A volcanic approach to CM points on Shimura curves

by

Frederick V. Saia

(Under the Direction of Pete L. Clark)

Abstract

This thesis is devoted to a study of CM points on the Shimura curves $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$, parametrizing abelian surfaces with quaternionic multiplication and extra level structure. We demonstrate an isogeny-volcano approach to CM points on these curves, generalizing work of Clark and Clark–Saia in the quaternion discriminant $D = 1$ case of elliptic modular curves $Y_0(M, N)_{/\mathbb{Q}}$ and $Y_1(M, N)_{/\mathbb{Q}}$, via consideration of CM components of QM-equivariant isogeny graphs over $\overline{\mathbb{Q}}$. This approach provides a description of the CM locus on $X_0^D(N)_{/\mathbb{Q}}$ for D a rational quaternion discriminant and $\gcd(D, N) = 1$, yielding for a given imaginary quadratic order $\mathfrak{o}$ a count of all $\mathfrak{o}$-CM points on $X_0^D(N)_{/\mathbb{Q}}$ with each possible residue field. This allows for a determination of all primitive residue fields and primitive degrees of $\mathfrak{o}$-CM points on $X_0^D(N)_{/\mathbb{Q}}$, and in particular allows for a computation of the least degree of a CM point on $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$, ranging over all orders. As an application, we leverage computations of these least degrees towards determining the existence of sporadic CM points on $X_0^D(N)_{/\mathbb{Q}}$.

Index words: [Shimura curve, complex multiplication, CM point, abelian surface, quaternionic multiplication, elliptic curve, abelian variety, modular curve]

A volcanic approach to CM points on Shimura curves

by

Frederick V. Saia

B.S., Tufts University, 2017

A Dissertation Submitted to the Graduate Faculty of the
University of Georgia in Partial Fulfillment of the Requirements for the Degree.

Doctor of Philosophy

Athens, Georgia

2023

A volcanic approach to CM points on Shimura curves

by

Frederick V. Saia

Major Professor: Pete L. Clark

Committee: Daniel Litt
Dino J. Lorenzini
Paul Pollack

Electronic Version Approved:

Ron Walcott
Dean of the Graduate School
The University of Georgia
May 2023

Dedication

To my mother, Lisa

Acknowledgments

My sincerest gratitude goes to my committee members, Pete Clark, Daniel Litt, Dino Lorenzini, and Paul Pollack, who have all been excellent educators and whose efforts have been integral in my mathematical development. My advisor, Pete, has been patient and singularly helpful in guiding me in the work that I discuss here. More generally, my thanks to Pete for introducing me to plenty of delightful mathematics, and for exhibiting admirable care for, and interest in, mathematical communication and exposition, which I have found motivating as a student. I am also grateful in particular to Dino for helping me become more careful and precise as a number theorist, and to Daniel for organizing numerous seminars and reading groups that were both fun and formative to me as a student. Thanks also to John Voight for helpful comments and encouragement related to the work appearing in this thesis.

I am deeply indebted to the current and former students and postdocs in number theory and arithmetic geometry at UGA who worked to build an active, collaborative, and friendly atmosphere. From student organized reading groups and seminars (even those over Zoom!), to less formal mathematical deliberations which could tend to dissolve to non-mathematical, it would be difficult to fully articulate the positive social and mathematical impact your time and efforts have had for me. Thanks here go to Paco Adajar, Ilkiz Bildik, Peter Cassels, Zack Garza (who may not call himself a number theorist, but belongs here nonetheless), Tyler Genao, Borys Kadets, Daniel Keliher, Mentzelos Melistas, Sasha Shmakov, Padma Srinivasan, Arvind Suresh, Makoto Suwama, Nicholas Triantafillou, and Haiyang Wang. I will single out Tyler Genao here, who has been on this path with me through its entirety, and helped to make it a considerably less isolated experience.

Laura Ackerley deserves countless thanks for all of her kindness and work towards bettering the graduate program and the experiences of graduate students, and I take this opportunity to again wish her a wonderful retirement. Lucy Barrera has done a great job filling in her role, and I thank her for all of her help during my final year.

Finally, I would like to thank my family and loved ones. I especially thank my sisters, Elisabeth and Sara, for providing support and encouragement as I moved a ways down the East Coast to do mathematics of all things, as well as Ashlyn, whose support and companionship have held me up throughout these years. This small space unfortunately does not have the capacity to express how grateful I am to you all.

Contents

Acknowledgments **v**

List of Figures **viii**

List of Tables **ix**

1 Introduction **1**

2 Background **8**

2.1 Shimura curves 8

2.2 Complex multiplication 21

2.3 Fields of moduli 26

3 Decompositions of QM abelian surfaces with CM **34**

4 QM-equivariant isogeny volcanoes **38**

4.1 QM-equivariant isogenies 38

4.2 Volcanoes 41

4.3 The action of Galois on $\mathcal{G}^D_{K,\ell,f_0}$ 49

4.4 The field of moduli of a QM-cyclic ℓ^a isogeny 51

4.5 Explicit description: $\mathfrak{f}_0^2\Delta_K < -4$ 52

4.6 Explicit description part II: $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$ 59

5 CM points on Shimura curves **69**

5.1 CM points on $X_0^D(\ell^a)_{/\mathbb{Q}}$ 69
5.2 Algebraic results on residue fields of CM points on $X^D(1)_{/\mathbb{Q}}$ 80
5.3 CM points on $X_0^D(N)_{/\mathbb{Q}}$ 87
5.4 CM points on $X_1^D(N)_{/\mathbb{Q}}$ 93
5.5 Sporadic CM points on Shimura Curves 96

List of Figures

4.1 $\ell = 3$ inert in K with $L = 2$ 53

4.2 $\ell = 3$ split in K with $L = 2$ 53

4.3 $\ell = 3$ ramified in K with $|V_0| = 1$ and $L = 2$ 54

4.4 $\ell = 3$ ramified in K with $|V_0| = 2$ and $L = 2$ 54

4.5 $\ell = 2$ inert with $L = 4$ 56

4.6 $\ell = 2$ split with $L = 4$ 56

4.7 $\mathfrak{f}_0^2\Delta_K = -8$ and $\ell = 2$ with $L = 3$ 57

4.8 $\Delta_K \neq -4$ with $\ell = 2, \mathrm{ord}_2(\Delta_K) = 2$ and $L = 3$ 58

4.9 $\Delta_K < -8$ with $\ell = 2, \mathrm{ord}_2(\Delta_K) = 3$ and $L = 3$ 59

4.10 $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-1}),\ell,1}$, ℓ split ($\ell = 5$, left) and inert ($\ell = 3$, right) up to level 2 62

4.11 $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-3}),\ell,1}$, ℓ split ($\ell = 7$, left) and inert ($\ell = 5$, right) up to level 2 62

4.12 $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-3}),2,1}$ up to level 4 63

4.13 the double cover $\widetilde{\mathcal{G}}$ of $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-1}),2,1}$ up to level 3 64

4.14 the double cover $\widetilde{\mathcal{G}}$ of $\mathcal{G} = \mathcal{G}_{\mathbb{Q}(\sqrt{-3}),3,1}$ up to level 2 66

4.15 $\mathfrak{f}_0^2\Delta_K = -4, \ell = 2$ up to level 3 67

4.16 $\mathfrak{f}_0^2\Delta_K = -4$, ℓ split ($\ell = 5$, left) and inert ($\ell = 3$, right) up to level 2 67

4.17 $\mathfrak{f}_0^2\Delta_K = -3, \ell = 3$ up to level 2 (left) and $\ell = 2$ up to level 3 (right) 67

4.18 $\mathfrak{f}_0^2\Delta_K = -3$, ℓ split ($\ell = 7$, left) and inert ($\ell = 5$, right) up to level 2 68

List of Tables

5.3 All 391 pairs (D, N) with $D > 1$ for which we remain unsure whether $X_0^D(N)_{/\mathbb{Q}}$ has a sporadic CM point 109

5.1 227 pairs (D, N) for which $X_0^D(N)_{/\mathbb{Q}}$ has a sporadic CM point of degree 2 via Lemma 5.5.8 110

5.2 64 pairs (D, N) with $\gcd(D, N) = 1$ for which $\delta(X_0^D(N)) = 2$, and hence $X_0^D(N)_{/\mathbb{Q}}$ has no sporadic points 111

Chapter 1

Introduction

For F a number field and E/F an elliptic curve, the group $E(F)$ of F-rational points on E is a finitely generated abelian group [Mor22]. Hence, we have a decomposition of $E(F)$ into a free part of some rank $r \geq 0$, and a finite torsion part:

$$E(F) \cong \mathbb{Z}^r \oplus E(F)_{\text{tors}}.$$

A natural question follows: which groups arise as $E(F)_{\text{tors}}$ for some elliptic curve E/F over a given number field F? A theorem of Merel [Mer96] provides that there are finitely many possibilities not only over a fixed F, but over a fixed degree $d = [F : \mathbb{Q}]$; that is, for any $d \in \mathbb{Z}^+$, there exists a constant $B(d) > 0$ such that

$$\#E(K)_{\text{tors}} \leq B(d)$$

for all elliptic curves E/F over a number field F of degree d.

The question of which groups arise as $E(F)_{\text{tors}}$ for some elliptic curve E/F has been answered for number fields F of degree $d = 1$, the case $F = \mathbb{Q}$, by work of Mazur [Maz77], for $d = 2$ by work of Kenku–Momose [KM88] and Kamienny [Kam92], and for $d = 3$ by recent work of Derickx–Etropolski–Morrow–van Hoeij–Zureick-Brown [DEMHZ21]. We should view this work as a feat; it does not appear likely that many similar results will be achieved without significant theoretical advances.

With that said, let us switch our vantage and study something of a dual problem – instead of fixing a degree d and asking about the possibilities of $E(K)_{\text{tors}}$, we may fix a possible torsion subgroup and ask:

Question 1.1. For a fixed group T, over which degrees d do we have a number field F of degree d and an elliptic curve E/F with $E(F)_{\text{tors}} \cong T$? More specifically, over which number fields F do we have such an elliptic curve?

This question fits into what is referred to as Mazur's Program B, and it has a natural reformulation as a problem in Diophantine geometry using the language of elliptic modular curves. For example, the existence of an elliptic curve E/F with

$$\mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)_{\text{tors}}$$

is equivalent to the existence of an F-rational point on the modular curve $Y_1(N)_{/\mathbb{Q}}$, that is, to the statement that $Y_1(N)_{/\mathbb{Q}}(F) \neq \emptyset$. This displays that Question 1.1 is intimately related to the following question:

Question 1.2. Over which degrees d do we have a number field F such that $Y_1(N)_{/\mathbb{Q}}$ has an F-rational point? More specifically, for which number fields F do we have $Y_1(N)_{/\mathbb{Q}}(F) \neq \emptyset$?

With this motivation, this thesis is devoted to studying rational points on the families of Shimura curves $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$, with the example of $X_1^1(N)_{/\mathbb{Q}} = Y_1(N)_{/\mathbb{Q}}$ being a special case. In particular, our study is focused on CM points on these moduli spaces, corresponding to elliptic curves and higher dimensional analogues with extra endomorphisms. The extra structure provided in the CM case often affords paths to greater results than can be achieved by similar means in the general case. Following foundational work of Silverberg on CM abelian varieties [Si88, Si92], much progress has been seen via this restriction in the study of elliptic curves over number fields (see, e.g., [CCS13, CP15, BCP17, BCS17, BP17, CP17, LR18, BC20a, BC20b]).

In particular, recent work of Clark and Clark–Saia [Cl23, CS23], continuing a research program from the perspective of CM points on modular curves (see [CCS13, BC20b, CGPS22]),

approaches the study of the CM locus on the modular curves $X_0(M,N)_{/\mathbb{Q}}$ and $X_1(M,N)_{/\mathbb{Q}}$ via a study of CM components of isogeny graphs of elliptic curves over $\overline{\mathbb{Q}}$. This includes the special cases of $X_0(1,N)_{/\mathbb{Q}} = X_0(N)_{/\mathbb{Q}}$ and $X_1(1,N)_{/\mathbb{Q}} = X_1(N)_{/\mathbb{Q}}$, while [Cl23] provides a general definition of these curves.

In this thesis, we undertake a similar study, generalizing in the $M = 1$ case to the more general setting of Shimura curves $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$, parametrizing abelian surfaces with quaternionic multiplication (QM) by the indefinite quaternion algebra B over $\mathbb{Q}$ of discriminant D, along with certain specified level structure. Our results allow for an algorithmic description of the $\mathfrak{o}$-CM locus on these curves for D the discriminant of any indefinite quaternion algebra over $\mathbb{Q}$, any positive integer N relatively prime to D, and $\mathfrak{o}$ any imaginary quadratic order.

Our convention is that the $\mathfrak{o}$-CM locus on either of these curves refers to the collection of fibers lying above $\mathfrak{o}$-CM points on $X^D(1)_{/\mathbb{Q}}$ under the natural modular maps (see Remark 2.3.7 for the alternate convention). The fiber over an $\mathfrak{o}$-CM point $x \in X^D(1)_{/\mathbb{Q}}$ under such a map is a finite Spec$\mathbb{Q}$-scheme, of the form $F = \mathrm{Spec}A$ for A some finite dimensional, hence Artinian, $\mathbb{Q}$-algebra A. We then have finitely many closed points on F, and for each point we have a corresponding residue field and a ramification index over x. For $\Delta < -4$ there is no ramification, and in the absence of ramification F is reduced, hence A is the product of those number fields arising as residue fields of closed points in F (with multiplicity). A Δ-CM point which is ramified over its image on $X^D(1)_{/\mathbb{Q}}$ has ramification index 2 if $\Delta = -4$ and 3 if $\Delta = -3$. With that said, our main algorithmic result for the first family has the following structure:

Algorithm 1.3 (The $\mathfrak{o}$-CM-locus on $X_0^D(N)_{/\mathbb{Q}}$)**.**

- *Input: an indefinite rational quaternion discriminant D, a positive integer N coprime to D, and an imaginary quadratic order $\mathfrak{o}$*
- *Output: the complete list of pairs (L, e) consisting of a number field L and $e \in \{1,2,3\}$ such that there exists an $\mathfrak{o}$-CM point on $X_0^D(N)_{/\mathbb{Q}}$ with $\mathbb{Q}(x) \cong L$ and with ramification*

index e respect to the natural map to $X^D(1)_{/\mathbb{Q}}$. For each such pair, we give a count of all closed $\mathfrak{o}$-CM points with that corresponding pair.

The $D = 1$ case of this algorithm results from the work of [Cl23] and [CS23]. For all D, we show the following: suppose that $x \in X_0^D(N)_{/\mathbb{Q}}$ has CM by the order $\mathfrak{o}(\mathfrak{f})$ of conductor $\mathfrak{f}$ in the imaginary quadratic field K. The residue field $\mathbb{Q}(x)$ is then either a ring class field $K(\mathfrak{f}')$ for some $\mathfrak{f}'$ with $\mathfrak{f} \mid \mathfrak{f}' \mid Nf$, or is isomorphic to an index 2 subfield of such a field $K(\mathfrak{f}')$. The ramification index mentioned in the algorithm is always 1 when the CM order has discriminant $\mathfrak{f}^2\Delta_K = \Delta < -4$, and otherwise can be at most 3. Algorithm 1.3 has been implemented, and is publicly available at [Rep] along with Magma code for all other computations described in this thesis.

In §2, we begin with relevant background and prior results on CM points on the Shimura curves of interest. We then provide results on concrete decompositions of QM abelian surfaces with CM as products of CM elliptic curves in §3, with the original results here being Theorem 3.4 and Corollary 3.5.

We then begin the work necessary for implementation of Algorithm 1.3. In §4.1 and §4.2, we consider QM-equivariant isogenies and the QM-equivariant ℓ-isogeny graph $\mathcal{G}_\ell^D$. We prove in Theorem 4.2.5 that a CM component of this graph for a prime ℓ and quaternion discriminant D has the structure of an ℓ-volcano for CM discriminant $\Delta < -4$. (We handle the slight deviation from the structure of an ℓ-volcano in the $\Delta \in \{-3, -4\}$ case in Proposition 4.4.1.)

We study the action of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ on such components in §4.3, allowing for an enumeration of closed point equivalence classes of paths in these graphs and hence a description the CM locus on a prime-power level Shimura curve $X_0^D(\ell^a)_{/\mathbb{Q}}$ as provided in §5.1. The algebraic results of §5.2 then feed into a description of the CM locus on $X_0^D(N)_{/\mathbb{Q}}$ for general level N coprime to D provided in §5.3, which provides Algorithm 1.3.

The ability to transition to information about the $\mathfrak{o}$-CM locus on $X_1^D(N)_{/\mathbb{Q}}$ is explained in §5.4, in which we prove the following result:

Theorem 1.4. *Suppose that $x \in X_0^D(N)_{/\mathbb{Q}}$ is a point with CM by the imaginary quadratic order of discriminant Δ. Let $\pi : X_1^D(N)_{/\mathbb{Q}} \to X_0^D(N)_{/\mathbb{Q}}$ denote the natural morphism.*

1. *If $\Delta < -4$, then π is inert over x.*

2. *Suppose that $\Delta \in \{-3, -4\}$.*

   (a) *If x is a ramified point of the map $X_0^D(N)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ or if $N \leq 3$, then π is inert over x.*

   (b) *Otherwise, we have*

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

   for the ramification index and residual degree of x, respectively, with respect to π.

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

Our work allows for a determination of all primitive residue fields and primitive degrees of $\mathfrak{o}$-CM points on $X_0^D(N)_{/\mathbb{Q}}$, as discussed in §5.3.3. Here, by a primitive residue field (respectively, degree) of $\mathfrak{o}$-CM points on $X_0^D(N)_{/\mathbb{Q}}$ we mean one that does not properly contain (respectively, does not properly divide) that of another $\mathfrak{o}$-CM point on the same curve. An abridged version of the main result here is as follows, with Theorem 5.3.3 providing the complete result:

Theorem 1.5. *Let $\mathfrak{o}(\mathfrak{f})$ denote the order of conductor $\mathfrak{f}$ in an imaginary quadratic field K, and let B denote the indefinite rational quaternion algebra of discriminant D. Suppose that K splits B, and that N is a positive integer relatively prime to D, with prime-power factorization $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. Then one of the following occurs:*

1. *There is a unique primitive residue field L of $\mathfrak{o}(\mathfrak{f})$-CM points on $X_0^D(N)_{/\mathbb{Q}}$, with L an index 2, totally complex subfield of a ring class field $K(Hf)$ for some $H \mid N$.*

2. *There are exactly 2 primitive residue fields of such points, with one of the same form as L in part (1) and the other being a ring class field of the form $K(Cf)$ with $C < B$.*

Knowledge of all primitive degrees provides the ability to compute the *least* degree $d_{\mathfrak{o},\mathrm{CM}}(X_0^D(N))$ of an $\mathfrak{o}$-CM point on $X_0^D(N)_{/\mathbb{Q}}$ for any imaginary quadratic order $\mathfrak{o}$. In §5.5, we discuss minimizing over orders $\mathfrak{o}$ to compute the least degree $d_{\mathrm{CM}}(X_0^D(N))$ of a CM point on $X_0^D(N)_{/\mathbb{Q}}$, and Proposition 5.5.1 allows one to transition from this to computations of least degrees of CM points on $X_1^D(N)_{/\mathbb{Q}}$.

A closed point x on a curve $X_{/\mathbb{Q}}$ is said to be **sporadic** if there are finitely many points y on $X_{/\mathbb{Q}}$ with $\deg(y) \leq \deg(x)$. We apply our least degree computations towards the existence of sporadic CM points on $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$ with the following as an abridged version of the end result (see Theorem 5.5.9):

Theorem 1.6. *Let $\mathcal{F}$ be the set of all 455 pairs (D, N) appearing in Tables 5.2 and 5.3. If $(D, N) \notin \mathcal{F}$ consists of a rational quaternion discriminant $D > 1$ and a positive integer N which is relatively prime to D, then $X_0^D(N)_{/\mathbb{Q}}$ has a sporadic CM point. If we have such a pair (D, N) with*

$$(D, N) \notin \mathcal{F} \cup \{(91, 5)\},$$

then $X_1^D(N)_{/\mathbb{Q}}$ has a sporadic CM point.

Our work determining residue fields of CM points on $X_0^D(N)_{/\mathbb{Q}}$ can be viewed as a generalization of prior work on the Diophantine arithmetic of Shimura curves via an alternate approach (specifically work of Jordan [Jor81] and González–Rotger [GR06] – see Theorem 2.3.6). Of course, our results are also aimed towards better understanding the torsion of low-dimensional abelian varieties over number fields, via restriction to a case with extra structure. On this point, the question of which number fields admit abelian surfaces with certain specified rational torsion subgroups is closely related to our results, just as in the elliptic modular case. A result of Jordan (see Theorem 2.3.3) clarifies this relationship.

Unlike the elliptic modular curves $X_0(N)_{/\mathbb{Q}}$, the curves $X_0^D(N)_{/\mathbb{Q}}$ for $D > 1$ have no cuspidal points. For this reason, understanding the CM points and, more generally, low degree points on Shimura curves may be of greater interest. Additionally, while our approach is in analogy to that of [Cl23] and [CS23] in the elliptic modular case, there are interesting deviations and difficulties arising in this work due to technical differences in the $D > 1$ case.

For example, fields of moduli are *not* necessarily fields of definition in the case of QM abelian surfaces, as noted in Jordan's Theorem 2.3.3. Further, while the field of moduli $\mathbb{Q}(x)$ of any CM point $x \in X(1)_{/\mathbb{Q}}$ has a real embedding, a result of Shimura (see Theorem 2.3.5) states that $X^D(1)_{/\mathbb{Q}}$ has *no real points* for $D > 1$. This fact is inherent in fundamental differences between our general study and the $D = 1$ case. It also opens the door for the potential of Hasse principal violations by Shimura curves, which has been a subject of significant study (see [Cl09, CSt18, RSY05]). If one aims to study the Hasse principle for Shimura curves over some fixed number field (respectively, over a fixed degree), then studying the CM points rational over that field (respectively, over number fields of that degree) seems to be a natural initial point of investigation, and so our results may be of interest in that direction.

Chapter 2

Background

2.1 Shimura curves

2.1.1 Modular curves

Prior to jumping to Shimura curves in general, we mention some things about the possibly more familiar setting of elliptic modular curves, with [DS05, §2] serving as a reference. First, we recall the familiar action of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ on the complex upper half plane $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ via linear fractional transformations: for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ and $z \in \mathbb{H}$, we have

$$\gamma \cdot z = \frac{az + b}{cz + d}.$$

For a given $z \in \mathbb{H}$, we have an elliptic curve $E_z := \mathbb{C}/\Lambda_z$, where $\Lambda_z =< 1, z >$ is the rank 2 lattice in $\mathbb{C}$ generated by 1 and z. Homothetic lattices yield isomorphic elliptic curves, such that any elliptic curve is isomorphic to one of this form, and moreover we have a bijective correspondence

$$\Gamma(1)\backslash\mathbb{H} \leftrightarrow \{\text{elliptic curves } E/\mathbb{C}\}/\cong .$$

That is, $E_z \cong E'_z$ if and only if $z = \gamma z'$ for some $\gamma \in \Gamma(1)$. This gives us our first instance of a classical modular curve over $\mathbb{C}$, denoted $Y(1) := \Gamma(1)\backslash\mathbb{H}$. The compactification $X(1) := \Gamma(1)\backslash\mathbb{H}^*$ has a single additional "cuspidal" point, which one can interpret as corresponding

to the isomorphism class of a nodal cubic curve. Via the j-invariant, we have $X(1) \cong \mathbb{P}^1_{\mathbb{C}}$, and one often refers to $X(1)$ as the "the j-line."

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

$$\Gamma(N) := \left\{ \gamma \in \Gamma(1) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

be the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ given by reduction modulo N . We call $H \leq \Gamma(1)$ a **congruence subgroup** if $\Gamma(N) \leq H$ for some $N \in \mathbb{Z}^+$, and given such a Γ we define

$$Y_H := H\backslash\mathbb{H} \quad \text{and} \quad X_H := H\backslash\mathbb{H}^*.$$

For $H \leq H'$ congruence subgroups, we then have a natural quotient map $Y_H \to Y_{H'}$ and $X_H \to X_{H'}$ of degree ([DS05, §3.1])

$$[\{\pm I\}H' : \{\pm I\}H] = \begin{cases} \dfrac{[H' : H]}{2} & \text{if } -I \in H' \text{ and } -I \notin H, \\ [H' : H] & \text{otherwise.} \end{cases}$$

In particular, we have natural maps from any X_H to the j-line $X(1)$, and hence can consider the fiber over any $j \in X(1)$. The points in this fiber have a moduli interpretation, corresponding to isomorphism classes of elliptic curves E, with $j(E) = j$, equipped with extra torsion structure which we may refer to as "H-level structure."

For instance, the curve $Y_{\Gamma(N)}$ has a moduli interpretation as parametrizing triples (E, P, Q) as follows: E is an elliptic curve over $\mathbb{C}$, and P and Q are points of order N on E such that the N-torsion $E[N]$ of E is generated by P and Q and such that, with

$$e_N : E[N] \times E[N] \to \mu_N$$

denoting the Weil pairing, we have $e_N(P, Q) = e^{2\pi i/N}$ ([DS05, p. 38]). In other words, this modular curve parametrizes elliptic curves with full level-N structure in this specific sense.

We mention here two other classical families of modular curves which will be especially relevant to us in this work: consider the congruence subgroups

$$\Gamma_0(N) := \left\{ \gamma \in \Gamma(1) \mid \gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{N} \right\}, \text{and}$$
$$\Gamma_1(N) := \left\{ \gamma \in \Gamma(1) \mid \gamma \equiv \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \pmod{N} \right\}.$$

We then have the following

Proposition 2.1.1. *1. The modular curve $Y_0(N) := Y_{\Gamma_0(N)}$ has $Y_0(N)(\mathbb{C})$ in bijective correspondence with the set of isomorphism classes of pairs (E, C) where E is an elliptic curve over $\mathbb{C}$ and $C \leq E[N]$ is a cyclic subgroup of order N.*

2. The modular curve $Y_1(N) := Y_{\Gamma_1(N)}$ has $Y_1(N)(\mathbb{C})$ in bijective correspondence with the set of isomorphism classes of pairs (E, P) where E is an elliptic curve over $\mathbb{C}$ and $P \in E[N]$ is a point of order N.

3. We have natural modular maps

$$Y_1(N) \xrightarrow{\pi_1} Y_0(N) \xrightarrow{\pi_0} Y(1)$$
$$[E, P] \mapsto [E, \langle P \rangle] \mapsto [E],$$

with $\deg(\pi_1) = max\left\{\frac{\phi(N)}{2}, 1\right\}$ and $\deg(\pi_0) = \psi(N)$, where ϕ denotes the Euler totient function and ψ denotes the Dedekind ψ function, that is the multiplicative function defined by

$$\psi(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

At this point, we have defined algebraic curves Y_H and X_H over $\mathbb{C}$ associated to a congruence subgroup H. In fact, for our families of interest we have models $Y_0(N)_{/\mathbb{Q}}$ and $Y_1(N)_{/\mathbb{Q}}$ (and similarly for the compactified versions) over the rationals which preserve the moduli interpretations mentioned above and are isomorphic to the defined complex curves

upon base change to $\mathbb{C}$. We will work with these rational models in this work, as we aim to study abelian varieties with torsion data over number fields. More generally, for a congruence subgroup H with $\Gamma(N) \leq H$, we have a model $Y_{H/\mathbb{Q}}$ which in general may not be geometrically connected, while there exists a nice model over the cyclotomic field $\mathbb{Q}(\zeta_N)$.

2.1.2 Quaternion algebras

Our transition from elliptic modular curves to the families of Shimura curves we are studying will involve a transition from considering the action of the split quaternion algebra $M_2(\mathbb{Q})$ over $\mathbb{Q}$ on the upper half plane $\mathbb{H}$, to considering that of an arbitrary indefinite quaternion algebra over $\mathbb{Q}$. We review here the basics we will need in quaternion arithmetic, all of which and more can be found in the classic [Vig80] as well as in the more modern treatment [Voi21].

Throughout this section, F will denote a field with $\mathrm{char}(F) \neq 2$. We call an F-algebra **simple** if it has no proper, non-trivial two-sided ideals. A **central simple algebra** over F is a finite dimensional associative F-algebra which is simple and has center equal to F. A **quaternion algebra** over F is a central simple algebra over F of dimension 4. Every quaternion algebra B over F has a presentation $B = \left(\frac{a,b}{F}\right)$ for some $a, b \in F^\times$, where $\left(\frac{a,b}{F}\right)$ denotes the F-algebra with generators α and β such that ([Voi21, Cor. 7.1.2])

$$\alpha^2 = a,\ \beta^2 = b, \quad \text{and } \alpha\beta = -\beta\alpha.$$

The Wedderburn–Artin Theorem ([Wed08, Art26], see also [Voi21, Thm. 7.3.10]) gives that any central simple algebra over F is isomorphic to a matrix algebra over a division ring, and so in the dimension 4 case it is forced that a quaternion algebra over F is either isomorphic to $M_2(F)$ or is itself a division algebra. As an example, in the case of $F = \mathbb{R}$ there are exactly two quaternion algebras over $\mathbb{R}$ up to isomorphism: we have the split quaternion algebra $M_2(\mathbb{R})$, and the Hamilton quaternions $\left(\frac{-1,-1}{\mathbb{R}}\right)$.

For B a quaternion algebra over F, we have a unique anti-involution $\alpha \mapsto \overline{\alpha}$ on B such that $\alpha\overline{\alpha} \in F$ for all $\alpha \in B$. Concretely, if $B = \left(\frac{a,b}{F}\right)$, then

$$\overline{x + y\alpha + z\beta + w\alpha\beta} = x - y\alpha - z\beta - w\alpha\beta.$$

We define the **reduced norm** on B to be the map

$$\begin{aligned} \mathrm{nrd} : & B \to F \\ & \alpha \mapsto \alpha\overline{\alpha}. \end{aligned}$$

The quaternion algebras relevant to our study will all be over $\mathbb{Q}$, so let us specify to the case of F a number field. For v a place of F, let F_v denote the completion of F at v and let

$$B_v := B \otimes_F F_v.$$

We say that B is **split** at v if $B_v \cong M_2(F_v)$, and we say that B is **ramified** at v if B_v is a division algebra over F_v. The set $\mathrm{Ram}(B)$ of places at which B is ramified is finite and of even cardinality, and we define the **discriminant of** B to be the product of all these places:

$$\mathrm{disc}(B) := \prod_{v \in \mathrm{Ram}(B)} v.$$

Two quaternion algebras B and B' over F are isomorphic if and only if $\mathrm{disc}(B) = \mathrm{disc}(B')$. We will let B_D denote the quaternion algebra over F of discriminant D, when F is understood from context.

Specifying to the case $F = \mathbb{Q}$, we will call B over $\mathbb{Q}$ **definite** if it is ramified at ∞, i.e., if

$$B \otimes_{\mathbb{Q}} \mathbb{R} \cong \left(\frac{-1,-1}{\mathbb{R}}\right),$$

and we will call B **indefinite** if it is split at ∞, i.e., if

$$B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}).$$

We then have the following bijections:

$$\left\{\begin{smallmatrix}\text{indefinite quaternion}\\ \text{algebras over } \mathbb{Q}\end{smallmatrix}\right\} / \cong \longleftrightarrow \left\{\begin{smallmatrix}\text{even cardinality sets of}\\ \text{rational prime numbers}\end{smallmatrix}\right\}, \text{ and}$$
$$\left\{\begin{smallmatrix}\text{definite quaternion}\\ \text{algebras over } \mathbb{Q}\end{smallmatrix}\right\} / \cong \longleftrightarrow \left\{\begin{smallmatrix}\text{odd cardinality sets of}\\ \text{rational prime numbers}\end{smallmatrix}\right\},$$

where in each case the isomorphism class of the quaternion algebra B_D corresponds to the set of finite primes dividing D.

An **order** of a $\mathbb{Q}$-algebra B of finite dimension is a lattice in B (that is, a full-rank $\mathbb{Z}$-submodule of B) which is a subring of B. A **maximal order** is one which is maximal with respect to containment, i.e., is not properly contained in another order. There exists a maximal order in every such B, and moreover every order in B is contained in a maximal order [Voi21, Prop. 15.5.2].

We also define an **Eichler order** to be an order in B which is the intersection of two maximal orders. If $\mathcal{O}'$ is an Eichler order contained in a maximal order $\mathcal{O}$, then the quantity $[\mathcal{O} : \mathcal{O}']$ is independent of the choice of $\mathcal{O}$ containing $\mathcal{O}'$ and we refer to it as the **level** of $\mathcal{O}'$ ([Voi21, §23.4.19]). A maximal order is then an Eichler order of level 1. In the theory of Shimura curves, Eichler orders serve the purpose of providing certain level structure. That said, we will work almost exclusively with maximal orders in this work, and will only refer to Eichler orders in commenting on how our approach to level structure compares to an alternate approach (see Remark 2.3.7).

Example 2.1.2. The order $M_2(\mathbb{Z})$ in the split quaternion algebra $M_2(\mathbb{Q})$ is a maximal order, and in fact any maximal order in $M_2(\mathbb{Q})$ is conjugate to $M_2(\mathbb{Z})$. For every $N \in \mathbb{Z}^+$, the order

$$\mathcal{O}_N := \left\{ \gamma \in M_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \pmod{N} \right\}$$

is an Eichler order of level N.

2.1.3 Shimura curves

For the remainder of this work, we will let B denote the indefinite quaternion algebra of discriminant D over $\mathbb{Q}$, and will fix a maximal order $\mathcal{O}$ in B. As B is indefinite, i.e., split at the infinite place, we have an isomorphism

$$\Psi : B \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R}).$$

We will also fix, using the terminology of [Voi21, §43.1], a **principal polarization** on $\mathcal{O}$. By this, we mean an element $\mu \in \mathcal{O}$ satisfying $\mu^2 + D = 0$, which induces the involution

$$\alpha \mapsto \alpha^* := \mu^{-1}\alpha\mu$$

on $\mathcal{O}$.

We start by defining the moduli spaces we are considering, and discussing the moduli interpretations of those families of particular interest to us in this study. The main source here is the foundational work of Shimura [Sh67]. Let $\mathcal{O}^1$ denote the units of reduced norm 1 in $\mathcal{O}$, which we realize as embedded in $\mathrm{SL}_2(\mathbb{R})$ via Ψ. The subgroup $\Gamma^D(1) := \Psi(\mathcal{O}^1) \subset \mathrm{SL}_2(\mathbb{R})$ is discrete, and is cocompact if and only if $D > 1$. Via the action of this subgroup on the upper-half plane $\mathbb{H}$ we define over $\mathbb{C}$ the Shimura curve

$$X^D(1) = X_{\Gamma^D(1)} := \Gamma^D(1)\backslash\mathbb{H}.$$

In the $D = 1$ case of $B \cong M_2(\mathbb{Q})$, we have that $\Gamma^1(1)$ is conjugate to $\mathrm{SL}_2(\mathbb{Z})$ and recover the elliptic modular setting; $X^1(1) \cong Y(1) \cong \mathbb{A}^1_{\mathbb{C}}$. For $D > 1$, we have that $X^D(1)$ is a compact Riemann surface. For any $z \in \mathbb{H}$, we get a rank 4 lattice Λ_z via the action of $\mathcal{O}$ on $\langle 1, z\rangle \in \mathbb{C}^2$ via the embedding Ψ above:

$$\Lambda_z := \mathcal{O} \cdot \langle 1, z\rangle \subseteq \mathbb{C}^2.$$

From this we obtain a complex torus

$$A_z := \mathbb{C}^2/\left(\mathcal{O} \cdot \langle 1, z\rangle\right)$$

of dimension 2, which comes equipped with an $\mathcal{O}$-action $\iota_z : \mathcal{O} \hookrightarrow \mathrm{End}(A_z)$. We require some rigidification data, namely a Riemann form, in order to recognize A_z as an abelian surface. It turns out that we always obtain such data in this setting; there is a *unique* principal polarization $\lambda_{z,\mu}$ on A_z such that the Rosati invoution on $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$ agrees with the involution induced by our polarization μ on $\psi(\mathcal{O})$ [Voi21, Lemma 43.6.23].

Definition 2.1.3. An $(\mathcal{O}, \mu)$**-QM abelian surface** over F is a triple (A, ι, λ) consisting of an abelian surface A over F, an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$ which we will refer to as the **quaternionic multiplication (QM) structure**, and a polarization λ on A such that the following diagram is commutative

$$\begin{array}{ccc} B & \xrightarrow{\iota} & \mathrm{End}^0(A) \\ \downarrow{\scriptstyle *} & & \downarrow{\scriptstyle \dagger} \\ B & \xrightarrow{\iota} & \mathrm{End}^0(A) \end{array}$$

where $\dagger$ denotes the Rosati involution corresponding to λ.

With this definition, we have moreover that $X^D(1)$ is the coarse moduli space of $(\mathcal{O}, \mu)-$QM abelian surfaces over $\mathbb{C}$, with the association $z \mapsto [(A_z, \iota_z, \lambda_{z,\mu})]$ [Voi21, Main Theorem 43.6.14].

Remark 2.1.4. For an abelian variety A over a field F, by $\mathrm{End}(A)$ we mean the ring of endomorphisms defined over the base field F. For an extension $F \subseteq L$, we set $A_{/L} := A \otimes_{\mathrm{Spec}F} \mathrm{Spec}L$ and put

$$\mathrm{End}_L(A) := \mathrm{End}(A_{/L}).$$

More generally, if $\Gamma \leq \Gamma^D(1) \subseteq \mathrm{SL}_2(\mathbb{R})$ has finite index in $\Gamma^D(1)$, we can consider the curve $X_\Gamma = \Gamma\backslash\mathbb{H}$, and for $\Gamma' \leq \Gamma$ there is a corresponding covering of curves $X_{\Gamma'} \to X_\Gamma$.

Our focus will be on the families of Shimura curves $X_0^D(N)$ and $X_1^D(N)$, for N a positive integer with $\gcd(D,N)=1$, with $X^D(1)=X_0^D(1)=X_1^D(1)$ being a special case of each. In these cases, a substantial result of Shimura [Sh67, Main Theorem I] concerning models of Shimura curves in provides that we have canonical rational models $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$. That is, such that

$$X_0^D(N)_{/\mathbb{Q}} \otimes_{\mathrm{Spec}\mathbb{Q}} \mathrm{Spec}\mathbb{C} \cong X_0^D(N)$$

and simiarly for $X_1^D(N)_{/\mathbb{Q}}$.

Following the careful exposition of [Buz97], let

$$R := \varprojlim_{\gcd(m,D)=1} \mathbb{Z}/m\mathbb{Z}$$

and fix an isomorphism $\kappa : \mathcal{O} \otimes_{\mathbb{Z}} R \to M_2(R)$. This map κ induces, for m relatively prime to D, a map

$$u_m : \mathcal{O} \otimes \widehat{\mathbb{Z}} \to \mathrm{Gl}_2\left(\mathbb{Z}/m\mathbb{Z}\right).$$

The curve $X_0^D(N)$ can then be described as the Shimura curve corresponding to the compact, open subgroup

$$u_N^{-1}\left(\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(\mathbb{Z}/N\mathbb{Z}) \mid c=0\right\}\right) \leq \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}.$$

Equivalently, fixing a level N Eichler order $\mathcal{O}_N$ in B, the curve $X_0(N)$ can be described, in the manner mentioned above, as that associated to the arithmetic group of units of reduced norm 1 in $\mathcal{O}_N$. The Shimura curve $X_1^D(N)$ is that corresponding to the compact, open subgroup

$$u_N^{-1}\left(\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Gl}_2(\mathbb{Z}/N\mathbb{Z}) \mid c=0 \text{ and } d=1\right\}\right) \leq \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}},$$

For N coprime to our quaternion discriminant D, the notion of "level N-structure" is group-theoretically just as in the elliptic modular case. In particular, we have a natural modular covering map $X_1^D(N) \to X_0^D(N)$ which is an isomorphism for $N \leq 2$, and has

degree $\phi(N)/2$ for $N \geq 3$. We continue to assume that N and D are coprime through this study. We now provide moduli interpretations for these families of Shimura curves as in [Cl03, §0.3.2].

Definition 2.1.5. Suppose that (A, ι, λ) and (A', ι', λ') are $(\mathcal{O}, \mu)$-QM abelian surfaces over F, we will call an isogeny $\varphi : A \to A'$ of the underlying abelian surfaces a **QM-cyclic N-isogeny** if it respects the polarizations and both of the following hold:

- The isogeny φ is QM-equivariant. That is, for all $\alpha \in \mathcal{O}$ we have

$$\iota'(\alpha) \circ \varphi = \varphi \circ \iota(\alpha).$$

- The kernel $\ker(\varphi)$ is a cyclic $\mathcal{O}$-module, with underlying $\mathbb{Z}$-module structure

$$\ker(\varphi) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

Proposition 2.1.6. *Let D be a rational quaternion discriminant and $N \in \mathbb{Z}^+$ coprime to D. The Shimura curve $X_0^D(N)$ is the coarse moduli space for any of the following moduli problems:*

1. *tuples (A, ι, λ, Q), where $(A, \iota, \lambda)/\mathbb{C}$ is an $(\mathcal{O}, \mu)$-QM abelian surface and $Q \leq A[N]$ is an order N^2 subgroup of the N-torsion subgroup of A which is stable under the action of $\mathcal{O}$.*

2. *QM-cyclic N-isogenies $\varphi : (A, \iota, \lambda) \to (A, \iota', \lambda')$ of $(\mathcal{O}, \mu)$-QM abelian surfaces.*

The curve $X_1^D(N)$ is in general the coarse moduli space for the following moduli problem: triples (A, ι, λ, P), where $(A, \iota, \lambda)/\mathbb{C}$ is a QM abelian surface and $P \in A[N]$ is a point of order N.

Because these interpretations hold for any choice of principal polarization μ of $\mathcal{O}$, and because a principal polarization λ on a pair (A, ι) is canonically determined from a fixed μ, moving forward we will suppress polarizations and refer simply to QM abelian surfaces (A, ι).

It is important to recognize that rigidification is lurking in the background, though, as it is essential in the initial formulation of our moduli problem.

Remark 2.1.7. Letting $\mathcal{O}_N$ denote an Eichler order of level N in B, the curve $X_0^D(N)$ has the equivalent interpretation of parametrizing pairs (A, ι) where $A/\mathbb{C}$ is a QM abelian surface and $\iota : \mathcal{O}_N \hookrightarrow \mathrm{End}(A)$. That said, interpretations (1) and (2) in Proposition 2.1.6 will be the primary ones used in our study (see Remark 2.3.7 for related comments). Thus, we will mainly speak of QM by maximal quaternion orders, and it will benefit us to spell out the connection between interpretations (1) and (2) here. Let (A, ι) be a QM abelian surface. The N-torsion of A is acted on by $\iota(\mathcal{O})$, and the corresponding representation factors through $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z} \cong M_2(\mathbb{Z}/N\mathbb{Z})$. The resulting map must then be equivalent to

$$M_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{End}(A[N]) \cong M_4(\mathbb{Z}/N\mathbb{Z})$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} a & 0 & b & 0 \\ 0 & a & 0 & b \\ c & 0 & d & 0 \\ 0 & c & 0 & d \end{pmatrix}.$$

This can be viewed as a case of Morita equivalence, but it is worth being explicit here: let e_1 and e_2 denote the standard idempotents in $M_2(\mathbb{Z}/N\mathbb{Z})$,

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

We then have $A[N] = e_1(A[N]) \oplus e_2(A[N])$, and $M_2(\mathbb{Z}/N\mathbb{Z})$ acts on this direct sum in precisely the way noted by the above map.

Any proper, nontrivial, $\mathcal{O}$-stable subgroup $Q \leq A[N]$ must then have order N^2 (this justifies our definition of QM-cyclic isogenies, along with the equivalence of the moduli interpretations presented above). Further, such a subgroup Q is determined by the cyclic

order N subgroup of $A[N]$: we have $Q = e_1(Q) \oplus e_2(Q)$ where each summand is cyclic of order N, and conversely $Q = \mathcal{O} \cdot e_i(Q)$ for $i = 1, 2$.

For our applications in §5.5, the genera of our Shimura curves of interest will be of use. The derivation of the following formula for the genus of $X_0^D(N)$ can be found in many locations, such as [Voi21, Thm. 39.4.20]:

Proposition 2.1.8.

$$g(X_0^D(N)) = 1 + \frac{\phi(D)\psi(N)}{12} - \frac{\epsilon_1(D,N)}{4} - \frac{\epsilon_3(D,N)}{3},$$

where

$$\epsilon_1(D,N) = \begin{cases} \prod_{p|D}\left(1 - \left(\frac{-4}{p}\right)\right)\prod_{p|N}\left(1 + \left(\frac{-4}{p}\right)\right) & \text{if } 4 \nmid N \\ 0 & \text{if } 4 \mid N \end{cases}$$

$$\epsilon_3(D,N) = \begin{cases} \prod_{p|D}\left(1 - \left(\frac{-3}{p}\right)\right)\prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right) & \text{if } 9 \nmid N \\ 0 & \text{if } 9 \mid N \end{cases}$$

are the numbers of elliptic $\mathbb{Z}[\sqrt{-1}]$-CM and elliptic $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$-CM points on $X_0^D(N)_{/\mathbb{Q}}$, respectively.

In the $D > 1$ case, a formula for the curve attached to a general finite index subgroup $\Gamma \leq \Gamma^D(1)$ seems harder to find in the literature, so we provide a derivation here:

Proposition 2.1.9. *Let $D > 1$ be an indefinite rational quaternion discriminant and $\Gamma \leq \Gamma^D(1)$ be a finite index subgroup, with $\pi : X_\Gamma \to X^D(1)$ the natural modular map. Let $d = deg(\pi)$, and let $\epsilon_1(\Gamma)$ and $\epsilon_3(\Gamma)$ denote the total number of elliptic points on $X(\Gamma)$ of order 2 and of order 3, respectively. We then have*

$$g(X_\Gamma) = 1 + \frac{d\phi(D)}{12} - \frac{\epsilon_1(\Gamma)}{4} - \frac{\epsilon_3(\Gamma)}{3}.$$

Proof. For a point $P \in X^D(1)$, let e_P denote the ramification index of P with respect to π. The Riemann–Hurwitz formula provides

$$2g(X_\Gamma) - 2 = d(2g(X^D(1)) - 2) + \sum_{P \in X^D(1)} (e_P - 1)\,.$$

We know that P is unramified with respect to π, that is, $e_P = 1$, unless possibly if P is an elliptic point on $X^D(1)$. For an elliptic point P on $X^D(1)$, we have $e_P = 1$ exactly if the points on X_Γ lying over P remain elliptic, and $e_P \in \{2, 3\}$ otherwise. We then have

$$\sum_{P \in X^D(1)} (e_P - 1) = \frac{d \cdot \epsilon_1(D,1) - \epsilon_1(\Gamma)}{2} + \frac{2(d \cdot \epsilon_3(D,1) - \epsilon_3(\Gamma))}{3}.$$

Hence, we find

$$\begin{aligned} 2g(X_\Gamma) - 2 &= d(2g(X^D(1)) - 2) + \frac{d \cdot \epsilon_1(D,1) - \epsilon_1(\Gamma)}{2} + \frac{2(d \cdot \epsilon_3(D,1) - \epsilon_3(\Gamma))}{3} \\ &= \frac{d\phi(D)}{6} - \frac{d \cdot \epsilon_1(\Gamma)}{2} - \frac{2d \cdot \epsilon_3(\Gamma)}{3}, \end{aligned}$$

which provides the stated equality. □

Example 2.1.10. Consider the case of $\Gamma = \Gamma_0^D(N)$. Here, the degree of the map $X_0^D(N) \to X^D(1)$ is $d = \psi(N)$. Let ν_1 and ν_3 denote, respectively, the number of order 2 and order 3 elliptic points on X_Γ lying over a given elliptic point of the same order on $X^D(1)$[1]. We then have $\nu_1 = \frac{\epsilon_1(D,N)}{\epsilon_1(D,1)}$ and $\nu_3 = \frac{\epsilon_3(D,N)}{\epsilon_3(D,1)}$, and, for a fixed elliptic point Q on $X^D(1)$,

$$\sum_{P \in \pi^{-1}(Q)} (e_P - 1) = \begin{cases} \dfrac{d - \nu_1}{2} & \text{if } Q \text{ is elliptic of order 2,} \\ \\ \dfrac{2(d - \nu_3)}{3} & \text{if } Q \text{ is elliptic of order 3.} \end{cases}$$

With this, we recover the stated formula of Proposition 2.1.8.

[1]The quantities ν_1 and ν_3 are well defined here; each of the ϵ_h fibers of π above elliptic points of order $h = 1$ and $h = 3$ are isomorphic via Atkin–Lehner involutions ω_p for primes $p \mid D$ which are inert in, respectively, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{3})$.

Example 2.1.11. Let $\Gamma = \Gamma_1^D(N)$ be the congruence subgroup corresponding to the Shimura curve $X_1^D(N)$. For $N \leq 2$, we have $X_1^D(N) \cong X_0^D(N)$, such that Proposition 2.1.8 applies. For $N \geq 3$, this curve has no elliptic points, so $\epsilon_1(\Gamma_1^D(N)) = \epsilon_3(\Gamma_1^D(N)) = 0$, and the degree of the natural map $X_1^D(N) \to X^D(1)$ is $d = \dfrac{\phi(N)\psi(N)}{2}$. We then find

$$g(X_1^D(N)) = 1 + \frac{\phi(N)\phi(D)\psi(N)}{24}.$$

More generally, for any Γ with X_Γ having no elliptic points we note that

$$g(X_\Gamma) = 1 + \frac{d\phi(D)}{12}.$$

2.2 Complex multiplication

2.2.1 Elliptic curves and complex multiplication

Let K be number field and let $\mathfrak{o}$ be an order in K, i.e., a finite index subring of the full ring of integers $\mathfrak{o}_K$ in K Letting $f = [\mathfrak{o}_K : \mathfrak{o}]$ denote this index, and letting Δ and Δ_K, respectively, denote the discriminants of $\mathfrak{o}$ and of $\mathfrak{o}_K$, we have the relation

$$\Delta = f^2 \Delta_K.$$

By a **fractional $\mathfrak{o}$-ideal**, we mean a subset of K which is nonzero and is finitely generated as an $\mathfrak{o}$-module, from which it follows that it is of the form $\alpha\mathfrak{a}$ for some $\alpha \in K^*$ and some $\mathfrak{o}$-ideal $\mathfrak{a}$ in K.

We let $I(\mathfrak{o})$ denote the group of invertible fractional $\mathfrak{o}$-ideals in K under multiplication of ideals. This commutative group has as a subgroup the group $P(\mathfrak{o})$ of principal $\mathfrak{o}$-ideals in K, and we define the **Picard group** of $\mathfrak{o}$ to be

$$\mathrm{Pic}(\mathfrak{o}) := I(\mathfrak{o})/P(\mathfrak{o}).$$

The **class number** of the order $\mathfrak{o}$ is the size $h(\mathfrak{o}) := |\mathrm{Pic}(\mathfrak{o})|$ of this finite group. By the existence theorem of global class field theory, there is a canonical finite abelian extension $K(\mathfrak{o})/K$ such that

$$\mathrm{Gal}(K(f)/K) = \mathrm{Pic}(\mathfrak{o}).$$

We call $K(\mathfrak{o})$ the **ring class field** of $\mathfrak{o}$. The case of $H = K(\mathfrak{o}_K)$ recovers the Hilbert class field of K, by which we mean that maximal unramified abelian extension of K. If $\mathfrak{o} \subseteq \mathfrak{o}'$ are orders in K, then this inclusion induces an inclusion $K(\mathfrak{o}') \subseteq K(\mathfrak{o})$ in the reverse direction, and a surjection $\mathrm{Pic}(\mathfrak{o}) \to \mathrm{Pic}(\mathfrak{o}')$ corresponding to the map $\mathfrak{a} \mapsto \mathfrak{a} \cdot \mathfrak{o}'$ on fractional ideals.

We now restrict to the case of K an imaginary quadratic field. Here, the study of orders in K is relatively simple: an order $\mathfrak{o}$ in K is uniquely determined up to isomorphism not only by its discriminant but also by its conductor $\mathfrak{f} := [\mathfrak{o}_K : \mathfrak{o}]$, with

$$\mathfrak{o}(\mathfrak{f}) := \mathbb{Z} + \mathfrak{f}\mathfrak{o}_K$$

providing the order of conductor $\mathfrak{f}$ for any $\mathfrak{f} \in \mathbb{Z}^+$. In this setting, we will use the notation $K(\mathfrak{f}) := K(\mathfrak{o}(f))$ to denote the ring class field of the order of conductor $\mathfrak{f}$. We also have alternate descriptions of the class group in this setting, and the following interpretation in particular will be useful to us. For K an imaginary quadratic field, denote by $I_K(\mathfrak{f}) \leq I(\mathfrak{o}_K)$ the subgroup generated by $\mathfrak{o}_K$-ideals prime to $\mathfrak{f}$, and let $P_{K,\mathbb{Z}}(\mathfrak{f}) \leq I_K(\mathfrak{f})$ be the subgroup generated by principal ideals of the form $\alpha \cdot \mathfrak{o}_K$ where $\alpha \in \mathfrak{o}_K$ satisfies $\alpha \equiv a \pmod{\mathfrak{f} \cdot \mathfrak{o}_K}$ for some $a \in \mathbb{Z}$ relatively prime to $\mathfrak{f}$. We then have the following [Cox13, Prop. 7.22]:

Proposition 2.2.1. *Let K be an imaginary quadratic field. There is then a natural isomorphism*

$$\mathrm{Pic}(\mathfrak{o}(\mathfrak{f})) \cong I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f})$$
$$\mathfrak{a} \mapsto \mathfrak{a} \cdot \mathfrak{o}_K,$$

Let ω_K denote the number of units in $\mathfrak{o}_K$. Concretely:

$$\omega_K := \#\mathfrak{o}_K^\times = \begin{cases} 2 & \text{if } \Delta < -4 \\ 4 & \text{if } \Delta = -4 \\ 6 & \text{if } \Delta = -3\,, \end{cases}$$

The following proposition and its corollary provide explicit relative class number formulae for imaginary quadratic orders (see [Cox13, Cor. 7.28]):

Proposition 2.2.2. *For a fixed imaginary quadratic field K, let $\mathfrak{d}(\mathfrak{f}) := [K(\mathfrak{f}) : K(1)]$. We then have*

$$\mathfrak{d}(\mathfrak{f}) = \begin{cases} 1 & \text{if } \mathfrak{f} = 1 \\ \dfrac{2\mathfrak{f}}{\omega_K} \displaystyle\prod_{\ell \mid \mathfrak{f}} \left(1 - \left(\frac{\Delta_K}{\ell}\right)\frac{1}{\ell}\right) & \text{otherwise.} \end{cases}$$

In particular, this function $\mathfrak{d}$ is multiplicative if and only if $\Delta_K < -4$.

Corollary 2.2.3. *Let K be an imaginary quadratic field, let $\mathfrak{f} \in \mathbb{Z}^+$, and let ℓ denote a prime number.*

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

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

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

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

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

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

Imaginary quadratic fields are notable in that class field theory is made explicit over these fields via the theory of complex multiplication, or CM for short. For $E \cong \mathbb{C}/\Lambda$ an elliptic curve over $\mathbb{C}$, we say that E has **complex multiplication**, and may refer to E as a CM elliptic curve, if

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

In this case, we have $\mathrm{End}(E) \cong \mathfrak{o}$ for an imaginary quadratic order $\mathfrak{o} = \mathfrak{o}(f)$ in some imaginary quadratic field K. In this case, we will say that E has K-CM, or that E has $\mathfrak{o}$-CM or $\mathfrak{f}^2\Delta_K$-CM if we want to specify the order by which we have complex multiplication. If $E_{/F}$ is an elliptic curve over a number field F with $E_{/\mathbb{C}} = E_{/F} \otimes_{\mathrm{Spec}F} \mathrm{Spec}\mathbb{C}$ having $\mathfrak{o}$-CM, then we say that $E_{/F}$ has **potential CM** by $\mathfrak{o}$. We further say that $E_{/F}$ has $\mathfrak{o}$-CM if $\mathrm{End}(E_{/F}) \cong \mathfrak{o}$.

The set of $\mathfrak{o}$-CM elliptic curves over $\mathbb{C}$ is in bijective correspondence with $\mathrm{Pic}(\mathfrak{o})$, and in fact is a torsor under $\mathrm{Pic}(\mathfrak{o})$ ([Cox13, Cor. 10.20]). Moreover, we have the following result ([Cox13, Thm. 11.1]):

Theorem 2.2.4. *Fix an imaginary quadratic field* K *and* $\mathfrak{f} \in \mathbb{Z}^+$*. If* E *is an elliptic curve with* $\mathfrak{o}(\mathfrak{f})$*-CM, then*

$$K(\mathfrak{f}) = K(j(E)),$$

where $j(E)$ *denotes the* j*-invariant of* E*.*

2.2.2 CM points on Shimura curves

Let B be a quaternion algebra over $\mathbb{Q}$ with $\mathcal{O}$ a fixed maximal order, and suppose that (A, ι) is a QM abelian surface over a number field F such that

$$\mathrm{End}^0(A) \cong B.$$

If A is non-simple, such that $A \sim E_1 \times E_2$ is isogenous (over an algebraic closure $\overline{F}$ of F) to a product of elliptic curves, then it must be the case that E_1 and E_2 are isogenous elliptic curves with complex multiplication (CM); we have

$$\mathrm{End}(E_1 \times E_2) = \begin{pmatrix} \mathrm{End}(E_1) & \mathrm{Hom}(E_2, E_1) \\ \mathrm{Hom}(E_1, E_2) & \mathrm{End}(E_2) \end{pmatrix},$$

and note that B embeds in $\mathrm{End}^0(E_1 \times E_2)$ if and only if E_1 and E_2 have CM by a common imaginary quadratic field K which splits B. In this case, then, we have $A \sim E^2$ where E is a K-CM elliptic curve and

$$B \otimes_{\mathbb{Q}} K \cong M_2(K).$$

In this case in which A is non-simple, we refer to (A, ι) as a **QM abelian surface with CM** and we call the corresponding point $[(A, \iota)] \in X^D(1)$ a **CM point**. We call a point x on $X_0^D(D)$ or $X_1^D(N)$ a CM point if it lies in the fiber over a CM point on $X^D(1)$ under the natural modular map.

If (A, ι) has K-CM, then the ring

$$\mathrm{End}_{\mathrm{QM}}(A) := \{\varphi \in \mathrm{End}(A) \mid \iota(\alpha) \circ \varphi = \varphi \circ \iota(\alpha) \text{ for all } \alpha \in \mathcal{O}\}$$

of QM-equivariant endomorphisms of A is an imaginary quadratic order in K. This exactly means that we have some $\mathfrak{f} \in \mathbb{Z}^+$ such that

$$\mathrm{End}_{\mathrm{QM}}(A) \cong \mathfrak{o}(\mathfrak{f}),$$

where $\mathfrak{o}(\mathfrak{f})$ denotes the unique order of conductor $\mathfrak{f}$ in K. We will call this $\mathfrak{f}$ the **central conductor** of (A, ι). We will refer to $[(A, \iota)] \in X^D(1)$, or to any point in the fiber over $[A, \iota]$ under some covering of Shimura curves $X \to X^D(1)$, as an $\mathfrak{o}(\mathfrak{f})$-CM point or an $\mathfrak{f}^2\Delta_K$-CM point when we wish to make the CM order clear.

This indeed generalizes the notion of CM points on classical elliptic modular curves: a CM point on a Shimura curve is exactly one that lies in the fiber over a CM point on $X^D(1)$, which is our analogue of the j-line for $D > 1$ (and is exactly $Y(1)$ when $D = 1$). That said, we find it important to note that this is not the only notion of a CM order attached to a QM abelian surface with CM that exists in the literature, and we expand on this point in Remark 2.3.7.

2.3 Fields of moduli

2.3.1 Beginning notions

The notion of a field of moduli originates in work of Matsusaka [Mat58] in the context of polarized varieties, which was followed by a further treatment for polarized abelian varieties given by Shimura [Sh59]. The context in which one may define fields of moduli was later carefully formalized by Koizumi with the notion of FM-systems and FM-structures [Koi72], though we will be less formal about the notion until the next section in which we carefully define fields of moduli for our objects of interest, QM abelian surfaces and QM-cyclic isogenies thereof.

Roughly, if we fix a field K and a separable closure K^{sep}, then for an algebraic structure X/K^{sep}, the field of moduli K_X of X (relative to K) is the field fixed by

$$H_X := \{\sigma \in \text{Aut}(K^{\text{sep}}/K) \mid X^\sigma \cong X\}.$$

The field of moduli of X is then characterized by the property that $X^\sigma \cong X$ if and only if the restriction $\sigma_{|_{K_X}}$ of σ to K_X is the identity map. We say that a field $L \subseteq K^{\text{sep}}$ is a field

of definition for X if there exists some X'/L such that

$$X' \otimes_{\mathrm{Spec}L} \mathrm{Spec}K^{\mathrm{sep}} \cong X.$$

For any field of definition L of X, we then necessarily have $K_X \subseteq L$. The field of moduli need not itself be a field of definition, however.

Example 2.3.1. Consider the genus 2 hyperelliptic curve $X/\mathbb{C}$ given by an affine model of the form:

$$X : \ y^2 = x^6 + ax^5 + bx^4 + x^3 - \sigma(b)x^2 + \sigma(a)x - 1.$$

where $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ denotes complex conjugation. Let $\iota : (x, y) \mapsto (x, -y)$ denote the hyperelliptic involution on X. If $f \in \mathrm{Aut}(X)$, then the induced map $\overline{f}$ on the quotient $X/\langle\iota\rangle \cong \mathbb{P}^1_{\mathbb{C}}$ must send branch points to branch points. If $a, b \in \mathbb{C}$ are chosen generically enough, it follows that the only branch-point preserving map on the quotient is trivial and thus that $\mathrm{Aut}(X) = \{\mathrm{id}_X, \iota\}$. If X had a field of definition $F \subsetneq \mathbb{C}$, then this automorphism group would be larger (with $\mathrm{Aut}(\mathbb{C}/F) \hookrightarrow \mathrm{Aut}(X)$), so $\mathbb{C}$ must be the minimal field of definition in this case.

We have an affine model

$$X^\sigma : \ y^2 = x^6 + \sigma(a)x^5 + \sigma(b)x^4 + x^3 - bx^2 + ax - 1,$$

and an isomorphism $X \cong X^\sigma$ induced by the birational map

$$\begin{aligned} f : \ \ X &\dashrightarrow X^\sigma \\ (x, y) &\longmapsto (-x^{-1}, ix^{-3}y). \end{aligned}$$

The field of moduli of X relative to $\mathbb{R}$ is therefore $\mathbb{R}_X = \mathbb{R}$. In this case, then, X does not have a model over its field of moduli. (This example is [an]. See [Po17, Exc. 4.1] and [Sh72, p. 177] for more general classes of examples of the same type.)

Related to Example 2.3.1, Huggins determined a sufficient condition for a hyperelliptic curve to be defined over its field of moduli [H06, Thm. 4.1.2]:

Theorem 2.3.2 (Huggins)**.** *Let X be a hyperelliptic curve given by the affine model $y^2 = f(x)$ over $\overline{K}$, where char$(K) \neq 2$. Let $\iota : (x, y) \mapsto (x, -y)$ denote the hyperelliptic involution on X. If Aut$(X)/\langle\iota\rangle$ is not cyclic, then X is defined over its field of moduli K_X relative to K.*

Generalizing work of Matsusaka and Shimura to more general structures and characteristics, Koizumi proved sufficient conditions for a structure to have a well-defined field of moduli and for a structure to have a field of definition which is a finite separable extension of its field of moduli, which apply for example to polarized curves and to polarized abelian varieties [Koi72, Thm. 2.2]. He also proved that, for $\mathrm{char}(K) \neq 2$, if X is a polarized abelian variety or a complete non-singular curve, then K_X can be characterized as the intersection of all fields of definition of structures isomorphic to X ([Koi72, Cor 3.2.2]).

When there exists a moduli space Y/K parametrizing our algebraic structures of interest, the field of moduli of such a structure $X/\overline{K}$ also has the characterization as the residue field of the corresponding point $x = [X] \in Y$. A first example here is the j-line $Y = Y(1)_{/\mathbb{Q}}$, parametrizing elliptic curves (which have a canonical polarization, so this is the dimension 1 case of polarized abelian varieties). For $x \in Y(1)_{/\mathbb{Q}}$, we have a model inducing x defined over its field of moduli; the residue field of x is $Y(1)_{/\mathbb{Q}}(x) \cong \mathbb{Q}(j(E))$ for some $E/\mathbb{Q}(j(E))$ inducing x, as $E^\sigma \cong E$ if and only if $j(E)^\sigma = j(E^\sigma) = j(E)$. For this reason, one often does not encounter discussion about the field of moduli versus fields of definition for elliptic curves (or in the more general context of elliptic curves with level structure, by celebrated work of Deligne–Rapoport [DR73, §4]). The analogous statement *does not* hold for $X^D(1)$ when $D > 1$, prompting the present discussion.

2.3.2 The field of moduli of a QM-cyclic isogeny

We start by spelling out the notions we have just laid out in the specific context of interest in this work. The **field of moduli** of a QM abelian surface (A, ι) defined over $\overline{\mathbb{Q}}$ is the fixed field of those automorphisms $\sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ such that $(A, \iota)^\sigma := (A^\sigma, \iota^\sigma)$ is isomorphic to

(A, ι) over $\overline{\mathbb{Q}}$. Here, A^σ is defined as the fiber product $A \otimes_{\mathrm{Spec}\overline{\mathbb{Q}}} \mathrm{Spec}\overline{\mathbb{Q}}$ over σ:

$$\begin{array}{ccc} A^\sigma & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathrm{Spec}\overline{\mathbb{Q}} & \xrightarrow{\sigma} & \mathrm{Spec}\overline{\mathbb{Q}}\,, \end{array}$$

and ι^σ is defined via the action of σ on endomorphisms of A. By an isomorphism of QM abelian surfaces, we mean an isomorphism of abelian surfaces $A^\sigma \cong A$ which is QM-equivariant. Equivalently, the field of moduli of (A, ι) is the residue field $\mathbb{Q}(x)$ of the corresponding point $x = [(A, \iota)]$ on $X^D(1)_{/\mathbb{Q}}$.

More generally, for a QM-cyclic isogeny $\varphi : (A, \iota) \to (A', \iota')$ defined over $\overline{\mathbb{Q}}$, the **field of moduli** of φ is the fixed field of

$$H(\varphi) := \left\{ \sigma \in \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \;\middle|\; \begin{array}{ccc} (A, \iota) & \xrightarrow{\varphi} & (A', \iota') \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ (A^\sigma, \iota^\sigma) & \xrightarrow{\varphi^\sigma} & ((A')^\sigma, (\iota')^\sigma) \end{array} \quad \begin{array}{c} \text{commutes, and the} \\ \text{vertical maps are} \\ \text{isomorphisms} \end{array} \right\}.$$

In other words, it is the minimal field over which φ is isomorphic to all of its Galois conjugates. Equivalently, it is the residue field of the corresponding point $[\varphi]$ on $X_0^D(N)_{/\mathbb{Q}}$.

We call a field F a **field of definition** for a QM-cyclic isogeny φ as above, or say that φ is defined or rational over F, if φ and both (A, ι) and (A, ι') can be given by equations defined over F. By this, we mean that we have φ' so that $\varphi' \otimes_F \mathbb{C} = \varphi$. It follows that if $x \in X_0^D(N)_{/\mathbb{Q}}$ corresponds to the class of φ, then any field of definition for φ contains the field of moduli $\mathbb{Q}(x)$.

In the analogous case of points on the elliptic modular curves $X_0(N)_{/\mathbb{Q}}$ and $X_1(N)_{/\mathbb{Q}}$, fields of moduli are always fields of definition and hence are minimal fields of definition. More generally, a result of Shimura states that a generic principally polarized abelian variety of odd dimension is rational over its field of moduli [Sh72, Thm. 1], and a result of Milne [Mil72, Thm.] provides that any principally polarized CM abelian variety also has this property.[2]

[2]By a CM abelian variety here, Milne means a principally polarized abelian variety A with multiplication by a CM field of degree $2\dim(A)$ over $\mathbb{Q}$. In particular, this implies that A is simple, and so this result does not apply to our main objects of study: QM abelian surfaces with CM.

It is not generally the case that fields of moduli are fields of definition for higher dimensional (polarized) abelian varieties, though, and this is a source of difficulty and interest in the study of their arithmetic. For instance, Shimura also proved that the generic principally polarized even-dimension abelian variety *does not* have a model defined over its field of moduli [Sh72, Thm. 2]. Particular towards our interests here, a QM abelian surface (or, more generally, a QM-cyclic isogeny) need not be rational over its field of moduli. However, we have the following result of Jordan [Jor81, Thm. 2.1.3]:

Theorem 2.3.3 (Jordan)**.** *Suppose that $(A,\iota)/\overline{\mathbb{Q}}$ is a QM abelian surface with QM by B and with $\mathrm{Aut}_{\mathrm{QM}}(A) = \{\pm 1\}$ (equivalently, (A,ι) does not have CM by $\Delta \in \{-3,-4\}$). Let $x = [(A,\iota)] \in X_0^D(1)_{/\mathbb{Q}}$ be the corresponding point. Then a field L containing $\mathbb{Q}(x)$ is a field of definition for (A,ι) if and only if it splits B, by which we mean if and only if $B \otimes_{\mathbb{Q}} L \cong M_2(L)$.*

If L is a field of definition for (A,ι), then the QM action on the holomorphic 1-forms of A/L yields a map $B \hookrightarrow M_2(L)$, so L must be a splitting field. The harder direction is the sufficiency, which Jordan accomplishes via a descent argument using Weil's descent criterion.

2.3.3 The CM case

Our attention in this study will primarily be aimed at determining fields of moduli, particularly in the presence of CM. We now recall prior work determining the field of moduli of a CM point on $X^D(1)_{/\mathbb{Q}}$.

The answer begins with a result of Shimura [Sh67, Main Thm. 1], and for this result and the remainder of this section we fix an imaginary quadratic field K and $\mathfrak{f} \in \mathbb{Z}^+$.

Theorem 2.3.4 (Shimura)**.** *Let $x \in X^D(1)_{/\mathbb{Q}}$ be an $\mathfrak{o}(\mathfrak{f})$-CM point with residue field $\mathbb{Q}(x)$. Then*

$$K \cdot \mathbb{Q}(x) = K(\mathfrak{f})$$

This tells us that in this setting there are two possibilities: either $\mathbb{Q}(x)$ is the ring class field $K(\mathfrak{f})$, or it is an index 2 subfield thereof. In the $D = 1$ elliptic modular case, the latter is always true; here we have that $\mathbb{Q}(x) \cong \mathbb{Q}(j(E))$ for E any $\mathfrak{o}(\mathfrak{f})$-CM elliptic curve. Following

the notation of [Cl23, CS23], we set

$$\mathbb{Q}(\mathfrak{f}) := \mathbb{Q}(j(\mathbb{C}/\mathfrak{o}(\mathfrak{f}))),$$

and refer to this field (or, often, any isomorphic field) as a **rational ring class field** corresponding to $\mathfrak{o}(\mathfrak{f})$. For $D > 1$, however, we will see that it is in a sense generically the case that $\mathbb{Q}(x) = K(\mathfrak{f})$. Furthermore, while $\mathbb{Q}(\mathfrak{f})$ always has a real embedding, and indeed is the subfield of $K(\mathfrak{f})$ fixed by complex conjugation, for $D > 1$ the residue field $\mathbb{Q}(x)$ can *never* have a real embedding by the following result of Shimura [Sh75, Thm. 0]:

Theorem 2.3.5 (Shimura)**.** *For any rational quaternion discriminant $D > 1$, we have $X^D(1)(\mathbb{R}) = \emptyset$.*

In his thesis [Jor81, §3], Jordan determined exactly when the residue field of a CM point $x \in X_0^D(1)$ is a ring class versus an index 2 subfield of a ring class field in the case of CM by the maximal order of K (i.e., the $\mathfrak{f} = 1$ case). Work of González–Rotger allows for a generalization of Jordan's result to arbitrary CM orders [GR06, §5].

To state their result, we first set the following notation: for D a rational quaternion discriminant and K an imaginary quadratic field splitting the rational quaternion algebra B of discriminant D, let

$$D(K) := \prod_{p|D,\, \left(\frac{K}{p}\right)=-1} p.$$

The assumption that K splits B is exactly the assumption that no prime divisor of D splits in K. From this we see that $D(K) = 1$ if and only if all primes dividing D ramify in K, while $D(K) > 1$ exactly when some prime dividing D is inert in K.

Theorem 2.3.6 (Jordan, González–Rotger)**.** *Let $x \in X^D(1)_{/\mathbb{Q}}$ be an $\mathfrak{o}(\mathfrak{f})$-CM point.*

1. *If $D(K) = 1$, then we have $\mathbb{Q}(x) = K(\mathfrak{f})$.*
2. *Otherwise, $[K(\mathfrak{f}) : \mathbb{Q}(x)] = 2$. In this case, $\mathbb{Q}(x) \subsetneq K(\mathfrak{f})$ is the subfield fixed by*

$$\sigma = \tau \circ \sigma_{\mathfrak{a}} \in \mathrm{Gal}(K(\mathfrak{f})/\mathbb{Q}),$$

where τ denotes complex conjugation and $\sigma_{\mathfrak{a}} \in \mathrm{Gal}(K(\mathfrak{f})/K)$ is the automorphism associated via the Artin map to a certain fractional ideal $\mathfrak{a}$ of $\mathfrak{o}(\mathfrak{f})$ with the property that

$$B \cong \left(\frac{\Delta_K, N_{K/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}}\right).$$

More specifically, $\mathfrak{a}$ is such that

$$\omega_{D(K)}(x^{\sigma_{\mathfrak{a}}}) = \tau(x),$$

where ω_m denotes the Atkin–Lehner involution on $X^D(1)_{/\mathbb{Q}}$ corresponding to a divisor $m \mid D$.

We reiterate that, in this result, the field $\mathbb{Q}(x)$ must be totally complex if and only if $D > 1$ by Theorem 2.3.5 and the discussion preceding it.

Remark 2.3.7. In fact, González–Rotger provide a generalization of Jordan's result to all CM points on $X_0^D(N)_{/\mathbb{Q}}$ for squarefree N. In comparing our work to [GR06], it is important for the reader to note that the definition of an $\mathfrak{o}$-CM point on $X_0^D(N)_{/\mathbb{Q}}$ that they work with is different from ours; whereas our definition is that a CM point has $\mathfrak{o}$-CM for an imaginary quadratic order $\mathfrak{o}$ if it lies over an $\mathfrak{o}$-CM point on $X^D(1)_{/\mathbb{Q}}$, their definition is that $x \in X_0^D(N)_{/\mathbb{Q}}$ has $\mathfrak{o}$-CM if it corresponds to a normalized optimal embedding of $\mathfrak{o}$ into an Eichler order of level N in B. The definition used in [GR06] provides a pleasantly uniform result similar to Jordan's $N = 1$ case, with every $\mathfrak{o}(\mathfrak{f})$-CM point $x \in X_0^D(N)_{/\mathbb{Q}}$ having field of moduli $\mathbb{Q}(x)$ with $K \cdot \mathbb{Q}(x) \cong K(\mathfrak{f})$.

This definition used by González–Rotger is common in the literature, appearing for example in work of Rotger and his collaborators and also in recent work of Padarariu–Schembri [PS22] in which the authors compute rational points on all Atkin–Lehner quotients of geometrically hyperelliptic Shimura curves. A main advantage of our definition and approach, beyond the generalization from squarefree N to all positive integers N that appears in the present work, is that it provides not just the residue fields of CM points but a description of the *fiber* of the covering $X_0^D(N)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ over any CM point. Additionally, as

previously remarked, our notion is a clear generalization of that appearing in the setting of modular curves.

Chapter 3

Decompositions of QM abelian surfaces with CM

There are strong analogies between QM abelian surfaces and elliptic curves, earning them the moniker of "fake elliptic curves" in the literature. Restricting to the case of a QM abelian surface (A, ι) with CM over $\mathbb{C}$, we have seen that in fact A is isogenous to a square of an elliptic curve with CM. Through a correspondence between QM abelian surfaces with CM and equivalance classes of certain binary quadratic forms, Shioda–Mitani [SM74] proved the following strengthening of this fact:

Theorem 3.1 (Shioda–Mitani)**.** *If $(A, \iota)/\mathbb{C}$ is a QM abelian surface with K-CM for an imaginary quadratic field K, then there exist K-CM elliptic curves E_1, E_2 over $\mathbb{C}$ such that*

$$A \cong E_1 \times E_2.$$

The number of distinct decompositions of a given A as above is finite, resulting from finiteness of the class number of any imaginary quadratic order in K. This theorem was generalized to higher dimensional complex abelian varieties isogenous to a power of a CM elliptic curve independently by Lange [La75] and Schoen [Sc92]. A generalization from $\mathbb{C}$ to an arbitrary field of definition F is a result of Kani [Ka11, Thm 2]:

Theorem 3.2 (Kani)**.** *If A/F is an abelian variety which is F-rationally isogenous to E^n, where E/F is a CM elliptic curve, then there exist CM elliptic curves $E_1/F, \ldots, E_n/F$ such that we have an isomorphism*

$$A \cong E_1 \times \cdots E_n$$

over the base field F.

Kani in fact says more, which is relevant in the case of QM abelian surfaces with CM [Ka11, Thm 67]: fixing a K-CM elliptic curve E/F with endomorphism ring of conductor $\mathfrak{f}_E$, there is a bijection

$$\left\{ \begin{array}{c} \text{F-isomorphism classes } [E'] \text{ with} \\ E \sim E' \text{ and } \mathfrak{f}_{E'} | \mathfrak{f}_E \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{F-isomorphism classes of abelian surfaces} \\ A/F \text{ with } A \sim E^2 \text{ and central conductor } \mathfrak{f}_A = \mathfrak{f}_E \end{array} \right\}$$

which sends an F-isomorphism class $[E']$ to the F-isomorphism class $[E \times E']$.

In order to obtain concrete decompositions of QM abelian surfaces with CM, the remaining task is to identify *which* such products of CM elliptic curves have potential quaternionic multiplication, i.e., can be given QM structures, and to further describe the classes of QM abelian surfaces with CM. The following result provides the number of such classes (see [Vig80, Cor. 5.12] and [AB04, Thm. 6.13]).

Proposition 3.3. *Let K be an imaginary quadratic field splitting B, and let $\mathfrak{f} \in \mathbb{Z}^+$. Let b denote the number of primes dividing D that are inert in K. The number of geometric $\mathfrak{o}(\mathfrak{f})$-CM points on $X^D(1)$ is then $2^b \cdot h(\mathfrak{o}(\mathfrak{f}))$, where $h(\mathfrak{o}(\mathfrak{f}))$ denotes the class number of the order $\mathfrak{o}(\mathfrak{f})$.*

In his thesis, Ufer touches on this topic of taking QM structures into account. In particular, he proves the following [Uf10, Thm. 2.7.12]: with the notation of Proposition 3.3, there exists a 2^b-to-1 correspondence

$$\left\{ K\text{-CM points on } X^D(1) \right\} \longrightarrow \{ K\text{-CM elliptic curves over } \mathbb{C} \} \, / \cong .$$

Based on the proof therein, it seems that Ufer could have said more, and so we do that here with reference to his argument:

Theorem 3.4. *Let $(A, \iota)/\mathbb{C}$ be a QM abelian surface with CM by $\mathfrak{o}(\mathfrak{f})$. There is then a unique $\mathfrak{o}(\mathfrak{f})$-CM curve $E_A/\mathbb{C}$, up to isomorphism, such that*

$$A \cong \mathbb{C}/\mathfrak{o}(\mathfrak{f}) \times E_A.$$

Additionally, there is a 2^b-to-1 correspondence

$$\left\{\mathfrak{o}(\mathfrak{f})\text{-CM points on } X^D(1)\right\} \longrightarrow \left\{\mathfrak{o}(\mathfrak{f})\text{-CM elliptic curves over } \mathbb{C}\right\} / \cong$$

sending a point $[(A, \iota)] \in X^D(1)$ to the class of E_A.

Proof. Part (2) of the proof of [Uf10, Thm. 2.7.12] details the construction of a QM-structure by a maximal order $\mathcal{O}$ in B on $E \times E'$ for E and E' both $\mathfrak{o}(\mathfrak{f})$-CM elliptic curves. The product $E \times E'$ with the constructed QM structure then corresponds to a CM point on $X^D(1)$ with central conductor $\mathfrak{f}$.

Let E, E' be K-CM elliptic curves. Part (3) of Ufer's proof explains that if the abelian surface $E \times E'$ has potential quaternionic multiplication then in fact it has 2^b non-isomorphic QM structures. Put differently but equivalently to therein: let W be the group generated by the Atkin–Lehner involutions ω_p on $X^D(1)$ for $p \mid D$ inert in K. The group $W \times \mathrm{Pic}(\mathfrak{o}(\mathfrak{f}))$ then acts simply transitively on the set of $\mathfrak{o}(\mathfrak{f})$-CM points on $X^D(1)$. If $[(A, \iota)] \in X^D(1)$ is such a point, then the action of any element $w \in W$ leaves $[A]$ unchanged, providing the claim (this is proved by Jordan [Jor81] in the $\mathfrak{f} = 1$ case, and extended to the general case by [GR06]). By the count of Proposition 3.3, Theorem 3.1 and the fact that $\mathbb{C}/\mathfrak{o}(\mathfrak{f}) \times E \cong \mathbb{C}/\mathfrak{o}(\mathfrak{f}) \times E'$ implies $E \cong E'$, the claimed result follows. □

Corollary 3.5. *Let $(A, \iota)/F$ be a QM abelian surface with CM by $\mathfrak{o} \subseteq \mathfrak{o}_K$. Suppose that $K \subseteq F$ and that we have an F-rational isogeny $A \sim E^2$ to the square of an elliptic curve. Fix E_1/F any elliptic curve with $\mathfrak{o}$-CM. There then exists an $\mathfrak{o}$-CM elliptic curve E_2/F, unique up to twist, such that $A \cong E_1 \times E_2$ over F.*

Proof. Let $E_{1/\mathbb{C}} := E_1 \otimes_{\mathrm{Spec}F} \mathrm{Spec}\mathbb{C}$ and $A_{/\mathbb{C}} := A \otimes_{\mathrm{Spec}F} \mathrm{Spec}\mathbb{C}$. Theorem 3.4 provides that there is a unique $\mathfrak{o}(\mathfrak{f})$-CM elliptic curve $\widetilde{E_2}/\mathbb{C}$ such that we have an isomorphism

$$h : A_{/\mathbb{C}} \to E_{1/\mathbb{C}} \times \widetilde{E_2}$$

By Theorem 2.3.4 and our assumption that $K \subseteq F$, the field of definition F of (A, ι) must contain the ring class field $K(\mathfrak{f})$. We therefore have a model E_2/F of $\widetilde{E_2}$ over F. We may transfer the QM structure ι on $A_{/\mathbb{C}}$ to a QM structure ι' on $E_{1/\mathbb{C}} \times \widetilde{E_2}$ via our isomorphism h, and this descends to a QM structure on $E_1 \times E_2$ over F as $K \subseteq F$.

Currently, we have that A and $E_1 \times E_2$ are twists. By our assumption that A is F-rationally isogenous to the square of an elliptic curve, Theorem 3.2 implies that there is a unique K-CM elliptic curve E_2'/F such that we get an F-rational isomorphism $A \cong E_1 \times E_2'$, and from Theorem 3.4 it must be the case that E_2' has $\mathfrak{o}(\mathfrak{f})$-CM, as we can transfer the QM structure on A to one on $E_1 \times E_2'$ via our isomorphism. By the uniqueness statement in Theorem 3.4, we see that E_2 and E_2' become isomorphic over some extension. $\square$

Chapter 4

QM-equivariant isogeny volcanoes

4.1 QM-equivariant isogenies

Our goal in the following section will be to determine the residue field of any CM point on $X_0^D(N)_{/\mathbb{Q}}$ for any N coprime to D, generalizing Theorem 2.3.6. A main component in accomplishing this in our work is the study of the structure of, and the action of automorphisms on, components of certain isogeny graphs. Paths in these graphs of consideration will be in correspondence with isogenies of QM abelian surfaces respecting their QM structures.

In this section, we prove facts about QM-equivariant isogenies needed in the proceeding section. Much of what we do in both this section and the next is in strong analogy to the case of isogenies of elliptic curves over $\overline{\mathbb{Q}}$ studied in work of Clark and Clark–Saia [Cl23, CS23]. We provide proofs here for completeness and for clarity of said analogy.

Lemma 4.1.1. *Let F be a field of characteristic zero, and let (A, ι) be a QM abelian surface over F which does not have CM by an order of discriminant $\Delta \in \{-3, -4\}$. For ℓ a prime number, the number of QM-equivariant ℓ-isogenies emanating from (A, ι) which are F-rational, up to isomorphism, is either $0, 1, 2,$ or $\ell + 1$.*

Proof. Note that ℓ being prime means we are counting isomorphism classes of QM-cyclic ℓ-isogenies. The hypotheses on A are equivalent to our QM abelian surface having no extra automorphisms. That is, $\mathrm{Aut}(A, \iota) = \{\pm 1\}$. In this case, we have a bijective correspondence between isomorphism classes of QM-equivariant ℓ-isogenies and $\mathcal{O}$-submodules of $A[\ell]$ of rank 1. Under this correspondence, the F-rational isogenies correspond to $\mathfrak{g}_F$-stable submodules.

Now, with the notation of Remark 2.1.7, we have that $e_1(Q) \leq e_1(A[N]) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ is a cyclic subgroup of order ℓ, and in this way we have a bijective correspondence between the non-trivial proper QM-stable subgroups of $A[\ell]$ and cyclic order ℓ subgroups of $e_1(A[\ell])$. This correspondence preserves the property of being $\mathfrak{g}_F$-stable. We have thus reduced to the situation of the elliptic curve case, and may proceed as such: we are counting $\mathfrak{g}_F$-stable cyclic order ℓ subgroups of $(\mathbb{Z}/\ell\mathbb{Z})^2$. The total number of cyclic order ℓ subgroups is $\ell+1$, and if more than 2 such subgroups are fixed then $\mathfrak{g}_F$ is forced to act by scalar matrices on $(\mathbb{Z}/\ell\mathbb{Z})^2$. □

4.1.1 Compositions of QM-cyclic isogenies

The following result is in analogy with [CS23, Prop 3.2].

Proposition 4.1.2. *Suppose that $\varphi = \varphi_2 \circ \varphi_1$ is a QM-cyclic isogeny, where $\varphi_i : (A_i, \iota_i) \to (A_{i+1}, \iota_{i+1})$ is a QM-cyclic isogeny for $i = 1, 2$.*

1. *We have*
$$\mathbb{Q}(\varphi) \supseteq \mathbb{Q}(\varphi_1) \cdot \mathbb{Q}(\varphi_2).$$

2. *If (A_2, ι_2) does not have CM by $\Delta \in \{-3, -4\}$, then*
$$\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi_1) \cdot \mathbb{Q}(\varphi_2).$$

Proof. The containment of part (1) is clear. The assumption that (A_2, ι_2) does not have -3 or -4 CM is equivalent to $\mathrm{Aut}((A_2, \iota_2)) = \{\pm 1\}$, and in this case the reverse containment in part (2) follows by the same argument as in [Cl23, Prop. 3.1 b)]. □

4.1.2 Reduction to prime power degrees

First, let us say something about rationality. Let $\varphi : (A, \iota) \to (A', \iota')$ be a QM-cyclic N-isogeny which is rational over F, where N has prime-power decomposition $N = \ell_1^{a_1} \dots \ell_r^{a_r}$. If Q is the kernel of this isogeny, then φ is isomorphic to the quotient $(A, \iota) \to (A/Q, \iota)$ (the latter pair provides a well-defined QM abelian surface as Q is stable under $\iota(\mathcal{O})$, though really we are abusing notation by referring to the QM-structure on the quotient as ι). We have a decompositon $Q = C \oplus D$ with each of C and D cyclic of order N, such that $\mathcal{O} \cdot C = \mathcal{O} \cdot D = Q$. This cyclic subgroup C then decomposes as

$$C = \bigoplus_{i=1}^{r} C_i$$

where $C_i \leq C$ is the unique subgroup of order $\ell_i^{a_i}$. Letting $Q_i = \mathcal{O} \cdot C_i$, each Q_i is QM stable and isomorphic to $(\mathbb{Z}/{\ell_i}^{a_i}\mathbb{Z})^2$.

From the uniqueness of $C_i \leq C$, and hence of the corresponding $\mathcal{O}$-cyclic subgroup $Q_i \leq Q$, we get that each Q_i is F-rational, resulting in F-rational QM-cyclic $\ell_i^{a_i}$-isogenies $\varphi_i : (A, \iota) \to (A/Q_i, \iota)$ for each i. On the other hand, given a collection of F-rational QM-cyclic $\ell_i^{a_i}$-isogenies with kernels Q_i, we get an F-rational QM-cyclic N-isogeny $(A, \iota) \to (A/Q, \iota)$ where $Q = \bigoplus_{i=1}^{r} Q_i$.

As for fields of moduli, more towards our needs for what follows, we have the following:

Proposition 4.1.3. *Let $N_1, \dots, N_r \in \mathbb{Z}^+$ be pairwise coprime, let k be a field of characteristic 0, and let $x \in X^D(1)_{/k}$ be a closed point which does not have CM by discriminant $\Delta \in \{-3, -4\}$. For each i, let $\pi_i : X_0^D(N_i)_{/k} \to X^D(1)_{/k}$ be the natural map, let $F_i = \pi_i^{-1}(x)$, and let F be the fiber over x of $\pi : X_0^D(N)_{/k} \to X^D(1)_{/k}$ where $N = N_1 \cdots N_r$. Then*

$$F = F_1 \otimes_{\mathrm{Spec} k(x)} \cdots \otimes_{\mathrm{Spec} k(x)} F_r.$$

Proof. This follows as in the $D = 1$ case of [Cl23, Prop. 3.5], using that $X_0^D(N)$ for $D > 1$ is a cover of $X^D(1)$ with the same corresponding subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ as in the case of $X_0(N) \to X(1)$. □

It follows that if $x \in X_0^D(N)_{/\mathbb{Q}}$ is a point which does not have -3 or -4-CM and $N = \prod_{i=1}^r \ell_i^{a_i}$, with $\pi_i : X_0^D(N)_{/\mathbb{Q}} \to X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$ the natural maps, then

$$\mathbb{Q}(x) = \mathbb{Q}(\pi_1(x)) \cdots \mathbb{Q}(\pi_r(x)).$$

4.2 Volcanoes

Fixing a prime ℓ, we describe in this section CM components of ℓ-isogeny graphs of QM abelian surfaces over $\overline{Q}$. We will use the work of this section to study CM points on the curves $X_0^D(\ell^a)_{/\mathbb{Q}}$ for $a \in \mathbb{Z}^+$ and D an arbitary indefinite rational quaternion discriminant, in analogy to the $D = 1$ elliptic modular case of [Cl23, CS23].

This study, like that of [Cl23, CS23], is motivated by the foundational work on isogeny volcanoes over finite fields by Kohel in his PhD thesis [Koh96] and by Fouquet [Fou01] and Fouquet–Morain [FM02]. We also recommend, and will refer to, a more recent, expository account of isogeny volcanoes in the finite field setting by Sutherland [Sut13].

4.2.1 QM-equivariant isogeny graphs

Fix a prime number ℓ and an imaginary quadratic field K. In [Cl23] and [CS23], the authors consider the multigraph with vertex set that of j-invariants of K-CM elliptic curves, and with edges corresponding to $\mathbb{C}$-isomorphism classes of cyclic ℓ-isogenies.

Here, we seek an analog for "fake elliptic curves," meaning QM abelian surfaces with QM by a fixed maximal order $\mathcal{O}$ of the indefinite rational quaternion algebra B of discriminant D with $\ell \nmid D$. We let $\mathcal{G}_\ell^D$ denote the directed multigraph with

- vertex set consisting of $\mathbb{C}$-isomorphism classes of $\mathcal{O}$-QM abelian surfaces, and
- edges from $v_1 = [(A_1, \iota_1)]$ to $v_2 = [(A_2, \iota_2)]$ corresponding to $\mathbb{C}$-isomorphism classes of QM-cyclic ℓ-isogenies $\varphi : (A_1, \iota_1) \to (A_2, \iota_2)$.

A given vertex v has $\ell + 1$ edges emanating from it, via the correspondence of QM-stable subgroups of $A_1[\ell]$ with cyclic order ℓ subgroups of $e_1(A_1[\ell]) \cong (\mathbb{Z}/\ell\mathbb{Z})^2$.

Because a QM structure ι determines a unique principal polarization, we have dual edges via dual isogenies as in the elliptic curve case. As long as the source vertex v_1 corresponds to an isomorphism class $[(A, \iota)]$ having only the single non-trivial automorphism $[-1]$, we obtain a bijection between the edges from v_1 to v_2 and those from v_2 to v_1; in this case, outward edges from v_1 are in bijective correspondence with QM-stable subgroups of $A_1[\ell]$ of order ℓ^2. This occurs precisely when $[(A, \iota)]$ does not have CM by discriminant $\Delta = -3$ or $\Delta = -4$.

Our attention will be to vertices in $\mathcal{G}_\ell^D$ corresponding to QM abelian surfaces with CM. For an abelian variety (A, ι) with QM by $\mathcal{O}$ and K-CM, recall that the central conductor of (A, ι) is defined to be the positive integer $\mathfrak{f}$ such that $\mathrm{End}_{\mathrm{QM}}(A) \cong \mathfrak{o}(\mathfrak{f}) \subseteq \mathfrak{o}_K$.

Lemma 4.2.1. *Suppose $\varphi : (A, \iota) \to (A', \iota')$ is a QM cyclic N-isogeny, with (A, ι) a QM abelian surface with K-CM. Then*

1. *The QM abelian surface (A', ι') also has K-CM.*
2. *Let $\mathfrak{f}$ and $\mathfrak{f}'$ denote the central conductors of (A, ι) and (A', ι'), respectively. Then $\mathfrak{f}$ and $\mathfrak{f}'$ differ by at most a factor of N. That is,*

$$\mathfrak{f} \mid N\mathfrak{f}' \text{ and } \mathfrak{f}' \mid Nf.$$

Proof. The argument is similar to that of the elliptic curve case. In our context, we need only remember that we care specifically about those endomorphisms commuting with the QM.

Consider the homomorphism

$$\begin{aligned} F : \mathrm{End}(A, \iota) &\longrightarrow \mathrm{End}(A', \iota') \\ \psi &\longmapsto \varphi \circ \psi \circ \hat{\varphi}. \end{aligned}$$

Because φ is assumed to be QM-equivariant, this restricts to a homomorphism

$$\mathrm{End}_{\mathrm{QM}}(A, \iota) \longrightarrow \mathrm{End}_{\mathrm{QM}}(A', \iota').$$

As in the argument in the elliptic curves case, the algebras of endomorphisms commuting with the quaternionic multiplication are isomorphic by the multiple $\frac{1}{N}F$ of the map above. That is,

$$K \cong \mathrm{End}_{\mathrm{QM}}(A, \iota) \otimes \mathbb{Q} \cong \mathrm{End}_{\mathrm{QM}}(A', \iota') \otimes \mathbb{Q}.$$

This completes part (a). Moreover, that

$$\frac{1}{N}F : \mathrm{End}_{\mathrm{QM}}(A, \iota) \otimes \mathbb{Q} \to \mathrm{End}_{\mathrm{QM}}(A', \iota')$$

is an isomorphism tells us that

$$N \cdot \mathrm{End}_{\mathrm{QM}}(A, \iota) \subseteq \mathrm{End}_{\mathrm{QM}}(A', \iota'),$$

yielding $\mathfrak{f}' \mid Nf$. Via the dual argument, we obtain $\mathfrak{f} \mid N\mathfrak{f}'$.

□

For an imaginary quadratic field K, we are therefore justified in defining $\mathcal{G}^D_{K,\ell}$ to be the subgraph of $\mathcal{G}^D_\ell$ consisting of vertices corresponding to QM abelian surfaces with K-CM. An edge in $\mathcal{G}^D_{K,\ell}$ corresponds to a class of QM-cyclic ℓ-isogenies $[\varphi : (A, \iota) \to (A', \iota')]$ between QM abelian surfaces with K-CM, and the above lemma tells us that as we move along paths in $\mathcal{G}^D_{K,\ell}$, the central conductors of vertices met have the same prime-to-ℓ part. It follows that $\mathcal{G}^D_{K,\ell}$ has a decomposition

$$\mathcal{G}^D_{K,\ell} = \bigsqcup_{(\mathfrak{f}_0,\ell)=1} \mathcal{G}^D_{K,\ell,\mathfrak{f}_0},$$

where $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ denotes the subgraph of $\mathcal{G}^D_{K,\ell}$ with vertices having corresponding central conductors of the form $\mathfrak{f}_0\ell^a$ for some $a \in \mathbb{N}$.

Any edge in $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ has vertices with corresponding central conductors $\mathfrak{f}$ and $\mathfrak{f}'$ satisfying $\mathfrak{f}/\mathfrak{f}' \in \{1, \ell, \ell^{-1}\}$. Defining the **level** of a vertex in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ having central conductor $\mathfrak{f}$ to be $\mathrm{ord}_\ell(\mathfrak{f})$, we note that a directed edge can do one of three things:

- increase the level by one, in which case we will call the edge **ascending**,
- decrease the level by one, in which case we will call the edge **descending**, or

- leave the level unchanged, in which case we will call the edge **horizontal**.

We will refer to ascending and descending edges collectively as **vertical** edges. For a connected component of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$, we refer to the subgraph consisting of level 0 vertices and horizontal edges between them as the **surface** of that component. In other words, the vertex set of the surface consists of vertices with corresponding central conductor $\mathfrak{f}_0$. This choice of terminology is reflective of the fact that we cannot have an ascending isogeny starting at level 0, and of the fact that horizontal edges can only occur between surface vertices, as the following lemma states.

Lemma 4.2.2. *Suppose that there is a horizontal edge in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ connecting vertices v_1 and v_2. Letting $\mathfrak{f}_i$ denote the central conductor corresponding to v_i for $i = 1, 2$, we then have $\mathfrak{f}_1 = \mathfrak{f}_2 = \mathfrak{f}_0$. Furthermore, the number of horizontal edges emanating from a given surface vertex in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ is $1 + \left(\frac{\Delta_K}{\ell}\right)$, hence is*

- 0 *if ℓ is inert in K,*
- 1 *if ℓ ramified in K, and*
- 2 *if ℓ is split in K.*

Proof. That $\mathfrak{f}_1 = \mathfrak{f}_2$ is part of our definition of horizontal edges. What we must prove is that ℓ does not divide $\mathfrak{f} := \mathfrak{f}_1 = \mathfrak{f}_2$.

The given edge corresponds to a QM-cyclic ℓ isogeny

$$\varphi : (A_1, \iota_1) \to (A_2, \iota_2),$$

where (A_i, ι_i) has central conductor $\mathfrak{f}$ for $i = 1, 2$. By Theorem 3.4, we have a decomposition of these two QM abelian surfaces resulting in an isomorphic isogeny ψ as below:

$$\begin{array}{ccc} (A_1, \iota_1) & \xrightarrow{\quad\varphi\quad} & (A_2, \iota_2) \\ \downarrow\cong & & \downarrow\cong \\ (E_1 \times E_1', \iota_1) & \xrightarrow{\psi} & (E_2 \times E_2', \iota_2), \end{array}$$

where each E_i and each E_i' is an elliptic curve with K-CM by conductor $\mathfrak{f}$ for $i = 1, 2$. Restricting ψ to E_1 and to E_1', respectively, yields isogenies of K-CM elliptic curves

$$\begin{aligned} E_1 &\longrightarrow \psi(E_1) =: E \subseteq E_2 \times E_2' \\ E_1' &\longrightarrow \psi(E_1') =: E' \subseteq E_2 \times E_2'. \end{aligned} \tag{4.1}$$

This provides the decomposition

$$E_2 \times E_2' \cong E \times E'.$$

The conductors of the endomorphism rings of E and E' must each be in the set $\{\mathfrak{f}, \ell\mathfrak{f}, \frac{1}{\ell}\mathfrak{f}\}$ and must have least common multiple $\mathfrak{f}$. This provides that either E or E' must have CM conductor $\mathfrak{f}$.

We now consider the corresponding isogeny of K-CM elliptic curves of conductor $\mathfrak{f}$ from (4.1). In doing so, [Cl23, Lemma 4.1] tells us that we must have $\ell \nmid f$. There, the result is reached using the correspondence between horizontal ℓ-isogenies of $\mathfrak{o}(\mathfrak{f}_0)$-CM elliptic curves over $\mathbb{C}$ with proper $\mathfrak{o}(\mathfrak{f}_0)$-ideals of norm ℓ. This also gives us the count of horizontal isogenies mentioned; we have the count in the elliptic curve case as in [Cl23], and from a horizontal isogeny of elliptic curves as in (4.1) we generate a QM-cyclic isogeny of our QM-abelian surfaces via the QM action. □

Each surface vertex has $1 + \left(\frac{\Delta_K}{\ell}\right)$ horizontal edges emanating from it, and therefore has $\ell - \left(\frac{\Delta_K}{\ell}\right)$ descending edges to level 1 vertices. For vertices away from the surface, we have the following:

Lemma 4.2.3. *If v is a vertex in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ at level $L > 0$. then there is one ascending vertex from v to a vertex in level $L - 1$, and the remaining ℓ edges from v are descending edges to distinct vertices in level $L + 1$.*

Proof. We will use the same type of counting argument one may use in the elliptic curve case, as in [Sut13, Lemma 6]. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ preserves the level of a given vertex, and hence preserves the notions of horizontal, ascending, and descending for edges.

As a result, the number of ascending, respectively descending, edges out of v must be the same as for any other vertex at level L by transitivity of this action on vertices at each level.

For $L = 1$, there are

$$\left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right) 2^b h(\mathfrak{o}(\mathfrak{f}_0)) = 2^b h(\mathfrak{o}(\ell\mathfrak{f}_0))$$

total descending vertices from surface vertices (where b is as in Proposition 3.3). The equality above states that this is equal to the total number of level 1 vertices, and so the edges must all be to distinct level 1 vertices. For $L > 1$, the result follows inductively using the same counting argument along with the fact that

$$h(\mathfrak{o}(\ell^L\mathfrak{f}_0)) = \ell \cdot h(\mathfrak{o}(\ell^{L-1}\mathfrak{f}_0)).$$

□

4.2.2 QM-equivariant isogeny volcanoes

For a prime number ℓ, we define here the notion of an ℓ-volcano. This notion for the most part agrees with that in the existing literature, with the only caveat being that in the original context of isogeny volcanoes over a finite field one has volcanoes of finite depth. In our case, working over an algebraically closed field in characteristic 0 as in [Cl23, CS23], we adjust the definition to allow for infinite depth volcanoes.

Definition 4.2.4. Let V be a connected graph with vertices partitioned into levels

$$V = \bigsqcup_{i \geq 0} V_i,$$

such that if $V_d = \emptyset$ for some d, then $V_i = \emptyset$ for all $i \geq d$. If such a d exists, we will refer to the smallest such d as the **depth** of V and to V_d for d the depth as the **floor** of V, and otherwise we will say that the depth of V is infinite.

Fixing a prime number ℓ, the graph V with its partioning is an **ℓ-volcano** if the following properties hold:

1. Each vertex not in the floor of V has degree $\ell + 1$, while any floor vertex has degree 1.
2. The subgraph V_0, which we call **the surface**, is regular of degree $0, 1$ or 2.
3. For $0 < i < d$ (colloquially: "below the surface" and "above the floor"), a vertex in V_i has one "ascending" edge to a vertex in V_{i-1}, and ℓ "descending" edges to distinct vertices in V_{i+1}. This accounts for all edges of V which are not "horizontal," by which we mean edges which are not between two surface vertices.

The results of the previous section have built to the following theorem, declaring that in most cases connected components of the subgraphs $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ of $\mathcal{G}^D_{K,\ell}$ earn the title of **QM-equivariant isogeny volcanoes** and justifying our use of terminology regarding edges and vertices in these subgraphs.

Theorem 4.2.5. *Fix an imaginary quadratic field K, a prime ℓ and a natural number $\mathfrak{f}_0$ with $(\ell, \mathfrak{f}_0) = 1$ and $\mathfrak{f}_0^2\Delta_K < -4$. Consider the graph $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ as an undirected graph by identifying edges with their dual edges as described above. Each connected component of this graph has the structure of an ℓ-volcano of infinite depth.*

A **path** in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ refers to a finite sequence of directed edges, say $e_1, \ldots, e_r$, such that the terminal vertex of e_i is the initial vertex of e_{i+1} for all $1 \leq i \leq r-1$. In the $\mathfrak{f}_0^2\Delta_K < -4$ case, because the edges in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ all have canonical inverse edges we are justified in using the following terminology: we call an edge **backtracking** if e_{i+1} is inverse to e_i for some edge e_i in the path. Note that in the case of ℓ ramified in K, a path consisting of two surface edges always is backtracking. If ℓ is split in K, a path consisting of traversing a loop at a surface vertex any number of times does not have backtracking.

In exact analogy to [Cl23, Lemma 4.2], our definitions and the results of this section lead us to the following correspondence:

Lemma 4.2.6. *Suppose that $\mathfrak{f}_0^2\Delta_K < -4$. We then have a bijective correspondence*

$$\left\{\begin{array}{c}\text{QM-cyclic } \ell^a \text{ isogenies of QM abelian surfaces with} \\ \text{K-CM and central conductor with prime-to-ℓ part } \mathfrak{f}_0\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{length } a \text{ non-backtracking} \\ \text{paths in } \mathcal{G}^D_{K,\ell,\mathfrak{f}_0}\end{array}\right\}.$$

In §5.1, we will describe the Galois orbits of such paths in order to describe the K-CM locus on $X_0^D(\ell^a)$ via the above correspondence. For this, the following observation will be of use: any non-backtracking length a path in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ for $\mathfrak{f}_0^2\Delta_K < -4$ can be written as a concatenation of paths P_1, P_2 and P_3, where P_1 is strictly ascending, P_2 is strictly horizontal and hence consists entirely of surface edges, and P_3 is strictly descending, such that the lengths of these paths (which may be 0) sum to a.

4.2.3 The field of moduli of a QM-cyclic ℓ isogeny

A QM-cyclic ℓ isogeny φ of K-CM abelian surfaces with $\ell \nmid D$ corresponds to an edge e in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$, say between vertices v and v' in levels L and L', respectively. Assume that $L \geq L'$, so either $L = L'$ or $L = L' + 1$.

An automorphism fixing e must fix both v and v', and so by Theorems 2.3.4 and 2.3.6 we have that either $\mathbb{Q}(\varphi) = K(\ell^L\mathfrak{f}_0)$, or $[K(\ell^L\mathfrak{f}_0) : \mathbb{Q}(\varphi)] = 2$. In the latter case, there exists an involution $\sigma \in \mathrm{Gal}(K(\ell^L\mathfrak{f}_0)/\mathbb{Q})$ fixing v, and we know precisely when this occurs by Theorem 2.3.6 – that is, when $D(K) = 1$.

Assume that $\mathfrak{f}_0^2\Delta_K < -4$, such that $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ has the structure of an ℓ-volcano. (We will deal with the case of $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$ in the remarks leading up to Proposition 4.4.1.) If e is the unique edge between v and a vertex in level L', then e is fixed by σ if and only if v is. This is the case unless $L = L' = 0$ and ℓ splits in K, in which case there are two edges from v to surface vertices (which are not necessarily unique, or distinct from v). In either of these cases, consider $[(E \times E', \iota)]$, with E having CM by $\mathfrak{o}(\mathfrak{f}_0)$, a decomposition of our QM abelian surface corresponding to v_1. The two outward edges from v then have corresponding kernels $\iota(\mathcal{O}) \cdot E[\mathfrak{p}]$ and $\iota(\mathcal{O}) \cdot E[\overline{\mathfrak{p}}]$, with $\mathfrak{p}$ a prime ideal in $\mathfrak{o}(\mathfrak{f}_0)$ of norm ℓ.

We claim that, in this situation, the involution $\sigma \in \mathrm{Gal}(K(\mathfrak{f}_0)/\mathbb{Q})$ fixing v cannot fix $\mathfrak{p}$, and hence cannot fix our edge e. Indeed, the exact statement of Theorem 2.3.6 says that

$\sigma = \tau\sigma_{\mathfrak{a}}$ for a certain ideal $\mathfrak{a}$ of $\mathfrak{o}(\mathfrak{f}_0)$, so to fix e it would have to be the case that $\sigma_{\mathfrak{a}}$ acts on e and hence on v by complex conjugation. It follows from [GR06, Lemma 5.10] that this cannot be the case, as $\omega_{D(K)}$ acts non-trivially on v. From this discussion, we reach the following result regarding fields of moduli corresponding to our edges.

Proposition 4.2.7. *Let φ be a QM cyclic ℓ-isogeny corresponding to an edge e from v to v' in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ as above, with $\mathfrak{f}_0^2\Delta_K < -4$.*

- *If $D(K) \neq 1$, i.e., if there is a prime $p \mid D$ which is inert in K, then $\mathbb{Q}(\varphi) = K(\ell^L\mathfrak{f}_0)$.*
- *Suppose that $D(K) = 1$.*
  - *If φ is a QM cyclic isogeny of QM abelian surfaces with CM by $\mathfrak{o}(\mathfrak{f}_0)$ and ℓ splits in K, then $\mathbb{Q}(\varphi) = K(\mathfrak{f}_0)$.*
  - *Otherwise, $[K(\ell^L\mathfrak{f}_0) : \mathbb{Q}(\varphi)] = 2$, with $\mathbb{Q}(\varphi)$ equal to the field of moduli corresponding to v as described in Theorem 2.3.6.*

4.3 The action of Galois on $\mathcal{G}^D_{K,\ell,f_0}$

We have an action of $\mathrm{Aut}(\mathbb{C})$ on $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$: an automorphism σ maps a vertex v corresponding to an isomorphism class of QM abelian surfaces $[(A,\iota)]$ to the vertex corresponding to $[(\sigma(A),\sigma(\iota))]$, and edges are mapped to edges via the action on the corresponding isomorphism classes of isogenies. This action factors through $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and preserves the level of a vertex. It follows that it also preserves the notions of ascending, descending and horizontal for paths.

For a fixed level $L \geq 0$, let $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0,L}$ denote the portion of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ from the surface (level 0) to level L:

$$\mathcal{G}^D_{K,\ell,\mathfrak{f}_0,L} := \bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,\ell,\mathfrak{f}_0}.$$

By Theorem 2.3.4, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0,L}$ factors through $\mathrm{Gal}(K(\ell^L\mathfrak{f}_0)/\mathbb{Q})$. If $D(K) \neq 1$, i.e., if there is some prime $p \mid D$ which is inert in K, then Theorem 2.3.6 says that the action of this group on V_L is free. Otherwise, each vertex v in level L is fixed by some

involution σ, and the class of QM abelian surfaces corresponding to v has field of moduli isomorphic to $K(\ell^L\mathfrak{f}_0)^\sigma$.

We now fix a vertex v in level L in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$, and suppose that $\sigma \in \mathrm{Gal}(K(\ell^L\mathfrak{f}_0)/\mathbb{Q})$ is an involution fixing v, forcing $D(K) = 1$. In the following two sections, we provide an explicit description of the action of σ on $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0,L}$ in all cases. First, we note here the number of vertices at each level fixed by σ.

Proposition 4.3.1. *Let $x \in X^D(1)_{/\mathbb{Q}}$ be an $\mathfrak{o}(\ell^L\mathfrak{f}_0)$-CM point fixed by an involution $\sigma \in \mathrm{Gal}(K(\ell^L\mathfrak{f}_0)/\mathbb{Q})$. Let b denote the number of prime divisors of D which are inert in K. For $0 \le L' \le L$, the number of vertices of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ in level L' fixed by σ is*

$$2^b \cdot \#\mathrm{Pic}(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))[2].$$

Proof. By Theorem 2.3.6, the involution σ is of the form $\sigma = \tau \circ \sigma_0$ for some $\sigma_0 \in \mathrm{Pic}(\mathfrak{o}(\ell^L\mathfrak{f}_0))$, where τ denotes complex conjugation. The set of vertices of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ at level L' has cardinality $2^b \cdot h(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))$, consisting of 2^b orbits under the action of $\mathrm{Pic}(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))$. Each orbit is a $\mathrm{Pic}(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))$-torsor, and σ_0 yields a bijection on each.

As a result, we have that the number of level L' vertices in a given orbit which are fixed by σ is the same as the number of elements of $\mathrm{Pic}(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))$ fixed by τ. As shown in [Cl23, Prop 2.6], this count is equal to $\#\mathrm{Pic}(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))[2]$, as τ acts on $\mathrm{Pic}(\mathfrak{o}(\ell^{L'}\mathfrak{f}_0))$ by inverting ideals. □

Regarding this count, by [Cox13, Prop 3.11] we have the following:

Lemma 4.3.2. *Let r denote the number of distinct odd prime divisors of a fixed imaginary quadratic discriminant Δ. Then $\mathrm{Pic}(\mathfrak{o}_\Delta)[2] \cong (\mathbb{Z}/2\mathbb{Z})^\mu$, where*

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

4.4 The field of moduli of a QM-cyclic ℓ^a isogeny

Let φ be a QM cyclic ℓ^a isogeny of K-CM abelian surfaces inducing a $\Delta = \mathfrak{f}^2\Delta_K$-CM point on $X_0^D(\ell^a)_{/\mathbb{Q}}$, with $\ell \nmid D$. Let P be the length a non-backtracking path in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ corresponding to φ, via Lemma 4.2.6, for the appropriate $\mathfrak{f}_0 \in \mathbb{Z}^+$. The ordered edges in P correspond to a decomposition

$$\varphi = \varphi_1 \circ \cdots \circ \varphi_a,$$

where each φ_i is a QM-cyclic ℓ-isogeny. If $\Delta < -4$, then Lemma 4.1.2 provides

$$\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi_1) \cdots \mathbb{Q}(\varphi_a),$$

and for $\mathfrak{f}_0^2\Delta_K < -4$ Proposition 4.2.7 determines $\mathbb{Q}(\varphi_i)$ for each i. Note that if $\mathbb{Q}(\varphi_i)$ is a ring class field for any i, then $\mathbb{Q}(\varphi)$ must contain K

For $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$, it is impossible to have $D(K) = 1$ unless $D = 1$, as Δ_K has only a single prime divisor while D has at least 2. This is of course consistent with, and can be seen from, the general fact that Shimura curves have no real points when $D > 1$; the residue field of a -3-CM or -4-CM point on $X^D(1)_{/\mathbb{Q}}$ must be K in this situation. By these observations and the discussion of the Galois action in the previous section, we have the following proposition.

Proposition 4.4.1. *Let $\varphi : (A, \iota) \to (A', \iota')$ be a QM-cyclic ℓ^a isogeny. Suppose that (A, ι) has K-CM with central conductor $\mathfrak{f}_A = \ell^a\mathfrak{f}_0$ and that (A', ι') has central conductor $f_{A'} = \ell^{a'}\mathfrak{f}_0$. Let $L = \max\{a, a'\}$. Let P be the path corresponding to φ in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0,L}$.*

- *If $D(K) \neq 1$, i.e., if there is a prime $p \mid D$ which is inert in K, then $\mathbb{Q}(\varphi) = K(\ell^L\mathfrak{f}_0)$.*
- *Suppose that $D(K) = 1$ and $\mathfrak{f}_0^2\Delta_K < -4$.*
  - *If ℓ splits in K and φ factors through an ℓ-isogeny of QM abelian surfaces with $\mathfrak{f}_0^2\Delta_K$-CM, then $\mathbb{Q}(\varphi) = K(\ell^L\mathfrak{f}_0)$.*

– *Suppose that we are not in the previous case. Let* $\sigma \in \mathrm{Gal}(K(\ell^L\mathfrak{f}_0)/\mathbb{Q})$ *be an involution fixing the class of* (A,ι) *or* (A',ι')*. If* σ *fixes the path* P*, then* $\mathbb{Q}(\varphi) = K(\ell^L\mathfrak{f}_0)^\sigma$*. Otherwise,* $\mathbb{Q}(\varphi) = K(\ell^L\mathfrak{f}_0)$*.*

We now explicitly analyze the Galois action in all cases as done in [Cl23, §5.3] and [CS23, §4.2] in the $D = 1$ case. (There are additional subtleties when $D = 1$ and $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$, handled in [CS23] in a manner we will recall.) Borrowing the notation therein, for a specified $K, \mathfrak{f}_0$, and ℓ we let

$$\tau_L := \#\mathrm{Pic}(\mathfrak{o}(\ell^L\mathfrak{f}_0)[2].$$

By Proposition 4.3.1, the number of vertices in level L' in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ which are fixed by an involution $\sigma \in \mathrm{Pic}(\ell^L\mathfrak{f}_0)$ of the type we are studying is $2^b \cdot \tau_{L'}$.

4.5 Explicit description: $\mathfrak{f}_0^2\Delta_K < -4$

In the current section, we assume $\mathfrak{f}_0^2\Delta_K < -4$, such that each component of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ has the structure of an ℓ-volcano of infinite depth. This is in exact parallel to [Cl23, §5.3], baring the same structure of results.

Let $0 \le L' \le L$, and let $\sigma \in \mathrm{Pic}(\ell^L\mathfrak{f}_0)$ be an involution fixing a vertex v in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ in level L. In the following lemmas, we describe the action of σ on $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0,L}$. In each case, we provide example figures of a component of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ (up to some finite level). In these graphs, vertices and edges colored purple are fixed by the action of the designated involution σ, while black edges and vertices are acted on non-trivially by σ. Without loss of generality based on the symmetry of our graph components, we will always take v to be the left-most vertex in level L in our figures.

Lemma 4.5.1. *Let* $\ell > 2$ *be a prime which is unramified in* K *and* $\mathfrak{f}_0 \in \mathbb{Z}^+$ *with* $\mathfrak{f}_0^2\Delta_K < -4$*. Let* v, L *and* σ *be as above with* $L \ge 1$*, and consider the action of* σ *on*

$$\bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,\ell,\mathfrak{f}_0}.$$

Each surface vertex has two descendants fixed by σ in level 1. For $1 \leq L' < L$, each fixed vertex in level L' has a unique fixed descendent in level $L' + 1$.

Proof. By Lemma 4.3.2 we have $\tau_1 = 2\tau_0$, while $\tau_{L'} = \tau_{L'+1}$ for $1 \leq L' < L$. The number of edges descending from a given vertex in level $L' \geq 1$ is ℓ, hence is odd, and so we immediately see that each fixed vertex in level L' with $1 \leq L' \leq L$ must have at least one fixed descendant in level $L' + 1$, hence exactly one by our count.

The number of descending edges from a given surface vertex is either $\ell+1$ or $\ell-1$ depending on whether ℓ is inert or split in K, hence is even in both cases. With our involution being of the form $\sigma = \tau\sigma_0$, a translated version of the argument of [CS23, Cor. 5.5] gives that each fixed surface vertex has at least one fixed descendant in level 1. Therefore, each fixed surface vertex must have at least two fixed descendants in level 1 by parity, giving the result. □

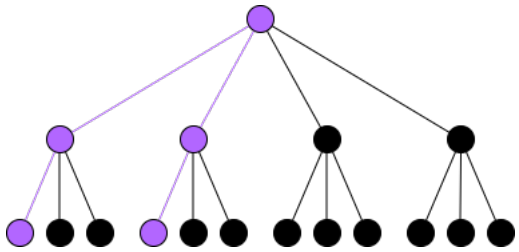

Figure 4.1: $\ell = 3$ inert in K with $L = 2$

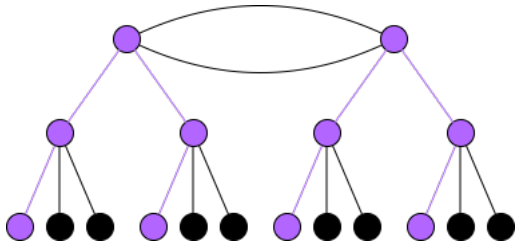

Figure 4.2: $\ell = 3$ split in K with $L = 2$

Lemma 4.5.2. *Let $\ell > 2$ be a prime that ramifies in K and $\mathfrak{f}_0 \in \mathbb{Z}^+$ with $\mathfrak{f}_0^2 \Delta_K < -4$. Let v, L and σ be as above, and consider the action of σ on*

$$\bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,\ell,\mathfrak{f}_0}.$$

Any vertex v' in level L' with $0 \leq L' < L$ which is fixed by σ has exactly one descendant in level $L'+1$ fixed by σ.

Proof. Each vertex in level L' has ℓ descendants in level $L'+1$. A descendant of v' must be sent to another descendant of v' by σ, by virtue of v' being fixed by σ. At least one descendant must be fixed by σ by the assumption that ℓ is odd. Lemma 4.3.2 gives that $\tau_{L'} = \tau_{L'+1}$, and so there must be exactly one fixed descendant of v'. □

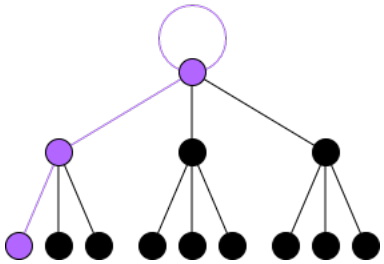

Figure 4.3: $\ell = 3$ ramified in K with $|V_0| = 1$ and $L = 2$

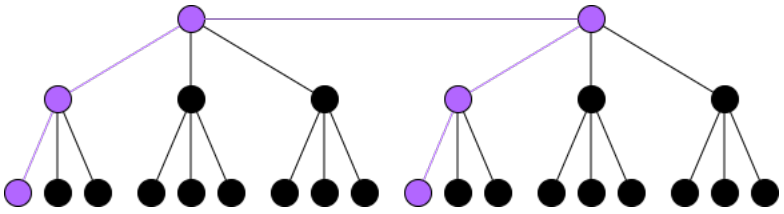

Figure 4.4: $\ell = 3$ ramified in K with $|V_0| = 2$ and $L = 2$

Lemma 4.5.3. *Suppose that $\ell = 2$ is unramified in K and that $\mathfrak{f}_0^2\Delta_K \neq -3$. Let v, L and σ be as above with $L \geq 1$, and consider the action of σ on*

$$\bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,2,\mathfrak{f}_0}.$$

1. *Every surface vertex fixed by σ has a unique fixed descendant in level 1.*

2. *Suppose $L \geq 2$. Each vertex in level 1 which is fixed by σ has all of its descendants in levels 2 to $min(L, 3)$ fixed by σ.*

3. *Let $3 \leq L' < L$. If v' is a vertex in level L' fixed by σ, then the vertex w in level L' which shares a neighbor in level $L' - 1$ with v' is also fixed by σ, and exactly one of v' and w has its two descendants in level $L' + 1$ fixed by σ.*

Proof. (1) Lemma 4.3.2 provides $\tau_1 = \tau_0$. If 2 is inert in K, then each fixed surface vertex has three neighbors in level 1 and hence at least one must be fixed. The count then implies exactly one of these neighbors must be fixed. If 2 splits in K, then each fixed surface vertex has exactly one neighbor in level 1 which then must be fixed.

(2) Lemma 4.3.2 provides $\tau_3 = 2\tau_2$ and $\tau_2 = 2\tau_1$. As each non-surface vertex has two immediate descendants in the next level, the claim follows.

(3) For $3 \leq L' < L$, we have $\tau_{L'+1} = \tau_L$. Let $v_{L'}$ be a fixed vertex in level L' having a fixed neighbor vertex in level $L' - 1$. By a parity argument, there must then be another fixed vertex $w_{L'}$ in level L' with the same neighbor in level $L' - 1$ as $v_{L'}$. By the count, it suffices to show that $v_{L'}$ and $w_{L'}$ cannot both have descendants fixed by σ.

Suppose to the contrary that $v_{L'+1}$ and $w_{L'+1}$ are σ-fixed neighbors of $v_{L'}$ and $w_{L'}$, respectively, in level $L' + 1$. We find that this cannot be the case as in [Cl23, Lemma 5.6 c]; this would imply that we have a QM-cyclic 2^4-isogeny which , upon restriction, would provide a cyclic, real 2^4-isogeny of elliptic curves with CM by $\Delta = 2^{2L+2}\mathfrak{f}_0^2\Delta_K$. This in turn implies the existence of a primitive, proper real $\mathfrak{o}(2^{L+1}\mathfrak{f}_0)$-ideal of index 16, which does not exist. □

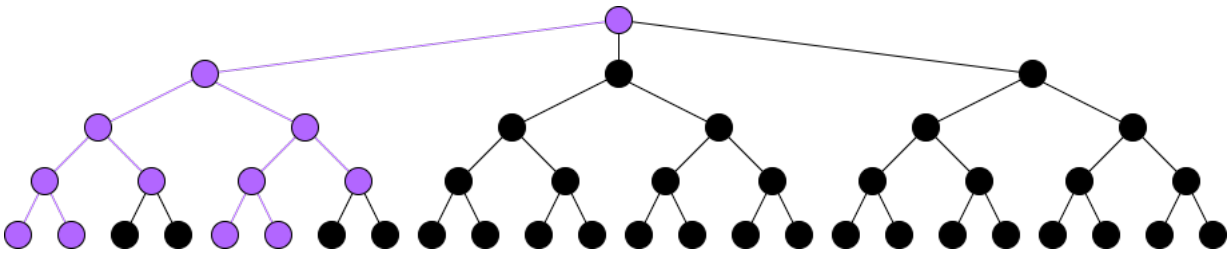

Figure 4.5: $\ell = 2$ inert with $L = 4$

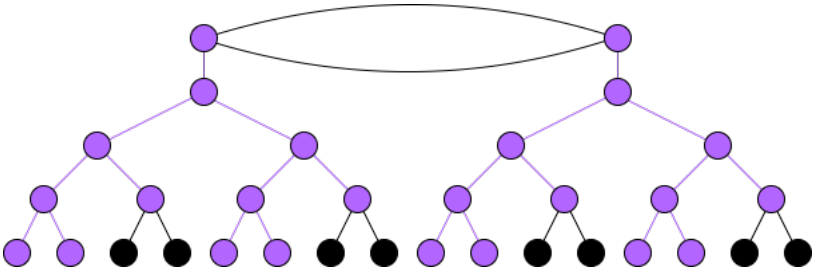

Figure 4.6: $\ell = 2$ split with $L = 4$

In the case of $\ell = 2$ ramifying in K, the discriminant of K must be of the form $\Delta_K = 4m$ for $m \equiv 2$ or $3 \pmod 4$, and so $\Delta_K \equiv 8$ or $12 \pmod{16}$. Hence, the discriminant of the order $\mathfrak{o}(\mathfrak{f}_0)$ corresponding to the surface of $\mathcal{G}^D_{K,2,\mathfrak{f}_0}$ will also lie in one of these congruence classes mod 16. Whether these components have a surface loop is answered by the following lemma.

Lemma 4.5.4. *Consider a component of $\mathcal{G}^D_{K,2,\mathfrak{f}_0}$ with 2 ramified in K. The surface V_0 of this component consists of a single vertex with a single self-loop if and only if $\Delta_K \in \{-4, -8\}$ and $\mathfrak{f}_0 = 1$.*

Proof. This proof comes down to a simple argument about ideals of norm 2 in $\mathfrak{o}(f_0)$, as in [Cl23, Lemma 5.7] □

The following lemmas therefore cover all possible cases.

Lemma 4.5.5. *Let $\Delta_K = -8$ and $\ell = 2$, and let v, L and σ be as above with $L \geq 1$. Consider the action of σ on*

$$\bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,2,1}.$$

1. *The two descendants in level* 1 *of the single surface vertex are fixed by* σ.

2. *For* $1 < L' < L$, *there are* 2 *vertices in level* L' *fixed by* σ *and they have a common neighbor vertex in level* $L' - 1$. *One of these must have both descendants in level* $L' + 1$ *fixed by* σ, *while the other has its direct descendants swapped by* σ.

Proof. There is a single vertex on the surface, as the class number of K is 1. Lemma 4.3.2 tells us that $\tau_1 = 2\tau_0$ in this case, so both descendants of the surface vertex are fixed by σ. For $1 \leq L' < L$, we have

$$\tau_{L'+1} = \tau_{L'} = 2,$$

so one of the fixed vertices in level L' must have both descendants in level $L' + 1$ fixed by σ, while the other has its vertices swapped by σ. □

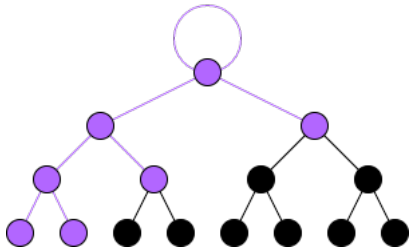

Figure 4.7: $\mathfrak{f}_0^2\Delta_K = -8$ and $\ell = 2$ with $L = 3$

Lemma 4.5.6. *Suppose that* $\Delta_K \equiv 12 \pmod{16}$ *and* $\mathfrak{f}_0^2\Delta_K \neq -4$ *with* $\ell = 2$. *Let* v, L *and* σ *be as above with* $L \geq 1$. *Consider the action of* σ *on*

$$\bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,2,\mathfrak{f}_0}.$$

1. *There are two surface vertices, both fixed by* σ. *One surface vertex, which we will denote by* v_0, *has both descendants in level* 1 *fixed by* σ, *while the other has its level* 1 *descendants swapped by* σ.

2. *If* $L \geq 2$ *(such that the action of* σ *is defined at level* 2*), then each of the* 4 *vertices in level* 2 *which descend from* v_0 *are fixed by* σ.

3. *For $2 \leq L' < L$ and for a vertex v' in level L' fixed by σ, let w denote the other level L' vertex sharing a neighbor vertex in level $L'-1$ with v' (which must also be fixed by σ). Exactly one of v' or w has both descendants in level $L'+1$ fixed by σ, while the other vertex has its direct descendants swapped by σ.*

Proof. In this case the surface has two σ-fixed vertices with a single edge between them. We have

$$\tau_1 = \tau_0 \quad \text{and} \quad \tau_2 = 2\tau_1$$

by Lemma 4.3.2, giving parts (1) and (2). For $2 \leq L' < L$, we have

$$\tau_{L'} = \tau_{L'-1},$$

so half of the σ-fixed vertices in level $L'-1$ must have both descendants in level L' fixed by σ, while the other half have their descendants in level L' swapped by σ. That there must be exactly one pair of fixed vertices in level L' descending from a given fixed vertex in level $L'-2$ follows as in part (3) of Lemma 4.5.3. □

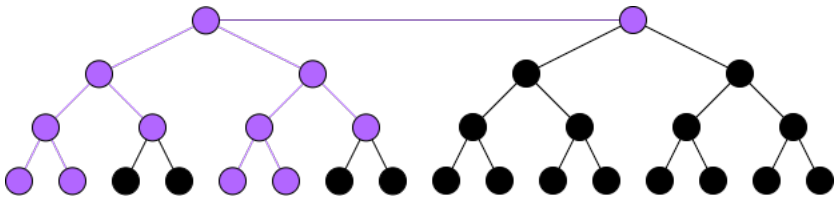

Figure 4.8: $\Delta_K \neq -4$ with $\ell = 2, \mathrm{ord}_2(\Delta_K) = 2$ and $L = 3$

Lemma 4.5.7. *Suppose that $\Delta_K \equiv 8 \pmod{16}$ with $\Delta_K < -8$ and $\ell = 2$. Let v, L and σ be as above with $L \geq 1$. Consider the action of σ on*

$$\bigsqcup_{i=0}^{L} V_i \subseteq \mathcal{G}^D_{K,2,\mathfrak{f}_0}.$$

1. *There are two surface vertices, both fixed by σ, and all 4 vertices in level 1 are fixed by σ.*

2. *For $1 \leq L' < L$ and for a vertex v' in level L' fixed by σ, let w denote the other level L' vertex sharing a neighbor vertex in level $L'-1$ with v'. Exactly one of v' or w has both descendants in level $L'+1$ fixed by σ, while the other vertex has its direct descendants swapped by σ.*

Proof. In this case again we have two σ-fixed vertices comprising our surface. Here Lemma 4.3.2 gives $\tau_1 = 2\tau_0$, providing part (1). For $1 \leq L' < L$, Lemma 4.3.2 gives $\tau_{L'} = \tau_{L'-1}$. The same argument as in part (3) of Lemma 4.5.6 then provides part (2). □

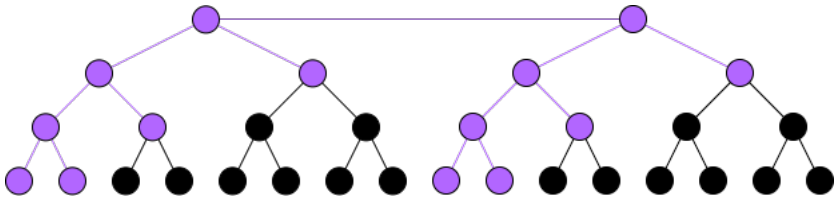

Figure 4.9: $\Delta_K < -8$ with $\ell = 2, \mathrm{ord}_2(\Delta_K) = 3$ and $L = 3$

4.6 Explicit description part II: $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$

Keeping our notation from the previous section, we now assume $\mathfrak{f}_0 = 1$ and $\Delta_K \in \{-3, -4\}$. As mentioned earlier in this section, we have $D(K) \neq 1$ if and only if $D \neq 1$ in this case. Therefore, if $D > 1$ then the action of $\mathrm{Gal}(K(\ell^L\mathfrak{f})/\mathbb{Q})$ on V_L is free for all $L \geq 0$. This is wonderful news for us; while the CM fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ require extra attention at other points in this study, they cause absolutely no difficulties as far as determining the explicit Galois action on $\mathcal{G}^D_{K,\ell,1}$ unless $D = 1$, which is the case handled in [CS23, §4]. There, much care goes into defining and explicitly describing an action of complex conjugation on CM components of isogeny graphs in these cases. We first recall the action in this $D = 1$ case, and then quickly remark further on the $D > 1$ case for clarity.

4.6.1 The case $D = 1$

For $D = 1$, we may orient ourselves (via choice of vertex) such that an involution $\sigma \in \mathrm{Gal}(K(\ell^L\mathfrak{f}_o)/\mathbb{Q})$ fixing a vertex in level L is complex conjugation, which we denote as $\sigma = \tau \in \mathrm{Gal}(K(\ell^L\mathfrak{f}_0)/\mathbb{Q}(\ell^L\mathfrak{f}_0)$. In this section, we handle the case of $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$, and hence $\mathcal{G}^1_{K,\ell,1}$ is not an ℓ volcano due to having edges with multiplicity between levels 0 and 1. That said, we still have the following:

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

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

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

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

$$j_L \coloneqq j(\mathbb{C}/\mathfrak{o}(\ell^L)).$$

In our diagrams, this is always the leftmost vertex in a given level. The lattice $\mathfrak{o}(\ell^L)$ gives rise to a particular model E_L over $\mathbb{Q}(j_L) \cong \mathbb{Q}(\ell^L)$ and hence to a particular model over $\mathbb{R}$. These models are compatible: for all $L \geq 1$, the upward edge from j_L to j_{L-1} is realized by the $\mathbb{Q}(j_L)$-rational isogeny $\mathbb{C}/\mathfrak{o}(\ell^L) \to \mathbb{C}/\mathfrak{o}(\ell^{L-1})$. With this setup, we now provide the explicit analysis of the action of τ in each case:

- Suppose $\Delta = -4$ and $\ell > 2$. We have $\tau_0 = 1$ and $\tau_L = 2$ for all $L \geq 1$. Each real vertex v in level $L \geq 1$ has an odd number, ℓ, of descendant vertices, so at least one of these must be fixed by complex conjugation, and it follows that v has exactly one real descendant.

It remains to discuss the action of complex conjugation on the set of directed edges emanating from the surface vertex v_0, which corresponds to "the" elliptic curve $E_{/\mathbb{C}}$ with j-invariant 1728. By [Cl23, Thm. 5.3], for any real elliptic curve and any odd prime ℓ, there are exactly 2 order ℓ-subgroups of $E(\mathbb{C})$ stabilized by complex conjugation. When $\ell \equiv 1 \pmod 4$ there are two surface loops corresponding to $E[\mathfrak{p}]$ and $E[\overline{\mathfrak{p}}]$ where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the two $\mathbb{Z}[\sqrt{-1}]$-ideals of norm ℓ. These two edges are interchanged by complex conjugation (independently of the chosen $\mathbb{R}$-structure on E). So the two real edges must be downward edges. For each real level one vertex v, there is a pair of edges from v_0 to v; evidently complex conjugation stabilizes the pair, so if one is real, then both are real. It follows that for exactly one of the two level 1 real vertices both edges from the surface to that vertex are real, whereas for the other level 1 real vertex neither edge is real. Which is which depends upon the chosen $\mathbb{R}$-structure on v_0: indeed, for each level 1 real vertex v, the unique upward edge $e : v \to v_0$ can be defined over $\mathbb{Q}(j(E_v))$ and hence over $\mathbb{R}$; this provides an $\mathbb{R}$-model for E on which the dual isogeny is real.

If our path starts at v_0 and ends at level L then it is clear that the field of moduli is $K(\ell^L)$ if the path includes a surface edge, and is isomorphic to $\mathbb{Q}(\ell^L)$ otherwise. The harder case is if our path starts at j_L with $L \geq 1$ and ascends to the surface. In this case, when we ascend to the surface we get the real model for E given by the lattice $\mathbb{Z}[\sqrt{-1}]$, and *in this real model* it is the two edges from j_0 to j_1 that are real. The significance of this for our counting problem is that if we start below the surface and ascend to the surface, then there is a unique way to extend the path so that the corresponding isogeny is fixed under complex conjugation: we take the unique edge from j_0 to j_1 that is not the inverse of the ascending edge from j_1 to j_0.

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

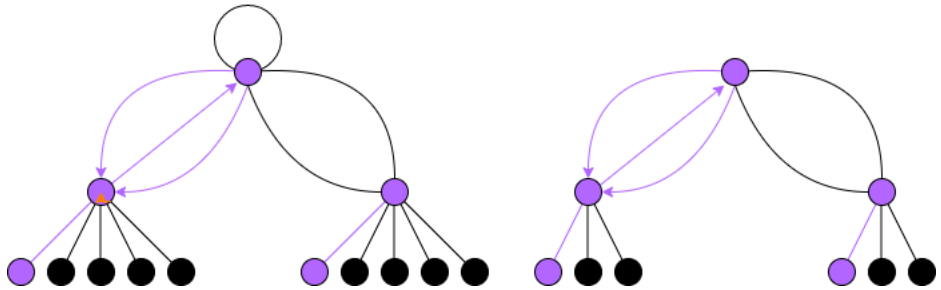

Figure 4.10: $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-1}),\ell,1}$, ℓ split ($\ell = 5$, left) and inert ($\ell = 3$, right) up to level 2

- Suppose $\Delta = -3$ and $\ell > 3$. As above, we have $\tau_0 = 1$ and $\tau_L = 2$ for all $L \geq 2$. And again, each real vertex v in level $L \geq 1$ has an odd number, ℓ, of descendant vertices, so v has a unique real descendant. If $\ell \equiv 1 \pmod 3$ there is a pair of surface loops that are interchanged by complex conjugation; if $\ell \equiv 2 \pmod 3$ there are no surface edges. So by [Cl23, Thm. 5.3] in either $\mathbb{R}$-model of "the" elliptic curve $E_{/\mathbb{C}}$ with j-invariant 0 corresponding to the surface vertex v_0 there are precisely 2 order ℓ-subgroups stable under complex conjugation. But this time things work out more nicely: there are three edges from v_0 to each of the two real level 1 vertices, which as a set are stable under complex conjugation. Since 3 is odd, at least one edge in each set must be fixed by τ, hence exactly one because there are three such edges in total.

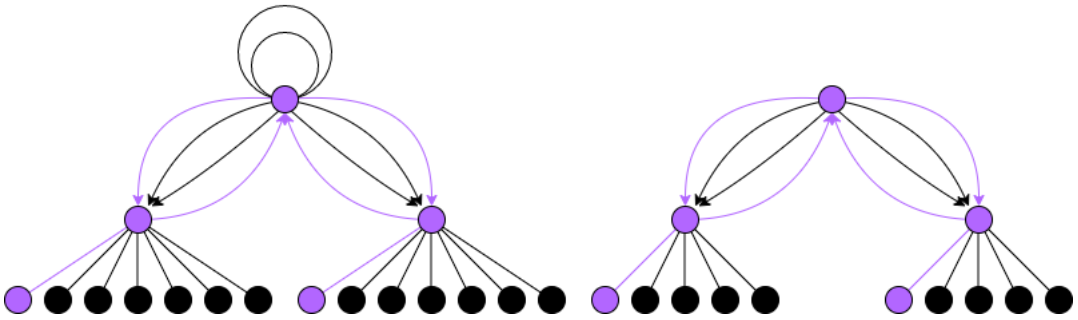

Figure 4.11: $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-3}),\ell,1}$, ℓ split ($\ell = 7$, left) and inert ($\ell = 5$, right) up to level 2

- Suppose $\Delta = -3$ and $\ell = 2$. Now we have $\tau_0 = \tau_1 = 1$, $\tau_2 = 2$ and $\tau_L = 4$ for all $L \geq 3$. This means that every vertex of level $L \leq 3$ is real. For each $L \geq 3$, the real vertices of level L can be partitioned into pairs in which each pair has a common neighbor in level $L-1$, and in each pair, exactly one of the two vertices has two real descendants and the other vertex has no real descendants. This follows from the same argument as in the proof of [Cl23, Lemma 5.7c)].

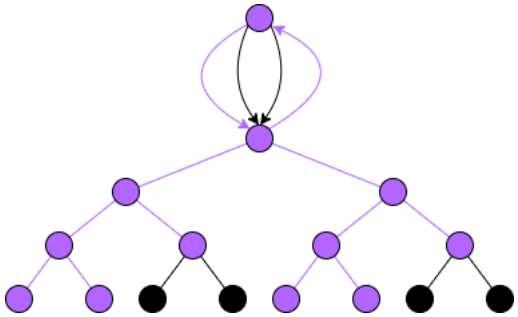

Figure 4.12: $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-3}),2,1}$ up to level 4

- Suppose $\Delta = -4$ and $\ell = 2$. We have $\tau_0 = \tau_1 = 1$ and $\tau_L = 2$ for all $L \geq 2$. For all $L \geq 2$, the vertex v_L corresponding to j-invariant j_L is real; the other real vertex in level L therefore must be the other descendant vertex from v_{L-1}.

  Let us now discuss the action of complex conjugation on edges. Let $E_{/\mathbb{C}}$ be "the" elliptic curve of j-invariant 1728. In either $\mathbb{R}$-model of E, the surface loop corresponds to the isogeny with kernel $E[\mathfrak{p}]$, where $\mathfrak{p}$ is the unique prime ideal of $\mathbb{Z}[\sqrt{-1}]$ lying over 2, which is stable under complex conjugation. If we choose the $\mathbb{R}$-model of E with real lattice $\mathbb{Z}[\sqrt{-1}]$, then all three order 2 subgroups are stable under complex conjugation: they can be seen quite clearly as $\frac{1}{2} + \mathbb{Z}[\sqrt{-1}]$, $\frac{\sqrt{-1}}{2} + \mathbb{Z}[\sqrt{-1}]$ and $\frac{1+\sqrt{-1}}{2} + \mathbb{Z}[\sqrt{-1}]$. So it may seem that we have defined an action of complex conjugation on $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-1}),2,1}$.

  However, this graph cannot be used for our study of isogenies! To see why, consider either of the two paths that starts at the vertex v_1 in level 1, ascends to level 0, takes the surface loop, and then descends back down to level 1. These correspond to two cyclic 8-isogenies with source elliptic curve of discriminant -16. However, contrary to

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

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

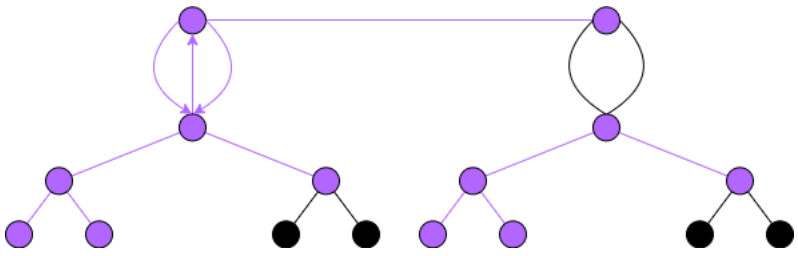

Figure 4.13: the double cover $\widetilde{\mathcal{G}}$ of $\mathcal{G}^1_{\mathbb{Q}(\sqrt{-1}),2,1}$ up to level 3

Remark 4.6.1.

a) In Figure 4.13, we did not draw the upward edge with initial vertex the level 1 vertex in the right hand copy of $\mathcal{G} = \mathcal{G}_{\mathbb{Q}(\sqrt{-1}),2,1}$. As far as the action of τ on $\widetilde{\mathcal{G}}$ is concerned, it is clear that this edge must be fixed. However the τ-fixedness of this edge has no elliptic curve interpretation; no nonbacktracking path starting in the lefthand copy of $\mathcal{G}$ in $\widetilde{\mathcal{G}}$ contains this edge. Drawing this edge as τ-fixed seems to invite confusion, so we have not done so.

b) It's interesting to compare $\widetilde{\mathcal{G}}$ to Figure 4.5. These graphs are not isomorphic, but their enumerations of real and complex paths are the same.

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

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

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

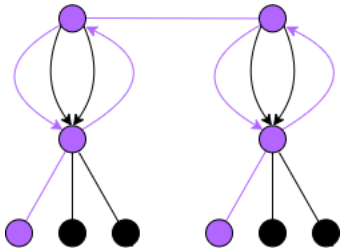

Figure 4.14: the double cover $\widetilde{\mathcal{G}}$ of $\mathcal{G} = \mathcal{G}_{\mathbb{Q}(\sqrt{-3}),3,1}$ up to level 2

While in the previous case the change of $\mathbb{R}$-structure changed the *number* of order $\ell = 2$ subgroups fixed by complex conjugation, in this case $\ell = 3$, so [Cl23, Thm. 5.1] applies to show that in any $\mathbb{R}$-model exactly one of the three "downward" order 3 subgroups is real. While in the previous case we needed to pass to the double cover in order to ensure the correctness of our enumeration of real and complex paths, in this case the enumeration of real and complex paths is the same whether we pass from $\mathcal{G}$ to $\widetilde{\mathcal{G}}$ or not.

4.6.2 The case $D > 1$

As we have noted, the action of $\mathrm{Gal}(K(\ell^L\mathfrak{f})/\mathbb{Q})$ on V_L is free for all $L \geq 0$ when $D > 1$. Still, we provide here example figures of components of $\mathcal{G}_{K,\ell,1}$ (up to finite level L) for each case as reference for the reader for the path type analysis and enumeration done in §5.1. In these cases, edges from level 0 to 1 have multiplicity, as exposited in [CS23, §3] and seen in the previous section, due to the presence of automorphisms that do not fix kernels of isogenies. We therefore *do not* have a one-to-one identification between edges and "dual" edges in this case, and so as in the referenced study we clearly denote edges with orientation and multiplicity between levels 0 and 1.

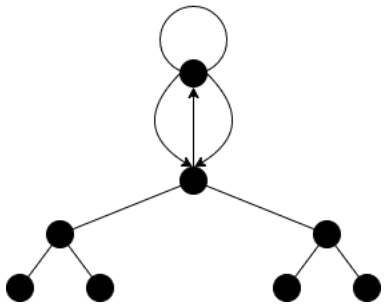

Figure 4.15: $\mathfrak{f}_0^2\Delta_K = -4, \ell = 2$ up to level 3

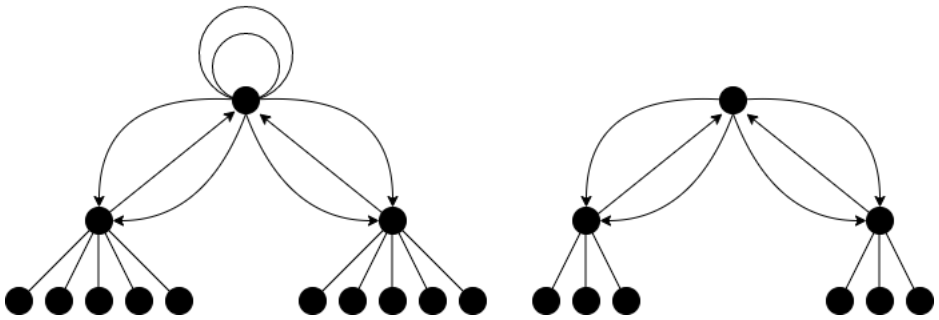

Figure 4.16: $\mathfrak{f}_0^2\Delta_K = -4$, ℓ split ($\ell = 5$, left) and inert ($\ell = 3$, right) up to level 2

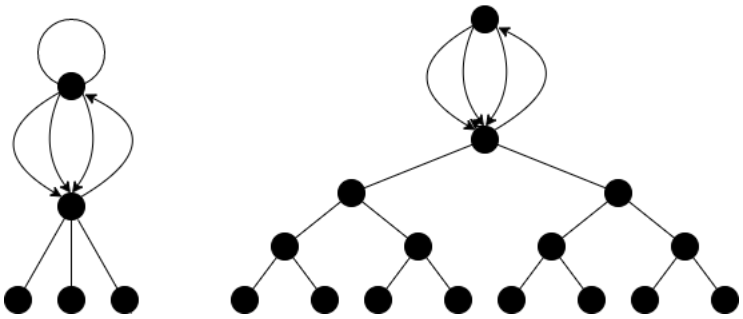

Figure 4.17: $\mathfrak{f}_0^2\Delta_K = -3, \ell = 3$ up to level 2 (left) and $\ell = 2$ up to level 3 (right)

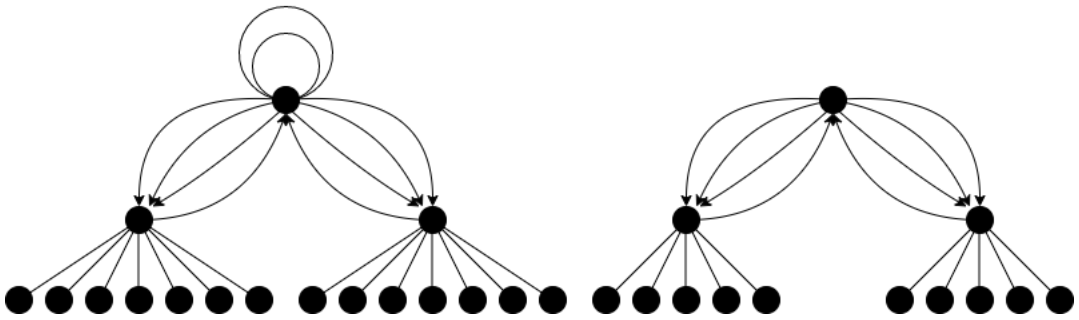

Figure 4.18: $\mathfrak{f}_0^2\Delta_K = -3$, ℓ split ($\ell = 7$, left) and inert ($\ell = 5$, right) up to level 2

Chapter 5

CM points on Shimura curves

5.1 CM points on $X_0^D(\ell^a)_{/\mathbb{Q}}$

We fix ℓ^a a prime power with $\ell \nmid D$ and $\Delta = \mathfrak{f}^2\Delta_K = \ell^{2L}\mathfrak{f}_0^2\Delta_K$, with $\gcd(\mathfrak{f}_0, \ell) = 1$, an imaginary quadratic discriminant. In this section, we describe the Δ-CM locus on $X_0^D(\ell^a)_{/\mathbb{Q}}$. To this aim, we fully classify all closed point equivalence classes, by which we mean $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits, of non-backtracking, length a paths in $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$. We record the number of classes of each type with each possible residue field (up to isomorphism).

In the $\mathfrak{f}_0^2\Delta_K \in \{-3, -4\}$ cases, the notion of backtracking in $\mathcal{G}^D_{K,\ell,1}$ has subtlety between levels 0 and 1 that is not present in isogeny volcanoes. We address this now: traversing *any* edge from a vertex v in level 0 to a vertex w in level 1 followed by the single edge from w to v corresponds to a composition of dual isogenies, and thus is backtracking. On the other hand, for a given isogeny φ corresponding to the edge e from w to v, there is a single edge from v to w corresponding to its dual $\widehat{\varphi}$. Therefore, traversing e followed by the other edge (respectively, either of the two other edges) from v to w *does not* count as backtracking in the case of $\mathfrak{f}_0^2\Delta_K = -4$ (respectively, $\mathfrak{f}_0^2\Delta_K = -3$).

With b denoting the number of prime divisors of D which are inert in K, we have 2^b Δ-CM points on $X^D(1)_{/\mathbb{Q}}$, with the fibers over each under the natural map from $X_0^D(\ell^a)_{/\mathbb{Q}}$

to $X^D(1)_{/\mathbb{Q}}$ being isomorphic via Atkin-Lehner involutions. In all cases, we then have

$$\sum_{C(\varphi)} e_\varphi d_\varphi = 2^b \deg(X_0(\ell^a) \to X(1)) = 2^b \psi(\ell^a) = 2^b(\ell^a + \ell^{a-1}),$$

where our sum is over closed-point equivalence classes $C(\varphi)$ of QM-cyclic ℓ^a isogenies φ with corresponding CM discriminant Δ.

The map $X_0^D(\ell^a)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ is ramified over Δ if and only if $\Delta \in \{-3, -4\}$. For example, for $\Delta = -4$ and $\ell^a = 2$, we have 2^{b+1} such classes, both having residual degree 1. Half of these classes, corresponding to self-loop edges at the surface, have no ramification, while each of the 2^b classes $C(\varphi)$ corresponding to a pair of descending edges to level 1 has $e_\varphi = 2$. More generally, for $\Delta \in \{-3, -4\}$ and path length a, we have that a closed point equivalence class has ramification, of index 2 or 3 in the respective cases of $\Delta = -4$ and -3, if and only if the paths in the class include a descending edge from level 0 to level 1. This allows for a check on the classifications and counts that we provide.

If $D(K) = 1$, then the path types showing up in our analysis of each $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ are exactly those appearing in [Cl23] and [CS23]. In this case, each graph $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ consists of 2^b copies of the analogous graph $\mathcal{G}_{K,\ell,\mathfrak{f}_0}$ from the $D = 1$ elliptic modular case. Moreover, we have shown that the action of relevant involutions on each component is identical to the action of complex conjugation in the $D = 1$ case, up to symmetry of our graphs. In each place where the isomorphism class of a residue field in the referenced $D = 1$ analysis is a rational ring class field, we have in its place here some totally complex, index 2 subfield of a ring class field as described in Theorem 2.3.6.

If at least one prime dividing D is inert in K, i.e., if $D(K) > 1$, then all of the residue fields of Δ-CM points on $X^D(1)_{/\mathbb{Q}}$, and hence on $X_0^D(\ell^a)_{/\mathbb{Q}}$, are ring class fields. The path types showing up are exactly those in [CS23], but the counts will in general differ from the case of the previous paragraph. Specifically, a given path type in our analysis in the case of $D(K) = 1$ consists of m classes with corresponding residue field $K(\mathfrak{f}')$ and n classes with corresponding residue field an index 2 subfield of $K(\mathfrak{f}')$ for some $\mathfrak{f}' \in \mathbb{Z}^+$ and $m, n \geq 0$.

In the case of $D(K) > 1$, the same path type then consists of $2m + n$ classes, each with corresponding residue field $K(\mathfrak{f}')$.

A non-backtracking length a path in $\mathcal{G}_{K,\ell,1}$ starting in level L consists of c ascending edges, followed by h horizontal edges, followed by d descending edges for some $c, h, d \geq 0$ with $c + h + d = a$. We denote this decomposition type of the path with the ordered triple (c, h, d).

5.1.1 Path type analysis: general case

We begin here by considering the portion of the path type analysis that is independent of ℓ and Δ_K.

I. There are classes consisting of strictly descending paths, i.e., with $(c, h, d) = (0, 0, a)$. If $D(K) \neq 1$, then there are 2^b such classes, each with residue field $K(\ell^a\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\ell^a\mathfrak{f})$.

II. If $a \leq L$, there are classes of strictly ascending paths, i.e., with $(c, h, d) = (a, 0, 0)$. If $D(K) \neq 1$, then there are 2^b such classes, each with corresponding residue field $K(\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\mathfrak{f})$.

III. If $L = 0$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$, then there classes of paths with $(c, h, d) = (0, 1, a - 1)$. If $D(K) \neq 1$, then there are 2^b such classes, each with corresponding residue field $K(\ell^{a-1}\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\ell^{a-1}\mathfrak{f})$.

IV. If $L = 0$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, then for each h with $1 \leq h \leq a$ there are classes of paths with $(c, h, d) = (0, h, a - h)$ and residue field $K(\ell^{a-h}\mathfrak{f})$. There are 2^{b+1} such classes if $D(K) \neq 1$, and there are 2^b such classes otherwise.

X. If $a > L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, then there are classes of paths with $(c, h, d) = (L, a - L, 0)$ and residue field $K(\mathfrak{f})$. There are 2^{b+1} such classes if $D(K) \neq 1$, and there are 2^b such classes otherwise.

5.1.2 Path type analysis: $\ell > 2$

Here we assume that ℓ is an odd prime.

V. If $L \geq 2$, then for each c with $1 \leq c \leq \min\{a-1, L-1\}$ there are paths which ascend at least one edge but not all the way to the surface, and then immediately descend at least one edge, with $(c, h, d) = (c, 0, a-c)$. Each such class has corresponding residue field $K(\ell^{\max\{a-2c,0\}}\mathfrak{f})$. There are $2^b(\ell-1)\ell^{\min\{c,a-c\}-1}$ such paths if $D(K) \neq 1$, and $2^{b-1}(\ell-1)\ell^{\min\{c,a-c\}-1}$ such paths otherwise.

VI. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = -1$, then there are paths which ascend to the surface and then immediately descend at least one edge, with $(c, h, d) = (L, 0, a-L)$. If $D(K) \neq 1$, then there are $2^b\ell^{\min\{L,a-L\}}$ classes of such paths with corresponding residue field $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$. Otherwise, there are $2^{b-1}\left(\ell^{\min\{L,a-L\}}-1\right)$ classes of such paths with corresponding residue field $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$, and 2^b classes of such paths with corresponding residue field an index 2 subfield of $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$.

VII. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$, then there are paths which ascend to the surface and then immediately descend at least one edge, with $(c, h, d) = (L, 0, a-L)$. Each such path has corresponding residue field $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^b(\ell-1)\ell^{\min\{L,a-L\}-1}$ classes of such paths. Otherwise, there are $2^{b-1}(\ell-1)\ell^{\min\{L,a-L\}-1}$ classes.

VIII. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$, then there are paths which ascend to the surface, follow one surface edge, and then possibly descend, with $(c, h, d) = (L, 1, a-L-1)$. If $D(K) \neq 1$, then there are $2^b\ell^{\min\{L,a-L-1\}}$ classes of such paths with corresponding residue field $K(\ell^{\max\{a-2L-1,0\}}\mathfrak{f})$. Otherwise, there are $2^{b-1}\left(\ell^{\min\{L,a-L-1\}}-1\right)$ classes of such paths with corresponding residue field $K(\ell^{\max\{a-2L-1,0\}}\mathfrak{f})$, and 2^b classes of such paths with corresponding residue field an index 2 subfield of $K(\ell^{\max\{a-2L-1,0\}}\mathfrak{f})$.

IX. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, then there are paths which ascend to the surface and then immediately descend at least one edge, with $(c, h, d) = (L, 0, a-L)$. If $D(K) \neq 1$, then there are $2^b(\ell-2)\ell^{\min\{L,a-L\}-1}$ classes of such paths with corresponding residue field $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$. Otherwise, there are $2^{b-1}\left((\ell-2)\ell^{\min\{L,a-L\}-1}-1\right)$ classes of such

paths with corresponding residue field $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$, and 2^b classes of such paths with corresponding residue field an index 2 subfield of $K(\ell^{\max\{a-2L,0\}}\mathfrak{f})$.

XI. If $a \geq L+2 \geq 3$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$, then for each $1 \leq h \leq a-L-1$ there are paths which ascend to the surface, traverse h edges on the surface, and then descend at least one edge, with $(c,h,d) = (L,h,a-L-h)$. Each such path has corresponding residue field $K(\ell^{\max\{a-2L-h,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^{b+1}(\ell-1)\ell^{\min\{L,a-L-h\}-1}$ classes of such paths. Otherwise, there are $2^b(\ell-1)\ell^{\min\{L,a-L-h\}-1}$ classes.

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

Here we assume that $\ell = 2$ with Δ_K odd.

V. If $L \geq 2$, we have classes consisting of paths which ascend at least one edge but not all the way to the surface, and then immediately descend at least one edge. We have the following types:

V$_1$. If $a \geq 2$, then there are classes with $(c,h,d) = (1,0,a-1)$. If $D(K) \neq 1$, then there are 2^b such classes, each with corresponding residue field $K(2^{a-2}\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(2^{a-2}\mathfrak{f})$.

V$_2$. If $L \geq a \geq 3$, then there are classes with $(c,h,d) = (a-1,0,1)$. If $D(K) \neq 1$, then there are 2^b such classes, each with corresponding residue field $K(2^{a-2}\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(2^{a-2}\mathfrak{f})$.

V$_3$. If $a \geq L+1 \geq 4$, then there are paths with $(c,h,d) = (L-1,0,a-L+1)$. If $D(K) \neq 1$, there are $2^{\min\{a-L+1,L-1\}+b-1}$ classes of such paths with corresponding residue field $K(2^{\max\{a-2L+2,0\}}\mathfrak{f})$. Otherwise, there are $2^b\left(2^{\min\{a-L+1,L-1\}-2}-1\right)$ classes of such paths with corresponding residue field $K(2^{\max\{a-2L+2,0\}}\mathfrak{f})$, and 2^{b+1} classes of such paths with corresponding residue field an index 2 subfield of $K(2^{\max\{a-2L+2,0\}}\mathfrak{f})$.

V$_4$. For each c with $2 \leq c \leq \min\{L-2, a-2\}$, there are paths with $(c,h,d) = (c,0,a-c)$. Each such path has corresponding residue field $K(2^{\max\{a-2c,0\}}\mathfrak{f})$. There are $2^{\min\{c,a-c\}+b-1}$

equivalence classes of such paths if $D(K) \neq 1$. Otherwise, there are $2^{\min\{c,a-c\}+b-2}$ such classes.

VI. If $a \geq L+1 \geq 2$ and $\left(\frac{\Delta_K}{2}\right) = -1$, there are paths that ascend to the surface and then immediately descend at least one edge, with $(c,h,d) = (L,0,a-L)$. Each such class has corresponding residue field $K(2^{\max\{a-2L,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^{\min\{L,a-L\}+b}$ classes of such paths. Otherwise, there are $2^{\min\{L,a-L\}-1+b}$ such classes.

XI. If $a \geq L+2$ and $\left(\frac{\Delta_K}{2}\right) = 1$, then for all $1 \leq h \leq a-L-1$ there are paths which ascend to the surface, traverse h horizontal edges, and then descend at least once, with $(c,h,d) = (L,h,a-L-h)$. Each such class has corresponding residue field $K(2^{\max\{a-2L-h,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^{\min\{L,a-L-h\}+b}$ classes of such paths. Otherwise, there are $2^{\min\{L,a-L-h\}+b-1}$ such classes.

5.1.4 Path type analysis: $\ell = 2, \mathrm{ord}_2(\Delta_K) = 2$

Here we assume that $\ell = 2$ with $\mathrm{ord}_2(\Delta_K) = 2$.

V. If $L \geq 2$, we have classes consisting of paths which ascend at least one edge but not all the way to the surface, and then immediately descend at least one edge. We have the following types:

V_1. If $a \geq 2$, then there are classes with $(c,h,d) = (1,0,a-1)$. If $D(K) \neq 1$, then there are 2^b such classes, each with corresponding residue field $K(2^{a-2}\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(2^{a-2}\mathfrak{f})$.

V_2. If $L \geq a \geq 3$, then there are classes with $(c,h,d) = (a-1,0,1)$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(\mathfrak{f})$. Otherwise, there are 2^b classes of such paths, each with corresponding residue field an index 2 subfield of $K(\mathfrak{f})$.

V_3. For each c with $2 \leq c \leq \min\{L-1, a-2\}$, there are paths $(c,h,d) = (c,0,a-c)$. Each such class has corresponding residue field $K(2^{\max\{a-2c,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^{\min\{c,a-c\}+b-1}$ classes of such paths. Otherwise, there are $2^{\min\{c,a-c\}+b-2}$ such classes.

VI. If $L \geq 1$, then we have paths which ascend to the surface and then immediately descend at least one edge, with $(c, h, d) = (L, 0, a - L)$. We have the following cases:

VI$_1$. Suppose $L = 1$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(2^{a-2}\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(2^{a-2}\mathfrak{f})$.

VI$_2$. Suppose $a = L + 1 \geq 3$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\mathfrak{f})$.

VI$_3$. Suppose $a \geq L + 2 \geq 4$. If $D(K) \neq 1$, then there are $2^{\min\{L,a-L\}+b-1}$ classes of such paths, each with corresponding residue field $K(2^{\max\{a-2L,0\}}\mathfrak{f})$. Otherwise, there are $2^b\left(2^{\min\{L,a-L\}-2} - 1\right)$ classes of such paths with corresponding residue field $K(2^{\max\{a-2L,0\}}\mathfrak{f})$, and 2^{b+1} classes of such paths with corresponding residue field an index 2 subfield of $K(2^{\max\{a-2L,0\}}\mathfrak{f})$.

VIII. If $a \geq L+1 \geq 2$, then we have paths which ascend to the surface, and then traverse the unique surface edge, and then possibly descend, with $(c, h, d) = (L, 1, a - L - 1)$. We have the following cases:

VIII$_1$. Suppose $a = L + 1$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\mathfrak{f})$.

VIII$_2$. Suppose $a \geq L + 2$. Each such path has corresponding residue field $K(2^{\max\{a-2L-1,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^{\min\{L,a-1-L\}+b}$ classes of such paths. Otherwise, there are $2^{\min\{L,a-1-L\}+b-1}$ such classes.

5.1.5 Path type analysis: $\ell = 2, \mathrm{ord}_2(\Delta_K) = 3$

Here we assume that $\ell = 2$ with $\mathrm{ord}_2(\Delta_K) = 3$. The types of paths occurring here are the same as in the previous section, owing to the fact that the structure of $\mathcal{G}^D_{K,\ell,\mathfrak{f}_0}$ here is the

same as therein. The corresponding residue field counts may differ, though, as the Galois action differs.

V. The analysis of this type is exactly as in §5.1.4.

VI. If $L \geq 1$, then we have paths which ascend to the surface and then immediately descend at least one edge, with $(c, h, d) = (L, 0, a - L)$. We have the following cases:

VI$_1$. Suppose $L = 1$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(2^{a-2}\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(2^{a-2}\mathfrak{f})$.

VI$_2$. Suppose $a = L + 1 \geq 3$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\mathfrak{f})$.

VI$_3$. If $a \geq L+2 \geq 4$, then each such class has corresponding residue field $K(2^{\max\{a-2L,0\}}\mathfrak{f})$. If $D(K) \neq 1$, then there are $2^{\min\{L,a-L\}+b-1}$ such classes. Otherwise, there are $2^{\min\{L,a-L\}+b-2}$ such classes.

VIII. If $a \geq L+1 \geq 2$, then we have paths which ascend to the surface, and then traverse the unique surface edge, and then possibly descend, with $(c, h, d) = (L, 1, a - L - 1)$. We have the following cases:

VIII$_1$. Suppose $a = L + 1$. If $D(K) \neq 1$, then there are 2^b classes of such paths, each with corresponding residue field $K(\mathfrak{f})$. Otherwise, there are 2^b such classes, each with corresponding residue field an index 2 subfield of $K(\mathfrak{f})$.

VIII$_2$. Suppose that $a \geq L + 2$. If $D(K) \neq -1$, then there are $2^{\min\{L,a-1-L\}+b}$ classes of such paths, each with corresponding residue field $K(2^{\max\{a-2L-1,0\}}\mathfrak{f})$. Otherwise, there are $2^b\left(2^{\min\{L,a-1-L\}-1} - 1\right)$ classes of such paths with corresponding residue field $K(2^{\max\{a-2L-1,0\}}\mathfrak{f})$, and 2^{b+1} classes with corresponding residue field an index 2 subfield of $K(2^{\max\{a-2L-1,0\}}\mathfrak{f})$.

5.1.6 Primitive residue fields of CM points on $X_0^D(\ell^a)_{/\mathbb{Q}}$

Fixing Δ an imaginary quadratic discriminant and $N \in \mathbb{Z}^+$ relatively prime to D, we say that a field F is a **primitive residue field for Δ-CM points on** $X_0^D(N)_{/\mathbb{Q}}$ if

- there is a Δ-CM point $x \in X_0^D(N)_{/\mathbb{Q}}$ with $\mathbb{Q}(x) \cong F$, and
- there does not exists a Δ-CM point $y \in X_0^D(N)_{/\mathbb{Q}}$ with $\mathbb{Q}(y) \cong L$ with $L \subsetneq F$.

The preceding path type analysis in this section allows us to determine primitive residue fields for prime powers $N = \ell^a$. It follows from this analysis that, In all cases, there are at most 2 primitive residue fields, and that each primitive residue field is either a ring classes field or an index 2 subfield of a ring class field.

The cases occurring here are in line with those in [Cl23] and [CS23], though here the primitive residue fields depend on whether $D(K) = 1$. In particular, if some prime dividing D is inert in K, then all residue fields of CM points on $X_0^D(\ell^a)_{/\mathbb{Q}}$ are ring class fields and hence there can only be one primitive residue field.

Case 1.1. Suppose $\ell^a = 2$.

Case 1.1a. Suppose $\left(\frac{\Delta}{2}\right) \neq -1$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.1b. Suppose $\left(\frac{\Delta}{2}\right) = -1$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(2\mathfrak{f})$. Otherwise, the only primitive residue field is $K(2\mathfrak{f})$.

Case 1.2. Suppose $\ell^a > 2, L = 0$ and $\left(\frac{\Delta}{\ell}\right) = 1$. If $D(K) = 1$, then the primitive residue fields are $K(\mathfrak{f})$ and an index 2 subfield of $K(\ell^a\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.3. Suppose $\ell^a > 2, L = 0$ and $\left(\frac{\Delta}{\ell}\right) = -1$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\ell^a\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\ell^a\mathfrak{f})$.

Case 1.4. Suppose $\ell^a > 2, L = 0$ and $\left(\frac{\Delta}{\ell}\right) = 0$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\ell^{a-1}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\ell^{a-1}\mathfrak{f})$.

Case 1.5. Suppose $\ell > 2, L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = 1$.

Case 1.5a. Suppose $a \leq 2L$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.5b. Suppose $a \geq 2L + 1$. If $D(K) = 1$, then the primitive residue fields are $K(\mathfrak{f})$ and an index 2 subfield of $K(\ell^{a-2L}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.6. Suppose $\ell > 2, L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = -1$.

Case 1.6a. Suppose $a \leq 2L$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.6b. Suppose $a \geq 2L + 1$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\ell^{a-2L}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\ell^{a-2L}\mathfrak{f})$.

Case 1.7. Suppose $\ell > 2, L \geq 1$ and $\left(\frac{\Delta_K}{\ell}\right) = 0$.

Case 1.7a. Suppose $a \leq 2L + 1$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.7b. Suppose $a \geq 2L + 2$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\ell^{a-2L-1}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\ell^{a-2L-1}\mathfrak{f})$.

Case 1.8. Suppose $\ell = 2, a \geq 2, L \geq 1$ and $\left(\frac{\Delta_K}{2}\right) = 1$.

Case 1.8a. Suppose $L = 1$. If $D(K) = 1$, then the primitive residue fields are $K(\mathfrak{f})$ and an index 2 subfield of $K(2^a f)$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.8b. Suppose $L \geq 2$ and $a \leq 2L-2$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.8c. Suppose $L \geq 2$ and $a \geq 2L-1$. If $D(K) = 1$, then the primitive residue fields are $K(\mathfrak{f})$ and an index 2 subfield of $K(2^{a-2L+2}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.9 Suppose $\ell = 2, a \geq 2, L \geq 1$ and $\left(\frac{\Delta_K}{2}\right) = -1$.

Case 1.9a. Suppose $L = 1$. If $D(K) = 1$, then the primitive residue fields are $K(2^{a-2}\mathfrak{f})$ and an index 2 subfield of $K(2^{a}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(2^{a-2}\mathfrak{f})$.

Case 1.9b. Suppose $L \geq 2$ and $a \leq 2L-2$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.9c. Suppose $L \geq 2$ and $a \geq 2L-1$. If $D(K) \neq 1$, then the primitive residue fields are $K(2^{\max\{a-2L,0\}}\mathfrak{f})$ and an index 2 subfield of $K(2^{a-2L+2}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(2^{\max\{a-2L,0\}}\mathfrak{f})$.

Case 1.10 Suppose $\ell = 2, a \geq 2, L \geq 1, \left(\frac{\Delta_K}{2}\right) = 0$ and $\mathrm{ord}_2(\Delta_K) = 2$.

Case 1.10a. Suppose $a \leq 2L$. If $D(K) \neq 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.10b. Suppose $a \geq 2L+1$. If $D(K) \neq 1$, then the primitive residue fields are $K(2^{a-2L-1}\mathfrak{f})$ and an index 2 subfield of $K(2^{a-2L}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(2^{a-2L-1}\mathfrak{f})$.

Case 1.11 Suppose $\ell = 2, a \geq 2, L \geq 1, \left(\frac{\Delta_K}{2}\right) = 0$ and $\mathrm{ord}_2(\Delta_K) = 3$.

Case 1.11a. Suppose $a \leq 2L+1$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(\mathfrak{f})$. Otherwise, the only primitive residue field is $K(\mathfrak{f})$.

Case 1.11b. Suppose $a \geq 2L+2$. If $D(K) = 1$, then the only primitive residue field is an index 2 subfield of $K(2^{a-2L-1}\mathfrak{f})$. Otherwise, the only primitive residue field is $K(2^{a-2L-1}\mathfrak{f})$.

5.1.7 Primitive degrees of CM points on $X_0^D(\ell^a)_{/\mathbb{Q}}$.

We say that a positive integer d is a **primitive degree for Δ-CM points on** $X_0^D(N)_{/\mathbb{Q}}$ if

- there is a a Δ-CM point of degree d on $X_0^D(N)_{/\mathbb{Q}}$, and
- there does not exist a Δ-CM point on $X_0^D(N)_{/\mathbb{Q}}$ of degree properly dividing d.

If d is such a degree, then the residue field of a degree d point on $X_0^D(N)_{/\mathbb{Q}}$ is a primitive residue field of Δ-CM points on $X_0^D(N)_{/\mathbb{Q}}$. For $N = \ell^a$ a prime power, we then have from the previous section that there are at most two primitive degrees.

While there are several cases that admit two primitive residue fields when $D(K) = 1$, the only case admitting two primitive degrees is Case 1.5b. In Case 1.5b, our two primitive residue fields are $K(\mathfrak{f})$ and an index 2 subfield L of $K(\ell^{a-2L}\mathfrak{f})$, with respective degrees $[K(\mathfrak{f}) : \mathbb{Q}] = 2h(\mathfrak{o}(\mathfrak{f}))$ and $[L : \mathbb{Q}] = \ell^{a-2L}h(\mathfrak{o}(\mathfrak{f}))$. As ℓ is odd, we indeed have two primitive degrees in this case.

5.2 Algebraic results on residue fields of CM points on $X^D(1)_{/\mathbb{Q}}$

We develop here algebraic number theoretic results on fields which arise as residue fields of CM points on $X^D(1)_{/\mathbb{Q}}$ which will feed into our main results. In particular, a determination of composita and tensor products of such fields will be needed in determining information about the CM locus on $X_0^D(N)_{/\mathbb{Q}}$ for general N from information at prime-power levels.

For an imaginary quadratic field K, we let $K(\mathfrak{f})$ denote the ring class field corresponding to the imaginary quadratic order $\mathfrak{o}(\mathfrak{f})$ of conductor $\mathfrak{f}$ in K, i.e., that of discriminant $\mathfrak{f}^2\Delta_K$.

Proposition 5.2.1. *Let K denote an imaginary quadratic field of discriminant Δ_K.*

1. *If* $\Delta_K \notin \{-3, -4\}$*, then for any* $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$ *we have*

$$K(\mathfrak{f}_1) \cdot K(\mathfrak{f}_2) = K(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)).$$

2. *Suppose* $\Delta_K \in \{-3, -4\}$.

   (a) *For any* $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathbb{Z}^+$ *with* $gcd(\mathfrak{f}_1, \mathfrak{f}_2) > 1$*, we have*

   $$K(\mathfrak{f}_1) \cdot K(\mathfrak{f}_2) = K(\mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)).$$

   (b) *If the class number of the order of discriminant* $\mathfrak{f}_1^2\Delta_K$ *is* 1*, i.e., if* $\mathfrak{f}_1^2\Delta_K \in S = \{-3, -4, -12, -16, -27\}$*, then*

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

   (c) *Suppose we have positive integers* $\mathfrak{f}_1, \ldots, f_r$ *which are all pairwise relatively prime and not in the* S *defined above. Then* $K(\mathfrak{f}_1) \cdots K(f_r) \subsetneq K(\mathfrak{f}_1 \cdots f_r)$*, with*

   $$[K(\mathfrak{f}_1 \cdots f_r) : K(\mathfrak{f}_1) \cdots K(f_r)] = \begin{cases} 2^{r-1} \text{ if } \Delta_K = -4 \\ 3^{r-1} \text{ if } \Delta_K = -3 \end{cases}.$$

3. *In all cases,* $K(\mathfrak{f}_1)$ *and* $K(\mathfrak{f}_2)$ *are linearly disjoint over* $K(\gcd(\mathfrak{f}_1, \mathfrak{f}_2))$.

Proof. Part (1) is [Cl23, Prop. 2.10]. We repeat the proof of part (2) here from [CS23, Prop. 2.1]:

We will use the classical description of ring class groups and ring class fields, with notation as in §2.2.1. Let $m = \gcd(\mathfrak{f}_1, \mathfrak{f}_2)$ and $M = \mathrm{lcm}(\mathfrak{f}_1, \mathfrak{f}_2)$. By class field theory, we have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(M)$ if and only if

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

Clearly in all cases we have

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

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

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

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

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

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

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

If this holds then

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

which is manifestly false.

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

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

which is again manifestly false.

2. (b) This is a trivial case, listed for completeness: if the order of discriminant $\mathfrak{f}_1^2\Delta_K$ has class number 1 then $K(\mathfrak{f}_1) = K(1)$ (and conversely), so $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(1)K(\mathfrak{f}_2) = K(\mathfrak{f}_2)$.[1]

2. (c) We claim that the extensions $K(\mathfrak{f}_1), \ldots, K(\mathfrak{f}_r)$ are mutually linearly disjoint over $K(1)$: that is,

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

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

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

and the latter expression can be evaluated using Proposition 2.2.2.

We now handle part (3). It is immediate that $K(m) \subseteq K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$. The case $m = 1$ is relatively simple: here $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$ has conductor dividing $\mathfrak{f}_1$ and $\mathfrak{f}_2$, so its conductor is the unit ideal, so $K(\mathfrak{f}_1) \cap K(\mathfrak{f}_2)$ is contained in the Hilbert class field of K, which is the ring class field $K(1)$.

We therefore suppose that $m > 1$, and thus by part 2.(a) we have $K(\mathfrak{f}_1)K(\mathfrak{f}_2) = K(M)$. We claim the formula

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

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

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

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

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

We now use Proposition 5.2.1 to get analogues of [Cl23, Prop. 2.10] and [CS23, Prop 2.2], in which "rational ring class fields" are generalized to those index 2 subfields of rings class fields which arise as residue fields of CM points on $X^D(1)_{/\mathbb{Q}}$.

Corollary 5.2.2. *Suppose that $x_1 \in X_0^D(N_1)_{/\mathbb{Q}}$ and $x_2 \in X_0^D(N_2)_{/\mathbb{Q}}$ are $\mathfrak{o}(\mathfrak{f})$-CM points, where $\mathfrak{o}(\mathfrak{f})$ is an imaginary quadratic order in K. For $i = 1, 2$, let $\mathfrak{f}_i \in \mathbb{Z}^+$ such that*

$$K \cdot \mathbb{Q}(x_i) \cong K(\mathfrak{f}_i).$$

Let $M = \gcd(N_1, N_2)$ and $m = \operatorname{lcm}(N_1, N_2)$, and suppose that $x \in X_0^D(M)_{/\mathbb{Q}}$ is a point lying above x_1 and x_2 which is fixed by an involution $\sigma \in \operatorname{Gal}(K(M)/K)$. Let $\pi : X_0^D(M)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ denote the natural map. Then

1. *The fields $\mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$ are linearly disjoint over $\mathbb{Q}(\pi(x))$.*
2. *We have*
$$\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} \mathbb{Q}(x_2) \cong \mathbb{Q}(x).$$
3. *We have*
$$\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2) \cong K(x).$$

Proof. The ring class fields $K(\mathfrak{f}_1)$ and $K(\mathfrak{f}_2)$ are linearly disjoint over $K(m)$ by Proposition 5.2.1. That $\mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$ are linearly disjoint over $\mathbb{Q}(\pi(x))$, and that

$$[\mathbb{Q}(x) : \mathbb{Q}(x_1) \cdot \mathbb{Q}(x_2)] = [K(x) : K(x_1) \cdot K(x_2] = [K(m) : K(\mathfrak{f}_1) \cdot K(\mathfrak{f}_2)],$$

follow by the same type of arguments as in the specific case of rational ring class fields in [Cl23, Prop. 2.10] and [CS23, Prop 2.2], using that $K(x) \cong K(x_1) \cdot K(x_2) \cong K(\mathfrak{f}_1) \cdot K(\mathfrak{f}_2)$ via Proposition 4.1.3 (note that the assumption that x is fixed by σ forces $\mathfrak{f}^2 \Delta_K < -4$ unless $D = 1$, so this proposition applies to handle the $D > 1$ case).

Part (2) now follows from the preceding remarks, combined with Proposition 5.2.1. As for part (3), first note that the fact that $\mathbb{Q}(x)$ is fixed by some involution $\sigma \in \mathrm{Gal}(K(M)/K)$ immediately implies that $h(\mathfrak{o}(\mathfrak{f})) > 1$ (as $X^D(1)_{/\mathbb{Q}}$ has no real points). We note that the map

$$\begin{aligned} \mathbb{Q}(x_1) \times K(x_2) &\longrightarrow K(x_1) \cdot K(x_2) \\ (x_1, x_2) &\longmapsto x_1 \cdot x_2 \end{aligned}$$

is $\mathbb{Q}(\pi(x))$-bilinear, and the induced map on the tensor product over $\mathbb{Q}(\pi(x))$ must be an isomorphism

$$\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2) \cong K(x_1) \cdot K(x_2)$$

as the two finite $\mathbb{Q}(\mathfrak{f})$-algebras here have the same dimension. The result then follows as $K(x_1) \cdot K(x_2) \cong K(x)$. □

Corollary 5.2.3. *Suppose that $x_1, x_2, \ldots, x_r$ are $\mathfrak{o}(\mathfrak{f})$-CM points with $x_i \in X_0^D(N_i)_{/\mathbb{Q}}$ for each $i = 1, \ldots, r$, where $\mathfrak{o}(\mathfrak{f})$ is an imaginary quadratic order in K. For each $i = 1, \ldots, r$, let $\mathfrak{f}_i \in \mathbb{Z}^+$ such that*

$$K \cdot \mathbb{Q}(x_i) \cong K(\mathfrak{f}_i).$$

Let $M = \gcd(N_1, \ldots, N_r)$ and $m = \mathrm{lcm}(N_1, \ldots, N_r)$. Let $\pi : X_0^D(M)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ denote the natural map. Let $S = \{-3, -4, -12, -16, -27\}$ be the set of discriminants of imaginary quadratic orders of class number 1 with $\Delta_K \in \{-3, -4\}$.

1. *Suppose that $r = 2$. If $\mathfrak{f}_1 \in S$, then we have*

$$K(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2) \cong K(x_2) \times K(x_2).$$

Now assuming $\mathfrak{f}_1, \mathfrak{f}_2 \notin S$, if $\Delta_K < -4$ or if $gcd(\mathfrak{f}_1, \mathfrak{f}_2) > 1$ then

$$K(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2) \cong K(M) \times K(M).$$

2. *Suppose that* $\Delta_K \in \{-3,-4\}$*, that* $\mathfrak{f}_1,\ldots,f_r \notin S$*, and that* $\mathfrak{f}_1,\ldots,f_r$ *are all pairwise relatively prime. We then have*

$$\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} \ldots \otimes_{\mathbb{Q}(\pi(x))} \mathbb{Q}(x_r) \cong K(x_1) \otimes_{\mathbb{Q}(\pi(x))} \ldots \otimes_{\mathbb{Q}(\pi(x))} K(x_r) \cong L^r,$$

with L *a subfield of* $K(M)$ *of index* 2^{r-1} *if* $\Delta_K = -4$ *and index* 3^{r-1} *if* $\Delta_K = -3$.

Proof. 1. Using part (3) of Corollary 5.2.2, we have

$$\begin{aligned} K(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2) &\cong \big(\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x)\big) \otimes_{\mathbb{Q}(\pi(x))} \big(\mathbb{Q}(x_2) \otimes_{\mathbb{Q}(\pi(x))} K(x)\big) \\ &\cong \big(\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} \mathbb{Q}(x_2)\big) \otimes_{\mathbb{Q}(\pi(x))} \big(K(x) \otimes_{\mathbb{Q}(\pi(x))} K(x)\big) \\ &\cong \big(\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} \mathbb{Q}(x_2)\big) \otimes_{\mathbb{Q}(\pi(x))} (K(x) \times K(x)) \\ &\cong \big(\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2)\big) \times \big(\mathbb{Q}(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2)\big). \end{aligned}$$

The stated result then follows from another use of Corollary 5.2.2 part (3) if $\mathbb{Q}(x_1)$ properly embeds in the ring class field $K(\mathfrak{f}_1)$. Otherwise, $\mathbb{Q}(x_i) \cong K(\mathfrak{f}_i)$ for $i = 1,2$ and $\mathbb{Q}(\pi(x)) \cong K(\mathfrak{f})$. The case of $\mathfrak{f}_1 \in S$ is then clear, so assume $\mathfrak{f}_1, \mathfrak{f}_2 \notin S$ and at least one of $\Delta_K < -4$ or $\gcd(\mathfrak{f}_1,\mathfrak{f}_2) > 1$ holds. It then follows from Proposition 5.2.1 that

$$\begin{aligned} K(x_1) \otimes_{\mathbb{Q}(\pi(x))} K(x_2) &\cong \big(K(\mathfrak{f}_1) \otimes_{K(\mathfrak{f})} K(\mathfrak{f}_2)\big) \times \big(K(x_1) \otimes_{K(\mathfrak{f})} K(\mathfrak{f}_2)\big) \\ &\cong K(M) \times K(M). \end{aligned}$$

2. This result follows similarly to the above argument using Proposition 5.2.1 once more. Note that our assumption that the $\mathfrak{f}_i$ are relatively prime forces $\mathbb{Q}(x_i)$ to be a ring class field for each i; this assumption gives $K \cdot \mathbb{Q}(\pi(x)) \cong K(1) = K$ as $\Delta_K \in \{-3,-4\}$, and our Shimura curves have no real points so indeed $\mathbb{Q}(\pi(x)) \cong K$.

□

5.3 CM points on $X_0^D(N)_{/\mathbb{Q}}$

In this section, we describe the Δ-CM locus on $X_0^D(N)_{/\mathbb{Q}}$ for any $N \in \mathbb{Z}^+$ relatively prime to D and any imaginary quadratic discriminant Δ. For $\Delta < -4$, this description is possible using the foundations we have built thus far, specifically Propositions 4.1.3 and 4.4.1, along with the path type analysis in §5.1. For $\Delta = \Delta_K \in \{-3, -4\}$, however, Proposition 4.1.3 does not apply.

We first elaborate on the description in former case, and then provide a result for compiling across prime powers in the case of $\Delta \in \{-3, -4\}$. Following this, we discuss primitive residue fields and degrees of Δ-CM points on $X_0^D(N)_{/\mathbb{Q}}$.

5.3.1 Compiling across prime powers: $\Delta < -4$

For a fixed prime ℓ relatively prime to D, let $\Delta = \ell^{2L}\mathfrak{f}_0^2\Delta_K$ with $\gcd(\mathfrak{f}_0, \ell) = 1$ be an imaginary quadratic discriminant. Fixing $a \in \mathbb{Z}^+$, let F be a fiber of the natural map $X_0^D(\ell^a)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ over a Δ-CM point $x \in X_0^D(1)_{/\mathbb{Q}}$ (recalling that there are 2^b such fibers, which are all isomorphic). We then have $F \cong \mathrm{Spec}A$ with

$$A = \prod_{j=0}^{a} {L_j}^{b_j} \times \prod_{k=0}^{a} K(\ell^k\mathfrak{f})^{c_k} \tag{5.1}$$

for some non-negative integers b_j, c_k, where L_j is an index 2 subfield of $K(\ell^j\mathfrak{f})$ for all $0 \leq j \leq a$. The explicit values b_j and c_k, based on ℓ^a and Δ, are determined by our path type analysis in §5.1.

Now assume $\Delta < -4$, let N denote a positive integer relatively prime to D, and let F be the fiber of $X_0^D(N)_{/\mathbb{Q}} \to X(1)_{/\mathbb{Q}}$ over a Δ-CM point $x \in X^D(1)_{/\mathbb{Q}}$. Let $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$ be the prime-power factorization of N, and for each $1 \leq i \leq r$ let F_i be the fiber of $X_0^D(\ell_i^{a_i})_{\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ over x. We then have

$$F_i \cong \mathrm{Spec}A_i$$

with each A_i of the form given in (5.1). Proposition 4.1.3 then provides that $F \cong \mathrm{Spec}A$ with

$$A = A_1 \otimes_{\mathbb{Q}(x)} \cdots \otimes_{\mathbb{Q}(x)} A_r.$$

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

$$M = M_1 \otimes_{\mathbb{Q}(x)} \cdots \otimes_{\mathbb{Q}(x)} M_r,$$

where for each $1 \leq i \leq r$ we have that M_i is isomorphic to $K(\ell_i^{j_i}\mathfrak{f})$, or a totally complex index 2 subfield thereof, for some $0 \leq j_i \leq a_i$.

Let s be the number of indices $1 \leq i \leq r$ such that K is contained in M_i, i.e., such that $M_i \cong K(\ell_i^{j_i})$ is a ring class field. The results of §5.2 then tell us that

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

where $L \subsetneq K(\ell_1^{j_1} \cdots \ell_r^{j_r})$ is a totally complex, index 2 subfield in the $s = 0$ case. (Note that $\ell_i^{\text{æ}_i}\Delta \in \{-12, -16, -27\}$ can only occur, due to the $\Delta < -4$ assumption, if $j_i = 0$, so these possibilities do not require special attention here.)

5.3.2 Compiling across prime powers: $\Delta \in \{-3, -4\}$

Here, we determine how to compile residue field information across prime-power level for $\Delta \in \{-3, -4\}$. We begin with a result in the $D = 1$ situation, wherein more work is required due to the fact that residue fields of -3 and -4-CM points on $X_0(N)_{/\mathbb{Q}}$ do not always contain the CM field K.

Proposition 5.3.1. *Suppose that $\varphi : E \to E'$ is a cyclic N-isogeny of K-CM elliptic curves, with N having prime-power factorization $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For each $i \in \{1, \ldots, r\}$, let $\varphi_i : E \to E_i$ be the ℓ_i-primary part of φ. Let b_i such that $\mathbb{Q}(\varphi_i)$ is isomorphic to either $K(\ell_i^{b_i})$ or to $\mathbb{Q}(\ell_i^{b_i})$. Then*

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

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

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

and let

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

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

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

It remains to show the containment $\mathbb{Q}(\varphi) \subseteq K(\ell_1^{b_1} \cdots \ell_r^{b_r})$. If $j(E) \notin \{0, 1728\}$, then this follows from [CS23, Thm. 4.1] and [Cl23, Prop. 3.5], so we suppose $j(E) \in \{0, 1728\}$. If $j(E') = j(E)$, then φ is (up to isomorphism on the target) an endomorphism of E, hence defined over K. If $j(E') \neq j(E)$ then $j(E') \notin \{0, 1728\}$, so our previous work applies via consideration of the dual isogeny as $\mathbb{Q}(\varphi) \cong \mathbb{Q}(\varphi^\vee)$. □

Proposition 5.3.1 provides bounds on the field of moduli of an isogeny. We now use this result to determine the exact field of moduli in the case where our source elliptic curve has -3-CM or -4-CM and $D = 1$, which we state from the perspective of determining the residue field of the corresponding CM point on $X_0(N)_{/\mathbb{Q}}$. We also handle the $D > 1$ case here:

Theorem 5.3.2. *Let $N \in \mathbb{Z}^+$ coprime to D with prime-power factorization $\ell_1^{a_1} \cdots \ell_r^{a_r}$, and suppose $x \in X_0^D(N)_{/\mathbb{Q}}$ is a Δ-CM point with $\Delta \in \{-3, -4\}$. Let $\pi_i : X_0^D(N)_{/\mathbb{Q}} \to X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$ denote the natural map, and let $x_i = \pi_i(x)$ for each $1 \leq i \leq r$. Let P_i be any path in the closed point equivalence class corresponding to x_i in $\mathcal{G}_{K,\ell_i,1}^D$, and let $d_i \geq 0$ be the number of descending edges in P_i (which is independent of the representative path).*

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

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

b) In every other case, we have

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

Proof. We first handle the case of $D > 1$. Because $\Delta \in \{-3, -4\}$, we know that the residue field of the image of x under the natural map to $X^D(1)_{/\mathbb{Q}}$ is necessarily K. Therefore, $K \subseteq \mathbb{Q}(x_i)$ for each i and hence $\mathbb{Q}(x_i) \cong K(\ell_i^{d_i})$ for each $1 \leq i \leq r$. We now argue similarly to as in the previous proposition:

Let $\varphi : (A, \iota) \to (A', \iota')$ be a QM-cyclic N-isogeny over $\mathbb{Q}(x)$ inducing x (necessarily there is such an isogeny, as $K \subseteq \mathbb{Q}(x)$). Let $Q = \ker(\varphi)$, let $C = e_1(Q)$, and for each $1 \leq i \leq r$ let $C_i \leq C$ be the Sylow ℓ_i subgroup of C. Let $\varphi_i : (A, \iota) \to (A/(\mathcal{O} \cdot C_i), \iota_i)$ be the ℓ_i-primary part of φ, and let $\mathfrak{f}_i$ denote the central conductor of $(A/(\mathcal{O} \cdot C_i), \iota)$ (where by ι here we really mean the induced QM structure on the quotient). Put

$$\mathcal{I} := \{i \mid d_i > 0\} = \{i \mid \mathrm{ord}_{\ell_i}(\mathfrak{f}_i) > 0\} \subseteq \{1, \ldots, r\}$$

and

$$Q' := \left\langle \{\mathcal{O} \cdot C_i\}_{i \in \mathcal{I}} \right\rangle \leq Q.$$

Our original isogeny φ then factors as $\varphi = \varphi'' \circ \varphi'$ where $\varphi' : (A, \iota) \to (A/Q', \iota)$. Because a QM-cyclic ℓ_i-isogeny preserves the prime-to-ℓ_i part of the central conductor, the central conductor of $(A/Q', \iota)$ must be divisible by $\ell_1^{d_1} \cdots \ell_r^{d_r}$. We then have

$$K(\ell_1^{d_1} \cdots \ell_r^{d_r}) \subseteq \mathbb{Q}(\varphi') \subseteq \mathbb{Q}(\varphi),$$

and it remains to show the reverse containment. If the central conductor of (A', ι') is also 1, then (up to isomorphism on the target) φ is a QM-equivariant endomorphism of (A, ι)

and therefore $\mathbb{Q}(\varphi) \subseteq K$ as desired. Otherwise, the dual isogeny $\varphi^\vee$ induces a Δ'-CM point $x' \in X_0^D(N)_{/\mathbb{Q}}$ with $\Delta' < -4$. We have $\mathbb{Q}(x) \cong \mathbb{Q}(x')$, and the claim then holds via an application of Proposition 4.1.3 to x'.

Now suppose that $D = 1$, and let $\varphi : E \to E'$ be a cyclic N-isogeny inducing the point x. For each $1 \leq i \leq r$, let $\varphi_i : E \to E_i$ be the ℓ_i-primary part of φ: that is, the kernel of φ_i is the ℓ_i-Sylow subgroup of the kernel of φ. We have two cases:

Case 1: Suppose that E' is also a Δ_K-CM elliptic curve. By [Cl23, §3.4], the isogeny φ is isomorphic over $\mathbb{C}$ to $E \to E/[I]$ for a nonzero ideal I of $\mathbb{Z}_K$, and we have $\mathbb{Q}(\varphi) \cong \mathbb{Q}(j(E)) = \mathbb{Q}$ if I is real ideal (i.e., $I = \overline{I}$) and $\mathbb{Q}(\varphi) = K(j(E)) = K$ is I is not a real ideal. If we factor $I = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r}$ into prime powers and $\mathfrak{p}_i$ lies over ℓ_i, then we have (up to an isomorphism on the target) that $\varphi_i : E \to E/[\mathfrak{p}_i^{c_i}]$. Notice that the path in $\mathcal{G}_{K,\ell_i,1}$ corresponding to φ_i lies entirely on the surface. If some ℓ_i splits in K, then $\mathfrak{p}_i^{c_i}$ is not a real ideal, so $\mathbb{Q}(\varphi) = K$. If no ℓ_i splits in K, then each $\mathfrak{p}_i^{c_i}$ is real, so I is real and $\mathbb{Q}(\varphi) = \mathbb{Q}$.

Case 2: Otherwise E' is a $\Delta = \mathfrak{f}^2\Delta_K$-CM elliptic curve for some $\mathfrak{f} > 1$. Since $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi^\vee)$, we may compute the field of moduli of the dual isogeny $\varphi^\vee : E' \to E$. Since $\operatorname{Aut} E' = \{\pm 1\}$, the rationality of a subgroup of E' is independent of the model, so we have $\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi_1) \cdots \mathbb{Q}(\varphi_r)$, and the result now follows from [Cl23, Thm. 5.1].

□

5.3.3 Primitive residue fields of CM points on $X_0^D(N)_{/\mathbb{Q}}$

The preceding results imply that the residue field of any Δ-CM point on $X_0^D(N)_{/\mathbb{Q}}$ is isomorphic to either a ring class field or an index 2 subfield of a ring class field arising as the residue field of a CM point on $X^D(1)_{/\mathbb{Q}}$ as described in Theorem 2.3.6. As a result, there are at most two primitive residue fields of Δ-CM points on $X_0^D(N)_{/\mathbb{Q}}$. Moreover, there exists a positive integer C such that an index 2 subfield of $K(Cf)$ is a primitive residue field of Δ-CM points on $X_0^D(N)_{/\mathbb{Q}}$ if and only if for each $1 \leq i \leq r$ there exists a positive integer C_i such that an index 2 subfield of $K(C_i\mathfrak{f})$ is a primitive residue field of Δ-CM points on $X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$.

We begin by investigating the cases in which we do have such a field as a primitive residue field, determining when we have two primitive residue fields and, if so, whether we have two primitive degrees of residue fields. Note that this assumption requires $D(K) = 1$, and hence $D = 1$ or $\Delta_K < -4$. Let $H_i = \ell_i^{h_i} \mid \ell_i^{a_i}$ be the unique positive integer such that an index 2 subfield L_i of $K(H_i\mathfrak{f})$ is a primitive residue field of Δ-CM points on $X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$ for each $1 \leq i \leq r$. Setting

$$H = H_1 \cdots H_r,$$

we have that a totally complex, index 2 subfield L of $K(H\mathfrak{f})$ is a primitive residue field of Δ-CM points on $X_0^D(N)_{/\mathbb{Q}}$ by the results of §5.3.1.

If L_i is the unique primitive residue field of Δ-CM points on $X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$ for each $1 \leq i \leq r$, then L is the unique primitive residue field for $X_0^D(N)_{/\mathbb{Q}}$. Otherwise, let $C_i = \ell_i^{c_i} \mid \ell_i^{a_i}$ be the smallest positive integer such that there is a Δ-CM point on $X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$ with residue field isomorphic to either $K(C_i\mathfrak{f})$ or an index 2 subfield thereof for each $1 \leq i \leq r$. Setting

$$C = C_1 \cdots C_r,$$

we then have that $K(Cf)$ is also a primitive residue field for $X_0^D(N)_{/\mathbb{Q}}$.

Now assume that we have two primitive residue fields, $L \subsetneq K(Hf)$ with $[K(Hf) : L] = 2$ and $K(C\mathfrak{f})$, of Δ-CM points on $X_0^D(N)_{/\mathbb{Q}}$. Set

$$d_1 := [L : \mathbb{Q}] \quad \text{and} \quad d_2 := [K(Cf) : \mathbb{Q}].$$

We note $C_i \leq H_i$ for each $1 \leq i \leq r$ by the definitions of these quantities. Further, by assumption we have at least one value of i such that $K(C_i\mathfrak{f})$ is a primitive residue field for $X_0^D(\ell_i^{a_i})_{/\mathbb{Q}}$, and thus

$$[K(C_i\mathfrak{f}) : \mathbb{Q}] \leq \frac{[K(H_i) : \mathbb{Q}]}{2} = [L_i : \mathbb{Q}].$$

It follows that $d_2 \leq d_1$. Therefore, we have a unique primitive degree of Δ-CM points on $X_0^D(N)$ if and only if $d_2 \mid d_1$, in which case d_2 is the unique primitive degree. The following result determines when this occurs:

Theorem 5.3.3. *Let $\Delta = \mathfrak{f}^2\Delta_K$ be an imaginary quadratic discriminant and let N be a positive integer relatively prime to D with prime power factorization $N = \ell_1^{a_1} \cdots \ell_r^{a_r}$. For each $1 \leq i \leq r$ let B_i, C_i and L_i be as above, and also let B, C, d_1, d_2 and L be as above. Let s be the number of indices $1 \leq i \leq r$ such that $K(B_i\mathfrak{f})$ is a primitive residue field of Δ-CM points on $X_0^D(\ell_i^{a_i})$ (or equivalently, such that $C_i < B_i$).*

1. *If $s = 0$, then L is the unique primitive residue field of Δ-CM points on $X_0^D(N)$, and d_1 is the unique primitive degree.*

2. *Suppose that $s \geq 1$ and that for some $1 \leq i \leq r$ with $C_i < B_i$ we are not in Case 1.5b with respect to Δ and the prime power $\ell_i^{a_i}$. We then have that L and $K(Cf)$ are the two primitive residue fields of Δ-CM points on $X_0^D(N)$, while d_2 is the unique primitive degree.*

3. *Suppose that $s \geq 1$ and that for all $1 \leq i \leq r$ with $C_i < B_i$ we are in Case 1.5b with respect to Δ and the prime power $\ell_i^{a_i}$. We then have that L and $K(Cf)$ are the two primitive residue fields of Δ-CM points on $X_0^D(N)$, and that d_1 and d_2 are the two primitive degrees of such points.*

Proof. The proof follows exactly as in [Cl23, Thm 9.2]; the main inputs here are the degrees of our residue fields, which are the same for our totally complex index 2 subfields of ring class fields as they are for the rational ring class fields appearing in the elliptic modular study. □

5.4 CM points on $X_1^D(N)_{/\mathbb{Q}}$

In this section, we prove Theorem 1.4, showing that there is a very close relationship between CM points on the Shimura curves $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$. This is a generalization of [CS23, Thm 1.2], which was specific to the $D = 1$ case, and allows us to go from our understanding of the Δ-CM locus on $X_0^D(N)_{/\mathbb{Q}}$ based on §5.3 to an understanding of that on $X_1^D(N)_{/\mathbb{Q}}$. We restate the result here for the convenience of the reader.

Theorem 1.4. *Suppose that $x \in X_0^D(N)_{/\mathbb{Q}}$ is a point with CM by the imaginary quadratic order of discriminant Δ. Let $\pi : X_1^D(N)_{/\mathbb{Q}} \to X_0^D(N)_{/\mathbb{Q}}$ denote the natural morphism.*

1. *If $\Delta < -4$, then π is inert over x.*

2. *Suppose that $\Delta \in \{-3, -4\}$.*

   (a) *If x is a ramified point of the map $X_0^D(N)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$ or if $N \leq 3$, then π is inert over x.*

   (b) *Otherwise, we have*

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

   for the ramification index and residual degree of x, respectively, with respect to π.

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

Proof. We first recall some relevant facts: for $N \leq 2$ the map π is an isomorphism. For $N \geq 3$ it is a $(\mathbb{Z}/N\mathbb{Z})^*/\{\pm 1\}$-Galois covering, hence has degree $\phi(N)/2$. All points on $X_1^D(N)_{/\mathbb{Q}}$ not having CM by discriminant $\Delta \in \{-3, -4\}$ are unramified over their image on $X^D(1)_{/\mathbb{Q}}$. For $N \geq 4$, just as in the $D = 1$ case, the curve $X_1^D(N)_{/\mathbb{Q}}$ has no elliptic points of periods 2 or 3, from which it follows that all -4 and -3-CM points on $X_1^D(N)_{/\mathbb{Q}}$ are ramified with ramification index 2 or 3, respectively. The curve $X_1^D(2)_{/\mathbb{Q}}$ has a single elliptic point of period 2 lying over each of the 2^b points on $X^D(1)_{/\mathbb{Q}}$ with -4-CM, while the curve $X_1^D(3)_{/\mathbb{Q}}$ has a single elliptic point of period 3 lying over each of the 2^b points on $X^D(1)_{/\mathbb{Q}}$ with -3-CM. (One can see these claims regarding elliptic points and ramification from elementary arguments involving congruence subgroups. For example, for $D = 1$ this is [DS05, Exc. 2.3.7]).

First, suppose that $\Delta < -4$. If $N \leq 2$ then this map is an isomorphism, so assume $N \geq 3$ in which case the degree of the map is $\frac{\phi(N)}{2}$. Let $\mathfrak{f}$ be the conductor of Δ, such that $\Delta = \mathfrak{f}^2 \Delta_K$, and consider a point $\tilde{x} \in \pi^{-1}(x)$. It suffices to show that $[K(\tilde{x}) : K(x)] = \frac{\phi(N)}{2}$, viewing π as a morphism over K.

Take $\varphi : (A, \iota) \to (A', \iota')$ to be a QM-cyclic N-isogeny over $K(x)$ inducing $x \in X_0^D(N)_{/K}$. By Theorem 2.3.4 we have that the field of moduli of (A, ι) is $K(\mathfrak{f})$, and we have a well

defined ± 1 Galois representation

$$\overline{\rho}_N : G_{\mathbb{K}(\mathfrak{f})} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

not depending on our choice of representative for x, as $\mathrm{Aut}(A, \iota) = \{\pm 1\}$. Letting $Q = \ker(\varphi) \leq A[N]$ and letting $P \in Q$ be a choice of generator (of $e_1(Q)$ as an abelian group, or equivalently of Q as an $\mathcal{O}$-module), then the action of $G_{K(\mathfrak{f})}$ on P is tracked by an isogeny character

$$\lambda : G_{\mathbb{K}(\mathfrak{f})} \to (\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

Theorem 3.4 gives that $A_{\mathbb{C}} := A \otimes_{\mathrm{Spec}\, K(x)} \mathrm{Spec}\, \mathbb{C}$ has a decomposition $\psi : A_{\mathbb{C}} \xrightarrow{\sim} \mathbb{C}/\mathfrak{o}(\mathfrak{f}) \times E_A$, where E_A is a Δ-CM elliptic curve over $\mathbb{C}$. The elliptic curves in this decomposition both have models over $K(\mathfrak{f})$, and hence a $K(\mathfrak{f})$-rational model for this product is a twist of A.

It then suffices, as our representation is independent of the choice of $K(\mathfrak{f})$-rational model, to consider the case $A = E \times E'$ with E and E' being Δ-CM elliptic curves over $K(\mathfrak{f})$. Here, our QM-stable subgroup $Q \leq A[N]$ corresponds to a cyclic subgroup of $E[N]$, and λ is induced by the Galois action on this cyclic subgroup. This ± 1 character λ is surjective by [St01] (see also [BC20b, Thm 1.4]). Therefore, if $\{P, -P\}$ is stable over an extension L of $K(\mathfrak{f})$, such that $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ is in the kernel of λ, we have

$$\frac{\phi(N)}{2} \mid [L : K(\mathfrak{f})],$$

and so indeed we have $[K(\tilde{x}) : K(x)] = \phi(N)/2$.

We next tackle case (2)(a), assuming that x is a ramified point of the map $X_0^D(N)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$. Equivalently, the point x is non-elliptic. In this case, we have that a representative $(A, \iota, Q)_{/K(x)}$ inducing x, where $Q \leq A[N]$ is a QM-cyclic subgroup, is well-defined up to quadratic twist, as all models for (A, ι) are defined over $K(x)$. The same argument as in the $\Delta < -4$ case above then applies.

We now assume that x is an elliptic Δ-CM point on $X_0^D(N)_{/\mathbb{Q}}$ with $\Delta \in \{-3, -4\}$. If $N = 2$, then π is an isomorphism, so the claim is trivial. If $N = 3$, the fact mentioned above

that there is one point lying over each elliptic point on $X^D(1)_{/\mathbb{Q}}$ is exactly the inertness claim. For $N \geq 4$, we know that x is elliptic while every point in $\pi^{-1}(x)$ is ramified with respect to the map $X_1^D(N)_{/\mathbb{Q}} \to X^D(1)_{/\mathbb{Q}}$, giving the claimed ramification index. The residual degree is therefore *at most* the claimed residual degree in each case.

To provide the lower bound on the residual degree, we modify the argument of the $\Delta < -4$ case slightly in a predictable way. If $\Delta = -4$, then a representative for x is well-defined up to quartic twist. We consider a representative of the form $(E_1 \times E_2, \iota, \mathcal{O} \cdot C)$ where E_1, E_2 are $\mathfrak{o}(\mathfrak{f})$-CM elliptic curves and $C \leq E_1[N]$ is a cyclic order N subgroup (again, via the type of argument as in the $\Delta < -4$ case using Theorem 3.4). Let $q_N : \mathfrak{o}_K \to \mathfrak{o}_K/N\mathcal{O}_K$ denote the quotient map. By tracking the action of Galois on a generator P of C we get a well-defined reduced mod N Galois representation

$$\overline{\rho_N} : \mathrm{Gal}(\mathbb{Q}(x)/\mathbb{Q}) \to (\mathcal{O}_K/N\mathcal{O}_K)^\times / q_N(\mathcal{O}_K^*)$$

which is surjective (see [BC20b, §1.3]). As the set $\{P, -P, iP, -iP\}$ is stable under the action of $\mathrm{Gal}(\mathbb{Q}(\tilde{x})/\mathbb{Q})$ for $\tilde{x} \in \pi^{-1}(x)$, we must have

$$\frac{\varphi(N)}{4} = \#\left(\overline{\rho_N}\left(\mathrm{Gal}(\mathbb{Q}(\tilde{x})/\mathbb{Q})\right)\right) \mid [\mathbb{Q}(\tilde{x}) : \mathbb{Q}(x)],$$

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

5.5 Sporadic CM points on Shimura Curves

Fix $D > 1$ an indefinite rational quaternion discriminant and $N \in \mathbb{Z}^+$ relatively prime to D. In analogy to prior work on degrees of CM points on certain classical families of elliptic modular curves [CGPS22], we may consider the least degree $d_{\mathrm{CM}}(X)$ of a CM-point on a Shimura curve X for the modular Shimura curves $X = X_0^D(N)_{/\mathbb{Q}}$ and $X = X_1^D(N)_{/\mathbb{Q}}$. For an imaginary quadratic order $\mathfrak{o}$, the results of §5.3.3 allow us to compute all primitive residue fields and degrees of $\mathfrak{o}$-CM points on $X_0^D(N)_{/\mathbb{Q}}$, and hence to compute the least degree

$\mathrm{d}_{\mathfrak{o},\mathrm{CM}}(X_0^D(N))$ of an $\mathfrak{o}$-CM point on $X_0^D(N)_{/\mathbb{Q}}$. Note that the least degree of an $\mathfrak{o}$-CM point on $X_0^D(N)_{/\mathbb{Q}}$ always satisfies

$$h(\mathfrak{o}) \mid d_{\mathfrak{o},\mathrm{CM}}(X_0^D(N)).$$

Using a complete list of all imaginary quadratic orders $\mathfrak{o}$ of class number up to 100, it then follows that if we have some order $\mathfrak{o}_0$ with

$$d_{\mathfrak{o}_0,\mathrm{CM}}(X_0^D(N)) \leq 100,$$

then we can solve the minimization over orders problem to compute the least degree of a CM point on $X_0^D(N)_{/\mathbb{Q}}$:

$$d_{\mathrm{CM}}(X_0^D(N)) = \min\left\{d_{\mathfrak{o},\mathrm{CM}}(X_0^D(N)) \mid h(\mathfrak{o}) \leq 100\right\}.$$

We have implemented an algorithm to compute least degrees over specified orders and, when possible, to compute $d_{\mathfrak{o},\mathrm{CM}}(X_0^D(N))$ exactly as described above. The relevant code, along with all other code used for the computational tasks described in this section, can be found at the repository [Rep]. One may also find there a list of computed exact values of $d_{\mathrm{CM}}(X_0^D(N))$, along with an order minimizing the degree, for all relevant pairs (D, N) with $DN < 10^5$. All computations described in this section are performed using [Magma].

Theorem 1.4 provides all of the information we need to go from least degrees of CM points on $X_0^D(N)_{/\mathbb{Q}}$ to least degrees of CM points on $X_1^D(N)_{/\mathbb{Q}}$. For ease of the relevant statement, we first generalize some terminology from [CGPS22]: we will call a pair (D, N) with $N \geq 4$

- **Type I** if D splits $\mathbb{Q}(\sqrt{-3})$, we have $\mathrm{ord}_3(N) \leq 1$, and N is not divisible by any prime $\ell \equiv 2 \pmod 3$, and
- **Type II** if D splits $\mathbb{Q}(\sqrt{-1})$, we have $\mathrm{ord}_2(N) \leq 1$, and N is not divisible by any prime $\ell \equiv 3 \pmod 4$.

Proposition 5.5.1. *Let $D > 1$ be a rational quaternion discriminant and $N \in \mathbb{Z}^+$ coprime to D.*

1. *If (D, N) is Type I, then*

$$d_{\mathrm{CM}}(X_1^D(N)) = \frac{\phi(N)}{3}.$$

2. *If (D, N) is not Type I and is Type II, then*

$$d_{\mathrm{CM}}(X_1^D(N)) = \frac{\phi(N)}{2}.$$

3. *If (D, N) is not Type I or Type II, then*

$$d_{\mathrm{CM}}(X_1^D(N)) = \frac{\phi(N)}{2} \cdot d_{\mathrm{CM}}(X_0^D(N)).$$

Proof. The natural map $X_1^D(N)_{/\mathbb{Q}} \to X_0^D(N)_{/\mathbb{Q}}$ has non-trivial ramification exactly when (D, N) is either Type I or Type II. In these cases, we have $d_{\mathrm{CM}}(X_0^D(N)) = 2$, which is as small as possible as the $D > 1$ assumption implies these curves have no rational points. The statements then follow immediately from the residual degrees with respect to this map provided by Theorem 1.4. □

For a curve $X_{/\mathbb{Q}}$, let $\delta(X)$ denote the least positive integer d such that X has infinitely points of degree d. We call a point $x \in X$ **sporadic** if

$$\deg(x) := [\mathbb{Q}(x) : \mathbb{Q}] < \delta(X).$$

That is, x is a sporadic point if there are only finitely points $y \in X$ with $\deg(y) \leq \deg(x)$. In the remainder of this section, we apply our least degree computations towards the question of whether the curves $X_0^D(N)_{/\mathbb{Q}}$ and $X_1^D(N)_{/\mathbb{Q}}$ have sporadic CM points.

5.5.1 An explicit upper bound on $d_{\mathrm{CM}}(X_0^D(N))$

In analogy to the Heegner hypothesis of the classical elliptic modular case, we make the following definition:

Definition 5.5.2. Let D be an indefinite quaternion discriminant and N a positive integer relatively prime to D. We will say that an imaginary quadratic discriminant Δ **satisfies the** (D, N) **Heegner hypothesis** if

1. for all primes $\ell \mid D$, we have $\left(\frac{\Delta}{\ell}\right) = -1$, and
2. for all primes $\ell \mid N$, we have $\left(\frac{\Delta}{\ell}\right) = 1$,

If Δ satisfies the (D, N) Heegner hypothesis, this implies the existence of a Δ-CM point on $X_0^D(N)_{/\mathbb{Q}}$ which is rational over $K(\mathfrak{f})$, the ring class field of conductor $\mathfrak{f}$ where $\Delta = \mathfrak{f}^2\Delta_K$. This point therefore has degree at most $2 \cdot h(\mathfrak{o}(\mathfrak{f}))$.

We provide an upper bound on the least degree of a CM point on $X_0^D(N)_{/\mathbb{Q}}$ as follows: let L be the least positive integer such that

- $\left(\frac{L}{p}\right) = -1$ for all odd primes $p \mid D$,
- $\left(\frac{L}{p}\right) = 1$ for all odd primes $p \mid N$, and
- we have

$$L \equiv \begin{cases} 5 \pmod 8 \text{ if } 2 \mid D \\ 1 \pmod 8 \text{ otherwise.} \end{cases}$$

Then $0 < L < 8DN$, and so $d_0 = L - 16DN$ is an imaginary quadratic discriminant satisfying the (D, N) Heegner hypothesis with $-16DN < d_0 < -8DN$. It follows that there exists a fundamental discriminant Δ_K of an imaginary quadratic field K satisfying the (D, N) Heegner hypothesis with $|\Delta_K| < 16DN$; take K such that d_0 corresponds to an order in K and hence $d_0 = \mathfrak{f}^2\Delta_K$ for some positive integer $\mathfrak{f}$.

For an imaginary quadratic field K of discriminant $\Delta_K < -4$, we have

$$h_K = h(\mathfrak{o}(\Delta_K)) \leq \frac{e}{2\pi}\sqrt{|d|}\log|d|$$

(see, e.g., [CCS13, Appendix]), such that the above provides

$$d_{\mathrm{CM}}(X_0^D(N)) \leq 2 \cdot h_K \leq \frac{4e}{\pi}\sqrt{DN}\log(16DN). \tag{5.2}$$

5.5.2 Shimura curves with infinitely many points of degree 2

If $\delta(X_0^D(N)) = 2$, then as $X_0^D(N)_{/\mathbb{Q}}$ has no real points it certainly does not have a sporadic point. We mention here all pairs (D, N) for which we know $\delta(X_0^D(N)) = 2$ based on the existing literature.

All genus 0 and 1 cases necessarily have $\delta(X_0^D(N)) = 2$, as we have no degree 1 points. Voight [Voi09] lists all (D, N) for which $X_0^D(N)_{/\mathbb{Q}}$ has genus zero:

$$\{(6,1),(10,1),(22,1)\},$$

and genus one:

$$\{(6,5),(6,7),(6,13),(10,3),(10,7),(14,1),(15,1),(21,1),(33,1),(34,1),(46,1)\}.$$

By a result of Abramovich–Harris [AH91], a nice curve X defined over $\mathbb{Q}$ of genus at least 2 with $\delta(X) = 2$ is either hyperelliptic over $\mathbb{Q}$, or is bielliptic and emits a degree 2 map to an elliptic curve over $\mathbb{Q}$ with positive rank. The pairs (D, N) for which $X_0^D(N)_{/\mathbb{Q}}$ is hyperelliptic of genus at least 2 were determined by Ogg[2] [Ogg83]:

$$\begin{aligned}\{&(6,11),(6,19),(6,29),(6,31),(6,37),(10,11),(10,23),(14,5),(15,2),\\ &(22,3),(22,5),(26,1),(35,1),(38,1),(39,1),(39,2),(51,1),(55,1),(58,1),(62,1),\\ &(69,1),(74,1),(86,1),(87,1),(94,1),(95,1),(111,1),(119,1),(134,1),\\ &(146,1),(159,1),(194,1),(206,1)\}.\end{aligned}$$

As for the bielliptic case, Rotger [Rot02] has determined all discriminants D such that $X^D(1) = X_0^D(1)$ is bielliptic, and further determines those for which this curve is bielliptc over $\mathbb{Q}$ and maps to a positive rank elliptic curve. All such discriminants D with $g(X_0^D(1)) \geq 2$

[2]Actually, for the pairs $(10, 19)$ and $(14, 5)$, the referenced work of Ogg says that the corresponding curves are hyperelliptic over $\mathbb{R}$. Ogg does not say whether that is the case over $\mathbb{Q}$, but work of Guo-Yang [GY17] answers negatively for the former pair and positively for the latter.

and with $X_0^D(1)_{/\mathbb{Q}}$ not hyperelliptic are as follows:

$$D \in \{57, 65, 77, 82, 106, 118, 122, 129, 143, 166, 210, 215, 314, 330, 390, 510, 546\}.$$

5.5.3 Sporadic CM points

In order to declare the existence of a sporadic CM point on a Shimura curve $X_0^D(N)_{/\mathbb{Q}}$, a main tool for us will be the following result of Frey [Frey94, Prop. 2] on the least degree $\delta(X)$ over which a nice curve $X_{/F}$ has infinitely many closed points:

Theorem 5.5.3 (Frey 1994)**.** *For a nice curve X defined over a number field F, we have*

$$\frac{\gamma_F(X)}{2} \leq \delta(X) \leq \gamma_F(X),$$

where $\gamma_F(X)$ denotes the F-gonality of X, i.e., is the least degree of a non-constant F-rational map to the projective line.

It follows from Theorem 5.5.3 that if

$$d_{\mathrm{CM}}(X_0^D(N)) < \frac{\gamma_{\mathbb{Q}}(X_0^D(N))}{2}, \tag{5.3}$$

then there exists a sporadic CM point on $X_0^D(N)_{/\mathbb{Q}}$. To complement this, a result of Abramovich ([Abr96, Thm. 1.1]) provides a lower bound on the gonality of a Shimura curve. Our cases of interest in applying this result are $X_0^D(N) = X_{\Gamma_0^D(N)}$ and $X_1^D(N) = X_{\Gamma_1^D(N)}$ (or, equivalently, $X_0^D(N) = X_{\mathcal{O}_N^1}$, where $\mathcal{O}_N$ is an Eichler order of level N in B, for the former curve).

Theorem 5.5.4 (Abramovich 1996)**.** *Let X_Γ be the Shimura curve corresponding to $\Gamma \leq \mathcal{O}^1$ a subgroup of the units of norm 1 in an order $\mathcal{O}$ of B. Then*

$$\frac{21}{200}(g(X_\Gamma) - 1) \leq \gamma_{\mathbb{C}}(X_\Gamma) \leq \gamma_{\mathbb{Q}}(X_\Gamma).$$

The following result will allow us to transfer information about the existence of sporadic points on $X_0^D(N)_{/\mathbb{Q}}$ to those on $X_1^D(N)_{/\mathbb{Q}}$:

Proposition 5.5.5. *Let $\pi : X_1^D(N)_{/\mathbb{Q}} \to X_0^D(N)_{/\mathbb{Q}}$ denote the natural modular map. Suppose that $P_0 \in X_0^D(N)_{/\mathbb{Q}}$ satisfies*

$$\deg(P_0) \leq \frac{21}{400}(g(X_0^D(N) - 1).$$

Then any $P \in X_1^D(N)_{/\mathbb{Q}}$ with $\pi(P) = P_0$ is sporadic.

Proof. For such a point $P \in X_1^D(1)_{/\mathbb{Q}}$, using the notation and results of Proposition 2.1.8 and Example 2.1.11 we have

$$\begin{aligned}
\deg(P) &\leq \deg(P_0) \cdot \deg(\pi) \\
&= \deg(P_0) \cdot \frac{\phi(N)}{2} \\
&\leq \frac{21}{400}\left(\frac{\phi(D)\psi(N)}{12} - \frac{\epsilon_1(D,N)}{4} - \frac{\epsilon_3(D,N)}{3}\right) \cdot \frac{\phi(N)}{2} \\
&\leq \frac{21}{400}\left(\frac{\phi(N)\phi(D)\psi(N)}{24}\right) \\
&= \frac{21}{400}(g(X_1^D(N) - 1).
\end{aligned}$$

It then follows from Theorem 5.5.4 that P is sporadic. □

We now obtain a lower bound on the genus of $X_0^D(N)$ that will be amenable to our arguments:

Lemma 5.5.6. *For $D > 1$ an indefinite rational quaternion discriminant and $N \in \mathbb{Z}^+$ relatively prime to D, we have*

$$\begin{aligned}
g(X_0^D(N)) - 1 &> \frac{DN}{12}\left(\frac{1}{e^\gamma \log\log D + \frac{3}{\log\log(D)}}\right) - \frac{7\sqrt{DN}}{3} \\
&\geq \frac{DN}{12}\left(\frac{1}{e^\gamma \log\log (DN) + \frac{3}{\log\log(6)}}\right) - \frac{7\sqrt{DN}}{3}.
\end{aligned}$$

Proof. We recall the genus formula from Proposition 2.1.8:

$$g(X_0^D(N)) = 1 + \frac{\phi(D)\psi(N)}{12} - \frac{\epsilon_1(D,N)}{4} - \frac{\epsilon_3(D,N)}{3},$$

where

$$\epsilon_1(D,N) = \begin{cases} \prod_{p|D}\left(1 - \left(\frac{-4}{p}\right)\right)\prod_{p|N}\left(1 + \left(\frac{-4}{p}\right)\right) & \text{if } 4 \nmid N \\ 0 & \text{if } 4 \mid N \end{cases}$$

$$\epsilon_3(D,N) = \begin{cases} \prod_{p|D}\left(1 - \left(\frac{-3}{p}\right)\right)\prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right) & \text{if } 9 \nmid N \\ 0 & \text{if } 9 \mid N. \end{cases}$$

We make use of the trivial bound $\psi(N) \geq N$, and the lower bound

$$\phi(D) > \frac{D}{e^\gamma \log\log D + \frac{3}{\log\log D}}.$$

For $M \in \mathbb{Z}^+$, let $\omega(M)$ and $d(M)$ denote, respectively, the number of distinct prime divisors of M and the number of divisors of M. We then have

$$\epsilon_1(D,N), \epsilon_3(D,N) \leq 2^{\omega(DN)} \leq d(DN) \leq d(D) \cdot d(N) \leq 4\sqrt{DN}.$$

Using these bounds along with the fact that $D \geq 6$ and $N \geq 1$, we arrive at the stated inequalities. □

The combination of this lemma with (5.2) and (5.3) guarantees a sporadic CM point on $X_0^D(N)_{/\mathbb{Q}}$ if

$$\frac{4e}{\pi}\sqrt{DN}\log(16DN) \leq \frac{7DN}{1600}\left(\frac{1}{e^\gamma \log\log(DN) + \frac{3}{\log\log(6)}}\right) - \frac{49\sqrt{DN}}{400}.$$

This inequality holds for all pairs (D,N) with $DN \geq 5.60483 \cdot 10^{10}$.

Ranging through pairs (D, N) with DN below this bound, we attempt to determine the fundamental imaginary quadratic discriminant Δ_K of smallest absolute value satisfying the (D, N)-Heegner hypothesis, and check whether

$$h_K < \frac{7\phi(D)\psi(N)}{3200} - \frac{49\sqrt{DN}}{800}. \tag{5.4}$$

We confirm that (5.4) holds, and thus a sporadic CM point on $X_0^D(N)_{/\mathbb{Q}}$ is ensured, for all pairs (D, N) with $DN > 15078$ aside from the 20 pairs comprising the following set $\mathcal{F}_1$:

$$\begin{aligned}\mathcal{F}_1 = \{&(101959, 210), (111397, 210), (141427, 210), (154583, 210), (164749, 210),\\ &(165053, 330), (174629, 330), (190619, 210), (192907, 210), (194051, 210),\\ &(199801, 330), (208351, 210), (218569, 210), (233519, 210), (240097, 210),\\ &(272459, 210), (287419, 210), (296153, 210), (304513, 210), (307241, 210)\}.\end{aligned}$$

For each pair $(D, N) \in \mathcal{F}_1$, it is not that the inequality (5.4) does not hold. Rather, there is no imaginary quadratic discriminant of class number at most 100 satisfying the (D, N)-Heegner hypothesis, such that we fail to perform the check using only such discriminants. For these pairs, we compute $d_{\mathrm{CM}}(X_0^D(N))$ exactly and find that for each the inequality

$$d_{\mathrm{CM}}(X_0^D(N)) < \frac{7\phi(D)\psi(N)}{1600} - \frac{49\sqrt{DN}}{400}$$

holds. By the preceding remarks, this confirms that the curve $X_0^D(N)_{/\mathbb{Q}}$ has a sporadic CM point for all $(D, N) \in \mathcal{F}_1$.

There are exactly 4691 pairs (D, N) with $DN \leq 15078$ for which the inequality (5.4) does not hold. For each of these, we perform an exact computation of $d_{\mathrm{CM}}(X_0^D(N))$. By the above, a sporadic CM points on $X_0^D(N)_{/\mathbb{Q}}$ is guaranteed if

$$d_{\mathrm{CM}}(X_0^D(N)) < \frac{21}{400}\left(\frac{\phi(D)\psi(N)}{12} - \frac{e_1(D, N)}{4} - \frac{e_3(D, N)}{3}\right). \tag{5.5}$$

Lemma 5.5.7. *There are exactly* 682 *pairs* (D, N) *consisting of a rational quaternion discriminant* $D > 1$ *and a positive integer* N *coprime to* D *such that the inequality* (5.5) *does not hold. For all such pairs we have* $d_{CM}(X_0^D(1)) \in \{2, 4, 6\}$*, and the largest value of* D *occuring among such pairs is* $D = 1770$*.*

Proof. This follows from direct computation. □

Lemma 5.5.8. *For each of the 227 pairs* (D, N) *in Table 5.1, the curve* $X_0^D(N)_{/\mathbb{Q}}$ *has a sporadic CM point.*

Proof. For each pair (D, N) appearing in the referenced table, from §5.5.2 we know that $X_0^D(1)_{/\mathbb{Q}}$ does not have infinitely many degree 2 points and hence $X_0^D(N)_{/\mathbb{Q}}$ does not have infinitely many degree 2 points. At the same time, this curve has a CM point of degree 2, which is therefore necessarily sporadic. □

We are now prepared to end with the main result of this section:

Theorem 5.5.9. *1. For each pair* (D, N) *in Table 5.2, the Shimura curve* $X_0^D(N)_{/\mathbb{Q}}$ *has no sporadic points. For each of these pairs, we have* $d_{CM}(X_0^D(N)) = 2$*.*

2. For each pair (D, N) *in Table 5.2 except for possibly the* 6 *in the following set:*

$$\{(6, 7), (6, 13), (6, 19), (6, 31), (6, 37), (10, 7)\},$$

the Shimura curve $X_1^D(N)_{/\mathbb{Q}}$ *has no sporadic CM points.*

3. For all pairs (D, N)*, consisting of a rational quaternion discriminant* $D > 1$ *and a positive integer* N *coprime to* D*, which are not among the* 64 *listed in Table 5.2 and the* 391 *pairs in Table 5.3, the Shimura curve* $X_0^D(N)_{/\mathbb{Q}}$ *has a sporadic CM point.*

4. For all pairs (D, N)*, consisting of a rational quaternion discriminant* $D > 1$ *and a positive integer* N *coprime to* D*, which are not listed in Table 5.2 or Table 5.3 and not equal to* $(91, 5)$*, the Shimura curve* $X_1^D(N)_{/\mathbb{Q}}$ *has a sporadic CM point.*

Proof. 1. These Shimura curves $X_0^D(N)_{/\mathbb{Q}}$ are exactly those for which we know that $\delta(X_0^D(N)) = 2$ via §5.5.2. That each such curve has a CM point of degree 2 follows from direct computation.

2. For each pair in this table, we have

$$\delta(X_1^D(N)) \leq 2 \cdot \deg(X_1^D(N) \to X_0^D(N)) = \max\{2, \phi(N)\}.$$

For each pair in this table other than the 6 listed pairs, we compute that

$$\max\{2, \phi(N)\} \leq d_{\mathrm{CM}}(X_1^D(N)).$$

3. This is an immediate consequence of the preceding discussion, including Lemmas 5.5.7 and 5.5.8.

4. By Proposition 5.5.5, we have that $X_1^D(N)_{/\mathbb{Q}}$ has a sporadic CM points for all pairs (D, N) aside from possibly the 682 referred to in Lemma 5.5.7. Of the 227 pairs in Table 5.1, we compute that each pair except for $(D, N) = (91, 5)$ satisfies

$$d_{\mathrm{CM}}(X_1^D(N)) = 2 < \delta(X_0^D(1)) \leq \delta(X_1^D(N)),$$

and hence we have a sporadic CM point on $X_1^D(N)_{/\mathbb{Q}}$ for all such pairs. The result then follows from part (2).

□

$(6, 17)$	$(6, 23)$	$(6, 25)$	$(6, 35)$	$(6, 41)$	$(6, 43)$	$(6, 47)$	$(6, 49)$	$(6, 53)$
$(6, 55)$	$(6, 59)$	$(6, 61)$	$(6, 65)$	$(6, 67)$	$(6, 71)$	$(6, 73)$	$(6, 77)$	$(6, 79)$
$(6, 83)$	$(6, 85)$	$(6, 89)$	$(6, 91)$	$(6, 95)$	$(6, 97)$	$(6, 101)$	$(6, 103)$	$(6, 107)$
$(6, 109)$	$(6, 113)$	$(6, 115)$	$(6, 119)$	$(6, 121)$	$(6, 125)$	$(6, 127)$	$(6, 131)$	$(6, 133)$

$(6, 137)$	$(6, 139)$	$(6, 143)$	$(6, 145)$	$(6, 149)$	$(6, 151)$	$(6, 155)$	$(6, 157)$	$(6, 161)$
$(6, 163)$	$(6, 167)$	$(6, 169)$	$(6, 173)$	$(6, 179)$	$(6, 181)$	$(6, 185)$	$(6, 187)$	$(6, 191)$
$(6, 193)$	$(6, 197)$	$(6, 199)$	$(6, 203)$	$(6, 211)$	$(6, 223)$	$(6, 227)$	$(6, 229)$	$(6, 233)$
$(6, 241)$	$(6, 287)$	$(6, 295)$	$(6, 319)$	$(6, 335)$	$(6, 355)$	$(6, 371)$	$(6, 407)$	$(10, 9)$
$(10, 13)$	$(10, 17)$	$(10, 19)$	$(10, 21)$	$(10, 27)$	$(10, 29)$	$(10, 31)$	$(10, 33)$	$(10, 37)$
$(10, 39)$	$(10, 41)$	$(10, 43)$	$(10, 47)$	$(10, 49)$	$(10, 51)$	$(10, 53)$	$(10, 57)$	$(10, 59)$
$(10, 61)$	$(10, 63)$	$(10, 67)$	$(10, 69)$	$(10, 71)$	$(10, 73)$	$(10, 77)$	$(10, 79)$	$(10, 81)$
$(10, 83)$	$(10, 87)$	$(10, 89)$	$(10, 91)$	$(10, 97)$	$(10, 101)$	$(10, 103)$	$(10, 107)$	$(10, 109)$
$(10, 113)$	$(10, 119)$	$(10, 141)$	$(10, 159)$	$(10, 161)$	$(10, 191)$	$(14, 3)$	$(14, 9)$	$(14, 11)$
$(14, 13)$	$(14, 15)$	$(14, 17)$	$(14, 19)$	$(14, 23)$	$(14, 25)$	$(14, 27)$	$(14, 29)$	$(14, 31)$
$(14, 33)$	$(14, 37)$	$(14, 39)$	$(14, 41)$	$(14, 43)$	$(14, 45)$	$(14, 47)$	$(14, 51)$	$(14, 53)$
$(14, 55)$	$(14, 59)$	$(14, 61)$	$(14, 67)$	$(14, 71)$	$(14, 73)$	$(14, 87)$	$(14, 95)$	$(15, 4)$
$(15, 7)$	$(15, 8)$	$(15, 11)$	$(15, 13)$	$(15, 14)$	$(15, 16)$	$(15, 17)$	$(15, 19)$	$(15, 22)$
$(15, 23)$	$(15, 26)$	$(15, 28)$	$(15, 29)$	$(15, 31)$	$(15, 32)$	$(15, 34)$	$(15, 37)$	$(15, 41)$
$(15, 43)$	$(15, 47)$	$(15, 49)$	$(15, 53)$	$(15, 68)$	$(21, 2)$	$(21, 4)$	$(21, 5)$	$(21, 8)$
$(21, 10)$	$(21, 11)$	$(21, 13)$	$(21, 16)$	$(21, 17)$	$(21, 19)$	$(21, 20)$	$(21, 22)$	$(21, 23)$
$(21, 25)$	$(21, 29)$	$(21, 31)$	$(21, 37)$	$(21, 38)$	$(21, 55)$	$(22, 7)$	$(22, 9)$	$(22, 13)$
$(22, 15)$	$(22, 17)$	$(22, 19)$	$(22, 21)$	$(22, 23)$	$(22, 25)$	$(22, 27)$	$(22, 29)$	$(22, 31)$

$(22, 35)$	$(22, 37)$	$(22, 41)$	$(22, 43)$	$(22, 51)$	$(26, 3)$	$(26, 5)$	$(26, 7)$	$(26, 9)$
$(26, 11)$	$(26, 15)$	$(26, 17)$	$(26, 19)$	$(26, 21)$	$(26, 23)$	$(26, 25)$	$(26, 27)$	$(26, 29)$
$(26, 31)$	$(26, 37)$	$(33, 2)$	$(33, 4)$	$(33, 5)$	$(33, 7)$	$(33, 8)$	$(33, 10)$	$(33, 13)$
$(33, 16)$	$(33, 17)$	$(33, 19)$	$(34, 3)$	$(34, 5)$	$(34, 7)$	$(34, 9)$	$(34, 11)$	$(34, 13)$
$(34, 15)$	$(34, 19)$	$(34, 23)$	$(34, 29)$	$(34, 35)$	$(35, 2)$	$(35, 3)$	$(35, 4)$	$(35, 6)$
$(35, 8)$	$(35, 9)$	$(35, 11)$	$(35, 12)$	$(35, 13)$	$(35, 17)$	$(38, 3)$	$(38, 5)$	$(38, 7)$
$(38, 9)$	$(38, 11)$	$(38, 13)$	$(38, 15)$	$(38, 17)$	$(38, 21)$	$(38, 23)$	$(39, 4)$	$(39, 5)$
$(39, 7)$	$(39, 8)$	$(39, 10)$	$(39, 11)$	$(39, 17)$	$(39, 20)$	$(39, 31)$	$(46, 3)$	$(46, 5)$
$(46, 7)$	$(46, 9)$	$(46, 11)$	$(46, 13)$	$(46, 15)$	$(46, 17)$	$(46, 19)$	$(51, 2)$	$(51, 4)$
$(51, 5)$	$(51, 7)$	$(51, 8)$	$(51, 10)$	$(51, 11)$	$(51, 13)$	$(51, 20)$	$(55, 2)$	$(55, 3)$
$(55, 4)$	$(55, 7)$	$(55, 8)$	$(57, 2)$	$(57, 4)$	$(57, 5)$	$(57, 7)$	$(57, 8)$	$(57, 11)$
$(58, 3)$	$(58, 5)$	$(58, 7)$	$(58, 9)$	$(58, 11)$	$(58, 13)$	$(62, 3)$	$(62, 5)$	$(62, 7)$
$(62, 9)$	$(62, 11)$	$(62, 13)$	$(62, 15)$	$(65, 2)$	$(65, 3)$	$(65, 4)$	$(65, 7)$	$(69, 2)$
$(69, 4)$	$(69, 5)$	$(69, 7)$	$(69, 11)$	$(74, 3)$	$(74, 5)$	$(74, 7)$	$(74, 9)$	$(74, 11)$
$(74, 15)$	$(77, 2)$	$(77, 3)$	$(77, 4)$	$(77, 5)$	$(77, 6)$	$(82, 3)$	$(82, 5)$	$(82, 7)$
$(86, 3)$	$(86, 5)$	$(86, 7)$	$(87, 2)$	$(87, 4)$	$(87, 5)$	$(87, 7)$	$(87, 8)$	$(94, 3)$
$(94, 5)$	$(94, 7)$	$(95, 2)$	$(95, 3)$	$(95, 4)$	$(95, 6)$	$(95, 9)$	$(106, 3)$	$(106, 5)$
$(106, 7)$	$(111, 2)$	$(111, 4)$	$(111, 5)$	$(111, 8)$	$(118, 3)$	$(118, 5)$	$(118, 7)$	$(119, 2)$

$(119, 3)$	$(119, 6)$	$(122, 3)$	$(122, 5)$	$(122, 7)$	$(129, 2)$	$(129, 7)$	$(134, 3)$	$(134, 5)$
$(134, 9)$	$(143, 2)$	$(143, 4)$	$(146, 3)$	$(146, 5)$	$(146, 7)$	$(159, 2)$	$(166, 3)$	$(183, 5)$
$(185, 4)$	$(194, 3)$	$(206, 3)$	$(215, 2)$	$(215, 3)$	$(219, 5)$	$(274, 5)$	$(326, 3)$	$(327, 2)$
$(327, 2)$	$(327, 4)$	$(335, 2)$	$(390, 7)$	$(546, 5)$				

Table 5.3: All 391 pairs (D, N) with $D > 1$ for which we remain unsure whether $X_0^D(N)_{/\mathbb{Q}}$ has a sporadic CM point

Table 5.1: 227 pairs (D, N) for which $X_0^D(N)_{/\mathbb{Q}}$ has a sporadic CM point of degree 2 via Lemma 5.5.8

$(85,1)$	$(85,2)$	$(85,3)$	$(85,4)$	$(91,1)$	$(91,2)$	$(91,3)$	$(91,4)$	$(91,5)$
$(93,1)$	$(93,2)$	$(93,4)$	$(93,5)$	$(115,1)$	$(115,2)$	$(115,3)$	$(123,1)$	$(123,2)$
$(133,1)$	$(133,2)$	$(133,3)$	$(141,1)$	$(141,2)$	$(142,1)$	$(142,3)$	$(142,5)$	$(145,1)$
$(145,2)$	$(145,3)$	$(155,1)$	$(155,2)$	$(158,1)$	$(158,3)$	$(158,5)$	$(161,1)$	$(161,2)$
$(177,1)$	$(177,2)$	$(178,1)$	$(178,3)$	$(183,1)$	$(183,2)$	$(185,1)$	$(185,2)$	$(187,1)$
$(201,1)$	$(201,2)$	$(202,1)$	$(202,3)$	$(203,1)$	$(205,1)$	$(209,1)$	$(213,1)$	$(213,2)$
$(214,1)$	$(214,3)$	$(217,1)$	$(218,1)$	$(218,3)$	$(219,1)$	$(219,2)$	$(221,1)$	$(226,1)$
$(226,3)$	$(235,1)$	$(237,1)$	$(237,2)$	$(247,1)$	$(249,1)$	$(253,1)$	$(254,1)$	$(259,1)$
$(262,1)$	$(265,1)$	$(267,1)$	$(274,1)$	$(278,1)$	$(287,1)$	$(291,1)$	$(295,1)$	$(298,1)$
$(299,1)$	$(301,1)$	$(302,1)$	$(303,1)$	$(305,1)$	$(309,1)$	$(319,1)$	$(321,1)$	$(323,1)$
$(326,1)$	$(327,1)$	$(329,1)$	$(334,1)$	$(335,1)$	$(339,1)$	$(341,1)$	$(346,1)$	$(355,1)$
$(358,1)$	$(362,1)$	$(365,1)$	$(371,1)$	$(377,1)$	$(381,1)$	$(382,1)$	$(386,1)$	$(391,1)$
$(393,1)$	$(394,1)$	$(395,1)$	$(398,1)$	$(403,1)$	$(407,1)$	$(411,1)$	$(413,1)$	$(415,1)$
$(417,1)$	$(422,1)$	$(427,1)$	$(437,1)$	$(445,1)$	$(446,1)$	$(447,1)$	$(451,1)$	$(453,1)$
$(454,1)$	$(458,1)$	$(462,1)$	$(466,1)$	$(469,1)$	$(471,1)$	$(473,1)$	$(478,1)$	$(481,1)$
$(482,1)$	$(485,1)$	$(489,1)$	$(493,1)$	$(497,1)$	$(501,1)$	$(502,1)$	$(505,1)$	$(511,1)$
$(514,1)$	$(515,1)$	$(517,1)$	$(519,1)$	$(526,1)$	$(535,1)$	$(537,1)$	$(538,1)$	$(542,1)$
$(543,1)$	$(545,1)$	$(553,1)$	$(554,1)$	$(562,1)$	$(565,1)$	$(566,1)$	$(570,1)$	$(573,1)$
$(579,1)$	$(586,1)$	$(591,1)$	$(597,1)$	$(614,1)$	$(622,1)$	$(626,1)$	$(633,1)$	$(634,1)$
$(662,1)$	$(669,1)$	$(674,1)$	$(681,1)$	$(687,1)$	$(690,1)$	$(694,1)$	$(698,1)$	$(699,1)$
$(706,1)$	$(714,1)$	$(717,1)$	$(718,1)$	$(734,1)$	$(746,1)$	$(758,1)$	$(766,1)$	$(770,1)$
$(778,1)$	$(794,1)$	$(798,1)$	$(802,1)$	$(818,1)$	$(838,1)$	$(842,1)$	$(858,1)$	$(862,1)$
$(866,1)$	$(870,1)$	$(878,1)$	$(886,1)$	$(898,1)$	$(910,1)$	$(914,1)$	$(922,1)$	$(926,1)$
$(930,1)$	$(934,1)$	$(958,1)$	$(966,1)$	$(1110,1)$	$(1122,1)$	$(1190,1)$	$(1218,1)$	$(1230,1)$
$(1254,1)$	$(1290,1)$	$(1302,1)$	$(1326,1)$	$(1330,1)$	$(1410,1)$	$(1482,1)$	$(1518,1)$	$(1554,1)$
$(1590,1)$	$(1770,1)$							

Table 5.2: 64 pairs (D, N) with $\gcd(D, N) = 1$ for which $\delta(X_0^D(N)) = 2$, and hence $X_0^D(N)_{/\mathbb{Q}}$ has no sporadic points

$(6, 1)$	$(6, 5)$	$(6, 7)$	$(6, 11)$	$(6, 13)$	$(6, 19)$
$(6, 29)$	$(6, 31)$	$(6, 37)$	$(10, 1)$	$(10, 3)$	$(10, 7)$
$(10, 11)$	$(10, 23)$	$(14, 1)$	$(14, 5)$	$(15, 1)$	$(15, 2)$
$(21, 1)$	$(22, 1)$	$(22, 3)$	$(22, 5)$	$(26, 1)$	$(33, 1)$
$(34, 1)$	$(35, 1)$	$(38, 1)$	$(39, 1)$	$(39, 2)$	$(46, 1)$
$(51, 1)$	$(55, 1)$	$(57, 1)$	$(58, 1)$	$(62, 1)$	$(65, 1)$
$(69, 1)$	$(74, 1)$	$(77, 1)$	$(82, 1)$	$(86, 1)$	$(87, 1)$
$(94, 1)$	$(95, 1)$	$(106, 1)$	$(111, 1)$	$(118, 1)$	$(119, 1)$
$(122, 1)$	$(129, 1)$	$(134, 1)$	$(143, 1)$	$(146, 1)$	$(159, 1)$
$(166, 1)$	$(194, 1)$	$(206, 1)$	$(210, 1)$	$(215, 1)$	$(314, 1)$
$(330, 1)$	$(390, 1)$	$(510, 1)$	$(546, 1)$		

Bibliography

[Abr96] D. Abramovich, *A linear lower bound on the gonality of modular curves.* International Mathematics Research Notices, Volume 1996, Issue 20, 1996.

[AH91] D. Abramovich and J. Harris, *Abelian varieties and curves in $W_d(C)$.* Compositio Mathematica 78. 1991.

[AB04] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms and Shimura curves.* CRM Monograph Series 22, American Mathematical Society, Providence, 2004.

[an] anonymous (https://mathoverflow.net/users/483658/anonymous), *Easiest example where field of definition is not field of moduli*, URL (version: 2022-06-06): `https://mathoverflow.net/q/424121`.

[Art26] E. Artin, *Zur Theorie der hyperkomplexen Zahlen.* Abh. Math. Sem. Hamburgischen Univ., 1926.

[BC20a] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves.* Pacific Journal of Mathematics, 2020.

[BC20b] A. Bourdon and P.L. Clark, *Torsion points and isogenies on CM elliptic curves.* Proceedings of the London Mathematical Society, 2020.

[BCP17] A. Bourdon, P.L. Clark, and P. Pollack, *Anatomy of torsion in the CM case.* Math. Z., 2017.

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

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

[Magma] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput., 24, 1997, 235–265.

[Buz97] K. Buzzard, *Integral models of certain Shimura curves*. Duke Math. J. 87, 1997.

[Cl03] P. L. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*. Harvard PhD. thesis, 2003.

[Cl09] P. L. Clark, *On the Hasse principle for Shimura curves*. Israel J. Math. 171, 2009.

[Cl23] P. L. Clark *CM elliptic curves: volcanoes, reality, and applications, part I*. Preprint: arXiv:2212.13316, 2023.

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

[CGPS22] P. L. Clark, T. Genao, P. Pollack, F. Saia, *The least degree of a cm point on a modular curve*, Journal of the London Mathematical Society, 2022.

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

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

[CS23] P. L. Clark and F. Saia, *CM elliptic curves: volcanoes, reality, and applications, part II*. Preprint, arXiv:2212.13327, 2023.

[CSt18] P. L. Clark and J. Stankewicz, *Hasse Principle Violations for Atkin-Lehner Twists of Shimura Curves*. Proc. Amer. Math. Soc. 146, 2018.

[Cox13] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* Second Edtiion. John Wiley & Sons, New York, 2013.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques.* Proc. Antwerpen Conference, vol. 2; Lecture Notes in Mathematics. Springer-Verlag, New York, (1973), 143-316.

[DEMHZ21] M. Derickx, A. Etropolski, M, van Hoeij, and D. Zureick-Brown, *Sporadic cubic torsion.* Algebra and Number Theory, 2021.

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

[Fou01] M. Fouquet, *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques.* École Polytechnique PhD. thesis, 2002.

[FM02] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm.* Algorithmic Number Theory Symposium 2002. Lecture Notes in Computer Science, vol 2369. Springer, 2002.

[Frey94] G. Frey, *Curves with infinitely many points of fixed degree.* Israel Journal of Mathematics 85, 1994.

[GR06] J. González and V. Rotger, *Non-elliptic shimura curves of genus one.* Journal of the Mathematical Society of Japan, 2006.

[GY17] J. Guo and Y. Yang, *Equations of hyperelliptic Shimura curves.* Compositio Mathematica 153, 2017.

[H06] B. Huggins, *Fields of moduli and fields of definition for curves*, University of California, Berkeley PhD. thesis, 2006.

[Jor81] B. W. Jordan, *On the Diophantine arithmetic of Shimura curves.* Harvard PhD. thesis, 1981.

[Kam92] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms.* Inventiones Mathematicae, 1992.

[Ka11] E. Kani, *Products of CM elliptic curves.* Collect. Math., 2011.

[KM88] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields.* Naguya Mathematical Journal, 1988.

[Koh96] D. Kohel, *Endomorphism rings of elliptic curves over finite fields.* University of California at Berkeley PhD. thesis, 1996.

[Koi72] S. Koizumi, *The fields of moduli for polarized abelian varieties and for curves*, Nagoya Math Journal, 1972.

[La75] H. Lange, *Produkte elliptischer kurven.* Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II, 1975.

[LR18] Á. Lozano-Robledo, *Galois representations attached to elliptic curves with complex multiplication.* Preprint: arXiv:1809.02584, 2018.

[Mat58] T. Matsusaka, *Polarized varieties, fields of moduli and generalized kummer varieties of polarized abelian varieties.* American Journal of Mathematics, 1958.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal.* Publications Mathématiques I.H.E.S., 1977.

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Inventiones Mathematicae, 1996.

[Mil72] J. Milne, *Abelian varieties defined over their fields of moduli.* Bulletin of the London Math. Society. 1972.

[Mor22] L. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.* Proc. Camb. Phil. Soc. Vol. 21, 1922.

[Ogg83] M. Artin and J. Tate, *Arithmetic and geometry: papers dedicated to I. R. Shafarevich on the occassion of his sixtieth birthday. Volume 1: Arithmetic*. A. P. Ogg, *Real points on Shimura curves* pp. 277-308. Springer Science and Business Media, New York, 1983.

[PS22] O. Padurariu and C. Schembri, *Rational points on Atkin–Lehner quotients of geometrically hyperelliptic Shimura curves*. Preprint, arXiv:2212.04553. 2022.

[Po17] B. Poonen, *Rational points on varieties*. American Mathematical Society, 2017.

[Rot02] V. Rotger, *On the group of automorphisms of Shimura curves and applications*. Compositio Mathematica 131, 2002.

[RSY05] V. Rotger, A. Skorobogatov and A. Yafaev, *Failure of the Hasse principle on Atkin-Lehner quotients of Shimura curves over* $\mathbb{Q}$. Moscow Math. Journal, 2005.

[Rep] F. Saia, *CM-Points-Shimura-Curves* Github Repository. `https://github.com/fsaia/CM-Points-Shimura-Curves`.

[Sc92] C. Schoen, *Produkte abelscher Varietäten und Moduln über Ordnungen*. J. Reine Angew. Math. 429, 1992.

[Sh59] G. Shimura, *On the theory of automorphic functions*. Annals of Mathematics, 1959.

[Sh67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*. Annals of Mathematics, 1967.

[Sh72] G. Shimura, *On the field of rationality for an abelian variety*. Nagoya Math. J. 1972.

[Sh75] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*. Mathematische Annalen 215, 1975.

[SM74] T. Shioda and N. Mitani, *Singular abelian surfaces and binary quadratic forms*. Classification of algebraic varieties and compact complex manifolds, pp. 259–287. Lecture Notes in Math., Vol. 412, Springer, Berlin, 1974.

[Si88] A. Silverberg, *Torsion points on abelian varieties of CM-type.* Compositio Math., 1988.

[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.

[Sil] J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994.

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

[Sut13] D. Sutherland, *Isogeny volcanoes.* Proceedings of the Tenth Algorithmic Number Theory Symposium, The Open Book Series Volume 1, 2013.

[Uf10] D. Ufer, *Shimura-Kurven, Endomorphismen und q-Parameter.* Universität Ulm PhD. thesis, 2010.

[Vig80] M. Vignèras. *Arithmètique des algébres de quaternions.* Lecture Notes in Mathematics 800, Springer, Berlin, 1980.

[Voi09] J. Voight, *Shimura curves of genus at most two.* Mathematics of Computation 78, 2009.

[Voi21] J. Voight, *Quaternion Algebras.* Graduate Texts in Mathematics 288, Springer, Cham, 2021.

[Wed08] J. H. Maclagan Wedderburn, *On hypercomplex numbers.* Proc. London Math. Soc., 1908.