CM ELLIPTIC CURVES: VOLCANOES, REALITY AND APPLICATIONS

PETE L. CLARK

Contents

1. Introduction

This paper continues work of the author and his collaborators on torsion points of CM elliptic curves over number fields and CM points on elliptic modular curves [CCS13], [CCRS14], [CP15], [BP17], [BCP17], [BCS17], [CP17], [BC20a], [BC20b], [CCM21], [CGPS].

1.1. **Some Modular Curves.** In the present work it will be convenient to take a geometric perspective, so we begin by recalling the notion of a modular curve $X(H)_{/\mathbb{Q}}$ attached to a

subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, as is developed in [Ma76].[1] For $N \in \mathbb{Z}^+$, let $E_{/\mathbb{Q}(t)}$ be an elliptic curve with j-invariant t. Then

$$\mathrm{Aut}(\mathbb{Q}(t, E[N])/\mathbb{Q}(t)) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

and we let $X(N)_{/\mathbb{Q}}$ be the smooth, projective integral (but not geometrically integral, if $N \geq 3$) curve with function field $\mathbb{Q}(X(N)) := \mathbb{Q}(t, E[N])^{\{\pm 1\}}$. Thus $\mathbb{Q}(X(N))/\mathbb{Q}(t)$ is Galois with group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. Identifying $\mathbb{Q}(t)$ with the function field of the j-line $X(1) \cong \mathbb{P}^1$, we get a Galois branched covering of curves $X(N) \to X(1)$. To any $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ we get a subextension $X(H) = X(N)^H$ of $X(N) \to X(1)$ and thus a corresponding intermediate covering

$$X(N) \to X(H) \to X(1).$$

Thus the spectrum of the function field $\mathbb{Q}(X(H))$ is the fiber of $\pi_H : X(H) \to X(1)$ over the generic point of $X(1)_{/\mathbb{Q}}$. The support of the fiber ∞_H of π_H over $\infty \in X(1)$ consists precisely of the cusps on $X(H)$, and we take $Y(H)_{/\mathbb{Q}}$ to be the smooth, integral affine curve $X(H) \setminus \infty_H$. We have $Y(1) \cong \mathbb{A}^1_{/\mathbb{Q}} = \mathrm{Spec}\, \mathbb{Q}[t]$, so a closed point $J \in Y(1)$ is given by an irreducible polynomial $J(t) \in \mathbb{Q}[t]$. For $J \neq t, t - 1728$ – an assumption that we will (unfortunately) make throughout most of the present work – computing the fibers $\pi_H^*(J)$ over J for all H is essentially the same as computing the "adelic Galois $\pm$-representation"

$$\rho : \mathfrak{g}_{\mathbb{Q}[t]/(J)} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})/\{\pm 1\}$$

on any elliptic curve with j-invariant j, where j is a root of J in $\overline{\mathbb{Q}}$. If F is a field of characteristic 0 and $E_{/F}$ is an elliptic curve such that the modulo N Galois $\pm$-representation

$$\overline{\rho_N} : \mathfrak{g}_K \to \mathrm{GL}_2(Z/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

has image in H, then E induces an F-rational point on $X(H)$. Two elliptic curves $(E_1)_{/F}$, $(E_2)_{/F}$ with j-invariants different from $0, 1728$ whose $\pm$-modulo N Galois representations lie in H induce the same point on $X(H)(F)$ iff they are quadratic twists of each other, and every point of $X(H)(F)$ whose image under $\pi : X(H)(F) \to X(1)(F) = \mathbb{P}^1(F)$ does not lie in $\{t, t - 1728, \infty\}$ arises from such an elliptic curve $E_{/F}$. Similarly, a closed point $P \in X(H)$ not lying over t or $t - 1728$ on $X(1)$ with residue field $\mathbb{Q}(P)$ corresponds to an elliptic curve $E_{/\mathbb{Q}(P)}$ with $\overline{\rho_N}(\mathfrak{g}_{\mathbb{Q}(P)}) \subset H$, well-defined up quadratic twist.

The modular curves of interest to us here are the following ones:

• The curve $X(N)_{/\mathbb{Q}}$ itself, a $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$-Galois cover of the j-line $X(1)$. For a field F of characteristic 0, an elliptic curve $E_{/F}$ with $j(E) \neq 0, 1728$ defines an F-rational point on $X(N)$ iff the mod N Galois $\pm$-representation $\overline{\rho_N} : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ is trivial iff for some quadratic twist E^χ of E the group scheme $E^\chi[N]$ is constant ("full N-torsion").

[1] We also recommend [Ro97] for an especially careful exposition.

• For positive integers $M \mid N$, we put $X_1(M,N) \coloneqq X(H_1(M,N))$, where $H_1(M,N) \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ is the subgroup

$$\left\{ \pm \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \mid \ b \equiv 0 \pmod{M},\ d \equiv 1 \pmod{M} \right\}.$$

We have $X(N) = X_1(N,N)$. At the other extreme, $X_1(N) \coloneqq X_1(1,N)$. We have

$$[\mathbb{Q}(X_1(M,N)) : \mathbb{Q}(X(1))] = \begin{cases} 1 & (M,N) = (1,1) \\ 3 & (M,N) = (1,2) \\ 6 & (M,N) = (2,2) \\ \frac{M\varphi(M)\varphi(N)\psi(N)}{2} & N \geq 3 \end{cases},$$

(see e.g. [CGPS, §7.2]), where $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$ and $\psi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is the unique multiplicative function such that $\psi(\ell^a) = (\ell+1)\ell^{a-1}$ for all prime powers ℓ^a. For a field F of characteristic 0, an elliptic curve $E_{/F}$ with $j(E) \neq 0, 1728$ defines an F-rational point on $X_1(M,N)$ iff for some quadratic twist E^χ there is an injective group homomorphism $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$. Thus the study of torsion subgroups of elliptic curves over number fields is very closely related to the study of closed points on $X_1(M,N)$.

• For positive integers $M \mid N$, we put $X_0(M,N) \coloneqq X(H_0(M,N))$, where $H_0(M,N) \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ is the subgroup

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \equiv 0 \pmod{M},\ a \equiv d \pmod{M} \right\}.$$

We have $X_0(N) \coloneqq X_0(1,N)$. We have

$$\mathbb{Q}(X_0(M,N)) : \mathbb{Q}(X(1))] = [\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} : H_0(M,N)] = M\varphi(M)\psi(N)$$

and thus also

$$\deg(X_1(M,N)) \to X_0(M,N)) = \begin{cases} 1 & N \leq 2 \\ \frac{\varphi(N)}{2} & N \geq 3 \end{cases}.$$

For a field F of characteristic 0, an elliptic curve $E_{/F}$ with $j(E) \neq 0, 1728$ defines an F-rational point on $X_0(M,N)$ iff there are F-rational isogenies $\iota_1 : E \to E'$, $\iota_2 : E \to E''$ such that $K_1 = (\mathrm{Ker}\, \iota_1)(\overline{F_1})$ is cyclic of order N, $K_2 = (\mathrm{Ker}\, \iota_2)(\overline{F})$ is cyclic of order M, and the subgroup of $E(\overline{F})$ generated by K_1 and K_2 is isomorphic to $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Equivalently, $E_{/F}$ admits an F-rational cyclic N-isogeny and Galois acts on $E[M]$ by scalar matrices.

1.2. **The Δ-CM Locus.** An elliptic curve over a field of characteristic 0 has **complex multiplication** if its geometric endomorphism ring is an order in an imaginary quadratic field. Imaginary quadratic orders are classified up to isomorphism by their discriminant Δ. Each discriminant is a negative integer congruent to 0 or 1 mod 4, each negative integer $\Delta \equiv 0, 1 \pmod 4$ is the discriminant of a unique imaginary quadratic order, and for each imaginary quadratic discriminant Δ there is a unique closed point $J_\Delta \in X(1)_{/\mathbb{Q}}$ corresponding to elliptic curves with CM by the order of discriminant Δ. Thus for any modular curve $X(H)_{/\mathbb{Q}}$, we have the **Δ-CM locus**, which is the fiber of the map $\pi : X(H) \to X(1)$

over the closed point J_Δ. This is a finite $\operatorname{Spec} \mathbb{Q}(J_\Delta)$-scheme, and it is étale if $\Delta < -4$.

A recent result of Bourdon-Clark nearly determines the Δ-CM locus on $X(N)_{/\mathbb{Q}}$:

Theorem 1.1 (Bourdon-Clark [BC20a])**.** *Let $\mathcal{O}$ be an order in the imaginary quadratic field K, with discriminant Δ, which we may write as $\Delta = \mathfrak{f}^2 \Delta_K$ for $\mathfrak{f} \in \mathbb{Z}^+$. Let $P \in X(N)_{/\mathbb{Q}}$ be a closed Δ-CM point, and let $\pi(P) = J_\Delta$ be its image on $X(1)_{/\mathbb{Q}}$.*

a) *Suppose that $N \geq 3$ or Δ is odd. Then we have*

$$\mathbb{Q}(P) = K(J_{N^2\Delta})K^{(N)},$$

where $K^{(N)}$ is the N-ray class field of K. Thus $\mathbb{Q}(P)$ contains K. Also we have

$$[\mathbb{Q}(P) : \mathbb{Q}(\pi(P))] = 2[\mathbb{Q}(P) : K(\pi(P))] = 2\#(\mathcal{O}/N\mathcal{O})^\times.$$

b) *Suppose that $N = 2$ and Δ is even. Then we have*

$$\mathbb{Q}(P) \cong \begin{cases} \mathbb{Q} & \Delta = -4 \\ \mathbb{Q}(J_{4\Delta}) & \Delta < -4 \end{cases}.$$

In particular $\mathbb{Q}(P)$ does not contain K. We also have

$$[\mathbb{Q}(P) : \mathbb{Q}(\pi(P))] = \begin{cases} 1 & \Delta = -4 \\ 2 & \Delta < -4 \end{cases}.$$

Remark. Let us compare Theorem 1.1 to some other results, both classical and recent.

a) When the order $\mathcal{O}$ is maximal – i.e., $\mathcal{O} = \mathbb{Z}_K$, the full ring of integers of K – we have $\Delta = \Delta_K$ and $K(P) = K(J_{N^2\Delta_K})K^{(N)} = K^{(N)}$, and this is a geometric phrasing of the "First Main Theorem of CM" [SII, Thm. II.5.6] in the case where the ideal is $N\mathbb{Z}_K$ for some $N \in \mathbb{Z}^+$.

b) Closely related results have been obtained by Stevenhagen [St01], Lozano-Robledo [LR19], and Campagna-Pengo [CP21]. All three of these authors take the perspective that the residue field $K(P)$ of any Δ-CM closed point on $X(N)_{/K}$ may be thought as the "N-ray class field of the nonmaximal order $\mathcal{O}$."[2] In fact, for any nonzero invertible $\mathcal{O}$-ideal I, Campagna-Pengo show that the field $K(\mathfrak{h}(E[I]))$ obtained by adjoining to K the values of a Weber function (which may be taken to be the x-coordinate, when $\Delta < -4$) on the I-torsion kernel $E[I]$ is the I-ray class field of the nonmaximal order $\mathcal{O}$. This fully generalizes the First Main Theorem of Complex Multiplication to all imaginary quadratic orders.

The only things left to know about the fiber of $\pi : X(N) \to X(1)$ over J_Δ are the number of closed points and, in the presence of ramification, the precise scheme-theoretic structure of the non-reduced fibers. The map $X(N) \to X(1)$ is unramified away from $0, 1728, \infty$, hence the same holds for all morphisms of modular curves. For $\Delta < -4$, locally at J_Δ we have an unramified Galois covering, so the number of closed points is simply the degree

[2]This occurs in the final version of [BC20a] as well, but identifying $K(P)$ as the compositum of a ray class field and a ring class field is a component of the proof given there.

of the covering (which we know: cf. §1.1) divided by $[\mathbb{Q}(P) : \mathbb{Q}]$. The reason that we said "nearly" above is that we do not address the scheme-theoretic structure of the fibers when $\Delta \in \{-3, -4\}$: as a rule we do not address $\Delta \in \{-3, -4\}$ (and most often not even $\Delta_K \in \{-3, -4\}$) in this paper.

1.3. **Our Goal.** The main goal of this paper is to pursue analogues of Theorem 1.1 for the Δ-CM locus on the modular curves $X_0(M, N)_{/\mathbb{Q}}$ and $X_1(M, N)_{/\mathbb{Q}}$. Since the coverings $X_1(M, N) \to X(1)$ and $X_0(M, N) \to X(1)$ are usually not Galois, the automorphism group need not act transitively on the fibers, so there may be more than one residue field of closed points in the Δ-CM locus. We will see that – for either of the families $X_0(M, N)$ and $X_1(M, N)$ – the Δ-CM locus can contain closed points of arbitrarily many different degrees.

The results obtained here generalize another recent work of Bourdon-Clark [BC20b], which determines for all Δ and $M \mid N$, the least degree of a closed Δ-CM point on $X_1(M, N)_{/K}$ and also over $X_1(M, N)_{/\mathbb{Q}}$. The latter result is equivalent to the determination of the least degree of a number field F for which there is a Δ-CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$.

Consider the following ambitious problem: for $d \in \mathbb{Z}^+$, determine all groups T that arise as a subgroup of $E(F)[\mathrm{tors}]$ for some elliptic curve E defined over a degree d number field. Work of Merel [Me96] shows that the set of (isomorphism classes of) such groups is finite for each d. However, at present the complete list of such groups is known only for $d = 1$ by work of Mazur [Ma77]), for $d = 2$ by work of Kenku-Momose and Kamienny [KM88], [Ka92] and for $d = 3$ by work of Derickx-Etropolski-van Hoeij-Morrow-Zureick-Brown [DEvHMZB20]. It might be possible to handle the case of $d = 4$ by similar methods, but to go beyond, say, $d = 10$ seems to require a major breakthrough to say the least.

In contrast, a sufficiently good understanding of the Δ-CM locus on the family of curves $X_1(M, N)_{/\mathbb{Q}}$ will yield a complete solution to the above problem upon restriction to the class of CM elliptic curves. In the CM case, much better bounds on $\#E(F)[\mathrm{tors}]$ in terms of $d = [F : \mathbb{Q}]$ are known by work of Silverberg [Si88], [Si92] and Clark-Pollack [CP15], [CP17]. If one knows all degrees of closed Δ-CM points on $X_1(M, N)_{/\mathbb{Q}}$ then one knows all pairs (M, N) for which there is a closed Δ-CM point of degree dividing d on $X_1(M, N)$, and thus the groups $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ are precisely the Δ-CM subtorsion groups in degree d. Moreover, since $[\mathbb{Q}(J_\Delta) : \mathbb{Q}]$ tends to infinity with Δ, only finitely many Δ arise in each degree d, so this yields a complete list of CM subtorsion groups in degree d.

Notice that we do not actually need the list of all degrees of closed Δ-CM points on $X_1(M, N)$ but rather only the list of all multiples of these degrees. Otherwise put, for applications to the determination of CM subtorsion groups it is enough to know all **primitive** degrees $[\mathbb{Q}(P) : \mathbb{Q}]$ of closed Δ-CM points on $X_1(M, N)_{/\mathbb{Q}}$, namely those degrees that are not a proper multiple of any other such degree. This turns out to simplify the answer considerably: Bourdon-Clark showed that every degree of a closed Δ-CM point on $X_1(M, N)_{/K}$ is a multiple of the least degree, and thus there is always a unque primitive

Δ-CM degree. On the other hand, [BC20b, Example 6.7] gives a case in which there are at least two primitive degrees of Δ-CM closed points on $X_1(N)_{/\mathbb{Q}}$, and therefore knowing the least degree does not give all degrees in which a Δ-CM elliptic curve can have a subgroup isomorphic to $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. In the present paper, we will *in principle* determine all degrees of Δ-CM closed points on $X_1(M,N)_{/\mathbb{Q}}$ when $\Delta_K < -4$, but the results seem too complicated to record once and for all. In a much more explicit way we will record all primitive degrees of Δ-CM closed points on $X_1(M,N)_{/\mathbb{Q}}$ when $\Delta_K < -4$: we find in particular that there are either one or two such degrees.

Theorem 1.1 implies that when $M \geq 3$ the residue field of $\mathbb{Q}(P)$ of every Δ-CM point on $X_1(M,N)_{/\mathbb{Q}}$ contains K, so the work of Bourdon-Clark computes the unique primitive degree of a Δ-CM point. Thus it remains to consider $M \in \{1,2\}$.

1.4. **Transition to $X_0(M,N)$.** Although most of the results of [BC20b] concern torsion subgroups of CM elliptic curves, a key ingredient in their proofs was the study of rational cyclic N-isogenies on CM elliptic curves. As Bourdon and I worked on [BC20b] we gradually became aware of the extent to which the torsion subgroups of CM elliptic curves are controlled by the existence or nonexistence of cyclic isogenies on CM elliptic curves rational over various fields. The natural map $X_1(N) \to X_0(N)$ is an isomorphism for $N \leq 2$ and a $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$-Galois cover for $N \geq 3$, which guarantees a connection between isogenies and torsion points: as is well known, if you have an elliptic curve defined over a number field F with an F-rational cyclic N-isogeny, then this elliptic curve has a point of order N rational over a field extension of F of degree at most $\frac{\varphi(N)}{2}$. But the results of [BC20b] show a much tigher relationship. This relationship is clarified by the following result that we will prove now, using the work of [BC20a].

Theorem 1.2. *Let $\Delta < -4$ be an imaginary quadratic discriminant, let $M \mid N$ be positive integers, and let $P \in X_0(M,N)_{/\mathbb{Q}}$ be a closed Δ-CM point. Then the map $\pi : X_1(M,N) \to X_0(M,N)$ is inert over P: that is, writing the fiber $\pi^*(P)$ as* Spec A *for a finite-dimensional $\mathbb{Q}(P)$-algebra A, we have that A is a field.*

Proof. If $N \leq 2$, then the map $X_1(M,N) \to X_0(M,N)$ is an isomorphism, so we may assume that $N \geq 3$, in which case it has degree $\frac{\varphi(N)}{2}$.

Let $\pi : X_0(N,N) \to X_0(M,N)$, and choose a point $\tilde{p} \in X_0(N,N)$ such that $\pi(\tilde{p}) = p$. Because the covering $X(N) = X_1(N,N) \to X_0(M,N)$ is the fiber product of the coverings $X_1(M,N) \to X_0(M,N)$ and $X_0(N,N) \to X_0(M,N)$, it suffices to show that the fiber of $X(N) \to X_0(N,N)$ over $\tilde{p}$ is inert. (If F is a number field, L/F is a finite degree field extension and A/F is a finite dimensional commutative F-algebra such that $L \otimes_F A$ is a field, then A is a field.) So we reduce to the case $M = N$ and write p in place of $\tilde{p}$. Similarly, it suffices to prove the inertness result for the map $X(N) \to X_0(N,N)$, viewed as a morphism of curves over the imaginary quadratic field K.

The closed point p comes from a Δ-CM elliptic curve $E_{/K(p)}$ for which the modulo N Galois representation $\rho_N : \mathfrak{g}_{K(p)} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ consists of scalar matrices. The elliptic curve E is well-determined up to a quadratic (since $\Delta < -4$) twist, and therefore the

reduced modulo N Galois representation

$$\overline{\rho}_N = (\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}) \circ \rho_N$$

is well-defined. By [BC20a, Thm. 4.1] we have $K(p) = K(N\mathfrak{f})$, the N-ring class field of K. The proof of *loc. cit.* shows that

$$[K(p) : K(\mathfrak{f})] = \frac{\#(\mathcal{O}/N\mathcal{O})^\times}{\varphi(N)},$$

while [BC20a, Thm 1.4] gives $\#\overline{\rho}_N(\mathfrak{g}_{K(\mathfrak{f})}) = \frac{\#(\mathcal{O}/N\mathcal{O})^\times}{2}$. From these two facts it follows that $\#\overline{\rho}_N(\mathfrak{g}_{K(p)}) = \frac{\varphi(N)}{2} = \deg(X(N) \to X_0(N,N))$, which establishes the result. □

Theorem 1.2 implies that, when $\Delta < -4$, knowing the degrees and multiplicities of the Δ-CM points on $X_0(M,N)_{/\mathbb{Q}}$, yields the degrees and multiplicities of the Δ-CM points on $X_1(M,N)_{/\mathbb{Q}}$: if $N \leq 2$ the curves are the same, while for $N \geq 3$, multiply each degree by $\frac{\varphi(N)}{2}$. The same holds for primitive degrees, with the upshot being that all the information we referred to above about Δ-CM closed points on $X_1(M,N)_{/\mathbb{Q}}$ can be immediately deduce from the corresponding information about Δ-CM closed poins on $X_0(M,N)_{/\mathbb{Q}}$.

For most of this paper we study Δ-CM points on the curves $X_0(M,N)_{/\mathbb{Q}}$. For this family of curves we can do more: for $\Delta_K < -4$ we determine not only the multiplicities and degrees of closed points in the Δ-CM locus but actually the residue fields themselves. It turns out that there are only two classes of such fields. As is standard, we call a field $K(J_\Delta)$ a **ring class field** (here this is understood to be relative to the fixed imaginary quadratic field K). We call a field isomorphic to $\mathbb{Q}(J_\Delta)$ a **rational ring class field**. Then:

Theorem 1.3. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant with $\Delta_K < -4$, and let $P \in X_0(M,N)_{/\mathbb{Q}}$ be a Δ-CM closed point. Then $\mathbb{Q}(P)$ is either a rational ring class field or a ring class field. More precisely: there is $N' \mid N$ such that $\mathbb{Q}(P)$ is isomorphic to either $\mathbb{Q}(J_{(N')^2\Delta})$ or to $K(J_{(N')^2\Delta})$.*

Our study of closed CM points on $X_0(M,N)$ comes roughly in four parts.

Step 1: We prove a result (Proposition 3.8) about fiber products of curves $X_0(M,N)_{/\mathbb{Q}}$ that reduces us to the case $X_0(\ell^a,\ell^b)_{/\mathbb{Q}}$ for a prime number ℓ. This result is neither deep nor difficult, but it is simply false for the curves $X_1(M,N)_{/\mathbb{Q}}$, which already gives a clue that we are on the right track by considering the curves $X_0(M,N)_{/\mathbb{Q}}$ instead.

Step 2: We are therefore reduced to considering (in general, pairs of) cyclic isogenies of prime power degree. This places us in a position to make use of the fact that the ℓ-powered isogeny graph on K-CM elliptic curves has a very simple structure, that of an **isogeny volcano**. This is probably the single most important ingredient in our analysis, and it is really remarkable the extent to which use of volcanoes reduces difficult problems in arithmetic geometry to either straightforward enumerative combinatorics or simple (albeit

sometimes tedious) bookkeeping. I am somewhat perplexed by the fact that isogeny volcanoes up until now have mainly been used in the study of elliptic curves over finite fields. I know of only one paper that uses isogeny volcanoes in characteristic zero, a recent one of Rosen-Shnidman [RS17]. Some of the enumerative work we do with isogeny volcanoes is very closely related to work done by Rosen-Shnidman.

Steps 1 and 2 yield a complete description of the Δ-CM locus on $X_0(M,N)_{/K}$: in this case (as follows from our discussion up until now, in fact) there is only one primitive residue field. Just as in the recent paper [BC20b], the greater part of the battle is to descend from modular curves over K to modular curves over $\mathbb{Q}$. In the present work, this amounts to an explicit understanding of the action of complex conjugation on the isogeny volcano.[3] This comes in two parts.

Step 3: We develop the algebraic number theory of rational ring class fields. I find it somewhat surprising that this did not already exist in the literature, given that these are precisely the number fields defined by the Hilbert class polynomials and thus have been the subject of intense study. Whereas the ring class fields are always Galois over $\mathbb{Q}$ but usually not abelian over $\mathbb{Q}$, the rational ring class fields are usually not Galois over $\mathbb{Q}$. A key concept here is that of **coreality** of K-CM j-invariants j and j', by which we mean that the number field $\mathbb{Q}(j,j')$ has a real place. In particular the compositum of two rational ring class fields is sometimes a rational ring class field and sometimes a ring class field, and we compute all such composita explicitly. Gauss's genus theory of binary quadratic forms also intervenes here.

Step 4: Using the algebraic work described in Step 3 we solve the graph-theoretic problem of how the involution of complex conjugation acts on the isogeny volcano. The case of $\ell = 2$ requires a more intricate analysis than that of $\ell > 2$. To complete the $\ell = 2$ case, we make use of results of Kwon [Kw99] on cyclic isogenies.

1.5. **Contents.** We now give a more detailed description of the contents of the paper.

Section 2 is mostly algebraic number theory: we introduce the algebraic number theory of ring class fields and rational ring class fields. This is related to the genus theory of binary quadratic forms and to the notion of a "real lattice" $\Lambda \subset \mathbb{C}$. The most important result here is probably Corollary 2.11, which will later be used to reduce the computation of the Δ-CM locus on $X_0(M,N)$ to the case where $M = \ell^a$, $N = \ell^b$ are both prime powers.

In Section 3 we study isogenies of elliptic curves in characteristic 0. Our initial setup includes the non-CM case. Whereas our main goal of this paper is to compute the field of moduli of an isogeny of CM elliptic curves, in this section we give a result, Proposition 3.3, that gives a simple answer in the non-CM case. In §3.4 we recall some structural results on

[3]This is not present in the work of [RS17], whereas the portion of the combinatorial analysis described in Step 2 above seems to be equivalent to what they did, although recorded somewhat differently.

isogenies in the CM case with a focus on the conductor of the endomorphism rings. In §3.5 we give the geometric result, Proposition 3.8, that reduces us from the study of $X_0(M,N)$ to that of $X_0(\ell^a,\ell^b)$.

In Section 4 we introduce the ℓ-power isogeny graph of complex elliptic curves and explain its "volcanic" structure. We claim no novelty here: all of these results can be found in the literature – we especially recommend [Su12] – but because this material is absolutely crucial for the rest of the paper we have decided to give an independent exposition.

In Section 5, the theoretical heart of the paper, we explicitly determine the action of complex conjugation on the isogeny volcano. There is an algebraic preliminary: §5.1 on "coreality," which studies when the number field $\mathbb{Q}(j,j')$ generated by two K-CM j-invariants contains K.

After Section 5 we are close to being able to prove main results of the paper. Section 6 is a bit of an interregnum, in which we show that the results that we have developed so far lead to short, transparent proofs of several prior results in the literature, including Kwon's classification of cyclic N-isogenies over $\mathbb{Q}(j)$ and Bourdon-Clark's classification of cyclic N-isogenies over $K(j)$ (in the $\Delta_K < -4$ case). In §6.4 we give some new applications to CM points on $X_0(N)$: for instance in Theorem 6.5 we show that for a subfield $F \subset \mathbb{C}$, the set of $N \in \mathbb{Z}^+$ such that $X_0(N)$ has an F-rational CM point is infinite iff F contains either the Hilbert class field of some imaginary quadratic field or infinitely many rational ring class fields. In §6.5 we analyze the projective N-torsion field of a CM elliptic curve (when $\Delta_K < -4$), strengthening a result of Parish that Bourdon-Clark used to prove Theorem 1.1. We have already mentioned that for all $N \geq 3$, for any K-CM elliptic curve E defined over a number field F, the N-torsion field $F(E[N])$ contains K. Theorem 6.10 implies that the *projective* N-torsion field $F(\mathbb{P}E[N])$ – i.e., the unique minimal extension of F over which the modulo N Galois representation consists entirely of scalar matrices – already contains K. This is the final ingredient we need in order to analyze the Δ-CM locus on $X_0(M,N)_{/\mathbb{Q}}$.

GO ON!

1.6. **Acknowledgments.** Were it not for my prior collaboration with Abbey Bourdon I would neither have thought to write this paper, nor would I be equipped with the technical ability to do so. Insights gained from the work of [BC20a] and [BC20b] – many of which came directly from her – have been put to use here, both directly and otherwise.

At the January 2019 AMS meeting in Baltimore, Drew Sutherland saw Bourdon speak on the work of [BC20b] and immediately suggested a volcanic approach to some of our work. Sutherland's remark amounts to the material of §6.2 of the present paper. This is a completely different proof of [BC20a, Thm. 6.18a)] from the one Bourdon and I originally gave and thus served as an illustration of the merits of the volcanic approach.

I am deeply grateful to Bourdon and Sutherland.

2. Orders, Class Groups, and Rational Ring Class Fields

2.1. **Orders in a number field.** For a number field K of degree d, a ($\mathbb{Z}$-)order in K is a subring $\mathcal{O}$ of K that is free of rank d as a $\mathbb{Z}$-module and has fraction field K. The ring of integers $\mathbb{Z}_K$ is an order in K, and every order $\mathcal{O}$ in K is contained in $\mathbb{Z}_K$ with finite index. Let Δ_K be the discriminant K (more precisely, of $\mathbb{Z}_K$). If $f \coloneqq [\mathbb{Z}_K : \mathcal{O}]$ and Δ is the discriminant of $\mathcal{O}$ (i.e., the discriminant of the trace form on $\mathcal{O}$), then we have $\Delta = f^2\Delta_K$.

The **class group (or Picard group)** $\operatorname{Pic}\mathcal{O}$ of an order is the group of invertible fractional $\mathcal{O}$-ideals modulo principal fractional $\mathcal{O}$-ideals. This is a finite commutative group [N, Thm. I.12.12]; its size is the **class number** $h_{\mathcal{O}}$ of $\mathcal{O}$. There is a canonical finite abelian extension $K(\mathcal{O})/K$, the **ring class field** of $\mathcal{O}$, such that $\operatorname{Aut}(K(\mathcal{O})/K)$ is canonically isomorphic to $\operatorname{Pic}\mathcal{O}$ [LD15, Thm. 4.2]. We write $K(1)$ for $K(\mathbb{Z}_K)$, the **Hilbert class field** of K, and we put $h_K \coloneqq [K(1) : K]$.

An inclusion of orders $\mathcal{O} \subset \mathcal{O}' \subset K$ yields an inclusion of ring class fields $K(\mathcal{O}') \subset K(\mathcal{O})$. Galois theory yields a surjection $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}\mathcal{O}'$; this is also the map induced by the push-forward $I \mapsto I\mathcal{O}'$ on invertible fractional ideals. In particular we have $h_K \mid h_{\mathcal{O}'} \mid h_{\mathcal{O}}$.

For an order $\mathcal{O}$ in a number field K, we define the **conductor ideal**

$$\mathfrak{f} = (\mathcal{O} : \mathbb{Z}_K) = \{x \in K \mid x\mathbb{Z}_K \subset \mathcal{O}\},$$

which is characterized as the largest ideal of $\mathbb{Z}_K$ that is contained in $\mathcal{O}$. The conductor of the abelian extension $K(\mathfrak{f})/K$ divides $\mathfrak{f}$ [LD15, Thm. 4.2]. The conductor ideal also appears in the relative class number formula [N, Thm. I.12.12]

$$\frac{h_{\mathcal{O}}}{h_K} = \frac{\#(\mathcal{O}/\mathfrak{f})^\times}{[\mathbb{Z}_K^\times : \mathcal{O}^\times]\#(\mathbb{Z}_K/\mathfrak{f})^\times}. \tag{1}$$

A nonzero fractional $\mathcal{O}$-ideal $\mathfrak{a}$ is **proper** if

$$(\mathfrak{a} : \mathfrak{a}) \coloneqq \{x \in K \mid x\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}.$$

If $\mathfrak{a}$ is an invertible fractional ideal then $x\mathfrak{a} \subset \mathfrak{a}$ iff $x \in \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$, so $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal. For an order $\mathcal{O}$, every proper fractional $\mathcal{O}$-ideal is invertible iff $\mathcal{O}$ is a Gorenstein ring [JT15, Characterization 4.2], and an order is Gorenstein if it is monogenic over $\mathbb{Z}$, i.e., if $\mathcal{O} = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}$ [JT15, Thm. 4.3].

2.2. **Imaginary quadratic orders.** Henceforth we suppose that K is an imaginary quadratic field. This vastly simplifies the structure of orders in K:[4] if $[\mathbb{Z}_K : \mathcal{O}] = f$ then

$$\mathcal{O} = \mathbb{Z} + f\mathbb{Z}_K,$$

and it follows that $\mathfrak{f} = f\mathbb{Z}_K$. (However $\mathfrak{f}$ is not principal, nor even invertible, as an ideal of $\mathcal{O}$.) Conversely, for any $f \in \mathbb{Z}^+$, we have that $\mathbb{Z} + f\mathbb{Z}_K$ is an order in K with index f and conductor ideal $f\mathbb{Z}_K$. Because of this simple relationship between f and $\mathfrak{f}$ in the quadratic case, from now on we will write $\mathfrak{f}$ for the positive integer $[\mathbb{Z}_K : \mathcal{O}]$.

[4]Everything that we say in this subsection for imaginary quadratic orders holds verbatim for real quadratic orders, except that the discriminant is positive and the unit group is infinite.

The discriminant of $\mathcal{O}$ is $\mathfrak{f}^2\Delta_K$, which is a negative integer congruent to 0 or 1 modulo 4. Distinct imaginary quadratic orders have different discriminants. Conversely, if Δ is a negative integer congruent to 0 or 1 modulo 4, we put

$$\tau_\Delta := \frac{\Delta + \sqrt{\Delta}}{2},$$

and then $\mathbb{Z}[\tau_\Delta]$ is an order in $\mathbb{Q}(\sqrt{\Delta})$ of discriminant Δ. It follows that every imaginary quadratic order $\mathcal{O}$ is monogenic, hence Gorenstein: proper fractional $\mathcal{O}$-ideals are invertible.

We denote the class number of the order of discriminant Δ by h_Δ.

If $\mathcal{O}$ is an imaginary quadratic order of discriminant Δ, we put

$$w_\Delta := \#\mathcal{O}^\times = \begin{cases} 6 & \Delta = -3 \\ 4 & \Delta = -4 \\ 2 & \Delta < -4 \end{cases}.$$

We also put $w_K := w_{\Delta_K}$.

2.3. **Ring class fields.** For an imaginary quadratic field K and $\mathfrak{f} \in \mathbb{Z}^+$, we denote by $K(\mathfrak{f})$ the ring class field of the unique order in K of conductor $\mathfrak{f}$. We have – eihter as a consequence of (1) or by [Cx89, Cor. 7.24]) – that

$$\mathfrak{d}(\mathfrak{f}) := [K(\mathfrak{f}) : K(1)] = \begin{cases} 1 & \mathfrak{f} = 1 \\ \frac{2}{w_K}\mathfrak{f}\prod_{\ell \mid \mathfrak{f}}\left(1 - \left(\frac{\Delta_K}{\ell}\right)\frac{1}{\ell}\right) & \mathfrak{f} \geq 2 \end{cases}. \tag{2}$$

For fixed K, the function $\mathfrak{d}$ is multiplicative in $\mathfrak{f}$ iff $\Delta_K < -4$.

From (2) we deduce the following formulas that will be useful later on.

Corollary 2.1. *Let K be an imaginary quadratic field, let $\mathfrak{f} \in \mathbb{Z}^+$, and let ℓ be a prime.*

a) *If $\mathfrak{f}^2\Delta_K = -3$, then*

$$[K(\ell\mathfrak{f}) : K(\mathfrak{f})] = [\mathbb{Q}(\sqrt{-3})(\mathfrak{f}) : \mathbb{Q}(\sqrt{-3})] = \begin{cases} \frac{\ell-1}{3} & \ell \equiv 1 \pmod 3 \\ 1 & \ell = 3 \\ \frac{\ell+1}{3} & \ell \equiv 2 \pmod 3 \end{cases}.$$

b) *If $\mathfrak{f}^2\Delta_K = -4$, then*

$$[K(\ell\mathfrak{f}) : K(\mathfrak{f})] = [\mathbb{Q}(\sqrt{-1})(\mathfrak{f}) : \mathbb{Q}(\sqrt{-1})] = \begin{cases} \frac{\ell-1}{2} & \ell \equiv 1 \pmod 4 \\ 1 & \ell = 2 \\ \frac{\ell+1}{2} & \ell \equiv 3 \pmod 4 \end{cases}.$$

c) *If* $\mathfrak{f}^2\Delta_K < -4$, *then*

$$[K(\ell\mathfrak{f}) : K(\mathfrak{f})] = \begin{cases} \ell - 1 & \left(\frac{\mathfrak{f}^2\Delta_K}{\ell}\right) = 1 \\ \ell & \left(\frac{\mathfrak{f}^2\Delta_K}{\ell}\right) = 0 \\ \ell + 1 & \left(\frac{\mathfrak{f}^2\Delta_K}{\ell}\right) = 1 \end{cases}.$$

Proposition 2.2. *Suppose* $\Delta_K < -4$. *Let* $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$, *and put* $m = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ *and* $M = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$. *As extensions of* $K(m)$, *the fields* $K(\mathfrak{f}_1)$ *and* $K(\mathfrak{f}_2)$ *are linearly disjoint and have compositum* $K(M)$.

Proof. Step 1: First we suppose that $m = 1$. For $i = 1, 2$, the conductor of the abelian extension $K(\mathfrak{f}_i)/K$ divides $\mathfrak{f}_i$, so the conductor of $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$ divides both $\mathfrak{f}_1$ and $\mathfrak{f}_2$, hence it divides $m = 1$, and it follows that $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2) = K(1)$. Since $K(\mathfrak{f}_1)/K(1)$ is Galois, this implies the linear disjointness.

Certainly we have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) \subset K(\mathfrak{f}_1\mathfrak{f}_2)$. Conversely, using the linear disjointness and the multiplicativity of $\mathfrak{d}$ we get

$$[K(\mathfrak{f}_1)K(\mathfrak{f}_2) : K(1)] = [K(\mathfrak{f}_1) : K][K(\mathfrak{f}_2) : K] = \mathfrak{d}(f_1)\mathfrak{d}(f_2) = \mathfrak{d}(f_1 f_2) = [K(\mathfrak{f}_1\mathfrak{f}_2) : K(1)],$$

so $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(\mathfrak{f}_1\mathfrak{f}_2)$.
Step 2: Again, we certainly have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) \subset K(M)$. Now write $\mathfrak{f}_1 = \prod_{i=1}^r \ell_i^{a_i}$, $\mathfrak{f}_2 = \prod_{i=1}^r \ell_i^{b_i}$, so $M = \prod_{i=1}^r \ell_i^{\max(a_i,b_i)}$. For all $1 \le i \le r$ the field $K(\mathfrak{f}_1)K(\mathfrak{f}_2)$ contains both $K(\ell_i^{a_i})$ and $K(\ell_i^{b_i})$ hence also $K(\ell_i^{\max(a_i,b_i)})$. Using Step 1 and an easy induction, we get

$$K(\mathfrak{f}_1)K(\mathfrak{f}_2) \supset K(\ell_1^{\max(a_1,b_1)}) \cdots K(\ell_r^{\max(a_r,b_r)}) = K(M).$$

Step 3: Since $K(\mathfrak{f}_1)$, $K(\mathfrak{f}_2)$ are Galois over K, they are linearly disjoint over $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$, so

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

$$= [K(\mathfrak{f}_1) : K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)][K(\mathfrak{f}_2) : K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)].$$

We claim that

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

Since $K(m) \subset K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$, the claim implies that $K(m) = K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$, which is sufficient to complete the proof. The claim equivalent to the identity

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

which holds for any multiplicative arithmetic function: using multiplicativity we reduce to $\mathfrak{f}_1 = \ell^a$, $\mathfrak{f}_2 = \ell^b$, in which case the claim is clear. □

2.4. **The connection with CM elliptic curves.** Let $E_{/\mathbb{C}}$ be an elliptic curve. There is a lattice Λ in $\mathbb{C}$, unique up to homothety, such that $E \cong \mathbb{C}/\Lambda$, and then we have

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subset \Lambda\}.$$

We say that E has **complex multiplication** if $\mathrm{End}(E)$ properly contains $\mathbb{Z}$, in which case it must be an imaginary quadratic order $\mathcal{O}$ [SI, Cor. III.9.4]. We say that E has $\mathcal{O}$-CM. If K is the fraction field of $\mathcal{O}$ we also say that E has K-CM.

Let $\mathcal{O}$ be an imaginary quadratic order, of discriminant Δ. Every $\mathcal{O}$-CM elliptic curve is uniformized by a lattice $\Lambda \subset K$, i.e., such that Λ is a fractional $\mathcal{O}$-ideal. The uniformizing lattice Λ must moreover be a proper (equivalently, invertible) $\mathcal{O}$-ideal. From this we deduce a bijection from $\mathrm{Pic}\,\mathcal{O}$ to the set of $\mathbb{C}$-isomorphism classes of $\mathcal{O}$-CM elliptic curves: in particular there are h_Δ $\mathcal{O}$-CM j-invariants. The identity of $\mathrm{Pic}\,\mathcal{O}$ corresponds to the elliptic curve $\mathbb{C}/\mathcal{O}$, and we put

$$j_\Delta := j(\mathbb{C}/\mathcal{O}).$$

If $\mathcal{O}$ is an order in K of conductor $\mathfrak{f}$, then we have [Cx89, Thm. 11.1]

$$K(\mathfrak{f}) = K(j(E)). \tag{3}$$

2.5. **Reality, part I: real moduli.** Complex conjugation acts on lattices in $\mathbb{C}$:

$$\Lambda \mapsto \overline{\Lambda} := \{\overline{z} \mid z \in \Lambda\}.$$

A lattice $\Lambda \subset \mathbb{C}$ is **real** if $\overline{\Lambda} = \Lambda$.

Lemma 2.3. *Let Λ be a lattice in $\mathbb{C}$. Then we have $j(\mathbb{C}/\overline{\Lambda}) = \overline{j(\mathbb{C}/\Lambda)}$.*

Proof. The j-invariant of a lattice depends only on its homothety class, so we may assume that $\Lambda = \mathbb{Z}1 \oplus \mathbb{Z}\tau$ for some $\tau \in \mathcal{H}$, and then $\overline{\Lambda} = \mathbb{Z}1 \oplus \mathbb{Z}\overline{\tau} = \mathbb{Z}1 \oplus \mathbb{Z} - \overline{\tau}$. Since $j(\tau) \in \mathbb{Q}(e^{2\pi i\tau}) \subset \mathbb{R}(e^{2\pi i\tau})$ and $e^{2\pi i(-\overline{\tau})} = \overline{e^{2\pi i\tau}}$, we have

$$j(\mathbb{C}/\overline{\Lambda}) = j(-\overline{\tau}) = \overline{j(\tau)} = j(\mathbb{C}/\Lambda). \qquad \square$$

Let $\mathfrak{a}$ be a proper $\mathcal{O}$-ideal. Then we have [Cx89, Lemma 7.14]

$$\mathfrak{a}\overline{\mathfrak{a}} = |\mathfrak{a}|\mathcal{O}, \tag{4}$$

where $|\mathfrak{a}| = \#\mathcal{O}/\mathfrak{a}$. It follows that $[\overline{\mathfrak{a}}] = [\mathfrak{a}]^{-1}$ in $\mathrm{Pic}\,\mathcal{O}(\Delta)$.

Lemma 2.4. [BCS17, Lemma 3.2a)] *For an elliptic curve $E_{/\mathbb{C}}$, the following are equivalent:*
(i) There is an elliptic curve $(E_0)_{/\mathbb{R}}$ such that $(E_0)_{/\mathbb{C}} \cong E$.
(ii) We have $j(E) \in \mathbb{R}$.
(iii) There is a real lattice $\Lambda \subset \mathbb{C}$ such that $E \cong \mathbb{C}/\Lambda$.
*An elliptic curve satisfying these equivalent conditions is said to be **real**.*

From this we deduce:

Corollary 2.5. [BCS17, Lemma 3.4] *For a proper fractional $\mathcal{O}$-ideal $\mathfrak{a}$, the following are equivalent:*
(i) The elliptic curve $\mathbb{C}/\mathfrak{a}$ is real.
(ii) The ideal class $[\mathfrak{a}]$ is real: $[\overline{\mathfrak{a}}] = [\mathfrak{a}]$.
(iii) The fractional ideal $\mathfrak{a}^2$ is principal, i.e., $[\mathfrak{a}] \in \operatorname{Pic}\mathcal{O}(\Delta)[2]$.

These equivalent conditions certainly hold when $\mathfrak{a}$ is a real ideal. Starting with a real ideal $\mathfrak{a}$ and scaling by $\alpha \in K^\times$ yields, in general, an ideal that is not real in the same class. However, by [BCS17, Lemma 3.6] every real ideal class contains an integral ideal $\mathfrak{a}$ that is real, proper and **primitive**: i.e., such that the isogeny $\mathbb{C}/\mathcal{O}(\Delta) \to \mathbb{C}/\mathfrak{a}^{-1}$ is cyclic.

For an order $\mathcal{O}$ in a number field K, letting $z \mapsto \overline{z}$ denote complex conjugation, we have $\overline{K(\mathcal{O})} = \overline{K}(\overline{\mathcal{O}})$. Since for an imaginary quadratic order $\mathcal{O}$ we have $\overline{\mathcal{O}} = \mathcal{O}$, this shows that $K(\mathfrak{f})$ is stable under complex conjugation, which acts nontrivially as it does so on the subfield K. Thus $\operatorname{Aut}(K(\mathfrak{f})/K)$ is a proper subgroup of $\operatorname{Aut}(K(\mathfrak{f})/\mathbb{Q})$, from which it follows that $K(\mathfrak{f})/\mathbb{Q}$ is Galois. By (4) complex conjugation acts on $\operatorname{Aut}(K(\mathfrak{f})/K)$ as inversion, and this yields an isomorphism of $\operatorname{Aut}(K(\mathfrak{f})/\mathbb{Q})$ with the semidirect product $\operatorname{Pic}\mathcal{O} \rtimes \langle c \rangle$.

Once again we have $\overline{\mathcal{O}} = \mathcal{O}$, and thus $j_\Delta = j(\mathbb{C}/\mathcal{O}) \in \mathbb{R}$. This shows that $\mathbb{Q}(\mathfrak{f}) \subset K(\mathfrak{f})^c$, and since both are number fields of degree h_Δ, we have $\mathbb{Q}(\mathfrak{f}) = K(\mathfrak{f})^c$. From this we get:

Proposition 2.6. *The number of roots j of H_Δ that lie in $\mathbb{Q}(\mathfrak{f})$ is $\#(\operatorname{Pic}\mathcal{O})[2]$.*

Corollary 2.7. *For an imaginary quadratic discriminant Δ, the following are equivalent:*
(i) *The extension $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is Galois.*
(ii) *The extension $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}$ is totally real.*
(iii) *Every Δ-CM j-invariant lies in $\mathbb{R}$.*
(iv) *We have $\operatorname{Pic}\mathcal{O} = (\operatorname{Pic}\mathcal{O})[2]$.*

Proof. The only part that does not follow immediately is (iv) $\implies$ (i). For this: if $\operatorname{Pic}\mathcal{O}$ is 2-torsion, then $\operatorname{Pic}\mathcal{O} \rtimes \langle c \rangle$ is actually a direct product, so $K(\mathfrak{f})/\mathbb{Q}$ is abelian and thus every subextension is Galois. □

It follows easily from work of Heilbronn that as we range over all imaginary quadratic orders, the ratio $\frac{\#\operatorname{Pic}\mathcal{O}}{\#(\operatorname{Pic}\mathcal{O})[2]}$ tends to ∞ with $|\Delta|$: see [CGPS, Lemma 2.2] for a more quantitatively precise version of this. In [Vo07], Voight supplies a list of 101 imaginary quadratic discriminants Δ satisfying the equivalent conditions of Corollary 2.7 and shows that the Generalized Riemann Hypothesis (GRH) implies that this list is complete.

Lemma 2.8. *For an imaginary quadratic discriminant Δ, let r be the number of distinct odd prime divisors of Δ. We define $\nu \in \mathbb{N}$ as follows:*

$$\nu = \begin{cases} r-1, \ \Delta \equiv 1 \pmod 4 \text{ or } \Delta \equiv 4 \pmod{16} \\ r, \ \Delta \equiv 8, 12 \pmod{16} \text{ or } \Delta \equiv 16 \pmod{32} \\ r+1, \ \Delta \equiv 0 \pmod{32}. \end{cases}$$

Then we have $\operatorname{Pic} \mathcal{O}(\Delta)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{\nu}$.

Proof. This is essentially due to Gauss and is part of the genus theory of binary quadratic forms. For a modern treatment see [Cx89, Prop. 3.11] or [HK13, Thm. 5.6.11]. □

A nonzero $\mathcal{O}$-ideal I is **primitive** if the additive group of $\mathcal{O}/I$ is cyclic. This holds iff there is no $N \geq 2$ such that $N^{-1}I$ remains an integral $\mathcal{O}$-ideal.

Theorem 2.9. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $\Delta = \mathfrak{f}^2 \Delta_K$.*

(i) *If there is a primitive, proper real $\mathcal{O}$-ideal of index N, then $N \mid \Delta$.*
(ii) *Let $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. There is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = N$ iff for all $1 \leq i \leq r$, there is a primitive, proper real $\mathcal{O}$-ideal I_i such that $[\mathcal{O} : I_i] = \ell_i^{a_i}$.*
(iii) *Let $\ell > 2$, and let $a \in \mathbb{Z}^+$. There is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = \ell^a$ iff $a = \operatorname{ord}_\ell(\Delta)$.*
(iv) *Let $\ell = 2$, and let $a \in \mathbb{Z}^+$.*
  i) *Suppose $16 \mid \Delta$. Then there is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = 2^a$ iff $a = 2$ or $a = \operatorname{ord}_2(\Delta) - 2$.*
  ii) *Suppose $2 \mid \Delta$ and $16 \nmid \Delta$. Then there is a primitive, proper real $\mathcal{O}$-ideal I such that $[\mathcal{O} : I] = 2^a$ iff $a = 1$.*

Proof. This is essentially due to S. Kwon [Kw99]. We have given a somewhat more explicit treatment following [BC20b, Lemma 5.6]. □

2.6. **Rational ring class fields.** Let $\Delta = \mathfrak{f}^2 \Delta_K$ be an imaginary quadratic discriminant. The **Hilbert class polynomial** $H_\Delta(t) \in \mathbb{C}[t]$ is the monic polynomial whose roots are the j-invariants of Δ-CM elliptic curves. It is known that $H_\Delta \in \mathbb{Z}[t]$ and that H_Δ is irreducible over K [Cx89, §13], so $K[t]/(H_\Delta) \cong K(\mathfrak{f})$.

The Hilbert class polynomial H_Δ is in particular irreducible over $\mathbb{Q}$ so is the minimal polynomial of j_Δ. We define the **rational ring class field**

$$\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}(j_\Delta) \cong \mathbb{Q}[t]/(H_\Delta).$$

(Our notation suppresses K. It might at first seem better to index the rational ring class field by its discriminant, from which we can recover K. But in practice the $\mathbb{Q}(\mathfrak{f})$ notation, which was introduced in [BC20a] and also used in [BC20b], seems more convenient.)

For fixed K, the rational ring class fields form a directed system in $\mathfrak{f}$: if $\mathfrak{f}_1 \mid \mathfrak{f}_2$ then $\mathbb{Q}(\mathfrak{f}_1) \subseteq \mathbb{Q}(\mathfrak{f}_2)$. To see this, let $\mathcal{O}$ and $\mathcal{O}'$ be the orders in K of conductor $\mathfrak{f}_1$ and $\mathfrak{f}_2$, so $\mathcal{O}' \subset \mathcal{O}$. It follows from [BC20b, §2.6] that the isogeny $\mathbb{C}/\mathcal{O}' \to \mathbb{C}/\mathcal{O}$ can be defined over $\mathbb{Q}(j(\mathbb{C}/\mathcal{O}')) = \mathbb{Q}(\mathfrak{f}_2)$. Therefore $\mathbb{Q}(\mathfrak{f}_2) \supset \mathbb{Q}(j(\mathbb{C}/\mathcal{O})) = \mathbb{Q}(\mathfrak{f}_1)$.

Proposition 2.10. *Suppose $\Delta_K < -4$. Let $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$, and put $m = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ and $M = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$.*
a) The fields $\mathbb{Q}(\mathfrak{f}_1)$ and $\mathbb{Q}(\mathfrak{f}_2)$ are linearly disjoint over $\mathbb{Q}(m)$.
b) We have $\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(M)$.

Proof. a) We have that $E \coloneqq \mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(m)} \mathbb{Q}(\mathfrak{f}_2)$ is an étale $\mathbb{Q}(m)$-algebra, hence isomorphic to a product of field extensions of $\mathbb{Q}(m)$. Extending scalars from $\mathbb{Q}(m)$ to $K(m)$, we get the $K(m)$-algebra $K(\mathfrak{f}_1) \otimes_{K(m)} K(\mathfrak{f}_2)$ [Co2, Thm. 6.22], which by Proposition 2.2 is the field $K(M)$. Thus E is a domain and hence a field, which shows that $\mathbb{Q}(\mathfrak{f}_1)$ and $\mathbb{Q}(\mathfrak{f}_2)$ are linearly disjoint over $\mathbb{Q}(m)$.
b) By part a) and the proof of Proposition 2.2, we have that $\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2)$ is a subextension of $\mathbb{Q}(M)/\mathbb{Q}(m)$ of degree $\frac{\mathfrak{d}(\mathfrak{f}_1)}{\mathfrak{d}(m)}\frac{\mathfrak{d}(\mathfrak{f}_2)}{\mathfrak{d}(m)} = \frac{\mathfrak{d}(M)}{\mathfrak{d}(m)} = [\mathbb{Q}(M) : \mathbb{Q}(m)]$, so $\mathbb{Q}(\mathfrak{f}_1)\mathbb{Q}(\mathfrak{f}_2) = \mathbb{Q}(M)$. □

Corollary 2.11. *Let $\mathfrak{f}, \mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$ with $\gcd(\mathfrak{f}_1, \mathfrak{f}_2) = \mathfrak{f}$, and put $M = \operatorname{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$. Then:*
a) We have $\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\mathfrak{f}_2) \cong \mathbb{Q}(M)$.
b) We have $\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_2) \cong K(M)$.
c) We have $K(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_2) \cong K(M) \times K(M)$.

Proof. a) This is immediate from Proposition 2.10.
b) The $\mathbb{Q}(\mathfrak{f})$-bilinear map $\mathbb{Q}(\mathfrak{f}_1) \times K(\mathfrak{f}_2) \to K(M)$ given by $(x, y) \mapsto xy$ induces a surjective homomorphism $\Phi : \mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_2) \to K(M)$ of $\mathbb{Q}(\mathfrak{f})$-algebras of equal, finite dimension, so Φ is an isomorphism.
c) Using part b), we have

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

so

$$\begin{aligned} K(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}_2) &\cong (\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f}))_{\otimes_{\mathbb{Q}(\mathfrak{f})}} (\mathbb{Q}(\mathfrak{f}_2) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f})) \\ &\cong (\mathbb{Q}(\mathfrak{f}_1) \otimes_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\mathfrak{f}_2)) \otimes_{\mathbb{Q}(\mathfrak{f})} (K(\mathfrak{f}) \otimes_{\mathbb{Q}(\mathfrak{f})} K(\mathfrak{f})) \\ &\cong \mathbb{Q}(M) \otimes_{\mathbb{Q}(\mathfrak{f})} (K(\mathfrak{f}) \times K(\mathfrak{f})) \cong K(M) \times K(M). \end{aligned}$$

□

3. Isogenies of Elliptic Curves

In this section we recall some basic facts and establish some results on isogenies of elliptic curves in characteristic 0. Some of our results pertain all elliptic curves, and one result (Proposition 3.3), focus specifically on elliptic curves *without* complex multiplication.

3.1. **Basic facts on isogenies.** Let F be a subfield of $\mathbb{C}$. For $i = 1, 2$, let $\iota_i : E_i \to E_i'$ be F-rational isogenies of elliptic curves. We say that ι_1 and ι_2 are **isomorphic** if there are F-rational isomorphisms $\alpha : E_1 \to E_2$ and $\beta : E_1' \to E_2'$ such that

$$\iota_2 = \beta \circ \iota_1 \circ \alpha^{-1}.$$

We have that ι_1 and ι_2 are isomorphic over $\overline{F}$ (the algebraic closure of F in $\mathbb{C}$) iff they are isomorphic over $\mathbb{C}$.

Let $\iota : E \to E'$ be an F-rational isogeny of degree N. Then its kernel K is an F-rational finite (necessarily étale, since we are in characteristic zero) subgroup scheme of E of order N. Let $q : E \to E/K$ be the quotient map. Then there is an F-isomorphism $\beta : E/K \to E'$ such that $\iota = \beta \circ q$, so q is isomorphic to ι over F. Now let $\iota_i : E \to E_i'$ for $i = 1, 2$ – that is, this time the two source elliptic curves are the same – and for $i = 1, 2$, let $K_i = \operatorname{Ker} \iota_i$.

If $K_1 = K_2 = K$ say, then ι_1 and ι_2 are both isomorphic to $E \to E/K$ and thus to each other. Conversely, if ι_1 and ι_2 are isomorphic then there is $\alpha \in \operatorname{Aut} E$ and $\beta : E_1' \to E_2'$ such that $\iota_2 = \beta \circ \iota_1 \circ \alpha^{-1}$. If $\alpha = \pm 1$, then $K_1 = K_2$. It follows that if $\operatorname{Aut}_F(E) = \{\pm 1\}$ then isomorphism classes of F-rational isogenies with source elliptic curve E correspond bijectively to finite F-subgroup schemes of E. When $j = 0, 1728$ and F contains $\mathbb{Q}(\sqrt{-3})$ (resp. $\mathbb{Q}(\sqrt{-1})$) we get that isomorphism classes of F-rational isogenies with source elliptic curve E correspond bijectively to $\operatorname{Aut}(E)$-orbits of finite F-subgroup schemes of E.

Lemma 3.1. *Let $E_{/F}$ be an elliptic curve such that $\operatorname{Aut}_F(E) = \{\pm 1\}$. Let ℓ be a prime number. The number of isomorphism classes of F-rational ℓ-isogenies with source elliptic curve E – equivalently, the number of F-rational points in the fiber of the F-morphism $X_0(\ell) \to X(1)$ over $j(E)$ – is 0, 1, 2 or $\ell + 1$.*

Proof. The hypothesis $\operatorname{Aut}_F(E) = \{\pm 1\}$ means that we need to count the number of $\mathfrak{g}_F = \operatorname{Aut}(\overline{F}/F)$-stable order ℓ-subgroups of $E[\ell]$, which is in turn equivalent to counting the $\mathfrak{g}_F$-stable lines in $E[\ell]$ viewed as a two-dimensional $\mathbb{Z}/\ell\mathbb{Z}$-vector space. Since the total number of lines in this space is $\ell + 1$, it suffices to see that more than two Galois-invariant lines makes all the lines Galois invariant. So let L_1 and L_2 be Galois invariant lines, and choose $e_i \in L_i \setminus \{0\}$ for $i = 1, 2$. Then e_1, e_2 is a $\mathbb{Z}/\ell\mathbb{Z}$-basis for $E[\ell]$ with respect to which Galois acts via diagonal matrices. A nonscalar diagonal matrix has distinct eigenvalues so does not fix any other line, and thus the only way for the Galois action to have more than two invariant lines is if it consists of scalar matrices, in which case all lines are invariant. □

3.2. **Factorization of isogenies.** Let $\iota : E \to E'$ be an isogeny of complex elliptic curves, with kernel K. There are positive integers $M \mid N$ such that

$$K \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

We say that ι is **cyclic** if $M = 1$.

Let $\iota' : E \to E''$ be another isogeny, with kernel K'. Then ι factors through ι' – i.e., there is an isogeny $\alpha : E'' \to E'$ such that $\iota = \alpha \circ \iota'$ – if and only if $K' \subset K$, and if this holds then $\operatorname{Ker} \alpha \cong K/K'$. In particular, since $E[M] \subset K$, we get a factorization

$$\iota = \iota_{\mathrm{cyc}} \circ [M],$$

where $\iota_{\mathrm{cyc}} : E \to E'$ is a cyclic $\frac{N}{M}$-isogeny.

Let $\iota : E \to E'$ be a cyclic N-isogeny, and factor $N = \ell_1 \cdots \ell_r$ into a product of not necessarily distinct primes which need not be in nondecreasing order. Put $E_1 = E$ and $E_{r+1} = E'$. We get a unique factorization $\iota = \iota_r \circ \cdots \circ \iota_1$ with $\iota_i : E_i \to E_{i+1}$ an ℓ_i-isogeny.

3.3. **The field of moduli of an isogeny.** An isogeny $\iota : E \to E'$ of complex elliptic curves has a **field of moduli** $\mathbb{Q}(\iota)$, characterized by each of the following properties:

• Let $H(\iota)$ be the subgroup of $\operatorname{Aut} \mathbb{C}$ such that for all $\sigma \in H(\iota)$, the isogeny ι is isomorphic over $\mathbb{C}$ to $\sigma(\iota) : \sigma(E) \to \sigma(E')$. Then $\mathbb{Q}(\iota) = \mathbb{C}^{H(\iota)}$.
• If E, E' and ι are defined over a subfield F of $\mathbb{C}$, then $\mathbb{Q}(\iota) \subset F$, and there is a model of

E, E' and ι defined over F.
• If ι is moreover cyclic of degree N, then $\mathbb{Q}(\iota)$ is isomorphic to the residue field of the induced point on the modular curve $X_0(N)$.

For any isogeny $\iota : E \to E'$, let $\iota^\vee : E' \to E$ be the dual isogeny: the unique isogeny such that $\iota^\vee \circ \iota = [\deg(\iota)]$.

If $\iota_1 : E_1 \to E_2$ and $\iota_2 : E_2 \to E_3$ are isogenies of complex elliptic curves, then

$$\mathbb{Q}(\iota_2 \circ \iota_1) \subset \mathbb{Q}(\iota_1)\mathbb{Q}(\iota_2).$$

In general we need not have equality: e.g. if $\iota_1 : E_1 \to E_2$ is an isogeny such that $\mathbb{Q}(\iota) \supsetneq \mathbb{Q}(j(E_1))$, then taking $\iota_2 : E_2 \to E_1$ to be the dual isogeny, we have $\mathbb{Q}(\iota_2 \circ \iota_1) = \mathbb{Q}([\deg \iota_1]) = \mathbb{Q}(j(E_1))$. However:

Proposition 3.2. a) *For an isogeny $\iota : E \to E'$ with associated cyclic isogeny $\iota_{\mathrm{cyc}} : E \to E'$, we have $\mathbb{Q}(\iota) = \mathbb{Q}(\iota_{\mathrm{cyc}})$.*
b) *If $\iota : E_1 \to E_3$ is a cyclic isogeny and $\iota = \iota_2 \circ \iota_1$ with $\iota_1 : E_1 \to E_2$ and $\iota_2 : E_2 \to E_3$, then $\mathbb{Q}(\iota) = \mathbb{Q}(\iota_1)\mathbb{Q}(\iota_2)$.*

Proof. a) Suppose that $\operatorname{Ker} \iota \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Then as above we have $\iota = \iota_{\mathrm{cyc}} \circ [M]_E$, where $\iota_{\mathrm{cyc}} : E \to E'$ is cyclic of degree $\frac{N}{M}$. Then we have $\mathbb{Q}(\iota)\mathbb{Q}(\iota_{\mathrm{cyc}})$. Indeed, as above we have $\mathbb{Q}(\iota_{\mathrm{cyc}}) = \mathbb{Q}(\iota_{\mathrm{cyc}})\mathbb{Q}([M]_E) \supseteq \mathbb{Q}(\iota)$. Conversely, there is a model of E defined over $\mathbb{Q}(\iota)$ and a $\mathbb{Q}(\iota)$-subgroup scheme K of E such that $E/K \cong_{\mathbb{C}} E'$. Then the morphism $E/E[M] \to E/K$ gives a $\mathbb{Q}(\iota)$-rational model of ι_{cyc}.
b) As above it is clear that $\mathbb{Q}(\iota) \supset \mathbb{Q}(\iota_1)\mathbb{Q}(\iota_2)$, so it suffices to show that ι_1 and ι_2 can each be defined over $\mathbb{Q}(\iota)$. For $i = 1, 2$ put $d_i := \deg \iota_i$, so $d_1 d_2 = \deg(\iota)$. There is a model of E_1 over $\mathbb{Q}(\iota)$ and a $\mathbb{Q}(\iota)$-rational subgroup scheme K with underlying group $\mathbb{Z}/d_1 d_2\mathbb{Z}$ such that $E_1 \to E_1/K$ gives a $\mathbb{Q}(\iota)$-rational model of ι, up to isomorphism. Put $K_1 := K[d_1]$, so K_1 is a $\mathbb{Q}(\iota)$-rational subgroup scheme that is cyclic of order d_1. The map $E \to E/K_1$ gives a $\mathbb{Q}(\iota)$-rational model for ι_1, up to isomorphism, and the map $E/K_1 \to E/K$ gives a $\mathbb{Q}(\iota)$-rational model for ι_2, up to isomorphism. □

If $\iota : E \to E'$ is an isogeny of elliptic curves, then clearly any field of definition for ι must also be a field of definition for E and for E', and thus we get $\mathbb{Q}(\iota) \supset \mathbb{Q}(j(E), j(E'))$. It turns out that in the absence of complex multiplication, this evident lower bound for the field of moduli is an equality.[5]

Proposition 3.3. *Let $\iota : E \to E'$ be an isogeny of elliptic curves defined over the complex numbers. If E (hence also E') does* not *have complex multiplication, then we have*

$$\mathbb{Q}(\iota) = \mathbb{Q}(j(E), j(E')).$$

Proof. Let $N = \deg \iota$. Put $F := \mathbb{Q}(j(E), j(E'))$, and choose a model $E_{/F}$. Let C be the kernel of ι. We may view C as an $\operatorname{Aut} E = \{\pm 1\}$, so automorphisms of E preserve C. Since $E' \cong E/C$ we have $j(E/C) = j(E') \in F$.

[5]It is hard for me to believe that the following result is new, but I have not found it in the literature.

We must show that for all $\sigma \in \mathfrak{g}_F$, we have $\sigma(C) = C$. Suppose that we have $\sigma(C) \neq C$ for some $\sigma \in \mathfrak{g}_F$, and consider the "transported" isogeny $\sigma(\iota) : E^\sigma \to (E/C)^\sigma$. Because E is defined over F, we have $E^\sigma = E$, and because $j(E/C) \in F$ we have that $(E/C)^\sigma$ is isomorphic to E/C hence also to E', so after composing $\sigma(\iota)$ with such an isomorphism we get a cyclic N-isogeny $\psi : E \to E'$ with kernel $\sigma(C)$.

Thus we are in the following situation: we have two complex elliptic curves E, E' and two cyclic N-isogenies $\iota, \psi : E \to E'$ with distinct kernels. We claim that this implies that E has complex multiplication. To see this, consider

$$\xi := \iota^\vee \circ \psi : E \to E,$$

an endomorphism of E of degree N^2. Since E does not have CM, we must have $\xi = \pm[N]$. But we have $\iota^\vee \circ \psi = [N]$ iff $\iota^\vee = \psi^\vee$ iff $\iota = \psi$. Similarly, we have $\iota^\vee \circ \psi = -[N]$ iff $\iota^\vee \circ (-\psi) = [N]$ iff $\iota = -\psi$. Either way we get $\ker \iota = \ker \psi$, a contradiction. □

The proof of Proposition 3.3 also establishes the following result.

Corollary 3.4. *Let $\iota : E \to E'$ be an isogeny of complex elliptic curves, of degree N. If $j(E) \notin \{0, 1728\}$ and $C = \operatorname{Ker} \iota$ is the unique order N subgroup of E such that $E/C \cong E'$, then $\mathbb{Q}(\iota) = \mathbb{Q}(j(E), j(E'))$.*

Example 3.5. *Let Δ be an imaginary quadratic discriminant, let $K = \mathbb{Q}(\sqrt{\Delta})$, let $\mathcal{O}$ be the order in K with discriminant Δ, and let p be a prime number such that $p \nmid \Delta$ and p splits completely in the Hilbert class field of K (the set of such primes has density $\frac{1}{2h_K}$ so is infinite). The hypotheses ensure that there is an element $\pi \in \mathcal{O}$ such that $p\mathcal{O} = (\pi)(\overline{\pi})$ with $(\pi) \neq (\overline{\pi})$. Let $E_{/\mathbb{C}}$ be any $\mathcal{O}$-CM elliptic curve. Let ι be multiplication by π, viewed as an isogeny from E to E. Its kernel is $E[(\pi)]$. Complex conjugation takes $E[(\pi)]$ to the distinct order p subgroup scheme $E[(\overline{\pi})]$. It follows that*

$$\mathbb{Q}(\iota) = K(j(E)) \supsetneq \mathbb{Q}(j(E)) = \mathbb{Q}(j(E), j(E')).$$

On the other hand, it will follow from the main results of this paper that if $\iota : E \to E'$ is an isogeny between elliptic curves with CM by an order in the imaginary quadratic field K, then we always have $\mathbb{Q}(\iota) = \mathbb{Q}(j(E), j(E'))$ or $\mathbb{Q}(\iota) = K(j(E), j(E'))$. It can happen that $K \in \mathbb{Q}(j(E), j(E'))$ so these fields coincide. However, as seen in Example 3.5 above, this does not always happen.

3.4. **Proper and pleasant isogenies.** All of the results of this section are recalled from [BC20b, §2.6]: the only novelty here is the introduction of the adjective "pleasant."

We call an isogeny $\varphi : E \to E'$ of K-CM elliptic curves a **proper isogeny** if $\operatorname{End}(E) \cong \operatorname{End}(E')$. For every proper isogeny there is a unique proper $\mathcal{O}$-ideal $\mathfrak{a}$ such that φ is isomorphic over $\mathbb{C}$ to $q : E \to E/E[\mathfrak{a}]$. Conversely, for every proper $\mathcal{O}$-ideal $\mathfrak{a}$ we have $\operatorname{End}(E/E[\mathfrak{a}]) = E$, so $q : E \to E/[\mathfrak{a}]$ is a proper isogeny, of degree $|\mathfrak{a}| := \#\mathcal{O}/\mathfrak{a}$. Moreover, for a proper isogeny $\varphi : E \to E'$ its field of moduli is $\mathbb{Q}(j(E))$ if the corresponding ideal $\mathfrak{a}$ is real – $\overline{\mathfrak{a}} = \mathfrak{a}$ – and is $K(j(E))$ otherwise.

Let $\mathfrak{f}' \mid \mathfrak{f}$, and let $\mathcal{O}$ (resp. $\mathcal{O}'$) be the order in K of conductor $\mathfrak{f}$ (resp. $\mathfrak{f}'$). If $E_{/\mathbb{C}}$ is an $\mathcal{O}$-CM elliptic curve, then there is an $\mathcal{O}'$-CM elliptic curve $\tilde{E}_{/\mathbb{C}}$ and an isogeny

$$\iota_{\mathfrak{f},\mathfrak{f}'} : E \to \tilde{E}$$

that is universal for isogenies from E to an $\mathcal{O}'$-CM elliptic curve $E'_{/\mathbb{C}}$. Moreover $\iota_{\mathfrak{f},\mathfrak{f}'}$ is cyclic of order $\frac{\mathfrak{f}}{\mathfrak{f}'}$ and the field of moduli of $\iota_{\mathfrak{f},\mathfrak{f}'}$ is $\mathbb{Q}(\mathfrak{f})$.

Lemma 3.6. *Let Δ be an imaginary quadratic discriminant, and let $E_{/\mathbb{C}}$ be a Δ-CM elliptic curve such that $j(E) \in \mathbb{R}$. Let $\iota : E \to E'$ be a proper isogeny, with associated proper $\mathcal{O}$-ideal $\mathfrak{a}$. The following are equivalent:*

(i) *We have $j(E') \in \mathbb{R}$.*
(ii) *We have $[\mathfrak{a}] \in (\operatorname{Pic}\mathcal{O})[2]$.*

Proof. By [BCS17, Lemma 3.6] there is a proper, real $\mathcal{O}$-ideal I such that $E \cong \mathbb{C}/I$, and then the isogeny $E \to E'$ is isomorphic to $\mathbb{C}/I \to \mathbb{C}/\mathfrak{a}^{-1}I$. By Lemma 2.3, we have $j(E') \in \mathbb{R}$ iff $j(\mathbb{C}/\mathfrak{a}^{-1}I) = j(\mathbb{C}/\overline{\mathfrak{a}^{-1}I}) = j(\mathbb{C}/\overline{\mathfrak{a}}^{-1}I)$. This holds iff $[\overline{\mathfrak{a}}^{-1}I] = [\mathfrak{a}^{-1}I] \in \operatorname{Pic}\mathcal{O}$ iff $[\mathfrak{a}] = [\overline{\mathfrak{a}}] \in \operatorname{Pic}\mathcal{O}$. Since $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}$, we also have $[\overline{\mathfrak{a}}] = [\mathfrak{a}]^{-1} \in \operatorname{Pic}\mathcal{O}$, hence these conditions hold iff $[\mathfrak{a}] \in (\operatorname{Pic}\mathcal{O})[2]$. □

We say an isogeny $\iota : E \to E''$ of K-CM elliptic curves over $\mathbb{C}$ is **pleasant** if the conductor $\mathfrak{f}'$ of $\operatorname{End}(E'')$ divides the conductor $\mathfrak{f}$ of $\operatorname{End}(E)$. Thus ι factors as $\varphi \circ \iota_{\mathfrak{f},\mathfrak{f}'}$ for a proper isogeny $\varphi : \tilde{E} \to E'$ that corresponds to a proper $\mathcal{O}'$-ideal $\mathfrak{a}$. It follows that

$$\mathbb{Q}(\iota) = \begin{cases} \mathbb{Q}(\mathfrak{f}) & \mathfrak{a} \text{ is real} \\ K(\mathfrak{f}) & \text{otherwise} \end{cases}.$$

A factor isogeny of a proper isogeny need not be proper, and similarly for pleasant isogenies. On the other hand, for a prime degree isogeny $\iota : E \to E'$, exactly one of the following holds: ι and $\iota^\vee$ are both proper and pleasant; ι is pleasant but not proper and $\iota^\vee$ is neither proper nor pleasant; $\iota^\vee$ is pleasant but not proper and ι is neither proper nor pleasant.

3.5. **Reduction to the prime power case.** Let $\varphi : E \to E'$ be a cyclic N-isogeny of elliptic curves defined over a subfield $F \subset \mathbb{C}$, so φ is equivalent to $E \to E/C$, for $C \subset E(\overline{F})$ a $\mathfrak{g}_F$-stable cyclic subgroup of order N. If $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ for primes $\ell_1 < \ldots < \ell_r$ and positive integers $a_1 < \ldots < a_r$, then $C = \bigoplus_{i=1}^r C_i$, where C_i is the unique subgroup of order $\ell_i^{a_i}$. The uniqueness guarantees that C_i is $\mathfrak{g}_F$-stable, hence $\varphi_i := E \to E/C_i$ is an F-rational cyclic $\ell_i^{a_i}$-isogeny. Conversely, given for each $1 \le i \le r$ an F-rational cyclic $\ell_i^{a_i}$-isogeny $\varphi_i : E \to E_i$, then taking $C_i = \operatorname{Ker}\varphi_i$, the map $E \to E/\langle C_1, \ldots, C_r\rangle$ is an F-rational cyclic $\ell_i^{a_i}$-isogeny. (Throughout we could have replaced prime powers by pairwise coprime positive integers $n_1, \ldots, n_r$, but no generality is gained by doing so.)

We now consider a subtly different setup: suppose that for $1 \le i \le r$ we are given a cyclic $\ell_i^{a_i}$-isogeny of complex elliptic curves $\varphi_i : E \to E_i$, each with field of moduli contained in a subfield $F \subset \mathbb{C}$. As above, let $C_i = \operatorname{Ker}\varphi_i$ and put $\varphi : E \to E/\langle C_1, \ldots, C_r\rangle$. Is the field of moduli of φ contained in F? It turns out that this is always the case

when $j(E) \notin \{0, 1728\}$. Indeed, if F is a subfield of $\mathbb{C}$ and $E_{/\mathbb{C}}$ is an elliptic curve with $j(E) \in F \setminus \{0, 1728\}$, then $\operatorname{Aut} E = \{\pm 1\}$, so for any two F-rational models of E and any $N \in \mathbb{Z}^+$, the two modulo N Galois representations differ by a quadratic character, and thus whether a finite subgroup of $E[N](\overline{F})$ is $\mathfrak{g}_F$-stable is independent of the chosen F-rational model. This shows that for any F-rational model of E and $1 \leq i \leq r$, there is a $\mathfrak{g}_F$-stable finite subgroup C_i of $E(\overline{F})$ of order $\ell_i^{a_i}$, and thus $E \to E/\langle C_1, \ldots, C_r\rangle$ is an F-rational cyclic $\ell_1^{a_1} \cdots \ell_r^{a_r}$-isogeny.

By [BC20b, Thm. 6.18c)], there are elliptic curves $(E_1)_{/\mathbb{Q}(\sqrt{-3})}$ and $(E_2)_{/\mathbb{Q}(\sqrt{-3})}$ such that $j(E_1) = j(E_2) = 0$, the curve E_1 admits a $\mathbb{Q}(\sqrt{-3})$-rational 2-isogeny and the curve E_2 admits a $\mathbb{Q}(\sqrt{-3})$-rational cyclic 9-isogeny, but there is no elliptic curve $E_{/\mathbb{Q}(\sqrt{-3})}$ that admits a $\mathbb{Q}(\sqrt{-3})$-rational cyclic 18-isogeny. By [BC20b, Cor. 5.11b)] the same holds with the ground field $\mathbb{Q}(\sqrt{-3})$ replaced by $\mathbb{Q}$ throughout the assertions of the previous sentence. On the other hand, [BC20b, Thm. 6.18b)] and [BC20a, Cor. 5.11a)] show that over $F = \mathbb{Q}$ or $F = \mathbb{Q}(\sqrt{-1})$, if for all $1 \leq i \leq r$ there is an elliptic curve $(E_i)_{/F}$ with j-invariant 1728 and admitting an F-rational cyclic $\ell_i^{a_i}$-isogeny, then there is an elliptic curve $E_{/F}$ with j-invariant 1728 and admitting an F-rational cyclic $\ell_1^{a_1} \cdots \ell_r^{a_r}$-isogeny. In both cases this comes from a complete enumeration of the set of positive integers N for which there is an elliptic curve with j-invariant 1728 and an F-rational cyclic N-isogeny. At present it is not clear to me whether a similar "primary decomposition" phenomenon holds for isogenies of elliptic curves with j-invariant 1728 defined over any fixed number field F.

Lemma 3.7. *Let $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. Let k be any field of characteristic 0, and let P be any closed point on $X_0(N)_{/k}$ such that $j(P) \notin \{0, 1728\}$. For all $1 \leq i \leq r$, let $\pi_i : X_0(N) \to X_0(\ell_i^{a_i})$ be the forgetful modular map, viewed as a morphism of k-schemes. Then the residue field $k(P)$ is the compositum $\prod_{i=1}^r k(\pi_i(P))$ of the residue fields $k(\pi_i(P))$ for $1 \leq i \leq r$.*

Proof. Let $l \coloneqq k(\pi_1(P)) \cdots k(\pi_r(P))$. The containment $k(P) \supset l$ is immediate (and holds for any finite morphisms $\{\pi_i : X \to Y_i\}_{i=1}^n$ of k-varieties). For the converse, the field of moduli of a point on $X_0(N)$ is always a field of definition, so over l we have for each $1 \leq i \leq r$ an elliptic curve E_i with j-invariant $j(P)$ and an l-rational cyclic $\ell_i^{a_i}$-isogeny $\varphi_i : E_i \to E_i'$. Let K_i be its kernel. Fix $E_{/l}$ an elliptic curve with $j(E) = j(P)$. Because $j(P) \notin \{0, 1728\}$, all the subgroups K_i remain l-rational on E. Let $K = K_1 + \ldots + K_r$. Then $\varphi : E \to E/K$ is an l-rational isogeny that induces the point $P \in X_0(N)$. □

In fact:

Proposition 3.8. *Let $N_1, \ldots, N_r \in \mathbb{Z}^+$ be pairwise coprime. For $1 \leq i \leq r$, let $M_i \in \mathbb{Z}^+$ be such that $M_i \mid N_i$. Let K be a field of characteristic 0, and let $p \in X(1)_{/K}$ be a closed point. For $1 \leq i \leq r$, let $\pi_i : X_0(M_i, N_i) \to X(1)$ be the natural map, let F_i be the fiber of π_i over p, and let F be the fiber of $X_0(M_1 \cdots M_r, N_1 \cdots N_r) \to X(1)$ over p. Then F is the fiber product of $F_1, \ldots, F_r$ over* $\operatorname{Spec} K(p)$.

Proof. Induction reduces us to the case of $r = 2$. We claim that $X_0(M_1M_2, N_1N_2) \to X(1)$ is the fiber product of $X_0(M_1, N_1) \to X(1)$ and $X_0(M_2, N_2) \to X(1)$ in the category of K-schemes. To see this, first we observe that the function fields $\mathbb{Q}(X_0(M_1, N_1))$

and $\mathbb{Q}(X_0(M_2,N_2))$ are linearly disjoint over $\mathbb{Q}$: for $i=1,2$ we have $\mathbb{Q}(X_0(M_i,N_i)) \subset \mathbb{Q}(X(N_i))$; the fields $\mathbb{Q}(X(N_1))$ and $\mathbb{Q}(X(N_2))$ are each Galois over $\mathbb{Q}(X(1))$; and we have $\mathbb{Q}(X(N_1)) \cap \mathbb{Q}(X(N_2)) = \mathbb{Q}(X(1))$. Second we observe that

$$[\mathbb{Q}(X_0(M_1,N_1)) \otimes_{\mathbb{Q}(X(1))} \mathbb{Q}(X_0(M_2,N_2)) : \mathbb{Q}(X(1))]$$
$$= [\mathbb{Q}(X_0(M_1,N_1)) : \mathbb{Q}(X(1))][\mathbb{Q}(X_0(M_2,N_2)) : \mathbb{Q}(X(1))]$$
$$= (M_1\varphi(M_1)\psi(N_1))(M_2\varphi(M_2)\psi(N_2)) = M_1M_2\varphi(M_1M_2)\psi(N_1N_2) = [\mathbb{Q}(X_0(M_1,N_1)) : \mathbb{Q}(X(1))].$$

Thus we have

$$\mathbb{Q}(X_0(M_1,N_1)) \otimes_{\mathbb{Q}(X(1))} \mathbb{Q}(X_0(M_2,N_2)) = \mathbb{Q}(X_0(M_1M_2,N_1N_2)),$$

establishing the claim. The closed point p gives a morphism $\operatorname{Spec} K(p) \to X(1)$. Since fiber products are preserved by base change, the $\operatorname{Spec} K(p)$-scheme $X_0(M_1M_2,N_1N_2) \times_{X(1)} \operatorname{Spec} K(p)$ is the fiber product of $X_0(M_1,N_1) \times_{X(1)} \operatorname{Spec} K(p)$ and $X_0(M_2,N_2) \times_{X(1)} \operatorname{Spec} K(p)$, and this establishes the result. □

Remark. Proposition 3.8 is an instance of moduli of isogenies behaving better than moduli of torsion points. The proof of Proposition 3.8 fails with $X_0(M_i,N_i)$ replaced by $X_1(M_i,N_i)$ because $[\mathbb{Q}(X_1(M_i,N_i)) : \mathbb{Q}(X_0(M_i,N_i))] = \frac{\varphi(N_i)}{2}$, and while $\varphi(N_i)$ is a multiplicative function of N_i, $\frac{\varphi(N_i)}{2}$ is not. Indeed the result is not true at the torsion level: the field of moduli $\mathbb{Q}(P)$ of a closed point $P \in X_1(N)_{/\mathbb{Q}}$ is obtained by adjoining to $j(P)$ the x-coordinate (a.k.a. Weber function) of the corresponding point of order N. If $N = N_1N_2$ with $\gcd(N_1,N_2)$ and p is a point of order N on an elliptic curve $E_{/F}$ then certainly $F(p) = F([N_1]p,[N_2]p)$, but there is no reason to expect $F(x(p)) = F(x([N_1]p),x([N_2]p))$ and indeed it is not hard to find counterexamples.

4. Isogeny Volcanoes

4.1. **The isogeny graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.** Fix a prime number ℓ and an imaginary quadratic field. We define a directed multigraph $\mathcal{G}_{K,\ell}$ as follows: the vertex set $\mathcal{V}$ of $\mathcal{G}_{\ell,K}$ 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. The edges are obtained as follows: let $\pi_1 : X_0(\ell) \to X(1)$ be the natural map, let $w_N \in \operatorname{Aut}(X_0(N))$ be the Atkin-Lehner involution, and let $\pi_2 : X_0(\ell) \coloneqq \pi_1 \circ \pi_2$: here we work with curves 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 $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$ be the ℓth modular polynomial. Then $e_{j'}$ is the multiplicity to which j' occurs as a root of the univariate polynomial $\Phi_\ell(j,Y)$.

Each $j \in \mathcal{V}$ has outward degree $\ell+1$. When $j \neq 0,1728$, the map π_1 is unramified over j, and we may identify the edges emanating from the vertex j with isomorphism classes of ℓ-isogenies with target elliptic curve E_j and thus also with order ℓ subgroups of E_j. There is at least one directed edge from j to j' iff there is an ℓ-isogeny $\iota : E_j \to E_{j'}$. The dual

isogeny $\iota^\vee : E_{j'} \to E_j$ then shows that there is at least one directed edge from j' to j. When $j, j' \notin \{0, 1728\}$, taking the dual isogeny gives a bijection from the set of directed edges $j \to j'$ to the set of directed edges $j' \to j$, so one may safely neglect orientations of such edges. This need not be the case if $j, j' \in \{0, 1728\}$.

Let $\iota : E \to E'$ be an ℓ-isogeny of K-CM elliptic curves. We put $\mathcal{O} \coloneqq \mathrm{End}(E)$ and $\mathcal{O}' \coloneqq \mathrm{End}(E')$. Thus $\mathcal{O}$ and $\mathcal{O}'$ are each orders in K. Let $\mathfrak{f}$ (resp. $\mathfrak{f}'$) be the conductor of $\mathcal{O}$ (resp. of $\mathcal{O}'$). Then by e.g. [BC20b, §5.5] we have

$$\frac{\mathfrak{f}}{\mathfrak{f}'} \in \{1, \ell, \ell^{-1}\}. \tag{5}$$

Lemma 4.1. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K of conductor divisible by a prime ℓ. Then no $\mathcal{O}$-CM elliptic curve $E_{/\mathbb{C}}$ admits a proper ℓ-isogeny. Equivalently, there is no proper $\mathcal{O}$-ideal of norm ℓ.*

Proof. First proof: Let $\mathfrak{p}$ be an ideal of norm ℓ, i.e., $\#\mathcal{O}/\mathfrak{p} = \ell$. Then $\mathfrak{p}$ is maximal and contains ℓ, so $\langle \mathfrak{p}, \mathfrak{f} \rangle \subset \langle \mathfrak{p}, \ell \rangle = \mathfrak{p}$. By [Co1, Thm. 6.1], this means that $\mathfrak{p}$ is not invertible, and thus by [Co1, Thm. 3.4] we have that $\mathfrak{p}$ is not proper.
Second proof: Following [Co1, Example 3.15] we will show there is a unique ideal of $\mathcal{O}$ of norm ℓ and explicitly construct it. Then we will find an explicit element of $(\mathfrak{p} : \mathfrak{p}) \setminus \mathcal{O}$ and thereby show that $\mathfrak{p}$ is not proper. Write

$$\mathcal{O}_K = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \tau_K.$$

Put $\tau \coloneqq \mathfrak{f}\tau_K$, so

$$\mathcal{O} = \mathbb{Z} \cdot 1 \oplus \mathbb{Z} \cdot \tau.$$

Let

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

Then as a $\mathbb{Z}$-module we have

$$\mathfrak{p} = \langle \ell, \mathfrak{f}, \tau \rangle_{\mathbb{Z}} = \mathbb{Z} \cdot \ell \oplus \mathbb{Z} \cdot \tau,$$

so $[\mathcal{O} : \mathfrak{p}] = \ell$. Since $\ell\mathfrak{p} \subset \mathfrak{p}$ and $\tau\mathfrak{p} \subset \mathfrak{p}$, $\mathfrak{p}$ is an ideal of $\mathcal{O}$. Since it has norm ℓ, it is maximal. We claim that it is the unique ideal of norm ℓ: if $\mathfrak{q}$ is an ideal of $\mathcal{O}$ of norm ℓ, then $\ell = 1 \cdot [\mathcal{O} : \mathfrak{q}] \in \mathfrak{q}$. Since $\ell \mid \mathfrak{f}$ we have

$$\mathfrak{p}^2 = (\ell\mathbb{Z} + \mathfrak{f}\mathcal{O}_K)^2 = \ell^2\mathbb{Z} + \ell\mathfrak{f}\mathcal{O}_K + \mathfrak{f}^2\mathcal{O}_K = \ell^2\mathbb{Z} + \ell\mathfrak{f}\mathcal{O}_K \subset \ell\mathcal{O} \subset \mathfrak{q}.$$

Since $\mathfrak{p}$ is prime this gives $\mathfrak{p} \subset \mathfrak{q}$; we have an inclusion of nonzero prime ideals in a one-dimensional domain, so $\mathfrak{p} = \mathfrak{q}$.

Now we claim that $\frac{\tau}{\ell} \in (\mathfrak{p} : \mathfrak{p})$, hence $(\mathfrak{p} : \mathfrak{p}) \supsetneq \mathcal{O}$ and $\mathfrak{p}$ is not proper. Let $a, b \in \mathbb{Z}$ be such that $\tau_K^2 = a + b\tau_K$. Then we have

$$\frac{\tau}{\ell}\ell = \tau \in \mathfrak{p}, \ \frac{\tau}{\ell}\tau = \frac{\mathfrak{f}^2}{\ell}\tau_K^2 = \frac{\mathfrak{f}^2}{\ell}(a + b\tau_K) = \frac{a\mathfrak{f}^2}{\ell} + \frac{b\mathfrak{f}}{\ell}\tau \in \mathbb{Z}\ell + \mathbb{Z}\tau = \mathfrak{p}. \qquad \square$$

It follows from (5) that if $\varphi : E \to E'$ is a cyclic ℓ-power isogeny of K-CM elliptic curves, $\mathfrak{f}$ is the conductor of $\mathrm{End}(E)$ and $\mathfrak{f}'$ is the conductor of $\mathrm{End}(E')$, then $\frac{\mathfrak{f}}{\mathfrak{f}'} \in \ell^{\mathbb{Z}}$. Thus the prime to ℓ part of the conductor is constant on each connected component of the graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$, so we may as well fix $\mathfrak{f}_0$, a positive integer prime to ℓ and let $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ be the induced subgraph consisting of all vertices with prime to ℓ conductor $\mathfrak{f}_0$.

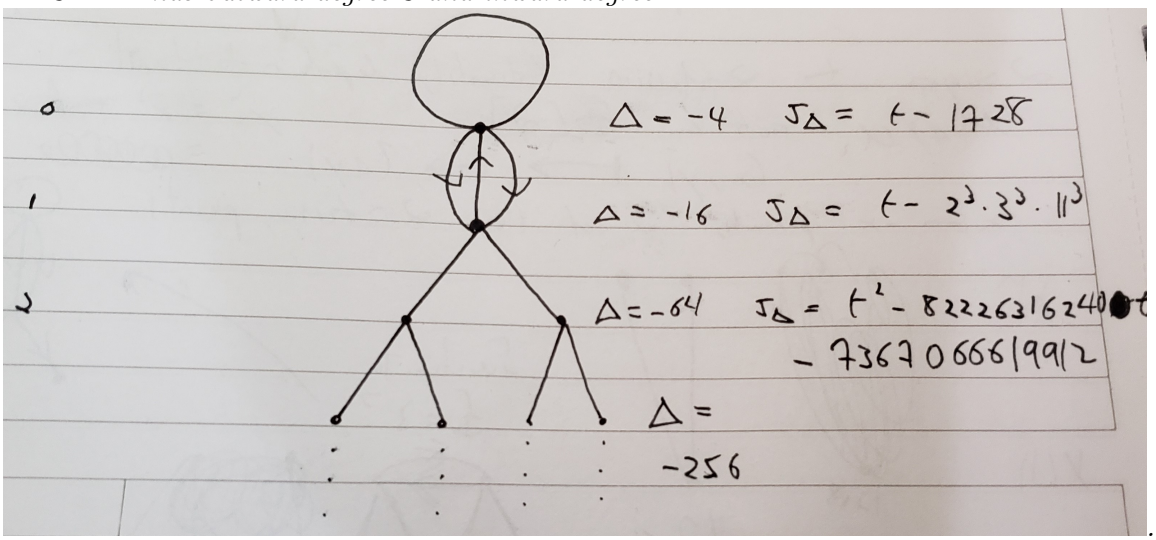
The **level** L of a vertex $j \in \mathcal{G}_{\ell,K}$ is $\mathrm{ord}_\ell(\mathfrak{f})$, where $\mathfrak{f}$ is the conductor of $\mathrm{End}(E_j)$. The **surface** of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ is the induced subgraph consisting of all vertices at level 0. Lemma 4.1 tells us that horizontal edges can only occur at the surface of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.

Example 4.2. *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.



Example 4.3. *Let $K = \mathbb{Q}(\sqrt{-3})$, $\ell = 3$ and $\mathfrak{f}_0 = 1$. The surface of this graph consists of CM j-invaraints of discriminant -3, of which there is 1: $j = 0$. Level one consists of CM*

j-invariants of discriminant -12, of which there is again 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

$$J_{-3\cdot 3^4} = t^3 + 185576290573466419200 0t^2 - 375065736503309107200000 0t + 333858672467351961600000000 0.$$

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.

4.2. **Volcanoes.** Fix a prime number ℓ. An ℓ-**volcano** V is a directed graph – possibly with loops and/or multiple edges – with a partitioning of its vertex set into levels $\{V_i\}_{i \in I}$ and a partitioning of its edge set into three subsets, called **horizontal**, **ascending** and **descending**. Here I is a nonempty downward closed subset of the natural numbers $\mathbb{N}$, and thus it is either $\mathbb{N}$ or $\{0, 1, \ldots, d\}$ for some $d \in \mathbb{N}$. The **depth** of V is the largest d such that V_d is nonempty if such a d exists and ∞ otherwise. If V has finite depth d, we we call the level V_d the **floor**. We require the following additional properties:
(0) For every edge $e : v \mapsto w$ there is a canonical inverse edge $\overline{e} : w \mapsto v$.[6]
(i) The subgraph V_0, called the **surface** is a regular graph of degree $s(V) \in \{0, 1, 2\}$. An edge is horizontal iff it connects two vertices in V_0.
(ii) The ascending edges are precisely as follows: for all positive $i \in I$ and each vertex x in V_i there is a unique $y \in V_{i-1}$ and an ascending edge $e : x \mapsto v$. The descending edges are precisely the inverses of the ascending edges.
(iii) Every vertex in the floor (if any) has degree 1.[7] Every other vertex x has degree $\ell + 1$. Thus if x has level $i \geq 1$ then it is connected to one vertex in level $i - 1$ and ℓ distinct vertices in level $i + 1$. If x has level 0 then it has $s(V)$ horizontal undirected edges and $\ell + 1 - s(V)$ descending edges emanating from x to distinct vertices in V_1.

We observe that for a fixed surface vertex v_0, the induced subgraph on the set of vertices that can by repeatedly descending from v_0 has the structure of a rooted tree with v_0 as the root.

We claim that if $\mathfrak{f}_0^2 \Delta_K < -4$, then the isogeny graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ is an isogeny volcano of infinite depth for which each vertex at the surface has degree $1 + \left(\frac{\Delta_K}{\ell}\right)$. In this regard,

[6]Thus by identifying e and $\overline{e}$ we get an undirected graph, from which V can be recovered, so this is an equivalent perspective. When we speak of the degree of a vertex, we mean of the underlying undirected graph, and we take the convention that an edge from x to x contributes one to the degree.

[7]This follows from the above properties, but is worth stating explicitly.

we have already shown (0). As for (i), the surface edges emanating outward from a surface vertex correspond to proper $\mathcal{O}$-ideals of norm ℓ. Since $\ell \nmid \mathfrak{f}_0$, every $\mathcal{O}$-ideal of norm ℓ is proper [Co1, Thm. 3.1] and the pushforward map $\mathfrak{a} \mapsto \mathfrak{a}\mathbb{Z}_K$ is a norm-preserving bijection from $\mathcal{O}$-ideals of norm ℓ to $\mathbb{Z}_K$-ideals of norm ℓ [Co1, Thm. 3.8]. Thus we reduce to the $\mathfrak{f}_0 = 1$ case, in which we certainly have 2, 1 or 0 ideals of norm ℓ according to whether ℓ is split, ramified or inert in K. Let us look more carefully at the three cases:

Inert Case: If $\left(\frac{\Delta_K}{\ell}\right) = -1$, then in the order $\mathcal{O}$ of conductor $\mathfrak{f}_0$ we have no ideals of order ℓ hence no surface vertices.

Ramified Case: If $\left(\frac{\Delta_K}{\ell}\right) = 0$, then in the order $\mathcal{O}$ of conductor $\mathfrak{f}_0$ we have a unique prime ideal $\mathfrak{p}$ that is proper and of norm ℓ. If $\mathfrak{p}$ is principal then every surface vertex has a unique, self-inverse loop. Otherwise, since $\mathfrak{p}^2 = (\ell)$ we have that $[\mathfrak{p}]$ has order 2 in $\operatorname{Pic}\mathcal{O}$, and the set of surface vertices is partitioned into pairs v_1, v_2, such that if v_1 corresponds to E then v_2 corresponds to $E/E[\mathfrak{p}]$, and each of these surface edges is self-inverse. Because the ideal $\mathfrak{p}$ is real, the field of moduli of $E \to E/E[\mathfrak{p}]$ is $\mathbb{Q}(\mathfrak{f}_0)$.

Split Case: If $\left(\frac{\Delta_K}{\ell}\right) = 1$, then in the order $\mathcal{O}$ of conductor $\mathfrak{f}_0$ we have $(\ell) = \mathfrak{p}\overline{\mathfrak{p}}$ for distinct prime ideals $\mathfrak{p}$, $\overline{\mathfrak{p}}$ of norm ℓ. Let r be the order of $[\mathfrak{p}]$ in $\operatorname{Pic}\mathcal{O}$. If $r = 1$ then every surface vertex has two distinct, mutually inverse loops corresponding to $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. If $r = 2$ – equivalently, if $[\mathfrak{p}] = [\overline{\mathfrak{p}}]$ then set of surface vertices is partitioned into pairs v_1, v_2 such that if v_1 corresponds to E then v_2 corresponds to $E/E[\mathfrak{p}] \cong E/E[\overline{\mathfrak{p}}] \cong E'$, say, and there are two edges $\mathfrak{p}$, $\overline{\mathfrak{p}}$ running from v_1 to v_2. The inverses of these edges correspond to the isogenies $E' \to E'/[\overline{\mathfrak{p}}]$ and $E' \to E'/E'[\mathfrak{p}]$ respectively. If $r \geq 3$ then the set of surface vertices is naturally partitioned into r-cycles. Finally, as a special case of the results on proper isogenies of the previous section, because the ideal $\mathfrak{p}$ is not real, the field of moduli of $E \to E/E[\mathfrak{p}]$ is $K(\mathfrak{f}_0)$.

Now let $L \geq 1$, and let $v \in V(\mathcal{G}_{K,\ell,\mathfrak{f}_0})$ be a vertex at level L, let $\mathfrak{f} = \ell^L\mathfrak{f}_0$, $\Delta = \mathfrak{f}^2\Delta_K$, and let E be the corresponding Δ-CM elliptic curve. From §3.3 we get that the unique (up to equivalence) ℓ-isogeny from E to an elliptic curve with conductor $\frac{\mathfrak{f}}{\ell}$ is $\iota_{\mathfrak{f},\frac{\mathfrak{f}}{\ell}}$, which has field of moduli $\mathbb{Q}(j(E))$. This shows in particular the exsistence and uniqueness of ascending edges emanating from a non-surface vertex, and clearly the descending edges are the inverses of the ascending edges. This shows (ii).

In our setup we have no floor, and we saw in §4.1 that every vertex in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ has outward degree $\ell + 1$. The rest of (iii) amounts to the claim that the only multiple edges and loops in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ lie in the surface. That there are no loops below the surface follows from Lemma 4.1. Consider first a surface vertex v_0. By Corollary 2.1c), the number of vertices at level 1 is equal to $\ell - \left(\frac{\Delta_K}{\ell}\right)$ times the number of vertices on the surface, which is also equal to the total number of edges descending from the surface. So if two distinct downard

edges emanating from v_0 had the same terminal vertex v_1, then some other vertex on level 1 would not be connected to any surface vertex, contrary to what we already know. Now let $L \geq 1$ and consider a vertex v_L at level L. Then Corollary 2.1c) shows that the number of vertices at level $L+1$ is ℓ times the number of vertices at level ℓ, which is also equal to the total number of edges descending from level L, so again no two edges emanating from v_L can have the same terminal vertex. This completes our proof that when $\mathfrak{f}_0^2 \Delta_K < -4$ the isogeny graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ is an ℓ-volcano.

4.3. **Paths and ℓ^a-isogenies.** A **path** in a directed graph consists of a finite sequence of directed edges $e_1, \ldots, e_N$ such that for all $1 \leq i \leq N-1$ the terminal vertex of e_i is the initial vertex of e_{i+1}. In a directed graph in which each edge has a canonical inverse edge, a path has **backtracking** if for some i we have that e_{i+1} is the inverse edge of e_i.

The notion of a backtracking path becomes a bit more subtle in the presence of loops or multiple edges. In our volcanoes, we should be clear about which surface edges yield backtracking. In the ramified case, a path that includes surface edges $v_0 \stackrel{e_1}{\to} w_0 \stackrel{e_2}{\to} v_0$ has backtracking (whether $v_0 = w_0$ or not). In the split case, a backtracking involving surface edges comes from traversing an edge corresponding to a prime ideal $\mathfrak{p}$ followed by an edge corresponding to its conjugate ideal $\overline{\mathfrak{p}}$. A loop at a surface vertex corresponding to a principal prime ideal $\mathfrak{p}$ can be traversed any number of times and is *not* backtracking.

Lemma 4.4. *Suppose that $\mathfrak{f}_0^2 \Delta_K < -4$. 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 volcano $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.*

Proof. Let $\varphi : E_0 \to E_a$ be a cyclic ℓ^a-isogeny of elliptic curves, each with K-CM and prime-to-ℓ-conductor $\mathfrak{f}_0$. As in §3.2, the isogeny φ factors uniquely into a length a sequence of ℓ-isogenies $\varphi_i : E_i \to E_{i+1}$, and in this way we get a path of length a in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$. A backtracking in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ corresponds to performing an ℓ-isogeny ι followed by its dual isogeny $\iota^\vee$ and thus φ would factor through $[\ell]$ and fail to be cyclic.

Conversely, a path of length a in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ yields a sequence of cyclic ℓ-isogenies $\{\varphi_i : E_i \to E_{i+1}\}_{i=0}^{a-1}$ and then $\varphi := \varphi_{a-1} \circ \ldots \varphi_0$ is an ℓ^a-isogeny. It remains to see that the lack of backtracking implies that φ is cyclic. This comes down to: for $1 \leq A \leq a$, if $\varphi = \varphi_{A-1} \circ \ldots \circ \varphi_0 : E_0 \to E_A$ is a cyclic k-isogeny and $\psi : E_A \to E'$ is an ℓ-isogeny, then if $\operatorname{Ker} \psi \neq \operatorname{Ker} \varphi_{A-1}^\vee$ then $\psi \circ \varphi$ is a cyclic ℓ^{A+1}-isogeny. Via uniformizing lattices this translates to the following claim: let

$$\Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_A \subset \mathbb{C}$$

be lattices with $[\Lambda_{i+1} : \Lambda_i] = \ell$ for all i and Λ_A/Λ_0 cyclic of order ℓ^A. Then of the $\ell+1$ lattices $\Lambda' \subset \mathbb{C}$ that contain Λ with index ℓ, there is exactly one such that Λ'/Λ_0 is not cyclic, namely $\frac{1}{\ell}\Lambda_{A-1}$. Indeed, by the structure theory of finitely generated $\mathbb{Z}$-modules there is a $\mathbb{Z}$-basis e_1, e_2 for Λ_A such that $e_1, \ell^A e_2$ is a $\mathbb{Z}$-basis for Λ_0 and thus $e_1, \ell e_2$ is a $\mathbb{Z}$-basis for Λ_{A-1}. The ℓ-torsion subgroup of $(\Lambda_0 \otimes \mathbb{Q})/\Lambda_0$ is generated by $\frac{1}{\ell}e_1$ and $\ell^{A-1}e_2$,

so a subgroup of $(\Lambda_0 \otimes \mathbb{Q})/\Lambda_0$ that contains Λ_1/Λ_0 has full ℓ-torsion iff it contains $\frac{1}{\ell}e_1$. But $\frac{1}{\ell}\Lambda_{A-1}$ is the unique lattice containing Λ_A with index ℓ and containing $\frac{1}{\ell}e_1$. □

Still under the assumption that $\mathfrak{f}_0^2\Delta_K < -4$, we observe that nonbacktracking paths in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ have a restricted form: every such path P is uniquely decomposed into a concentation $P_3 \circ P_2 \circ P_1$ of three paths, though some of them may have length 0. Namely, P_1 consists entirely of ascending edges, P_2 consists entirely of horizontal edges and P_3 consists entirely of descending edges. To see this we observe that an equivalent statement is that a surface edge can only be followed by another surface edge or descending edge, while a descending edge can only be followed by a descending edge. The former statement is clear – as we are at the surface, we cannot ascend – and once we have descended, we are not at the surface so have no horizontal edges and a descent followed by an ascent is a backtrack.

5. The Action of Complex Conjugation on the Isogeny Volcano

Fix K and $\mathfrak{f}_0$ such that $\mathfrak{f}_0^2\Delta_K < -4$. Let ℓ be a prime number.

In this section we will define and study an action of complex conjugation – more precisely, of the group $\mathfrak{g}_{\mathbb{R}} = \{1, c\}$ – on the isogeny volcano $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ by graph automorphisms. Although our definition is natural and straightforward, it seems not to have been made before: so far as we know, all prior work on isogeny volcanoes has been done in the setting where the ground field contains the CM field K. It is this definition that gives us the leverage we need to completely analyze isogenies of CM elliptic curves over $\mathbb{Q}(j)$.

5.1. **Reality, part II: coreality.** In this section we will determine the isomorphism class of the number field generated by the j-invariants of two elliptic curves with CM by the same imaginary quadratic field K, assuming that $\Delta_K < -4$.

Let $j, j' \in \mathbb{C}$ be K-CM j-invariants, of discriminants Δ, Δ' and conductors $\mathfrak{f}, \mathfrak{f}'$.

We say j, j' are **coreal** if the number field $\mathbb{Q}(j, j')$ admits a real embedding.

Suppose first that there is a prime number ℓ and integers $a \geq a' \geq 1$ such that $\mathfrak{f} = \ell^a$, $\mathfrak{f}' = \ell^{a'}$. In this case we claim that j, j' are coreal if for any field embedding $\iota : \mathbb{Q}(j, j') \hookrightarrow \mathbb{C}$, we have $\iota(j) \in \mathbb{R} \implies \iota(j') \in \mathbb{R}$. The latter condition is clearly sufficient for coreality: indeed, there is an embedding $\iota : \mathbb{Q}(j) \hookrightarrow \mathbb{R} \subset \mathbb{C}$, so our assumption gives

$$\iota(\mathbb{Q}(j, j')) = \mathbb{Q}(\iota(j), \iota(j')) \subset \mathbb{R}.$$

Conversely, suppose that $\mathbb{Q}(j, j')$ admits a real embedding, and let $\iota : \mathbb{Q}(j, j) \hookrightarrow \mathbb{C}$ be such that $\iota(j) \in \mathbb{R}$. Then $\iota(j) \in K(j_\Delta)^c = \mathbb{Q}(\mathfrak{f})$. Since $a' \leq a$ we have $\mathbb{Q}(\iota(j')) \subset K(\mathfrak{f})$ and $\mathbb{Q}(\iota(j), \iota(j')) = K(\mathfrak{f})$ iff $\iota(j') \notin \mathbb{R}$. Since j, j' are coreal we have $\mathbb{Q}(\iota(j), \iota(j')) \cong \mathbb{Q}(j, j')$ admits a real embedding, so it cannot contain K and thus $\iota(j') \in \mathbb{R}$.

In the above setup, to determine the coreality of j, j' we may reduce via simultaneous Galois conjugacy to the case $j = j_\Delta$, and then the set of Δ'-CM j-invariants j' such that

j, j' are coreal are precisely the real roots of the Hilbert class polynomial $H_{\Delta'}(t)$, of which there are precisely $h_2(\Delta') := \#\operatorname{Pic}\mathcal{O}(\Delta')[2]$. If j, j' are coreal we have $\mathbb{Q}(j, j') \cong \mathbb{Q}(\mathfrak{f})$, while if j, j' are not coreal, we have $\mathbb{Q}(j, j') = K(\mathfrak{f})$.

Everything done above goes through verbatim in the somewhat more general case that $\mathfrak{f}' \mid \mathfrak{f}$: namely j, j' are coreal iff for all $\iota : \mathbb{Q}(j, j') \hookrightarrow \mathbb{C}$ we have $\iota(j) \in \mathbb{R} \implies \iota(j') \in \mathbb{R}$, so we may Galois conjguate to the case $j = j_\Delta$, and then $\mathbb{Q}(j, j') \cong \mathbb{Q}(\mathfrak{f})$ if j, j' are coreal and $\mathbb{Q}(j, j') = K(\mathfrak{f})$ otherwise. This includes the case in which $\mathfrak{f}' = 1$ and in particular the case in which $\mathfrak{f} = \mathfrak{f}' = 1$.

We remark that if $\mathfrak{f}' \nmid \mathfrak{f}$ it can happen that j, j' are coreal, $j \in \mathbb{R}$ and $j' \notin \mathbb{R}$. For instance, suppose that $K = \mathbb{Q}(\sqrt{-7})$ and $\mathfrak{f} = 1$, so $j \in \mathbb{Q}$. Then $\mathbb{Q}(j, j') = \mathbb{Q}(j') \cong \mathbb{Q}(\mathfrak{f}')$ has a real embedding, so j, j' are coreal, but for all sufficiently large $\mathfrak{f}'$ there are non-real $(\mathfrak{f}')^2\Delta_K$-CM j-invariants.

We now return to the general case: we have $j = j(E)$, $j' = j(E')$, where E (resp. E') is a Δ-CM elliptic curve (resp. Δ'-CM elliptic curve) for $\Delta = \mathfrak{f}^2\Delta_K$ (resp. $\Delta' = (\mathfrak{f}')^2\Delta_K$). We put $M := \operatorname{lcm}(\mathfrak{f}, \mathfrak{f}')$.

There is a canonical $\mathbb{Q}(j)$-rational isogeny from E to a Δ_K-CM elliptic curve E_0 and we put $j_0 := j(E_0)$; similarly we define $j_0' = j(E_0')$. If j_0, j_0' are coreal then $\mathbb{Q}(j_0, j_0') = \mathbb{Q}(1)$, while if j_0, j_0' are not coreal then $\mathbb{Q}(j_0, j_0') = K(1)$, the Hilbert class field of K. Since $\mathbb{Q}(j_0, j_0') \subset \mathbb{Q}(j, j')$, if j_0, j_0' are not coreal then $\mathbb{Q}(j, j')$ contains K and then it is easy to see that $\mathbb{Q}(j, j') = K(M)$.

From now on we assume that j_0, j_0' are coreal and thus $\mathbb{Q}(j_0) = \mathbb{Q}(j_0') = F_0$, say. We treat this case by a primary decomposition argument. Write

$$\mathfrak{f} = \ell_1^{a_1} \cdots \ell_r^{a_r},\ \mathfrak{f}' = \ell_1^{a_1'} \cdots \ell_r^{a_r'}, a_i, a_i \in \mathbb{N}, A_i := \max(a_i, a_i') \in \mathbb{Z}^+.$$

For all $1 \le i \le r$, there is a canonical $\mathbb{Q}(j)$-rational isogeny from E to a $(\Delta_i = \ell_i^{2a_i}\Delta_K)$-CM elliptic curve E_i, and we put $j_i = j(E_i)$, and in a similar way we define E_i' and $j_i' = j(E_i')$. If we Galois conjugate j to j_Δ then each j_i gets Galois conjugated to j_{Δ_i}, so it follows from Proposition 2.10 that $\mathbb{Q}(j) = \mathbb{Q}(j_1, \ldots, j_r)$, and similarly we have $\mathbb{Q}(j') = \mathbb{Q}(j_1', \ldots, j_r')$. Put $M = \operatorname{lcm}(\mathfrak{f}, \mathfrak{f}')$. If for some $1 \le i \le r$ we have that j_i, j_i' are *not* coreal, then

$$\mathbb{Q}(j, j') = K(M) = K(\ell_1^{A_1} \cdots \ell_r^{A_r}).$$

Otherwise we have that j_i, j_i' are coreal for all $1 \le i \le r$, so for each $1 \le i \le r$, we have $F_i := \mathbb{Q}(j_i, j_i') \supset \mathbb{Q}(j_0)$. It follows from Corollary 2.11 and an easy inductive argument that

$$\mathbb{Q}(j, j') = F_1 \cdots F_r \cong F_1 \otimes_{F_0} F_2 \otimes_{F_0} \cdots \otimes_{F_0} F_r \cong \mathbb{Q}(M).$$

In particular, we get:

Theorem 5.1. *Let $\Delta_K < -4$, and let j, j' be K-CM j-invariants, of conductors $\mathfrak{f}, \mathfrak{f}''$, and put $M := \operatorname{lcm}(\mathfrak{f}, \mathfrak{f}')$.*

a) *If j, j' are coreal, then $\mathbb{Q}(j, j') \cong \mathbb{Q}(M)$.*

b) *If j, j' are not coreal, then $\mathbb{Q}(j, j') = K(M)$.*

Proof. We saw above that $\mathbb{Q}(j, j')$ is either isomorphic to $\mathbb{Q}(M)$ or equal to $K(M)$. Since $\mathbb{Q}(M)$ has a real embedding and $K(M)$ does not, the result follows. □

The following is an immediate consequence.

Corollary 5.2. *Let K be an imaginary quadratic field with $\Delta_K < -4$.*

a) *The compositum of finitely many ring class fields of K is a ring class field of K.*
b) *The compositum of finitely many rational ring class fields of K is either a rational ring class field of K or a ring class field of K.*

5.2. $\operatorname{Aut}\mathbb{C}$ **acts on** $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$**.** In fact we have an action of the group $\operatorname{Aut}\mathbb{C}$ on $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$. If $j \in \mathbb{C}$ is any Δ-CM j-invariant and $\sigma \in \operatorname{Aut}\mathbb{C}$, then $\sigma(j)$ is also a Δ-CM j-invariant. The action on edges is by "transport of structure": we map the ℓ-isogeny $\iota : E \to E'$ to the ℓ-isogeny $\sigma(\iota) : \sigma(E) \to \sigma(E')$. This action factors through the quotient $\mathfrak{g}_{\mathbb{Q}} = \operatorname{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Because the elliptic curves with CM by a fixed discriminant Δ form a single Galois conjugacy class, the group $\mathfrak{g}_{\mathbb{Q}}$ acts transitively on the set of vertices of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ of fixed level $L \geq 0$.

Let c be the image of complex conjugation in $\mathfrak{g}_{\mathbb{Q}}$. We call a vertex or an edge of $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ **real** if it is fixed by complex conjuation and **complex** otherwise. Complex vertices and edges occur in conjugate pairs.

We begin with some simple but useful observations concerning this definition:

• Complex conjugation maps ascending edges to ascending edges, horizontal edges to horizontal edges, and descending edges to descending edges.

• An edge $e \in \mathcal{G}_{K,\ell,\mathfrak{f}_0}$ determines a point $P_e \in X_0(\ell)(\mathbb{C})$. Because $X_0(\ell)$ is a curve over $\mathbb{Q}$, it has a canonical $\mathbb{R}$-model, which determines an action of complex conjugation on $X_0(\ell)(\mathbb{C})$. Under this action we have $c(P_e) = P_{c(e)}$. In particular, e is real iff P_e is real.

• An edge is real iff its inverse edge is real.

• If an edge $e : v \mapsto w$ are real, then both v and w are real.

• For vertices v and w in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$, there is a unique edge e from v to w iff there is a unique edge $c(e)$ from $c(v)$ to $c(w)$. When this occurs, knowing $c(v)$ and $c(w)$ determines $c(e)$. In particular, in this case the converse of the above observation holds: $e : v \mapsto w$ is real iff v and w are real.

• Keeping in mind that we have assumed $\mathfrak{f}_0^2\Delta_K < -4$, the only possible multiple edges from v to w are surface edges in the split case. As we have seen, in the split case the two surface edges emanating from a vertex v correspond to prime ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ lying over ℓ.

These edges always are always complex and form a conjugate pair. They have the same terminal vertex iff $[\mathfrak{p}]$ has order at most 2 in $\operatorname{Pic}\mathcal{O}$.

• As mentioned above, all surface edges are complex in the split case. In the ramified case, a surface edge $e : v \mapsto w$ is real iff v is real iff w is real. An ascending edge $e : v \mapsto w$ is real iff v is real: clearly if e is real, then so is v, and conversely, if v is real, then $c(e)$ is an ascending edge emanating from v, of which e is the only one. By passing to inverses, we deduce that a descending edge $e : v \mapsto w$ is real iff w is real.

5.3. **The field of moduli of a cyclic ℓ^a-isogeny.** The following result computes the field of moduli of a cyclic ℓ^a-isogeny of CM elliptic curves in the $\mathfrak{f}_0^2\Delta_K < -4$ case.

Theorem 5.3. *Let $\varphi : E \to E'$ be a cyclic ℓ^a-isogeny of CM elliptic curves such that $\mathfrak{f}_0^2\Delta_K < -4$. Let $\mathfrak{f}$ be the maximum of the conductor of $\operatorname{End}(E)$ and the conductor of $\operatorname{End}(E')$.*

a) *If ℓ splits in K and φ factors through an ℓ-isogeny of $\mathfrak{f}_0\Delta_K$-CM elliptic curves, then $\mathbb{Q}(\varphi) = K(\mathfrak{f})$. In every other case we have $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$.*
b) *If $j(E)$ and $j(E')$ are not coreal then we have $\mathbb{Q}(\varphi) = K(\mathfrak{f})$.*
c) *Suppose that $j(E)$ and $j(E')$ are coreal. Then if the conductor of E' divides the conductor of E we have $\mathbb{Q}(j(E), j(E')) = \mathbb{Q}(j(E))$, while if the conductor of E divides the conductor of E' we have $\mathbb{Q}(j(E), j(E')) = \mathbb{Q}(j(E'))$.*

Proof. Let $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ (resp. $\Delta' = \ell^{2L'}\mathfrak{f}_0^2\Delta_K$) be the discriminant of the endomorphism ring of E (resp. of E'). We have $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi^\vee)$, and the assertions of Theorem 5.3 hold for φ iff they hold for $\varphi^\vee$, so by replacing φ with $\varphi^\vee$ is necessary we may assume that $L \geq L'$, so that the conductor $\ell^{L'}\mathfrak{f}_0$ of E' divides the conductor $\ell^L\mathfrak{f}_0$ of E.

For $\sigma \in \mathfrak{g}_\mathbb{Q}$, we have $\mathbb{Q}(\sigma(\varphi)) = \sigma(\mathbb{Q}(\varphi)) \cong \mathbb{Q}(\varphi)$, so up to replacing the field of moduli by an isomorphic number field we may replace ι by $\sigma(\iota) : \sigma(E) \to \sigma(E')$ and thus we may assume that $j(E) = j_\Delta$.

As in §4.3, φ determines a nonbacktracking path $P(\varphi)$ of length a in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$. Now put $E_0 := E$, $E_a := E'$; for $0 \leq i \leq a$, let $\varphi_i : E_i \to E_{i+1}$ be the ℓ-isogeny corresponding to the ith edge of the path P. By Proposition 3.2b) we have $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi_1)\cdots\mathbb{Q}(\varphi_a)$. Then $K(\mathfrak{f}) \supseteq \mathbb{Q}(j(E), j(E'))$. Each ascending ℓ-isogeny $\varphi_i : E_i \to E_{i+1}$ is defined over $\mathbb{Q}(j(E_i)) \subseteq K(\mathfrak{f})$; each horizontal edge is defined over $K(\mathfrak{f}_0) \subseteq K(\mathfrak{f})$; and each descending ℓ-isogeny $\varphi_i : E_i \to E_{i+1}$ is defined over $\mathbb{Q}(j(E_{i+1}) \subseteq K(\mathfrak{f})$. So we have

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

If ℓ splits in K and for some i the ℓ-isogeny $\varphi_i : E_i \to E_{i+1}$ induces a horizontal edge, then $K \subset \mathbb{Q}(\varphi_i) \subset \mathbb{Q}(\varphi)$, and thus we must have $\mathbb{Q}(\varphi) = K(\mathfrak{f})$. Next suppose that $P(\varphi)$ contains no such edge. Then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E_0), \ldots, j(E_a))$.

Let v and w are two vertices in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ corresponding to elliptic curves E_v and E_w. If there is a path from v to w consisting entirely of ascending edges, then $\mathbb{Q}(j(E_v)) \supset \mathbb{Q}(j(E_w))$. In the case that ℓ ramifies in K, if $e : v \to w$ is a horizontal edge, then $\mathbb{Q}(j(E_v)) = \mathbb{Q}(j(E_w))$.

From this we deduce:

$$\mathbb{Q}(\varphi) = \mathbb{Q}(j(E_0), \ldots, j(E_a)) = \mathbb{Q}(j(E_0), j(E_a)) = \mathbb{Q}(j(E), j(E')).$$

This establishes part a). Part b) is immediate from Theorem 5.1. As for part c), we have reduced to the case $L' \leq L$, so if $j(E)$ and $j(E')$ are coreal then after our Galois conjugation we have $j(E') \in K(\mathfrak{f}) \cap \mathbb{R} = \mathbb{Q}(\mathfrak{f}) = \mathbb{Q}(j(E))$, so $\mathbb{Q}(j(E), j(E')) = \mathbb{Q}(j(E))$. But this identity is unchanged by replacing $j(E)$ and $j(E')$ by $\sigma(j(E))$ and $\sigma(j(E'))$ for any $\sigma \in \mathfrak{g}_{\mathbb{Q}}$, so indeed we have $\mathbb{Q}(j(E), j(E')) = \mathbb{Q}(j(E))$. □

Our next major task is to fix an imaginary quadratic discriminant $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ with $\mathfrak{f}_0^2\Delta_K < -4$ and a prime power ℓ^a and to compute the fiber of $X_0(\ell^a) \to X(1)$ over J_Δ. In order to do this, as above we may consider cylic ℓ^a-isogenies $\varphi : E \to E'$ such that $j(E) = j_\Delta$, and as we range over all length a nonbacktracking paths in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ with terminal vertex w corresponding to an elliptic curve E', we need to understand for which of these paths we have that j_Δ and $j(E')$ are coreal. For this we need a more explicit description of the action of $\mathfrak{g}_{\mathbb{R}}$ on $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$, which we provide in the next section. We also need to modify the above approach slightly, since switching to the dual isogeny so as to ensure that $j(E)$ has level at least as large as the level of $j(E')$ is not a good approach to the coming combinatorial problem. We handle the latter first:

Suppose that we have a nonbacktracking path P of length a in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ corresponding to $\varphi : E \to E'$, and such that E is $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$-CM and E' is $\Delta' = \ell^{2L'}\mathfrak{f}_0^2\Delta_K$-CM with $L' > L$, and put $\mathfrak{f} = \ell^L\mathfrak{f}_0$, $\mathfrak{f}' = \ell^{L'}\mathfrak{f}_0$. By the above analysis, the field of moduli $\mathbb{Q}(\varphi)$ is either $\mathbb{Q}(j(E'))$ (which is isomorphic though not necessarily equal to $\mathbb{Q}(\mathfrak{f}')$) or $K(j(E')) = K(\mathfrak{f}')$. If the path P contains a horizontal edge in the split case then we have $\mathbb{Q}(\varphi) = K(\mathfrak{f}')$, so suppose that is not the case. Then we have $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E'))$ iff j_Δ and $j(E')$ are coreal. Let P_1 be the maximal initial segment of the path P that terminates at a vertex in level L, and let P_2 be the rest of the path, so P_2 consists entirely of $L' - L$ descending edges. Let $a_1 < a$ be the length of P_1, and let $\varphi_1 : E \to E_1$ be the corresponding factor isogeny. Then $\mathbb{Q}(j(E_1)) \subset \mathbb{Q}(j(E'))$, so if j_Δ and $j(E')$ are coreal then so are j_Δ and $j(E_1)$, and since E and E_1 have the same endomorphism ring, this occurs iff $j(E_1) \in \mathbb{R}$. Conversely, if $j(E_1) \in \mathbb{R}$ then $\mathbb{Q}(j(E_1)) = \mathbb{Q}(j_\Delta)$ and thus

$$\mathbb{Q}(j_\Delta, j(E')) = \mathbb{Q}(j(E_1), j(E')) = \mathbb{Q}(j(E')).$$

Since we wish to count closed points in the fiber of $X_0(\ell^a) \to X(1)$ over J_Δ, we need to impose an equivalence relation on paths: any path in the same $\mathfrak{g}_{\mathbb{Q}(\mathfrak{f})}$-orbit as $P(\varphi)$ determines the same closed point on $X_0(\ell^a)$ as $P(\varphi)$. The size of this Galois orbit is

$$d_\varphi \coloneqq [\mathbb{Q}(\varphi) : \mathbb{Q}(\mathfrak{f})].$$

Complex conjugation acts on paths in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$, and a path is real iff each of its edges is real.

Lemma 5.4. *We maintain notation as above. Put*

$$\epsilon_\varphi \coloneqq \begin{cases} 1 & P_1 \text{ is real} \\ 2 & \text{otherwise} \end{cases}.$$

Then:

a) *If $L \geq L'$, then we have $d_\varphi = \epsilon_\varphi$.*

b) *If $L = 0$ and $L' > L$, then we have $d_\varphi = \epsilon_\varphi(\ell + \left(\frac{\Delta_K}{\ell}\right))\ell^{L'-L-1}$.*

c) *If $0 < L < L'$, then we have $d_\varphi = \epsilon_\varphi \ell^{L'-L}$.*

Proof. This follows easily from the description of $\mathbb{Q}(\varphi)$ we have given. □

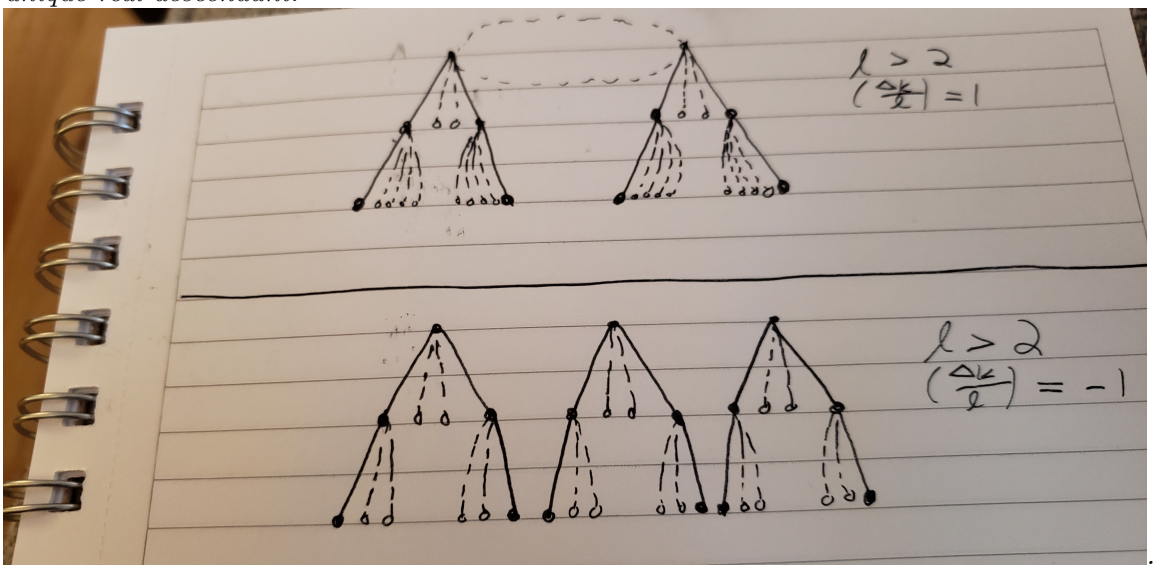
We can also explicitly describe the $\mathfrak{g}_{\mathbb{Q}(\mathfrak{f})}$-orbit on $P(\varphi)$: it consists of all paths obtained from P_1 by descending $\max(L' - L, 0)$ times as well as all paths obtained from $\overline{P_1}$ by descending $\max(L' - L, 0)$ times. We will say that two paths in the same $\mathfrak{g}_{\mathbb{Q}(\mathfrak{f})}$-orbit are **closed point equivalent**.

5.4. **Explicit description of the action of complex conjugation on $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$.** We now give an explicit description of the action of complex conjugation on the isogeny volcano – up to $\mathfrak{g}_{\mathbb{R}}$-equivariant graph-theoretic isomorphism – in all cases. For $L \geq 0$, put

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

By Corollary 2.5, $\mathfrak{r}_L$ is the number of real vertices in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ at level L. Lemma 2.8 computes $\mathfrak{r}_L$ in terms of $\mathfrak{r}_0$.

Lemma 5.5. *Suppose that $\ell > 2$ is a prime that is unramified in K. Then every real surface vertex has exactly two real descendants, while every real non-surface vertex has a unique real descendant.*



Proof. In this case Lemma 2.8 gives

$$\mathfrak{r}_1 = 2\mathfrak{r}_0, \forall L \geq 1,\ \mathfrak{r}_{L+1} = \mathfrak{r}_L.$$

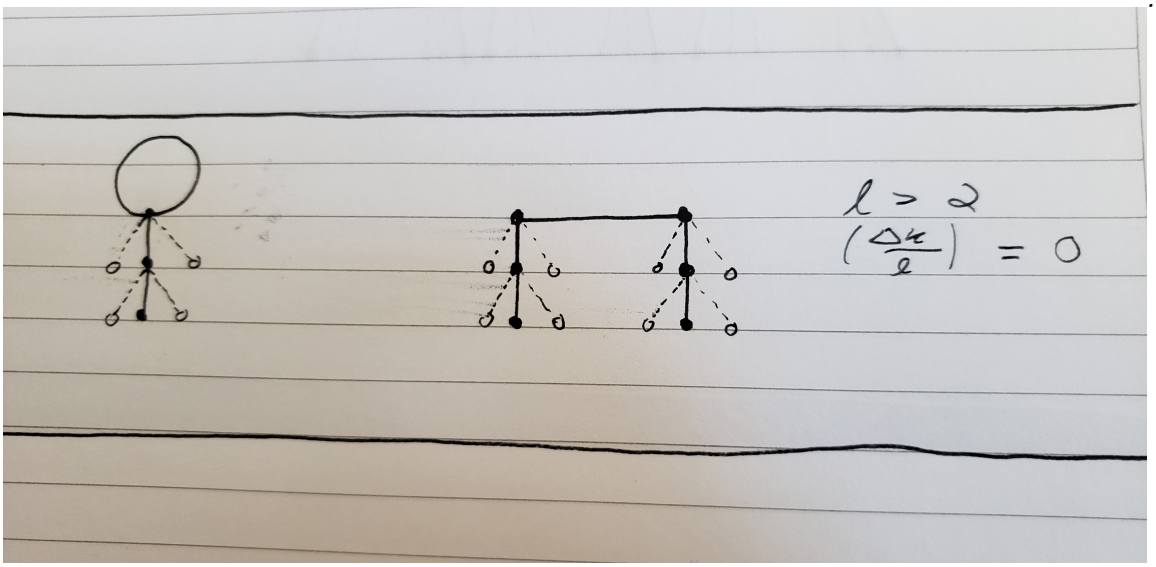
Otherwise put, there are twice as many real vertices in level 1 as on the surface, and for all $L \geq 1$ the number of real vertices at level L is the same.

Let v_0 be a real surface vertex, corresponding to an $\mathfrak{f}_0^2\Delta_K$-CM elliptic curve $E_{/\mathbb{C}}$ with $j(E) \in \mathbb{R}$. Choose a real model $E_{/\mathbb{R}}$. Since $E(\mathbb{R})$ is isomorphic to either S^1 or $S^1 \times \mathbb{Z}/2\mathbb{Z}$ [SII, Cor. V.2.3.1], E has an $\mathbb{R}$-point of order ℓ and thus has an $\mathbb{R}$-rational cyclic subgroup C of order ℓ. The map $E \to E/C$ then defines a real edge with initial vertex v_0.

Case 1: Suppose that ℓ is inert in K. In this case there are $\ell + 1$ descending edges emanating from v_0. As above, at least one is real, which leaves an action of $\mathfrak{g}_{\mathbb{R}}$ on the other ℓ descending vertices. Since ℓ is odd, at least one additonal edge must be real. This shows that every real vertex has at least two descending real edges. Since distinct descending real edges connect to distinct real vertices in level 1 and there are twice as many real vertices in level 1 as in level 0, it must be the case that every real vertex has exactly two real descendants. Now suppose that $L \geq 1$ and v_L is a real vertex at level L. Then $\mathfrak{g}_{\mathbb{R}}$ acts on the ℓ descending vertices, and since ℓ is odd there must be at least one real descendant. Since the number of real vertices in level $L + 1$ is equal to the number of real vertices in level L, each real vertex in level L must have a unique real descendant.

Case 2: Suppose that ℓ splits in K. The argument is very similar, except now there is a conjugate pair of complex edges emanating from every real surface vertex v_0, leaving $\ell - 1$ descending edges from v_0. As above, at least one of these must be real, and since $\ell - 2$ is odd, another one must be real, and the same argument shows that exactly two descendants of v_0 must be real. The argument that every real vertex in level $L \geq 1$ has a unique real descendant is the same as in Case 1. □

Lemma 5.6. *Suppose that $\ell > 2$ is a prime that ramifies in K. Then every real vertex has a unique real descendant.*



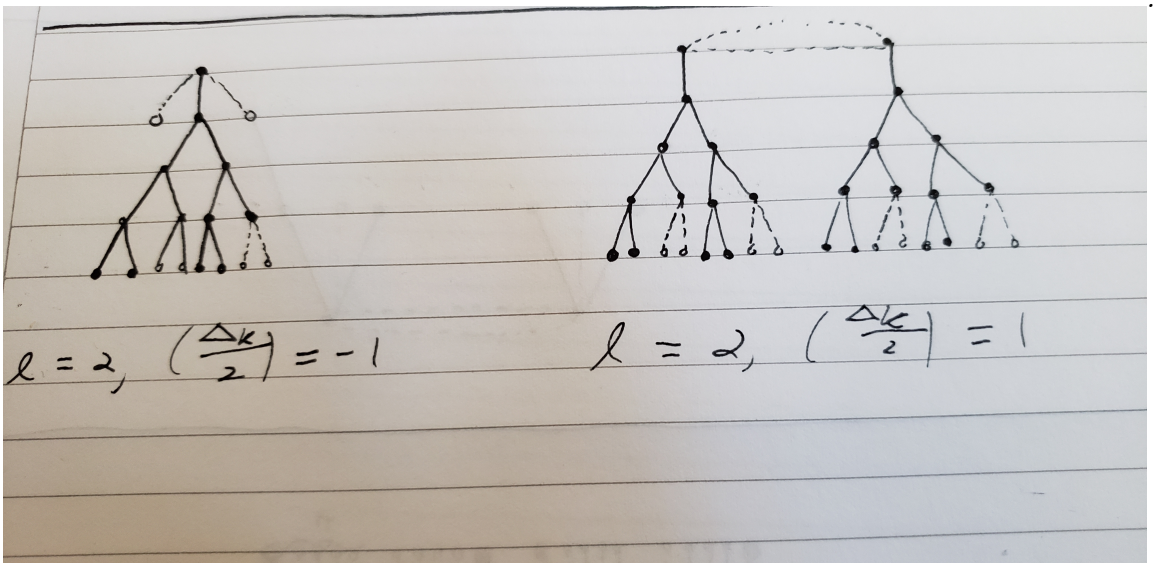
Proof. In this case Lemma 2.8 gives

$$\mathfrak{r}_{L+1} = \mathfrak{r}_L \ \forall L \geq 0.$$

Since ℓ ramifies in K, each real vertex has ℓ descending vertices, and since ℓ is odd, one of these vertices must be real. The same counting argument as above shows that each real vertex has a unique real descendant. □

Lemma 5.7. *Suppose that $\ell = 2$ does not ramify in K. Then:*

a) *Every real surface vertex has a unique real descendant.*
b) *For $L \in \{1, 2\}$, both of the descendants of every real vertex of level L are real.*
c) *For $L \geq 3$, we partition the real vertices of level L into pairs of vertices $\{v_L, w_L\}$, such that v_L and w_L are adjacent to the same vertex u_{L-1} in level $L-1$. Then exactly one of v_L and w_L has two real descendants and the other has no real descendants.*



Proof. In this case Lemma 2.8 gives

$$\mathfrak{r}_1 = \mathfrak{r}_0,\ \mathfrak{r}_2 = 2\mathfrak{r}_1,\ \mathfrak{r}_3 = 2\mathfrak{r}_2,\ \mathfrak{r}_{c+1} = \mathfrak{r}_c\ \forall c \geq 3.$$

a) If 2 is inert in K, then every real surface vertex has three descendants. Since 3 is odd, at least one must be real. Since the number of real vertices in level 1 is the same as in level 0, exactly one must be real, establishing part a) in this case. If 2 splits in K, then every real surface vertex has a unique descending vertex, which must therefore be real.
b) For all $L \geq 1$, every vertex at level L has exactly two descendant vertices. Since $\mathfrak{r}_2 = 2\mathfrak{r}_1$ and $\mathfrak{r}_3 = 2\mathfrak{r}_2$, it must be that for $L \in \{1, 2\}$ every real vertex at level L has both of its descendants real.
c) Suppose now that $L \geq 3$ and let v_L, w_L be a pair of real vertices at level L as in the statement of the result. (If v_L is real and is incident to u_{L-1} in level $L-1$, then u_{L-1} is real with at least one of its two descendant vertices real, so the other one, w_L, must also be real.) If we can show that v_L and w_L do not both have descendant real vertices, then an easy counting argument using $\mathfrak{r}_{L+1} = \mathfrak{r}_L$ establishes the desired conclusion. So assume

now, and let v_{L+1} be a real descendant of v_L and w_{L+1} be a real descendant of w_L. Then

$$v_{L+1} \mapsto v_L \mapsto u_{L-1} \mapsto w_L \mapsto w_{L+1}$$

is a proper, real cyclic 2^4-isogeny with source elliptic curve having discriminant $\Delta = 2^{2L+2}\mathfrak{f}_0^2\Delta_K$, so there is a primitive, proper real $\mathcal{O}(\Delta)$-ideal of index 16. But by Theorem 2.9, if there is a primitive, proper cyclic real $\mathcal{O}(\Delta)$-ideal of index 2^a, then $a = 2$ or $a = \mathrm{ord}_2(\Delta) - 2 = 2L \geq 6$, a contradiction. □

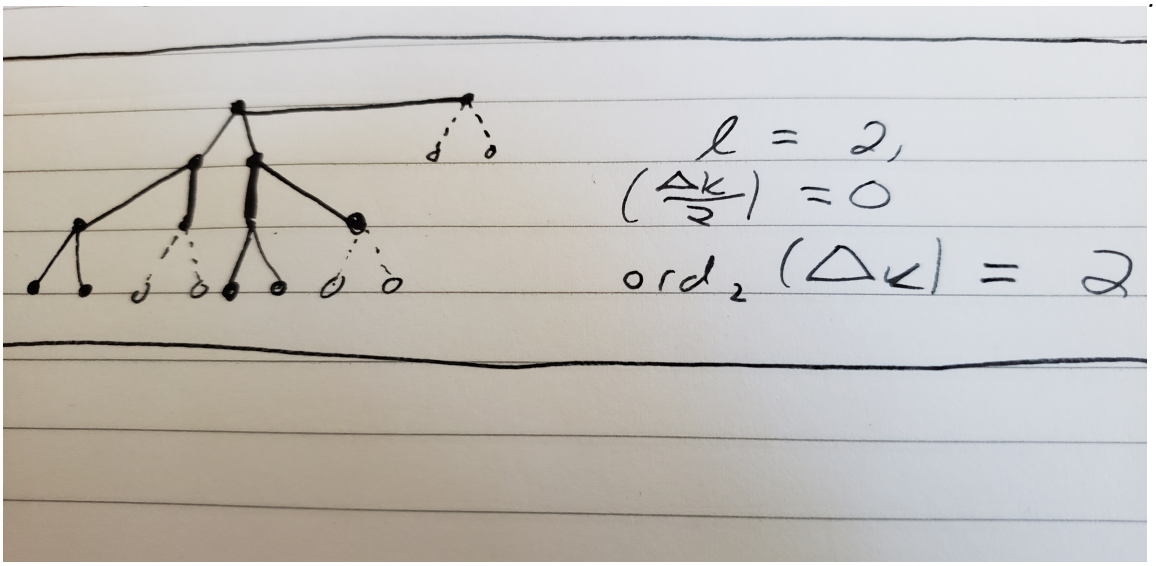
To describe the structure in the next case we need a simple preliminary result.

Lemma 5.8. *Let Δ be an even imaginary quadratic discriminant, let $\mathcal{O}$ be the imaginary quadratic order of discriminant Δ, and let $\mathfrak{p}$ be the unique ideal of $\mathcal{O}$ of norm 2. Then $\mathfrak{p}$ is principal iff $\Delta \in \{-4, -8\}$.*

Proof. For any $N \in \mathbb{Z}^+$, there is a principal $\mathcal{O}$-ideal of norm N iff N is integrally represented by the quadratic form $x^2 + |\frac{\Delta}{4}|y^2$. This form represents 2 iff $\Delta \in \{-4, -8\}$. □

Lemma 5.9. *Suppose that $\ell = 2$ ramifies in K and that $\mathrm{ord}_2(\Delta_K) = 2$. Then:*

a) *The set of real surface vertices is canonically partitioned into pairs $\{v_0, w_0\}$ such that v_0 has two real descendants and w_0 has no real descendants.*
b) *Every descendant vertex of a real vertex in level 1 is real.*
c) *For $L \geq 2$, we partition the real vertices of level L into pairs of vertices $\{v_L, w_L\}$, such that v_L and w_L are adjacent to the same vertex u_{L-1} in level $L - 1$. Then exactly one of v_L and w_L has two real descendants and the other has no real descendants.*



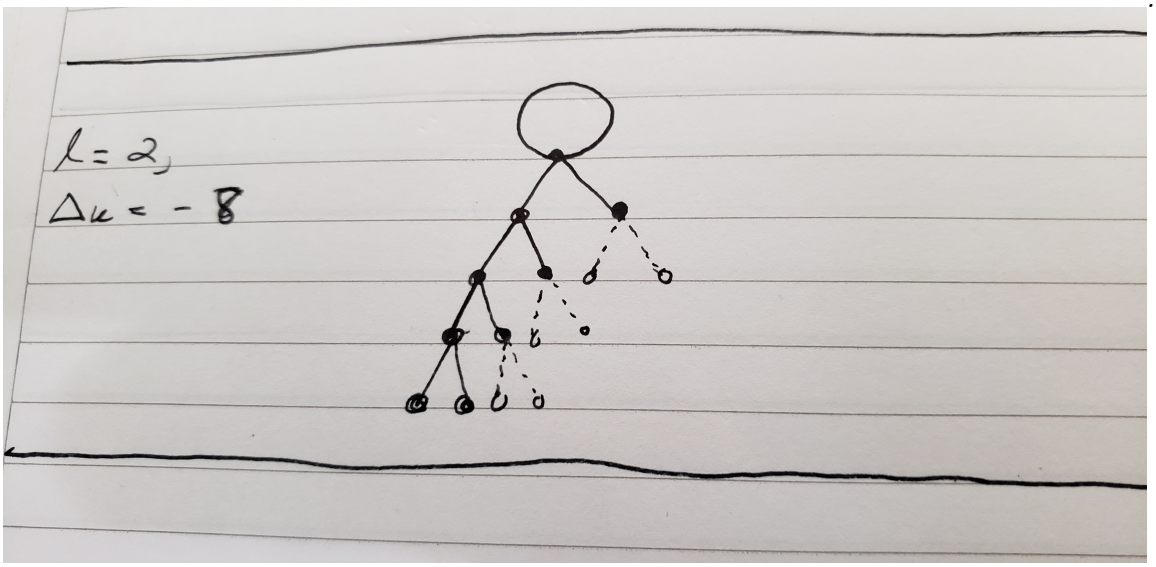
Proof. In this case Lemma 2.8 gives

$$\mathfrak{r}_1 = \mathfrak{r}_0, \ \mathfrak{r}_2 = 2\mathfrak{r}_1, \ \mathfrak{r}_{L+1} = \mathfrak{r}_L \ \forall L \geq 2.$$

a) Let $\mathcal{O}_0$ be the imaginary quadratic order of discriminant $\mathfrak{f}_0^2 \Delta_K$. Since 2 divides Δ_K and does not divide $\mathfrak{f}_0$, the ring $\mathcal{O}_0$ has a unique prime ideal $\mathfrak{p}$ of norm 2, which is moreover proper. Since $\mathfrak{p}^2 = (2)$, the class $[\mathfrak{p}] \in \operatorname{Pic} \mathcal{O}$ has order at most 2, and since $\Delta_K = -4$ has been excluded, by Lemma 5.8 the class $[\mathfrak{p}]$ has order exactly 2. This implies that there are no surface loops and indeed gives the partition of the set of surface vertices into pairs: it is the decomposition of $\operatorname{Pic} \mathcal{O}_0$ into cosets of $\{1, [\mathfrak{p}]\}$. Because $\mathfrak{r}_1 = \mathfrak{r}_0$, a counting argument shows that if the conclusion of part a) did not hold there would be a pair real vertices v_0, w_0 linked by a surface edge such that neither v_0 nor w_0 have any real descendants. But in this case the real elliptic curve corresponding to v_0 would admit no real cyclic 4-isogeny, whereas as we have observed above, every real elliptic curve admits a real cyclic N-isogeny for all positive integers N.
b) This follows from $\mathfrak{r}_2 = 2\mathfrak{r}_1$.
c) The argument for this is the same as for Lemma 5.7c). □

Lemma 5.10. *Suppose that $\ell = 2$ and $\Delta_K = -8$. Then:*

a) *There is one surface vertex v_0, which is real.*
b) *Both of the descendants v_1, w_1 of v_0 are real.*
c) *For all $L \geq 1$, there are two real vertices v_L, w_L in level L that are descendants of the same real vertex v_{L-1} in level L. The vertex v_L has two real descendants v_{L+1}, w_{L+1}, and the vertex w_L has no real descendants.*

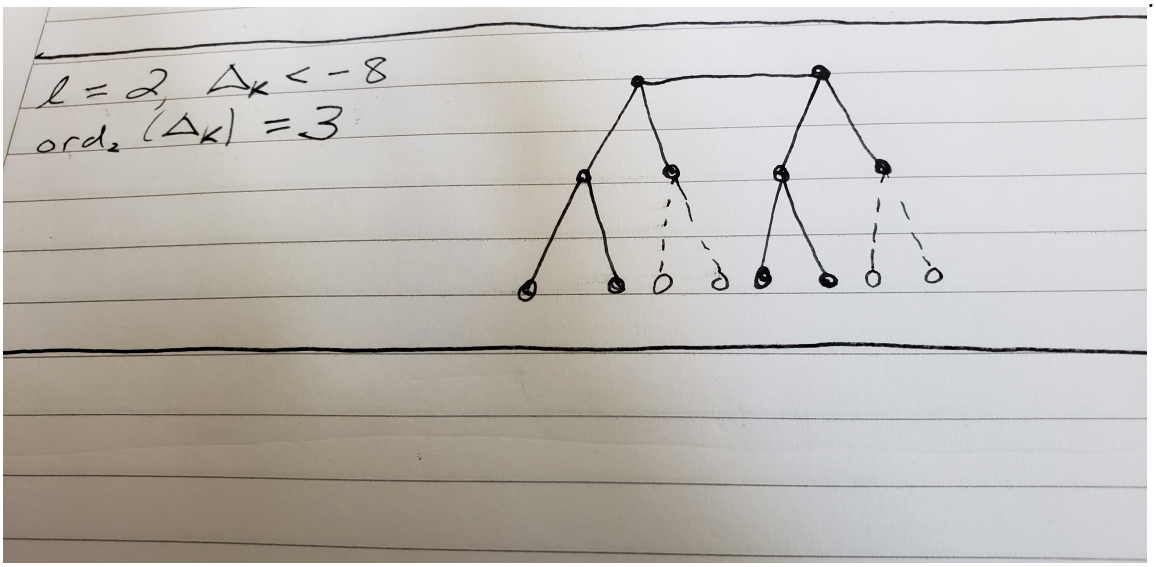


Proof. We have $\mathfrak{r}_1 = 2\mathfrak{r}_0 = 2$ and $\mathfrak{r}_{L+1} = \mathfrak{r}_L = 2$ for all $L \geq 1$. Also we have $h_{-8} = 1$. The claimed structure follows from this, and we leave the details to the reader. □

Lemma 5.11. *Suppose that $\ell = 2$ ramifies in K, $\operatorname{ord}_2(\Delta_K) = 3$ and $\Delta_K < -8$. Then:*

a) *Every descendant vertex of a real surface vertex is real.*

b) *For $L \geq 1$, we partition the real vertices of level L into pairs of vertices $\{v_L, w_L\}$, such that v_L and w_L are adjacent to the same vertex u_{L-1} in level $L-1$. Then exactly one of v_L and w_L has two real descendants and the other has no real descendants.*



Proof. We have $\mathfrak{r}_1 = 2\mathfrak{r}_0$ and $\mathfrak{r}_{L+1} = \mathfrak{r}_L$ for all $L \geq 1$. The arguments are similar to those in the previous cases and may be left to the reader. □

6. Some Applications

6.1. **The Field of Moduli of an Isogeny.**

Lemma 6.1. *Let K be an imaginary quadratic field with $\Delta_K < -4$, and let $\varphi : E \to E'$ be an isogeny of complex K-CM elliptic curves. Then we have*

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

Proof. Proposition 3.3a) reduces us to the case in which φ is a cyclic N-isogeny. Certainly we have that $K(\varphi)$ contains both $\mathbb{Q}(\varphi)$ and $K(j(E), j(E'))$, so it is enough to show that $K(\varphi) \subset K(j(E), j(E'))$.

If $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ then $\varphi = \varphi_r \circ \ldots \circ \varphi_1$, where $\varphi_i : E_{i-1} \to E_i$ is a cyclic $\ell_i^{a_i}$-isogeny. (Thus $E_0 = E$ and $E_r = E'$.) For $0 \leq i \leq r$, let $\mathfrak{f}_i$ be the conductor of E_i. Put $M := \mathrm{lcm}(\mathfrak{f}_0, \mathfrak{f}_r)$. By (3) and Proposition 2.2 we have

$$K(j(E), j(E')) = K(\mathfrak{f}_0)K(\mathfrak{f}_r) = K(M).$$

From our isogeny volcano analysis, we know that

$$K(\varphi_i) = K(j(E_i), j(E_{i+1})) = K(\mathrm{lcm}(\mathfrak{f}_i, \mathfrak{f}_{i+1})).$$

Moreover, for all $1 \leq i \leq r$ we have $\mathfrak{f}_i/\mathfrak{f}_{i-1} \in \ell_i^{\mathbb{Z}}$, from which it follows that for all $1 \leq i \leq r$ and $0 \leq j \leq r$ we have $\mathrm{ord}_{\ell_i}(\mathfrak{f}_j) \leq \mathrm{ord}_{\ell_i}(M)$ and thus

$$K(\varphi) = K(\varphi_1) \cdots K(\varphi_r) \subset K(M). \qquad \square$$

Theorem 6.2. *Let K be an imaginary quadratic field with $\Delta_K < -4$, and let $\varphi : E \to E'$ be an isogeny of complex K-CM elliptic curves. Then:*

a) *If $j(E)$ and $j(E')$ are not coreal, then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E')) = K(j(E), j(E'))$.*

b) *If $j(E)$ and $j(E')$ are coreal and there is a prime ℓ that splits in K such that φ_{cyc} factors through a proper ℓ-isogeny then $\mathbb{Q}(\varphi) = K(j(E), j(E')) \supsetneq \mathbb{Q}(j(E), j(E'))$.*

c) *Suppose that φ_{cyc} has prime power degree. If $j(E)$ and $j(E')$ are coreal and for no prime ℓ that splits in K does φ_{cyc} factor through a proper ℓ-isogeny, then $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E')) \subsetneq K(j(E), j(E'))$.*

Proof. Once again, by Proposition 3.3a) we may assume that φ is a cyclic N-isogeny. In view of Lemma 6.1, we have

$$\mathbb{Q}(j(E), j(E')) \subset \mathbb{Q}(\varphi) \subset K(\varphi) = K(j(E), j(E')). \tag{6}$$

Moreover, by Theorem 5.1 we have $\mathbb{Q}(j(E), j(E')) = K(j(E), j(E'))$ iff $j(E)$ and $j(E')$ are not coreal. From this and (6) part a) follows immediately. If ℓ splits in K and φ factors through a proper ℓ-isogeny ι, we know that $\mathbb{Q}(\varphi) \supset \mathbb{Q}(\iota) \supset K$ and thus $\mathbb{Q}(\varphi) = K(j(E), j(E'))$, which shows part b).

c) Finally, assume that $N = \ell^a$ is a prime power, that $j(E)$ and $j(E')$ are coreal, and that if ℓ splits in K the isogeny φ does not factor through a proper ℓ-isogeny. In this case, our theory of isogeny volcanoes shows that $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$: indeed, the acending part of the corresponding path yields an isogeny that is defined over $\mathbb{Q}(j(E))$, which shows that the j-invariant of each vertex in this portion of the path lies in $\mathbb{Q}(j(E))$. Surface vertices, which exist only in the ramified case, are therefore defined over $\mathbb{Q}(j(E))$, while the descending part of the corresponding path yields an isogeny that is defined over $\mathbb{Q}(j(E'))$. So the isogeny φ is defined over $\mathbb{Q}(j(E), j(E'))$. $\square$

Remark. I suspect that Theorem 6.2c) holds without the hypothesis that φ_{cyc} has prime power degree. Otherwise and perhaps more simply put, for any cyclic N-isogeny of CM elliptic curves that does not factor through a proper ℓ-isogeny for a prime ℓ that splits in K, I suspect that $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$, just as Proposition 3.3 shows is the case for all elliptic curves without complex multiplication.

Having spoken of Proposition 3.3, let us point out that the method of proof there is related to the above proof when $N = \ell^a$ is a prime power. Indeed, the structure of the ℓ-isogeny volcano shows that, excluding surface edges in the split case, any two vertices in the volcano that are joined by a path are joined by a *unique* nonbacktracking path. (More precisely, if a nonbacktracking path of length a in the ℓ-isogeny volcano does not contain a split surface edge, it is the unique path from its initial vertex to its terminal vertex of length a, and every other path is longer.) It certainly follows that the given isogeny $\varphi : E \to E'$ is the unique cyclic N-isogeny between E and E', so the first part of the proof of Proposition 3.3 shows that $\mathbb{Q}(\varphi) = \mathbb{Q}(j(E), j(E'))$. It may be that a corresponding uniqueness result

holds in the general case. It is not so clear to me at the moment how to analyze when $E/C_1 \cong E/C_2$ for finite subgroups C_1, C_2 of equal size.

Corollary 6.3. *Let $\Delta = \mathfrak{f}^2\Delta_K$ with $\Delta_K < -4$, let $E_{/\mathbb{C}}$ be a Δ-CM elliptic curve and let $\varphi : E \to E'$ be an isogeny. Then there is $M \in \mathbb{Z}^+$ such that the field of moduli $\mathbb{Q}(\varphi)$ of φ is isomorphic to either $\mathbb{Q}(M\mathfrak{f})$ or to $K(M\mathfrak{f})$.*

6.2. **$K(\mathfrak{f})$-rational cyclic N-isogenies.** The following is a result of Bourdon-Clark [BC20a, Thm. 6.18a)].

Theorem 6.4. *Let $\Delta < -4$, and write $\Delta = \mathfrak{f}^2\Delta_K$. For $N \in \mathbb{Z}^+$, there is a Δ-CM elliptic curve $E_{/K(\mathfrak{f})}$ and a $K(\mathfrak{f})$-rational cyclic N-isogeny $\varphi : E \to E'$ iff Δ is a square in $\mathbb{Z}/4N\mathbb{Z}$.*

Here we suppose moreover that $\Delta_K < -4$ and give a different proof of Theorem 6.4. As explained in §3.5, since $\Delta_K < -4$, for a positive integer $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ there is a $K(\mathfrak{f})$-rational cyclic N-isogeny with source elliptic curve Δ-CM iff for all $1 \leq i \leq r$ there an $K(\mathfrak{f})$-rational cyclic $\ell_i^{a_i}$-isogeny with source elliptic curve Δ-CM. Moreover, we have that Δ is a square in $\mathbb{Z}/4\ell_1^{a_1} \cdots \ell_r^{a_r}\mathbb{Z}$ iff Δ is a square in $\mathbb{Z}/4\ell_i^{a_i}\mathbb{Z}$ for all $1 \leq i \leq r$, so we reduce to the case in which $N = \ell^a$ is a prime power. Let $M(\Delta, \ell)$ be the supremum of positive integers a such that some (equivalently, every) Δ-CM elliptic curve has a $K(\mathfrak{f})$-rational cyclic ℓ^a-isogeny. If $L = \mathrm{ord}_\ell(\mathfrak{f})$, this quantity can be understood in terms of the volcano $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ as the supremum of all lengths of nonbacktracking paths starting at a vertex of level L and ending at a level $L' \leq L$.

• Suppose that $\left(\frac{\Delta_K}{\ell}\right) = 1$. In this case $M(\Delta, \ell) = \infty$: indeed, we can ascend to the surface and follow by a nonbacktracking path of arbitrary length on the surface. Writing $\Delta = \mathfrak{f}^2\Delta_K$, it is enough to check that Δ_K is a square modulo $4\ell^a$ for all positive integers a, which holds iff it is a square modulo ℓ^a for all positive integers a and is indeed the case by Hensel's Lemma since this holds modulo ℓ if $\ell > 2$ (resp. modulo 8 if $\ell = 2$).

• Suppose that $\left(\frac{\Delta}{\ell}\right) = -1$. In this case we have $L = 0$ so we are on the surface an are in the inert case so have no surface vertices, so (as seen in Case 1) *every* nonbacktracking path of positive length ends lower than it starts. If $\ell > 2$ then our assumption gives that Δ is not a square modulo ℓ. If $\ell = 2$ then our assumption gives $\Delta \equiv 5 \pmod 8$ hence is not a square modulo $8 = 4\ell$.

• Suppose that $L = \mathrm{ord}_\ell(\mathfrak{f}) \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = -1$. In this case the longest nonbacktracking path starting at level L and ending no deeper than level L is a path that ascends to the surface and descends back down to level L, so $M(\Delta, \ell) = 2L$. One checks that the largest a such that $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ is a square modulo ℓ^a is $a = 2L$: see the end of [BC20a, §7.4] for the details.

• Suppose that $\left(\frac{\Delta_K}{\ell}\right) = 0$. In this case the longest nonbacktracking path starting at level L and ending no deeper than level L is a path that ascends to the surface, takes the

unique surface edge and then descends back down to level L, so $M(\Delta, \ell) = 2L + 1$. One checks that the largest a such that $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ is a square modulo $4\ell^a$ is $a = 2L + 1$ see the end of [BC20a, §7.4] for the details.

Remark. That isogeny volcanoes give a different and arguably more transparent approach to Theorem 6.4 when $\Delta_K < 4$ was pointed out to me by A. Sutherland in January 2019. This was how I first learned of the utility of isogeny volcanoes to CM points on modular curves, and I am greatly indebted to him for it.

6.3. $\mathbb{Q}(\mathfrak{f})$**-rational cyclic** N**-isogenies.** Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic order with $\Delta_K < -4$. For a positive integer N, let $I(\Delta, N)$ be the condition that there is a Δ-CM elliptic curve E defined over a number field F isomorphic to $\mathbb{Q}(\mathfrak{f})$ (and thus $F = \mathbb{Q}(j(E))$) such that E admits an F-rational cyclic N-isogeny. In [Kw99], S. Kwon determined all pairs (Δ, N) (again, with $\Delta_K < -4$) for which $I(\Delta, N)$ holds. We will deduce this result, along with some later generalizations, from the present work.

As we have seen, it is no loss of generality to assume that we have a Δ-CM elliptic curve defined over $\mathbb{Q}(\mathfrak{f}) = \mathbb{Q}(j(\mathbb{C}/\mathcal{O})$. As in the previous section we immediately reduce to the case $N = \ell^a$ is a prime power. Indeed, for each prime ℓ, we let $m_\ell(\Delta)$ be the largest non-negative integer a such that $I(\Delta, \ell^a)$ holds. We will see shortly that for each fixed Δ we have $m_\ell(\Delta) = 0$ for all sufficiently large primes ℓ. It then follows that $I(\Delta_N)$ holds iff $N \mid \prod_\ell \ell^{m_\ell(\Delta)}$.

We have the following "volcanic" interpretation of $m_\ell(\Delta)$: it is the longest length a of a real path in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ starting at level L and ending at level L' such that $\mathbb{Q}(\ell^{2L'}\mathfrak{f}_0^2\Delta_K) \hookrightarrow \mathbb{Q}(\ell^{2L}\mathfrak{f}_0^2\Delta_K)$ (as we will see, in all but one case the latter condition simplifies to $L' \le L$).

• Suppose that $\ell > 2$ and $\left(\frac{\Delta_K}{\ell}\right) \neq 0$. Then such a path must begin with an upward component – there are no real horizontal edges and $\mathbb{Q}(\ell\mathfrak{f}) \supsetneq \mathbb{Q}(\mathfrak{f})$ in this case. The longest such path ascends all the way to the surface and then descends back down to level L, which is possible because every real surface vertex has two real descendants in this case. Thus we get $m_\ell(\Delta) = 2L$.

• Suppose that $\ell > 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$. If $L = 0$ the only nontrivial such path takes the unique horizontal edge emanating from the corresponding surface vertex, so $m_\ell(\Delta) = 1$. Otherwise the longest such path ascends to the surface, takes the unique horizontal edge, and descends back to level L. Thus in general we get $m_\ell(\Delta) = 2L + 1$.

• Suppose that $\ell = 2$ and $\left(\frac{\Delta}{2}\right) = 1$. In this case $L = 0$ and there are no real horizontal edges, so we must descend. We have $\mathbb{Q}(2\mathfrak{f}) = \mathbb{Q}(\mathfrak{f})$ and $[\mathbb{Q}(4\mathfrak{f}) : \mathbb{Q}(2\mathfrak{f})] = 2$ so that we can descend once: $m_2(\Delta) = 1$.

• Suppose that $\ell = 2$ and $\left(\frac{\Delta}{2}\right) = -1$. In this case $L = 0$, there are no horizontal edges and

$\mathbb{Q}(2\mathfrak{f}) \supsetneq \mathbb{Q}(\mathfrak{f})$, so $m_2(\Delta) = 0$.

• Suppose that $\ell = 2$, $\left(\frac{\Delta}{2}\right) = 0$ and $\left(\frac{\Delta_K}{2}\right) \neq 0$. If $L = 0$ then we must go downward, but $\mathbb{Q}(\ell\mathfrak{f}) \supsetneq \mathbb{Q}(\mathfrak{f})$, so $m_2(\Delta) = 0$. If $L = 1$ we can go upward once and then there is no nonbacktracking real edge, so $m_2(\Delta) = 1$. If $L \geq 2$ then the longest path ascends to level 1 and then descends back to level L (cf. Lemma 5.5), so we have $m_2(\Delta) = 2L - 2$.

• Suppose that $\ell = 2$, $\left(\frac{\Delta_K}{2}\right) = 0$ and $\mathrm{ord}_2(\Delta_K) = 2$. In this case we have $\mathbb{Q}(2\mathfrak{f}) \supsetneq \mathbb{Q}(\mathfrak{f})$, we want the length of the longest real path ending at level $L' \leq L$. If $L = 0$ we can take the horizontal edge, giving $m_2(\Delta) = 1$. If $L \geq 1$ we can ascend to the surface and then descend back down to level L, giving $m_2(\Delta) = 2L$.

• Suppose that $\ell = 2$, $\left(\frac{\Delta_K}{2}\right) = 0$ and $\mathrm{ord}_2(\Delta_K) = 3$. Again we have $\mathbb{Q}(2\mathfrak{f}) \supsetneq \mathbb{Q}(\mathfrak{f})$, so we want the length of the longest real path ending at level $L' \leq L$. If $L = 0$ we can take the horizontal edge, giving $m_2(\Delta) = 1$. If $L \geq 1$ we can ascend to the surface, take the horizontal edge and then descend back down to level L, giving $m_2(\Delta) = 2L + 1$.

This agrees with Kwon's result. To confirm this it is easier to check against [BC20b, Prop. 6.4], which records $m_\ell(\Delta)$ in all cases in which $\ell \mid \Delta$.

Remark. The factorization of a pleasant isogeny given in §3.4 is essentially due to Kwon and is a key part of his proof of the classification of cyclic N-isogenies over $\mathbb{Q}(j(E))$. He also develops and uses some ideal theory of imaginary quadratic orders. Thus our approach to Kwon's results is relatively similar to his, the main difference being use of isogeny volcanoes. Let us also recall that in the determination of the action of complex conjugation on the isogeny volcano in some $\ell = 2$ cases we used Kwon's Theorem 2.9.

6.4. **Finiteness of isogenies over a number field.** In the previous two sections we proved two results of the the following form: for an imaginary quadratic discriminant $\Delta = \mathfrak{f}^2\Delta_K$ with $\Delta_K < -4$ and a number field F, we found all positive integers N such that there is an F-rational Δ-CM point on $X_0(N)$. Using our Classification Theorem we can derive similar results for any number field F.

In [BC20b, Thm. 5.3] it is shown that Kwon's classification of $\mathbb{Q}(\mathfrak{f})$-rational cyclic isogenies remains valid if $\mathbb{Q}(\mathfrak{f})$ is replaced by any number field that contains neither K nor a field isomorphic to $\mathbb{Q}(\ell\mathfrak{f})$ for any prime ℓ. The theory presented here makes this extension immediate. More generally, for any subfield F of $\mathbb{C}$, Corollary 6.3 implies that the set of positive integers N for which $X_0(N)$ has an F-rational Δ-CM point depends only on whether F contains K and for which $\mathfrak{f} \in \mathbb{Z}^+$ it contains a number field isomorphic to $\mathbb{Q}(\mathfrak{f})$.

In the next result, by "a rational ring class field" we mean a number field of the form $\mathbb{Q}(j(E))$ for some CM elliptic curve $E_{/\mathbb{C}}$. A number field is a rational ring class field if it is isomorphic to $\mathbb{Q}(j_\Delta)$ for some imaginary quadratic discriminant Δ.

Theorem 6.5. *Let F be a subfield of $\mathbb{C}$.*

a) *Suppose that F contains either the Hilbert class field of some imaginary quadratic field or infinitely many rational ring class fields. Then the set of positive integers N such that $X_0(N)$ has an F-rational CM point is infinite.*
b) *Suppose that F does not contain the Hilbert class field of any imaginary quadratic field and contains only finitely many rational ring class fields. Then the set of positive integers N such that $X_0(N)$ has an F-rational Δ-CM point is finite.*

Proof. a) Suppose first that there is an imaginary quadratic field K such that F contains the Hilbert class field $K(1)$ of K. Since $K(1) = K(j_\Delta)$, the field F contains j_Δ and K and hence, for each prime ℓ that splits in K and all $a \in \mathbb{Z}^+$, there is a $K(1)$-rational cyclic ℓ^a-isogeny $\varphi : E \to E'$ where $j(E) = j_{\Delta_K}$, establishing the claim in this case.

Next suppose that F contains infinitely many rational ring class fields. Since each rational ring class field has finitely many Galois conjugates, this holds iff there is an infinite set $\{\Delta_n\}_{n=1}^\infty$ of imaginary quadratic discriminants such that for all $n \in \mathbb{Z}^+$ F contains a subfield isomorphic to $\mathbb{Q}(j_{\Delta_n})$. It follows that either the set of prime numbers ℓ that divide Δ_n for some $n \in \mathbb{Z}^+$ is infinite or for all $A \in \mathbb{Z}^+$ there is $n_A \in \mathbb{Z}^+$, a prime number ℓ_A and an $a_A \in \mathbb{Z}^+$ such that $\ell_A^{a_A} \mid \Delta_A$. It follows from the results in the previous section (and from Kwon's Theorem, in particular) that when $\Delta_K < -4$, if $\ell^A \mid \Delta$, then there is a $\mathbb{Q}(j_\Delta)$-rational Δ-CM point on $X_0(\ell^A)$. By [BC20b, Remark 5.2, Corollary 5.11], the assertions of the previous sentence hold also when $\Delta_K \in \{-3, -4\}$. This completes the proof of part a).
b) Suppose that F contains no Hilbert class field of an imaginary quadratic field and contains only finitely many rational ring class fields. Then the set of imaginary quadratic discriminants Δ such that F contains the j-invariant of any Δ-CM elliptic curve is finite, so it is enough to fix an imaginary quadratic discriminant Δ such that F contains a subfield isomorphic to $\mathbb{Q}(j_\Delta)$ and show that the set of positive integers N such that $X_0(N)$ admits an F-rational Δ-CM point is finite. Then F does not contain K, for if so it would contain the ring class field of discriminant Δ and hence the Hilbert class field of K, contrary to our hypothesis.

We claim that we may further restrict to the case $\Delta = \Delta_K$. Indeed, if $\Delta = \mathfrak{f}^2\Delta_K$ and there is a cyclic N-isogeny $\varphi : E \to E'$ defined over F with E a Δ-CM elliptic curve, let C_N be the kernel of φ. Let $\iota_{\mathfrak{f},1} : E \to \tilde{E}$ be the canonical, F-rational cyclic $\mathfrak{f}$-isogeny described in §3.4. Then $\tilde{C}_N \coloneqq \iota_{\mathfrak{f},1}(C_N)$ is an F-rational subgroup scheme of the Δ_K-CM elliptic curve $E_{/F}$ of order a multiple of $\frac{N}{\gcd(N,\mathfrak{f})}$. In our situation $\mathfrak{f}$ is bounded, so N becomes arbitrarily large iff $\frac{N}{\gcd(N,\mathfrak{f})}$ does, in which case $\tilde{E} \to \tilde{E}/\tilde{C}_N$ exhibits F-rational cyclic Δ_K-CM isogenies of arbitarily large degree.

Let ℓ be a prime number such that $\ell \nmid 2\Delta_K$, and suppose $\varphi : E \to E'$ is an F-rational ℓ-isogeny with E a Δ_K-CM elliptic curve. Since Δ_K is the discriminant of the maximal order $\mathbb{Z}_K$ in K, such an isogeny must be horizontal or descending, and since ℓ does not ramify in K the only possible horizontal edges occur when ℓ splits in K and these have field of moduli containing K, hence not contained in F. Therefore E' must be an $\ell^2\Delta_K$-CM

elliptic curve, meaning that $\mathbb{Q}(j(E'))$ is isomorphic to $\mathbb{Q}(\ell)$. By hypothesis this only holds for finitely many primes ℓ.

It remains to show that for each prime number ℓ there is a positive integer A such that no Δ_K-CM elliptic curve admits an F-rational cyclic ℓ^A-isogeny. Fix a prime ℓ, and let $\varphi : E \to E'$ be an F-rational cyclic ℓ^a-isogeny, with E a Δ_K-CM elliptic curve. Because of our assumption on F, there is a positive integer B such if we factor E into ℓ-isogenies, then the conductor of the endomorphism ring of the source elliptic curve of every factor isogeny divides ℓ^B. In particular, if $\mathfrak{f}'$ is the conductor of $\mathrm{End}(E')$ and $L' \coloneqq \mathrm{ord}_\ell(\mathfrak{f}')$, then $L' \leq B$. If there were F-rational cyclic ℓ^a-isogenies $\varphi_a : E \to E'$ with E Δ_K-CM for all $a \in \mathbb{Z}^+$, then for all $a \in \mathbb{Z}^+$ there is some $0 \leq L_a \leq B$ and an F-rational proper cyclic ℓ^a-isogeny of Δ_a-CM elliptic curves, where $\Delta_a = \ell^{2L_a}\Delta_K$. (This is just because of the Pigeonhole Principle: since only finitely many endomorphism rings appear in the factor isogenies of the φ_a, as a approaches infinity at least one endomorphism ring must appear arbitrarily often.) Since F does not contain K, a proper cyclic ℓ^a isogeny of $\mathcal{O}$-CM elliptic curves is the kernel isogeny $E_1 \to E_1/[\mathfrak{a}]$ attached to a primitive proper real $\mathcal{O}(\Delta_a)$-ideal $\mathfrak{a}$ of norm ℓ^a. By [BCS17, Cor. 3.8] we must have

$$\ell^a = |\mathfrak{a}| \mid \Delta_a = \ell^{2L_a}\Delta_K \mid \ell^{2B}\Delta_K,$$

and for sufficiently large a, this gives a contradiction. □

Remark. The end of the proof of Theorem 6.5 is desgined to hold also in the cases in which $\Delta_K \in \{-3, -4\}$, where we have less precise information on the isogeny graphs. If we assume that $\Delta = \mathfrak{f}^2\Delta_K$ is an imaginary quadratic order with $\Delta_K < -4$, arguments similar to the proof of Kwon's Theorem show that if L is the largest non-negative integer such that F contains a subfield isomorphic to $\mathbb{Q}(j_{\ell^{2L}\Delta_K})$ then there is no F-rational cyclic ℓ^{2L+2}-isogeny $\varphi : E \to E'$ with E a Δ-CM elliptic curve.

The proof of Theorem 6.5 shows that if F contains no Hilbert class field of an imaginary quadratic field and only finitely many rational ring class fields, the set of positive integers N such that $X_0(N)$ has an F-rational CM point is not only finite but explicitly bounded in terms of the finite set of discriminants Δ such that F contains a rational ring class field of discriminant Δ. (This was clear in more generality when $\Delta_K < -4$, but the proof addresses the cases $\Delta_K \in \{-3, -4\}$ as well.) As mentioned in §2.5, we have that $h_\Delta = [\mathbb{Q}(j_\Delta) : \mathbb{Q}]$ approaches infinity with $|\Delta|$, so not only does every number field F contain finitely many rational ring class fields, but the set of discriminants of such fields can be bounded in terms of $[F : \mathbb{Q}]$ alone. Moreover, no number field of odd degree contains any imaginary quadratic field, let alone its Hilbert class field. Accordingly, we deduce the following result.

Corollary 6.6. a) *For a number field F, the following are equivalent:*
   (i) *The set of $N \in \mathbb{Z}^+$ such that $X_0(N)$ has an F-rational CM point is infinite.*
   (ii) *The field F contains the Hilbert class field of an imaginary quadratic field.*

b) *Fix $d \in \mathbb{Z}^+$. As we vary over all degree d number fields F that contain no Hilbert class field of an imaginary quadratic field, there are only finitely many positive integers N such that $X_0(N)$ has an F-rational CM point.*

c) *For each odd $d \in \mathbb{Z}^+$, there are only finitely many $N \in \mathbb{Z}^+$ such that $X_0(N)$ has a closed CM point of degree d.*

We end this section with a brief comparison to the non-CM case. A preliminary result:

Lemma 6.7. a) *Let F be a number field. Suppose that for all sufficiently large prime numbers ℓ, all the noncuspidal F-rational points on $X_0(\ell)$ are CM points. Then the set of $N \in \mathbb{Z}^+$ such that $X_0(N)$ has a noncuspidal, non-CM F-rational point is finite.*

b) *Let $d \in \mathbb{Z}^+$. Suppose that for all sufficiently large prime numbers ℓ, all the noncuspidal degree d closed points on $X_0(\ell)$ are CM points. Then the set of $N \in \mathbb{Z}^+$ such that $X_0(N)$ has a noncuspidal, non-CM closed point of degree d is finite.*

Proof. a) By the assumption and the discussion at the beginning of §3.5, it suffices to show that for each fixed prime ℓ, there is $A = A(\ell)$ such that no non-CM elliptic curve $E_{/F}$ admits an F-rational cyclic ℓ^A-isogeny. By a result of K. Arai [Ar08], there is $L = L(\ell, F)$ such that for every non-CM elliptic curve $E_{/F}$, the image of the ℓ-adic Galois representation $\rho_{E,\ell^\infty} : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ contains the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^L\mathbb{Z})$. Thus E admits no F-rational cyclic ℓ^{L+1}-isogeny.
b) In fact, under the hypotheses of Arai's Theorem, there is such an L that depends only on ℓ and $[F : \mathbb{Q}]$ [CP18, Thm. 2.3a)], and the result follows. This generalization of Arai's Theorem is essentially due to Cadoret and Tamagawa [CT12] and a simpler proof had earlier been sketched by J. Rouse: cf. [CP18, Rem. 2.4]. □

Corollary 6.8. *Assume the Generalized Riemann Hypothesis (GRH), and let F be a number field containing no Hilbert class field of an imaginary quadratic field. Then the set of $N \in \mathbb{Z}^+$ such that $X_0(N)(F)$ has noncupidal points is finite.*

Proof. By [LV14, Cor. 6.5], there are only finitely many prime numbers ℓ such that there is an elliptic curve $E_{/F}$ that admits an F-rational ℓ-isogeny. The result follows from this, Lemma 6.7 and Corollary 6.6a). □

Larson-Vaintrob actually show that over any number field F, conditionally on GRH, for all sufficiently large primes ℓ, if there is an F-rational ℓ-isogeny of elliptic curves with isogeny character $\chi : \mathfrak{g}_F \to (\mathbb{Z}/\ell\mathbb{Z})^\times$, there is an F-rational ℓ-isogeny of K-CM elliptic curves with isogeny character $\psi : \mathfrak{g}_F \to (\mathbb{Z}/\ell\mathbb{Z})^\times$ such that F contains K (and hence also $K(1)$) and $\chi^{12} = \psi^{12}$. Since isogenies of CM elliptic curves are now well understood, in Corollary 6.8 it would be very desirable to remove the hypothesis that F contains no Hilbert class field of an imaginary quadratic field and limit the conclusion to the the non-CM case. Using Theorem **??** and $\chi^{12} = \psi^{12}$, one can get an upper bound on the index of the image of χ. This is useful for certain applications to the torsion subgroup – cf. [CMP18, Thm. 1.8]. It is unfortunately not so clear how to use it to further study isogenies in the non-CM case.

6.5. **The Projective Torsion Field.** Let F be a subfield of $\mathbb{C}$, let $N \geq 2$, let $E_{/F}$ be an elliptic curve, and let

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

be its modulo N Galois representation. The center of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ consists of the subgroup of scalar matrices, isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$, and we define the **projective modulo N Galois representation**

$$\mathbb{P}\rho_N : \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/(\mathbb{Z}/N\mathbb{Z})^\times$$

to be the composite of ρ_N with the quotient map $q : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/(\mathbb{Z}/N\mathbb{Z})^\times$. One can view this as the action of $\mathfrak{g}_F$ on the lines (i.e., one-dimensional free $\mathbb{Z}/N\mathbb{Z}$-submodules) in $E[N](\overline{F})$. The **projective N-torsion field of E** $F(\mathbb{P}E[N])$ is the fixed field $\overline{F}^{\mathrm{Ker}\,\mathbb{P}\rho_N}$. It is a finite Galois extension of F, the unique minimal field extension of F over which Galois acts on $E[N]$ by scalar matrices. The latter interpretation implies that the projective torsion field is also the compositum of all fields of moduli $F(\varphi)$ where $\varphi : E \to E'$ is a cyclic N-isogeny.

Passing from $E_{/F}$ to a quadratic twist $E^D_{/F}$ does not change the projective Galois representation hence also does not change the projective torsion field. This need not be the case for quartic twists when $j = 1728$ or sextic twists when $j = 0$, so from now until the end of this section we assume that $j(E) \notin \{0, 1728\}$. In this case the projective Galois representation depends only on the closed point $j(E) \in X(1)_{/F}$. Determining the projective torsion field when $F = \mathbb{Q}(j(E))$ amounts to computing the fiber over $j(E)$ in the Galois covering of F-curves $X_0(N, N) \to X(1)$: if $f = [F(\mathbb{P}E[N]) : F]$ then when $N \geq 3$, the fiber over $j(E)$ consists of $\frac{\#\,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}{f\,\frac{\varphi(N)}{2}}$ closed points, each with residue field $F(\mathbb{P}E[N])$.

We would like to compute the projective torsion field in the CM case: again, for now we suppose that $\Delta < -4$. Thus we choose an elliptic curve $E_{/\mathbb{Q}(\mathfrak{f})}$ with $j(E) = j_\Delta$, and for all $N \geq 2$ we wish to determine $\mathbb{Q}(\mathfrak{f})(\mathbb{P}E[N])$. The determination of the compositum of this field with K is a result of Parish.

Theorem 6.9 (Parish)**.** *Let $\Delta < -4$. Then for all $N \geq 2$, the projective torsion field of any Δ-CM elliptic curve $E_{/K(\mathfrak{f})}$ is the ring class field $K(N\mathfrak{f})$.*

As an application of the present techniques, we will prove the following result.

Theorem 6.10. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant with $\Delta_K < -4$. Let $N \geq 2$, let F be a number field isomorphic to $\mathbb{Q}(\mathfrak{f})$, and let $E_{/F}$ be a Δ-CM elliptic curve (so $F = \mathbb{Q}(j(E))$). We put*

$$P(\Delta, N) \coloneqq F(\mathbb{P}E[N]).$$

Then:

a) *If $N = 2$ and Δ is even, then $P(\Delta, 2) \cong \mathbb{Q}(2\mathfrak{f})$.*
b) *In all other cases we have $P(\Delta, N) = K(N\mathfrak{f})$.*

Proof. Step 1: By Theorem 6.9 – or by the material of §7.1 – we have $P(\Delta, N) \subset K(N\mathfrak{f})$. On the other hand, there is a cyclic N-isogeny $\varphi : E \to \tilde{E}$ defined over $\mathbb{C}$ such that $\tilde{E}$ is a complex $N^2\Delta$-CM elliptic curve, so $P(\Delta, N)$ contains a subfield isomorphic to $\mathbb{Q}(N\mathfrak{f})$. Thus what we must show is that $P(\Delta, N)$ does not contain K iff $N = 2$ and Δ is even.

Because $\mathrm{Aut}(\mathbb{C})$ acts transitively on the vertices at each level of the isogeny volcano, we may assume without loss of generality that the curve $\tilde{E}$ above has j-invariant $j_{N^2\Delta}$ and thus that E has j-invariant j_Δ, so $F = \mathbb{Q}(\mathfrak{f})$. Having assumed this we have $P(\Delta, N) \supset \mathbb{Q}(N\mathfrak{f})$ and equality occurs iff every cyclic N-isogeny $\varphi : E \to E'$ can be defined over $\mathbb{Q}(N\mathfrak{f})$. This holds iff for all $M \mid N$ every cyclic M-isogeny $\varphi : E \to E'$ can be defined over $\mathbb{Q}(N\mathfrak{f})$. If $N > 2$, then N is divisible either by an odd prime ℓ or by 4. Moreover, if $M = \ell^a$ is any prime power, then every cyclic ℓ^a-isogeny with source E can be defined over $\mathbb{Q}(\ell^a\mathfrak{f})$ iff every length a nonbacktracking path in the isogeny volcano that starts at j_Δ is real.
Step 2: Suppose that ℓ is an odd prime. We claim that there is always a non-real edge in the ℓ-volcano emanating from j_Δ. This follows almost immediately from Lemmas 5.5 and 5.6. If $\left(\frac{\Delta_K}{\ell}\right) = 1$ and $L = \mathrm{ord}_\ell(\mathfrak{f}) = 0$, then there is a nonreal pair of horizontal edges emanating from j_Δ, while in every other case there is a nonreal descendant vertex.
Step 3: Suppose that $\ell^a = 4$. In this case, it follows from Lemmas 5.7, 5.9, 5.10 and 5.11 that there is always a nonreal path of length 2 emanating from j_Δ in the 2-volcano.
Step 4: Suppose $N = 2$ and Δ is odd. Then $L = 0$. If $\left(\frac{\Delta}{2}\right) = 1$, then j_Δ is a split surface vertex, so once again there is a nonreal pair of edges emanating from it. If $\left(\frac{\Delta}{2}\right) = -1$ then by Lemma 5.7a) the vertex j_Δ has a pair of nonreal descendants.
Step 5: Suppose $N = 2$ and Δ is even. In this case, Lemmas 5.9, 5.10 and 5.11 show that all the 2-isogenies emanating from j_Δ are rational over $\mathbb{Q}(2\Delta)$. □

Clearly Theorem 6.10 strengthens Theorem 6.9 in the case where $\Delta_K < -4$. It also strengthens [BCS17, Lemma 3.15] in this case, as that result asserts that for a Δ-CM elliptic curve E defined over a number field F and $N \geq 2$, we have $F(E[N]) \supset K$ if $N \geq 3$ or ($N = 2$ and Δ is odd). Thus not only does the N-torsion field contain K (except when $N = 2$ and Δ is odd), already the projective N-torsion field contains K. When $N = 2$, the N-torsion field and the projective N-torsion field coincide and Theorem 6.10 was already known: indeed, by [BC20b, Lemma 8.4] for all $\Delta \neq -4$ we have $\mathbb{Q}(j(E))(E[2]) = \mathbb{Q}(2\mathfrak{f})$. As recorded in [BCS17, Remark 4.4], the elliptic curve $y^2 = x^3 - x$ shows that $\Delta = -4$ is indeed an exception to this statement.

Remark. Theorem 6.10 ought to hold for all Δ-CM curves with $\Delta < -4$.

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

Let ℓ be a prime number, and let $\Delta = \ell^{2A}\mathfrak{f}_0^2\Delta_K$ be an imaginary quadratic discriminant such that $\mathfrak{f}_0^2\Delta_K < -4$. In this section we will compute the fiber of $X_0(\ell^a) \to X(1)$ over J_Δ: there is no ramification, so we determine which residue fields occur and with what multiplicity. 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.

As described above, without loss of generality we may take our source elliptic curve to have j-invariant j_Δ and then our task is 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 $\mathcal{C}(P)$ as in §5.2 and record the field of moduli for each equivalence class (again, here we record any number field isomorphic to $\mathbb{Q}(f)$ as $\mathbb{Q}(f)$).
(iii) Record the number of closed point equivalence classes that give rise to each field of moduli.

One check on the accuracy of the calculation 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

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

Since the map $X_0(\ell^a) \to X(1)$ is unramified over J_Δ, we must have

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

where the sum extends over closed point equivalence classes.

As above, we split the path into the concatentation $P_1 \cup P_2$, where P_1 is the maximal initial segment of P that terminates at a vertex of level K and P_2 is the remainder of the path, which consists of $\max(L' - L, 0)$ descending edges. Let a_1 be the length of P_1 and a_2 be the length of P_2.

7.1. **Path type analysis I.** We consider paths of length a in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ beginning at j_Δ of level $L \geq 0$. Every such path consists of $b \geq 0$ ascending edges followed by $h \geq 0$ horizontal edges followed by $d \geq 0$ descending edges. For each L, value of $\left(\frac{\Delta_K}{\ell}\right)$ and value of $\mathrm{ord}_2(\Delta_K)$ when $\ell = 2$, we list all possible triples (b,h,d) that occur and for each triple, list the number of closed point equivalence classes and their residue fields.

For some of the types the classification differs when $\ell = 2$. We begin in this section with the portion of the analysis that holds for all primes ℓ.

I. There is always a unique closed point equivalence class $[P_\downarrow]$ of paths $(b,h,d) = (0,0,a)$ – i.e., consisting of a descending edges. The residue field of this path is $\mathbb{Q}(\ell^a\mathfrak{f})$.
II. If $a \leq L$ then there is a unique path $P_\uparrow$ with $(b,h,d) = (a,0,0)$ – i.e., consisting of a ascending edges. The residue field of this path is $\mathbb{Q}(\mathfrak{f})$.
III. In the case $L = 0$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$ there are paths with $(b,h,d) = (0,1,a-1)$. Such paths form one closed point equivalence class, with residue field $\mathbb{Q}(\ell^{a-1}\mathfrak{f})$.
IV. In the case $L = 0$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, for each $1 \leq h \leq a$ there is one complex conjugate pair of paths with $(b,h,d) = (0,h,a-h)$ and residue field $K(\ell^{a-h}\mathfrak{f})$.

X. If $L \geq 1$ and $a - L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, there is one closed point equivalence class of paths with $(b, h, d) = (L, a - L, 0)$ and residue field $K(\mathfrak{f})$.

7.2. Path type analysis II: $\ell > 2$.

V. If $L \geq 2$, for all $1 \leq b \leq \min(a - 1, L - 1)$, there are paths with $(b, h, d) = (b, 0, a - b)$. They fall into $\frac{\ell-1}{2}\ell^{\min(b,a-b)-1}$ closed point equivalence classes, each with residue field $K(\ell^{\max(a-2b,0)}\mathfrak{f})$.
VI. If $a > L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = -1$ there are paths with $(b, h, d) = (L, 0, a - L)$. There is one closed point equivalence class of paths with residue field $\mathbb{Q}(\ell^{\max(a-2L,0)}\mathfrak{f})$. There are $\frac{\ell^{\min(L,a-L)}-1}{2}$ closed point equivalence classes of paths with residue field $K(\ell^{\max(a-2L,0)}\mathfrak{f})$.
VII. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$, there are paths with $(b, h, d) = (L, 0, a-L)$. There are $\frac{\ell-1}{2}\ell^{\min(L,a-L)-1}$ closed point equivalence classes, each with residue field $K(\ell^{\max(a-2L,0)}\mathfrak{f})$.
VIII. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$, there are paths with $(b, h, d) = (L, 1, a-L-1)$. One of them is real and has residue field $\mathbb{Q}(\ell^{\max(a-2L-1,0)}\mathfrak{f})$. There are $\frac{\ell^{\min(L,a-L-1)}-1}{2}$ closed point equivalence classes of paths with residue field $K(\ell^{\max(a-2L-1,0)}\mathfrak{f})$.[8]
IX. If $a \geq L + 1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, there are paths with $(b, h, d) = (L, 0, a - L)$. There is one closed point equivalence class of such paths with residue field $\mathbb{Q}(\ell^{\max(a-2L,0)}\mathfrak{f})$. There are $\frac{(\ell-2)\ell^{\min(L,a-L)-1}-1}{2}$ closed point equivalence classes[9] of such paths with residue field $K(\ell^{\max(a-2L,0)}\mathfrak{f})$.
XI. If $L \geq 1$, $a - L \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, then for all $1 \leq h \leq a - L - 1$ there are $(\ell - 1)\ell^{\min(L,a-L-h)-1}$ closed point equivalence classes of paths with $(b, h, d) = (L, h, a - L - h)$ and residue field $K(\ell^{\max(a-2L-h,0)}\mathfrak{f})$.

7.3. Path type analysis III: $\ell = 2$, $\left(\frac{\Delta_K}{2}\right) \neq 0$.

In this case, **Type V.** consists of paths that ascend but not all the way to the surface and then descend at least once. There are several cases.

V_1. If $L \geq 2$, then for all $a \geq 2$ there is one closed point equivalence class of paths with $(b, h, d) = (1, 0, a - 1)$. The residue field is $\mathbb{Q}(2^{a-2}\mathfrak{f})$.
V_2. If $L \geq a \geq 3$, there is one closed point equivalence class of paths with $(b, h, d) = (a - 1, 0, 1)$. The residue field is $\mathbb{Q}(\mathfrak{f})$.
V_3. If $a > L \geq 3$, there are paths with $(b, h, d) = (L - 1, 0, a - L + 1)$. There are two closed point equivalence classes of such paths with residue field $\mathbb{Q}(2^{\max(a-2L+2,0)}\mathfrak{f})$ and $2^{\min(a-L+1,L-1)-2} - 1$ closed point equivalence classes of such paths with residue field

[8] Thus there are no such classes iff $a = L + 1$.
[9] Thus when $\ell = 3$ and $\min(L, a - L) = 1$ there are no paths of this kind; otherwise there are.

$K(2^{\max(a-2L+2,0)}\mathfrak{f})$.
V_4. If $2 \le b \le \min(L-2, a-2)$, there are paths with $(b,h,d) = (b,0,a-b)$. There are $2^{\min(b,a-b)-2}$ closed point equivalence classes of such paths with residue field $K(2^{\max(a-2b,0)}\mathfrak{f})$.
VI. If $a > L \ge 1$ and $\left(\frac{\Delta_K}{2}\right) = -1$, there are paths with $(b,h,d) = (L,0,a-L)$. There are $2^{\min(L,a-L)-1}$ closed point equivalence classes of such paths with residue field $K(2^{\max(a-2L,0)}\mathfrak{f})$.
(We omit IX. because when $\ell = 2$ and $\left(\frac{\Delta_K}{2}\right) = 1$ there are no paths that ascend to the surface and then descend back down immediately.)
XI. If $a - L \ge 2$ and $\left(\frac{\Delta_K}{2}\right) = 1$, then for all $1 \le h \le a-L-1$ there are paths with $(b,h,d) = (L,h,a-L-h)$. There are $2^{\min(L,a-L-h)-1}$ such paths with residue field $K(2^{\max(a-2L-h,0)}\mathfrak{f})$.

7.4. **Path type analysis IV:** $\ell = 2$, $\mathrm{ord}_2(\Delta_K) = 2$.

In this case, **Type V.** consists of paths that ascend but not all the way to the surface and then descend at least once.
V_1. If $L \ge 2$, then for all $a \ge 2$ there is one closed point equivalence class of paths with $(b,h,d) = (1,0,a-1)$. The residue field is $\mathbb{Q}(2^{a-2}\mathfrak{f})$.
V_2. If $L \ge a \ge 3$, there is one closed point equivalence class of paths with $(b,h,d) = (a-1,0,1)$. The residue field is $\mathbb{Q}(\mathfrak{f})$.
V_3. If $2 \le b \le \min(L-1, a-2)$, there are paths with $(b,h,d) = (b,0,a-b)$. They fall into $2^{\min(b,a-b)-2}$ closed point equivalence classes, each with residue field $K(2^{\max(a-2b,0)}\mathfrak{f})$.

In this case, **Type VI.** consists of paths that ascend to the surface and then immediately descend at least once: $(b,h,d) = (L,0,a-L)$.
VI_1. If $L = 1$, then there is one closed point equivalence class of such paths, with residue field $\mathbb{Q}(2^{a-2}\mathfrak{f})$.
VI_2. If $a = L+1 \ge 3$, there is one closed point of equivalence classes of such paths, with residue field $\mathbb{Q}(\mathfrak{f})$.
VI_3. If $a \ge L+2 \ge 4$, then there are two closed point equivalence classes of such paths with residue field $\mathbb{Q}(2^{\max(a-2L,0)}\mathfrak{f})$ and $2^{\min(L,a-L)-2} - 1$ closed point equivalence classes of such paths with residue field $K(2^{\max(a-2L,0)}\mathfrak{f})$.[10]

In this case, **Type VIII.** consists of paths that ascend to the surface, then take the unique surface edge. The remaining portion of such a path, if any, must be a descent. Thus we have $a \ge L+1 \ge 2$ and $(b,h,d) = (L,1,a-L-1)$.
$VIII_1$. If $a = L+1$, there is one closed point equivalence class of such paths, with residue field $\mathbb{Q}(\mathfrak{f})$.

[10]This means that there are no paths of the latter type iff $a = L+2$.

VIII$_2$. If $a \geq L+2$, there are $2^{\min(L,a-1-L)-1}$ closed point equivalence classes of such paths, each with residue field $K(2^{\max(a-2L-1,0)}\mathfrak{f})$.

7.5. **Path type analysis V: $\ell = 2$, $\mathrm{ord}_2(\Delta_K) = 3$.** In this case the isogeny graph has the same structure as in the previous section, but with a different action of complex conjugation. Thus the classification of paths is the same as before, but with sometimes different results on which of them are real.

As above **Type V.** consists of paths ascending but not to the surface and then descend at least once: we need $L \geq 2$.
V$_1$. If $L \geq 2$, then for all $a \geq 2$ there is one closed point equivalence class of paths with $(b,h,d) = (1,0,a-1)$. The residue field is $\mathbb{Q}(2^{a-2}\mathfrak{f})$.
V$_2$. If $L \geq a \geq 3$, there is one closed point equivalence class of paths with $(b,h,d) = (a-1,0,1)$. The residue field is $\mathbb{Q}(\mathfrak{f})$.
V$_3$. If $2 \leq b \leq \min(L-1, a-2)$, there are paths with $(b,h,d) = (b,0,a-b)$. They fall into $2^{\min(b,a-b)-2}$ closed point equivalence classes, each with residue field $K(2^{\max(a-2b,0)}\mathfrak{f})$.

As above **Type VI.** consists of paths that ascend to the surface and then immediately descend at least once: $(b,h,d) = (L,0,a-L)$.
VI$_1$. If $L = 1$, then there is one closed point equivalence class of such paths, with residue field $\mathbb{Q}(2^{a-2}\mathfrak{f})$.
VI$_2$. If $a = L+1 \geq 3$, there is one closed point of equivalence classes of such paths, with residue field $\mathbb{Q}(\mathfrak{f})$.
VI$_3$. If $a \geq L+2 \geq 4$, then there are $2^{\min(L,a-L)-2}$ closed point equivalence classes of such paths, with residue field $K(2^{\max(a-2L,0)}\mathfrak{f})$.

Type VIII. as above consists of paths that ascend to the surface, then take the unique surface edge. The remaining portion of such a path, if any, must be a descent. Thus we have $a \geq L+1 \geq 2$ and $(b,h,d) = (L,1,a-L-1)$.
VIII$_1$. If $a = L+1$, there is one closed point equivalence class of such paths, with residue field $\mathbb{Q}(\mathfrak{f})$.
VIII$_2$. If $a \geq L+2$, there are 2 closed point equivalence classes of such paths with residue field $\mathbb{Q}(2^{\max(a-2L-1,0)}\mathfrak{f})$ and $2^{\min(L,a-1-L)-1} - 1$ closed point equivalence classes of such classes with residue field $K(2^{\max(a-2L-1,0)}\mathfrak{f})$.

8. Closed CM points on $X_0(\ell^{a'}, \ell^a)_{/\mathbb{Q}}$

Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant with $\Delta_K < -4$. Let $1 \leq a' \leq a$ be positive integers. In this section we compute primitive residue fields of Δ-CM points on the modular curve $X_0(\ell^{a'}, \ell^a)_{/\mathbb{Q}}$. Every closed Δ-CM point $\tilde{P} \in X_0(\ell^{a'}, \ell^a)_{/\mathbb{Q}}$ is induced by a Δ-CM elliptic curve $E_{/\mathbb{Q}(\tilde{P})}$ that admits a $\mathbb{Q}(\tilde{P})$-rational cyclic ℓ^a-isogeny and also has Galois acting on $E[\ell^{a'}]$ by scalar matrices, and such an elliptic curve is well-defined up to

quadratic twist. Let

$$\pi : X_0(\ell^{a'}, \ell^a) \to X_0(\ell^a)$$

be the natural map, a $\mathbb{Q}$-morphism of degree $(\ell - 1)\ell^{2a'-1}$, and let $P \coloneqq \pi(\tilde{P})$. Thus we have

$$\mathbb{Q}(\tilde{P}) = \mathbb{Q}(P)(\mathbb{P}E[\ell^{a'}]).$$

By adjusting $E_{/\mathbb{Q}(\tilde{P})}$ by a quadratic twist, we may assume that E arises by base change from an elliptic curve defined over $\mathbb{Q}(j(E))$.

8.1. $\ell^{a'} > 2$ **or** Δ **is odd.** Suppose that either $\ell^{a'} > 2$ or Δ is odd. Then Theorem 6.10 shows that

$$\mathbb{Q}(\tilde{P}) = \mathbb{Q}(P)K(\ell^{a'}\mathfrak{f}).$$

First of all, because $\mathbb{Q}(P)$ is either a rational ring class field or a ring class field and a compositum of a rational ring class field and a ring class field is a ring class field, it follows that $\mathbb{Q}(\tilde{P})$ is a ring class field $K(M\mathfrak{f})$ with (by Theorem 6.10) some positive integer $M \mid \ell^a$.

Next, as we will see in the following section, there is either one primitive residue field of a closed CM-point on $X_0(\ell^a)_{/\mathbb{Q}}$, necessarily isomorphic to $\mathbb{Q}(B\mathfrak{f})$ – in which case the only primitive residue field of a closed CM-point on $X_0(\ell^{a'}, \ell^a)_{/\mathbb{Q}}$ is $K(\mathrm{lcm}(\ell^{a'}, B)\mathfrak{f})$ – or two primitive residue fields of closed CM-points on $X_0(\ell^a)_{/\mathbb{Q}}$, necessarily isomorphic to $\mathbb{Q}(B\mathfrak{f})$ and $K(C\mathfrak{f})$ with $C \mid B$ – in which case the only primitive residue field of a closed CM-point on $X_0(\ell^{a'}, \ell^a)_{/\mathbb{Q}}$ is $K(\mathrm{lcm}(\ell^{a'}, C)\mathfrak{f})$.

8.2. $\ell^{a'} = 2$ **and** Δ **is even.** Suppose that $\ell^{a'} > 2$ or Δ is even. By Theorem 6.10, the field $\mathbb{Q}(\tilde{P})$ is the compositum of $\mathbb{Q}(P)$ and a field isomorphic to $\mathbb{Q}(2\mathfrak{f})$. Since $\mathbb{Q}(P)$ is either a rational ring class field or a ring class field, it follows that $\mathbb{Q}(\tilde{P})$ is either a rational ring class field isomorphic to $\mathbb{Q}(M\mathfrak{f})$ with $M \mid N$ or is a ring class field $K(M\mathfrak{f})$ with $M \mid N$.

Next we will determine all primitive residue fields of closed Δ-CM points $\tilde{P}$ on $X_0(2, 2^a)_{/\mathbb{Q}}$. As above it follows from Theorem 6.10 that $\mathbb{Q}(\tilde{P})$ contains a number field isomorphic to $\mathbb{Q}(2\mathfrak{f})$. As usual we put $L = \mathrm{ord}_\ell(\mathfrak{f})$. Since $2 \mid \Delta = \mathfrak{f}^2\Delta_K$, when $L = 0$ we have that $\left(\frac{\Delta_K}{2}\right) = 0$. In what follows it is no loss of generality to restrict to Δ-CM closed points $\tilde{P} \in X_0(2, 2^a)$ for which $j(\tilde{P}) = j_\Delta$, and we shall do so.

Case 1: Suppose $L = 0$ and $\mathrm{ord}_2(\Delta_K) = 2$. We refer to Figure XX.. Since $j(\tilde{P}) = j_\Delta$, we have $\mathbb{Q}(j(E), E[2]) = \mathbb{Q}(v_1, v_2, v_3, v_4) = \mathbb{Q}(2\mathfrak{f})$. The unique primitive residue field of a closed point on $X_0(2^a)$ with j-invariant j_Δ is a number field isomorphic but not equal to $\mathbb{Q}(2^{a-1}\mathfrak{f})$, coming from the path that consists of one horizontal edge followed by $a - 1$ downward edges. For the (unique, up to quadratic twist) elliptic curve $E_{/\mathbb{Q}(P)}$, we have that $\mathbb{Q}(P)(E[2]) = \mathbb{Q}(P, v_3, v_4) = K(2^{a-1}\mathfrak{f})$, because $j(v_3)$ and $j(v_5)$ are not coreal. There is also a Δ-CM point P on $X_0(2^a)_{/\mathbb{Q}}$ with $j(E) = v_1$ and $\mathbb{Q}(P) = \mathbb{Q}(2^a\mathfrak{f})$, with the path consisting of a downward edges. Since the isogeny $v_1 \to v_2$ is rational over $\mathbb{Q}(P_1) \subset \mathbb{Q}(P)$,

this point lifts to a point (more precisely, splits into two points) $\tilde{P}$ on $X_0(2,2^a)_{/\mathbb{Q}}$ with $\mathbb{Q}(\tilde{P}) = \mathbb{Q}(2^a\mathfrak{f})$.

In this case there are precisely two Δ-CM closed points on $X_0(2^a)$ with j-invariant j_Δ and we analyzed the lifts of both of them to $X_0(2,2^a)_{/Q}$, so in this case $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-1}\mathfrak{f})$ are not only the only primitive residue fields of Δ-CM closed points on $X_0(2,2^a)_{/\mathbb{Q}}$: they are, up to isomorphism, the only such residue fields.

Case 2: Suppose $L = 0$ and $\mathrm{ord}_2(\Delta_K) = 3$. The unique primitive residue field of a Δ-CM closed point P on $X_0(2^a)$ is $\mathbb{Q}(2^{a-1}\mathfrak{f})$. We refer to Figure XX. For any lift of P to $\tilde{P} \in X_0(2,2^a)$ we have $\mathbb{Q}(\tilde{P}) = \mathbb{Q}(P, v_3, v_4) = \mathbb{Q}(P) = \mathbb{Q}(2^{a-1}\mathfrak{f})$ since v_3 and v_4 are coreal. This is clearly the only primitive residue field of a Δ-CM point on $X_0(2,2^a)_{/\mathbb{Q}}$.

Case 3: Suppose $\left(\frac{\Delta_K}{2}\right) = 1$ and $L = 1$. The primitive residue fields of Δ-CM closed points P_1, P_2 on $X_0(2^a)$ are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(\mathfrak{f})$. The path corresponding to P_1 consists of a downward edges, so the unique upward edge gives an additional 2-isogeny that is still defined over $\mathbb{Q}(P_1)$, so the residue fields of the (two) lifts of P_1 to $X_0(2,2^a)$ are $\mathbb{Q}(P_1) = \mathbb{Q}(2^a\mathfrak{f})$. The path corresponding to P_2 consists of an upward edge followed by $a-1$ horizontal edges. For a lift $\tilde{P_2}$ of P_2 to $X_0(2,2^a)_{/Q}$, the residue field $\mathbb{Q}(\tilde{P_2})$ contains $K(\mathfrak{f})$, a number field isomorphic to $\mathbb{Q}(\mathfrak{f})$ and satisfies $[\mathbb{Q}(\tilde{P_2}) : \mathbb{Q}(P_2] \leq 2$, so $\mathbb{Q}(\tilde{P_2}) \cong K(2\mathfrak{f})$. These yield all primitive residue fields.

Case 4: Suppose $\left(\frac{\Delta_K}{2}\right) = 1$, $L \geq 2$ and $a \leq 2L-2$. The unique primitive residue field of a Δ-CM closed point on $X_0(2^a)_{/\mathbb{Q}}$ is isomorphic to $\mathbb{Q}(\mathfrak{f})$, so the unique primitive residue field of Δ-CM closed point on $X_0(2,2^a)_{/\mathbb{Q}}$ is isomorphic to $\mathbb{Q}(2\mathfrak{f})$.

Case 5: Suppose $\left(\frac{\Delta_K}{2}\right) = 1$, $L \geq 2$ and $a \geq 2L-1$. The primitive residue fields of Δ-CM closed points P_1, P_2 on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(\mathfrak{f})$. The point P_1 corresponds to a path that ascends to level 1 and then descends to level $a-2L+2 > L$. The structure of complex conjugation on the isogeny volcano shows that the two vertices descending from $j(E)$ are each coreal with the terminal vertex, so P_1 lifts to (two) closed points $\tilde{P_1}$ on $X_0(2,2^a)_{/\mathbb{Q}}$ with residue field $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$. It follows as in Case 3 above that the lift of P_2 to $\tilde{P_2}$ on $X_0(2,2^a)_{/\mathbb{Q}}$ has residue field $K(2\mathfrak{f})$ and that these are all the primitive residue fields.

Case 6: Suppose $\left(\frac{\Delta_K}{2}\right) = -1$, $L = 1$ and $a = 2$. The primitive residue fields of Δ-CM points P_1, P_2 on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^2\mathfrak{f})$ and $K(\mathfrak{f})$. The path corresponding to P_1 is downward of length 2, so an upward edge gives another 2-isogeny rational over $\mathbb{Q}(P_1)$ and thus $\mathbb{Q}(\tilde{P_1}) = \mathbb{Q}(2^2\mathfrak{f})$. As in above cases, we must have $\mathbb{Q}(\tilde{P_2}) = K(2\mathfrak{f})$ and these are the only primitive residue fields.

Case 7: Suppose $\left(\frac{\Delta_K}{2}\right) = -1$, $L = 1$ and $a \geq 3$. The analysis is similar to the above: the primitive residue fields of Δ-CM points $P_1, P_@$ on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-2}\mathfrak{f})$, but since $a \geq 3$, the number field $\mathbb{Q}(2\mathfrak{f})$ can be embedded in $K(2^{a-2}\mathfrak{f})$, so the primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-2}\mathfrak{f})$.

Case 8: Suppose $\left(\frac{\Delta_K}{2}\right) = -1$, $L \geq 2$ and $a \leq 2L-2$. The only primitive residue field of a Δ-CM closed point on $X_0(2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(\mathfrak{f})$, so the only primitive residue field of a Δ-CM closed point on $X_0(2, 2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(2\mathfrak{f})$.

Case 9: Suppose $\left(\frac{\Delta_K}{2}\right) = -1$, $L \geq 2$ and $a \in \{2L-1, 2L\}$. The primitive residue fields of Δ-CM closed points P_1, P_2 on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(\mathfrak{f})$. A Similar argument to the above cases shows that the primitive residue fields of Δ-CM closed points on $X_0(2, 2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2\mathfrak{f})$.

Case 10: Suppose $\left(\frac{\Delta_K}{2}\right) = -1$, $L \geq 2$ and $a \geq 2L+1$. The primitive residue fields of Δ-CM closed points P_1, P_2 on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2^{a-2L}\mathfrak{f})$. A similar argument to the above cases shows that the primitive residue fields of Δ-CM closed points on $X_0(2, 2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2^{a-2L}\mathfrak{f})$.

Case 11: Suppose $\mathrm{ord}_2(\Delta_K) = 2$, $L \geq 1$ and $a \leq 2L$. The only primitive residue field of a Δ-CM closed point on $X_0(2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(\mathfrak{f})$. So the only primitive residue field of a Δ-CM closed point on $X_0(2, 2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(2\mathfrak{f})$.

Case 12: Suppose $\mathrm{ord}_2(\Delta_K) = 2$, $L \geq 1$ and $a = 2L+1$. The primitive residue fields of Δ-CM closed points on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L}\mathfrak{f})$ and $K(\mathfrak{f})$. A similar argument to the above cases shows that the primitive residue fields of Δ-CM closed points on $X_0(2, 2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L}\mathfrak{f})$ and $K(2\mathfrak{f})$.

Case 13: Suppose $\mathrm{ord}_2(\Delta_K) = 2$, $L \geq 1$ and $a \geq 2L+2$. The primitive residue fields of Δ-CM closed points on $X_0(2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L}\mathfrak{f})$ and $K(2^{a-2L-1}\mathfrak{f})$. A similar argument to the above cases shows that the primitive residue fields of Δ-CM closed points on $X_0(2, 2^a)_{/\mathbb{Q}}$ are $\mathbb{Q}(2^{a-2L}\mathfrak{f})$ and $K(2^{a-2L-1}\mathfrak{f})$.

Case 14: Suppose $\mathrm{ord}_2(\Delta_K) = 3$, $L \geq 1$ and $a \leq 2L+1$. The only primitive residue field of a Δ-CM closed point on $X_0(2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(\mathfrak{f})$, so the only primitive residue field of a Δ-CM closed point on $X_0(2, 2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(2\mathfrak{f})$.

Case 15: Suppose $\mathrm{ord}_2(\Delta_K) = 3$, $L \geq 1$ and $a \geq 2L+2$. The only primitive residue field of a Δ-CM closed point on $X_0(2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$. A similar argument to the above

cases shows that the only primitive residue field of a Δ-CM closed point on $X_0(2,2^a)_{/\mathbb{Q}}$ is $\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$.

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

9.1. **Compiling Across Prime Powers.** Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant with $\Delta_K < -4$. For any prime power ℓ^a, the fiber F of $X_0(\ell^a) \to X(1)$ over the closed point J_Δ is a finite étale $\mathbb{Q}(J_\Delta)$-scheme: that is, it is isomorphic to a product of finite degree field extensions of $\mathbb{Q}(\mathfrak{f})$. More precisely, there are non-negative integers $b_0, \ldots, b_a, c_1, \ldots, c_{a-1}$ such that $F \cong \operatorname{Spec} A$, where

$$A \cong \prod_{j=0}^{a} \mathbb{Q}(\ell^j\mathfrak{f})^{b_j} \times \prod_{k=0}^{a-1} K(\ell^k\mathfrak{f})^{c_k}, \tag{7}$$

and the tables in the Appendix give the b_j's and c_k's.

We now explain how the previous results allow us to compute the fiber $F = \operatorname{Spec} A$ of $X_0(N) \to X(1)$ over J_Δ for any positive integer $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For $1 \le i \le r$, let $F_i = \operatorname{Spec} A_i$ be the fiber of $X_0(\ell_i^{a_i}) \to X(1)$ over J_Δ. By Proposition 3.8 we have

$$A \cong A_1 \otimes_{\mathbb{Q}(J_\Delta)} \cdots \otimes_{\mathbb{Q}(J_\Delta)} A_r. \tag{8}$$

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

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

where for $1 \le i \le r$ 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 $0 \le j_i \le a-1$. In the former case, it follows from Corollary 2.11a) that

$$\mathbb{Q}(\ell_1^{j_1}\mathfrak{f}) \otimes_{\mathbb{Q}(\mathfrak{f})} \cdots \otimes \mathbb{Q}(\ell_r^{j_r}\mathfrak{f}) \cong \mathbb{Q}(\ell_1^{j_1} \cdots \ell_r^{j_r}\mathfrak{f}).$$

Suppose now that the number of $1 \le i \le r$ such that B_i contains K is $s \ge 1$. In this case, it follows from parts b) and c) of Corollary 2.11 that

$$B \cong K(\ell_1^{j_1} \cdots \ell_r^{j_r})^s.$$

From this we deduce:

Corollary 9.1. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant with $\Delta_K < -4$. Let $N \in \mathbb{Z}^+$. Let P be a Δ-CM closed point on $X_0(N)$.*

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 $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ be the prime power decomposition of N. For $1 \le i \le r$, let $\pi_i : X_0(N) \to X_0(\ell_i^{a_i})$ be the natural map and put $P_i := \pi_i(P)$. 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.*

9.2. **Primitive Residue Fields.** Fix $\Delta = \mathfrak{f}^2\Delta_K$ with $\Delta_K < -4$ and $N \in \mathbb{Z}^+$. We say that a residue field F of a closed Δ-CM point on $X_0(N)$ is **primitive** if there is no other residue field L of a closed Δ-CM point on $X_0(N)$ such that L embeds as a proper subfield of F. There is always a closed Δ-CM point with residue field isomorphic to $\mathbb{Q}(N\mathfrak{f})$, and from this it follows that there is exactly one $B \mid N$ for which there is a primitive residue field isomorphic to $\mathbb{Q}(B\mathfrak{f})$: this residue field is obtained by taking, for each $1 \leq i \leq r$, the natural number 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 some Δ-CM point on $X_0(\ell_i^{a_i})$; then we have

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

There is at most one other primitive residue field of a Δ-CM point on $X_0(N)$, necessarily of the form $K(C\mathfrak{f})$ for some $C \mid N$: this additional primitive field occurs iff there are two primitive residue fields for Δ-CM points on $X_0(\ell_i^{a_i})$ for some $1 \leq i \leq r$, in which case for $1 \leq i \leq r$ we let c_i be the least natural number C_i for which there is a Δ-CM point on $X_0(\ell_i^{a_i})$ with residue field isomorphic to either $\mathbb{Q}(\ell_i^{C_i}\mathfrak{f})$ or to $K(\ell_i^{C_i}\mathfrak{f})$; then we have

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

For any prime power ℓ^a, we now record the natural numbers b and (if applicable) c referred to above. In all cases the results follow from the more detailed computations of the Appendix but can be more easily shown by direct contemplation of the action of complex conjugation on the isogeny volcano.[11] In what follows when we say "F is a residue field" we mean that "there is a residue field isomorphic to F." Put $L := \mathrm{ord}_\ell(\mathfrak{f})$.

Case 1: Supose $\ell^a = 2$.
Case 1a: Suppose $\left(\frac{\Delta}{2}\right) \neq -1$. If $\left(\frac{\Delta}{2}\right) = 1$, then $\mathbb{Q}(2\mathfrak{f}) = \mathbb{Q}(\mathfrak{f})$ is a residue field, so $\mathbb{Q}(\mathfrak{f})$ is the unique primitive residue field. If $\left(\frac{\Delta}{2}\right) = 0$, then $\mathbb{Q}(\mathfrak{f})$, so $\mathbb{Q}(\mathfrak{f})$ is the unique primitive residue field.
Case 1b: Suppose $\left(\frac{\Delta}{2}\right) = -1$. By §9.1.1 the unique residue field is $\mathbb{Q}(2\mathfrak{f})$.
Case 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 3: Suppose $\ell^a > 2$ and $\left(\frac{\Delta}{\ell}\right) = -1$. The only primitive residue field is $\mathbb{Q}(\ell^a\mathfrak{f})$.
Case 4: Suppose $\ell^a > 2$, $\left(\frac{\Delta}{\ell}\right) = 0$ and $L = 0$. The only primitive residue field is $\mathbb{Q}(\ell^{a-1}\mathfrak{f})$.
Case 5: Suppose $\ell > 2$, $L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$.
Case 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 5b: Suppose $a > 2L$. Then the primitive residue fields are $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$ and $K(\mathfrak{f})$.
Case 6: Suppose $\ell > 2$, $L \geq 1$, and $\left(\frac{\Delta_K}{\ell}\right) = -1$.
Case 6a: Suppose $a \leq 2L$. As in Case 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 6b: Suppose $a > 2L$. In this case the only primitive residue field is $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$.

[11] The main point of the following page is in fact to name the various cases, so that the complete data can be displayed in a single table.

Case 7: Suppose $\ell > 2$, $L \geq 1$, $\left(\frac{\Delta_K}{\ell}\right) = 0$.
Case 7a: Suppose $a \leq 2L+1$. As in Case 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 7b: Suppose $a \geq 2L+2$. In this case the only primitive residue field is $\mathbb{Q}(\ell^{a-2L-1}\mathfrak{f})$.
Case 8: Suppose $\ell = 2$, $L \geq 1$, and $\left(\frac{\Delta_K}{2}\right) = 1$.
Case 8a: Suppose $L = 1$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(\mathfrak{f})$.
Case 8b: Suppose $L \geq 2$ and $a \leq 2L-2$. The only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 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 9: Suppose $\ell = 2$, $L \geq 1$, and $\left(\frac{\Delta_K}{2}\right) = -1$.
Case 9a: Suppose $L = 1$. The primitive residue fields are $\mathbb{Q}(2^a\mathfrak{f})$ and $K(2^{a-2}\mathfrak{f})$.
Case 9b: Suppose $L \geq 2$ and $a \leq 2L-2$. The only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 9c: Suppose $L \geq 2$ and $a \geq 2L-1$. The primitive residue fields are $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$ and $K(2^{\max(a-2L,0)})$.
Case 10: Suppose $\ell = 2$, $L \geq 1$, $\left(\frac{\Delta_K}{2}\right) = 0$, and $\mathrm{ord}_2(\Delta_K) = 2$.
Case 10a: Suppose $a \leq 2L$. The only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 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 11: Suppose $\ell = 2$, $L \geq 1$, $\left(\frac{\Delta_K}{2}\right) = 0$, and $\mathrm{ord}_2(\Delta_K) = 3$.
Case 11a: Suppose $a \leq 2L+1$. The only primitive residue field is $\mathbb{Q}(\mathfrak{f})$.
Case 11b: Suppose $a \geq 2L+2$. The only primitive residue field is $\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$.

Case	b	$d_b = [\mathbb{Q}(\ell^b\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]$	c	$d_c = [K(\ell^c\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})]$	$d_c < d_b$?	$d_c \mid d_b$?
1a)	0	1	-	-	-	-
1b)	1	3	-	-	-	-
2	a	$\ell^{a-1}(\ell-1)$	0	2	$\iff \ell^a > 3$	Y
3	a	$\ell^{a-1}(\ell+1)$	-	-	-	-
4	$a-1$	ℓ^{a-1}	-	-	-	-
5a)	0	1	-	-	-	-
5b)	$a-2L$	ℓ^{a-2L}	0	2	Y	N
6a)	0	1	-	-	-	-
6b)	$a-2L$	ℓ^{a-2L}	-	-	-	-
7a)	0	1	-	-	-	-
7b)	$a-2L-1$	ℓ^{a-2L-1}	-	-	-	-
8a)	a	2^a	0	2	Y	Y
8b)	0	1	-	-	-	-
8c)	$a-2L+2$	2^{a-2L+2}	0	2	$\iff a \geq 2L$	Y
9a)	a	2^a	$a-2$	2^{a-1}	Y	Y
9b)	0	1	-	-	-	-
9c)	$a-2L+2$	2^{a-2L+2}	$a-2L$	2^{a-2L+1}	Y	Y
10a)	0	1	-	-	-	-
10b)	$a-2L$	2^{a-2L}	$a-2L-1$	2^{a-2L}	N	Y
11a)	0	1	-	-	-	-
11b)	$a-2L-1$	2^{a-2L-1}	-	-	-	-

Let us discuss the last two columns of the table. In every case in which there are two primitive residue fields $\mathbb{Q}(\ell^b\mathfrak{f})$ and $K(\ell^c\mathfrak{f})$ for Δ-CM points on $X_0(\ell^a)$, we have that

$$d_c = [K(\ell^c\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})] \leq [\mathbb{Q}(\ell^b\mathfrak{f})] = d_b.$$

Thus when there are two primitive residue fields, the *least* degree of a Δ-CM point on $X_0(\ell^a)$ is always d_c (and, of course, when there is only one primitive residue field, the least degree is d_b). As the table shows, in most of the cases when there are two primitive residue fields, we have $d_c < d_b$: equality occurs precisely in Case 2 when $\ell^a = 3$, in Case 8c) when $L = 2a-1$ and in Case 10b).

We are also interested in whether $d_c \mid d_b$. When this is the case although there are two primitive residue fields, the only **primitive degree** of a Δ-CM point on $X_0(\ell^a)$ is d_c. This is relevant because in many applications we are primarily interested in the degrees of F-valued CM points on modular curves, where F is some number field. For instance, suppose $D \in \mathbb{Z}^+$ and we would like to classify all finite groups that arise up to isomorphism as $E(F)[\mathrm{tors}]$ for some elliptic curve E defined over some degree D number field F. It is equivalent to determine the set of pairs of positive integers $M \mid N$ such that the modular curve $X_1(M,N)_{/\mathbb{Q}}$ has a closed point of degree $d \mid D$: indeed, each F-valued point of $X_1(M,N)_{/\mathbb{Q}}$ induces a closed point P and an embedding $\mathbb{Q}(P) \hookrightarrow F$. Conversely, if P is a closed point on $X_1(M,N)_{/\mathbb{Q}}$ then by Merel's Theorem there are only finitely many pairs of

positive integers $\tilde{M}, \tilde{N}$ with $\tilde{M} \mid \tilde{N}$, $M \mid \tilde{M}$ and $N \mid \tilde{N}$ and a closed point $\tilde{P}$ on $X_1(\tilde{M}, \tilde{N})$ lying over P such that $\mathbb{Q}(\tilde{P}) = \mathbb{Q}(\mathbb{P})$. (In other words we may restrict attention to pairs (M, N) such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is the full torsion subgroup of some elliptic curve $E_{/\mathbb{Q}(P)}$.) If $d \coloneqq [\mathbb{Q}(P) : \mathbb{Q}]$, then for any $D \in \mathbb{Z}^+$ such that $d \mid D$ and $\frac{D}{d} > 1$, by [BCS17, Thm. 2.1] there are infinitely many number fields $F \supset \mathbb{Q}(P)$ such that $[F : \mathbb{Q}] = D$ and there is an elliptic curve $E_{/F}$ with $E(F)[\text{tors}] \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

To solve this problem in the CM case we restrict to the finite set of imaginary quadratic discriminants Δ such that $h_\Delta \mid D$ and for each such Δ, to find all pairs $M \mid N$ for which there is a Δ-CM closed point of primitive degree $d \mid D$.

Let us look back at Case 5b): we have a prime power ℓ^a with $\ell > 2$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $L \geq 1$ and $a > 2L$. In this case we have not just two primitive residue fields of Δ-CM points on $X_0(\ell^a)$ but also two primitive degrees: 2 and ℓ^{a-2L}.

Suppose $M \mid N$ are positive integers and $\Delta < -4$. By Theorem **??** the multiset of degrees of closed Δ-CM points on $X_1(M, N)$ is obtained from the multiset of degrees of closed Δ-CM points on $X_0(M, N)$ by multiplying by $\begin{cases} 1 & N \leq 2 \\ \frac{\varphi(N)}{2} & N \geq 3 \end{cases}$. It follows that there is more than one primitive degree of a Δ-CM closed point on $X_0(M, N)$ iff there is more than one primitive degree of a Δ-CM closed point on $X_1(M, N)$, which by the work of [BC20b] can only happen if $M \leq 2$.

Coming back to the case $M = 1$, $N = \ell^a$ with $\ell > 2$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $L \geq 1$ and $a > 2L$, we find that the primitive degrees of closed Δ-CM points on $X_1(\ell^a)$ are

$$\frac{\varphi(\ell^a)}{2} \cdot \ell^{a-2L} = \frac{\ell^{2a-2L-1}(\ell-1)}{2} \text{ and } \frac{\varphi(\ell^a)}{2} \cdot 2 = \varphi(\ell^a) = \ell^{a-1}(\ell-1).$$

The existence of multiple primitive degrees in this case was previously shown in [BC20b, Example 6.7]. In that work the least degree of a Δ-CM point on $X_1(M, N)$ was determined (for all Δ and $M \mid N$); by [BC20b, Thm. 6.6] the least degree in this case is indeed $d_c = \varphi(\ell^a) = \ell^{a-1}(\ell-1)$. In [BC20b, Example 6.7] the other primitive degree d_b was not determined precisely (nor was it shown there was exactly one other primitive degree), but rather a Galois-theoretic argument was used to show that $\text{ord}_2(d_b) < \text{ord}_2(d_c)$. We see now that $d_b = \frac{\ell^{2a-2L-1}(\ell-1)}{2}$ and thus $\text{ord}_2(d_b) = \text{ord}_2(d_c) - 1$.

Theorem 9.2. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant, and let $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ be the prime power decompostion of a positive integer. 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 $X_0(\ell_i^{a_i})$. Let c_i be equal to b_i if there is a unique primitive residue field of Δ-CM points on $X_0(\ell_i^{a_i})$ and otherwise let it be such that the unique non-real primitive residue field of a closed Δ-CM point on $X_0(\ell_i^{a_i})$ 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 $X_0(\ell_i^{a_i})$.

a) *If $s = 0$, then $\mathbb{Q}(B\mathfrak{f})$ is the unique primitive residue field of a Δ-CM point on $X_0(N)$, so the unique primitive degree of Δ-CM points on $X_0(N)$ 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 $X_0(\ell_i^{a_i})$ and we are not in Case 5b) with respect to Δ and $\ell_i^{a_i}$, then the unique primitive degree of Δ-CM points on $X_0(N)$ 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 $X_0(\ell_i^{a_i})$ we are in Case 5b), then there are two primitive degrees of Δ-CM points on $X_0(N)$: $[\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}]$ and $[K(C\mathfrak{f}) : \mathbb{Q}]$.*

Proof. Step 1: The case $s = 0$ follows from the discussion at the beginning of this section. Henceforth we suppose $s \geq 1$. In this case there are (up to isomorphism) two primitive residue fields of Δ-CM closed points on $X_0(N)$: $\mathbb{Q}(B\mathfrak{f})$ and $K(C\mathfrak{f})$. Put

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

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 $X_0(\ell_i^{a_i})$; if there is any non-real such field, we take F_i to be nonreal. Since 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 $[K(\ell_i^{c_i}\mathfrak{f}) : \mathbb{Q}] \mid [\mathbb{Q}(\ell_i^{b_i}\mathfrak{f}) : \mathbb{Q}]$, it follows that

$$\dim_{\mathbb{Q}(\mathfrak{f})} F_1 \otimes_{\mathbb{Q}(\mathfrak{f})} \otimes \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} F_r \leq \dim_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\ell_1^{b_1}\mathfrak{f}) \otimes_{\mathbb{Q}(\mathfrak{f})} \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} \mathbb{Q}(\ell_r^{b_r}\mathfrak{f}) = [\mathbb{Q}(B\mathfrak{f}) : \mathbb{Q}(\mathfrak{f})].$$

Since also

$$F_1 \otimes_{\mathbb{Q}(\mathfrak{f})} \cdots \otimes_{\mathbb{Q}(\mathfrak{f})} F_r \cong K(C\mathfrak{f})^s, \tag{9}$$

it follows that $\mathbf{c} \leq \mathbf{b}$. Thus there is a unique primitive degree iff $\mathbf{c} \mid \mathbf{b}$.
Step 2: Since $K(C\mathfrak{f}) \subset K(B\mathfrak{f}) = K\mathbb{Q}(B\mathfrak{f})$, 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. Moreover we have

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

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

so in the $s = 1$ case it follows that $\mathbf{c} \mid \mathbf{b}$ iff there is some $1 \leq i \leq r$ such that there are two primitive residue fields of Δ-CM closed points on $X_0(\ell_i^{a_i})$ for which we have

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

which holds iff

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

Consulting the Table above, we see that this holds in every case in which there are two primitive residue fields *except* Case 5b). □

References

[Ar08] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves.* J. Théor. Nombres Bordeaux 20 (2008), 23–43.

[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.

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

[BCS17] A. Bourdon, P.L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields.* Trans. Amer. Math. Soc. 369 (2017), 8457-–8496.

[BP17] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields.* Int. Math. Res. Not. IMRN 2017, no. 16, 4923–4961.

[CA] P.L. Clark, *Commutative Algebra.* `http://math.uga.edu/~pete/integral2015.pdf`

[CCM21] M. Chou, P.L. Clark and M. Milosevic, *Acyclotomy of torsion in the CM case.* To appear in the Ramanujan Journal.

[CCRS14] P.L. Clark, P. Corn, A. Rice and J. Stankewicz, *Computation on elliptic curves with complex multiplication.* LMS J. Comput. Math. 17 (2014), 509–535.

[CGPS] P.L. Clark, T. Genao, P. Pollack and F. Saia, *The least degree of a CM point on a modular curve.* `http://alpha.math.uga.edu/~pete/least_CM_degree-1226.pdf`

[CMP18] P.L. Clark, M. Milosevic, P. Pollack, *Typically bounding torsion.* J. Number Theory 192 (2018), 150–167.

[CCS13] P.L. Clark, B. Cook and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice).* Int. J. Number Theory 9 (2013), 447–479.

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

[CP17] P.L. Clark and P. Pollack, *The truth about torsion in the CM case, II.* Q. J. Math. 68 (2017), 1313–1333.

[CP18] P.L. Clark and P. Pollack, *Pursuing polynomial bounds on torsion.* Israel J. Math. 227 (2018), 889–909.

[CP21] F. Campagna and R. Pengo, *Entanglement in the family of division fields of elliptic curves with complex multiplication.* `https://arxiv.org/abs/2006.00883`

[CT12] A. Cadoret and A. Tamagawa, *A uniform open image theorem for ℓ-adic representations, I.* Duke Mathematical Journal 161 (2012), 2605–2634.

[Co1] K. Conrad, *The conductor ideal.* `www.math.uconn.edu/~kconrad/blurbs/gradnumthy/conductor.pdf`

[Co2] K. Conrad, *Tensor Products II* `https://kconrad.math.uconn.edu/blurbs/linmultialg/tensorprod2.pdf`

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

[DEvHMZB20] M. Derickx, A. Etropolski, M. van Hoeij, J.S. Morrow and D. Zureick-Brown, *Sporadic Cubic Torsion.* `https://arxiv.org/abs/2007.13929`

[FM02] M. Foquet and F. Morain, *Isogeny volcanoes and the SEA algorithm.* Algorithmic number theory (Sydney, 2002), 276–291, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[HK13] F. Halter-Koch, *Quadratic irrationals.* An introduction to classical number theory. Pure and Applied Mathematics. CRC Press, Boca Raton, FL, 2013.

[JT15] C.U. Jensen and A. Thorup, *Gorenstein orders.* J. Pure Appl. Algebra 219 (2015), 551–562.

[Ka92] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms.* Invent. Math. 109 (1992), 221–229.

[KM88] M.A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Math. J. 109 (1988), 125–149.

[Ko96] D. R. Kohel, *Endomorphism rings of elliptic curves over finite fields.* Ph.D. thesis, Univ. California, Berkeley, 1996.

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

[LD15] C. Lv and Y.P. Deng, *On orders in number fields: Picard groups, ring class fields and applications.* Sci. China Math. 58 (2015), 1627–1638.

[LR19] Á. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication.* `https://arxiv.org/abs/1809.02584`

[LV14] E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties.* Journal of the Institute of Mathematics of Jussieu 13 (2014), 517–559.

[Ma76] B. Mazur, *Rational points on modular curves.* Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107–148. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

[Ma77] B. Mazur, *Modular curves and the Eisenstein ideal. With an appendix by Mazur and M. Rapoport.* Inst. Hautes Études Sci. Publ. Math. (1977), 33–186.

[Me96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), 437–449.

[N] J. Neukirch, *Algebraic number theory.* Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.

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

[Ro97] D.E. Rohrlich, *Modular curves, Hecke correspondence, and L-functions.* Modular forms and Fermat's last theorem (Boston, MA, 1995), 41–100, Springer, New York, 1997.

[RS17] J. Rosen and A. Shnidman, *Extensions of CM elliptic curves and orbit counting on the projective line.* Res. Number Theory 3 (2017), Paper No. 9, 13 pp.

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

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

[Si88] A. Silverberg, *Torsion points on abelian varieties of CM-type.* Compositio Math. 68 (1988), 241–249.

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

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

[Su12] A.V. Sutherland, *Isogeny volcanoes.* `https://arxiv.org/abs/1208.5370`

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

[We73] P.J. Weinberger, *Exponents of the class groups of complex quadratic fields.* Acta Arith. 22 (1973), 117–124.

10. Appendix

10.1. **Cases 1-3:** $L = 0$.

10.1.1. *Case 1:* $L = 0$, $\left(\frac{\Delta_K}{\ell}\right) = -1$.

Residue Field	Multiplicity
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\ell^a\mathfrak{f})$

The path type that occurs in this case is I.

10.1.2. *Case 2:* $L = 0$, $\left(\frac{\Delta_K}{\ell}\right) = 0$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f}\ell^{a-1})$	1
$\mathbb{Q}(\mathfrak{f}\ell^a)$	1

Primitive Residue Fields: $\mathbb{Q}(\ell^{a-1}\mathfrak{f})$

The path types that occur in this case are I. and III.

10.1.3. *Case 3:* $L = 0$, $\left(\frac{\Delta_K}{\ell}\right) = 1$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	1
$K(\ell\mathfrak{f})$	1
$\vdots$	$\vdots$
$K(\ell^{a-1}\mathfrak{f})$	1
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

Primitive Residue Fields: $\begin{cases} \mathbb{Q}(\ell^a\mathfrak{f}),\ K(\mathfrak{f}) & \ell^a > 2 \\ \mathbb{Q}(2\mathfrak{f}) = \mathbb{Q}(\mathfrak{f}) & \ell^a = 2 \end{cases}$

The path types that occur in this case are I. and IV.

10.2. **Case 4:** $L \geq a = 1$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$\mathbb{Q}(\mathfrak{f}\ell)$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I. and II.

10.3. **Case 5:** $L \geq a \geq 2$**,** $\ell > 2$**.** Put $\gamma(a) \coloneqq \begin{cases} 1 & a \text{ odd} \\ 2 & a \text{ even} \end{cases}$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell^{\lfloor \frac{a}{2} \rfloor}-1}{2}$
$K(\ell^{\gamma(a)}\mathfrak{f})$	$\frac{(\ell-1)\ell^{\lfloor \frac{a-1}{2} \rfloor}-1}{2}$
$K(\ell^{\gamma(a)+2}\mathfrak{f})$	$\frac{(\ell-1)\ell^{\lfloor \frac{a-1}{2} \rfloor}-2}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^{a}\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., II. and V.

10.4. **Cases 6-9:** $L \geq a \geq 2$**,** $\ell = 2$**.**

10.4.1. *Case 6:* $L \geq a = 2,\ \ell = 2$*.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$\mathbb{Q}(4\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., II. and V_1.

10.4.2. *Case 7:* $L \geq a = 3,\ \ell = 2$*.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$\mathbb{Q}(2\mathfrak{f})$	1
$\mathbb{Q}(2^3\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I. II. V_1 and V_2.

10.4.3. *Case 8:* $L \geq a \geq 4$*,* $\ell = 2$*,* $A = 2a$ *is even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{A-1}-1$
$K(2^2\mathfrak{f})$	2^{A-3}
$K(2^4\mathfrak{f})$	2^{A-4}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

Again $b = 0$ yields the closed point equivalence class $[P_\downarrow]$ with residue field $\mathbb{Q}(2^a\mathfrak{f})$, while $b = a$ yields the path $P_\uparrow$, with residue field $\mathbb{Q}(\mathfrak{f})$. For all paths with $b = 1$, the initial subpath P_1 consists of one ascent followed by one (unique) descent, so P_1 is real, and we get one closed point equivalence class of paths with residue field $\mathbb{Q}(2^{a-2}\mathfrak{f})$. It follows from Lemmas 5.7, 5.9, 5.10 and 5.11 that for $2 \le b \le a-1$ the segment P_1 is not real and thus the residue field contains K. For $2 \le b < A$ the path P_1 consists of b ascents followed by b descents. There are 2^{b-1} such paths, which fall into 2^{b-2} closed point equivalence classes. There are $a-2b$ further descents, so all in all there are 2^{b-1} closed point equivalence classes of paths, each with residue field $K(2^{a-2b}\mathfrak{f})$.

10.4.4. *Case 9:* $L \ge a \ge 5$, $\ell = 2$, $a = 2A+1$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{A-1}-1$
$K(2\mathfrak{f})$	2^{A-2}
$K(2^3\mathfrak{f})$	2^{A-3}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

Again $b = 0$ yields the closed point equivalence class $[P_\downarrow]$ with residue field $\mathbb{Q}(2^a\mathfrak{f})$. The case $b = 1$ yields a unique closed point equivalence class with residue field $\mathbb{Q}(2^{a-2}\mathfrak{f})$. For $2 \le b \le A$, by the same results cited above the second descent means that the residue field contains K, and there are 2^{b-2} closed point equivalence classes of such paths, each with residue field $K(2^{a-2b}\mathfrak{f})$. For $A+1 \le b \le a-2$ the residue field again contains K and there are 2^{a-b-2} closed point equivalence classes of such paths, each with residue field $K(\mathfrak{f})$.

10.5. **Cases 10-12:** $L \geq 1$**,** $a > L$**,** $\left(\frac{\Delta_K}{\ell}\right) = -1$**,** $\ell > 2$**.**

10.5.1. *Case 10:* $L = 1$, $a \geq 2$, $\left(\frac{\Delta_K}{\ell}\right) = -1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\ell^{a-2}\mathfrak{f})$	1
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^{a}\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\ell^{a-2}\mathfrak{f})$

The path types that occur in this case are I. and VI.

10.5.2. *Case 11:* $2 \leq L \leq \frac{a}{2}$, $\left(\frac{\Delta_K}{\ell}\right) = -1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$	1
$K(\ell^{a-2L}\mathfrak{f})$	$\frac{\ell^L-1}{2}$
$K(\ell^{a-2L+2}\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$K(\ell^{a-2L+4}\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-4}\mathfrak{f})$	$\frac{(\ell-1)\ell}{2}$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^{a}\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$

The path types that occur in this case are I., V. and VI.

10.5.3. *Case 12:* $\frac{a}{2} < L < a$, $\left(\frac{\Delta_K}{\ell}\right) = -1$, $\ell > 2$. Put $\gamma(a) \coloneqq \begin{cases} 1 & a \text{ odd} \\ 2 & a \text{ even} \end{cases}$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell^{\lfloor \frac{a}{2} \rfloor}-1}{2}$
$K(\mathfrak{f}\ell^{\epsilon})$	$\frac{(\ell-1)\ell^{\lfloor \frac{a-1}{2} \rfloor-1}}{2}$
$\vdots$	$\vdots$
$K(\mathfrak{f}\ell^{a-2})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\mathfrak{f}\ell^{a})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V. and VI.

10.6. **Cases 13-20:** $L \geq 1$**,** $a > L$**,** $\left(\frac{\Delta_K}{\ell}\right) = 0$**,** $\ell > 2$**.**

10.6.1. *Case 13:* $L = 1$, $a = 2$, $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., VII. and VIII.

10.6.2. *Case 14:* $L = 1$, $a = 3$, $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell-1}{2}$
$K(\ell\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., VII. and VIII.

10.6.3. *Case 15:* $L = 1$, $a \geq 4$, $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\ell^{a-3}\mathfrak{f})$	1
$K(\ell^{a-3}\mathfrak{f})$	$\frac{\ell-1}{2}$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\ell^{a-3}\mathfrak{f})$

The path types that occur in this case are I., VII. and VIII.

10.6.4. *Case 16:* $L \geq 2$, $a \geq 2L + 1$, $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\ell^{a-2L-1}\mathfrak{f})$	1
$K(\ell^{a-2L-1}\mathfrak{f})$	$\frac{\ell^L-1}{2}$
$K(\ell^{a-2L}\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-1}}{2}$
$K(\ell^{a-2L+2}\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$K(\ell^{a-2L+4}\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\ell^{a-2L-1}\mathfrak{f})$

The path types that occur in this case are I., V. VII. and VIII.

10.6.5. *Case 17:* $L \geq 2$, $a = 2L$, $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-1}}{2} + \frac{\ell^{a/2-1}-1}{2}$
$K(\ell^2\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-2}}{2}$
$K(\ell^4\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V. VII. and VIII.

10.6.6. *Case 18:* $L \geq 2$, $a = 2L-1$, $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$K(\ell\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V. VII. and VIII.

10.6.7. *Case 19:* $L \geq 2$, $L+1 \leq a \leq 2L-2$, a *even,* $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{(\ell-1)(\ell^{a-L-1}+\ell^{a-L}+\ldots+\ell^{a/2-1}}{2} + \frac{\ell^{a-L-1}-1}{)}2$
$K(\ell^2\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-2}}{2}$
$K(\ell^4\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V. VII. and VIII.

10.6.8. *Case 20:* $L \geq 2$, $L+1 \leq a \leq 2L-3$, a *odd,* $\left(\frac{\Delta_K}{\ell}\right) = 0$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{(\ell-1)(\ell^{a-L-1}+\ell^{a-L}+\ldots+\ell^{\frac{a-1}{2}-1})}{2} + \frac{\ell^{a-L-1}-1}{2}$
$K(\ell\mathfrak{f})$	$\frac{(\ell-1)\ell^{\frac{a-1}{2}-1}}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{(\ell-1)\ell^{\frac{a-1}{2}-2}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V. VII. and VIII.

10.7. **Cases 21-33:** $L \geq 1$, $a > L$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

10.7.1. *Case 21:* $L = 1$, $a = 2$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell-3}{2}+1$
$\mathbb{Q}(\ell^2\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., IX. and X.

10.7.2. *Case 22:* $L = 1$, $a \geq 3$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	ℓ
$K(\ell\mathfrak{f})$	$\ell - 1$
$K(\ell^2\mathfrak{f})$	$\ell - 1$
$\vdots$	$\vdots$
$K(\ell^{a-3}\mathfrak{f})$	$\ell - 1$
$\mathbb{Q}(\ell^{a-2}\mathfrak{f})$	1
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-3}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\ell^{a-2}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., IX., X., XI.

10.7.3. *Case 23:* $L = 2$, $a = 3$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$1 + \frac{\ell-3}{2}$
$K(\ell\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^3\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX. and X.

10.7.4. *Case 24:* $L = 3$, $a = 4$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$1 + \frac{\ell-3}{2} + \frac{(\ell-1)\ell}{2}$
$K(\ell^2\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX. and X.

10.7.5. *Case 25:* $L = 4$, $a = 5$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$1 + \frac{\ell-3}{2} + \frac{(\ell-1)\ell}{2}$
$K(\ell\mathfrak{f})$	$\frac{\ell-1}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX. and X.

10.7.6. *Case 26:* $L \geq 5$ *odd*, $a = L + 1$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$1 + \frac{\ell-3}{2} + \frac{(\ell-1)(\ell+\ldots+\ell^{a/2-1})}{2}$
$K(\ell^2\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-2}}{2}$
$K(\ell^4\mathfrak{f})$	$\frac{(\ell-1)(\ell^{a/2-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX. and X.

10.7.7. *Case 27:* $L \geq 6$ *even*, $a = L + 1$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$1 + \frac{\ell-3}{2} + \frac{(\ell-1)(\ell+\ldots+\ell^{L/2-1})}{2}$
$K(\ell\mathfrak{f})$	$\frac{(\ell-1)\ell^{L/2-1}}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{(\ell-1)\ell^{L/2-2}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX. and X.

10.7.8. *Case 28:* $L \geq 2$, $a \geq 2L+2$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	ℓ^L
$K(\ell\mathfrak{f})$	$(\ell-1)\ell^{L-1}$
$K(\ell^2\mathfrak{f})$	$(\ell-1)\ell^{L-1}$
$\vdots$	$\vdots$
$K(\ell^{a-2L-1}\mathfrak{f})$	$(\ell-1)\ell^{L-1}$
$\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$	1
$K(\ell^{a-2L}\mathfrak{f})$	$\frac{(\ell-2)\ell^{L-1}-1}{2}$
$K(\ell^{a-2L+2}\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-4}\mathfrak{f})$	$\frac{(\ell-1)\ell}{2}$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V., IX., X. and XI.

10.7.9. *Case 29:* $L \geq 2$, $a = 2L+1$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	ℓ^L
$\mathbb{Q}(\ell\mathfrak{f})$	1
$K(\ell\mathfrak{f})$	$\frac{(\ell-2)\ell^{L-1}-1}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-4}\mathfrak{f})$	$\frac{(\ell-1)\ell}{2}$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\ell^{a-2L}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V., IX., X. and XI.

10.7.10. *Case 30:* $L \geq 2$, $a = 2L$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\ell^{L-1} + \frac{(\ell-2)\ell^{L-1}-1}{2}$
$K(\ell^2\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX., X. and XI.

10.7.11. *Case 31:* $L \geq 2$, $a = 2L-1$, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\ell^{L-2} + \frac{(\ell-2)\ell^{L-2}-1}{2}$
$K(\ell\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-2}}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{(\ell-1)\ell^{L-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX., X. and XI.

10.7.12. *Case 32:* $L \geq 2$, $L+2 \leq a \leq 2L-2$, a *even*, $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell^{a/2}-1}{2}$
$K(\ell^2\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-2}}{2}$
$K(\ell^4\mathfrak{f})$	$\frac{(\ell-1)\ell^{a/2-3}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX., X. and XI.

10.7.13. *Case 33:* $L \geq 2$, $L+2 \leq a \leq 2L-3$, a *odd,* $\left(\frac{\Delta_K}{\ell}\right) = 1$, $\ell > 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	1
$K(\mathfrak{f})$	$\frac{\ell^{\frac{a-1}{2}}-1}{2}$
$K(\ell\mathfrak{f})$	$\frac{(\ell-1)\ell^{\frac{a-1}{2}-1}}{2}$
$K(\ell^3\mathfrak{f})$	$\frac{(\ell-1)\ell^{\frac{a-1}{2}-2}}{2}$
$\vdots$	$\vdots$
$K(\ell^{a-4}\mathfrak{f})$	$\frac{(\ell-1)\ell}{2}$
$K(\ell^{a-2}\mathfrak{f})$	$\frac{\ell-1}{2}$
$\mathbb{Q}(\ell^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V., IX., X. and XI.

10.8. **Cases 34-43:** $L \geq 1$, $a > L$, $\ell = 2$, $\left(\frac{\Delta_K}{2}\right) = -1$.

10.8.1. *Case 34:* $L = 1$, $a \geq 2$.

Residue Field	Multiplicity
$K(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^a\mathfrak{f})$, $K(2^{a-2}\mathfrak{f})$

The path types that occur in this case are I. and VI.

10.8.2. *Case 35:* $L = 2$, $a = 3$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	1
$\mathbb{Q}(2\mathfrak{f})$	1
$\mathbb{Q}(8\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1. and VI.

10.8.3. *Case 36:* $L = 2$, $a \geq 4$.

Residue Field	Multiplicity
$K(2^{a-4}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	2
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2}\mathfrak{f})$, $K(2^{a-4}\mathfrak{f})$

The path types that occur in this case are I., V_1 and VI.

10.8.4. *Case 37:* $L = 3$, $a = 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$\mathbb{Q}(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3. and VI.

10.8.5. *Case 38:* $L = 3$, $a = 5$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2
$\mathbb{Q}(2\mathfrak{f})$	2
$\mathbb{Q}(2^3\mathfrak{f})$	1
$\mathbb{Q}(2^5\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3. and VI.

10.8.6. *Case 39:* $L = 3$, $a \geq 6$.

Residue Field	Multiplicity
$K(2^{a-6}\mathfrak{f})$	4
$\mathbb{Q}(2^{a-4}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-4}\mathfrak{f})$, $K(2^{a-6}\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3. and VI.

10.8.7. *Case 40:* $4 \leq L < a \leq 2L - 6$, a *even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{a/2-1}$
$K(2^2\mathfrak{f})$	$2^{a/2-3}$
$K(2^4\mathfrak{f})$	$2^{a/2-4}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3. and VI.

10.8.8. *Case 41:* $4 \leq L < a \leq 2L-5$, *a odd.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a-3}{2}}-1$
$K(2\mathfrak{f})$	$2^{\frac{a-5}{2}}$
$K(2^3\mathfrak{f})$	$2^{\frac{a-7}{2}}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3. and VI.

10.8.9. *Case 42:* $5 \leq L$, $a = 2L-4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{a-L+1}-1$
$K(2^2\mathfrak{f})$	2^{a-L-1}
$K(2^4\mathfrak{f})$	2^{a-L-2}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3. and VI.

10.8.10. *Case 43:* $L \geq 4$, $a \geq 2L$.

Residue Field	Multiplicity
$K(2^{a-2L}\mathfrak{f})$	2^{L-1}
$\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$	2
$K(2^{a-2L+2}\mathfrak{f})$	$2^{L-3}-1$
$K(2^{a-2L+4}\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$, $K(2^{a-2L}\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., V_4. and VI.

10.9. **Cases 44-64:** $L \geq 1$**,** $a > L$**,** $\ell = 2$**,** $\left(\frac{\Delta_K}{2}\right) = 1$**.**

10.9.1. *Case 44:* $L = 1$, $a = 2$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2
$\mathbb{Q}(4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(4\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I. and X.

10.9.2. *Case 45:* $L = 1$, $a = 3$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2
$\mathbb{Q}(8\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(8\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I. and X. and XI.

10.9.3. *Case 46:* $L = 1$, $a \geq 4$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2
$K(2\mathfrak{f})$	1
$\vdots$	$\vdots$
$K(2^{a-3}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I. and X. and XI.

10.9.4. *Case 47:* $L = 2$, $a = 3$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	1
$\mathbb{Q}(2\mathfrak{f})$	1
$\mathbb{Q}(2^3\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1. and X.

10.9.5. *Case 47:* $L = 2$, $a = 4$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2
$\mathbb{Q}(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, X. and XI.

10.9.6. *Case 48:* $L = 2$, $a = 5$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	4
$\mathbb{Q}(2^3\mathfrak{f})$	1
$\mathbb{Q}(2^5\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^3\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, X. and XI.

10.9.7. *Case 49:* $L = 2$, $a \geq 6$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	4
$K(2\mathfrak{f})$	2
$\vdots$	$\vdots$
$K(2^{a-5}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, X. and XI.

10.9.8. *Case 50:* $L = 3$, $a = 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$\mathbb{Q}(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., X. and XI.

10.9.9. *Case 51:* $L = 3$, $a = 5$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2
$\mathbb{Q}(2\mathfrak{f})$	2
$\mathbb{Q}(2^3\mathfrak{f})$	1
$\mathbb{Q}(2^5\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., X. and XI.

10.9.10. *Case 52:* $L = 3$, $a = 6$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	4
$\mathbb{Q}(2^2\mathfrak{f})$	2
$\mathbb{Q}(2^4\mathfrak{f})$	1
$\mathbb{Q}(2^6\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., X. and XI.

10.9.11. *Case 53:* $L = 3$, $a = 7$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	8
$\mathbb{Q}(2^3\mathfrak{f})$	2
$\mathbb{Q}(2^5\mathfrak{f})$	1
$\mathbb{Q}(2^7\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^3\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., X. and XI.

10.9.12. *Case 54:* $L = 3$, $a \geq 8$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	8
$K(2\mathfrak{f})$	4
$\vdots$	$\vdots$
$K(2^{a-7}\mathfrak{f})$	4
$\mathbb{Q}(2^{a-4}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(2^{a-4}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., X. and XI.

10.9.13. *Case 55:* $4 \leq L < a \leq 2L - 6$, *a even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a}{2}-1} - 1$
$K(2^2\mathfrak{f})$	$2^{\frac{a}{2}-3}$
$K(2^4\mathfrak{f})$	$2^{\frac{a}{2}-4}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.14. *Case 56:* $4 \leq L < a \leq 2L - 5$, *a odd.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a-1}{2}-1} - 1$
$K(2\mathfrak{f})$	$2^{\frac{a-1}{2}-2}$
$K(2^3\mathfrak{f})$	$2^{\frac{a-1}{2}-3}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.15. *Case 57:* $L \geq 4$, $a = 2L - 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-3} - 1$
$K(2^2\mathfrak{f})$	2^{L-5}
$K(2^4\mathfrak{f})$	2^{L-6}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.16. *Case 58:* $L \geq 4$, $a = 2L - 3$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-3} - 1$
$K(2\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.17. *Case 59:* $L \geq 4$, $a = 2L - 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-2} - 1$
$K(2^2\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.18. *Case 60:* $L \geq 4$, $a = 2L - 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-2} - 1$
$K(2^2\mathfrak{f})$	2^{L-4}
$K(2^4\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.19. *Case 61:* $L \geq 4$, $a = 2L - 1$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2^{L-2}
$\mathbb{Q}(2\mathfrak{f})$	2
$K(2\mathfrak{f})$	$2^{L-3} - 1$
$K(2^3\mathfrak{f})$	2^{L-4}
$K(2^5\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.20. *Case 62:* $L \geq 4$, $a = 2L$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2^{L-1}
$\mathbb{Q}(2^2\mathfrak{f})$	2
$K(2^2\mathfrak{f})$	$2^{L-3} - 1$
$K(2^4\mathfrak{f})$	2^{L-4}
$K(2^6\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^2\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.21. *Case 63:* $L \geq 4$, $a = 2L + 1$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2^L
$\mathbb{Q}(2^3\mathfrak{f})$	2
$K(2^3\mathfrak{f})$	$2^{L-3} - 1$
$K(2^5\mathfrak{f})$	2^{L-4}
$K(2^7\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^3\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1, V_3., V_4., X. and XI.

10.9.22. *Case 64:* $L \geq 4$, $a \geq 2L + 2$.

Residue Field	Multiplicity
$K(\mathfrak{f})$	2^L
$K(2\mathfrak{f})$	2^{L-1}
$K(2^2\mathfrak{f})$	2^{L-1}
$\vdots$	$\vdots$
$K(2^{2-2L-1}\mathfrak{f})$	2^{L-1}
$\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$	2
$K(2^{a-2L+2}\mathfrak{f})$	$2^{L-3} - 1$
$K(2^{a-2L+4}\mathfrak{f})$	2^{L-4}
$K(2^{a-2L+6}\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2L+2}\mathfrak{f})$, $K(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., V_4., X. and XI.

10.10. **Cases 65-79:** $L \geq 1$, $a > L$, $\ell = 2$, $\mathrm{ord}_2(\Delta_K) = 2$.

10.10.1. *Case 65:* $L = 1$, $a = 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$\mathbb{Q}(2^2\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., VI_1. and VIII_1.

10.10.2. *Case 66:* $L = 1$, $a \geq 3$.

Residue Field	Multiplicity
$K(2^{a-3}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2}\mathfrak{f})$, $K(2^{a-3}\mathfrak{f})$

The path types that occur in this case are I., VI_1. and VIII_2.

10.10.3. *Case 67:* $L = 2$, $a = 3$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$\mathbb{Q}(2\mathfrak{f})$	1
$\mathbb{Q}(2^3\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., VI_2. and VIII_1.

10.10.4. *Case 68:* $L = 2$, $a = 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$\mathbb{Q}(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., VI_3. and VIII_2.

10.10.5. *Case 69:* $L = 2$, $a \geq 5$.

Residue Field	Multiplicity
$K(2^{a-5}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-4}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-4}\mathfrak{f})$, $K(2^{a-5}\mathfrak{f})$

The path types that occur in this case are I., V_1., VI_3. and $VIII_2$.

10.10.6. *Case 70:* $L = 3$, $a = 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$\mathbb{Q}(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_2., $VIII_1$.

10.10.7. *Case 71:* $L = 3$, $a = 5$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$K(2\mathfrak{f})$	1
$\mathbb{Q}(2^3\mathfrak{f})$	1
$\mathbb{Q}(2^5\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.8. *Case 72:* $L = 3$, $a = 6$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	3
$K(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1
$\mathbb{Q}(2^6\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.9. *Case 73:* $L \geq 3$, $a \geq 2L + 1$.

Residue Field	Multiplicity
$K(2^{a-2L-1}\mathfrak{f})$	2^{L-1}
$\mathbb{Q}(2^{a-2L}\mathfrak{f})$	2
$K(2^{a-2L}\mathfrak{f})$	$2^{L-2}-1$
$K(2^{a-2L+2}\mathfrak{f})$	2^{L-3}
$K(2^{a-2L+4}\mathfrak{f})$	2^{L-2}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2L}\mathfrak{f})$, $K(2^{a-2L-1}\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.10. *Case 74: $L \geq 4$, $a = L+1$, a odd.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a-3}{2}}-1$
$K(2\mathfrak{f})$	$2^{\frac{a-5}{2}}$
$K(2^3\mathfrak{f})$	$2^{\frac{a-7}{2}}$
$\vdots$	$\vdots$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_2, $VIII_1$.

10.10.11. *Case 75: $L \geq 5$, $a = L+1$, a even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a}{2}-1}-1$
$K(2^2\mathfrak{f})$	$2^{\frac{a}{2}-3}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_2, $VIII_1$.

10.10.12. *Case 76:* $L \geq 4$, $a = 2L$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-1} - 1$
$K(2^2\mathfrak{f})$	2^{L-3}
$K(2^4\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.13. *Case 77:* $L \geq 4$, $a = 2L - 1$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-2} - 1$
$K(2\mathfrak{f})$	2^{L-3}
$K(2^3\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.14. *Case 77:* $L \geq 4$, $a = 2L - 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-2} - 1$
$K(2^2\mathfrak{f})$	2^{L-4}
$K(2^4\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.15. *Case 78:* $L \geq 4$, $L+2 \leq a \leq 2L-3$, *a odd.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a-1}{2}-1}-1$
$K(2\mathfrak{f})$	$2^{\frac{a-1}{2}-2}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.10.16. *Case 79:* $L \geq 6$, $L+2 \leq a \leq 2L-4$, *a even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a}{2}-1}-1$
$K(2^2\mathfrak{f})$	$2^{\frac{a}{2}-3}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11. **Cases 80-95:** $L \geq 1$, $a > L$, $\ell = 2$, $\mathrm{ord}_2(\Delta_K) = 3$.

10.11.1. *Case 80:* $L = 1$, $a = 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$\mathbb{Q}(2^2\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., VI_1. and $VIII_1$.

10.11.2. *Case 81:* $L = 1$, $a \geq 3$.

Residue Field	Multiplicity
$\mathbb{Q}(2^{a-3}\mathfrak{f})$	2
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-3}\mathfrak{f})$

The path types that occur in this case are I., VI_1. and VIII_2.

10.11.3. *Case 82:* $L = 2$, $a = 3$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$\mathbb{Q}(2\mathfrak{f})$	1
$\mathbb{Q}(2^{3}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., VI_2. and VIII_1.

10.11.4. *Case 83:* $L = 2$, $a = 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$\mathbb{Q}(2^{2}\mathfrak{f})$	1
$\mathbb{Q}(2^{4}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., VI_3. and VIII_2.

10.11.5. *Case 84:* $L = 2$, $a \geq 5$.

Residue Field	Multiplicity
$\mathbb{Q}(2^{a-5}\mathfrak{f})$	2
$K(2^{a-5}\mathfrak{f})$	1
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-5}\mathfrak{f})$

The path types that occur in this case are I., V_1., VI_3. and VIII_2.

10.11.6. *Case 85:* $L = 3$, $a = 4$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$\mathbb{Q}(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_2., $VIII_1$.

10.11.7. *Case 86:* $L = 3$, $a = 5$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	1
$K(2\mathfrak{f})$	1
$\mathbb{Q}(2^3\mathfrak{f})$	1
$\mathbb{Q}(2^5\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.8. *Case 87:* $L = 3$, $a = 6$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	3
$K(2^2\mathfrak{f})$	1
$\mathbb{Q}(2^4\mathfrak{f})$	1
$\mathbb{Q}(2^6\mathfrak{f})$	1

Primitive Residue Fields: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.9. *Case 88:* $L \geq 3$, $a \geq 2L + 1$.

Residue Field	Multiplicity
$\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$	2
$K(2^{a-2L-1}\mathfrak{f})$	$2^{L-1}-1$
$K(2^{a-2L}\mathfrak{f})$	2^{L-2}
$K(2^{a-2L+2}\mathfrak{f})$	2^{L-3}
$K(2^{a-2L+4}\mathfrak{f})$	2^{L-2}
$\vdots$	$\vdots$
$K(2^{a-6}\mathfrak{f})$	2
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(2^{a-2L-1}\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.10. *Case 89: $L \geq 4$, $a = L+1$, a odd.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a-3}{2}}-1$
$K(2\mathfrak{f})$	$2^{\frac{a-5}{2}}$
$K(2^3\mathfrak{f})$	$2^{\frac{a-7}{2}}$
$\vdots$	$\vdots$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_2, $VIII_1$.

10.11.11. *Case 90: $L \geq 5$, $a = L+1$, a even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a}{2}-1}-1$
$K(2^2\mathfrak{f})$	$2^{\frac{a}{2}-3}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_2, $VIII_1$.

10.11.12. *Case 91:* $L \geq 4$, $a = 2L$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-1} - 1$
$K(2^2\mathfrak{f})$	2^{L-3}
$K(2^4\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.13. *Case 92:* $L \geq 4$, $a = 2L - 1$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-2} - 1$
$K(2\mathfrak{f})$	2^{L-3}
$K(2^3\mathfrak{f})$	2^{L-4}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.14. *Case 93:* $L \geq 4$, $a = 2L - 2$.

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{L-2} - 1$
$K(2^2\mathfrak{f})$	2^{L-4}
$K(2^4\mathfrak{f})$	2^{L-5}
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^a\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.15. *Case 94:* $L \geq 4$, $L+2 \leq a \leq 2L-3$, *a odd.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a-1}{2}-1}-1$
$K(2\mathfrak{f})$	$2^{\frac{a-1}{2}-2}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.

10.11.16. *Case 95:* $L \geq 6$, $L+2 \leq a \leq 2L-4$, *a even.*

Residue Field	Multiplicity
$\mathbb{Q}(\mathfrak{f})$	2
$K(\mathfrak{f})$	$2^{\frac{a}{2}-1}-1$
$K(2^2\mathfrak{f})$	$2^{\frac{a}{2}-3}$
$\vdots$	$\vdots$
$K(2^{a-4}\mathfrak{f})$	1
$\mathbb{Q}(2^{a-2}\mathfrak{f})$	1
$\mathbb{Q}(2^{a}\mathfrak{f})$	1

PRIMITIVE RESIDUE FIELDS: $\mathbb{Q}(\mathfrak{f})$

The path types that occur in this case are I., V_1., V_3., VI_3, $VIII_2$.