pi : X_0(N) \to X(1)$ over p, and for $1 \leq i \leq r$ let F_i be the fiber of $X_0(\ell_i^{a_i}) \to X(1)$ over p. Then we show that F is the fiber product of $F_1, \ldots, F_r$ over $\operatorname{Spec}\mathbb{Q}(p)$. Since each F_i is the spectrum of a finite product of number fields, each isomorphic to either a rational ring class field or a ring class field, F is determined by F_i in terms of tensor products of these rational ring class fields and ring class fields.
Step 2b: Letting $\mathbb{Q}(\mathfrak{f}) \coloneqq \mathbb{Q}(j(\mathbb{C}/\mathcal{O}(\mathfrak{f}^2\Delta_K)))$ be the rational ring class field of conductor $\mathfrak{f}$, we show that

$$K(\mathfrak{f}_1) \otimes_{K(\gcd(\mathfrak{f}_1,\mathfrak{f}_2)} K(\mathfrak{f}_2) = K(\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)) \tag{1}$$

and

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\gcd(\mathfrak{f}_1,\mathfrak{f}_2)} \mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(\operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)). \tag{2}$$

[2]Since closed points on $X_0(\ell^a)$ correspond to certain equivalence classes of paths, the actual answer is slightly more complicated than this but can still be determined from the action of complex conjugation on the isogeny graph.

These identities allow us to write down F explicitly as a product of number fields.

Step 3: Lifting a point P on $X_0(N)$ induced by an isogeny $\varphi : E \to E'$ to a point $\tilde{P}$ $X_0(M,N)$ involves scalarizing the modulo M Galois representation on E, with the effect that $\mathbb{Q}(\tilde{P})$ is obtained from $\mathbb{Q}(P)$ by adjoining the projective M-torsion field $\mathbb{Q}(P)(\mathbb{P}E[M])$. This uses that because $\Delta < -4$, the projective M-torsion field is independent of the choice of $\mathbb{Q}(P)$-rational model. Indeed, for all $M \geq 3$, if E is a $\Delta = \mathfrak{f}^2\Delta_K$-CM elliptic curve, we find that $\mathbb{Q}(P)(\mathbb{P}E[M]) = \mathbb{Q}(P)K(M\mathfrak{f})$.

1.3. **The $\Delta_K \in \{-3,-4\}$ case.** When $\Delta_K \in \{-3,-4\}$ and E is a $\Delta = \mathfrak{f}^2\Delta_K$-CM elliptic curve, then for certain $\mathfrak{f} > 1$ *some* of the above steps still hold. However, when $\mathfrak{f} = 1$, *none* of the above arguments hold as stated. While some of the change are routine, in several places we have to make arguments that are significantly more intricate than those of [Cl22a]. Let us describe the modifications:

Step 1a: When $\Delta_K \in \{-3,-4\}$, ℓ is a prime numer, and $\mathfrak{f}_0 > 1$, then again the ℓ-power isogeny graph of a $(\Delta = (\ell^L\mathfrak{f}_0)^2\Delta_K)$-CM elliptic curve is an ℓ-volcano. When $\mathfrak{f}_0 = 1$, the ℓ-power isogeny graph is no longer an ℓ-volcano. This is in fact the least of our worries, as the deviation from "volcanoness" is minor and had already been well understood: the differences involve multiple edges descending from the surface and in subtleties involving orientations of edges which necessitate more care in the notion of a "nonbacktracking path." The structural information we need is found, for instance, in [Su13].

Step 1b: When $\mathfrak{f}_0^2\Delta_K \in \{-3,-4\}$, there is in fact *no* canonical action of complex conjugation on the ℓ-isogeny graph. To define the action of complex conjugation on isogenies, we need *a priori* a chosen $\mathbb{R}$-model on the elliptic curve. Every real elliptic curve has precisely two nonisomorphic $\mathbb{R}$-models. When $\Delta < -4$ these two $\mathbb{R}$-models are quadratic twists of each other, so the action of $\mathfrak{g}_{\mathbb{R}}$ on finite subgroup schemes of $E_{/\mathbb{R}}$ is independent of the choice of $\mathbb{R}$-model. However, when $\Delta \in \{-3,-4\}$ this is no longer the case.

It turns out that when $\mathfrak{f}_0^2\Delta_K \in \{-3,-4\}$, in most cases we can define a *noncanonical* action of $\mathfrak{g}_{\mathbb{R}}$ on the ℓ-isogeny graph that allows us to determine fields of modulo of Δ-CM points on $X_0(N)$ in terms of real and complex paths, as in [Cl22a]. But there are two cases in which we need to pass from this isogeny graph to a certain double cover and define an action of $\mathfrak{g}_{\mathbb{R}}$ on that. By looking carefully on how surface edges change the $\mathbb{R}$-structure of a Δ_K-CM elliptic curve we are able to carry out the analysis as in [Cl22a].

Step 2a: The fiber product result referred to above [Cl22a, Prop. 3.5] is false when $j \in \{0, 1728\}$: the modular curve $X_0(\ell_1^{a_1} \cdots \ell_r^{a_r})$ is a desingularization of the fiber product of the morphisms $X_0(\ell_i^{a_i}) \to X(1)$. For lack of this scheme-theoretic result we need other techniques to compute the composite level fibers. We make use of the Atkin-Lehner involution w_N to reduce to either the $\Delta_K < -4$ case or the case when both the source and target are Δ_K-CM, in which case we have a *proper* isogeny in the sense of [Cl22a, §3.4] and we can reason via $\mathbb{Z}_K$-ideals.

Step 2b: When $\Delta \in \{-3, -4\}$, equations (1) and (2) hold for certain pairs $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$ and fail for others: in general the compositum $K(\mathfrak{f}_1)K(\mathfrak{f}_2)$ is a proper subfield of $K(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2))$; and the same holds for rational ring class fields $\mathbb{Q}(\mathfrak{f}_1)$ and $\mathbb{Q}(\mathfrak{f}_2)$. In §2 we use class field theory to show that it is still the case that $K(\mathfrak{f}_1)$ and $K(\mathfrak{f}_2)$ are linearly disjoint over $K(\gcd(\mathfrak{f}_1, \mathfrak{f}_2))$ and to determine the index of $K(\mathfrak{f}_1)K(\mathfrak{f}_2)$ in $K(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2))$; we do the same for rational ring class fields; and again we calculate tensor products of rational ring class fields and ring class fields. This calculation is relatively straightforward, but the difference in the answer causes complications related to Step 2a: when $\Delta_K < -4$, if N_1, N_2 are coprime positive integers, to show that the residue field $\mathbb{Q}(P)$ of a point $P \in X_0(N)$ contains e.g. a ring class field $K(N_1N_2)$, it suffices to show that it contains each of $K(N_1)$ and $K(N_2)$. When $\Delta_K \in \{-3, -4\}$, we cannot argue in this way. Instead our method is to find a rationally isogenous elliptic curve with CM conductor divisible by N_1N_2.

Step 3: When $\Delta \in \{-3, -4\}$, the projective M-torsion field $F(\mathbb{P}E[M])$ of a Δ-CM elliptic curve may depend upon the model. Nevertheless we compute the residue field $\mathbb{Q}(P)$ for any Δ-CM point $P \in X_0(M, M)$ (this amounts to computing the minimal possible projective M-torsion field as we range over models). Using this and the maps $\alpha : X_0(M, N) \to X_0(M, M)$ and $\beta : X_0(M, N) \to X_0(N)$, we can bootstrap from $\beta(P) \in X_0(N)$ to $P \in X_0(M, N)$, with some care: the case $\Delta = -4$ behaves exceptionally to all the rest.

1.4. **The CM fibers of $X_1(M, N) \to X_0(M, N)$ are connected.** In [Cl22a, Thm. 1.2], the first author showed an especially close relationship between points on $X_0(M, N)$ and points on $X_1(M, N)$ for points which do not have CM by $\Delta \in \{-3, -4\}$. In particular, this theorem states that the fiber of the map $X_1(M, N) \to X_0(M, N)$ is inert over any point which does not have CM by one of these two discriminants. This has the important consequence that determining the degrees of closed Δ-CM points on $X_0(M, N)$ and on $X_1(M, N)$ are *equivalent problems*. The following theorem generalizes this result to include points with -3 and -4-CM.

Theorem 1.1. *Let $M \mid N \in \mathbb{Z}^+$, and suppose that $x \in X_0(M, N)_{/\mathbb{Q}}$ is a Δ-CM point. Let $\pi : X_1(M, N) \to X_0(M, N)$ denote the natural morphism.*

(i) *If $\Delta < -4$ or if $M \geq 2$, then π is inert over x.*

(ii) *Suppose that $\Delta \in \{-3, -4\}$ and $M = 1$.*

(a) *If x is a ramified point of the map $X_0(M, N) \to X(1)$ or if $N \leq 3$, then π is inert over x.*

(b) *Otherwise, i.e., if $N \geq 4$ and x is an elliptic point on $X_0(M, N)$, then we have*

$$e_\pi(x) = \begin{cases} 2 & \text{if } \Delta = -4 \\ 3 & \text{if } \Delta = -3 \end{cases} \quad \text{and} \quad f_\pi(x) = \begin{cases} \phi(N)/4 & \text{if } \Delta = -4 \\ \phi(N)/6 & \text{if } \Delta = -3 \end{cases}$$

for the ramification index and residual degree of x.

In particular, in all cases we have that the fiber of π over x consists of a single point.

Proof. For the proof, we first recall some basic relevant facts: for $N \leq 2$ the map π is an isomorphism. For $N \geq 3$ it is a $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$-Galois covering, hence has degree $\phi(N)/2$. All points on $X(N) = X_1(N,N)$ not above $0, 1728 \in X(1)$ are unramified. For $N \geq 4$ the curve $X_1(N)$ (and hence $X(N)$) has no elliptic points of periods 2 or 3, from which it follows that all points over $0, 1728 \in X(1)$ are ramified with ramification index 2 or 3. The curve $X_1(2)$ has a single elliptic point of period 2 over $1728 \in X(1)$, while the curve $X_1(3)$ has a single elliptic point of period 3 over $0 \in X(1)$. (One can see these claims regarding elliptic points and ramification from elementary arguments involving congruence subgroups, in fact this is [DS05, Exc. 2.3.7]).

For $\Delta < -4$ the claim is [Cl22a, Thm 1.2], so suppose that $\Delta \in \{-3, -4\}$. For $M \geq 2$, the point x must be non-elliptic (i.e., is a ramified point of the map $X_0(M,N) \to X(1)$). We can see this, for instance, via our analysis of paths on $\mathcal{G}_{K,\ell,1}$ for any prime $\ell \mid M$; in all cases we find that any pair of independent $\ell^{a'}$ isogenies for $a' \geq 1$ must include at least one with a corresponding path in $\mathcal{G}_{K,\ell,1}$ which descends, and hence any -3 or -4-CM point on $X_0(\ell^{a'}, \ell^a)$, and hence on $X_0(M,N)$ for $M \geq 2$, must be non-elliptic. In this case we then have that a pair $(E,C)_{/\mathbb{Q}(x)}$ inducing x is well-defined up to quadratic twist, as all models for E are defined over $\mathbb{Q}(x)$. For this reason, the same argument involving the modulo N $\pm$-Galois representation given in [Cl22a, Thm 1.2] applies. Similarly, this argument applies in case $(2)(a)$ if x is a ramified point of the map $X_0(M,N) \to X(1)$.

We now assume that x is an elliptic Δ-CM point on $X_0(M,N)$ with $\Delta \in \{-3, -4\}$. If $N = 2$, then π is an isomorphism, so the claim is trivial. If $N = 3$, then because there is a single elliptic point on $X_1(3)$ it follows that it must comprise the entire fiber above x, giving the inertness claim. Assuming now that $N \geq 4$, we know that x is elliptic while every point in $\pi^{-1}(x)$ is ramified with respect to the map $X_1(N) \to X(1)$, giving the claimed ramification index. Note that it follows that the residual degree is at most the claimed residual degree in each case.

To provide the lower bound on the residual degree, we need only modify the argument of the $\Delta < -4$ case slightly in a predictable way. If $\Delta = -4$, then a pair $(E,C)_{\mathbb{Q}(x)}$ inducing x is well-defined up to quartic twist. Letting $q_N : \mathbb{Z}_K \to \mathbb{Z}_K/N\mathbb{Z}_K$ denote the quotient map, by tracking that action of Galois on a generator P of C we get a well-defined reduced mod N Galois representation

$$\overline{\rho_N} : \mathfrak{g}_{\mathbb{Q}(x)} \to (\mathbb{Z}_K/N\mathbb{Z}_K)^\times / q_N(\mathbb{Z}_K^*)$$

which is independent of the chosen model and surjective (see [BC20a, §1.3]). As the set $\{P, -P, iP, -iP\}$ is stable under the action of $\mathfrak{g}_{\mathbb{Q}(y)}$ for $y \in \pi^{-1}(x)$, we then must have

$$\frac{\phi(N)}{4} = \#\left(\overline{\rho_N}\left(\mathfrak{g}_{\mathbb{Q}(x)}\right)\right) \mid [\mathbb{Q}(y) : \mathbb{Q}(x)],$$

giving the result for $\Delta = -4$. For $\Delta = -3$, exchanging "quartic" for "cubic" and μ_4 for μ_3 results in the required divisibility $\frac{\phi(N)}{6} \mid f_\pi(x)$.

□

Remark 1.2. The $M = 1$ with $\Delta < -4$ case of Theorem 1.1 is used explicitly in [CGPS22] to transfer from knowledge of the *least* degree of a Δ-CM point on $X_1(N)$, which is computed in [BC20b], to knowledge of the least degree of a Δ-CM point on $X_0(N)$. A shadow of Theorem 1.1 is also seen in the referenced study in the $\Delta \in \{-3, -4\}$ case. A positive integer N is of Type I or Type II, using the terminology of [CGPS22], if $X_0(N)$ has an elliptic point of order 3 or 2, respectively. If N is of type I, then there is a single primitive degree among all elliptic points on $X_0(N)$ which is the least degree of a -4-CM point on $X_0(N)$. In this case, the single point lying above any elliptic -4-CM point on $X_1(N)$ provides the least degree of a -4-CM point on $X_1(N)$ (and the analogous statements hold for Type II and $\Delta = -3$).

2. Composita of Ring Class Fields and of Rational Ring Class Fields

Let K be an imaginary quadratic field, of discriminant Δ_K. We put

$$w_K := \#\mathbb{Z}_K^\times = \begin{cases} 6 & \text{if } \Delta_K = -3 \\ 4 & \text{if } \Delta_K = -4 \\ 2 & \text{if } \Delta_K < -4 \end{cases}.$$

Let $\mathcal{O}$ be a $\mathbb{Z}$-order in K. For $\mathfrak{f} \in \mathbb{Z}^+$, there is a unique $\mathbb{Z}$-order $\mathcal{O}$ in K with $[\mathbb{Z}_K : \mathcal{O}] = \mathfrak{f}$ and then $\mathfrak{f}\mathbb{Z}_K$ is the conductor ideal $(\mathcal{O} : \mathbb{Z}_K)$ [Cl22a, §2.1]. We denote by $K(\mathfrak{f})$ the **ring class field** of $\mathcal{O}$ [Cl22a, §2.3]. If $j_\Delta := j(\mathbb{C}/\mathcal{O})$, then we have

$$K(\mathfrak{f}) = K(j_\Delta).$$

We recall from [Cx89, Cor. 7.24] the formula

$$\mathfrak{d}(\mathfrak{f}) := [K(\mathfrak{f}) : K(1)] = \begin{cases} 1 & \text{if } \mathfrak{f} = 1 \\ \frac{2}{\#\mathbb{Z}_K^\times}\mathfrak{f}\prod_{\ell \mid \mathfrak{f}}\left(1 - \left(\frac{\Delta_K}{\ell}\right)\frac{1}{\ell}\right) & \text{if } \mathfrak{f} \geq 2 \end{cases}. \tag{3}$$

As in [Cl22a, §2.6], we also define the **rational ring class field**

$$\mathbb{Q}(\mathfrak{f}) := \mathbb{Q}(j_\Delta).$$

In [Cl22a, §2] we studied composita of ring class fields and of rational ring class fields (with a fixed imaginary quadratic field K, in both cases) when $\Delta_K < -4$. The results were quite clean: for $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$, the fields $K(\mathfrak{f}_1)$ and $K(\mathfrak{f}_2)$ are linearly disjoint over $K(\gcd(\mathfrak{f}_1, \mathfrak{f}_2))$ and we have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2))$ [Cl22a, Prop. 2.2] and the same holds with each $K(\mathfrak{f}_i)$ replaced by $\mathbb{Q}(\mathfrak{f}_i)$ [Cl22a, Prop. 2.10a)].

Here we treat $\Delta_K \in \{-3, -4\}$.

Proposition 2.1. *Let K be a quadratic field with $\Delta_K \in \{-3, -4\}$, let $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$, and put*

$$m := \gcd(\mathfrak{f}_1, \mathfrak{f}_2), \ M := \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2).$$

a) *Suppose that $m > 1$. Then:*

$$K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(M).$$

b) *If the order of discriminant* $\mathfrak{f}_1^2\Delta_K$ *has class number* 1*, then we have*

$$K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(\mathfrak{f}_2).$$

c) *Let* $\mathfrak{f}_1, \ldots, \mathfrak{f}_r \in \mathbb{Z}^+$ *be pairwise relatively prime, and further assume that:*
- *If* $\Delta_K = -3$*, then no* $\mathfrak{f}_i$ *lies in* $\{1, 2, 3\}$*; and*
- *If* $\Delta_K = -4$*, then no* $\mathfrak{f}_i$ *lies in* $\{1, 2\}$.

Then:

$$[K(\mathfrak{f}_1 \cdots \mathfrak{f}_r) : K(\mathfrak{f}_1) \cdots K(\mathfrak{f}_r)] = \left(\frac{w_K}{2}\right)^{r-1}.$$

d) *In all cases we have that* $K(\mathfrak{f}_1)$ *and* $K(\mathfrak{f}_2)$ *are linearly disjoint over* $K(m)$*, and thus* $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2) = K(m)$.

Proof. We will use the classical description of ring class groups and ring class fields, with notation as in [Cx89, §7]. For $\mathfrak{f} \in \mathbb{Z}^+$, let $I_K(\mathfrak{f})$ be the group of fractional $\mathbb{Z}_K$-ideals prime to $\mathfrak{f}$ and let $P_{K,\mathbb{Z}}(\mathfrak{f})$ be the subgroup of principal fractional ideals generated by an element $\alpha \in \mathbb{Z}_K$ such that $\alpha \equiv a \pmod{\mathfrak{f}\mathbb{Z}_K}$ for some $a \in \mathbb{Z}$ with $\gcd(a, \mathfrak{f}) = 1$. By class field theory, we have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(M)$ if and only if

$$P_{K,\mathbb{Z}}(\mathfrak{f}_1) \cap P_{K,\mathbb{Z}}(\mathfrak{f}_2) = P_{K,\mathbb{Z}}(M).$$

Clearly in all cases we have

$$P_{K,\mathbb{Z}}(\mathfrak{f}_1) \cap P_{K,\mathbb{Z}}(\mathfrak{f}_2) \supseteq P_{K,\mathbb{Z}}(M).$$

a) • Suppose $\Delta_K = -4$ and $m > 1$, so the units of $\mathbb{Z}_K$ are $\pm 1, \pm\sqrt{-1}$. Let $(\alpha) \in P_{K,\mathbb{Z}}(\mathfrak{f}_1) \cap P_{K,\mathbb{Z}}(\mathfrak{f}_2)$. We may choose α such that

$$\alpha \equiv a_{\mathfrak{f}_1} \pmod{\mathfrak{f}_1\mathbb{Z}_K}$$

and then there is $u \in \mathbb{Z}_K^\times$ such that

$$u\alpha \equiv a_{\mathfrak{f}_2} \pmod{\mathfrak{f}_2\mathbb{Z}_K}.$$

If $u \in \{\pm 1\}$, then the argument of Case 1 works to show that $(\alpha) \in P_{K,\mathbb{Z}}(M)$. After replacing α with $-\alpha$ if necessary, the other case to consider is that

$$\sqrt{-1}\alpha \equiv a_{\mathfrak{f}_2} \pmod{\mathfrak{f}_2\mathbb{Z}_K}.$$

If this holds then

$$\frac{a_{\mathfrak{f}_2}}{a_{\mathfrak{f}_1}} \equiv i \pmod{m\mathbb{Z}_K},$$

which is manifestly false.

• Suppose $\Delta_K = -3$ and $m > 1$, so the units of $\mathbb{Z}_K$ are $\pm 1, \pm\omega, \pm\overline{\omega}$, where $\omega = \frac{1+\sqrt{-3}}{2}$. As above, we may suppose that $\alpha \equiv a_{\mathfrak{f}_1} \pmod{\mathfrak{f}_1\mathbb{Z}_K}$ and α is congruent modulo $\mathfrak{f}_2\mathbb{Z}_K$ to either $\omega a_{\mathfrak{f}_2}$ or to $\overline{\omega}a_{\mathfrak{f}_2}$. We then get

$$\frac{a_{\mathfrak{f}_2}}{a_{\mathfrak{f}_1}} \equiv \omega \text{ or } \overline{\omega} \pmod{m\mathbb{Z}_K},$$

which is again manifestly false.

b) This is a trivial case, listed for completeness: if the order of discriminant $\mathfrak{f}_1^2\Delta_K$ has class

number 1 then $K(\mathfrak{f}_1) = K(1)$ (and conversely), so $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(1)K(\mathfrak{f}_2) = K(\mathfrak{f}_2)$.[3]
c) We claim that the extensions $K(\mathfrak{f}_1), \ldots, K(\mathfrak{f}_r)$ are mutually linearly disjoint over $K(1)$: that is,

$$K(\mathfrak{f}_1) \otimes_{K(1)} \cdots \otimes_{K(1)} K(\mathfrak{f}_r) = K(\mathfrak{f}_1) \cdots K(\mathfrak{f}_r).$$

Since everything in sight is Galois, it is enough to check that $(K(\mathfrak{f}_1) \cdots K(\mathfrak{f}_{r-1})) \cap K(\mathfrak{f}_r) = K(1)$. But the conductor of $K(\mathfrak{f}_1) \cdots K(\mathfrak{f}_{r-1})$ divides $\mathfrak{f}_1 \cdots \mathfrak{f}_{r-1}$ and the conductor of $K(\mathfrak{f}_r)$ divides $\mathfrak{f}_r$, so the conductor of their intersection is the unit ideal, so the intersection is contained in the Hilbert class field $K(1)$, hence is equal to $K(1)$. From this it follows that

$$[K(\mathfrak{f}_1 \cdots \mathfrak{f}_r) : K(\mathfrak{f}_1) \cdots K(\mathfrak{f}_r)] = \frac{\delta(\mathfrak{f}_1 \cdots \mathfrak{f}_r)}{\prod_{i=1}^r \delta(\mathfrak{f}_i)},$$

and the latter expression may be evaluated using (3).
d) It is immediate that $K(m) \subseteq K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$.

The case $m = 1$ is easy: then $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$ has conductor dividing $\mathfrak{f}_1$ and $\mathfrak{f}_2$, so its conductor is the unit ideal, so $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$ is contained in the Hilbert class field of K, which is the ring class field $K(1)$.

Henceforth we suppose that $m > 1$, and thus by part a) we have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(M)$. We claim the formula

$$\mathfrak{d}(m)\mathfrak{d}(M) = \mathfrak{d}(\mathfrak{f}_1)\mathfrak{d}(\mathfrak{f}_2).$$

First we observe that this formula $g(m)g(M) = g(\mathfrak{f}_1)g(\mathfrak{f}_2)$ holds for any multiplicative function $g : \mathbb{Z}^+ \to \mathbb{C}$. If we had $\Delta_K < -4$ then the function $\mathfrak{d}$ would be multiplicative. Instead we have $\Delta_K \in \{-3, -4\}$, in which case $\mathfrak{d}$ is a constant multiple of a multiplicative function *except for its value at* 1. This justifies the claim. The claim can be rewritten as

$$[K(\mathfrak{f}_1)K(\mathfrak{f}_2) : K(m)] = [K(M) : K(m)] = [K(\mathfrak{f}_1) : K(m)][K(\mathfrak{f}_2) : K(m)],$$

so $K(\mathfrak{f}_1)$ and $K(\mathfrak{f}_2)$ are linearly disjoint over $K(m)$, and thus $K(m) = K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$. □

Proposition 2.2. *Let K be a quadratic field with $\Delta_K \in \{-3, -4\}$. Let $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$, and put $m = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$, $M = \operatorname{lcm}(\mathfrak{f}_1\mathfrak{f}_2)$. Let*

$$\mathcal{D} := \{-3, -4, -12, -16, -27\};$$

this is the set of imaginary quadratic disciminants $\Delta = \mathfrak{f}^2\Delta_K$ with fundamental discriminant $\Delta_K \in \{-3, -4\}$ and class number 1. Let

$$S := \{\mathfrak{f} \in \mathbb{Z}^+ \mid \mathfrak{f}^2\Delta_K \in \mathcal{D}\}.$$

a) *The fields $\mathbb{Q}(\mathfrak{f}_1)$ and $\mathbb{Q}(\mathfrak{f}_2)$ are linearly disjoint over $\mathbb{Q}(m)$:*

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_2) \cong \mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2).$$

b) *If $\mathfrak{f}_1 \in S$, then we have:*

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_2) \cong \mathbb{Q}(\mathfrak{f}_2),$$
$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} K(\mathfrak{f}_2) \cong K(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_2) \cong K(\mathfrak{f}_2),$$

[3]This gives rise to cases in in which $K(M) \supsetneq K(\mathfrak{f}_1)K(\mathfrak{f}_2)$: e.g. when $\Delta_K = -3$ we have $K(2)K(3) = K(1)$ but $[K(6) : K(1)] = 3$.

and

$$K(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} K(\mathfrak{f}_2) \cong K(\mathfrak{f}_2) \times K(\mathfrak{f}_2).$$

c) *If* $\mathfrak{f}_1, \mathfrak{f}_2 \notin S$ *and* $m > 1$, *then we have*

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_2) \cong \mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(M),$$
$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} K(\mathfrak{f}_2) \cong \mathbb{Q}(\mathfrak{f}_2)K(\mathfrak{f}_2) = K(M),$$

and

$$K(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} K(\mathfrak{f}_2) \cong K(M) \times K(M).$$

d) *Let* $\mathfrak{f}_1, \ldots, \mathfrak{f}_r$ *be elements of* $\mathbb{Z}^+ \backslash S$ *that are pairwise relatively prime. Then* $\mathbb{Q}(\mathfrak{f}_1) \cdots \mathbb{Q}(\mathfrak{f}_r)$ *is a subfield of* $\mathbb{Q}(\mathfrak{f}_1 \cdots \mathfrak{f}_r)$ *of index* $\left(\frac{w_K}{2}\right)^{r-1}$, *and moreover*

$$\mathbb{Q}(\mathfrak{f}_1) \cdots \mathbb{Q}(\mathfrak{f}_r) \cong \mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \cdots \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_r),$$
$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \cdots \mathbb{Q}(\mathfrak{f}_{r-1}) \otimes_{\mathbb{Q}(m)} K(\mathfrak{f}_r) \cong \mathbb{Q}(\mathfrak{f}_1) \cdots \mathbb{Q}(\mathfrak{f}_{r-1})K(\mathfrak{f}_r).$$

Finally, if $2 \leq s \leq r$, *then*

$$\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \cdots \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_{r-s}) \otimes_{\mathbb{Q}(m)} K(\mathfrak{f}_{r-s+1}) \otimes_{\mathbb{Q}(\mathfrak{f})} \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_r) \cong (K(\mathfrak{f}_1) \cdots K(\mathfrak{f}_r))^{2^{s-1}}.$$

Proof. a) As in the proof of [Cl22a, Prop. 2.10], this follows from the fact that $K(\mathfrak{f}_1)$ and $K(\mathfrak{f}_2)$ are linearly disjoint over $K(m)$.
b) If $\mathfrak{f}_1 \in S$, then $\mathbb{Q}(m) = \mathbb{Q}(\mathfrak{f}_1) = \mathbb{Q}(1)$, and all the statements follow easily.
c) Using part a) and Proposition 2.1a), we get

$$[\mathbb{Q}(M) : \mathbb{Q}(m)] = [K(M) : K(m)] = [K(\mathfrak{f}_1)K(\mathfrak{f}_2) : K(m)] = [K(\mathfrak{f}_1) \otimes_{K(m)} K(\mathfrak{f}_2) : K(m)]$$
$$= [\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_2) : \mathbb{Q}(m)] = [\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) : \mathbb{Q}(m)],$$

so $\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(M)$. The other two statements of part c) follow easily.
d) Again it follows from Proposition 2.1 that the field extensions $\mathbb{Q}(\mathfrak{f}_1), \ldots, \mathbb{Q}(\mathfrak{f}_r)$ are mutually linearly disjoint over $\mathbb{Q}(1)$. So

$$[\mathbb{Q}(\mathfrak{f}_1) \cdots \mathbb{Q}(\mathfrak{f}_r) : \mathbb{Q}(1)] = \prod_{i=1}^{r} [\mathbb{Q}(\mathfrak{f}_i) : \mathbb{Q}(1)] = \left(\frac{w_K}{2}\right)^{1-r} [\mathbb{Q}(\mathfrak{f}_1 \cdots \mathfrak{f}_r) : \mathbb{Q}(1)].$$

The other two statements of part d) follow easily. □

3. The Isogeny Graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$

3.1. **Defining the graph.** Let K be an imaginary quadratic field, and let ℓ be a prime number. There is a directed multigraph $\mathcal{G}_{K,\ell}$ as follows: the vertex set $\mathcal{V}$ of $\mathcal{G}_{K,\ell}$ is the set of j-invariants $j \in \mathbb{C}$ of **K-CM** elliptic curves, i.e., j-invariants of complex elliptic curves with endomorphism ring an order in the imaginary quadratic field K. In general, for $j \in \mathcal{V}$ we denote by E_j a complex elliptic curve with j-invariant j. As for the edges: let $\pi_1 : X_0(\ell) \to X(1)$ be the natural map, let $w_N \in \mathrm{Aut}(X_0(N))$ be the Atkin-Lehner involution, and let $\pi_2 \coloneqq \pi_1 \circ w_N$: here we work over $\mathbb{C}$. For $j, j' \in \mathcal{V}$, write

$$(\pi_2)_* \pi_1^*([j]) = \sum_P e_P [P].$$

Then the number of directed edges from j to j' is $e_{j'}$. Equivalently, let $E_{/\mathbb{C}}$ be any elliptic curve with j-invariant j. Then the number of edges from j to j' is the number of cyclic order ℓ subgroups C of E such that $j(E/C) = j'$.

In [Cl22a, §4] we recalled the complete structure of the graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ when $\mathfrak{f}_0^2\Delta_K < -4$ and saw in particular that it was an ℓ-volcano in the sense of [Cl22a, §4.2]. Now we need to describe the structure of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ when $\mathfrak{f}_0^2\Delta_K \geq -4$: i.e., when $\mathfrak{f}_0 = 1$ and $\Delta_K \in \{-3, -4\}$.

3.2. $\Delta_K = -4$**.** Suppose $\Delta_K = -4$, $\mathfrak{f}_0 = 1$, and let ℓ be a prime number.

Example 3.1. *Let $K = \mathbb{Q}(\sqrt{-1})$, $\ell = 2$ and $\mathfrak{f}_0 = 1$. The surface of this graph consists of CM j-invariants of discriminant -4, of which there is 1: $j = 1728$. Level one consists of CM j-invariants of discriminant -16, of which there is again 1: $j = 2^3 \cdot 3^3 \cdot 11^3$. Level two consists of CM j-invariants of discriminant -64, of which there are 2. As always, they form a single Galois orbit. We have*

$$J_{-64}(t) = t^2 - 82226316240t - 7367066619912.$$

There is one horizontal edge at the surface (a loop), corresponding to the unique $\mathbb{Z}[\sqrt{-1}]$-ideal $\mathfrak{p}_2$ of norm 2. The remaining two edges emanating outward from $j = 1728$ connect it to $j = 2^3 \cdot 3^3 \cdot 11^3$. This corresponds to the fact that the pullback of the degree 1 divisor J_{1728} under $\pi : X_0(2) \to X(1)$ is $[J_{1728}] + 2[J_{2^3 \cdot 3^3 \cdot 11^3}]$.

One of the three order 2 subgroups of E_{1728} is $E[\mathfrak{p}_2]$. The other two are interchanged by the action of μ_4/μ_2 on $E_{1728}[2]$.
The vertex $j = 1728$ has outward degree 3 and inward degree 2, while the vertex $j = 2^3 \cdot 3^3 \cdot 11^3$ has outward degree 3 and inward degree 4.

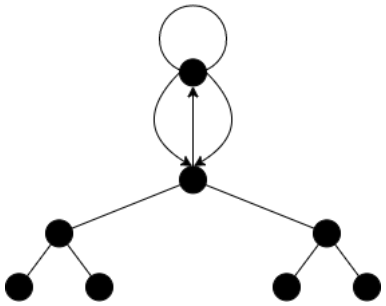

FIGURE 1. the graph $\mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$ up to level 3

Next suppose $\ell \equiv 1 \pmod 4$. Then there are two loops emanating from the surface vertex v_0, corresponding to the two prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2 = \overline{\mathfrak{p}_1}$ of $\mathbb{Z}[\sqrt{-1}]$ lying over ℓ. Let v_1 be any one of the $\frac{\ell-1}{2}$ level one vertices. There are two directed edges from v_0 to v_1. The natural action of μ_4/μ_2 on edges with emanating from v_0 fixes each of the two surface loops and interchanges the pair of edges from v_0 to v_1. For each vertex at level $L \geq 1$ there is one

upward edge and ℓ downward edges.

Finally suppose $\ell \equiv 3 \pmod 4$. There are no surface edges. For each vertex v_1 at level 1 there are two edges from v_0 to v_1. These two edges are interchanged by the μ_4/μ_2-action. For each vertex at level $L \geq 1$ there is one upward edge and ℓ downward edges.

3.3. $\Delta_K = -3$**.** Suppose $\Delta_K = -3$, $\mathfrak{f}_0 = 1$, and let ℓ be a prime number.

Example 3.2. *Let $K = \mathbb{Q}(\sqrt{-3})$, $\ell = 3$ and $\mathfrak{f}_0 = 1$. The surface of this graph consists of CM j-invariants of discriminant -3, of which there is 1: $j = 0$. Level one consists of CM j-invariants of discriminant $-3 \cdot 3^2$, of which there is again 1: $j = -2^{15} \cdot 3 \cdot 5^3$. Level two consists of CM j-invariants of discriminant $-3 \cdot 3^4$, of which there are 3, forming a single Galois orbit. We have $J_{-3\cdot 3^4} =$*

$$t^3+185576290573466419200 0t^2-375065736503309107200000 0t+33385867246735196160000000 00.$$

There is one horizontal edge at the surface (a loop), corresponding to the unique $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$-ideal $\mathfrak{p}_3$ of norm 3. The remaining three edges emanating outward from $j = 0$ connect it to $j = -2^{15} \cdot 3 \cdot 5^3$. This corresponds to the fact that the pullback of the degree 1 divisor J_0 under $\pi : X_0(3) \to X(1)$ is $[J_0] + 3[J_{-2^{15}\cdot 3\cdot 5^3}]$.

One of the four order 3 subgroups of E_0 is $E[\mathfrak{p}_3]$. The other three are interchanged by the action of μ_6/μ_2 on $E_0[2]$.
The vertex $j = 0$ has outward degree 4 and inward degree 2, while the vertex $j = -2^{15} \cdot 3 \cdot 5^3$ has outward degree 4 and inward degree 6.

Next suppose $\ell \equiv 1 \pmod 3$. Then there are two loops emanating from the surface vertex v_0 corresponding to the two prime ideals of $\mathbb{Z}[\zeta_6]$ lying over ℓ. Let v_1 be any one of the $\frac{\ell-1}{3}$ level one vertices. There are three directed edges from v_0 to v_1. The natural action of μ_6/μ_4 on surface edges fixes each of the two surface loops and cyclically permutes the three edges from v_0 to v_1.

Finally suppose $\ell \equiv 2 \pmod 3$. There are no surface edges. For each vertex v_1 at level 1 there are three edges from v_0 to v_1. These edges are cyclically permuted by the μ_4/μ_2-action. For each vertex at level $L \geq 1$ there is one upward edge and ℓ downward edges.

3.4. **Paths and ℓ^a-isogenies.** When $\mathfrak{f}_0^2\Delta_K < -4$, [Cl22a, Lemma 4.2] gives a bijective correspondence between isomorphism classes of cyclic ℓ^a isogenies $\varphi : E \to E'$ where $E_{/\mathbb{C}}$ is a K-CM elliptic curve for which the prime to ℓ part of the conductor of the endomorphism ring is $\mathfrak{f}_0$ and length a nonbacktracking paths in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$. In these cases every edge in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ has a canonical inverse edge, so the directedness of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ does not really intervene.

When $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$, the notion of a nonbacktracking path in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ is a bit more subtle when the path involves ascent to and descent from the surface. If we descend from any surface vertex v_0 to a level one vertex v_1 and then ascend back to v_0, then the latter edge must represent the dual isogeny of the former edge, since it is the *unique* isogeny between these two elliptic curves, so this counts as backtracking. On the other hand, if we start at a level one vertex v_1 take the unique edge $e : v_1 \to v_0$ and then descend back down to v_1, we have a choice of 2 edges when $\Delta_K = -4$ and 3 edges when $\Delta_K = -3$. Then e

corresponds to an ℓ-isogeny $\varphi : E_1 \to E_0$ and exactly one of the edges from v_0 to v_1, say e', corresponds to $\varphi^\vee$. So a path containing e followed by e' counts as backtracking, but a path containing e followed by any other edge from v_0 to v_1 does not.

With this understanding, [Cl22a, Lemma 4.2] extends to all Δ_K, ℓ and $\mathfrak{f}_0$.

Lemma 3.3. *Let K be an imaginary quadratic field, ℓ a prime number and $\mathfrak{f}_0$ a positive integer prime to ℓ. There is a bijective correspondence from the set of isomorphism classes of cyclic ℓ^a-isogenies of CM elliptic curves with endomorphism algebra K and prime-to-ℓ-conductor $\mathfrak{f}_0$ to the set of length a paths without backtracking in the isogeny graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.*

Moreover the proof of [Cl22a, Lemma 4.2] still works to establish Lemma 3.3.

4. Action of Complex Conjugation on $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$

This section is the analogue of [Cl22a, §5] for $\mathfrak{f}_0^2\Delta_K \in \{-3, 4\}$. We define an action of $\mathfrak{g}_{\mathbb{R}} = \{1, c\}$ on the isogeny graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ that is crucial for our subsequent analysis...almost. We will see that in two cases there is *no* such action that is suitable for our purposes, so instead we define an action on a certain double cover of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.

4.1. The Field of Moduli of a Cyclic ℓ^a-isogeny.

Theorem 4.1. *Let ℓ^a be a prime power, let K be an imaginary quadratic field, and let $\varphi : E \to E'$ be a cyclic ℓ^a-isogeny of K-CM elliptic curves over $\mathbb{C}$, and let $\mathbb{Q}(\varphi)$ be the field of moduli of φ. Let $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ be the discriminant of the endomorphism ring of E (here $\gcd(\mathfrak{f}_0, \ell) = 1$), let $\Delta' = \ell^{2L'}\mathfrak{f}_0^2\Delta_K$ be the discriminant of the endomorphism ring of E', and put $\overline{L} = \max(L, L')$ and $\mathfrak{f} = \ell^{\overline{L}}\mathfrak{f}_0$. Then:*

a) *There is a field embedding $\mathbb{Q}(\mathfrak{f}) \hookrightarrow \mathbb{Q}(\varphi)$.*
b) *We have $\mathbb{Q}(\varphi) \subseteq K(\mathfrak{f})$.*

Proof. This result is a special case of [Cl22a, Thm. 5.1] when $\mathfrak{f}_0^2\Delta_K < -4$, so we may assume that $\Delta_K \in \{-3, -4\}$ and $\mathfrak{f}_0 = 1$. a) Certainly $\mathbb{Q}(\varphi)$ contains both $\mathbb{Q}(j(E)) \cong \mathbb{Q}(\ell^L\mathfrak{f}_0)$ and $\mathbb{Q}(j(E')) \cong \mathbb{Q}(\ell^{L'}\mathfrak{f}_0)$. At least one of these fields is isomorphic to $\mathbb{Q}(\ell^{\overline{L}}\mathfrak{f}_0) = \mathbb{Q}(\mathfrak{f})$.
b) As usual, without loss of generality we may assume that $j(E) = j_\Delta$. Let $(E_0)_{/K(\mathfrak{f})}$ be any K-CM elliptic curve with endomorphism ring of discriminant $\mathfrak{f}^2\Delta_K$. Since $\Delta \mid \mathfrak{f}^2\Delta_K$, there is a canonical $K(\mathfrak{f})$-rational isogeny φ_0 with source elliptic curve E_0 and whose target elliptic curve has j-invariant $j_\Delta = j(E)$. We choose this target elliptic curve as our model for E over $K(\mathfrak{f})$, and our task is to show that for this model of E, the kernel of φ is a $\mathfrak{g}_{K(\mathfrak{f})}$-stable subgroup. In fact we will show that if φ is any cyclic ℓ^a-isogeny with source elliptic curve $E_{/K(\mathfrak{f})}$ and target elliptic curve of level L', then φ is defined over $K(\mathfrak{f})$ in the sense that its kernel is $g_{K(\mathfrak{f})}$-stable.

The isogeny φ decomposes into $\varphi_3 \circ \varphi_2 \circ \varphi_1$ with $\varphi_1 : E \to E_1$ ascending, $\varphi_2 : E_1 \to E_2$ horizontal and $\varphi_3 : E_2 \to E'$ descending. We define $b, h, d \in \mathbb{N}$ by

$$\deg \varphi_1 = \ell^b,\ \deg \varphi_2 = \ell^h,\ \deg \varphi_3 = \ell^d.$$

The isogeny φ_1 is unique, so it is certainly defined over $K(\mathfrak{f})$. If $\varphi_2 \neq 1$, then φ_2 is, up to isomorphism on its target, given as $E_1 \to E_1/E_1[I]$ for a nonzero $\mathbb{Z}_K$-ideal I, so φ_2

is defined over $K(j(E_1)) = K \subseteq K(\mathfrak{f})$. Thus it suffices to show that the descending ℓ^d-isogeny $\varphi_3 : E_2 \to E'$ is defined over $K(\mathfrak{f})$. For this the more difficult case is when E_2 lies at the surface. If E_2 lies below the surface, then whether the kernel of φ_3 is $\mathfrak{g}_{K(\mathfrak{f})}$-stable is independent of the model of E_2, and the dual isogeny $\varphi_3^\vee : E' \to E_2$ is ascending so is defined over $K(j(E')) = K(j_{\Delta'}) \subseteq K(\mathfrak{f})$ on any model of E', so φ_3 is also defined over $K(\mathfrak{f})$. Thus we may assume that E_2 lies at the surface. Since $\varphi_2 : E_1 \to E_2$ is horizontal, also E_1 lies at the surface. By our choice of E, we have that E_1 is the target elliptic curve of a cyclic $K(\mathfrak{f})$-rational ℓ^a-isogeny with source elliptic curve E_0. By [BC20a, Prop. 4.5] and its proof, we have that the modulo $\ell^{\overline{L}}$-Galois representation on $(E_1)_{/K(\mathfrak{f})}$ consists of scalar matrices, which means that every cyclic $\ell^{\overline{L}}$-isogeny on E_1 is defined over $K(\mathfrak{f})$. Since $d = L' \leq \overline{L}$, the same holds for every cyclic ℓ^d-isogeny on E_1. If $\varphi_2 = 1$ this tells us directly that φ_3 is defined over $K(\mathfrak{f})$. In general: since φ_2 is horizontal, $\mathbb{Z}_K$ has class number 1 and $K(\mathfrak{f})$ contains K, then φ_2 is given, up to an isomorphism on the tareget, by a $K(\mathfrak{f})$-rationally defined endomorphism of E_2, so E_3 is $K(\mathfrak{f})$-rationally isomorphic to E_2. It follows that every downward cyclic ℓ^b-isogeny on E_2 has $\mathfrak{g}_{K(\mathfrak{f})}$-stable kernel, so φ_3 is defined over $K(\mathfrak{f})$. □

Thus we get a simple dichotomy for the field of moduli $\mathbb{Q}(\varphi)$ of a cyclic ℓ^a-isogeny φ: for the specific value of $\mathfrak{f}$ given in Theorem 4.1 in terms of the endomorphism rings of the source and target elliptic curves of φ, we know that $\mathbb{Q}(\varphi)$ is isomorphic to either $\mathbb{Q}(\mathfrak{f})$ or to $K(\mathfrak{f})$. As in [Cl22a, §5], we can resolve this dichotomy by understanding the action of complex conjugation on paths in the isogeny graph.

4.2. **Action of Complex Conjugation on $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.** First of all we have an action of complex conjugation — by this we will always really mean an action of the group $\mathfrak{g}_R = \{1, c\}$ — on the set of vertices of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$: indeed, the vertices are j-invariants of complex elliptic curves, so this is just obtained by restricting the natural action of c on $\mathbb{C}$. From [Cl22a, §2.5] we know that for all $L \in \mathbb{Z}^{\geq 0}$, the number of real vertices in level L is

$$\mathfrak{r}_L := \#\operatorname{Pic}\mathcal{O}(\ell^{2L}\mathfrak{f}_0^2\Delta_K)[2],$$

and Gauss's genus theory of binary quadratic formulas yields a formula for $\mathfrak{r}_L$ in terms of the number of odd prime divisors of Δ and the class of Δ modulo 32 [Cl22a, Lemma 2.8].

In the absence of multiple edges, this action of c on the vertex set of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ determines the action on the graph. When $\mathfrak{f}_0^2\Delta_K < -4$ the only possible multiple edges are surface edges, on which the action of c is easy to understand: the two nonisomorphic $\mathbb{R}$-structures on a real vertex differ from each other by quadratic twisting by -1, so the action of complex conjugation on the set of order ℓ-subgroups is independent of the choice of $\mathbb{R}$-structure. The answer is then that an edge running beween two real surface vertices is *not* fixed by complex conjugation in the split case and is fixed by complex conjugation in the ramified case (there are no surface edges in the inert case).

We are in the case where $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$. Then we still have:

• If v is a vertex at level $L \geq 1$ and $e : v \to w$ is a downward edge, then it is the only edge from v to w, so e is real if and only if v and w are. (Again, because we are below the surface, $\operatorname{Aut} E_v = \{\pm 1\}$, so the action of complex conjugation on subgroups of E_v is independent of the chosen $\mathbb{R}$-model.)

• An upward edge $e : v \to w$ gets mapped under complex conjugation to the unique upward edge with initial vertex $c(v)$, so e is real if and only if v is real.

The trickier cases are those of a surface edge and of an edge running from the (unique, real) surface vertex v_0 to a real level 1 vertex. We will discuss these in detail shortly.

In general, we make use of the following convention: for all $L \in \mathbb{Z}^{\geq 0}$ we mark one vertex at level L: the one with j-invariant

$$j_L \coloneqq j(\mathbb{C}/\mathcal{O}(\ell^{2L}\Delta_K)).$$

In our diagrams, this is always the leftmost vertex in a given level. The lattice $\mathcal{O}(\ell^{2L}\Delta_K)$ gives rise to a particular model E_L over $\mathbb{Q}(j_{\ell^{2L}\Delta_K})$ and hence to a particular model over $\mathbb{R}$. These models are compatible: for all $L \geq 1$, the upward edge from j_L to j_{L-1} is realized by the $\mathbb{Q}(j_L)$-rational isogeny $\mathbb{C}/\mathcal{O}(\ell^{2L}\Delta_K) \to \mathbb{C}/\mathcal{O}(\ell^{2L-2}\Delta_K)$.

• Suppose $\Delta = -4$ and $\ell > 2$. We have $\mathfrak{r}_0 = 1$ and $\mathfrak{r}_L = 2$ for all $L \geq 1$. Each real vertex v in level $L \geq 1$ has an odd number, ℓ, of descendant vertices, so at least one of these must be fixed by complex conjugation, and it follows that v has exactly one real descendant.

It remains to discuss the action of complex conjugation on the set of directed edges emanating from the surface vertex v_0, which corresponds to "the" elliptic curve $E_{/\mathbb{C}}$ with j-invariant 1728. By [Cl22a, Thm. 5.3], for any real elliptic curve and any odd prime ℓ, there are exactly 2 order ℓ-subgroups of $E(\mathbb{C})$ stabilized by complex conjugation. When $\ell \equiv 1 \pmod 4$ there are two surface loops corresponding to $E[\mathfrak{p}]$ and $E[\overline{\mathfrak{p}}]$ where $\mathfrak{p}, \overline{\mathfrak{p}}$ are the two $\mathbb{Z}[\sqrt{-1}]$-ideals of norm ℓ. These two edges are interchanged by complex conjugation (independently of the chosen $\mathbb{R}$-structure on E). So the two real edges must be downward edges. For each real level one vertex v, there is a pair of edges from v_0 to v; evidently complex conjugation stabilizes the pair, so if one is real, then both are real. It follows that for exactly one of the two level 1 real vertices both edges from the surface to that vertex are real, whreas for the other level 1 real vertex neither edge is real. Which is which depends upon the chosen $\mathbb{R}$-structure on v_0: indeed, indeed, for each level 1 real vertex v, the unique upward edge $e : v \to v_0$ can be defined over $\mathbb{Q}(j(E_v))$ and hence over $\mathbb{R}$; this provides an $\mathbb{R}$-model for E on which the dual isogeny is real.

If our path starts at v_0 and ends up at level L then it is clear that the field of moduli is $K(\ell^L)$ if the path includes a surface edge and $\mathbb{Q}(\ell^L)$ otherwise. The harder case is if our

path starts at j_L with $L \geq 1$ and ascends to the surface. In this case when we ascend to the surface we get the real model for E given by the lattice $\mathbb{Z}[\sqrt{-1}]$, and *in this real model* it is the two edges from j_0 to j_1 that are real. The significance of this for our counting problem is that if we start below the surface and ascend to the surface there is a unique way to extend the path so that the corresponding isogeny is fixed under complex conjugation: we take the unique edge from j_0 to j_1 that is not the inverse of the ascending edge from j_1 to j_0.

Thus one sees that in this case we *are* able to define an action of $\mathfrak{g}_R$ on $\mathcal{G}_{K,\ell,1}$, but to do so we had to make a choice that was appropriate for our applications.

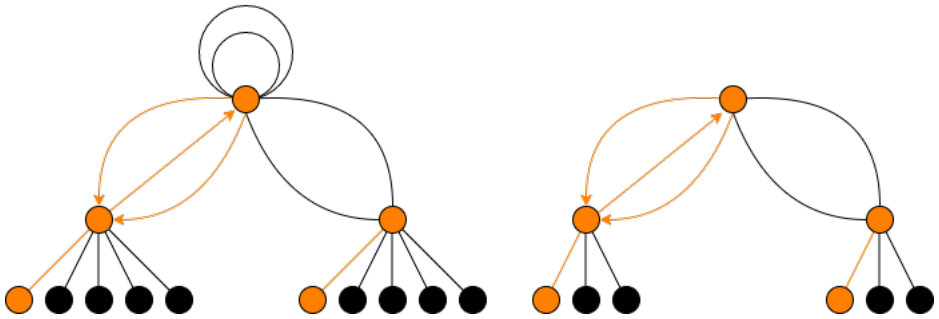

FIGURE 2. $\mathcal{G}_{\mathbb{Q}(\sqrt{-1}),\ell,1}$ up to level 2 in the cases of ℓ split ($\ell = 5$, left) and inert ($\ell = 3$, right) in $\mathbb{Q}(\sqrt{-1})$, with vertices and edges fixed by complex conjugation colored orange

• Suppose $\Delta = -3$ and $\ell > 3$. As above, we have $\mathfrak{r}_0 = 1$ and $\mathfrak{r}_L = 2$ for all $L \geq 2$. And again, each real vertex v in level $L \geq 1$ has an odd number, ℓ, of descendant vertices, so v has a unique real descendant. If $\ell \equiv 1 \pmod 3$ there is a pair of surface loops that are interchanged by complex conjugation; if $\ell \equiv 2 \pmod 3$ there are no surface edges. So by [Cl22a, Thm. 5.3] in either $\mathbb{R}$-model of "the" elliptic curve $E_{/\mathbb{C}}$ with j-invariant 0 corresponding to the surface vertex v_0 there are precisely 2 order ℓ-subgroups stable under complex conjugation. But this time things work out more nicely: there are three edges from v_0 to each of the two real level 1 vertices, which as a set are stable under complex conjugation. Since 3 is odd, at least one edge in each set must be fixed by c, hence exactly one because there are two such edges altogether.

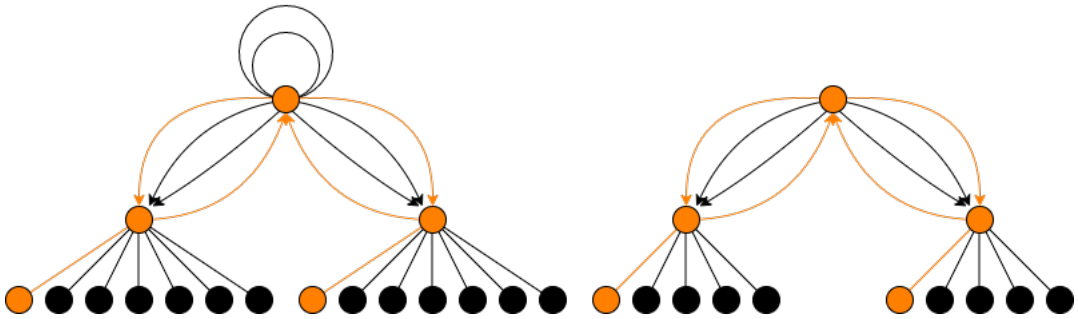

FIGURE 3. $\mathcal{G}_{\mathbb{Q}(\sqrt{-3}),\ell,1}$ up to level 2 in the cases of ℓ split ($\ell = 7$, left) and inert ($\ell = 5$, right) in $\mathbb{Q}(\sqrt{-3})$, with vertices and edges fixed by complex conjugation colored orange

• Suppose $\Delta = -3$ and $\ell = 2$. Now we have $\mathfrak{r}_0 = \mathfrak{r}_1 = 1$, $\mathfrak{r}_2 = 2$ and $\mathfrak{r}_L = 4$ for all $L \geq 3$. This means that every vertex of level $L \leq 3$ is real. For each $L \geq 3$, the real vertices of level L can be partitioned into pairs in which each pair has a common neighbor in level $L - 1$, and in each pair, exactly one of the two vertices has two real descendants and the other vertex has no real descendants. This follows from the same argument as in the proof of [Cl22a, Lemma 5.7c)].

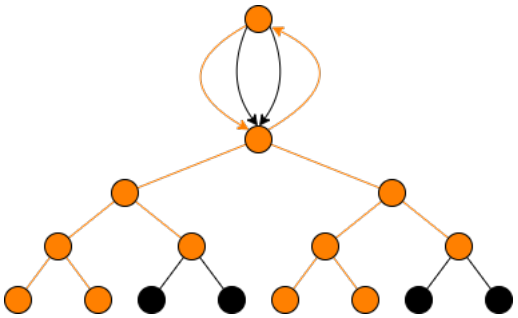

FIGURE 4. $\mathcal{G}_{\mathbb{Q}(\sqrt{-3}),2,1}$ up to level 4, with vertices and edges fixed by complex conjugation colored orange

• Suppose $\Delta = -4$ and $\ell = 2$. We have $\mathfrak{r}_0 = \mathfrak{r}_1 = 1$ and $\mathfrak{r}_L = 2$ for all $L \geq 2$. For all $L \geq 2$, the vertex v_L corresponding to j-invariant $j_L = j(\mathbb{C}/\mathcal{O}(-2^{2L+2})$ is real; the other real vertex in level L therefore must be the other descendant vertex from v_{L-1}.

Let us now discuss the action of complex conjugation on edges. Let $E_{/\mathbb{C}}$ be "the" elliptic curve of j-invariant 1728. In either $\mathbb{R}$-model of E, the surface loop corresponds to the isogeny with kernel $E[\mathfrak{p}]$, where $\mathfrak{p}$ is the unique prime ideal of $\mathbb{Z}[\sqrt{-1}]$ lying over 2, which is stable under complex conjugation.

If we choose the $\mathbb{R}$-model of E with real lattice $\mathbb{Z}[\sqrt{-1}]$, then all three order 2 subgroups are stable under complex conjugation: they can be seen quite clearly as $\frac{1}{2} + \mathbb{Z}[\sqrt{-1}]$, $\frac{\sqrt{-1}}{2} + \mathbb{Z}[\sqrt{-1}]$ and $\frac{1+\sqrt{-1}}{2} + \mathbb{Z}[\sqrt{-1}]$. So it may seem that we have defined an action of complex conjugation on $\mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$.

However this graph cannot be used for our study of isogenies! To see why, consider either of the two paths that starts at the vertex v_1 in level 1, ascends to level 0, takes the surface loop, and then descends back down to level 1. These correspond to two cyclic 8-iosgenies with source elliptic curve of discriminant -16. However, contrary to what the graph suggests, neither of these two isogenies is defined over $\mathbb{R}$. Our graph is letting us down because the surface loop, which can be realized on uniformizing lattices as $\mathbb{C}/\mathbb{Z}[\zeta_4] \to \mathbb{C}/(1+\zeta_4)\mathbb{Z}[\zeta_4]$ is an isogeny of real elliptic curves, but the source and target have different $\mathbb{R}$-structures. Recall that every elliptic curve $E_{/\mathbb{C}}$ with $j(E) \in \mathbb{R}$ has precisely two nonisomorphic $\mathbb{R}$-models [SiII, Prop. V.2.2]. When $j \notin \{0, 1728\}$, these two models are just quadratic -1 twists of each other, but this is not the case when $j \in \{0, 1728\}$. When $j = 1728$ (i.e., $\Delta = -4$), for our purposes the most useful way to distinguish between the two models is to observe that in the model $\mathbb{C}/\mathbb{Z}[\zeta_4]$ all three order 2 subgroups are real, whereas in the model $\mathbb{C}/(1+\zeta_4)\mathbb{Z}[\zeta_4]$ there is exaxctly one real order 2 subgroup, generated by $1 + (1+\zeta_4)\mathbb{Z}[\zeta_4]$. This means that in our length 3 paths considered above, once we take the surface loop, we arrive at an elliptic curve over $\mathbb{R}$ for which the two order 2 subgroups that correspond to the 2 downward edges from v_0 to v_1 are now interchanged by complex conjugation.

We remedy this by passing from $\mathcal{G} = \mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$ to the double cover $\widetilde{\mathcal{G}}$ by unwrapping the surface loop, to get a graph that now at each level L, consists of two copies of the vertex set of $\mathcal{G}$ at level L. We decree that complex conjugation acts on the second copy of the vertex set the same way it does on the first copy. The surface edge between the two copies of v_0 is real, but in the second copy the two downward edges from v_0 to v_1 are now complex. Complex conjugation acts on all other edges in the second copy the same as it does in the first copy (away from the surface the action of complex conjugation on cyclic subgroups is independent of the choice of $\mathbb{R}$-model).

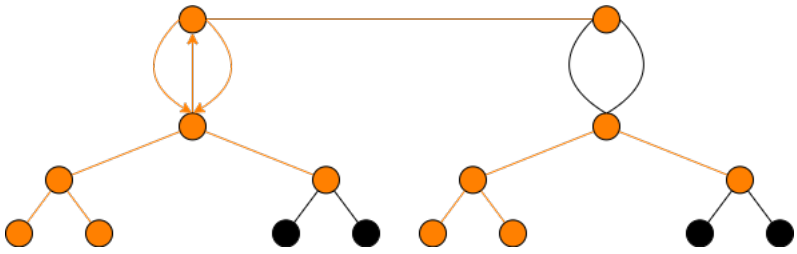

FIGURE 5. the double cover $\widetilde{\mathcal{G}}$ of $\mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$ up to level 3, with vertices and edges fixed by complex conjugation colored orange

Remark 4.2.

a) In Figure 5, we did not draw the upward edge with initial vertex the level 1 vertex in the right hand copy of $\mathcal{G} = \mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$. As far as the group action of $\mathfrak{g}_{\mathbb{R}}$ on $\widetilde{\mathcal{G}}$ is concerned, it is clear that this edge must be c-fixed. However the c-fixedness of this edge has no elliptic curve interpretation – no nonbacktracking path starting in the lefthand copy of $\mathcal{G}$ in $\widetilde{\mathcal{G}}$ contains this edge. Drawing this edge as c-fixed seems to invite confusion, so we have not done so.
b) It's interesting to compare $\widetilde{\mathcal{G}}$ to the graph of [Cl22a, Lemma 5.7]. These graphs are not isomorphic, but their enumerations of real and complex paths are the same.
c) It is also interesting (and perhaps confusing, at first) to compare the change of real structures induced by the horizontal edge in $\mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$ to the end of the proof of Theorem 4.1, in which the source and target curves of a horizontal edge are rationally isomorphic. The difference is that in the setting of Theorem 4.1 the ground field contains K. As for the horizontal edge, it corresponds to the ideal $(1+\zeta_4)$, which is real and principal...but not "real-principal": i.e., it is not generated by a real element and thus its kernel is not the kernel of an $\mathbb{R}$-rationally defined endomorphism.

• Suppose $\Delta = -3$ and $\ell = 3$. We have $\mathfrak{r}_L = 1$ for all $L \geq 0$, so the unique real vertex in level L is v_L, corresponding to the elliptic curve $\mathbb{C}/\mathcal{O}(-3^{2L+1})$.

There is a sort of "more benign" analogue of the phenomenon encountered in the previous case: the surface loop in this graph corresponds to the $\mathbb{R}$-isogeny $\mathbb{C}/\mathbb{Z}[\zeta_6] \to \mathbb{C}/(1-\zeta_3)\mathbb{Z}[\zeta_6]$. The source and target elliptic curves are isomorphic over $\mathbb{C}$ but have different $\mathbb{R}$-structures. Indeed, by [BCS17, Lemma 3.2], if Λ_1 and Λ_2 are real lattices in $\mathbb{C}$, then they determine the same $\mathbb{R}$-isomorphism class of elliptic curves if and only if they are real homothetic: there is $\alpha \in \mathbb{R}^\times$ such that $\Lambda_2 = \alpha\Lambda_1$. The two lattices $\mathbb{Z}[\zeta_6]$ and $(1-\zeta_3)\mathbb{Z}[\zeta_6]$ are not real homothetic: one can see this directly or use [BCS17, Lemma 3.6a)].

So we defined an action of complex conjugation on the three downward edges with initial vertex the surface vertex v_0: one is real and two are complex. After we take the surface loop we are now considering the action of complex conjugation on a nonisomorphic real elliptic curve. Because of this, the principled response is to again pass from $\mathcal{G}_{\mathbb{Q}(\sqrt{-3}),3,1}$ to the double cover $\widetilde{\mathcal{G}}$ by unwrapping the surface loop to get a graph that at each level L consists of two copies of the vertex set of $\mathcal{G}$ at level L, and we define the action of complex conjugation in the same way as above.

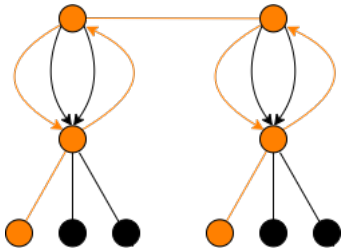

FIGURE 6. the double cover $\widetilde{\mathcal{G}}$ of $\mathcal{G}_{\mathbb{Q}(\sqrt{-3}),3,1}$ up to level 2, with vertices and edges fixed by complex conjugation colored orange

While in the previous case the change of $\mathbb{R}$-structure changed the *number* of order $\ell = 2$ subgroups fixed by complex conjugation, in this case $\ell = 3$, so [Cl22a, Thm. 5.1] applies to show that in any $\mathbb{R}$-model exactly one of the three "downward" order 3 subgroups is real. So while in the previous case we needed to pass to the double cover in order to ensure the correctness of our enumeration of real and complex paths, in this case the enumeration of real and complex paths is the same whether we pass from $\mathcal{G}$ to $\widetilde{\mathcal{G}}$ or not.

5. CM Points on $X_0(\ell^a)_{/\mathbb{Q}}$

Let ℓ be a prime number, and let $\Delta = \ell^{2L}\Delta_K$ be an imaginary quadratic discriminant with $\Delta_K \in \{-3, -4\}$. In this section we will compute the fiber of $X_0(\ell^a) \to X(1)$ over J_Δ. For $\Delta < -4$ there is no ramification, so we determine which residue fields occur and with what multiplicity. For $\Delta \in \{-3, -4\}$, a closed point on $X_0(\ell^a)$ in the fiber over J_Δ has ramification, of index 2 or 3 in the respective cases of $\Delta = -4$ and -3, exactly when a path in its closed point equivalence class includes a descending edge from level 0 to level 1, i.e. exactly when the path is not completely horizontal. The residue field of a closed point on a finite-type $\mathbb{Q}$-scheme is a number field that is well-determined up to isomorphism; it is not well-defined as a subfield of $\mathbb{C}$. Thus when we write that the residue field is $\mathbb{Q}(\mathfrak{f})$ for some $\mathfrak{f} \in \mathbb{Z}^+$, we mean that it is isomorphic to this field.
Without loss of generality we may take our source elliptic curve to have j-invariant j_Δ. Our task is then to:

(i) Enumerate all nonbacktracking length a paths P in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.
(ii) Sort them into closed point equivalence classes $\mathcal{C}(P)$, and record the field of moduli for each equivalence class (we record any number field isomorphic to $\mathbb{Q}(f)$ as $\mathbb{Q}(f)$).
(iii) Record how many closed point equivalence classes give rise to each field of moduli.
In §3.4 we have addressed the added subtlety in the notion of backtracking when $f_0^2\Delta_K \in \{-3, -4\}$, and in §4.2 we have provided a meaningful description of the action of complex conjugation on paths in $\mathcal{G}_{K,\ell,1}$. This provides the means to carry out our path-type analysis steps (i) through (iii), just as done in [Cl22a, §7] for $f_0^2\Delta_K < -4$. What we find is that the resulting enumeration of path types and corresponding residue fields for $f_0^2\Delta_K \in \{-3, -4\}$ is *exactly* as in [Cl22a, §7] for any given ℓ and splitting behavior of ℓ in K, and so we refer

the reader to the enumeration provided therein.

A check on the accuracy of our calculations is as follows: let $\psi : \mathbb{Z}^+ \to \mathbb{Z}^+$ be the multiplicative function such that for any prime power ℓ^a we have $\psi(\ell^a) = \ell^{a-1}(\ell+1)$. For all $N \in \mathbb{Z}^+$, we have (e.g. [CGPS22, Lemma 4.1a)])

$$\deg(X_0(N) \to X(1)) = \psi(N).$$

Letting d_φ and e_φ denote, respectively, the residual degree and ramification index of the closed point $[\varphi]$ with respect to the map $X_0(\ell^a) \to X(1)$, we must have

$$\sum_{C(\varphi)} d_\varphi \cdot e_\varphi = \psi(\ell^a) = \ell^a + \ell^{a-1},$$

where the sum extends over closed point equivalence classes of points in the fiber over J_Δ.

6. The Projective Torsion Field

Let F be a field of characteristic 0, let $E_{/F}$ be an elliptic curve, and let $N \in \mathbb{Z}^{\geq 2}$. The **projective N-torsion field** $F(\mathbb{P}E[N])$ is the kernel of the modulo N projective Galois representation, i.e., the composite homomorphism

$$\overline{\rho_N} : \mathfrak{g}_F \stackrel{\rho_N}{\to} \operatorname{Aut} E[N] \to \operatorname{Aut} \mathbb{P}E[N],$$

where $\mathbb{P}E[N]$ denotes the projectivization of the 2-dimensional $\mathbb{Z}/N\mathbb{Z}$-module $E[N](\overline{F})$. After choosing a $\mathbb{Z}/N\mathbb{Z}$-basis for $E[N]$, we may view $\overline{\rho_N}$ as a homomorphism from $\mathfrak{g}_F$ to $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. Thus $F(\mathbb{P}E[N])/F$ is a finite degree Galois extension. The projective N-torsion field of E/F is also characterized as the minimal algebraic extension of F over which all cyclic N-isogenies with source elliptic curve E are defined.

The following result is a small refinement of [BC20a, Prop. 4.5].

Proposition 6.1. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant, let $N \geq 2$, and let $E_{/K(N\mathfrak{f})}$ be a Δ-CM elliptic curve.*

a) *The following are equivalent:*
   (i) *We have $K(N\mathfrak{f})(\mathbb{P}E[N]) = K(N\mathfrak{f})$.*
   (ii) *There is a $K(N\mathfrak{f})$-rational cyclic N-isogeny $\varphi : E \to E'$, where E' is an $N^2\Delta$-CM elliptic curve.*

b) *For every Δ-CM elliptic curve $E_{/K(N\mathfrak{f})}$, there is an elliptic curve $E_0/K(N\mathfrak{f})$ with $j(E_0) = j(E)$ and such that E_0 satisfies the equivalent conditions of part a). Moreover, an elliptic curve $E'_{/K(N\mathfrak{f})}$ with $j(E') = j(E)$ satisfies the equivalent conditions of part a) if and only if E' is a quadratic twist of E_0.*

Proof. As usual, it is no loss of generality to assume that $j(E) = j_\Delta$.
a) The implication (ii) $\implies$ (i) follows from [BC20a, Prop. 4.5] and its proof. As for (i) $\implies$ (ii), we may take φ to be the dual of the isogeny $\psi : \mathbb{C}/\mathcal{O}(N^2\Delta) \to \mathbb{C}/\mathcal{O}(\Delta)$, which because of (i) must be $K(N\mathfrak{f})$-rational on E.
b) The isogeny ψ is defined over $\mathbb{Q}(N\mathfrak{f})$, hence also over $K(N\mathfrak{f})$. Since $N^2\Delta < -4$, the

$K(N\mathfrak{f})$-rational model of an elliptic curve with j-invariant $j_{N^2\Delta}$ is unique up to quadratic twist. If F is a field of characteristic different from 2, $\psi : E_1 \to E_2$ is an F-rational isogeny with kernel C, and $d \in F^\times/F^{\times 2}$, then C remains F-rational on the quadratic twist E_1^d and we have $E_1^d/C \cong_F E_2^d$. This shows that the elliptic curve E_0 of part b) exists and is unique up to quadratic twist; finally, quadratic twists do not change rationality of isogenies hence do not change projective torsion fields. □

For an imaginary quadratic discriminant Δ, let $\mathcal{O}(\Delta)$ be the imaginary quadratic order of discriminant Δ and let

$$w_\Delta := \#\mathcal{O}(\Delta)^\times.$$

Theorem 6.2. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant, and let $N \geq 3$.*

a) *Let $P \in X_0(N,N)$ be a Δ-CM closed point. Then $\mathbb{Q}(P) = K(N\mathfrak{f})$.*

b) *Let F be a field of characteristic 0, and let $E_{/F}$ be a Δ-CM elliptic curve. Then $F(\mathbb{P}E[N]) \supseteq K(N\mathfrak{f})$ and $[F(\mathbb{P}E[N]) : FK(N\mathfrak{f})] \mid \frac{\#w_\Delta}{2}$.*

Proof. Again we may assume without loss of generality that $j(P) = j_\Delta$.
a) By Proposition 6.1, there is a Δ-CM elliptic curve $E_{/K(N\mathfrak{f})}$ on which the projective modulo N Galois representation is trivial. This elliptic curve induces a Δ-CM closed point $P_0 \in X_0(N,N)$ such that $\mathbb{Q}(P_0)$ can be embedded into $K(N\mathfrak{f})$. Moreover, in the notation of [Cl22a, §1.1], the subgroup $H_0(N,N)$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ used to define the modular curve $X_0(N,N)$ is the subgroup of scalar matrices, which is normal, hence $X_0(N,N) \to X(1)$ is a Galois covering of curves over $\mathbb{Q}$. It follows that all residue fields of closed points of $X_0(N,N)$ lying over the closed point J_Δ of $X(1)$ are isomorphic. It follows that $\mathbb{Q}(P)$ is isomorphic to a subfield of $K(N\mathfrak{f})$. By [DR73, Prop. VI.3.2] there is an elliptic curve $E_{/\mathbb{Q}(P)}$ inducing P with trivial projective modulo N Galois representation. As in the proof of Proposition 6.1 we have a $\mathbb{Q}(P)$-rational isogeny $\varphi : E \to E'$ with $j(E') = j_{N^2\Delta}$, so $\mathbb{Q}(P)$ contains $\mathbb{Q}(N\mathfrak{f})$. Since $[K(N\mathfrak{f}) : \mathbb{Q}(N\mathfrak{f})] = 2$, we have either $\mathbb{Q}(P) = \mathbb{Q}(N\mathfrak{f})$ or $\mathbb{Q}(P) = K(N\mathfrak{f})$. However, if $\mathbb{Q}(P) = \mathbb{Q}(N\mathfrak{f})$, then since $\mathbb{Q}(N\mathfrak{f}) \subset \mathbb{R}$, we get a real elliiptic curve with real projective N-torsion field, contradicting [Cl22a, Cor. 5.4].
b) From part a) we know that $F(\mathbb{P}E[N]) \supseteq K(N\mathfrak{f})$. Consider the base extension of E to $L := FK(N\mathfrak{f})$. It follows from part a) that there is a character $\chi : \mathfrak{g}_L \to \mu_{w_\Delta}$ such that the twist of $E_{/L}$ by χ has trivial projective mod N Galois representation. There is then a cyclic field extension M/L of degree dividing $\frac{w_\Delta}{2}$ such that

$$\chi(\mathfrak{g}_M) \subset \{\pm 1\},$$

which means that there is a quadratic twist of $E_{/M}$ for which the projective mod N Galois representation is trivial. But quadratic twists do not affect the projective modulo N Galois representation, so the projective Galois representation on $E_{/M}$ is trivial, and $[M : FK(N\mathfrak{f})] \mid \frac{w_\Delta}{2}$. □

When $N = 2$, the projective N-torsion field of an elliptic curve $E_{/F}$ is just its 2-torsion field $F(E[2])$. Because of this the $N = 2$ analogue of Theorem 6.2 had already been known, but for future reference we record the result anyway.

Proposition 6.3. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant, let F be a field of characteristic 0, and let $E_{/F}$ be a Δ-CM elliptic curve. Let $P \in X_0(2,2)_{/\mathbb{Q}}$ be a Δ-CM point. Then:*

a) *If $\Delta < -4$ is odd, then $\mathbb{Q}(P) = K(2\mathfrak{f})$.*
b) *If $\Delta < -4$ is even, then $\mathbb{Q}(P) \cong \mathbb{Q}(2\mathfrak{f})$.*
c) *If $\Delta = -4$, then $\mathbb{Q}(P) = \mathbb{Q} = \mathbb{Q}(2\mathfrak{f})$.*
d) *If $\Delta = -3$, then $\mathbb{Q}(P) = K = K(2\mathfrak{f})$.*

Proof. Again, because $X_0(2,2) = X(2) \to X(1)$ is a Galois covering, all the residue fields of P on $X_0(2,2)$ lying over the closed point J_Δ of $X(1)$ are isomorphic.
a),b) Suppose $\Delta < -4$. The results follow from [BCS17, Thm. 4.2] together with the observation that there is a point P of order 2 on $E(\overline{F})$ such that $E/\langle P\rangle$ has 4Δ-CM. (They can also be obtained from an analysis of 2-isogeny graphs.)
c) The -4-CM elliptic curve $E : y^2 = x^3 - x$ has $\mathbb{Q}(E[2]) = \mathbb{Q}$.
d) For all $B \in \mathbb{Q}^\times$, the curve

$$E_B : y^2 = x^3 + B$$

is a -3-CM elliptic curve with $\mathbb{Q}([E])2) = \mathbb{Q}(\zeta_3, B^{1/3})$. Each of these fields contains $\mathbb{Q}(\zeta_3) = K$, so $\mathbb{Q}(P) \supseteq K$. Moreover $\mathbb{Q}(E_1) = K$, so $\mathbb{Q}(P) = K$. □

7. Primitive Residue Fields of CM points on $X_0(\ell^{a'}, \ell^a)$

Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant, let ℓ be a prime and let $0 \le a' \le a$ be integers. In this section we extend the work of [Cl22a, §7], determining all primitive residue fields and degrees of Δ-CM points on $X_0(\ell a', \ell^a)$, to the cases in which $\Delta_K \in \{-3, -4\}$.

It is no loss of generality to assume that the j-invariant of our Δ-CM elliptic curve is j_Δ, and we shall do so throughout this section.

For $X(H)_{/\mathbb{Q}}$ a modular curve, we call the residue field $\mathbb{Q}(P)$ of a closed Δ-CM point $P \in X(H)$ a **primitive residue field** of Δ-CM points on $X(H)$ if there is no other Δ-CM point $Q \in X(H)$ together with an embedding of the residue field $\mathbb{Q}(Q)$ into $\mathbb{Q}(P)$ as a proper subfield. We call the degree $d = [\mathbb{Q}(P) : \mathbb{Q}]$ a **primitive degree** of Δ-CM points on $X(H)$ if there is no Δ-CM point $Q \in X(H)$ such that $[\mathbb{Q}(Q) : \mathbb{Q}]$ properly divides d.

Throughout this section, when working with a $\Delta = \mathfrak{f}^2\Delta_K$-CM point we put

$$L \coloneqq \mathrm{ord}_\ell(\mathfrak{f}).$$

7.1. $X_0(\ell^a)$**.** In the case of $a' = 0$, i.e., of $X_0(\ell^a)$, our results of §5 imply immediately that the case analysis is exactly as in [Cl22a, §8.1]. We recall the answer here for completeness:

Case 1.1: Suppose $\ell^a = 2$.
Case 1.1a: Suppose $\left(\frac{\Delta}{2}\right) \neq -1$. The primitive residue field is $\mathbb{Q}(\mathfrak{f})$ (which equals $\mathbb{Q}(2\mathfrak{f})$

when $\left(\frac{\Delta}{2}\right) = 1$).
Case 1.1b: Suppose $\left(\frac{\Delta}{2}\right) = -1$. The primitive residue field is $\mathbb{Q}(2\mathfrak{f})$.
Case 1.2: Suppose $\ell^a > 2$ and $\left(\frac{\Delta}{\ell}\right) = 1$. The primitive residue fields are $\mathbb{Q}(\ell^a\mathfrak{f})$ and $K(\mathfrak{f})$.
Case 1.3: Suppose $\ell^a > 2$ and $\left(\frac{\Delta}{\ell}\right) = -1$. The primitive residue field is $\mathbb{Q}(\ell^a\mathfrak{f})$.
Case 1.4: Suppose $\ell^a > 2$, $\left(\frac{\Delta}{\ell}\right) = 0$ and $L = 0$. The primitive residue field is $\mathbb{Q}(\ell^{a-1}\mathfrak{f})$.
Case 1.5: Suppose $\ell > 2$, $L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$.
Case 1.5a: Suppose $a \leq 2L$. In this case there is a $\mathbb{Q}(\mathfrak{f})$-rational cyclic ℓ^a-isogeny, so the only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.5b: Suppose $a > 2L$. Then the primitive residue fields are $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$ and $K(\mathfrak{f})$.
Case 1.6: Suppose $\ell > 2$, $L \geq 1$, and $\left(\frac{\Delta_K}{\ell}\right) = -1$.
Case 1.6a: Suppose $a \leq 2L$. As in Case 1.5a, there is a $\mathbb{Q}(\mathfrak{f})$-rational cyclic ℓ^a-isogeny, so the only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.6b: Suppose $a > 2L$. In this case the primitive residue field is $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$.
Case 1.7: Suppose $\ell > 2$, $L \geq 1$, $\left(\frac{\Delta_K}{\ell}\right) = 0$.
Case 1.7a: Suppose $a \leq 2L+1$. As in Case 1.5a, there is a $\mathbb{Q}(\mathfrak{f})$-rational cyclic ℓ^a-isogeny, so the only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.7b: Suppose $a \geq 2L+2$. In this case the primitive residue field is $\mathbb{Q}(\ell^{a-2L-1}\mathfrak{f})$.
Case 1.8: Suppose $\ell = 2$, $a \geq 2$, $L \geq 1$, and $\left(\frac{\Delta_K}{2}\right) = 1$.
Case 1.8a: Suppose $L = 1$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(\mathfrak{f})$.
Case 1.8b: Suppose $L \geq 2$ and $a \leq 2L-2$. The primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.8c: Suppose $L \geq 2$ and $a \geq 2L-1$. The primitive residue fields are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(\mathfrak{f})$.
Case 1.9: Suppose $\ell = 2$, $a \geq 2$, $L \geq 1$, and $\left(\frac{\Delta_K}{2}\right) = -1$.
Case 1.9a: Suppose $L = 1$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-2}\mathfrak{f})$.
Case 1.9b: Suppose $L \geq 2$ and $a \leq 2L-2$. The primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.9c: Suppose $L \geq 2$ and $a \geq 2L-1$. The primitive residue fields are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2^{\max(a-2L,0)}\mathfrak{f})$.
Case 1.10: Suppose $\ell = 2$, $a \geq 2$, $L \geq 1$, $\left(\frac{\Delta_K}{2}\right) = 0$, and $\mathrm{ord}_2(\Delta_K) = 2$.
Case 1.10a: Suppose $a \leq 2L$. The primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.10b: Suppose $a \geq 2L+1$. The primitive residue fields are $\mathbb{Q}(2^{a-2L}\mathfrak{f})$ and $K(2^{a-2L-1}\mathfrak{f})$.
Case 1.11: Suppose $\ell = 2$, $a \geq 2$, $L \geq 1$, $\left(\frac{\Delta_K}{2}\right) = 0$, and $\mathrm{ord}_2(\Delta_K) = 3$.
Case 1.11a: Suppose $a \leq 2L+1$. The primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 1.11b: Suppose $a \geq 2L+2$. The primitive residue field is $\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$.

7.2. **A field of moduli result.** Now suppose that $1 \leq a' \leq a$ are integers, and let $P \in X_0(\ell^{a'}, \ell^a)$ be a closed Δ-CM point. Then we have morphisms

$$\alpha : X_0(\ell^{a'}, \ell^a) \to X_0(\ell^{a'}, \ell^{a'}) \text{ and } \beta : X_0(\ell^{a'}, \ell^a) \to X_0(\ell^a).$$

Theorem 7.1. *Let ℓ be a prime number, let $1 \leq a' \leq a$ be positive integers and let $P \in X_0(\ell^{a'}, \ell^a)$ be a closed Δ-CM point.*

a) *We have*
$$\mathbb{Q}(\alpha(P), \beta(P)) \subseteq \mathbb{Q}(P) \subseteq K(\alpha(P), \beta(P)).$$
b) *We have $\mathbb{Q}(P) = \mathbb{Q}(\alpha(P), \beta(P))$ if* any *of the following conditions holds:*
(i) $\Delta \neq -4$.
(ii) $\ell^{a'} \geq 3$.
(iii) $a = 1$.

Proof. Since $\mathbb{Q}(P)$ is an extension of both $\mathbb{Q}(\alpha(P))$ and $\mathbb{Q}(\beta(P))$, clearly
$$\mathbb{Q}(P) \supseteq \mathbb{Q}(\alpha(P), \beta(P)).$$
If $\Delta < -4$, then conversely $\mathbb{Q}(P) \subseteq \mathbb{Q}(\alpha(P), \beta(P))$: indeed, in this case, the projective torsion field is independent of the model. So we may suppose $\Delta \in \{-3, -4\}$.
Step 2: We will show that
$$K(\alpha(P), \beta(P)) = K(\ell^{a'}\mathfrak{f})K(\beta(P)). \tag{4}$$
Since $\Delta \in \{-3, -4\}$, the point $\beta(P) \in X_0(\ell^a)$ corresponds to a path of length a with initial vertex at the surface; if the terminal vertex has level L', then $K(\beta(P)) = K(\ell^{L'})$, so if we put
$$\overline{L} \coloneqq \max(a', L'),$$
then
$$K(\alpha(P), \beta(P)) = K(\ell^{\overline{L}}).$$
We may factor an isogeny inducing $\beta(P)$ as $\varphi_d \circ \varphi_h$ where φ_h is horizontal and φ_d is descending of length L'. By the results of §6, there is an elliptic curve $E_{/K(\ell^{\overline{L}})}$ with j-invariant j_Δ on which the modulo $\ell^{\overline{L}}$ Galois representation is given by scalar matrices. The point $\beta(P)$ is induced by a cyclic ℓ^a-isogeny of $\mathbb{C}$-elliptic curves $\varphi : E \to E'$; since $\Delta = \Delta_K$, this isogeny factors as $\varphi_d \circ \varphi_h$, where $\varphi_h : E \to E''$ is horizontal of degree $\ell^{a-L'}$ and $\varphi_d : E'' \to E'$ is descending of degree $\ell^{L'}$. We claim that every isogeny of this form is defined over $K(\ell^{\overline{L}})$. Indeed, as in the proof of Theorem 4.1 we have that φ_h is defined over $K(\ell^{\overline{L}})$ and moreover $E'' \cong_{K(\ell^{\overline{L}})} E$. It follows that the modulo $\ell^{L'}$-Galois representation on E'' is given by scalar matrices, so φ_d is also defined over $K(\ell^{\overline{L}})$ and thus φ is as well.
Step 3: By Theorem 6.2 and Proposition 6.3 we have that $\mathbb{Q}(\alpha(P)) = K(\ell^{a'}\mathfrak{f})$ if either $\ell^{a'} \geq 3$ or Δ is odd. Thus in either of these cases we have
$$\mathbb{Q}(P) = K(\ell^{a'}\mathfrak{f})\mathbb{Q}(\beta(P)). \tag{5}$$
Step 4: Finally, if $a = 1$ then $\alpha : X_0(2,2) \to X_0(2)$ is the identity map, so $\mathbb{Q}(P) = \mathbb{Q}(\alpha(P))$ holds trivially. □

Corollary 7.2. *Let $a \geq 2$, and let $P \in X_0(2, 2^a)$ be a -4-CM point. Let $\varphi : E \to E'$ be an isogeny of complex elliptic curves inducing $\beta(P) \in X_0(2^a)$.*

a) *If φ is purely descending, then $\mathbb{Q}(P) = \mathbb{Q}(\beta(P)) \cong \mathbb{Q}(2^a)$.*

b) *Otherwise,* $\mathbb{Q}(P) = K(\beta(P)) = K(2^{a-1})$.

Proof. Since $j_E = 1728$, there are precisely two possibilities for φ: it either consists of a descending edges, or it has one horizontal edge followed by $a-1$ descending edges.

In the former case, we have $\mathbb{Q}(\varphi) \cong \mathbb{Q}(2^a)$. Moreover, on the model of E that makes φ $\mathbb{Q}(\varphi)$-rational, we evidently have a descending $\mathbb{Q}(\varphi)$-rational 2-isogeny. As for any -4-CM elliptic curve defined over $\mathbb{Q}(\varphi)$, we have a horizontal $\mathbb{Q}(\varphi)$-rational 2-isogeny. Thus the $\mathfrak{g}_{\mathbb{Q}(\varphi)}$-action on the three order 2 subgroup schemes of E fixes two of the subgroups, so it must also fix the third. We conclude that $\mathbb{Q}(P) = \mathbb{Q}(\beta(P))$ in this case.

Now suppose that φ consists of a horizontal edge followed by $a-1 \geq 1$ descending edges. Now $\mathbb{Q}(\varphi) \cong \mathbb{Q}(2^{a-1})$, which is real number field, so if $\mathbb{Q}(P) = \mathbb{Q}(\beta(P))$ then we would have $\mathbb{Q}(P) \cong \mathbb{Q}(2^{a-1})$, a real number field. But as we saw in §4.2, the horizontal 2-isogeny $\iota : E \to E'$ on a real ellliptic curve with j-invariant 1728 interchanges the two $\mathbb{R}$-structures on this elliptic curve, and on precisely one of the two $\mathbb{R}$-structures do we have an $\mathbb{R}$-rational descending 2-isogeny. If $\mathbb{Q}(P) \subseteq \mathbb{R}$ then we would have $\mathbb{R}$-rational descending 2-isogenies defined on both the source and target of ι, which is not possible. Therefore in this case $\mathbb{Q}(P) \supseteq \mathbb{Q}(\beta(P))$, so by Theorem 7.1 we have $\mathbb{Q}(P) = K(\beta(P)) = K(2^{a-1})$. □

7.3. $X_0(\ell^{a'}, \ell^a)$**.** Using Theorem 7.1, Corollary 7.2 and the work of §5 and §6, it is easy to compute all primitive residue fields $\mathbb{Q}(P)$ of Δ-CM points $P \in X_0(\ell^{a'}, \ell^a)$. Indeed:

• Suppose $\ell^{a'} \geq 3$. Then for any Δ-CM point $P \in X_0(\ell^{a'}, \ell^a)$, equation (5) applies. So if L' is the minimal level such that there is a nonbacktracking path in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ starting in level L (where $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$), the unique primitive residue field is $K(\ell^{\max(a',L')})$. So:

Case 2.1: If $\left(\frac{\Delta_K}{\ell}\right) = 1$, the primitive residue field is $K(\ell^{a'}\mathfrak{f})$.
Case 2.2: If $\left(\frac{\Delta_K}{\ell}\right) = -1$, the primitive residue field is $K(\ell^{\max(a',a-2L)}\mathfrak{f})$.
Case 2.3: If $\left(\frac{\Delta_K}{\ell}\right) = 0$, the primitive residue field is $K(\ell^{\max(a',a-2L-1)}\mathfrak{f})$.

• Suppose $\ell^{a'} = 2$ and Δ is odd. Again equation (5) applies and the unique primitive residue field is $K(2^{\max(a',L')}\mathfrak{f}) = K(2^{\max(1,L')}\mathfrak{f})$. So:

Case 3.1: If $a = 1$, the primitive residue field is $K(2\mathfrak{f})$.
Case 3.2: If $a \geq 2$ and $\left(\frac{\Delta}{2}\right) = 1$, the primitive residue field is $K(2\mathfrak{f}) = K(\mathfrak{f})$.
Case 3.3: If $a \geq 2$ and $\left(\frac{\Delta}{2}\right) = -1$, the primitive residue field is $K(2^a\mathfrak{f})$.

• Suppose $\ell^{a'} = 2$ and Δ is even. For a Δ-CM point $P \in X_0(2, 2^a)$ Theorem 7.1 and Corollary 7.2 tell us that if $\Delta \neq -4$, if $a = 1$ or if an isogeny φ inducing $\beta(P)$ is purely descending then

$$\mathbb{Q}(P) = \mathbb{Q}(\alpha(P), \beta(P)),$$

and otherwise we have $\mathbb{Q}(P) = K(2^{a-1}) = K(2^{a-1}\mathfrak{f})$.

Our casework for Δ-CM points on $X_0(2, 2^a)$ is then as follows:

Case 4.0: $a = 1$. The primitive residue field is $\mathbb{Q}(2\mathfrak{f})$.

Case 4.1: $a \geq 2$, $L = 0$ and $\mathrm{ord}_2(\Delta_K) = 2$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-1}\mathfrak{f})$.
Case 4.2: $a \geq 2$, $L = 0$ and $\mathrm{ord}_2(\Delta_K) = 3$. The primitive residue field is $\mathbb{Q}(2^{a-1}\mathfrak{f})$.
Case 4.3: $a \geq 2$, $L = 1$ and $\left(\frac{\Delta_K}{2}\right) = 1$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2\mathfrak{f})$.
Case 4.4: $\left(\frac{\Delta_K}{2}\right) = 1$, $L \geq 2$ and $2 \leq a \leq 2L - 1$. The primitive residue field is $\mathbb{Q}(2\mathfrak{f})$.
Case 4.5: $\left(\frac{\Delta_K}{2}\right) = 1$, $L \geq 2$ and $a \geq 2L$. The primitive residue fields are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2\mathfrak{f})$.
Case 4.6: $\left(\frac{\Delta_K}{2}\right) = -1$, $L = 1$ and $a = 2$. The primitive residue fields are $\mathbb{Q}(2^2\mathfrak{f})$ and $K(2\mathfrak{f})$.
Case 4.7: $\left(\frac{\Delta_K}{2}\right) = -1$, $L = 1$ and $a \geq 3$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-2}\mathfrak{f})$.
Case 4.8: $\left(\frac{\Delta_K}{2}\right) = -1$, $L \geq 2$ and $2 \leq a \leq 2L - 1$. The primitive residue field is $\mathbb{Q}(2\mathfrak{f})$.
Case 4.9: $\left(\frac{\Delta_K}{2}\right) = -1$, $L \geq 2$ and $a = 2L$. The primitive residue fields are $\mathbb{Q}(2^2\mathfrak{f})$ and $K(2\mathfrak{f})$.
Case 4.10: $\left(\frac{\Delta_K}{2}\right) = -1$, $L \geq 2$ and $a \geq 2L + 1$. The primitive residue fields are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2^{a-2L}\mathfrak{f})$.
Case 4.11: $\mathrm{ord}_2(\Delta_K) = 2$, $L \geq 1$ and $2 \leq a \leq 2L+1$. The primitive residue field is $\mathbb{Q}(2\mathfrak{f})$.
Case 4.12: $\mathrm{ord}_2(\Delta_K) = 2$, $L \geq 1$ and $a \geq 2L + 2$. The primitive residue fields are $\mathbb{Q}(2^{a-2L}\mathfrak{f})$ and $K(2^{a-2L-1}\mathfrak{f})$.
Case 4.13: $\mathrm{ord}_2(\Delta_K) = 3$, $L \geq 1$ and $2 \leq a \leq 2L+1$. The primitive residue field is $\mathbb{Q}(2\mathfrak{f})$.
Case 4.14: $\mathrm{ord}_2(\Delta_K) = 3$, $L \geq 1$ and $a \geq 2L + 2$. The primitive residue field is $\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$.

8. CM points on $X_0(M, N)_{/\mathbb{Q}}$

Throughout this section $\Delta = \mathfrak{f}^2\Delta_K$ is an imaginary quadratic discriminant with $\Delta_K \in \{-3, -4\}$, and $M \mid N$ are positive integers. We now discuss how to use our work developed thus far to determine the Δ-CM locus on $X_0(M, N)_{/\mathbb{Q}}$. In §8.1 we recall how the compiling across prime powers process works for $\Delta < -4$, and in §8.2 we provide a result for compiling across prime powers for $\Delta \in \{-3, -4\}$. In the remainder of this section, we give an explicit description of all primitive residue fields and primitive degrees in this case.

8.1. **Compiling Across Prime Powers with $\Delta < -4$.** For this section, we suppose $\Delta < -4$ with $\Delta_K \in \{-3, -4\}$. With this assumption, [Cl22a, Prop. 3.5] applies and

our compiling across prime powers process works much the same as in [Cl22a, §9.1]. We elaborate here for completeness of our discussion.

For a prime ℓ and integers $0 \le a' \le a$, the fiber F of $X_0(\ell^{a'}, \ell^a) \to X(1)$ over the closed point J_Δ is a finite étale $\mathbb{Q}(J_\Delta)$-scheme, i.e. is isomorphic to a product of finite degree field extensions of $\mathbb{Q}(\mathfrak{f})$. Our work up to now shows that the residue field of any CM point on $X_0(\ell^{a'}, \ell^a)$ is either a ring class field or a rational ring class field, and so there are non-negative integers $b_0, \ldots, b_a, c_1, \ldots, c_a$ such that $F \cong \operatorname{Spec} A$, where

$$A = \prod_{j=0}^{a} \mathbb{Q}(\ell^j \mathfrak{f})^{b_j} \times \prod_{k=0}^{a} K(\ell^k \mathfrak{f})^{c_k}. \tag{6}$$

When $a' = 0$, the explicit values of the b_j's and c_k's can be determined from our results in §5. When $\ell^{a'} \ge 3$ or Δ is odd, by Theorem 6.2 we have $b_j = 0$ for all $0 \le j \le a$.

We now explain how the previous results allow us to compute the fiber $F = \operatorname{Spec} A$ of $X_0(M, N) \to X(1)$ over J_Δ for any positive integers $M \mid N$, where $M = \ell_1^{a_1'} \cdots \ell_r^{a_r'}$ and $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For $1 \le i \le r$, let $F_i \cong \operatorname{Spec} A_i$ be the fiber of $X_0(\ell_i^{a_i'}, \ell_i^{a_i}) \to X(1)$ over J_Δ. By [Cl22a, Prop 3.5] we have

$$A \cong A_1 \otimes_{\mathbb{Q}(J_\Delta)} \cdots \otimes_{\mathbb{Q}(J_\Delta)} A_r. \tag{7}$$

It follows that A is isomorphic to a direct sum of terms of the form

$$B \coloneqq B_1 \otimes_{\mathbb{Q}(\mathfrak{f})} \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} B_r,$$

where for $1 \le i \le r$ we have that B_i is isomorphic to either $\mathbb{Q}(\ell_i^{j_i}\mathfrak{f})$ for some $0 \le j_i \le a$ or to $K(\ell^{j_i}\mathfrak{f})$ for some $0 \le j_i \le a$.

Let s be the number of indices $1 \le i \le r$ such that K is contained in B_i, i.e. such that $B_i \cong K(\ell_i^{j_i})$. Because $\mathfrak{f} > 1$, Proposition 2.2 gives:f

$$B \cong \begin{cases} \mathbb{Q}(\ell_1^{j_1} \cdots \ell_r^{j_r}\mathfrak{f}) & \text{if } s = 0 \\ K(\ell_1^{j_1} \cdots \ell_r^{j_r}\mathfrak{f})^{2^{s-1}} & \text{otherwise.} \end{cases}$$

(Note that $\ell_i^{2j_i}\Delta \in \{-12, -16, -27\}$ can only occur if $j_i = 0$, due to our $\mathfrak{f} > 1$ assumption.) We therefore reach the following extension of [Cl22a, Theorem 9.1]:

Theorem 8.1. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant with $\Delta < -4$. Let $M \mid N \in \mathbb{Z}^+$. Let P be a Δ-CM closed point on $X_0(M, N)$.*

a) *The residue field $\mathbb{Q}(P)$ is isomorphic to either $\mathbb{Q}(M\mathfrak{f})$ or $K(M\mathfrak{f})$ for some $M \mid N$.*

b) *Let $M = \ell_1^{a_1} \cdots \ell_r^{a_r}$, $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ be the prime power decompositions of M and N. For $1 \le i \le r$, let $\pi_i : X_0(M, N) \to X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ be the natural map and put $P_i \coloneqq \pi_i(P)$. The following are equivalent:*

(i) *The field $\mathbb{Q}(P)$ is formally real.*

(ii) *The field $\mathbb{Q}(P)$ does not contain K.*

(iii) *For all $1 \le i \le r$, the field $\mathbb{Q}(P_i)$ is formally real.*

iv) *For all $1 \le i \le r$, the field $\mathbb{Q}(P_i)$ does not contain K.*

8.2. **Compiling Across Prime Powers with $\Delta \in \{-3,-4\}$.** Throughout this section, we assume that $\Delta \in \{-3,-4\}$.

Proposition 8.2. *Suppose that $\varphi : E \to E'$ is a cyclic N-isogeny, with N having prime-power factorization $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For each $i \in \{1,\dots,r\}$, let $\varphi_i : E \to E_i$ be the ℓ_i-primary part of φ. Let b_i such that $\mathbb{Q}(\varphi_i)$ is isomorphic to either $K(\ell_i^{b_i})$ or to $\mathbb{Q}(\ell_i^{b_i})$. Then*

$$\mathbb{Q}(\ell_1^{b_1} \cdots \ell_r^{b_r}) \subseteq \mathbb{Q}(\varphi) \subseteq K(\ell_1^{b_1} \cdots \ell_r^{b_r}).$$

Proof. Let $C = \ker(\varphi)$, and for each $i \in \{1,\dots,r\}$ let $C_i \leq C$ be the Sylow-ℓ_i subgroup of C, that is $C_i = \ker(\varphi_i)$. Let $\mathfrak{f}$ denote the conductor of $\mathrm{End}(E)$, and for $1 \leq i \leq r$ let $\mathfrak{f}_i$ denote the conductor of $\mathrm{End}(E_i)$. Let

$$\mathcal{I} = \{i \mid \mathrm{ord}_{\ell_i}(\mathfrak{f}_i) > \mathrm{ord}_{\ell_i}(\mathfrak{f}))\} \subseteq \{1,\dots,r\},$$

and let

$$C' = \left\langle \{C_i\}_{i \in \mathcal{I}} \right\rangle \subseteq C.$$

Then φ factors as $\varphi = \varphi'' \circ \varphi'$, where $\varphi' : E \to E/C'$. Using the fact that isogenies of degree prime to ℓ_i cannot change the ℓ_i-part of the conductor, we see that $\mathrm{End}(E/C')$ has conductor divisible by $\ell_1^{b_1} \cdots \ell_r^{b_r}$. Thus we have

$$\mathbb{Q}(\ell_1^{b_1} \cdots \ell_r^{b_r}) \subseteq \mathbb{Q}(\varphi') \subseteq \mathbb{Q}(\varphi).$$

It remains to show the containment $\mathbb{Q}(\varphi) \subseteq K(\ell_1^{b_1} \cdots \ell_r^{b_r})$. If $j(E) \notin \{0, 1728\}$, then this follows from Theorem 4.1 and [Cl22a, Prop. 3.5], so we suppose $j(E) \in \{0, 1728\}$. If $j(E') = j(E)$, then φ is (up to isomorphism on the target) an endomorphism of E, hence defined over K. If $j(E') \neq j(E)$ then $j(E') \notin \{0, 1728\}$, so our previous work applies via consideration of the dual isogeny as $\mathbb{Q}(\varphi) \cong \mathbb{Q}(\varphi^\vee)$. □

Proposition 8.2 provides bounds on the field of moduli of an isogeny. We now use this result to determine the exact field of moduli in the case where our source elliptic curve has -3-CM or -4-CM, which we state from the perspective of determining the residue field of the corresponding CM point on $X_0(N)$.

Theorem 8.3. *Let $N \in \mathbb{Z}^+$ with prime-power factorization $\ell_1^{a_1} \cdots \ell_r^{a_r}$, and suppose $x \in X_0(N)$ is a Δ-CM point with $\Delta \in \{-3,-4\}$. Let $\pi_i : X_0(N) \to X_0(\ell_i^{a_i})$ be the natural map, and let $x_i = \pi_i(x)$. Let P_i be any path in the closed point equivalence class corresponding to x_i in $\mathcal{G}_{K,\ell_i,1}$, and let $d_i \geq 0$ be the number of descending edges in P_i.*

a) *If there is some $1 \leq i \leq r$ such that ℓ_i splits in K and the path P_i contains a surface edge, then*

$$\mathbb{Q}(x) = K(\ell_1^{d_1} \cdots \ell_r^{d_r}).$$

b) *In every other case, we have*

$$\mathbb{Q}(x) \cong \mathbb{Q}(\ell_1^{d_1} \cdots \ell_r^{d_r}).$$

Proof. Let $\varphi : E \to E'$ be a cyclic N-isogeny inducing the point x. For each $1 \leq i \leq r$, let $\varphi_i : E \to E_i$ be the ℓ_i-primary part of φ: that is, the kernel of φ_i is the ℓ_i-Sylow subgroup of the kernel of φ.
Case 1: Suppose that E' is also a Δ_K-CM elliptic curve. By [Cl22a, §3.4], the isogeny φ is isomorphic over $\mathbb{C}$ to $E \to E/[I]$ for a nonzero ideal I of $\mathbb{Z}_K$, and we have $\mathbb{Q}(\varphi) \cong \mathbb{Q}(j(E)) = \mathbb{Q}$ if I is real ideal (i.e., $I = \overline{I}$) and $\mathbb{Q}(\varphi) = K(j(E)) = K$ is I is not a real ideal. If we factor $I = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r}$ into prime powers and $\mathfrak{p}_i$ lies over ℓ_i, then we have (up to an isomorphism on the target) that $\varphi_i : E \to E/[\mathfrak{p}_i^{c_i}]$. Notice that the path in $\mathcal{G}_{K,\ell_i,1}$ corresponding to φ_i lies entirely on the surface. If some ℓ_i splits in K, then $\mathfrak{p}_i^{c_i}$ is not a real ideal, so $\mathbb{Q}(\varphi) = K$. If no ℓ_i splits in K, then each $\mathfrak{p}_i^{c_i}$ is real, so I is real and $\mathbb{Q}(\varphi) = \mathbb{Q}$.
Case 2: Otherwise E' is a $\Delta = \mathfrak{f}^2\Delta_K$-CM elliptic curve for some $\mathfrak{f} > 1$. Since $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi^\vee)$, we may compute the field of moduli of the dual isogeny $\varphi^\vee : E' \to E$. Since $\operatorname{Aut} E' = \{\pm 1\}$, the rationality of a subgroup of E' is independent of the model, so we have $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi_1) \cdots \mathbb{Q}(\varphi_r)$, and the result now follows from [Cl22a, Thm. 5.1]. □

Corollary 8.4. *Let $\varphi : E \to E'$ be an isogeny of K-CM elliptic curves defined over $\mathbb{C}$. Let $\mathfrak{f}$ (resp. $\mathfrak{f}'$) be the conductor of $\operatorname{End}(E)$ (resp. of $\operatorname{End}(E')$). Then the field of moduli $\mathbb{Q}(\varphi)$ of φ contains a subfield isomorphic to $\mathbb{Q}(\operatorname{lcm}(\mathfrak{f}, \mathfrak{f}'))$.*

Proof. Theorems 8.1 and 8.3 imply that $\mathbb{Q}(\varphi)$ is isomorphic to $\mathbb{Q}(M\mathfrak{f})$ or $K(M\mathfrak{f})$ for some $M \in \mathbb{Z}^+$. Using the fact that $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi^\vee)$ we find that $\mathfrak{f}' \mid M\mathfrak{f}$, and the result follows. □

When $\Delta_K < -4$, then Corollary 8.4 holds just because $\mathbb{Q}(\iota) \supseteq \mathbb{Q}(j(E), j(E'))$. However:

Corollary 8.5. *Let $\Delta_K \in \{-3, -4\}$, let $\mathfrak{f}, \mathfrak{f}'$ be coprime positive integers not lying in the set S of Proposition 2.1: that is, if $\Delta_K = -3$ then $\mathfrak{f}, \mathfrak{f}' > 3$ and if $\Delta_K = -4$ then $\mathfrak{f}, \mathfrak{f}' > 2$. Let $\varphi : E \to E'$ be an isogeny of K-CM elliptic curves defined over $\mathbb{C}$ such that $\operatorname{End}(E)$ has conductor $\mathfrak{f}$ and $\operatorname{End}(E')$ has conductor $\mathfrak{f}'$. Then φ cannot be defined over $K(j(E), j(E'))$.*

Proof. This follows from Corollary 8.4 and Proposition 2.1. □

Next we obtain a version of Theorem 8.3 in the $M \geq 2$ case, finding in particular that the residue field of a CM point on $X_0(M, N)$ is isomorphic to either a rational ring class field or a ring class field in all cases.

Theorem 8.6. *Let $M, N \in \mathbb{Z}^{\geq 2}$ with $M \mid N$, and write*

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

Let

$$\alpha : X_0(M, N) \to X_0(M, M), \ \beta : X_0(M, N) \to X_0(N)$$

and

$$\forall 1 \leq i \leq r, \ \pi_i : X_0(N) \to X_0(\ell_i^{a_i})$$

be the canonical maps. Let $\Delta \in \{-3, -4\}$, let P be a Δ-CM closed point of $X_0(M, N)$ and let $y_i \coloneqq \pi_i(\beta(P))$. Let d_i be the number of descending edges in y_i, and put

$$\overline{d_i} \coloneqq \max(a_i', d_i).$$

a) *Suppose $M \geq 3$ or ($M = 2$ and $\Delta = -3$). Then*

$$\mathbb{Q}(P) = K(\ell_1^{\overline{d_1}} \cdots \ell_r^{\overline{d_r}}).$$

b) *Suppose $M = 2$ and $\Delta = -4$; we put $\ell_1 = 2$.*

(i) *If $a_1 \geq 2$ and $y_1 \in X_0(2^a)$ is not purely descending, then*

$$\mathbb{Q}(P) = K(\ell_1^{\overline{d_1}} \cdots \ell_r^{\overline{d_r}}).$$

(ii) *Otherwise, we have*

$$\mathbb{Q}(P) \cong \begin{cases} K(2^{a_1} \cdot \ell_2^{d_2} \cdots \ell_r^{d_r}) & \text{if } K \subseteq \mathbb{Q}(y_i) \text{ for some } 2 \leq i \leq r, \\ \mathbb{Q}(2^{a_1} \cdot \ell_2^{d_2} \cdots \ell_r^{d_r}) & \text{otherwise.} \end{cases}$$

Proof. a) Our hypotheses on M imply (cf. §6) that

$$\mathbb{Q}(\alpha(P)) = K(\ell_1^{a_1'} \cdots \ell_r^{a_r'}).$$

In particular, this implies that $\mathbb{Q}(P) \supset K$. Applying Proposition 8.3 we get

$$K(\beta(P)) = K(\ell_1^{d_1} \cdots \ell_r^{d_r}).$$

Using this and Proposition 2.1a), we get:

$$\mathbb{Q}(P) \supseteq \mathbb{Q}(\alpha(P), \beta(P)) = K(\alpha(P), \beta(P)) = K(\ell_1^{a_1'} \cdots \ell_r^{a_r'}) K(\ell_1^{d_1} \cdots \ell_r^{d_r}) = K(\ell_1^{\overline{d_1}} \cdots \ell_r^{\overline{d_r}}).$$

Conversely, using Proposition 6.1, let $E_{/K(\ell_1^{\overline{d_1}} \cdots \ell_r^{\overline{d_r}})}$ be an elliptic curve with j-invariant j_Δ and with modulo $\ell_1^{\overline{d_1} \cdots \overline{d_r}}$-Galois representation given by scalar matrices. For $1 \leq i \leq r$, let $\varphi_i : E \to E_i$ be a cyclic $\ell_i^{a_i}$-isogeny of $\mathbb{C}$-elliptic curves containing d_i descending edges. It follows from the proof of Theorem 7.1, that the kernel C_i of φ_i is a $K(\ell_1^{\overline{d_1}} \cdots \ell_r^{\overline{d_r}})$-rational subgroup scheme, hence so is $C = \langle C_1, \ldots, C_r \rangle$, which is the kernel of φ. Thus we have found a $K(\ell_1^{\overline{d_1}} \cdots \ell_r^{\overline{d_r}})$-rational model of P.

b) (i) By Corollary 7.2, we have $\mathbb{Q}(P) \supseteq K$. The rest of the argument is the same as that of part a).

(ii) First, suppose that y_1 is purely descending and let $\varphi : E \to E'$ be an isogeny defined over $\mathbb{Q}(\beta(P))$ that induces the point $\pi_1(\beta(P)) \in X_0(2^{a_1})$. Then the initial edge of φ is downward, so as in the proof of Corollary 7.2 every order 2 subgroup of E is $\mathbb{Q}(\beta(P))$-rational. This provides $\mathbb{Q}(P) = \mathbb{Q}(\beta(P))$, and the stated isomorphism then follows from Proposition 8.3.

Lastly, suppose that $a_1 = 1$ and that the 2-isogeny inducing y_1 is horizontal. This final case can be reduced to the previous one via automorphisms of the modular curve $X_0(2, N)$. Indeed, observe that the map $\pi : X_0(2, N) \to X_0(\frac{N}{2})$ is a $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ Galois cover. The level N-structure associated to $X_0(2, N)$ may viewed as an elliptic curve equipped with an ordered triple (C, C_1, C_2), where C is a cyclic subgroup of E of order $\frac{N}{2}$ and C_1 and C_2 are distinct cyclic subgroups of E of order 2. The map π can then be viewed as $(E, C, C_1, C_2) \mapsto (E, \langle C, C_1 \rangle)$. The $GL_2(\mathbb{Z}/2\mathbb{Z})$ action fixes E and C, and on the pair (C_1, C_2) the action is the natural and simply transitive one on pairs of order 2 subgroups of

$E[2]$. Therefore if $P \in X_0(2,N)$ is induced by a tuple (E, C, C_1, C_2) with C_1 a horizontal 2-isogeny, then C_2 is necessarily descending and we have $\mathbb{Q}(P) = \mathbb{Q}(P')$ where P' is induced by (E, C, C_2, C_1). By the previous case, we have that

$$\mathbb{Q}(P') = \mathbb{Q}(\beta(P'))$$

is the field of moduli of the isogeny $E \to E/\langle C, C_2\rangle$. Again, the stated isomorphism follows via Proposition 8.3. □

Theorems 8.3 and 8.6 are the key ingredients for the determination of primitive residue fields and primitive degrees of Δ-CM points on $X_0(M,N)$, which we will provide in the next section. However, there remains the problem of computing the set of all Δ-CM points on $X_0(M,N)$ with a given rational ring class field or ring class field as residue field. The following results solve this problem.

Theorem 8.7. *Let $N \in \mathbb{Z}^{\geq 2}$ have prime power factorization $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For $1 \leq i \leq r$, let $P_i \in X_0(\ell_i^{a_i})$ be a Δ-CM point, and let $\pi_i : X_0(N) \to X_0(\ell_i^{a_i})$ denote the natural map. Let $\mathcal{F}$ be the set of closed points $P \in X_0(N)$ such that $\pi_i(P) = P_i$ for all $1 \leq i \leq r$. Put*

$$s \coloneqq \#\{1 \leq i \leq r \mid \mathbb{Q}(P_i) \text{ contains } K\}.$$

If $s = 0$, then $\#\mathcal{F} = 1$. If $s \geq 1$, then $\mathcal{F}$ consists of 2^{s-1} points, each with residue field the same ring class field.

Proof. Step 1: Suppose that $\Delta = \mathfrak{f}^2\Delta_K < -4$. Let F be the fiber of $X_0(N) \to X(1)$ over J_Δ, and for $1 \leq i \leq r$ let F_i be the fiber of $X_0(\ell_i^{a_i}) \to X(1)$ over J_Δ. Then by [Cl22a, Prop. 3.5] we have that F is the fiber product of $F_1, \ldots, F_r$ over $\operatorname{Spec} \mathbb{Q}(\mathfrak{f})$. By our hypothesis, we have either $\Delta_K < -4$ or $\mathfrak{f} > 1$. If $\Delta_K < -4$, the result follows from this and [Cl22a, Prop. 2.10], as is recorded in [Cl22a, §9.1]. If $\Delta_K \in \{-3, -4\}$ and $\mathfrak{f} > 1$, the result follows from this and Proposition 2.2.

For the remainder of the argument we suppose that $\Delta \in \{-3, -4\}$. Let $P \in \mathcal{F}$, let $\varphi : E \to E'$ be an isogeny inducing the point P, and put $C \coloneqq \operatorname{Ker} \varphi^\vee$. The endomorphism ring of E' has discriminant $(\mathfrak{f}')^2\Delta_K$ for some $\mathfrak{f}' \mid N$.
Step 2: We suppose that $\mathfrak{f}' > 1$. For each $1 \leq i \leq r$, let $C_i \coloneqq C[\ell_i^{a_i}]$ and $(\varphi^\vee)_i$ be the isogeny $E' \to E'/C_i =: E_i$. Then $\varphi^\vee$ factors as $\psi_i \circ (\varphi^\vee)_i$, wehre $\psi_i : E_i \to E$ is a cyclic $\frac{N}{\ell_i^{a_i}}$-isogeny. Let $\mathfrak{f}_i$ be the conductor of the endomorphism ring of E_i, so $\operatorname{ord}_{\ell_i}(\mathfrak{f}_i) = 0$, since the conductor of $\operatorname{End}(E)$ is 1 and $\deg(\psi_i)$ is prime to ℓ_i.

For $1 \leq i \leq r$, the path in $\mathcal{G}_{K,\ell_i,1}$ corresponding to $(\varphi^\vee)_i$ therefore terminates at the unique surface vertex, hence it consists of $\operatorname{ord}_{\ell_i}(\mathfrak{f}')$ ascending edges, which are uniquely determined by E', followed by $a_i - \operatorname{ord}_{\ell_i}(\mathfrak{f}_i)$ horizontal edges. If ℓ_i does not split in K the path corresponding to $(\varphi^\vee)_i$ is therefore uniquely determined, whereas if ℓ_i splits in K there are two such paths which are complex conjugates of each other and therefore determine the same closed point equivalence class. Let $P_i' \in X_0(N)$ be the $\mathfrak{f}^2\Delta_K$-CM point induced by $(\varphi^\vee)_i$, and let $\mathcal{F}'$ be the set of closed points $P' \in X_0(N)$ such that $\pi_i(P') = P_i'$ for all $1 \leq i \leq r$. Thus passage to the dual isogeny gives a residue-field preserving bijection from $\mathcal{F}$ to $\mathcal{F}'$. Let $1 \leq i \leq r$. Because the path corresponding to P_i begins at the surface and

the path corrsesponding to P_i' ends at the surface, we have that $\mathbb{Q}(P_i)$ contains K if and only if ℓ_i splits in K in $\mathrm{ord}_{\ell_i}(\mathfrak{f}') < a_i$ if and only if $\mathbb{Q}(P_i')$ contains K. Applying Step 1, we get that if $s = 0$ then $\#\mathcal{F} = \#\mathcal{F}' = 1$, while if $s \geq 1$ then

$$\#\mathcal{F} = \#\mathcal{F}' = 2^{s-1}.$$

Step 3: We suppose that $\mathfrak{f}' = 1$. In this case every element of $\mathcal{F}$ is induced by an isogeny $\varphi_I : E \to E/E[I]$ for I a nonzero $\mathbb{Z}_K$-ideal such that $\mathbb{Z}_K/I$ is cyclic, and $\deg \varphi_I = ||I|| \coloneqq \#\mathbb{Z}_K/I$. Moreover the field of moduli of φ_I is $\mathbb{Q}$ if $I = \overline{I}$ and K otherwise [Cl22a, §3.4]. For distinct I and J, the isogenies φ_I and φ_J induce the same closed point on $X_0(N)$ if and only if $J = \overline{I}$, so closed point equivalence classes in this case correspond to orbits under $\mathfrak{g}_{\mathbb{R}}$. For a prime power ℓ^a, there is an ideal I of norm ℓ^a such that $\mathbb{Z}_K/I$ is cyclic if and only if (ℓ ramifies in $\mathbb{Z}_K$ and $a = 1$) or ℓ splits in K. In the ramified case there is a unique ideal of norm ℓ, while in the split case the two ideals of norm ℓ^a are $\mathfrak{p}^a$ and $\overline{\mathfrak{p}}^a$ where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the two primes of $\mathbb{Z}_K$ lying over ℓ. If s is the number of $1 \leq i \leq r$ such that ℓ_i splits in $\mathbb{Z}_K$, then if $s = 0$ then N the unique prime number that ramifies in $\mathbb{Z}_K$ so $\#\mathcal{F} = 1$. If $s \geq 1$, then the number of ideals I of norm N such that $\mathbb{Z}_K/I$ is cyclic is 2^s, and the number of $\mathfrak{g}_{\mathbb{R}}$-orbits of such ideals is 2^{s-1}. □

Corollary 8.8. *Let $M \mid N$ be in $\mathbb{Z}^+$ with prime-power factorizations $M = \ell_1^{a_1'} \cdots \ell_r^{a_r'}$ and $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ with $\ell_1 \leq \ldots \leq \ell_r$. Let $\pi : X_0(M,N) \to X_0(N)$ denote the natural map, and let $\pi_i : X_0(N) \to X_0(\ell_1^{a_1})$ denote the natural map for $1 \leq i \leq r$. Let $P_i \in X_0(\ell_1^{a_1})$ be Δ-CM points for each index i, and let $\mathcal{F}$ be the set of closed points $P \in X_0(M,N)$ such that $\pi_i(\pi(P)) = P_i$ for all $1 \leq i \leq r$. For each $1 \leq i \leq r$, let d_i denote the number of descending edges occurring in a path in $\mathcal{G}_{K,\ell_i,f_0}$ corresponding to P_i. Put*

$$s := \#\{1 \leq i \leq r \mid \mathbb{Q}(P_i) \text{ contains } K\},$$

and put

$$\epsilon = \begin{cases} 1 & \text{if } s = 0, (M,\Delta) = (2,-4) \text{ and } a_1 \notin \{1, d_1\}, \\ 0 & \text{otherwise.} \end{cases}$$

We then have that $\mathcal{F}$ consists of

$$\#\mathcal{F} = 2^{\max(s-1,0)-\epsilon} \cdot M\varphi(M) \cdot \left(\prod_{i \text{ with } a_i' > d_i = 0} \ell_i^{a_i'-1} \left(\ell_i - \left(\frac{\Delta}{\ell_i} \right) \right) \right)^{-1} \cdot \left(\prod_{i \text{ with } a_i' > d_i > 0} \ell_i^{a_i'-d_i} \right)^{-1}$$

points with isomorphic residue fields.

Proof. Given a point $P' \in X_0(N)$, Theorem 8.6 determines the residue field of any point $Q \in \pi^{-1}(P')$ in terms of P' and M, so we know that each point in $\mathcal{F}$ has the same residue field up to isomorphism. If $\Delta < -4$ then the map π is unramified. If $\Delta = -4$ (resp. $\Delta = -3$), then the map π has ramification index 1 if and only if the path in $\mathcal{G}_{K,\ell,1}$ corresponding to x_i is purely horizontal for each i. Therefore, because $M \geq 2$ (see the discussion in §1.4 for more details), the point P necessarily has ramification index $e = 2$ (resp. $e = 3$) exactly with respect to π in this situation, and otherwise has ramification

index 1. In any event, letting $P' \in X_0(N)$ be a point with $\pi_i(P') = P_i$ for all $1 \leq i \leq r$, we must have that the number of points $P \in \mathcal{F}$ lying above P' is

$$\frac{\deg(\pi)}{e \cdot [\mathbb{Q}(P) : \mathbb{Q}(\pi(P))]} = \frac{M\varphi(M)}{e \cdot [\mathbb{Q}(P) : \mathbb{Q}(\pi(P))]}$$

The $\epsilon = 1$ case, by Theorem 8.6, is exactly the case in which $\mathbb{Q}(P')$ is isomorphic to a rational ring class field while $\mathbb{Q}(P)$ is a ring class field. In the $\epsilon = 0$ case, we then have

$$\begin{aligned} e \cdot [\mathbb{Q}(P) : \mathbb{Q}(\pi(P))] &= e \cdot \left[\mathbb{Q}\left(\ell_1^{\max\{a_1', d_1\}} \cdots \ell_1^{\max\{a_1', d_1\}}\right) : \mathbb{Q}\left(\ell_1^{d_1} \cdots \ell_r^{d_r}\right)\right) \\ &= \left(\prod_{i \text{ with } a_i' > d_i = 0} \ell_i^{a_i' - 1}\left(\ell_i - \left(\frac{\Delta_K}{\ell_i}\right)\right)\right) \cdot \left(\prod_{i \text{ with } a_i' > d_i > 0} \ell_i^{a_i' - d_i}\right), \end{aligned}$$

while the only change in this quantity in the $\epsilon = 1$ case is an additional factor of 2. This combined with the result of the previous theorem gives the result as stated. □

8.3. **Primitive Residue Fields and Primitive Degrees I.** In this section and the next, we extend the results of [Cl22a, §9.2-9.3] to handle $\Delta_K \in \{-3, -4\}$. Given our extensions of the results on primitive residue fields of Δ-CM points on $X_0(\ell^{a_1'}, \ell^{a_1})$ for ℓ prime and on compiling across prime powers this proceeds nearly exactly as therein.

In this section, as in [Cl22a, §9.2], we suppose that either $M = 1$ or that ($M = 2$ and Δ is even). This assumption implies that there is a closed Δ-CM point on $X_0(M, N)$ with residue field isomorphic to $\mathbb{Q}(N\mathfrak{f})$, and therefore there is a unique $B \mid N$ such that $\mathbb{Q}(B\mathfrak{f})$ is a primitive residue field of Δ-CM points on $X_0(M, N)$. For each $1 \leq i \leq r$, take b_i to be the least integer B_i such that $\mathbb{Q}(\ell_i^{B_i}\mathfrak{f})$ is isomorphic to the residue field of a Δ-CM point on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$. We then have

$$B = \ell_1^{b_1} \cdots \ell_r^{b_r}.$$

There is at most one other primitive residue field of a Δ-CM point on $X_0(M, N)$, and there is one other exactly when there are two primitive residue fields for Δ-CM points on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ for some $1 \leq i \leq r$. In this case, letting c_i, for $1 \leq i \leq r$, be the least natural number C_i such that there is a Δ-CM point on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ with residue field isomorphic to either $\mathbb{Q}(\ell_i^{C_i}\mathfrak{f})$ or to $K(\ell_i^{C_i}\mathfrak{f})$, we have that the other primitive residue field is $K(C\mathfrak{f})$, where

$$C = \ell_1^{c_1} \cdots \ell_r^{c_r}.$$

If there is a unique primitive residue field of Δ-CM points on $X_0(M, N)$, then of course there is a unique primitive degree $[\mathbb{Q}(P) : \mathbb{Q}]$ of such points. Supposing we are in the case of two primitive residue fields $\mathbb{Q}(B\mathfrak{f})$ and $K(C\mathfrak{f})$, we put

$$\mathbf{b} \coloneqq [\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}] \quad \text{and} \quad \mathbf{c} \coloneqq [K(C\mathfrak{f}) : \mathbb{Q}].$$

We will have a unique primitive degree if and only if one of $\mathbf{b}$ and $\mathbf{c}$ divides the other, and we will soon see that we always have $\mathbf{c} \leq \mathbf{b}$, so the question is whether $\mathbf{c} \mid \mathbf{b}$. This divisibility certainly holds if the analogous divisibility holds at every prime power, but as seen in [Cl22a] this is not a necessary condition. The following theorem determines exactly

the situation, generalizing [Cl22a, Thm. 9.2]. The proof is only mildly more complicated than the proof of this prior result, owing to handling the $\Delta = -4$ case.

Theorem 8.9. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant, and let $M = \ell_1^{a_1'} \cdots \ell_r^{a_r'} \mid N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. We suppose that either $M = 1$ or ($M = 2$ and Δ is even). For $1 \leq i \leq r$, let $b_i \geq 0$ be the unique natural number such that $\mathbb{Q}(\ell_i^{b_i}\mathfrak{f})$ occurs up to isomorphism as a primitive residue field of a closed Δ-CM point on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$. Let c_i be equal to b_i if there is a unique primitive residue field of Δ-CM points on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ and otherwise let it be such that the unique non-real primitive residue field of a closed Δ-CM point on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ is $K(\ell_i^{c_i}\mathfrak{f})$. Put $B \coloneqq \ell_1^{b_1} \cdots \ell_r^{b_r}$ and $C \coloneqq \ell_1^{c_1} \cdots \ell_r^{c_r}$. Let s be the number of $1 \leq i \leq r$ such that there is a non-real primitive residue field of a closed Δ-CM point on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$.*

a) *If $s = 0$, the unique primitive residue field of a Δ-CM point on $X_0(M, N)$ is $\mathbb{Q}(B\mathfrak{f})$, so the unique primitive degree of a Δ-CM point on $X_0(M, N)$ is $[\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}]$.*

b) *If $s \geq 1$ and there is some $1 \leq i \leq r$ such that there are two primitive residue fields of closed Δ-CM points on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ and we are not in Case 1.5b) with respect to Δ and $\ell_i^{a_i}$, then:*
   (i) *There are two primitive residue fields of Δ-CM points on $X_0(M, N)$: $\mathbb{Q}(B\mathfrak{f})$ and $K(C\mathfrak{f})$.*
   (ii) *The unique primitive degree of Δ-CM points on $X_0(M, N)$ is $[K(C\mathfrak{f}) : \mathbb{Q}]$.*

c) *If $s \geq 1$ and for all $1 \leq i \leq r$ such that there are two primitive residue fields of closed Δ-CM points on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ we are in Case 1.5b), then there are two primitive degrees of Δ-CM points on $X_0(M, N)$: $[\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}]$ and $[K(C\mathfrak{f}) : \mathbb{Q}]$.*

Proof. The case $s = 0$ is immediate from the above discussion. Henceforth we suppose $s \geq 1$. We then have (up to isomorphism) two primitive residue fields of Δ-CM closed points on $X_0(M, N)$: $\mathbb{Q}(B\mathfrak{f})$ and $K(C\mathfrak{f})$, and as above we put

$$\mathbf{b} \coloneqq [\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}], \ \mathbf{c} \coloneqq [K(C\mathfrak{f}) : \mathbb{Q}].$$

For each $1 \leq i \leq r$, let F_i be a primitive residue field of a closed point of a Δ-CM elliptic curve on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$; if there is any non-real such field, take F_i to be nonreal. Note that for each i such that there are two primitive residue fields $\mathbb{Q}(\ell_i^{b_i}\mathfrak{f})$ and $K(\ell_i^{c_i}\mathfrak{f})$ we have $[K(\ell_i^{c_i}\mathfrak{f}) : \mathbb{Q}] \leq [\mathbb{Q}(\ell_i^{b_i}\mathfrak{f}) : \mathbb{Q}]$. By Propositions 2.1 and 2.2, there is $0 \leq r' \leq r - 1$ such that

$$\begin{aligned} 2^{s-1} \cdot [K(C\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})] &= \left(\frac{\omega_K}{2}\right)^{r'} \cdot \left(\dim_{\mathbb{Q}(\mathfrak{f})} F_1 \otimes_{\mathbb{Q}(\mathfrak{f})} \otimes \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} F_r\right) \\ &\leq \left(\frac{\omega_K}{2}\right)^{r'} \cdot \left(\dim_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\ell_1^{b_1}\mathfrak{f}) \otimes_{\mathbb{Q}(\mathfrak{f})} \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\ell_r^{b_r}\mathfrak{f})\right) \\ &= [\mathbb{Q}(\ell_1^{b_1}\mathfrak{f}) \cdots \mathbb{Q}(\ell_r^{b_r}) : \mathbb{Q}(\mathfrak{f})]. \end{aligned}$$

It follows that $\mathbf{c} \leq \mathbf{b}$. Thus there is a unique primitive degree exactly when $\mathbf{c} \mid \mathbf{b}$, as claimed in the above discussion.

Because $K(C\mathfrak{f}) \subseteq K(B\mathfrak{f}) = K\mathbb{Q}(B\mathfrak{f})$, we have $\mathbf{c} \mid 2\mathbf{b}$. In particular, we have $\mathrm{ord}_p(\mathbf{c}) \leq \mathrm{ord}_p(\mathbf{b})$ for every odd prime p.

Case 1: Suppose $\Delta_K \neq -4$. By Proposition 2.1 we have

$$\mathrm{ord}_2(\mathbf{c}) = 1 + \mathrm{ord}_2([\mathbb{Q}(C\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]) = 1 + \sum_{i=1}^{r} [\mathbb{Q}(\ell^{c_i}\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]$$

$$\mathrm{ord}_2(\mathbf{b}) = \mathrm{ord}_2([\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]) = \sum_{i=1}^{r} [\mathbb{Q}(\ell^{b_i}\mathfrak{f} : \mathbb{Q}(\mathfrak{f})].$$

It follows that $\mathbf{c} \mid \mathbf{b}$ if and only if there is some $1 \leq i \leq r$ such that there are two primitive residue fields of Δ-CM closed points on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ for which we have

$$\mathrm{ord}_2([\mathbb{Q}(\ell^{c_i}\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]) < \mathrm{ord}_2([\mathbb{Q}(\ell^{b_i}\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})],$$

which holds if and only if

$$\mathrm{ord}_2([K(\ell^{c_i}\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]) \leq \mathrm{ord}_2([\mathbb{Q}(\ell^{b_i}\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})].$$

This holds in every case in which there are two primitive residue fields *except* Case 1.5b).

Case 2: Suppose $\Delta_K = -4$. Let $r_{\mathbf{c}}$ be the number of indices $1 \leq i \leq r$ such that ${\ell_i}^{2c_i}\Delta_K \notin \{-4, -16\}$, and let $r_{\mathbf{b}}$ be the number of indices $1 \leq i \leq r$ such that ${\ell_i}^{2b_i}\Delta_K \notin \{-4, -16\}$. We have $0 \leq r_{\mathbf{c}} \leq r_{\mathbf{b}} \leq r$. Proposition 2.1 then gives:

$$\begin{aligned}
\mathrm{ord}_2(\mathbf{c}) &= 1 + \mathrm{ord}_2\left([\mathbb{Q}(C) : \mathbb{Q}]\right) \\
&= 1 + \mathrm{ord}_2\left([\mathbb{Q}(C) : \mathbb{Q}({\ell_1}^{c_1}) \cdots \mathbb{Q}({\ell_r}^{c_r})]\right) + \mathrm{ord}_2\left([\mathbb{Q}({\ell_1}^{c_1}) \cdots \mathbb{Q}({\ell_r}^{c_r}) : \mathbb{Q}]\right) \\
&= r_{\mathbf{c}} + \sum_{i=1}^{r} \mathrm{ord}_2\left([\mathbb{Q}({\ell_i}^{c_i}) : \mathbb{Q}]\right)
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{ord}_2(\mathbf{b}) &= \mathrm{ord}_2\left([\mathbb{Q}(B) : \mathbb{Q}]\right) \\
&= \mathrm{ord}_2\left([\mathbb{Q}(B) : \mathbb{Q}({\ell_1}^{b_1}) \cdots \mathbb{Q}({\ell_r}^{b_r})]\right) + \mathrm{ord}_2\left([\mathbb{Q}({\ell_1}^{b_1}) \cdots \mathbb{Q}({\ell_r}^{b_r}) : \mathbb{Q}]\right) \\
&= r_{\mathbf{b}} - 1 + \sum_{i=1}^{r} \mathrm{ord}_2\left([\mathbb{Q}({\ell_i}^{b_i}) : \mathbb{Q}]\right).
\end{aligned}$$

We see then that $\mathbf{c} \mid \mathbf{b}$ if and only if

$$\sum_{i=1}^{r} \mathrm{ord}_2\left([\mathbb{Q}({\ell_i}^{c_i}) : \mathbb{Q}]\right) < r_{\mathbf{b}} - r_{\mathbf{c}} + \sum_{i=1}^{r} \mathrm{ord}_2\left([\mathbb{Q}({\ell_i}^{b_i}) : \mathbb{Q}]\right).$$

We find that $\mathbf{c} \mid \mathbf{b}$ if and only if $r_{\mathbf{b}} > r_{\mathbf{c}}$ or there is some $1 \leq i \leq r$ such that $c_i < b_i$ for which we are *not* in Case 1.5b) with respect to Δ and $\ell_i^{a_i}$. Comparing with the statement of the result, we must show: in every case in which $r_{\mathbf{b}} > r_{\mathbf{c}}$ there is some $1 \leq i \leq r$ for which $c_i < b_i$ and we are not in Case 1.5b) for Δ and $\ell_i^{a_i}$. So:

• If $\Delta \notin \{-4, -16\}$, then $r_{\mathbf{b}} = r_{\mathbf{c}}$, so there are two primitive degrees if and only if we are

in Case 1.5b) for all $1 \leq i \leq r$ for which $c_i < b_i$, as claimed.
• If $\Delta \in \{-4, -16\}$ then Case 1.5b) cannot occur for any i and thus $\mathbf{c} \mid \mathbf{b}$, as claimed. □

8.4. **Primitive Residue Fields and Primitive Degrees II.** In this section we treat the case in which either $M \geq 3$, or ($M = 2$ and Δ is odd). Thanks to the work of §7, this case follows exactly as in [Cl22a, §9.3]. In particular, our assumptions imply that there is a unique primitive residue field, which is a ring class field $K(C\mathfrak{f})$.

Let $M = \ell_1^{a_1'} \cdots \ell_r^{a_r'}$ and $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For an index $i \in \{1, \ldots, r\}$, if the only primitive residue field of a Δ-CM point on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ is $\mathbb{Q}(\ell^c\mathfrak{f})$ then put $c_i := c$. Otherwise, the primitive residue fields of Δ-CM points on $X_0(\ell_i^{a_i'}, \ell_i^{a_i})$ are of the form $\mathbb{Q}(\ell^b\mathfrak{f})$ and $K(\ell^c\mathfrak{f})$, and we put $c_i := c$. We then have

$$C = \ell_1^{c_i} \cdots \ell_r^{c_r}.$$

References

[BC20a] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. 305 (2020), 43–88.

[BC20b] A. Bourdon and P.L. Clark, *Torsion points and rational isogenies on CM elliptic curves*. J. Lond. Math. Soc. (2) 102 (2020), 580–622.

[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.

[CGPS22] P.L. Clark, T. Genao, P. Pollack and F. Saia, *The least degree of a CM point on a modular curve*. J. Lond. Math. Soc. (2) 105 (2022), 825–883.
`http://alpha.math.uga.edu/~pete/least_CM_degree-1226.pdf`

[Cl22a] P.L. Clark, *CM elliptic curves: volcanoes, reality and applications, Part I.*

[Cx89] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* John Wiley & Sons, New York, 1989.

[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.

[DS05] F. Diamond and J. Shurman, *A first course in modular forms*. Graduate texts in mathematics, 228. Springer, New York, 2005.

[LLS15] Y. Lamzouri, X. Li and K. Soundararajan, *Conditional bounds for the least quadratic nonresidue and related problems.* Math. Comp. 84 (2015), 2391–2412.

[SiI] J.H. Silverman, *The arithmetic of elliptic curves*. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

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

[Su13] A.V. Sutherland, *On the evaluation of modular polynomials.* ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, 531–555, Open Book Ser., 1, Math. Sci. Publ., Berkeley, CA, 2013.