

RM-KLPT: Algebraic Pathfinding for Superspecial Abelian Surfaces with Maximal Real Multiplication

Mingjie Chen¹, Thomas Decru¹, Péter Kutas^{2,3}, Mickaël Montessinos²,
Sebastian A. Spindler⁴, and Nicolas Swanson⁵

¹ KU Leuven, Belgium

² Eötvös Loránd University, Hungary

³ University of Birmingham, United Kingdom

⁴ University of the Bundeswehr Munich, Germany

⁵ University of Waterloo, Canada

Abstract. The isogeny graphs of superspecial abelian surfaces with maximal real multiplication were first studied by Charles, Goren, and Lauter in 2009, when they constructed the RM-CGL hash function on these graphs and proved that they are Ramanujan. As a consequence, these graphs enjoy optimal expansion properties, which are either absent or difficult to establish in other higher-dimensional isogeny graphs.

In this paper, we take a closer look at these graphs from a cryptographic perspective, and attempt to demonstrate that they are the natural generalization of the supersingular ℓ -isogeny graph to dimension two.

To this end, we tackle two algorithmic problems: We design and implement the RM-KLPT algorithm to solve the algebraic pathfinding problem in these isogeny graphs by solving a norm equation in ideals of a quaternion algebra over a real quadratic field. Further, we revisit the RM-CGL hash function, provide a proof-of-concept implementation, and showcase that knowledge of the initial surface's algebraic description leads to a second-preimage attack on the hash function through our RM-KLPT algorithm.

RM-KLPT resembles the one-dimensional KLPT algorithm much more closely than KLPT² does. This is due to the existence of a higher-dimensional analogue of the Deuring correspondence in the RM setting, which yields significantly shorter paths ($\sim p^3$) compared to KLPT².

Finally, we conclude by discussing potential cryptographic constructions that may be built from RM-KLPT.

Keywords: Isogenies, Abelian Surfaces, Real Multiplication, KLPT, CGL

1 Introduction

Starting with the devastating attacks on SIKE [CD23; Mai+23; Rob23], in which a lemma of Kani [Kan97] on embedding a one-dimensional isogeny into a higher-dimensional one played a significant role, higher-dimensional generalizations of elliptic curve isogenies have become a major driving force in isogeny-based cryptography in recent years. Constructive techniques [PR23; Rob25] emerging from these attacks have proven crucial both for improving existing schemes, such as SQIsign [Bas+25b; Dar+24; Nak+24], and for enabling new cryptographic constructions such as the PRISM signature scheme [Bas+26; Bas+25a] and the effective group action framework PEGASIS [Dar+25a]. However, the resulting protocols are one-dimensional in the sense that they rely on the hardness of computing endomorphism rings of supersingular elliptic curves, and they use higher-dimensional isogenies primarily as a tool for computing one-dimensional isogenies more efficiently.

Moving to higher dimensions has the advantage that the corresponding endomorphism ring problem is believed to be harder than that for supersingular elliptic curves. This allows one to work with smaller characteristics, which admit faster finite field arithmetic. In fact, higher-dimensional isogenies had already been studied in the field prior to the SIKE attacks, primarily from the perspective of generalizing the supersingular isogeny graph to higher dimensions.

The situation, however, becomes substantially more complicated, as it is not clear what the natural analogue of supersingular elliptic curves and their isogenies should be in the higher-dimensional setting. While isogeny graphs of superspecial abelian varieties have been the primary focus [CDS20; FT19; Tak18], LeGrow, Ti, and Zobernig [LTZ23] also considered graphs of supersingular non-superspecial abelian surfaces, though these do not generalize the one-dimensional graphs. Unfortunately, these higher-dimensional approaches fail to provide the strong expansion properties available in the one-dimensional setting. Indeed, although the graph of superspecial abelian varieties remains connected, it fails to be Ramanujan in general [JZ26]. Nevertheless, it still exhibits reasonable expansion properties [FS22] and, when equipped with a level structure, is conjectured to be weakly Ramanujan for $\ell = 2, 3$ in dimension two [DR26]. On the other hand, the graph of supersingular non-superspecial abelian surfaces is not even connected, and the question of its expansion properties within a connected component was left open in [LTZ23].

Beyond graph-theoretical studies, efforts have been made in generalizing algebraic methods in dimension one to dimension two. The most famous example is generalizing the KLPT algorithm [Koh+14], which solves the path-finding algorithm on the supersingular ℓ -isogeny graphs, to superspecial (ℓ, ℓ) -isogeny graph of abelian surfaces through the KLPT² algorithm [Cas+25]. Despite the successful generalization, one major drawback of [Cas+25] and even its improvement [PRS26] is that the output size is significantly higher than that of KLPT, which complicates the task of generalizing schemes like SQIsign [DF+20] to this setting. As a consequence, we either need more efficient algorithms or a different choice of higher dimensional analogues of supersingular isogeny graphs.

Another graph that is much less considered in the isogeny community is the ℓ -isogeny graph of superspecial abelian surfaces with real multiplication (RM), introduced by Charles, Goren, and Lauter in 2009 [CGL09]. In this setting, superspecial abelian varieties of dimension g are equipped with a real multiplication by a totally real field K of degree g , that is, with an embedding of the ring of integers R_K into the endomorphism ring of the variety. In the same paper, the authors show that when the field K has strict class number 1, these graphs are Ramanujan. As an application, they leverage these graphs to propose an analogue of their well-known one-dimensional CGL hash function [CLG09], which we refer to as RM-CGL. Besides the Ramanujan property, the algebraic perspective on these graphs provides a higher-dimensional extension of the well-known Deuring correspondence in dimension one. The RM version of this correspondence was studied by Nicole in 2005 [Nic05], albeit with applications to Hilbert modular forms in mind. The one-dimensional Deuring correspondence has seen numerous applications in isogeny-based cryptography, and this RM extension appears to be the first higher-dimensional instance with comparable cryptographic potential. This motivates the question of whether the RM isogeny graph is a more natural analogue of the 1-dimensional setting. As a fundamental algorithmic tool, we are particularly interested in the following question on this graph:

The algebraic pathfinding problem:

*Given the endomorphism rings (or equivalent algebraic information) of vertices on the RM isogeny graph, can we do pathfinding on this graph?
If yes, what is the expected output length?*

The closer analogue to the Deuring correspondence naturally motivates the problem of looking for a real multiplication preserving version of algebraic pathfinding. One might hope that, since the problem seems close to the one-dimensional counterpart, statements from elliptic curves translate better to the real multiplication setting than to the general superspecial setting.

1.1 Our contributions

All of the implementations referred to below are written in SageMath [Sage]. We provide implementations in two separate repositories:

- RM-KLPT: <https://gitlab.com/Mickanos/real-multiplication>
- RM-CGL: <https://github.com/NicSwansonwaterloo/RMIsogenies>

The RM-KLPT algorithm. We refine the Ibukiyama–Katsura–Oort correspondence [IKO86] with real multiplication, and then provide an analogue of the KLPT algorithm in this refined framework: Given the IKO description (g_1, a_1) and (g_2, a_2) of two principally polarized superspecial abelian surfaces with real multiplication by a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ of small discriminant and strict class number 1, our algorithm solves the following system of equations:

$$\begin{aligned}\gamma a_1 &= a_2 \gamma, \\ \gamma^* g_2 \gamma &= g_1 \ell^n,\end{aligned}\tag{1}$$

where ℓ is a rational prime that is inert in K and γ lies in $M_2(\mathcal{O}_0)$ for some fixed maximal order $\mathcal{O}_0$ in $\mathcal{B}_{p,\infty}$, the quaternion $\mathbb{Q}$ -algebra of discriminant p .

While the framework we work in looks similar to the two-dimensional variant of the KLPT algorithm [Cas+25], our algorithm is spiritually much closer to the original KLPT algorithm [Koh+14]. Indeed, after finding an initial isogeny $(g_1, a_1) \rightarrow (g_2, a_2)$ that is compatible with the real multiplications, our problem turns into a norm-finding problem over a quaternion algebra over K ; in fact, the quaternion algebra we need to consider is precisely the K -scalar extension of the quaternion algebra $\mathcal{B}_{p,\infty}$ that underlies the KLPT algorithm in dimension 1. Having established all steps for this translation, the main remaining technical work of the construction of our RM-KLPT algorithm lies in the adaptation of the techniques from [Koh+14] to our base field K . In the end, we show that the output isogeny is of size $\sim p^3$. We also implement the RM-KLPT algorithm to demonstrate its practicality, and we provide experimental evidence for the heuristics of Section 5. It is highly important to note that this **asymptotically matches** the output length of the 1-dimensional KLPT algorithm, whereas KLPT² variants produce much longer paths [Cas+25; PRS26]. This shows that working with superspecial abelian varieties with small real multiplication might be the most promising higher dimensional generalization of supersingular elliptic curves.

A concrete realization of the RM-CGL hash function. We revisit the RM-CGL hash function introduced in [CGL09]. Unlike RM-KLPT, it does not require knowledge of endomorphism rings nor their associated algebraic data. We show how to represent and transport real multiplication with standard (d, d) - and (ℓ, ℓ) -isogeny computations, allowing us to traverse RM isogeny graphs in dimension two using well-known isogeny algorithms [Dar+25b; LR16]. We also provide a theta-coordinate based implementation of RM-CGL for $K = \mathbb{Q}(\sqrt{5})$ and $\ell = 2$.

A second preimage attack on the RM-CGL hash function. Finally, we leverage our RM-KLPT algorithm to break the second preimage resistance of the RM-CGL hash function when given the algebraic data associated with the initial vertex. This shows that the starting surface in the RM-CGL hash function needs to be chosen carefully, similarly to how the original CGL hash function [CLG09] in dimension one should be instantiated with a supersingular elliptic curve of unknown endomorphism ring (cf. [Eis+18; Eis+20]). Note that this is a strict advantage over the KLPT² algorithm, which fails to break the second preimage resistance of the corresponding hash function [CDS20] since it produces a ‘bad’ chain of (ℓ, ℓ) -isogenies with high probability, as discussed in [Cas+25, Section 5.4].

1.2 Outline

In Section 2 we give the necessary preliminaries for this work. In Section 3 we introduce the definitions of superspecial abelian surfaces with real multiplications, their isogenies and the resulting isogeny graph. In Section 4 we define the algebraic path-finding problem in both the IKO framework (Problem 4.13) and the quaternion language (Problem 4.18), and we show that Problem 4.13 reduces to Problem 4.18. In Section 5 we introduce our main algorithm RM-KLPT that solves Problem 4.18, for which we generalize many 1-dimensional KLPT subroutines. In Section 6 we describe an instantiation of the RM-CGL hash function from [CGL09], and we show an algebraic second preimage attack on this hash function. Finally, we discuss some future directions in Section 7.

1.3 Acknowledgments

We would like to thank Yan Bo Ti and Damien Robert for helpful discussions, and Travis Morrison, Victoria de Quehen, Chloe Martindale and Jason LeGrow for organizing the 2025 BIRS workshop “Isogeny Graphs in Cryptography” at which this project started. We also want to thank all anonymous reviewers for their feedback.

Mingjie Chen and Thomas Decru are supported by Fonds voor Wetenschappelijk Onderzoek (FWO) with reference numbers 12A4L26N and 1245025N respectively, by the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788), by the Research Council KU Leuven grant C14/24/099 and by CyberSecurity Research Flanders with reference number VOEWICS02. Péter Kutas is partly supported by EPSRC through grant number EP/V011324/1, and he is also supported by the Hungarian Ministry of Innovation and Technology NRDI Office within the framework of the Quantum Information National Laboratory Program. Mickaël Montessinos and Péter Kutas are supported by the grant “EXCELLENCE-151343”. Nicolas Swanson is supported by the NSERC Alliance Consortia Quantum Grant “Accelerating the transition to quantum-resistant cryptography” (ALLRP 578463–2022), the NSERC Canada Graduate Research Scholarship program, and CryptoWorks21.

2 Preliminaries and notation

2.1 Superspecial abelian surfaces

A *superspecial abelian surface* over $\mathbb{F}_{p^2}$ is an abelian surface that is isomorphic to a product of two supersingular elliptic curves. While all such surfaces are isomorphic due to a theorem of Deligne [Shi79, Theorem 3.5], we can equip them with *principal polarizations* and only consider between them the *polarized isogenies* $\varphi: (A, \lambda) \rightarrow (A', \lambda')$ of *reduced degree* $\deg(\varphi) \in \mathbb{N}$. With this we can separate these surfaces into (polarized) products of two supersingular elliptic curves, of which we find $\Theta(p^2)$, and into superspecial *Jacobians* of genus-2 curves, of which we find $\Theta(p^3)$. We provide more background on these surfaces in Appendix A.1.

2.2 Quaternion algebras

The quaternion algebra $\mathcal{B}_{p,\infty}$ is a $\mathbb{Q}$ -algebra of dimension four defined with respect to a prime number p . In particular, if $p \equiv 3 \pmod{4}$, the algebra $\mathcal{B}_{p,\infty}$ admits a basis $(1, \mathbf{i}, \mathbf{j}, \mathbf{ij})$ such that $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = -p$ and $\mathbf{ij} = -\mathbf{ji}$. In this article we will mainly work in the matrix algebra $M_2(\mathcal{B}_{p,\infty})$ of 2×2 -matrices with entries in $\mathcal{B}_{p,\infty}$. For more details on quaternion algebras, see Appendix A.2.

2.3 The strict class group of a number field

To ensure that our isogeny graphs with real multiplication will be Ramanujan, we want to enforce that the quadratic field K has strict class number 1. In Appendix A.3 we provide more background on the strict class group of a number field, including a proof of the following statement:

Corollary 2.1. *The real quadratic field $K = \mathbb{Q}(\sqrt{d})$ has strict class number 1 if and only if it has class number 1 and the following equivalent conditions holds:*

- (i) *Every totally positive unit in $R_K^\times$ is a square in $R_K^\times$.*
- (ii) *The fundamental unit ε_K is neither totally positive nor totally negative.*
- (iii) *$N_{K/\mathbb{Q}}(\varepsilon_K) = -1$.*

Moreover, in this case d is a prime with $d \not\equiv 3 \pmod{4}$, i.e. $d = 2$ or $d \equiv 1 \pmod{4}$.

2.4 Notation

Throughout the paper we fix a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ of strict class number 1 and discriminant d_K ; note that, by Corollary 2.1, we have $d_K = d$ unless $d = 2$ (for which $d_K = 8$). We let R_K denote the ring of integers of K and $\alpha_K \in \{\sqrt{d}, \frac{1+\sqrt{d}}{2}\}$ its standard generator, i.e. $R_K = \mathbb{Z}[\alpha_K]$. We write R_K^+ for the totally positive elements in R_K , and $R_K^{\times,+} = R_K^\times \cap R_K^+$ for the totally positive units in R_K . Furthermore we fix a prime $p > 5$ that is unramified in K , i.e. $p \nmid d$, and let $\mathbb{N} \ni \ell \neq p$ denote another prime that is unramified in K . Finally, we fix a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$ of known endomorphism ring $\mathcal{O}_0 = \text{End}(E_0)$.

3 Superspecial abelian varieties with real multiplication and their isogeny graphs

In this section, we first introduce superspecial abelian surfaces with real multiplication and their isogenies, and then we discuss the resulting real multiplication isogeny graphs from [CGL09] in dimension two.

3.1 Superspecial abelian surfaces with real multiplication

Definition 3.1. ([CGL09, Section 2.2]) A *superspecial abelian surface with real multiplication by K* , or *K -superspecial surface* for short, is a triple (A, ι, λ) such that

- A is a superspecial abelian surface over $\mathbb{F}_{p^2}$,
- $\iota: R_K \hookrightarrow \text{End}(A)$ is a ring embedding, and
- $\lambda: A \rightarrow A^\vee$ is an R_K -equivariant principal polarization with respect to the induced embedding $\iota^\vee: R_K \hookrightarrow \text{End}(A^\vee)$, i.e.

$$\lambda \circ \iota(x) = \iota(x)^\vee \circ \lambda \quad \text{for all } x \in R_K.$$

Definition 3.2. Let $(A_1, \iota_1, \lambda_1), (A_2, \iota_2, \lambda_2)$ be two K -superspecial surfaces:

- A morphism of abelian surfaces $\varphi: A_1 \rightarrow A_2$ is called a *K -linear morphism* if it is R_K -equivariant, i.e.,

$$\varphi \circ \iota_1(x) = \iota_2(x) \circ \varphi \quad \text{for all } x \in R_K.$$

A K -linear morphism is called a *K -linear isogeny* if its underlying morphism of abelian surfaces is an isogeny. If, in addition, it is polarized with respect to λ_1 and λ_2 , it is called a *polarized K -linear isogeny*.

- A K -linear isogeny

$$\varphi: (A_1, \iota_1, \lambda_1) \rightarrow (A_2, \iota_2, \lambda_2)$$

is called a *K -linear equivalence* if its underlying morphism of abelian surfaces is an isomorphism. It is called a *K -linear isomorphism* if it additionally preserves the principal polarizations.

- Two K -superspecial surfaces are called *equivalent* (resp. *isomorphic*) if there exists a K -linear equivalence (resp. a K -linear isomorphism) between them.
- Two K -linear isogenies $\varphi_1: (A, \iota, \lambda) \rightarrow (A_1, \iota_1, \lambda_1)$, $\varphi_2: (A, \iota, \lambda) \rightarrow (A_2, \iota_2, \lambda_2)$ are called *equivalent* (resp. *isomorphic*) if there exists a K -linear equivalence (resp. a K -linear isomorphism)

$$\alpha: (A_1, \iota_1, \lambda_1) \rightarrow (A_2, \iota_2, \lambda_2) \quad \text{such that} \quad \varphi_2 = \alpha \circ \varphi_1.$$

For a given K -superspecial surface (A, ι, λ) , any unit $u \in R_K^\times$ induces another K -superspecial surface $(A, \iota, \iota(u)^\vee \circ \lambda \circ \iota(u))$, together with the K -linear isomorphism

$$\iota(u^{-1}): (A, \iota, \lambda) \rightarrow (A, \iota, \iota(u)^\vee \circ \lambda \circ \iota(u)). \quad (2)$$

The assumption that K has strict class number 1 implies that the real multiplication ι actually already determines the principal polarization λ on A uniquely up to the K -linear isomorphisms coming from $\iota(R_K^\times)$ as above. This is shown in [CGL09, Section 2.2] in the language of schemes (see also [Nic05, pp. 73–74]), but we will also provide an algebraic proof later in Corollary 4.14.

To define a notion of degree for a K -linear isogeny $\varphi: (A_1, \iota_1, \lambda_1) \rightarrow (A_2, \iota_2, \lambda_2)$, we write

$$\tilde{\varphi} := \lambda_1^{-1} \varphi^\vee \lambda_2: (A_2, \iota_2, \lambda_2) \rightarrow (A_1, \iota_1, \lambda_1)$$

for the *reverse K -linear isogeny* $\tilde{\varphi}$ of φ . The following lemma shows that this reverse isogeny generalizes the one-dimensional notion of dual isogenies for an adjusted definition of the degree; it follows from [CGL09, p. 6] (see also [Nic05, Section 2.5.3]), but we will independently derive it in Corollary 4.11.

Lemma 3.3. Let $\varphi: (A_1, \iota_1, \lambda_1) \rightarrow (A_2, \iota_2, \lambda_2)$ be a K -linear isogeny. Then we have $\tilde{\varphi} \circ \varphi \in \iota_1(R_K^+)$, $\varphi \circ \tilde{\varphi} \in \iota_2(R_K^+)$ and

$$\iota_1^{-1}(\tilde{\varphi} \circ \varphi) = \iota_2^{-1}(\varphi \circ \tilde{\varphi}).$$

The above allows us to define the degree of a K -linear isogeny:

Definition 3.4. ([CGL09, Section 2.2.2], [Nic05, Section 2.5.3]) Consider a K -linear isogeny $\varphi: (A_1, \iota_1, \lambda_1) \rightarrow (A_2, \iota_2, \lambda_2)$. Then the K -degree of φ is defined as $\deg_K^{\lambda_1, \lambda_2}(\varphi) := \iota_1^{-1}(\tilde{\varphi} \circ \varphi)$.

Remark 3.5. The K -linear isogeny φ has integer degree $\deg_K^{\lambda_1, \lambda_2}(\varphi) \in \mathbb{N}_{>0}$ if and only if it actually is a polarized isogeny of reduced degree $\deg_K^{\lambda_1, \lambda_2}(\varphi)$.

The multiplicativity of the degree follows from a straightforward calculation:

Lemma 3.6. For two K -linear isogenies $(A_1, \iota_1, \lambda_1) \xrightarrow{\varphi} (A_2, \iota_2, \lambda_2) \xrightarrow{\psi} (A_3, \iota_3, \lambda_3)$ we have $\deg_K^{\lambda_1, \lambda_3}(\psi \circ \varphi) = \deg_K^{\lambda_2, \lambda_3}(\psi) \cdot \deg_K^{\lambda_1, \lambda_2}(\varphi)$.

Since the real multiplication determines the polarization uniquely up to K -linear isomorphism, it seems natural to omit it from our notation and write (A, ι) . We must, however, resolve the ambiguity in the K -degree arising from the K -linear isomorphisms in Equation (2). To this end, we leverage the fact that polarizations are uniquely determined up to a unit: For any K -linear isogeny $\varphi: (A, \iota_A) \rightarrow (B, \iota_B)$ together with R_K -equivariant polarizations $\lambda_{A,1}, \lambda_{A,2}$ on (A, ι_A) and $\lambda_{B,1}, \lambda_{B,2}$ on (B, ι_B) , we can find a unit $u \in R_K^\times$ such that

$$\deg_K^{\lambda_{A,1}, \lambda_{B,1}}(\varphi) = u^2 \cdot \deg_K^{\lambda_{A,2}, \lambda_{B,2}}(\varphi).$$

Importantly, our assumption that $\text{Cl}^+(K)$ is trivial shows (cf. Corollary 2.1) that this is equivalent to the equality of ideals

$$\deg_K^{\lambda_{A,1}, \lambda_{B,1}}(\varphi) \cdot R_K = \deg_K^{\lambda_{A,2}, \lambda_{B,2}}(\varphi) \cdot R_K,$$

thus motivating the following definition:

Definition 3.7. Let $\varphi: (A_1, \iota_1) \rightarrow (A_2, \iota_2)$ be a K -linear isogeny. We say that φ has K -degree $\deg_K(\varphi) = I$ for an ideal $I \subseteq R_K$ if and only if, for a/any choice of K -linear polarizations λ_i on (A_i, ι_i) , we have $\deg_K^{\lambda_1, \lambda_2}(\varphi) \cdot R_K = I$.

3.2 RM isogeny graphs and their Ramanujan property

We are now ready to introduce the RM isogeny graph(s). In addition to our notations and conventions from Section 2.4, we let $\mathfrak{l} \subseteq R_K$ denote a prime ideal above ℓ , i.e. $\mathfrak{l} \cap \mathbb{Z} = \ell\mathbb{Z}$.

Definition 3.8. The *RM isogeny graph* $\mathcal{G}_K(p, \mathfrak{l})$ is the (directed multi-)graph consisting of

- vertices the set of equivalence classes of K -superspecial surfaces over $\mathbb{F}_{p^2}$, and
- edge set containing, for each vertex pair (v_1, v_2) , edges $v_1 \rightarrow v_2$ corresponding to the number of K -linear isogenies $v_1 \rightarrow v_2$ of K -degree $\mathfrak{l}$ up to equivalence.

Remark 3.9. Due to the scaling isomorphisms (2), Corollary 2.1 and Lemma 3.3 (cf. Corollaries 4.11 and 4.14), two K -superspecial surfaces are equivalent if and only if they are isomorphic. However, these notions differ for isogenies: Two K -linear isogenies φ, ψ are equivalent if and only if there is a $u \in R_K^\times$ such that $\iota_2(u) \circ \varphi$ and ψ are isomorphic. In particular, φ and $\iota_2(u) \circ \varphi$ are equivalent for any $u \in R_K^\times$, but they are isomorphic if and only if $u \in \{\pm 1\}$.

These RM isogeny graphs have been studied extensively in [CGL09, Sections 3-4]; we summarize their properties in the following theorem, which is a combination of the results in *loc. cit.* (specialized to dimension 2) and mostly well-known results on Ramanujan graphs. For completeness we provide a more extensive discussion in Appendix B, where we also explain how the special structure of $\mathcal{G}_K(p, \ell)$ allows for more straightforward spectral-theoretic arguments than a general analysis of the graph's Laplacian.

Theorem 3.10. The RM isogeny graph $\mathcal{G}_K(p, \mathfrak{l})$ has the following properties:

- (a) $\mathcal{G}_K(p, \mathfrak{l})$ has $n = \Theta(p^2 d^{3/2})$ vertices.
- (b) $\mathcal{G}_K(p, \mathfrak{l})$ is (out-)regular of degree $\ell^f + 1$ where $f = f(\mathfrak{l}|\ell) \in \{1, 2\}$ denotes the inertia degree of $\mathfrak{l}$ (over ℓ).
- (c) The adjacency matrix $\mathcal{A}$ of $\mathcal{G}_K(p, \mathfrak{l})$ (for a fixed vertex numbering) is self-adjoint with respect to a suitable inner product (cf. Equation (7)).
- (d) $\mathcal{G}_K(p, \mathfrak{l})$ is a Ramanujan graph: It has the eigenvalue $\ell^f + 1$ with multiplicity 1, and all other of its eigenvalues lie in the interval

$$\left[-2\sqrt{\ell^f}, 2\sqrt{\ell^f}\right].$$

In particular, $\mathcal{G}_K(p, \mathfrak{l})$ is connected with diameter at most

$$2 \log_{\ell^f}(n) + 2 \log_{\ell^f}(72) + 1.$$

Remark 3.11. To use the real multiplication isogeny graph $\mathcal{G}_K(p, \mathfrak{l})$ in practice, we would like to have strong expansion properties, so that vertices are not too far apart and random walks mix reasonably fast. Theorem 3.10 highlights a notable obstacle that we want to avoid to this end: If the prime ℓ splits as $\ell = \mathfrak{l}_1 \cdot \mathfrak{l}_2$,

then the spectral expansion of $\mathcal{G}_K(p, \mathfrak{l}_i)$ in Theorem 3.10 is noticeably worse than in the inert case; for example, our diameter bound turns into⁶ roughly $4 \log_\ell(d^{3/4} \cdot p) + c$ instead of $2 \log_\ell(d^{3/4} \cdot p) + c$. For this reason we will choose our real multiplication such that the rational prime ℓ is inert in K from now on; for simplicity we will then write $\mathcal{G}_K(p, \ell) := \mathcal{G}_K(p, \ell R_K)$.

Similarly to the 1-dimensional setting, it also seems desirable to avoid small cycles for optimal mixing times. We provide in Proposition B.11 of Appendix B an easily verifiable criterion that ensures that our graph $\mathcal{G}_K(p, \ell)$ does not contain any loops or multi-edges.

4 The algebraic side: Refining the IKO correspondence with real multiplication

In this section, we take an algebraic look at the K -superspecial surfaces and their K -linear isogenies we defined in Section 3. By adopting the Ibukiyama–Katsura–Oort (IKO) correspondence [IKO86] and refining it with real multiplication, we show that the geometric path-finding problem in $\mathcal{G}_K(p, \ell)$ can be translated to a matrix equation akin to the one solved in the KLPT² algorithm [Cas+25] (cf. Equation (4) and Problem 4.13).

While this equation is generally much harder to solve than in dimension one, as indicated by the output length of KLPT² [Cas+25; PRS26], the additional condition of K -linearity enables us to translate the geometric objects to a quaternion K -algebra. Through this, we reduce solving the KLPT²-like equation to a norm finding problem in a quaternion ideal in Theorem 4.20, thus simplifying the algebraic path finding problem significantly by enabling an approach analogous to the one-dimensional KLPT algorithm [Koh+14].

4.1 Real multiplication in the IKO framework

Recall that the isomorphism classes of principally polarized superspecial abelian surfaces are all represented by E_0^2 equipped with different principal polarizations $\lambda \in \text{PPol}(E_0^2)$, as discussed at the end of Section A.1. Therefore, our restriction to superspecial abelian surfaces allows us to make use of the IKO correspondence for principally polarized superspecial abelian surfaces as described in [Cas+25]. Via this IKO correspondence (or IKO framework), our surfaces can be represented as 2×2 -matrices over the endomorphism ring $\mathcal{O}_0 = \text{End}(E_0)$:

Proposition 4.1. ([Cas+25, Section 2.3]) Let λ_0 denote the product polarization on E_0^2 . Then the map $\lambda \mapsto \lambda_0^{-1} \lambda =: g_\lambda$ defines a bijection

$$\text{PPol}(E_0^2) \rightarrow \left\{ \begin{pmatrix} s & z \\ \bar{z} & t \end{pmatrix} \mid s, t \in \mathbb{Z}_{>0}, z \in \mathcal{O}_0, st - z\bar{z} = 1 \right\} \subseteq \text{GL}_2(\mathcal{O}_0).$$

⁶ One might instead want to consider the ‘combined’ graph $\mathcal{G}_K(p, \mathfrak{l}_1, \mathfrak{l}_2)$. According to [CGL09, Theorem 4.2] this graph is regular of degree $2\ell + 2$, and all its other eigenvalues are bounded above by $4\sqrt{\ell}$; in particular, this graph has less edges per vertex (unless $\ell = 2$) and worse expansion properties than in the inert case.

Moreover, for any two $\lambda_1, \lambda_2 \in \text{PPol}(E_0^2)$ we have

$$(E_0^2, \lambda_1) \cong (E_0^2, \lambda_2) \iff \exists u \in \text{GL}_2(\mathcal{O}_0): g_{\lambda_2} = u^* \cdot g_{\lambda_1} \cdot u,$$

and the polarized isogenies $(E_0^2, \lambda_1) \rightarrow (E_0^2, \lambda_2)$ of reduced degree $N \in \mathbb{N}$ correspond bijectively to matrices $\gamma \in M_2(\mathcal{O}_0)$ such that $\gamma^* g_{\lambda_2} \gamma = N \cdot g_{\lambda_1}$.

This motivates us to also translate real multiplications to the IKO framework:

Lemma 4.2. Let $\lambda \in \text{PPol}(E_0^2)$ be a principal polarization, and let $a \in M_2(\mathcal{O}_0)$ such that $\mathbb{Z}[a] \cong R_K$. Then the embedding $\iota_a: R_K \hookrightarrow M_2(\mathcal{O}_0)$, $\alpha_K \mapsto a$ defines a real multiplication on (E_0^2, λ) if and only if

$$g_\lambda a = a^* g_\lambda.$$

Proof. By the discussion in [Cas+25, p. 9] (which is also implicit in Proposition 4.1), a^* represents the endomorphism $\varphi^\vee$ dual to the endomorphism φ represented by a . Since $\iota_a(\alpha_K)$ determines ι_a uniquely, the claim follows. $\square$

The above results allow us to only work with matrix equations in $M_2(\mathcal{O}_0)$:

Definition 4.3. We define a (*superspecial*) K -RM pair to be a pair (g, a) where $g = g_\lambda \in \text{GL}_2(\mathcal{O}_0)$ is the g -matrix of some $\lambda \in \text{PPol}(E_0^2)$, and the matrix $a \in M_2(\mathcal{O}_0)$ defines a real multiplication ι_a on (E_0^2, λ) according to Lemma 4.2. Note that, with respect to the Rosati involution $\gamma^\dagger := g^{-1} \gamma^* g$ on $M_2(\mathcal{O}_0)$ induced by g , the condition $ga = a^* g$ is equivalent to a being fixed by said Rosati involution, i.e. $a = a^\dagger = g^{-1} a^* g$.

Remark 4.4. Note that the K -RM pair (g, a) lives in the algebraic world, that is, it is hard to compute it from the geometric description of a vertex of $\mathcal{G}_K(p, \ell)$. Without the extra real multiplication it was shown that computing the g -matrix associated to a principally polarized superspecial surface is equivalent to endomorphism ring computation (in an appropriate sense) under the generalized Riemann hypothesis [PRS26, Theorem 4.12]. Furthermore, the proof of this equivalence goes through an isomorphism $\text{End}(A) \cong M_2(\mathcal{O}_0)$, and this allows us to translate our knowledge of the real multiplication between the different descriptions.

Naturally, the notion of K -linear isogenies also translates to matrices. First, we record the following criterion for a matrix $\gamma \in M_2(\mathcal{O}_0)$ to represent an isogeny $E_0^2 \rightarrow E_0^2$.

Lemma 4.5. An endomorphism $\varphi: E_0^2 \rightarrow E_0^2$ is an isogeny if and only if its matrix representation $\gamma \in M_2(\mathcal{O}_0)$ satisfies that $\gamma \in M_2(\mathcal{B}_{p,\infty})^\times$.

Proof. If γ is invertible, then clearing the denominator of the inverse yields a matrix $\delta \in M_2(\mathcal{O}_0)$ and an integer $n \in \mathbb{N}$ such that $\gamma\delta = n = \delta\gamma$. For the morphism $\psi: E_0^2 \rightarrow E_0^2$ represented by δ we then have

$$\varphi \circ \psi = [n] = \psi \circ \varphi.$$

The first equality shows that φ is surjective, and due to the second the kernel $\ker(\varphi) \subseteq E_0^2[n]$ is finite, so φ is an isogeny.

Conversely, if γ is not invertible, then we find a nonzero matrix $\delta \in M_2(\mathcal{O}_0)$ such that $\delta\gamma = 0$; therefore the nonzero endomorphism ψ represented by δ satisfies $\psi \circ \varphi = 0$, i.e. φ cannot be surjective. $\square$

Second, we classify the matrices in $M_2(\mathcal{O}_0)$ that represent K -linear morphisms, which is immediately verified from the definitions.

Lemma 4.6. Let (g_1, a_1) and (g_2, a_2) be two K -RM pairs with $g_i = g_{\lambda_i}$, and consider a morphism $\varphi: (E_0^2, \iota_1, \lambda_1) \rightarrow (E_0^2, \iota_2, \lambda_2)$ with $\iota_i := \iota_{a_i}$. Then φ is K -linear if and only if its matrix representation $\gamma \in M_2(\mathcal{O}_0)$ satisfies $\gamma a_1 = a_2 \gamma$.

Definition 4.7. We define a *(K-)RM-homomorphism* $(g_1, a_1) \rightarrow (g_2, a_2)$ (between two K -RM pairs) to be a matrix $\gamma \in M_2(\mathcal{O}_0)$ representing a K -linear morphism, i.e. γ satisfies

$$\gamma a_1 = a_2 \gamma.$$

Moreover, we define a *(K-)RM-isogeny* $(g_1, a_1) \rightarrow (g_2, a_2)$ to be a (K) -RM-homomorphism $\gamma \in M_2(\mathcal{O}_0)$ that also satisfies $\gamma \in M_2(\mathcal{B}_{p,\infty})^\times$ (cf. Lemma 4.5).

4.2 The underlying quaternion algebra and the K -degree

In the following result we use the IKO framework to establish the quaternion world in which our RM objects live. Explicitly, we associate to a K -RM pair (g, a) a quaternion K -algebra whose standard involution is induced by g . For the proof of this statement we need the following small additional calculation, which is easily verified:

Lemma 4.8. Let $g = \begin{pmatrix} s & z \\ z & t \end{pmatrix}$ with $z \in \mathcal{B}_{p,\infty}$ and $s, t \in \mathbb{Q}$ with $st - \text{Nrd}(z) = 1$. Then the matrix $\beta = \begin{pmatrix} s & z \\ 0 & 1 \end{pmatrix}$ satisfies $\beta^* \beta = sg$.

Proposition 4.9. Let (g, a) be a K -RM pair. Then the centralizer $\text{Cent}^0(a)$ of a in $M_2(\mathcal{B}_{p,\infty})$ is isomorphic to the quaternion K -algebra $\mathcal{B}_{p,\infty} \otimes K$, and the Rosati involution $\gamma^\dagger = g^{-1} \gamma^* g$ restricts to the unique standard involution on this quaternion K -algebra. In particular, the reduced norm on $\text{Cent}^0(a)$ is given by

$$\text{Cent}^0(a) \rightarrow K, c \mapsto c^\dagger c = cc^\dagger.$$

Proof. The element a gives an embedding $R_K \hookrightarrow M_2(\mathcal{O}_0)$ and thus an embedding $K \hookrightarrow M_2(\mathcal{B}_{p,\infty})$. Applying the double centralizer theorem (Proposition A.16), we see that $\text{Cent}^0(a) = \text{Cent}_{M_2(\mathcal{B}_{p,\infty})}(K)$ is a four-dimensional central simple algebra over K , i.e. a quaternion K -algebra.

As $M_2(\mathbb{Q})$ contains⁷ a field isomorphic to K , the Skolem–Noether theorem (Proposition A.15) yields an $\alpha \in M_2(\mathcal{B}_{p,\infty})^\times$ with $K \subseteq \alpha^{-1} M_2(\mathbb{Q}) \alpha$, and therefore

$$\alpha^{-1} \mathcal{B}_{p,\infty} \alpha = \text{Cent}_{M_2(\mathcal{B}_{p,\infty})}(\alpha^{-1} M_2(\mathbb{Q}) \alpha) \subseteq \text{Cent}_{M_2(\mathcal{B}_{p,\infty})}(K) = \text{Cent}^0(a).$$

⁷ Indeed, for $a^2 = d$ we find $\begin{pmatrix} 0 & d \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{Q})$; computing a suitable conjugating element in the Skolem–Noether theorem, one can compute the centralizer of a from the one of this matrix explicitly.

Since $\mathcal{B}_{p,\infty}$, embedded via the conjugation by α , lies in the centralizer $\text{Cent}^0(a)$, we get the K -algebra homomorphism

$$\mathcal{B}_{p,\infty} \otimes K \rightarrow \text{Cent}^0(a), \beta \otimes \gamma \mapsto \alpha^{-1} \beta \alpha \cdot \gamma,$$

and this map is injective because $\mathcal{B}_{p,\infty} \otimes K$ is simple. As the domain and codomain both have K -dimension four, we thus have found the desired isomorphism.

Next, we check that the Rosati involution restricts to a K -linear automorphism of $\text{Cent}^0(a)$: By definition we have $a^\dagger = a$, and for any $c \in \text{Cent}^0(a)$ we further find

$$c^\dagger a = c^\dagger a^\dagger = (ac)^\dagger = (ca)^\dagger = a^\dagger c^\dagger = ac^\dagger,$$

so $c^\dagger$ lies in $\text{Cent}^0(a)$ again and the Rosati involution $\cdot^\dagger$ acts K -linearly on $\text{Cent}^0(a)$. Now, let us show that the elements fixed by $\cdot^\dagger$ are exactly the scalars in K : Due to Lemma 4.8 we can find a matrix $\beta \in M_2(\mathcal{B}_{p,\infty})$ such that $sg = \beta^* \beta$ for the top-left entry $s \in \mathbb{Z}_{>0}$ of g . For any element $h \in M_2(\mathcal{B}_{p,\infty})$ we then have

$$\beta h^\dagger \beta^{-1} = \beta g^{-1} h^* g \beta^{-1} = s \beta^{-*} h^* s^{-1} \beta^* = (\beta h \beta^{-1})^*, \quad (3)$$

i.e. $h^\dagger = h$ happens if and only if $\beta h \beta^{-1}$ is Hermitian. In particular, due to $a^\dagger = a$ we first see that $a_\beta = \beta a \beta^{-1}$ is a Hermitian square root of d , so we find an $r \in \mathbb{Q}$ and a $z \in \mathcal{B}_{p,\infty}$ such that $a_\beta = \begin{pmatrix} r & z \\ \bar{z} & -r \end{pmatrix}$, where necessarily $z \neq 0$ since d is square-free. Moreover, any other Hermitian matrix $\delta = \begin{pmatrix} x & f \\ \bar{f} & y \end{pmatrix}$, parametrized by $x, y \in \mathbb{Q}$ and $f \in \mathcal{B}_{p,\infty}$, commutes with a_β if and only if the product

$$a_\beta \cdot \delta = \begin{pmatrix} rx + z\bar{f} & rf + yz \\ x\bar{z} - r\bar{f} & \bar{z}f - ry \end{pmatrix}$$

is Hermitian. This forces $\bar{z}f \in \mathbb{Q}$, i.e. $f = t \cdot z$ for some $t \in \mathbb{Q}$ (from the diagonal entries) and further $rt + y = x - rt$ (from the anti-diagonal entries). Therefore $y = x - 2rt$ and we obtain

$$\delta = (x - rt) + t \cdot a_\beta \in \mathbb{Q} + \mathbb{Q}a_\beta = \mathbb{Q}(a_\beta),$$

so

$$\text{Sym}^*(\text{Cent}^0(a_\beta)) := \{\delta \in \text{Cent}^0(a_\beta) : \delta^* = \delta\} = \mathbb{Q}(a_\beta).$$

Finally, Equation (3) shows that the Rosati-invariant elements $\text{Sym}^\dagger(\text{Cent}^0(a))$ of $\text{Cent}^0(a)$ satisfy

$$\text{Sym}^\dagger(\text{Cent}^0(a)) = \beta^{-1} \cdot \text{Sym}^*(\text{Cent}^0(a_\beta)) \cdot \beta = \beta^{-1} \mathbb{Q}(a_\beta) \beta = K.$$

This proves that the Rosati involution $\cdot^\dagger$ indeed induces the standard involution on $\text{Cent}^0(a)$, and the result follows by uniqueness of this standard involution (Proposition A.12). $\square$

Knowing the structure of the centralizer of a , we can show that there are no nonzero singular K -RM homomorphisms:

Corollary 4.10. *Every nonzero K -RM homomorphism is an isogeny.*

Proof. Let $\gamma: (g_1, a_1) \rightarrow (g_2, a_2)$ be a K -RM homomorphism. Applying the Skolem–Noether theorem (Proposition A.15) to the embeddings $K \hookrightarrow M_2(\mathcal{B}_{p,\infty})$ given by mapping the generator of R_K to a_i , $i = 1, 2$, we find an invertible matrix $\delta \in M_2(\mathcal{B}_{p,\infty})^\times$ such that $a_2 = \delta^{-1}a_1\delta$. Clearing denominators to assume $\delta \in M_2(\mathcal{O}_0)$, Lemma 4.5 hence shows that we have a K -RM isogeny⁸ $\delta: (g_2, a_2) \rightarrow (g_1, a_1)$, and $\delta\gamma \in \text{Cent}(a_1)$ is nonzero since δ is invertible. Moreover, $\text{Cent}^0(a_1) \cong \mathcal{B}_{p,\infty} \otimes K$ is a division algebra by Proposition 4.9 since K is a real quadratic field and $\mathcal{B}_{p,\infty}$ is ramified at ∞ (cf. [Voi21, Proposition 14.6.7]), so $\delta\gamma$ is invertible in $\text{Cent}^0(a_1) \subseteq M_2(\mathcal{B}_{p,\infty})$. Thus $\gamma \in M_2(\mathcal{B}_{p,\infty})^\times$, i.e. γ is an isogeny by Lemma 4.5. $\square$

As previously described in the geometric setting in Section 3.1 (cf. Lemma 3.3), we arrive at a notion of degree for K -linear isogenies:

Corollary 4.11. *Let $\gamma: (g_1, a_1) \rightarrow (g_2, a_2)$ be a K -RM isogeny. Then the map*

$$\tilde{\gamma} := g_1^{-1}\gamma^*g_2: (g_2, a_2) \rightarrow (g_1, a_1)$$

is a K -RM isogeny. Furthermore we have $\tilde{\gamma}\gamma \in R_{\mathbb{Q}(a_1)}^+$, $\gamma\tilde{\gamma} \in R_{\mathbb{Q}(a_2)}^+$, and, with respect to the RM embeddings induced from each a_i ,

$$\iota_{a_1}^{-1}(\tilde{\gamma}\gamma) = \iota_{a_2}^{-1}(\gamma\tilde{\gamma}).$$

Proof. In view of Lemma 4.5 we see immediately that $\tilde{\gamma}$ is indeed a K -RM isogeny; in particular, $\tilde{\gamma}\gamma$ is nonzero (as it is an isogeny). Now applying the Rosati involution induced by g_1 , we have

$$(\tilde{\gamma}\gamma)^\dagger = g_1^{-1}(\tilde{\gamma}\gamma)^*g_1 = g_1^{-1}\gamma^*(g_1^{-1}\gamma^*g_2)^*g_1 = g_1^{-1}\gamma^*g_2\gamma = \tilde{\gamma}\gamma,$$

and Proposition 4.9 yields $\tilde{\gamma}\gamma \in \mathbb{Q}(a_1)$. Furthermore $\tilde{\gamma}\gamma \in M_2(\mathcal{O}_0)$ is integral over $\mathbb{Z}$ by [Voi21, Corollary 10.3.3], which yields $\tilde{\gamma}\gamma \in R_{\mathbb{Q}(a_1)}$.

Next, let us show that $\tilde{\gamma}\gamma$ is totally positive: Since $\tilde{\gamma}\gamma \in R_{\mathbb{Q}(a_1)}$ is integral, we find $t, n \in \mathbb{Z}$ such that $(\tilde{\gamma}\gamma)^2 - t\tilde{\gamma}\gamma + n = 0$. To prove that $\tilde{\gamma}\gamma$ lies in $R_{\mathbb{Q}(a_1)}^+$, we need to show that t and n are both non-negative. By Lemma 4.8 we find $\beta_1, \beta_2 \in M_2(\mathcal{B}_{p,\infty})$ and $s_1, s_2 \in \mathbb{N}$ such that $s_i \cdot g_i = \beta_i^*\beta_i$. Setting $\delta := \beta_2\gamma\beta_1^{-1}$ and $s := s_1s_2^{-1}$, we obtain

$$\begin{aligned} s \cdot \delta^*\delta &= s_1s_2^{-1} \cdot \beta_1^{-*}\gamma^*\beta_2^*\beta_2\gamma\beta_1^{-1} = s_1\beta_1^{-*}\gamma^*g_2\gamma\beta_1^{-1} \\ &= s_1\beta_1 \cdot \beta_1^{-1}\beta_1^{-*}\gamma^*g_2\gamma \cdot \beta_1^{-1} = \beta_1g_1^{-1}\gamma^*g_2\gamma\beta_1^{-1} = \beta_1(\tilde{\gamma}\gamma)\beta_1^{-1}. \end{aligned}$$

Thus $s \cdot \delta^*\delta$ also vanishes at the polynomial $x^2 - tx + n$, and hence $\delta^*\delta$ satisfies

$$(\delta^*\delta)^2 - \frac{t}{s}(\delta^*\delta) + \frac{n}{s^2} = \frac{1}{s^2}((s \cdot \delta^*\delta)^2 - t(s \cdot \delta^*\delta) + n) = 0.$$

Via a straightforward calculation it now follows that $\frac{t}{s} \geq 0$ and $\frac{n}{s^2} \geq 0$, and in view of $s > 0$ we deduce that $\tilde{\gamma}\gamma$ is totally positive.

⁸ Alternatively we could have invoked the much stronger Theorem 3.10 here.

Due to $\tilde{\gamma} = \gamma$ we symmetrically get $\gamma\tilde{\gamma} \in R_{\mathbb{Q}(a_2)}^+$. Finally, since γ is an RM-isogeny, we have

$$\gamma\tilde{\gamma}\gamma = \gamma\iota_{a_1}(\iota_{a_1}^{-1}(\tilde{\gamma}\gamma)) = \iota_{a_2}(\iota_{a_1}^{-1}(\tilde{\gamma}\gamma))\gamma,$$

and canceling γ from the right yields the desired equality $\iota_{a_1}^{-1}(\tilde{\gamma}\gamma) = \iota_{a_2}^{-1}(\gamma\tilde{\gamma})$. $\square$

Definition 4.12. The K -degree of a K -RM isogeny $\gamma: (g_1, a_1) \rightarrow (g_2, a_2)$ is defined as $\deg_K^{g_1, g_2}(\gamma) := \iota_{a_1}^{-1}(\tilde{\gamma}\gamma) \in R_K^+$. For completeness (cf. Corollary 4.10) we set $\deg_K^{g_1, g_2}(0) := 0$. We omit the matrices g_1, g_2 in the exponent if they are clear from the context.

Note that, by definition, any K -RM homomorphism $\gamma: (g_1, a_1) \rightarrow (g_2, a_2)$ satisfies the equation

$$\gamma^* g_2 \gamma = g_1 \cdot \iota_{a_1}(\deg_K^{g_1, g_2}(\gamma)). \quad (4)$$

In particular, a K -RM isogeny is polarized if and only if its K -degree lies in $\mathbb{N}$ (cf. Remark 3.5), and solving the equation system (1) translates to the problem of finding a K -linear isogeny of ℓ -power K -degree:

Problem 4.13. *Given two K -RM pairs (g_1, a_1) and (g_2, a_2) , find a K -linear isogeny $\gamma \in \text{Hom}((g_1, a_1), (g_2, a_2))$ of K -degree $\deg_K^{g_1, g_2}(\gamma) = \ell^e$, where $\ell \in \mathbb{N}$ is a fixed prime number inert in K and such that $\ell \ll p$.*

While the definition of K -RM homomorphisms does not explicitly link them to the g -matrices of the domain and codomain, the K -linearity of the corresponding polarizations still imposes a strong restriction, leading to the degree equation (4). In fact, under our assumption that $\text{Cl}^+(K) = 1$, the real multiplication determines the g -matrix uniquely up to units in $R_K^\times$, as hinted at in Section 3.1.

Corollary 4.14. *Suppose that we have two K -RM pairs (g_1, a) and (g_2, a) with the same matrix $a \in M_2(\mathcal{O}_0)$. Then there is a $u \in R_K^\times$ such that $g_2 = \iota_a(u)^* g_1 \iota_a(u)$.*

Proof. Since both K -RM pairs have the same matrix a , the identity matrix defines an RM-isogeny $\text{Id}_2: (g_1, a) \rightarrow (g_2, a)$. From Corollary 4.11 we therefore deduce

$$R_K^+ \ni \deg_K^{g_1, g_2}(\text{Id}_2) = \iota_a^{-1}(g_1^{-1}g_2),$$

and analogously we obtain $\iota_a^{-1}(g_2^{-1}g_1) \in R_K^+$. Thus $\iota_a^{-1}(g_1^{-1}g_2) \in R_K^{\times, +}$, and due to Corollary 2.1 we find a $u \in R_K^\times$ such that $\iota_a(u)^2 = g_1^{-1}g_2$. Finally, this yields $g_2 = g_1 \cdot \iota_a(u) \cdot \iota_a(u) = \iota_a(u)^* \cdot g_1 \cdot \iota_a(u)$ since (g_1, a) is a K -RM pair. $\square$

Remark 4.15. Knowing that the real multiplication essentially determines the polarization on our K -superspecial surface, it is natural to ask, conversely, whether one can compute all real multiplications that turn a given superspecial surface into a K -superspecial surface. In Appendix D we discuss how, as long as d is sufficiently small, one can effectively enumerate all such real multiplications.

4.3 The Deuring correspondence with RM

In this section, we introduce the quaternion version of the path-finding problem (Problem 4.18), and in our main theorem (Theorem 4.20) we show that we can reduce Problem 4.13 to Problem 4.18. Table 1 contains a simple comparison of the quaternion language and the IKO framework, which summarizes relevant results from Section 4.2 and Section 4.3.

	Quaternion language	IKO framework
endomorphism algebra	$\mathcal{B}_{p,\infty} \otimes K$	$\text{Cent}^0(a)$
involution	standard involution $\alpha \mapsto \bar{\alpha}$	Rosati involution $a \mapsto a^\dagger := g^{-1}a^*g$
endomorphism rings	Eichler orders $\mathcal{R} \subseteq \mathcal{B}_{p,\infty} \otimes K$ of discriminant p	$\text{Cent}(a) = \text{Cent}^0(a) \cap M_2(\mathcal{O}_0)$
isogenies	left $\mathcal{R}$ -ideals	$\gamma \in M_2(\mathcal{O}_0)$ such that $\gamma a_1 = a_2 \gamma$

Table 1. Geometry/arithmetic objects in two algebraic languages.

Let (g_1, a_1) and (g_2, a_2) be K -RM pairs. We write $\text{Hom}((g_1, a_1), (g_2, a_2))$ for the set of K -RM homomorphisms from (g_1, a_1) to (g_2, a_2) . This Hom set has a natural structure of an R_K -module, via multiplication by $\iota_{a_1}(x)$ on the right or, equivalently, by $\iota_{a_2}(x)$ on the left, for any $x \in R_K$.

Proposition 4.16. Let (g, a) be a K -RM pair. Then

$$\text{Cent}(a) := \text{Cent}^0(a) \cap M_2(\mathcal{O}_0)$$

is the ring $\text{Hom}((g, a), (g, a))$ of K -linear endomorphisms, and it is an Eichler order of discriminant p in $\text{Cent}^0(a)$. Moreover, the reduced norm form of $\text{Cent}(a)$ coincides with the K -degree of RM-homomorphisms.

Proof. [Nic05, Theorem 2.5.27] shows that $\text{Cent}(a)$ is an Eichler order of discriminant p , and the other claims follow from Proposition 4.9 since, for $\gamma \in \text{Cent}(a)$, $\tilde{\gamma} = \gamma^\dagger$ is the conjugate of γ as a quaternion in $\text{Cent}^0(a)$. $\square$

If $\gamma \in \text{Hom}((g_1, a_1), (g_2, a_2))$ is nonzero, we set $I_\gamma := \text{Hom}((g_2, a_2), (g_1, a_1))\gamma$.

Lemma 4.17. With notations as above, I_γ is an integral left $\text{Cent}(a_1)$ -ideal of norm⁹ $\deg_K(\gamma)$.

Proof. This is analogous to [Nic05, Lemma 2.5.16]; while we make a different choice on sides, the proof may be adapted in a straightforward fashion. $\square$

⁹ As we assume that K has strict class number 1, we may always represent the norm (ideal) of a quaternion ideal by a totally positive algebraic integer; we refer to such an integer as the norm of the ideal, which is well-defined modulo totally positive units, i.e. as a class in $R_K^+/R_K^{+,\times}$.

We may now introduce the quaternion version of the pathfinding problem:

Problem 4.18. *Let I be an integral ideal in $\mathcal{B}_{p,\infty} \otimes K$ such that the left order of I is an Eichler order of discriminant p which contains $\mathbf{i}$ and $\mathbf{j}$. Compute $z \in I$ such that $\text{Nrd}(z)/N(I) = \ell^e$ for some $e \in \mathbb{N}$, where $\ell \in \mathbb{N}$ is a small prime inert in K such that $\ell \ll p$.*

Before we reduce Problem 4.13 to this problem, we observe that it is straightforward to compute a K -RM pair (g_0, a_0) such that $\text{Cent}(a_0)$ satisfies the hypothesis of Problem 4.18.

Lemma 4.19. For the real quadratic field $K = \mathbb{Q}(\sqrt{d})$ of strict class number 1, there is a K -RM pair (Id_2, a) , where $a \in M_2(\mathbb{Z})$ may be computed in polynomial time. Then, $\text{Cent}(a) = \mathcal{O}_0 \iota_a(R_K)$.

Proof. Once we have found $a \in M_2(\mathbb{Z})$, then $\text{Cent}_{M_2(\mathcal{B}_{p,\infty})}(M_2(\mathbb{Q})) = \mathcal{B}_{p,\infty} \cdot \text{Id}_2$ immediately shows that $\text{Cent}(a)$ contains $\mathbf{i} \cdot \text{Id}_2$ and $\mathbf{j} \cdot \text{Id}_2$, so that $\text{Cent}(a)$ has the correct shape (in view of Proposition 4.16).

If $d = 2$ we may choose $a = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, so let us assume $d > 2$; due to Corollary 2.1 we then know that d is a prime such that $d \equiv 1 \pmod{4}$.

By [Neu99, Theorem I.1.1] there thus exist $x, y \in \mathbb{Z}$ such that $d = x^2 + y^2$. Moreover, since d is odd, exactly one of x, y is odd. We assume, without loss of generality, that $2 \mid y$, and write $x = 2s + 1$ and $y = 2t$ with $s, t \in \mathbb{Z}$. Now we simply set

$$a = \begin{pmatrix} s+1 & t \\ t & -s \end{pmatrix} \in M_2(\mathbb{Z}),$$

and check that this satisfies the minimal polynomial of $\alpha_K = \frac{1+\sqrt{d}}{2}$. Indeed, a clearly has trace 1, and we further have

$$\det(a) = -\frac{1}{4}((2s)^2 + 4s + (2t)^2) = -\frac{1}{4}(x^2 - 1 + y^2) = \frac{1-d}{4}.$$

Finally, note that we can find the above decomposition of d as a sum of two squares in polynomial time with Cornacchia's algorithm since d is a prime. $\square$

Theorem 4.20. Problem 4.13 reduces to Problem 4.18 in polynomial time.

Proof. Let (g_1, a_1) and (g_2, a_2) , ℓ, e be as in Problem 4.13. We first show that we can compute an ideal I_γ whose left order contains $\mathbf{i}, \mathbf{j}$ which corresponds to some $\gamma \in \text{Hom}((g_1, a_1), (g_2, a_2))$: Without loss of generality we may assume that $\text{Cent}(a_1)$ contains $\mathbf{i}$ and $\mathbf{j}$, as otherwise we can apply Lemma 4.19 to compute a K -RM pair (g_0, a_0) with this property, solve Problem 4.13 twice and combine the solutions.

To compute one such ideal I_γ , we start with computing a basis of the space $\mathbb{Q} \cdot \text{Hom}((g_2, a_2), (g_1, a_1))$ by solving a system of linear equations. A $\mathbb{Z}$ -basis of $\text{Hom}((g_2, a_2), (g_1, a_1))$ may then be computed efficiently using [Mic08, Lemma 3.1]. Likewise, we may compute $\gamma \in \text{Hom}((g_1, a_1), (g_2, a_2))$ and deduce a basis of I_γ .

Now, solving Problem 4.18 gives $z \in I_\gamma$ such that $\deg_K(z) = \ell^e N(I_\gamma)$. We claim that $\delta = \gamma \tilde{z} \iota_{a_1}(\deg_K(\gamma))^{-1}$ is a solution to Problem 4.13.

By construction of I_γ , there exists a $\nu \in \text{Hom}((g_2, a_2), (g_1, a_1))$ such that $z = \nu\gamma$. By multiplicativity of the degree, $\deg_K(\nu) = \ell^e$. Then,

$$\tilde{z} = g_1^{-1} z^* g_1 = g_1^{-1} \gamma^* g_2 g_2^{-1} \nu^* g_1 = \tilde{\gamma} \tilde{\nu}.$$

It follows that $\gamma \tilde{z} = \gamma \tilde{\gamma} \tilde{\nu} = \iota_{a_2}(\deg_K(\gamma)) \tilde{\nu} = \tilde{\nu} \iota_{a_1}(\deg_K(\gamma))$. Therefore we have $\delta = \tilde{\nu} \in \text{Hom}((g_1, a_1), (g_2, a_2))$ and $\deg_K(\delta) = \deg_K(\nu) = \ell^e$. $\square$

5 Finding paths in the quaternion world: The RM-KLPT algorithm

This section is dedicated to solving Problem 4.18. Accordingly, we make the following assumptions (see also Section 2.4): K is a totally real quadratic field with trivial strict class group $\text{Cl}^+(K) = 1$, and p is an unramified prime such that $p \equiv 3 \pmod{4}$. Finally, $\mathcal{R}_0$ is an Eichler order of discriminant p in $\mathcal{B}_{p,\infty} \otimes K$ which contains $\mathbf{i}$ and $\mathbf{j}$ such that $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = -p$, and $\mathbf{ij} = -\mathbf{ji}$.

Let us first give the RM-KLPT algorithm. We note that the named subroutines used are described in more detail below. Both the subroutines and the structure of the algorithm are similar to those of the KLPT algorithm, as described in [DF+20].

Algorithm 1: RM-KLPT

Input: An integral left $\mathcal{R}_0$ -ideal I
Input: A prime number $\ell \in \mathbb{N}$ inert in K
Output: Some $z \in I$ such that $\text{Nrd}(z) = \ell^e N(I)$ for some $e \in \mathbb{N}$

```

1  $J, x \leftarrow \text{EquivalentPrimeIdeal}(I)$  ; //  $N_J = N(J)$ 
2  $e_0 \leftarrow \max(0, \lceil \log_\ell(p) + \log_\ell(\log(p)) - \log_\ell(N_{K/\mathbb{Q}}(N_J)) / 2 \rceil)$ ;
3  $\eta \leftarrow \text{RepresentAlgebraicInteger}(R_K, \ell^{e_0} N_J)$ ;
4  $C, D \leftarrow \text{IdealModConstraint}(J, \eta)$ ;
5  $\mu \leftarrow \text{StrongApproximation}_\ell(N_J, C, D, R_K)$ ; //  $\text{Nrd}(\mu) = \ell^{e_1}$ 
6 return  $\eta \mu x^{-1} N(I)$ 
```

Theorem 5.1. Assuming Heuristics 5.4, 5.5, 5.7, 5.8, 5.10, 5.13 and 5.14, Algorithm 1 is correct and runs in polynomial time. Assuming that d is constant, the input I lies in a uniformly random class of left $\mathcal{R}_0$ -ideals, and $\ell \ll p$, the output is a polarized RM-isogeny of expected degree $\ell^e = \tilde{\mathcal{O}}(p^3)$.

We will prove Theorem 5.1 after we describe all of its subroutines. Combining it with Theorem 4.20, we get

Corollary 5.2. *Let (g_1, a_1) and (g_2, a_2) be K -RM pairs, with K having strict class number 1, and let ℓ be a rational prime that is inert in K . Then an RM-isogeny from (g_1, a_1) to (g_2, a_2) of K -degree a power of ℓ may be computed in polynomial time assuming Heuristics 5.4, 5.5, 5.7, 5.8, 5.10, 5.13 and 5.14.*

Subroutines. We shall need the following subroutines, most of them analogous to those of the KLPT algorithm:

- EquivalentPrimeIdeal(I):** Given a fractional ideal I in $\mathcal{B}_{p,\infty} \otimes K$, computes an element $x \in I$ of reduced norm $N_I \cdot N_J$, with $N_J \in R_K^+$ a prime element. Outputs J, x , where $J = I \frac{\bar{x}}{N_I}$. See Section 5.1 for a detailed discussion.
- SumOfSquares(x):** Given a totally positive $x \in R_K^+$, returns $a, b \in R_K$ such that $a^2 + b^2 = x$, or $\perp$ if such a, b do not exist. See for instance [Mur+24, Algorithm 4.1] for a polynomial-time algorithm for this task.
- RepresentAlgebraicInteger(M):** Given a totally positive $M \in R_K^+$ lying in the norm image $\text{Nrd}(\mathcal{R}_0)$ of $\mathcal{R}_0$, output $x \in \mathcal{R}_0$ of norm M . See Section 5.2 for a detailed discussion.
- IdealModConstraint(I, β):** Given an ideal I of $\mathcal{B}_{p,\infty} \otimes K$ of prime norm $N_I \in R_K^+$ and some β in the left order of I , finds $C, D \in R_K$ such that $\beta(C\mathbf{j} + D\mathbf{k}) \in I$. This algorithm is completely analogous to its eponym from [DF+20], the computation happens in the finite residue field of N_I , and then some lifts C and D are chosen freely.
- StrongApproximation $_\ell(N, C, D)$:** Given a prime element $N \in R_K^+$, $C, D \in R_K$, find $\mu \in \mathcal{R}_0$ such that $\text{Nrd}(\mu)$ is a power of ℓ , and $\mu \equiv \lambda(C\mathbf{j} + D\mathbf{k}) \pmod{N\mathcal{R}_0}$ for some $\lambda \in R_K$. See Section 5.3 for a detailed discussion.

Proof (of Theorem 5.1). Algorithm 1 runs in polynomial time by Lemmas 5.6, 5.11 and 5.16 below.

After Line 1, we have $J = I \frac{\bar{x}}{N(I)}$, and $N_J = \text{Nrd}(x)/N(I)$ is prime. Line 2 computes e_0 such that $N_{K/\mathbb{Q}}(\ell^{e_0} N_J) > p^2(\log p)^2$, ensuring that Line 3 behaves correctly by Lemma 5.11. By construction of **IdealModConstraint** and **StrongApproximation**, we have $\eta\mu \in J$ and $\text{Nrd}(\eta\mu) = N_J \ell^{e_0+e_1}$.

It follows that $\eta\mu x^{-1}N(I)$ lies in I , has reduced norm $N(I)\ell^{e_0+e_1}$. That is, Algorithm 1 is correct.

It remains to estimate the size of the output. Let $\alpha = N_{K/\mathbb{Q}}(N_J)$. By construction, we have

$$\max(1, p \log(p)/\sqrt{\alpha}) \leq \ell^{e_0} \leq \ell \max(1, p \log(p)/\sqrt{\alpha}).$$

Combining Heuristic 5.7 and the assumption that $\ell \ll p$, the expectation of ℓ^{e_0} is asymptotically $\tilde{\mathbf{O}}(\sqrt{p}/\sqrt{d})$.

By Lemma 5.6, the expectation of α is $\mathbf{O}(dp)$. Then, the output μ on Line 5 has degree $\mathbf{O}(p\alpha^{\frac{3}{2}}d)$ by Lemma 5.16, and thus the final isogeny has degree $\tilde{\mathbf{O}}(p^3 d^2)$; as the size of d is assumed to be constant, we get an output of expected degree $\ell^e = \tilde{\mathbf{O}}(p^3)$. $\square$

Remark 5.3. A natural candidate for generalisation of Algorithm 1 is to accept as input totally positive prime elements $\ell \in R_K^+$ that are not inert rational primes. While most of the methods can be adapted in a straightforward manner, difficulties arise within the **StrongApproximation** subroutine. The crux of the matter is that for a general $\ell \in R_K^+$, the two real embeddings of ℓ^e become increasingly imbalanced in size as e grows. The estimates in Lemma 5.16 ensuring that $\ell^e - M$ is totally positive for $M \in R_K^+$ are then no longer valid.

Experimentally, we find that in such circumstances, Algorithm 1 may provide an output of size $\tilde{\mathbf{O}}(p^6)$ in reasonable time. However, it is likely that an apt modification of Algorithm 5 would reduce this bound.

5.1 Finding an equivalent prime ideal

This subroutine is a direct analogue of the subroutine of the same name in the original KLPT algorithm, except it must now be done over the real quadratic field K . We adopt a similar approach as for the rational version.

Algorithm 2: EquivalentPrimeIdeal

Input: I a fractional left $\mathcal{R}_0$ -ideal and a prime $\ell \in R_K$
Output: (J, x) , where $x \in I$ has norm $N(I)N_J$, with $N_J \in R_K$ prime and such that ℓ is not a square in $R_K/N_J R_K$, and $J = I^{\frac{\bar{x}}{N(I)}}$

- 1 Let L be the rank 8 $\mathbb{Z}$ -module I with quadratic form
 $q(x) = \text{tr}_{K/\mathbb{Q}}(\text{Nrd}(x)/N(I))$;
- 2 Let $x_1, \dots, x_8$ be an LLL-reduced basis of L ;
- 3 **for** $a_1, \dots, a_8$ in $\mathbb{Z} \cap [-1, 1]$ **do**
- 4 $x \leftarrow \sum_{i=1}^8 a_i x_i$;
- 5 **if** $N_J := \text{Nrd}(x)/N(I)$ is prime in R_K and ℓ is not a square mod N_J **then**
- 6 $J \leftarrow I^{\frac{\bar{x}}{N(I)}}$;
- 7 **return** (J, x)
- 8 **end**
- 9 **end**

Heuristic 5.4. Let I be an ideal in $\mathcal{B}_{p,\infty} \otimes K$ representing a uniformly randomly sampled left ideal class of a fixed Eichler order of discriminant p , and let ℓ be a prime in R_K . Let q be the quadratic form $x \mapsto \text{tr}_{K/\mathbb{Q}}(\text{Nrd}(x)/N(I))$ (independent of the choice of I within a left ideal class). Let $(x_1, \dots, x_8)$ be an LLL-reduced $\mathbb{Z}$ -basis of I with respect to q . Then, with overwhelming probability, there exists $e \in I$ of the form $e = \sum_{i=1}^8 e_i x_i$, with $|e_i| \leq 1$, such that $N = \text{Nrd}(e)/N(I)$ is a prime in R_K , and $(\frac{\ell}{N}) = -1$.

Heuristic 5.5. Let I, q and $x_1, \dots, x_8$ be as in Heuristic 5.4. Then, there exists a constant B , independent of p and d , such that for $1 \leq i \leq 8$, the expectation of $\frac{\max_{1 \leq j \leq 8} q(x_j)}{q(x_i)}$ is bounded from above by B .

Lemma 5.6. Algorithm 2 is correct and terminates in expected polynomial time. The expected size of $N_{K/\mathbb{Q}}(N(J))$ is asymptotically $\mathbf{O}(dp)$ for I lying in a uniformly random class of left ideals (with respect to a fixed Eichler order of discriminant p).

Proof. According to Proposition 4.16, the order $\text{Cent}(a) = \text{Cent}^0(a) \cap M_2(\mathcal{O}_0)$ has discriminant p . By Heuristic 5.4, the algorithm outputs a correct result. The search step takes a constant amount of tries and the LLL reduction may be done in polynomial time as the rank of the lattice is constant.

Since the order has discriminant p , the determinant of the Gram matrix associated to the norm form $\text{Nrd}(x)/N(I)$ is $p^2/16$. The Gram matrix associated to the quadratic form $q(x) := \text{tr}_{K/\mathbb{Q}}(\text{Nrd}(x)/N(I))$ on L as defined in Step 1 then has determinant $d^4(p^2/16)^2$. Since $(x_1, \dots, x_8)$ is an LLL-reduced basis, Heuristic 5.5 implies that the expectation of $\max_{1 \leq j \leq 8} q(x_j)$ is bounded from above by $2^{3/4} B^{7/8} d^{1/2} p^{1/2}$. It follows by construction that if e is the output of Algorithm 2 with input I , the expectation of $q(e)$ is $\mathbf{O}(d^{1/2} p^{1/2})$. Since the norm $\text{Nrd}(e)/N(I)$ is totally positive, we get

$$N_{K/\mathbb{Q}}(\text{Nrd}(e)/N(I)) \leq (\text{tr}_{K/\mathbb{Q}}(\text{Nrd}(e)/N(I)))^2.$$

It follows that $N_{K/\mathbb{Q}}(\text{Nrd}(e)/N(I))$ has expectation $\mathbf{O}(dp)$. $\square$

As we expect the norm of the ideal computed by Algorithm 2 to not have a large variance, and to never be larger than $p^2 \log(p)^2$, we state the following heuristic:

Heuristic 5.7. Let I be an ideal in $\mathcal{B}_{p,\infty} \otimes K$ representing a uniformly randomly sampled left ideal class of a fixed Eichler order of discriminant p . Then, the expectation of $\max(1, p(\log(p))/\sqrt{N_{K/\mathbb{Q}}(N_J)})$ is asymptotically $\tilde{\mathbf{O}}(\sqrt{p}/\sqrt{d})$.

5.2 Representing algebraic integers

Since we assume that $\mathcal{R}_0$ contains the usual quaternion basis, finding an element of norm $M \in R_K^+$ in $\mathcal{R}_0$ reduces to finding $b, r, s, t \in R_K$ such that

$$b^2 + r^2 + ps^2 + pt^2 = M.$$

In Algorithm 3, a crucial step is to sample points $(z_1, z_2) \in \mathbb{Z}^2$ contained in a parallelogram in $\mathbb{R}^2$, determined by the target norm $M := M_1 + \alpha_K M_2$, namely:

$$\begin{aligned} 0 &< z_1 + \alpha_K z_2 < M_1/p + \alpha_K M_2/p, \\ 0 &< z_1 + \bar{\alpha}_K z_2 < M_1/p + \bar{\alpha}_K M_2/p. \end{aligned} \tag{5}$$

Such sampling can be implemented by, for instance, computing a linear transformation T sending the parallelogram above to the unit square $S = [0, 1]^2$, and then sampling vectors in $[0, 1]^2 \cap T\mathbb{Z}^2$. We denote this sampling procedure by $\text{SampleParallelogram}(M)$, which returns a uniformly random pair (z_1, z_2) .

Algorithm 3: Sample_{s,t}

Input: $M \in R_K^+$ totally positive
Output: $s, t \in R_K$ such that $M - ps^2 - pt^2$ is totally positive

```

1  $z_1, z_2 \leftarrow \text{SampleParallelogram}(M);$ 
2  $z \leftarrow z_1 + z_2\alpha_K;$ 
3 if  $(z)$  is not a prime ideal in  $R_K$  then
4   | Go to Step 1;
5 end
6 if  $\left(\frac{-1}{(z)}\right) \neq 1$  then
7   | Go to Step 1;
8 end
9  $s, t \leftarrow \text{SumOfSquares}(z);$ 
10 return  $s, t$ 
```

Since $\text{Cl}(K) = 1$ by our assumption, R_K is a principal ideal domain. We introduce the following heuristic, which is an analogue of the assumption made in [Koh+14, Section 3.1] on integers represented by a quadratic form to have a cleaner runtime analysis of the algorithm.

Heuristic 5.8. Let $z := z_1 + z_2\alpha_K$ where $z_1, z_2 \leftarrow \text{SampleParallelogram}(M)$. The probability of an ideal (z) generated this way being a prime ideal in R_K is the same as for random ideals of the same norm. Among the ideals (z) that are prime, the probability of (z) satisfying $\left(\frac{-1}{(z)}\right) = 1$ is $\frac{1}{2}$.

Lemma 5.9. Let $M \in R_K^+$ be totally positive with $N_{K/\mathbb{Q}}(M) > cp^2$ for a small constant c that is determined by α_K . Algorithm 3 is correct and terminates in expected polynomial time.

Proof. Let z be as defined in Step 2. The parallelogram equations given by Equation (5) are equivalent to ensuring that z and $M - pz$ are both totally positive. The algorithm samples such z until z can be written as a sum of squares in R_K by enforcing that (z) is a prime ideal in R_K and that $\left(\frac{-1}{(z)}\right) = 1$. The correctness of Algorithm 3 is then clear.

Each of the steps in this algorithm can be done efficiently, and the main thing is to estimate the expected repetition of Step 1. By Landau's prime ideal theorem [Lan03], the probability of random ideals $\mathfrak{a} \subseteq R_K$ with $N_{K/\mathbb{Q}}(\mathfrak{a}) \leq N$ being prime can be estimated by $\frac{1}{N}$. By Heuristic 5.8, we can estimate the probability of (z) being a prime ideal by $\frac{1}{\log N_{K/\mathbb{Q}}(z)}$. Since $N_{K/\mathbb{Q}}(z) \leq N_{K/\mathbb{Q}}(M/p)$, this probability is bounded below by $\frac{1}{\log N_{K/\mathbb{Q}}(M/p)}$. Therefore, the expected repetition of Step 1 is less than $2 \log N_{K/\mathbb{Q}}(M/p)$. As long as the parallelogram defined by Equation (5) contains enough points in $\mathbb{Z}^2$, this algorithm will terminate in expected polynomial time. Since the parallelogram has area $\frac{N_{K/\mathbb{Q}}(M/p)}{\sqrt{d_K}}$, one needs to ensure that $\frac{N_{K/\mathbb{Q}}(M/p)}{2\sqrt{d_K}} > 2 \log N_{K/\mathbb{Q}}(M/p)$. This requires that $M > cp^2$ for some constant c depending on α_K . $\square$

Algorithm 4: RepresentAlgebraicInteger(M)

Input: $M \in R_K^+$ totally positive
Output: $x = b + r\mathbf{i} + s\mathbf{j} + t\mathbf{k}$ such that $b, r, s, t \in R_K$ and $\text{Nrd}(x) = M$
1 $s, t \leftarrow \text{Sample_s_t}(M)$;
2 $z' \leftarrow M - ps^2 - pt^2$;
3 **if** (z') is not a prime in R_K **then**
4 | Go to Step 1;
5 **end**
6 **if** $\left(\frac{-1}{(z')}$ $\neq 1$ **then**
7 | Go to Step 1;
8 **end**
9 $b, r \leftarrow \text{SumOfSquares}(z')$;
10 **return** $b + r\mathbf{i} + s\mathbf{j} + t\mathbf{k}$

We introduce a heuristic similar to Heuristic 5.8 for z' generated in Step 2 of Algorithm 4.

Heuristic 5.10. Let $z' := M - ps^2 - pt^2$ where $s, t \leftarrow \text{Sample_s_t}(M)$. The probability of ideals (z') generated this way being a prime ideal in R_K is the same as for random ideals of the same norm. Among the ideals (z') that are prime, the probability of (z') satisfying $\left(\frac{-1}{(z')}$ $= 1$ is $\frac{1}{2}$.

Lemma 5.11. Let $M \in R_K^+$ be totally positive with $N_{K/\mathbb{Q}}(M) > (\log^2 p)p^2$. Then Algorithm 4 is correct, and terminates in expected polynomial time.

Proof. The proof follows that of Lemma 5.9. The only difference lies in the estimation of the probability of ideals (z') being prime. Since $N_{K/\mathbb{Q}}(z') \leq N_{K/\mathbb{Q}}(M)$, by Heuristic 5.10, we can use $\frac{1}{\log N_{K/\mathbb{Q}}(M)}$ as a lower bound of this probability. This means that the expected repetition of Step 1 is $2 \log N_{K/\mathbb{Q}}(M)$. This requires that $\frac{N_{K/\mathbb{Q}}(M/p)}{2\alpha_K} > (2 \log N_{K/\mathbb{Q}}(M/p))(2 \log N_{K/\mathbb{Q}}(M))$; the condition we have on $N_{K/\mathbb{Q}}(M)$ ensures that this holds, and then the algorithm terminates in expected polynomial time. $\square$

5.3 Strong approximation by an element of ℓ -power norm

Our version of strong approximation over a real quadratic field is, again, very close to the version over the rational numbers. The only technical difficulty is adjusting the so-called Petit-Smith trick [DF+20, Remark 4] that is crucial in obtaining the $\tilde{\mathbf{O}}(p^3)$ bound in the original KLPT algorithm. We start by showing how a certain problem appearing in $\text{StrongApproximation}_\ell$ can be viewed as a closest vector problem (CVP):

Proposition 5.12. Assume that ℓ is a small rational prime integer and that we have $\lambda, C, D \in R_K$ such that $\ell^{e_1} - p(\lambda^2 C^2 + \lambda^2 D^2)$ is divisible by N . Then one can find a solution (s, t) of

$$\ell^{e_1} - p((\lambda C + Ns)^2 + (\lambda D + Nt)^2) \equiv 0 \pmod{N^2}$$

such that $\text{tr}_{K/\mathbb{Q}}((\lambda C + Ns)^2 + (\lambda D + Nt)^2)$ is minimal in polynomial time.

Proof. The equation $\ell^{e_1} - p((\lambda C + Ns)^2 + (\lambda D + Nt)^2) \equiv 0 \pmod{N^2}$ can be rewritten as $-p(2\lambda NsC + 2\lambda NtD) \equiv p\lambda^2 C^2 + p\lambda^2 D^2 - \ell^{e_1} \pmod{N^2}$. Since we assume that $\ell^{e_1} - p(\lambda^2 C^2 + \lambda^2 D^2)$ is divisible by N , there exists $B \in R_K$ such that $\frac{\ell^{e_1} - p(\lambda^2 C^2 + \lambda^2 D^2)}{N} = B$. Thus the equation

$$-p(2\lambda NsC + 2\lambda NtD) \equiv p\lambda^2 C^2 + p\lambda^2 D^2 - \ell^{e_1} \pmod{N^2}$$

can be rewritten as $-p(2\lambda sC + 2\lambda tD) \equiv B \pmod{N}$.

This is a linear equation in s, t so its solution set consists of the sum of a particular solution (s_0, t_0) and a solution (s_1, t_1) to the homogeneous equation $-p(2\lambda sC + 2\lambda tD) \equiv 0 \pmod{N}$. Note that the solution set (s_1, t_1) to the homogeneous equation forms a lattice L where elements in $(x, y) \in R_K^2$ are endowed with Euclidean norm $\sqrt{\text{tr}_{K/\mathbb{Q}}(x^2 + y^2)}$. Now observe that

$$(\lambda C + Ns)^2 + (\lambda D + Nt)^2 = (\lambda C + Ns_0 + Ns_1)^2 + (\lambda D + Nt_0 + Nt_1)^2,$$

as $(s, t) = (s_0 + s_1, t_0 + t_1)$. Hence the field trace of this quantity can be viewed as the square of the Euclidean distance from $(\lambda C + Ns_0, \lambda D + Nt_0)$ to $(-Ns_1, Nt_1)$. Minimizing this trace amounts to solving a closest vector problem for the lattice NL , which is a lattice of dimension 4. In such a low dimension, the CVP can be solved in polynomial time with the BKZ algorithm and Babai's rounding algorithm. $\square$

We now analyze the **StrongApproximation _{ℓ}** algorithm (Algorithm 5). To prove that it is correct and runs in polynomial time, we state two heuristics:

Heuristic 5.13. Assume that N is the norm of the ideal output by Algorithm 2 with input an ideal in $\mathcal{B}_{p,\infty} \otimes K$ representing a uniformly randomly sampled left ideal class of a fixed Eichler order of discriminant p , and that C and D are lifts of uniformly random elements of R_K/NR_K . Then, there exists a constant $B \in \mathbb{N}$ such that the first and last Minkowski minima m_1 and m_4 of the lattices encountered in Step 4 (i.e., the solution set to $-p(2\lambda NsC + 2\lambda NtD) \equiv 0 \pmod{N^2}$) satisfy

$$\frac{m_4}{m_1} \leq B.$$

Heuristic 5.14. If the input of Algorithm 5 is as in Heuristic 5.13, and M is sampled as in Line 4, the probability that (M) is a prime ideal in R_K is the same as for random ideals of the same norm. Among the ideals (M) that are prime, the probability of (M) satisfying $\left(\frac{-1}{(M)}\right) = 1$ is $\frac{1}{2}$.

Algorithm 5: StrongApproximation_ℓ

Input: A totally positive prime $N \in R_K^+$ with $N_{K/\mathbb{Q}}(N) = \alpha$, $C, D \in R_K$
Output: $\mu \in \mathcal{R}_0$ such that $\text{Nrd}(\mu) = \ell^{e_1}$ for some $e_1 \in \mathbb{N}$, and
 $\mu = \lambda(C\mathbf{j} + D\mathbf{k}) \pmod{N\mathcal{R}_0}$ for some $\lambda \in R_K$

- 1 Set $e_1 \in \mathbb{N}$ such that $\ell^{e_1} \geq p\alpha^{\frac{3}{2}}d$ and such that $\ell^{e_1}/p(C^2 + D^2)$ is a quadratic residue modulo N ;
- 2 Set $\lambda \in R_K/NR_K$ such that $\lambda^2 \equiv \ell^{e_1}/p(C^2 + D^2) \pmod{N}$;
- 3 **while** *True* **do**
- 4 Sample $s, t \in R_K$ as described in Proposition 5.12 such that
 $M := \ell^{e_1} - p((\lambda C + Ns)^2 + (\lambda D + Nt)^2) \equiv 0 \pmod{N^2}$;
- 5 **if** M is prime in R_K **then**
- 6 $S \leftarrow \text{SumOfSquares}(M/N^2)$;
- 7 **if** $S \neq \perp$ **then**
- 8 Sample $(b, r) \leftarrow S$;
- 9 **return** $\lambda(C\mathbf{j} + D\mathbf{k}) + N(b + r\mathbf{i} + s\mathbf{j} + t\mathbf{k})$
- 10 **end**
- 11 **end**
- 12 **end**

Remark 5.15. Heuristic 5.13 is needed as we would like to provide CVP bounds, which for a balanced lattice are close to the bound on the shortest vectors. However, if the lattice is very skewed, then CVP errors can be close to the second minima, and thus would provide a worse bound. This heuristic is implicitly present already in the original SQIsign when the Petit-Smith trick is applied [DF+20, Remark 4].

Lemma 5.16. Under Heuristics 5.13 and 5.14, Algorithm 5 is correct and terminates in expected polynomial time.

Proof. The proof is very similar to its rational counterpart in KLPT. What has to be checked is that the bound set in Step 1 is accurate. In order to not run into an infinite loop, we need to set bounds such that M , as defined in Step 4, is totally positive, since otherwise it can never be written as a sum of two squares. Once we ensure that M is totally positive, Heuristic 5.14 ensures that the number of loops is polynomial in $\log p$.

In order to show that the bound for ℓ^{e_1} is correct we have to calculate the determinant of the lattice L that appears in Proposition 5.12, which is the collection of (s, t) pairs satisfying

$$-p(2\lambda sC + 2\lambda tD) \equiv 0 \pmod{N},$$

endowed with the Euclidean metric $\sqrt{\text{tr}_{K/\mathbb{Q}}(x^2 + y^2)}$. By observing that for any choice of s there is a corresponding t , one has an R_K -module basis of the form $(1, u), (0, N)$, which implies that the determinant of L is αd^2 . Note that the actual CVP instance of Proposition 5.12 deals with the lattice NL , whose determinant then is $\alpha^3 d^2$.

By Heuristic 5.13, the CVP error can be bounded by the square root of the determinant (we have a dimension 4 lattice, but we care about the square distance), which shows that M will be totally positive with the provided choice of ℓ^{e_1} . $\square$

6 On the RM-CGL hash function

The algebraic description of K -superspecial abelian varieties through RM-pairs allows us to find paths in $\mathcal{G}_K(p, \mathfrak{l})$ using RM-KLPT; however, just as in the one-dimensional setting, it is unclear how to do so given only geometric representations of two arbitrary vertices. Nevertheless, we can still compute outgoing edges in $\mathcal{G}_K(p, \mathfrak{l})$ directly from a tuple (A, ι, λ) . In this section, we explain how to perform these computations concretely, and we build the RM-CGL hash-function.

Recall that $\mathcal{G}_K(p, \mathfrak{l})$ is an $(\ell^f + 1)$ -regular Ramanujan graph, where f is the inertia degree of $\mathfrak{l}$ over ℓ . Any graph with good expansion properties naturally indicates a hash function construction by taking seeded non-backtracking walks through the graph and outputting the final vertex.

Formally, let $\mathcal{V}$ denote the vertex set of $\mathcal{G}_K(p, \mathfrak{l})$ and let $v_0 \in \mathcal{V}$ be any starting vertex. At the first step, exclude one fixed outgoing edge from v_0 ; thereafter, exclude the dual of the edge just traversed. By fixing a deterministic rule labeling the remaining ℓ^f edges by $\{0, \dots, \ell^f - 1\}$,¹⁰ a message parsed as an ℓ^f -ary string $m = m_1 \cdots m_r$ then determines a non-backtracking walk

$$v_0 \xrightarrow{m_1} v_1 \xrightarrow{m_2} \cdots \xrightarrow{m_r} v_r.$$

The RM-CGL hash function is then defined as

$$H: \{0, \dots, \ell^f - 1\}^* \longrightarrow \mathcal{V}, \quad m = m_1 \cdots m_r \longmapsto v_r.$$

6.1 Implementing the RM-CGL hash function

To evaluate H in practice, we must choose suitable parameters, concretely specify the data representing vertices, and compute isogenies between them while retaining the real multiplication.

We first choose p to be coprime to d and ℓ , and also take ℓ to be inert in K , both for the stronger expansion discussed in Remark 3.11 and also so that we may utilize existing efficient (ℓ, ℓ) -isogeny algorithms described in [Dar+25b; FT19; LR16]. With this choice, the RM-CGL hash functions resembles the genus-2 hash function of Castryck, Decru, and Smith [CDS20], which similarly encodes messages as walks through the polarized $(2, 2)$ -isogeny graph and outputs invariants of the final PPAS. Our construction similarly uses (ℓ, ℓ) -isogenies, but each PPAS admits RM and restricts outgoing edges to those with R_K -stable kernels.

¹⁰ For example, order the edges lexicographically by their binary encodings.

Remark 6.1. In the unrestricted polarized (ℓ, ℓ) -isogeny graph, excluding dual edges does not prevent the kernel of the next isogeny from intersecting that of the preceding dual. This yields “bad extensions” from composite kernels isomorphic to $\mathbb{Z}/\ell^2\mathbb{Z} \times (\mathbb{Z}/\ell\mathbb{Z})^2$ and leads to trivial collisions, which is why Castryck, Decru, and Smith explicitly exclude them [CDS20, Section 7.1]. For consecutive K -linear isogenies $\varphi: A \rightarrow B$ and $\psi: B \rightarrow C$, however, $\ker \widehat{\varphi}$ and $\ker \psi$ are one-dimensional over $R_K/\ell R_K \cong \mathbb{F}_{\ell^2}$ in $B[\ell]$. Non-backtracking makes these lines distinct, hence their intersection is trivial and $\ker(\psi \circ \varphi) \cong (\mathbb{Z}/\ell^2\mathbb{Z})^2$, automatically excluding such bad extensions.

To concretely represent our vertices, we may use the same models for PPASs used in the unrestricted (ℓ, ℓ) -isogeny graph, together with data specifying the real multiplication. The embedding $\iota: R_K \hookrightarrow \text{End}(A)$ is determined by the single endomorphism $\sigma := \iota(\alpha_K)$, where $R_K = \mathbb{Z}[\alpha_K]$. Under our strict class number one assumption, $\alpha_K = (1 + \sqrt{d})/2$ when $d \neq 2$. Note that the map $\sigma \in \text{End}(A)$ is not a polarized N -isogeny for any positive integer N when $d \neq 2$.

In this context, an (ℓ, ℓ) -isogeny $\varphi: (A, \lambda) \rightarrow (A', \lambda')$, is compatible with the RM determined by σ and σ' precisely when $\sigma' \circ \varphi = \varphi \circ \sigma$. Computing σ' from φ and σ is a familiar problem in oriented supersingular isogeny graphs [Arp+23]; here, we first show that stability of $\ker \varphi$ under σ guarantees the existence of a unique compatible σ' .

Proposition 6.2. Let (A, ι, λ) be a K -superspecial surface with $\sigma = \iota(\alpha_K)$. If $\varphi: (A, \lambda) \rightarrow (A', \lambda')$ is a polarized (ℓ, ℓ) -isogeny with $\sigma(\ker \varphi) \subseteq \ker \varphi$, then there exists a unique embedding $\iota': R_K \hookrightarrow \text{End}(A')$ making (A', ι', λ') a K -superspecial surface and φ a K -linear isogeny.

Proof. Due to the stability condition $\sigma(\ker \varphi) \subseteq \ker \varphi$, the kernel of φ is contained in $\ker(\varphi \circ \sigma)$. By the universal property of isogenies, this map factors uniquely through φ , yielding a $\sigma' \in \text{End}(A')$ such that $\sigma' \circ \varphi = \varphi \circ \sigma$. It remains to show that $\alpha_K \mapsto \sigma'$ defines an embedding $\iota': R_K \hookrightarrow \text{End}(A')$ that is compatible with λ' .

Let $m(x)$ be the minimal polynomial of α_K . The identity $\sigma' \circ \varphi = \varphi \circ \sigma$ gives $m(\sigma') \circ \varphi = \varphi \circ m(\sigma) = 0$. Since φ is surjective, $m(\sigma') = 0$. Using that m is irreducible over $\mathbb{Q}$, the minimal polynomials of α_K and σ' agree, and so the assignment $\alpha_K \mapsto \sigma'$ indeed defines an embedding $\iota': R_K \hookrightarrow \text{End}(A')$.

Lastly, we have to show that ι' is R_K -equivariant, i.e. that $(\sigma')^\vee \circ \lambda' = \lambda' \circ \sigma'$. Since φ is a polarized and ι is R_K -equivariant, we have $\varphi^\vee \circ \lambda' \circ \varphi = \ell \lambda$ and $\sigma^\vee \circ \lambda = \lambda \circ \sigma$. Taking the dual of $\sigma' \circ \varphi = \varphi \circ \sigma$, we obtain

$$\varphi^\vee \circ ((\sigma')^\vee \circ \lambda') \circ \varphi = \sigma^\vee \circ (\ell \lambda) = (\ell \lambda) \circ \sigma = \varphi^\vee \circ (\lambda' \circ \sigma') \circ \varphi.$$

Canceling the isogenies $\varphi^\vee$ and φ then gives the desired compatibility and (A', ι', λ') defines a K -superspecial surface determined uniquely by σ' . $\square$

Proposition 6.2 shows that evaluating σ on $A[\ell]$ suffices to determine the kernels of K -linear (ℓ, ℓ) -isogenies. To enumerate all outgoing edges from a vertex, one can enumerate all $\ell^3 + \ell^2 + \ell + 1$ maximally isotropic subgroups G of $A[\ell]$ and restrict to the $\ell^2 + 1$ R_K -stable ones by checking $\sigma(G) \subseteq G$.

Remark 6.3. Filtering maximally isotropic subgroups for σ -stable ones only requires the action of σ on $A[\ell]$, rather than its evaluation on arbitrary points. For a walk of fixed length r , one can therefore begin with a basis of $A[\ell^r]$ and the action of σ on this basis, then transport both along the walk. Each ℓ -isogeny loses one level of ℓ -power torsion, leaving enough data to select the next kernel. Choosing p with $\ell^r \mid p+1$ makes this torsion rational. Although this approach may be more efficient for fixed-length walks, we instead retain data sufficient to evaluate σ on arbitrary points, allowing walks of arbitrary length.

To evaluate σ on arbitrary points, we cannot directly use the usual algorithms for polarized isogenies, since σ is not a polarized (N, N) -isogeny when $d \neq 2$. We instead work with the polarized d -isogeny $\tau := \iota(\sqrt{d})$, which determines σ through

$$\tau = 2\sigma - 1, \quad \sigma = \frac{1 + \tau}{2}$$

when $d \equiv 1 \pmod{4}$. This allows us to represent the RM data using polarized isogeny algorithms: given $P \in A(\mathbb{F}_{p^2})$, choose any Q with $[2]Q = P$ and compute

$$\sigma(P) = \sigma([2]Q) = Q + \tau(Q).$$

Thus, an RM vertex can be represented uniquely by (A, λ) together with a (d, d) -endomorphism τ .

The kernel of τ determines τ up to post-composition by polarized automorphism, but such an automorphism may not be K -linear. Hence, additional auxiliary data is needed to represent a vertex up to K -equivalence. For example, τ and $-\tau$ share the same kernel but determine the conjugate RM embeddings given by

$$\sigma = \iota\left(\frac{1+\sqrt{d}}{2}\right) \quad \text{and} \quad \sigma' = \iota\left(\frac{1-\sqrt{d}}{2}\right).$$

These represent the same RM vertex precisely when there is a polarized automorphism f of (A, λ) satisfying $f \circ \sigma = \sigma' \circ f$. We therefore retain auxiliary information alongside the kernel to resolve this ambiguity. The following proposition shows that the action of τ on $A[n]$ suffices, where $n \geq 3$ is any integer coprime to $d\ell p$.

Proposition 6.4. Let (A, ι, λ) be a K -superspecial surface, let $\tau = \iota(\sqrt{d})$, and let $n \geq 3$ be coprime to $d\ell p$. Then (A, ι, λ) is uniquely determined up to K -isomorphism by $(A, \lambda, \ker \tau, \tau|_{A[n]})$.

Proof. Suppose another RM embedding ι' on (A, λ) gives $\tau' = \iota'(\sqrt{d})$ with the same kernel and action on $A[n]$. As p is unramified in K , τ, τ' are separable polarized (d, d) -isogenies, so $\ker(\tau) = \ker(\tau')$ yields $\tau = u\tau'$ for some polarized automorphism u of (A, λ) .

Since n is coprime to d , the restriction of τ' to $A[n]$ is a bijection. Thus the equality $\tau|_{A[n]} = \tau'|_{A[n]}$ implies that $u|_{A[n]}$ is the identity. As $n \geq 3$ and p is coprime to n , [Mil08, Proposition I.14.4(b)] gives $u = [1]$. Hence $\tau = \tau'$, and therefore $\iota = \iota'$. $\square$

Proposition 6.4 shows that a vertex of $\mathcal{G}_K(p, \ell)$ can be represented by the tuple $(A, \lambda, \ker \tau, \tau|_{A[n]})$, for $n \geq 3$ coprime to $d\ell p$. However, this is just one representative of the K -equivalence class that defines the vertex, and the output of the RM-CGL function should ideally be invariant under K -equivalences. Thus, at the final step of the walk, one would like to compute invariants analogous to the j -invariant in dimension one. Such invariants are known as Gundlach invariants; for $K = \mathbb{Q}(\sqrt{5})$, explicit expressions as quotients of Hilbert modular forms are given in [MR20, Theorem A.9].

In our implementation, we instead obtain a unique output by enumerating polarized isomorphisms originating from (A, λ) , transporting RM data accordingly, and selecting the lexicographically smallest encoding. This yields a unique representative of the K -equivalence class reasonably quickly, without requiring an explicit conversion from our representative to the Gundlach invariants.

Our proof-of-concept theta-coordinate-based implementation for $K = \mathbb{Q}(\sqrt{5})$, $\ell = 2$, $p \approx 2^{256}$ and $n = 3$ hashes a length 388 4-ary string in about 40 seconds¹¹. For details on this implementation, see Appendix C.

6.2 An algebraic second preimage attack on RM-CGL hashing

We now leverage our RM-KLPT algorithm to break the second preimage resistance of the RM-CGL hash function if we know the endomorphism ring of the starting vertex, analogously to the one-dimensional case [Eis+20]. This is in contrast to the general KLPT² algorithm: While the latter also finds a chain of (ℓ, ℓ) -isogenies, the corresponding hash function [CDS20] requires the chain to compose to an (ℓ^e, ℓ^e) -isogeny to prevent trivial collisions coming from “bad extensions”. While the chains produced by KLPT² contain bad extensions with overwhelming probability [Cas+25, Section 5.4], non-backtracking walks in the RM isogeny graph automatically avoid them (see Remark 6.1).

Per the discussion in Remark 4.4, we assume that our endomorphism ring knowledge translates to knowledge of the corresponding K -RM pair (g, a) of the starting vertex. With this setup, we obtain the following result:

Corollary 6.5. *Under the heuristics of Theorem 5.1, the RM-CGL hash function is not second preimage resistant if the K -RM pair (g, a) of its starting vertex is known.*

Proof. Let (A, ι, λ) be a K -superspecial surface, and let

$$\varphi = \varphi_k \circ \cdots \circ \varphi_1 : (A, \iota, \lambda) \rightarrow (A_k, \iota_k, \lambda_k)$$

be the non-backtracking chain of polarized K -linear (ℓ, ℓ) -isogenies encoding a given message m , with ℓ inert in K as in Section 6. As discussed in [Cas+25, Section 5.3(ii)], our knowledge of g allows us to adapt the `IsogenyToMatrix` algorithm [Cas+25, Algorithm 6] to compute both the matrix $\gamma \in M_2(\mathcal{O}_0)$ representing the isogeny φ and the target g -matrix g_k corresponding to (A_k, λ_k) .

¹¹ Timed on an Apple M4 MacBook Pro using `rm.cgl.py` from our RM-CGL repository with default parameters.

Moreover, from the K -linearity we can directly compute $a_k = \gamma a \gamma^{-1}$ corresponding to the real multiplication ι_k on (A_k, λ_k) .

We now apply the reduction of Theorem 4.20 and our RM-KLPT algorithm (Algorithm 1), as in Corollary 5.2, with the additional restriction that **StrongApproximation** $_\ell$ (Algorithm 5) in Step 5 returns a μ such that its norm satisfies $\ell^{e_0} \cdot \text{Nrd}(\mu) = \ell^e$ with $e \not\equiv k \pmod{2}$; since $\text{Nrd}(\mu)$ only needs to be sufficiently large, this restriction is easily achievable. We therefore obtain a matrix $\gamma' \in M_2(\mathcal{O}_0)$ of K -degree ℓ^e , where $e \not\equiv k \pmod{2}$, encoding a polarized K -linear isogeny from (A, ι, λ) to $(A_k, \iota_k, \lambda_k)$.

As discussed in [Cas+25, Section 5.3(i)], we may now apply¹² the generalized **MatrixToIsogeny** algorithm [Cas+25, Algorithm 5] to translate γ' into a chain of polarized K -linear (ℓ, ℓ) -isogenies. Finally, we remove backtracking and call the resulting chain ψ . Each cancellation removes a factor of $[\ell]$, reducing the walk length by two without changing the endpoint. Thus ψ still has length of opposite parity to k , so it encodes a different message with the same hash value. $\square$

7 Future work

The one-dimensional Deuring correspondence plays a significant role in isogeny-based cryptography. It lies at the core of the SQIsign family of constructions, ranging from the original one-dimensional SQIsign [DF+20], to the newer variant SQIsignHD [Dar+24], and more recent two-dimensional approaches such as [Bas+25b; Nak+24].

With the RM-KLPT algorithm at hand, one natural direction is to construct an analogue of one-dimensional SQIsign in the RM setting. This, however, comes with several technical challenges. For instance, RM-KLPT would need to be generalized to finding paths between two random vertices, without requiring the path to pass through a distinguished starting vertex. In addition, an efficient ideal-to-isogeny algorithm would need to be developed, among other ingredients.

Another direction is to explore higher-dimensional variants of SQIsign, such as SQIsignHD, SQIsign2D-West, SQIsign2D-East. The core idea behind these constructions is the ability to represent a short one-dimensional isogeny by embedding it into an isogeny of higher dimension (typically two or four). In the RM setting, short isogenies between two vertices can likewise be found, for instance via the **EquivalentPrimeIdeal** algorithm (Algorithm 2). The challenge is then to embed such isogenies into higher-dimensional ones, ideally without exceeding dimension four.

We leave the investigation of SQIsign variants in the RM setting for future work. Beyond these natural SQIsign analogues, many other one-dimensional constructions may admit meaningful generalizations in this setting.

As our current techniques are limited to real quadratic fields of strict class number 1 and small discriminant, another natural direction for future work is to extend our computational framework to more general settings.

¹² This application requires the reduced norm of γ' in $M_2(\mathcal{O}_0)$ to be a square, which is satisfied since this reduced norm is exactly $N_{K/\mathbb{Q}}(\deg_K(\gamma')) = (\ell^e)^2$.

References

- [Arp+23] S. Arpin, M. Chen, K. E. Lauter, R. Scheidler, K. E. Stange, and H. T. N. Tran. “Orienteering with One Endomorphism”. In: *La Matematica* 2.3 (Sept. 2023), pp. 523–582. ISSN: 2730-9657.
- [Bas+26] A. Basso, G. Borin, W. Castryck, M. Corte-Real Santos, R. Invernizzi, A. Leroux, L. Maino, F. Vercauteren, and B. Wesolowski. *PRISM with a pinch of salt: Simple, Efficient and Strongly Unforgeable Signatures from Isogenies*. Cryptology ePrint Archive, Paper 2026/443. 2026.
- [Bas+25a] A. Basso, G. Borin, W. Castryck, M. C. Santos, R. Invernizzi, A. Leroux, L. Maino, F. Vercauteren, and B. Wesolowski. “PRISM: Simple and Compact Identification and Signatures from Large Prime Degree Isogenies”. In: *PKC 2025 Proceedings, Part III*. Vol. 15676. Lecture Notes in Computer Science. 2025, pp. 300–332.
- [Bas+25b] A. Basso, P. Dartois, L. De Feo, A. Leroux, L. Maino, G. Pope, D. Robert, and B. Wesolowski. “SQIsign2D–West: The Fast, the Small, and the Safer”. In: *Advances in Cryptology – ASIACRYPT 2024*. Ed. by K.-M. Chung and Y. Sasaki. Springer, Singapore, 2025, pp. 339–370. ISBN: 978-981-96-0891-1.
- [BS25] S. Boscardin and S. A. Spindler. *Exploring Kaneko’s bound: On multi-edges, loops and the diameter of the supersingular ℓ -isogeny graph*. Cryptology ePrint Archive, Paper 2025/1361. 2025.
- [Bro74] E. Brown. “Class numbers of real quadratic number fields”. In: *Transactions of the American Mathematical Society* 190 (1974), pp. 99–107. ISSN: 1088-6850.
- [CD23] W. Castryck and T. Decru. “An Efficient Key Recovery Attack on SIDH”. In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 423–447.
- [Cas+25] W. Castryck, T. Decru, P. Kutas, A. Laval, C. Petit, and Y. B. Ti. “KLPT²: Pathfinding in Dimension Two and Applications”. In: *Advances in Cryptology – CRYPTO 2025*. Ed. by Y. Tauman Kalai and S. F. Kamara. Cham: Springer Nature Switzerland, 2025, pp. 167–200.
- [CDS20] W. Castryck, T. Decru, and B. Smith. “Hash functions from superspecial genus-2 curves using Richelot isogenies”. In: *J. Math. Cryptol.* 14.1 (2020), pp. 268–292.
- [CGL09] D. X. Charles, E. Z. Goren, and K. E. Lauter. “Families of Ramanujan Graphs and Quaternion Algebras”. In: *CRM Proceedings and Lecture Notes*. Vol. 47. 2009.
- [CLG09] D. X. Charles, K. E. Lauter, and E. Z. Goren. “Cryptographic Hash Functions from Expander Graphs”. In: *Journal of Cryptology* 22.1 (2009), pp. 93–113.
- [Dar+25a] P. Dartois, J. K. Eriksen, T. B. Fouotsa, A. H. L. Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren, and B. Wesolowski.

- “PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies”. In: *CRYPTO 2025 Proceedings, Part I*. Vol. 16000. Lecture Notes in Computer Science. 2025, pp. 67–99.
- [Dar+24] P. Dartois, A. Leroux, D. Robert, and B. Wesolowski. “SQIsignHD: New Dimensions in Cryptography”. In: *Advances in Cryptology – EUROCRYPT 2024*. Ed. by M. Joye and G. Leander. Cham: Springer Nature Switzerland, 2024, pp. 3–32.
- [Dar+25b] P. Dartois, L. Maino, G. Pope, and D. Robert. “An Algorithmic Approach to $(2, 2)$ -Isogenies in the Theta Model and Applications to Isogeny-Based Cryptography”. In: *Advances in Cryptology – ASIACRYPT 2024*. Ed. by K.-M. Chung and Y. Sasaki. Singapore: Springer Nature Singapore, 2025, pp. 304–338.
- [DF+20] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. “SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies”. In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by S. Moriai and H. Wang. Springer, Cham, 2020, pp. 64–93. ISBN: 978-3-030-64837-4.
- [DR26] T. Decru and K. Reijnders. “Expander Properties of Superspecial Isogeny Digraphs with Level Structure”. In: *Advances in Cryptology – CRYPTO 2026*. Ed. by N. Heninger and M. Rosulek. Cham: Springer Nature Switzerland, 2026, pp. 478–505.
- [Eis+18] K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”. In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by J. B. Nielsen and V. Rijmen. Cham: Springer International Publishing, 2018, pp. 329–368.
- [Eis+20] K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, and J. Park. “Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs”. In: *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium*. Ed. by S. D. Galbraith. Vol. 4. Open Book Series. Berkeley, CA: Mathematical Sciences Publishers, 2020, pp. 215–232.
- [FS22] E. Florit and B. Smith. “Automorphisms and isogeny graphs of abelian varieties, with applications to the superspecial Richelot isogeny graph”. In: *Arithmetic, Geometry, Cryptography, and Coding theory 2021*. Vol. 779. Contemporary mathematics. American Mathematical Society, 2022, 103–132.
- [FT19] E. V. Flynn and Y. B. Ti. “Genus Two Isogeny Cryptography”. In: *PQCrypto 2019 Proceedings*. Vol. 11505. Lecture Notes in Computer Science. 2019, pp. 286–306.
- [Gha24] W. Gbantous. “Loops, multi-edges and collisions in supersingular isogeny graphs”. In: *Advances in Mathematics of Communications* 18(4) (2024), pp. 935–955.

- [IKO86] T. Ibukiyama, T. Katsura, and F. Oort. “Supersingular curves of genus two and class numbers”. In: *Compositio Mathematica* 57.2 (1986), pp. 127–152.
- [JZ26] B. W. Jordan and Y. Zaytman. “Isogeny graphs of superspecial abelian varieties and Brandt matrices”. In: *Journal of the Mathematical Society of Japan* (Mar. 2026), pp. 1–40.
- [Kan97] E. Kani. “The number of curves of genus two with elliptic differentials.” In: *Journal für die reine und angewandte Mathematik* 485 (1997), pp. 93–122.
- [Koh+14] D. Kohel, K. Lauter, C. Petit, and J.-P. Tignol. “On the quaternion ℓ -isogeny path problem”. In: *LMS Journal of Computation and Mathematics* 17.A (2014), 418–432.
- [KP22] P. Koymans and C. Pagano. “Higher genus theory”. In: *International Mathematics Research Notices* 2022.4 (Feb. 2022), pp. 2772–2823.
- [Lan03] E. Landau. “Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes”. In: *Mathematische Annalen* 56.4 (1903), pp. 645–670.
- [LTZ23] J. LeGrow, Y. B. Ti, and L. Zobernig. “Supersingular Non-Superspecial Abelian Surfaces in Cryptography”. In: *Transactions on Mathematical Cryptology* 3.2 (2023), pp. 11–23.
- [LR16] D. Lubicz and D. Robert. “Arithmetic on abelian and Kummer varieties”. In: *Finite Fields and Their Applications* 39 (2016), pp. 130–158. ISSN: 1071-5797.
- [LR22] D. Lubicz and D. Robert. “Fast change of level and applications to isogenies”. In: *Research in Number Theory* 9 (2022).
- [Mai+23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. “A Direct Key Recovery Attack on SIDH”. In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 448–471.
- [Mic08] D. Micciancio. “Efficient reductions among lattice problems”. In: *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA '08. USA: Society for Industrial and Applied Mathematics, 2008, 84–93.
- [MR20] E. Milio and D. Robert. “Modular polynomials on Hilbert surfaces”. In: *Journal of Number Theory* 216 (2020), pp. 403–459. ISSN: 0022-314X.
- [Mil08] J. S. Milne. *Abelian Varieties*. Course notes, version 2.0. 2008. Available at <https://www.jmilne.org/math/CourseNotes/AV.pdf>.
- [Mur+24] G. Mureau, A. Pellet-Mary, G. Pliatsok, and A. Wallet. “Cryptanalysis of Rank-2 Module-LIP in Totally Real Number Fields”. In: *Advances in Cryptology – EUROCRYPT 2024*. Ed. by M. Joye and G. Leander. Cham: Springer Nature Switzerland, 2024, pp. 226–255. ISBN: 978-3-031-58754-2.
- [Nak+24] K. Nakagawa, H. Onuki, W. Castryck, M. Chen, R. Invernizzi, G. Lorenzon, and F. Vercauteren. “SQIsign2D-East: A New Signature

- Scheme Using 2-Dimensional Isogenies”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part III*. Ed. by K. Chung and Y. Sasaki. Vol. 15486. Lecture Notes in Computer Science. Springer, 2024, pp. 272–303.
- [Neu99] J. Neukirch. *Algebraic Number Theory*. Trans. by N. Schappacher. Grundlehren der mathematischen Wissenschaften 322. Springer Berlin Heidelberg, 1999.
- [Nic05] M.-H. Nicole. “Superspecial abelian varieties, theta series and the Jacquet–Langlands correspondence”. PhD thesis. McGillUniversity, 2005.
- [PR23] A. Page and D. Robert. *Introducing Clapoti(s): Evaluating the isogeny class group action in polynomial time*. Cryptology ePrint Archive, Paper 2023/1766. 2023.
- [PRS26] A. Page, D. Robert, and J. Soumier. “On the Conversion of Module Representations for Higher Dimensional Supersingular Isogenies”. In: *Advances in Cryptology – CRYPTO 2026*. Ed. by N. Heninger and M. Rosulek. Cham: Springer Nature Switzerland, 2026, pp. 415–446.
- [Piz80] A. Pizer. “An algorithm for computing modular forms on $\Gamma_0(N)$ ”. In: *Journal of Algebra* 64.2 (1980), pp. 340–390. ISSN: 0021-8693.
- [Rob23] D. Robert. “Breaking SIDH in Polynomial Time”. In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 472–503.
- [Rob25] D. Robert. “On the Efficient Representation of Isogenies”. In: *Number-Theoretic Methods in Cryptology*. Ed. by A. Dabrowski, J. Pieprzyk, and J. Pomykała. Cham: Springer Nature Switzerland, 2025, pp. 3–84. ISBN: 978-3-031-82380-0.
- [Sage] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.8)*. <https://www.sagemath.org>. 2025.
- [Sar18] N. T. Sardari. “Diameter of Ramanujan Graphs and Random Cayley Graphs”. In: *Combinatorica* 39 (2018), pp. 427–446.
- [Shi79] T. Shioda. “Supersingular K3 surfaces”. In: *Algebraic Geometry. Summer Meeting, Copenhagen, August 7-12, 1978*. Ed. by K. Lønsted. Lecture Notes in Mathematics 732. Berlin, Heidelberg: Springer, 1979.
- [Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. English. 2nd. Vol. 106. Grad. Texts Math. Springer New York, NY, 2009. ISBN: 978-0-387-09493-9; 978-0-387-09494-6.
- [Tak18] K. Takashima. “Efficient Algorithms for Isogeny Sequences and Their Cryptographic Applications”. In: *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*. 2018, pp. 97–114.

- [Voi21] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics 288. Springer, Cham, 2021. ISBN: 978-3-030-56692-0.
- [Zag81] D. B. Zagier. *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*. German. Hochschultext. Springer-Verlag Berlin Heidelberg, 1981. ISBN: 978-3-540-10603-6.

A Further background

A.1 Superspecial abelian surfaces

In the following we fix a prime $p > 5$. We assume some familiarity with elliptic curves and isogenies over finite fields (see [Sil09] for the main definitions and results) as well as the definition of an abelian surface; note that we will only encounter abelian surfaces that are isomorphic to products of two elliptic curves.

An *isogeny* $\varphi: A_1 \rightarrow A_2$ between two abelian surfaces over $\mathbb{F}_{p^2}$ is a morphism of varieties inducing a surjective group homomorphism $A_1(\overline{\mathbb{F}_p}) \rightarrow A_2(\overline{\mathbb{F}_p})$ with finite kernel, and an *isomorphism* is an isogeny that admits an inverse isogeny under composition. An *endomorphism* of A is a morphism $A \rightarrow A$ of abelian surfaces¹³, and we write $\text{End}(A)$ for the ring of endomorphisms of A .

Definition A.1. A *superspecial abelian surface* is an abelian surface A over $\mathbb{F}_{p^2}$ such that A is isomorphic over $\overline{\mathbb{F}_p}$ to E_0^2 for some supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$.

The following result shows that the choice of the curve E_0 in the above definition does not matter; unfortunately, however, it also shows that we only have one isomorphism class of superspecial abelian surfaces.

Theorem A.2. (Deligne, [Shi79, Thm. 3.5]) For any supersingular elliptic curves E_1, E_2, E_3, E_4 over $\mathbb{F}_{p^2}$ there is an isomorphism $E_1 \times E_2 \cong E_3 \times E_4$.

To properly separate such surfaces into different isomorphism classes, one endows them with (*principal*) *polarizations*. For our purposes the following slightly imprecise definition will be sufficient, as we use the Ibukiyama–Katsura–Oort correspondence [IKO86] as described in [Cas+25] to translate the concept into a more palpable notion in Section 4.

Definition A.3. Let A be an abelian surface. A *polarization* $\lambda: A \rightarrow A^\vee$ is an isogeny that is induced by an ample divisor on A . If the degree of λ (as a morphism of surfaces) is equal to 1, the polarization λ is called *principal*, and we call the pair (A, λ) a *principally polarized abelian surface*, or *PPAS* for short.

We now restrict our attention to isomorphisms – and, more generally, to isogenies – that are compatible with polarizations:

Definition A.4. Let (A_1, λ_1) and (A_2, λ_2) be two PPASs. A *polarized isogeny* $\varphi: (A_1, \lambda_1) \rightarrow (A_2, \lambda_2)$ is an isogeny $\varphi: A_1 \rightarrow A_2$ such that there exists an integer $N \in \mathbb{N}$ satisfying

$$N\lambda_1 = \varphi^\vee \circ \lambda_2 \circ \varphi.$$

The integer N is called the *reduced degree* $\text{degrd}(\varphi) = N$ of φ , and we call φ an *N -isogeny*. If $N = 1$, φ is called an *isomorphism of PPASs*¹⁴.

¹³ The induced group homomorphism may fail to be surjective or of finite kernel.

¹⁴ In this case, φ is invertible and φ^{-1} is again a 1-isogeny.

Finally, let us consider the classification of isomorphism classes of superspecial principally polarized abelian surfaces. We can view the problem in two ways. First, the following result describes representatives of the isomorphism classes of superspecial PPASs, together with canonical principal polarizations for each representative:

Theorem A.5. ([Cas+25, Section 2.2], [CDS20, Proposition 1]) Every superspecial principally polarized abelian surface over $\mathbb{F}_{p^2}$ is either the product of two supersingular elliptic curves over $\mathbb{F}_{p^2}$, equipped with the product polarization, or the Jacobian of a genus-2 curve over $\mathbb{F}_{p^2}$, equipped with a canonical polarization coming from the Abel–Jacobi map. Moreover, there are $\Theta(p^2)$ different (polarized) products up to isomorphism, and $\Theta(p^3)$ different superspecial Jacobians.

The second approach is to relate everything back to a base point: Fix a supersingular elliptic curve E_0 , and let (A, λ) be a superspecial PPAS. By Definition A.1 and Theorem A.2, there exists an (unpolarized) isomorphism $\varphi: E_0^2 \rightarrow A$ of abelian surfaces. With this data, one can show that

$$\lambda' := \varphi^\vee \circ \lambda \circ \varphi$$

defines a principal polarization¹⁵ on E_0^2 , and φ now defines an isomorphism of PPASs $(E_0^2, \lambda') \rightarrow (A, \lambda)$. For this reason the classification of isomorphism classes of superspecial PPASs comes down to understanding the set $\text{PPol}(E_0^2)$ of principal polarizations on E_0^2 , as well as when two principal polarizations on E_0^2 define isomorphic PPASs. We will utilize this viewpoint from Section 4 onward.

A.2 Quaternion algebras

Let K be a field of characteristic different from 2. If $a, b \in K^\times$, we consider the K -algebra

$$\left(\frac{a, b}{K} \right) = K \oplus Ki \oplus Kj \oplus Kij$$

with multiplication defined by the following rules:

$$i^2 = a; \quad j^2 = b; \quad ij = -ji.$$

Definition A.6. A *quaternion algebra* over K is a K -algebra isomorphic to $\left(\frac{a, b}{K} \right)$ for some $a, b \in K^\times$.

Example A.7. The matrix algebra $M_2(K)$ is a quaternion algebra over K . Indeed, we get an isomorphism $M_2(K) \xrightarrow{\sim} \left(\frac{1, 1}{K} \right)$ from the following mapping:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mapsto i \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto j.$$

A quaternion algebra isomorphic to $M_2(K)$ is called *split*, and any non-split quaternion algebra is a division algebra.

¹⁵ If the ample divisor D on A induces λ , then the pullback of D along φ is an ample divisor on E_0^2 that induces λ' .

Observe that if L is a field extension of K , $\left(\frac{a,b}{K}\right) \otimes_K L \simeq \left(\frac{a,b}{L}\right)$. In particular, if $\mathcal{B}$ is a quaternion algebra over K and L is an extension of K , then $\mathcal{B}_L := \mathcal{B} \otimes_K L$ is a quaternion algebra over L .

Definition A.8. Let $\mathcal{B}$ be a quaternion K -algebra and let $\mathfrak{p}$ be a prime (finite or archimedean) of K . Then we say that $\mathcal{B}$ ramifies at $\mathfrak{p}$ if $\mathcal{B}_{K_{\mathfrak{p}}}$ is not split.

Example A.9. ([Piz80, Proposition 5.1]) Let p be a prime. The quaternion algebra $\mathcal{B}_{p,\infty}$ ubiquitous in the theory of superspecial abelian varieties is defined as the quaternion $\mathbb{Q}$ -algebra which ramifies at p and at ∞ . We have the following:

$$\begin{aligned} \mathcal{B}_{2,\infty} &\simeq \left(\frac{-1, -1}{\mathbb{Q}} \right) \\ \mathcal{B}_{p,\infty} &\simeq \left(\frac{-1, -p}{\mathbb{Q}} \right) && \text{if } p \equiv 3 \pmod{4} \\ \mathcal{B}_{p,\infty} &\simeq \left(\frac{-2, -p}{\mathbb{Q}} \right) && \text{if } p \equiv 5 \pmod{8} \\ \mathcal{B}_{p,\infty} &\simeq \left(\frac{-q, -p}{\mathbb{Q}} \right) && \text{if } p \equiv 1 \pmod{8} \end{aligned}$$

where, in the last case, $q \equiv 3 \pmod{4}$ and p is not a quadratic residue mod q .

Definition A.10. Let $\mathcal{A}$ be a K -algebra. An *involution* $\bar{\cdot}: \mathcal{A} \rightarrow \mathcal{A}$ is a K -linear map such that:

- $\bar{1} = 1$;
- $\bar{\alpha} = \alpha$ for $\alpha \in K$;
- $\overline{\beta\alpha} = \bar{\alpha}\bar{\beta}$ for $\alpha, \beta \in \mathcal{A}$.

An involution is further called *standard* if the following is true for all $\alpha \in \mathcal{A}$:

- $\alpha\bar{\alpha} \in K$.

Example A.11. The quaternion algebra $\left(\frac{a,b}{K}\right)$ admits a standard involution defined by $\bar{\mathbf{i}} = -\mathbf{i}$ and $\bar{\mathbf{j}} = -\mathbf{j}$.

Proposition A.12. ([Voi21, Sections 3.2, 3.4]) A quaternion algebra admits a unique standard involution, which is referred to as *conjugation*. In particular, such a standard involution is always of the form described in Example A.11.

Quaternion algebras are the degree 2 example of the larger class of central simple algebras:

Definition A.13. A K -algebra $\mathcal{A}$ is called *central simple* if it satisfies the following properties:

- $\mathcal{A}$ is central. That is, $\text{Cent}(\mathcal{A}) := \{\alpha \in \mathcal{A}: \alpha\beta = \beta\alpha \text{ for all } \beta \in \mathcal{A}\} = K$.
- $\mathcal{A}$ is simple. That is, the only two-sided ideals of $\mathcal{A}$ are $\mathcal{A}$ itself and (0) .

Example A.14. Let $\mathcal{B}$ be a quaternion algebra over K . Then for $g \in \mathbb{N}$, $M_g(\mathcal{B})$ is a central simple algebra.

Central simple algebras have a lot of strong properties, two of which are the following:

Proposition A.15. (The Skolem–Noether theorem, [Voi21, Thm. 7.7.1]) Let $\mathcal{A}$ be a simple K -algebra and let $\mathcal{B}$ be a central simple K -algebra. Suppose that $f, g: \mathcal{A} \rightarrow \mathcal{B}$ are (necessarily injective) homomorphisms. Then there exists $T \in \mathcal{B}^\times$ such that $f(\alpha) = T^{-1}g(\alpha)T$ for all $\alpha \in \mathcal{A}$.

Proposition A.16. (The double centralizer theorem, [Voi21, Prop. 7.7.8]) Let $\mathcal{B}$ be a central simple K -algebra and let $\mathcal{A}$ be a simple subalgebra of $\mathcal{B}$. We write

$$\text{Cent}_{\mathcal{B}}(\mathcal{A}) := \{\beta \in \mathcal{B}: \beta\alpha = \alpha\beta \text{ for all } \alpha \in \mathcal{A}\}$$

for the centralizer of $\mathcal{A}$ in $\mathcal{B}$. We then have the following:

1. $\text{Cent}_{\mathcal{B}}(\mathcal{A})$ is a simple K -algebra
2. $\dim_K(\mathcal{B}) = \dim_K(\mathcal{A}) \cdot \dim_K(\text{Cent}_{\mathcal{B}}(\mathcal{A}))$
3. $\text{Cent}_{\mathcal{B}}(\text{Cent}_{\mathcal{B}}(\mathcal{A})) = \mathcal{A}$
4. $\text{Cent}(\mathcal{A}) = \text{Cent}(\text{Cent}_{\mathcal{B}}(\mathcal{A}))$

A.3 Strict class groups

Let K be a number field. Recall that the *class group* $\text{Cl}(K)$ of K is defined as the quotient I_K/P_K of the group I_K of fractional ideals of K by the subgroup P_K of principal fractional ideals of K , i.e. the subgroup of fractional ideals of the form aR_K for some $a \in K^\times$.

Definition A.17. Let P_K^+ denote the subgroup of principal fractional ideals generated by *totally positive* elements, i.e. any $I \in P_K^+$ can be written as $I = a \cdot R_K$ for some $a \in K$ such that $\sigma(a) > 0$ for any real embedding $\sigma: K \hookrightarrow \mathbb{R}$. Then the quotient $\text{Cl}^+(K) := I_K/P_K^+$ is called the *strict class group* or *narrow class group* of K .

It is well-known that the class group of K is finite (see, for example, [Neu99, Theorem I.6.3]). Going through the definitions, one can derive from this also the finiteness of the strict class group via a well-known exact sequence. We denote by K^+ the totally positive elements in $K^\times$, and by $R_K^{\times,+}$ the totally positive elements in $R_K^\times$.

Proposition A.18. We have an exact sequence¹⁶

$$1 \rightarrow R_K^\times/R_K^{\times,+} \rightarrow K^\times/K^+ \rightarrow \text{Cl}^+(K) \rightarrow \text{Cl}(K) \rightarrow 1$$

where the first map is induced by the inclusion $R_K^\times \hookrightarrow K^\times$, the middle map by sending $a \in K^\times$ to the class of aR_K in $\text{Cl}^+(K)$, and the last map by identifying $\text{Cl}(K) = I_K/P_K \cong \text{Cl}^+(K)/(P_K/P_K^+)$ as a quotient of $\text{Cl}^+(K)$ according to the third isomorphism theorem. In particular, $\text{Cl}^+(K)$ is finite.

¹⁶ Meaning that at every group, the image of the incoming homomorphism is equal to the kernel of the next map.

Proof. It is clear that all maps are well-defined, that the first map is injective, and that the last map is surjective with kernel P_K/P_K^+ . Moreover, the assignment $a \mapsto aR_K$ clearly induces isomorphisms $P_K \cong K^\times/R_K^\times$ and $P_K^+ \cong K^+/R_K^{\times,+}$ since $R_K^{\times,+} = K^+ \cap R_K^\times$. From this we immediately see that $R_K^\times/R_K^{\times,+}$ is the kernel of the middle map $K^\times/K^+ \rightarrow \text{Cl}^+(K)$, and that the image of this middle map is P_K/P_K^+ , so the sequence is indeed exact.

Furthermore, note that both quotients $K^\times/K^+$ and $R_K^\times/R_K^{\times,+}$ are finite: Letting $\sigma_1, \dots, \sigma_r$ denote the real embeddings $\sigma_i: K \hookrightarrow \mathbb{R}$, we immediately see that K^+ is the kernel of the group homomorphism

$$K^\times \rightarrow (\mathbb{Z}/2\mathbb{Z})^r, a \mapsto (\text{sgn } \sigma_i(a))_{i=1}^r. \quad (6)$$

Thus K^+ has finite index in $K^\times$, and the finiteness of $\text{Cl}^+(K)$ follows from the finiteness of $\text{Cl}(K)$. $\square$

Definition A.19. The order of the strict class group $\text{Cl}^+(K)$ is called the *strict class number* of K .

From now on we restrict our attention to real quadratic fields $K = \mathbb{Q}(\sqrt{d})$, where $d > 1$ is a square-free integer. To limit the square-free d for which we can have strict class number 1, we use the following result on the 2-torsion of $\text{Cl}^+(K)$ that goes back to Gauss' genus theory.

Lemma A.20. ([KP22, Section 1], [Bro74, Section 2]) The 2-torsion of the strict class group $\text{Cl}^+(K)$ of $K = \mathbb{Q}(\sqrt{d})$ satisfies

$$\# \text{Cl}^+(K)[2] = 2^{\omega(d_K)-1}$$

where $\omega(d_K)$ denotes the number of distinct prime factors of d_K . In particular, the strict class number of K is odd if and only if d is a prime with $d \not\equiv 3 \pmod{4}$.

To close out this section, we now focus on the case of strict class number 1. Recall that, by Dirichlet's unit theorem [Neu99, Theorem I.7.4], we can find a *fundamental unit* $\varepsilon_K \in R_K^\times$ such that $R_K^\times = \pm \varepsilon_K^{\mathbb{Z}}$. With this preparation, we can describe when such fields have strict class number 1:

Corollary A.21. $K = \mathbb{Q}(\sqrt{d})$ has strict class number 1 if and only if it has class number 1 and the following equivalent conditions hold:

- (i) Every totally positive unit in $R_K^\times$ is a square in $R_K^\times$.
- (ii) The fundamental unit ε_K is neither totally positive nor totally negative.
- (iii) $N_{K/\mathbb{Q}}(\varepsilon_K) = -1$.

Moreover, in this case d is a prime with $d \not\equiv 3 \pmod{4}$, i.e. $d = 2$ or $d \equiv 1 \pmod{4}$.

Proof. Let $\sigma_1, \sigma_2: K \hookrightarrow \mathbb{R}$ be the real embeddings of K , and let us first argue the equivalence of the three statements: Since $N_{K/\mathbb{Q}}(\varepsilon_K) = \sigma_1(\varepsilon_K) \cdot \sigma_2(\varepsilon_K)$ and $|N_{K/\mathbb{Q}}(\varepsilon_K)| = 1$ (due to the integrality of ε_K), we immediately obtain the equivalence between (ii) and (iii).

Further, if (i) holds, then $R_K^{\times,+} = \varepsilon_K^{2\mathbb{Z}}$, and hence the totally negative units are given by $R_K^{\times,-} = -\varepsilon_K^{2\mathbb{Z}}$; thus $\varepsilon_K \notin \pm\varepsilon_K^{2\mathbb{Z}}$ is neither totally positive nor totally negative, i.e. claim (ii) holds.

Next, let us assume that (ii) holds; our goal is to show that (i) holds and that $\text{Cl}^+(K) = \{1\}$ if and only if $\text{Cl}(K) = \{1\}$. By assumption the four elements $\{\pm 1, \pm \varepsilon_K\} \subseteq R_K^\times$ show that both the sign homomorphism (6) and its restriction to $R_K^\times$ are surjective. As the respective kernels are K^+ and $R_K^{\times,+}$, we obtain

$$R_K^\times / R_K^{\times,+} \cong (\mathbb{Z}/2\mathbb{Z})^2 \cong K^\times / K^+,$$

and the exact sequence from Proposition A.18 shows that $\text{Cl}^+(K) \cong \text{Cl}(K)$. Furthermore we see that $R_K^{\times,+}$ has index 4 in $R_K^\times$; as the subgroup of squares $\varepsilon_K^{2\mathbb{Z}} = R_K^{\times 2} \subseteq R_K^{\times,+}$ also has index 4 in $R_K^\times$, we deduce claim (i).

Finally, the claim on the shape of d follows immediately from Lemma A.20 since 1 is odd. $\square$

B On RM isogeny graphs

In this section we provide a more thorough account of the RM isogeny graphs $\mathcal{G}_K(p, \mathfrak{l})$ introduced in Section 3.2.

B.1 Vertices, edges and the Ramanujan property

First we want to determine the number of vertices of $\mathcal{G}_K(p, \mathfrak{l})$, for which we need the following asymptotic for the *Dedekind zeta function* $\zeta_K(s)$ of K at $s = -1$. We provide a full proof at the end of this appendix (see Corollary B.15), after giving more background on this zeta function and its functional equation.

Lemma B.1. The Dedekind zeta function ζ_K of K satisfies $|\zeta_K(-1)| = \Theta(d^{3/2})$.

Proof sketch. The functional equation of ζ_K yields $\zeta_K(-1) = d_K^{3/2} \frac{1}{4\pi^4} \zeta_K(2)$, and from the definition and the absolute convergence of the infinite product representation of $\zeta_K(2)$ one can derive $1 \leq \zeta_K(2) \leq \zeta_{\mathbb{Q}}(2)^2 = \pi^4/36$. $\square$

With the more general analysis performed in [CGL09, Proposition 3.6] we can now immediately derive an asymptotic vertex count for $\mathcal{G}_K(p, \mathfrak{l})$; note that this asymptotic can be turned into explicit bounds through the proof of Corollary B.15.

Proposition B.2. The number n of vertices of $\mathcal{G}_K(p, \mathfrak{l})$ satisfies $n = \Theta(p^2 d^{3/2})$.

Proof. Specializing [CGL09, Proposition 3.6(2)] to dimension 2 gives

$$\frac{1}{2} \cdot |\zeta_K(-1)| \cdot (p-1)^2 \leq n \leq 120 \cdot |\zeta_K(-1)| \cdot (p^2 + 1),$$

and the claim follows from Lemma B.1. $\square$

Having understood the number of vertices better, let us turn our attention to the edges. As in the one-dimensional setting we are again dealing with regular graphs, meaning that all vertices have the same number of outgoing edges:

Proposition B.3. ([CGL09, Proposition 3.6(1)]) The graph $\mathcal{G}_K(p, \mathfrak{l})$ is regular of degree $\ell^f + 1$, with $f = f(\mathfrak{l}|\ell) \in \{1, 2\}$ the inertia degree of $\mathfrak{l}$ (over ℓ).

Proof sketch. The equivalence classes of $\mathfrak{l}$ -isogenies defined on a K -superspecial surface (A, ι, λ) correspond to the maximal cyclic subgroups of $A[\mathfrak{l}] \cong (R_K/\mathfrak{l})^2$. As $R_K/\mathfrak{l}$ is a finite field of order ℓ^f , the claim follows. $\square$

Now again let $f := f(\mathfrak{l}|\ell) \in \{1, 2\}$ denote the inertia degree of $\mathfrak{l}$ above ℓ . Furthermore let $\mathcal{V} = \{[A_1, \iota_1, \lambda_1], \dots, [A_n, \iota_n, \lambda_n]\}$ be the vertex set of $\mathcal{G}_K(p, \mathfrak{l})$. Define the quantities

$$w_i := |\text{End}_K(A_i, \iota_i, \lambda_i)^\times / \iota_i(R_K^\times)|,$$

where $\text{End}_K(A_i, \iota_i, \lambda_i)$ is the ring of K -linear morphisms $(A_i, \iota_i, \lambda_i) \rightarrow (A_i, \iota_i, \lambda_i)$. We obtain on $\mathbb{C}^\mathcal{V}$ an inner product via sesquilinear extension of

$$\langle [A_i, \iota_i, \lambda_i], [A_j, \iota_j, \lambda_j] \rangle := \frac{1}{w_j} \cdot \delta_{i,j}. \quad (7)$$

This inner product captures the failure of $\mathcal{G}_K(p, \mathfrak{l})$ to be undirected, i.e. the failure of its adjacency matrix to be symmetric, in the following sense:

Proposition B.4. ([CGL09, Proposition 3.2]) The quantities w_i are finite, and the adjacency matrix $\mathcal{A}$ of $\mathcal{G}_K(p, \mathfrak{l})$ is self-adjoint¹⁷ with respect to the weighted inner product (7). In particular, for any two vertices $x, y \in \mathcal{V}$ the distance from x to y coincides with the distance from y to x , and $\mathcal{A}$ is diagonalizable with real eigenvalues.

Proof. The first two claims are contained in [CGL09, Proposition 3.2], although we also provide a finiteness proof in Lemma B.7. From the self-adjointness we see that there is at least one edge $v_1 \rightarrow v_2$ in $\mathcal{G}_K(p, \mathfrak{l})$ if and only if there is at least one edge $v_2 \rightarrow v_1$ for any $v_1, v_2 \in \mathcal{V}$; lastly, the final claim is a direct consequence of the spectral theorem for self-adjoint matrices. $\square$

Importantly, the use of the weighted inner product (7) allows us to capture the Ramanujan property even in the directed case:

Theorem B.5. ([CGL09, Theorem 4.2]) The adjacency matrix $\mathcal{A}$ of $\mathcal{G}_K(p, \mathfrak{l})$ has the eigenvalue $\ell^f + 1$ with multiplicity one, and all other of its eigenvalues lie in the interval

$$\left[-2\sqrt{\ell^f}, 2\sqrt{\ell^f} \right].$$

In particular, $\mathcal{G}_K(p, \mathfrak{l})$ is connected.

¹⁷ As an operator $v \mapsto \mathcal{A} \cdot v$ on $\mathbb{C}^\mathcal{V} \cong \mathbb{C}^n$.

Comments on the proof. The proof of this statement in the undirected case is given in [CGL09, Theorem 4.2], and it also works in the directed case; the only change is that the adjacency matrix is not symmetric anymore (i.e. not self-adjoint with respect to the standard inner product), but this defect is fixed by instead considering the inner product (7) as in Proposition B.4. Note that the connectedness follows from the fact that the (out-)regularity degree has multiplicity one as an eigenvalue, since the connected components of the graph define linearly independent eigenvectors to this eigenvalue.

Since we defer the main work of the above proof to [CGL09, Theorem 4.2], let us emphasize also that this proof of Theorem B.5 requires that the real quadratic field K has strict class number 1.

B.2 Distances in RM isogeny graphs

The Ramanujan property of $\mathcal{G}_K(p, \mathfrak{l})$ gives us strong control over distances in this isogeny graph. This can be deduced from general spectral analysis of the graph's Laplacian, but the self-adjointness of $\mathcal{A}$ allows for a more direct spectral approach. Indeed, in view of Proposition B.4, the following result is a straightforward adaptation of [BS25, Theorem 31], where we write $w_x := w_i$ for a vertex $x = [A_i, \iota_i, \lambda_i] \in \mathcal{V}$.

Proposition B.6. Let $\mathcal{X}, \mathcal{Y} \subseteq \mathcal{V}$ be two sets of vertices in $\mathcal{G}_K(p, \mathfrak{l})$, and let $N \in \mathbb{N}_0$ such that there is no path of length at most N between any $x \in \mathcal{X}$ and any $y \in \mathcal{Y}$. Then

$$N < 2 \log_{\ell^f} \left(\frac{2}{\sqrt{c_{\mathcal{X}} c_{\mathcal{Y}}}} \cdot c_{\mathcal{V}} \right)$$

where, for any vertex set $\mathcal{Z} \subseteq \mathcal{V}$, $c_{\mathcal{Z}} := \sum_{z \in \mathcal{Z}} w_z^{-1}$ gives the weighted sum of vertices in $\mathcal{Z}$.

As the weighted vertex sums in the above result are somewhat opaque, we shed some light on them by bounding the weight factors w_i in the 2-dimensional setting:

Lemma B.7. For any K -superspecial surface (A, ι, λ) we have

$$1 \leq |\mathrm{End}_K(A, \iota, \lambda)^{\times} / \iota(R_K^{\times})| \leq |\mathrm{Aut}(A, \lambda) / \{\pm 1\}| \leq 36,$$

where $\mathrm{Aut}(A, \lambda)$ denotes the group of polarized isomorphisms $(A, \lambda) \rightarrow (A, \lambda)$.

Proof. According to Lemmas 3.3 and 3.6 the K -linear degree map $\deg_K^{\lambda, \lambda}$ induces a group homomorphism $\mathrm{End}_K(A, \iota, \lambda)^{\times} \rightarrow R_K^{\times, +}$. Moreover, for any $u \in R_K^{\times}$ we find $\deg_K^{\lambda, \lambda}(\iota(u)) = u^2$, so we further obtain a group homomorphism

$$\overline{\deg}_K: \mathrm{End}_K(A, \iota, \lambda)^{\times} / \iota(R_K^{\times}) \rightarrow R_K^{\times, +} / R_K^{\times 2}.$$

Now suppose that the class of a K -linear endomorphism $\varphi \in \mathrm{End}_K(A, \iota, \lambda)^{\times}$ lies in the kernel of the degree homomorphism $\overline{\deg}_K$.

Then we find a unit $u \in R_K^\times$ such that $\deg_K^{\lambda,\lambda}(\varphi) = u^2 = \deg_K^{\lambda,\lambda}(\iota(u))$, and the multiplicativity of the K -degree yields

$$\deg_K^{\lambda,\lambda}(\varphi \circ \iota(u^{-1})) = 1.$$

Therefore $\varphi \circ \iota(u^{-1})$ lies in the group $\text{Aut}_K(A, \iota, \lambda)$ of K -linear polarized automorphisms of (A, ι, λ) ; due to $\text{Aut}_K(A, \iota, \lambda) \cap \iota(R_K^\times) = \{\pm 1\}$ we thus see that the kernel of $\overline{\deg}_K$ is isomorphic to $\text{Aut}_K(A, \iota, \lambda)/\{\pm 1\}$ by the second isomorphism theorem.

Moreover, as we assume K to have strict class number 1, the codomain of $\overline{\deg}_K$ is trivial (cf. Corollary 2.1(i)), and thus the kernel embedding

$$\text{Aut}_K(A, \iota, \lambda)/\{\pm 1\} \hookrightarrow \text{End}_K(A, \iota, \lambda)^\times / \iota(R_K^\times)$$

is an isomorphism. Since $\text{Aut}_K(A, \iota, \lambda)/\{\pm 1\}$ embeds into $\text{Aut}(A, \lambda)/\{\pm 1\}$, we obtain the middle inequality.

Finally, the reduced automorphism group $\text{Aut}(A, \lambda)/\{\pm 1\}$ has order at most 36 according to [FS22, Figures 2&3] as we assume $p > 5$, which immediately gives the last inequality. $\square$

The above control on the weight factors now gives us a bound on the diameter of our graph:

Corollary B.8. *The diameter of $\mathcal{G}_K(p, \mathfrak{l})$ is at most*

$$2 \log_{\ell f}(n) + 2 \log_{\ell f}(72) + 1.$$

Proof. Let d be the diameter of $\mathcal{G}_K(p, \mathfrak{l})$, and pick two vertices $x, y \in \mathcal{V}$ at distance d . Then Proposition B.6 is applicable with $\mathcal{X} = \{x\}$, $\mathcal{Y} = \{y\}$ and $N = d - 1$, and the bound follows in view of Lemma B.7. $\square$

As in the case for general Ramanujan graphs, we do not expect the above diameter bound to be tight (see also the experiments in [Sar18]). Moreover, we can prove that at least ‘most’ vertex pairs are already at distance at most $\log_{\ell f}(n)$. To formalize this, we follow the same approach as [Sar18, Theorem 1.5] and [BS25, Corollary 34]:

Corollary B.9. *Let $\epsilon > 0$ and fix an integer $N \in \mathbb{N}$ with*

$$N \geq (1 + \epsilon) \log_{\ell f}(n).$$

Further pick a vertex x of $\mathcal{G}_K(p, \mathfrak{l})$ and let $\mathcal{V}(x, N) \subseteq \mathcal{V}$ denote the set of vertices in $\mathcal{G}_K(p, \mathfrak{l})$ to which there is no path from x of length at most N . Then

$$|\mathcal{V}(x, N)| < 144 \cdot w_x \cdot n^{1-\epsilon}$$

Proof. Applying Proposition B.6 with $\mathcal{X} = \{x\}$ and $\mathcal{Y} = \mathcal{V}(x, N)$ gives

$$(1 + \epsilon) \log_{\ell f}(n) \leq N < 2 \log_{\ell f} \left(\frac{2}{\sqrt{c_{\mathcal{X}} c_{\mathcal{Y}}}} \cdot n \right),$$

so taking powers to base ℓ^f yields $n^{1+\epsilon} < \frac{4}{c_{\mathcal{X}} c_{\mathcal{Y}}} n^2$. Rearranging for $c_{\mathcal{Y}} = c_{\mathcal{V}(x,N)}$ in view of Lemma B.7, we thus obtain

$$\frac{1}{36} \cdot |\mathcal{V}(x, N)| \leq c_{\mathcal{V}(x,N)} < 4 \cdot w_x \cdot n^{1-\epsilon}.$$

□

Remark B.10. Note that the estimate $|\mathcal{V}(x, N)| \leq 36 \cdot c_{\mathcal{V}(x,N)}$ above is quite crude, but sufficient for an asymptotic growth bound with respect to n . Also note that, except for the precise analysis of the weight factors w_i , all of the above results can easily be extended to arbitrary dimensions.

B.3 Avoiding loops and multi-edges in RM-isogeny graphs

Another issue that may potentially increase minimal distances between vertices in the graph is the existence of multi-edges and loops. For this reason we analyze how we may choose our parameters such that both loops and multi-edges do not occur in $\mathcal{G}_K(p, \ell)$; note that in dimension 1 this has been analyzed in [Gha24, Section 3] via the language of Brandt matrices, which would also be at our disposal as explained in [CGL09, Section 3.1].

Proposition B.11. Assume that we have $d > 16\ell^2$, and that d is a quadratic residue modulo p . Then the following holds:

- If $\left(\frac{t^2 - 4\ell}{p}\right) = 1$ for all $t \in \mathbb{Z} \cap [0, 2\sqrt{\ell})$, then $\mathcal{G}_K(p, \ell)$ has no loops.
- If $\left(\frac{t^2 - 4\ell^2}{p}\right) = 1$ for all $t \in \mathbb{Z} \cap [0, 2\ell)$, then $\mathcal{G}_K(p, \ell)$ has no multiple edges.

Proof. As explained in [CGL09, Subsection 4.3], a loop in $\mathcal{G}_K(p, \ell)$ would yield a CM extension $M = K(\sqrt{t^2 - 4\ell})$ for some $t \in R_K$, and a multi-edge would yield a CM extension $M = K(\sqrt{t^2 - 4\ell^2})$ for some $t \in R_K$. In particular, $t^2 - 4\ell$ resp. $t^2 - 4\ell^2$ would have to be totally negative, i.e. both embeddings $\sigma_1, \sigma_2: K \hookrightarrow \mathbb{R}$ would satisfy $\sigma_i(t)^2 < 4\ell^e$ for $i, e \in \{1, 2\}$.

Our goal now is to ensure that every $t \in R_K$ such that $\sigma_i(t^2) < 4\ell^2$ is an integer. To this end we write $t = a + b\sqrt{d}$, where $2a, 2b \in \mathbb{Z}$, to obtain

$$|2b|\sqrt{d} = |\sigma_1(t) - \sigma_2(t)| \leq |\sigma_1(t)| + |\sigma_2(t)| \leq 2 \cdot \sqrt{4\ell^2} = 4\ell.$$

Therefore the integer $2b$ has to satisfy $|2b| < (4\ell)/\sqrt{d} = \sqrt{16\ell^2/d} < 1$, and we obtain $t \in \mathbb{Q} \cap R_K = \mathbb{Z}$.

Finally, since we derived this CM extension from a K -linear endomorphism, it would have to embed into the quaternion algebra $\mathcal{B}_{p,\infty} \otimes K$ by Proposition 4.9. As p splits in $\mathbb{Q}(\sqrt{d})$ by the assumption that d is a quadratic residue modulo p , this would imply by [Voi21, Proposition 14.6.7] that a prime ideal above p in K does not split in $M = K(\sqrt{m})$. However, due to Galois theory this in turn forces p to be inert in $\mathbb{Q}(\sqrt{m})$, contradicting our respective assumption that m is a quadratic residue modulo p .

□

B.4 The Dedekind zeta function of a real quadratic field at $s = -1$

To close out this section, we provide some background on the Dedekind zeta function, with the goal to prove the asymptotic $|\zeta_K(-1)| = \Theta(d^{3/2})$ of Lemma B.1 for a totally real field $K = \mathbb{Q}(\sqrt{d})$. This background aims to be sufficient for our desired statement; a more comprehensive treatment of the occurring objects can be found in [Neu99, Sections VII.1-5] and [Zag81, Chapters 4, 11].

Definition B.12. ([Neu99, Def. VII.5.1 & Prop. VII.5.2], [Zag81, p.96]) The *Dedekind zeta function* ζ_K of a number field K is defined as

$$\zeta_K(s) := \sum_{\mathfrak{a}} [R_K : \mathfrak{a}]^{-s}$$

where the sum runs over all non-zero integral ideals $\mathfrak{a}$ of K . This expression converges absolutely in the half-space $\operatorname{Re}(s) > 1$ and uniformly in $\operatorname{Re}(s) \geq 1 + \delta$ for every $\delta > 0$. Moreover, it can also be expressed as the (absolutely convergent) infinite product

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - [R_K : \mathfrak{p}]^{-s}}$$

where the product runs over all prime ideals $\mathfrak{p}$ of R_K .

Importantly, the Dedekind zeta function ζ_K admits an analytic continuation to $\mathbb{C} \setminus \{1\}$, and it satisfies a functional equation. For our purposes, we do not need to know the precise definition of the analytic continuation, so the following result will be sufficient since the analytic continuation is unique by the identity theorem.

Proposition B.13. ([Neu99, Corollary VII.5.11]) The Dedekind zeta function ζ_K of a number field K has a unique analytic continuation to $\mathbb{C} \setminus \{1\}$, and for $s \notin \{0, 1\}$ this continuation (again denoted by ζ_K) satisfies the functional equation

$$\zeta_K(1-s) = |d_K|^{s-1/2} \left(\cos \frac{\pi s}{2}\right)^{r_1+r_2} \left(\sin \frac{\pi s}{2}\right)^{r_2} L_{\mathbb{C}}(s)^n \cdot \zeta_K(s)$$

where r_1 denotes the number of real embeddings $K \hookrightarrow \mathbb{R}$, $r_2 = \frac{1}{2}(n - r_1)$ denotes the number of pairs of (non-real) complex embeddings $K \hookrightarrow \mathbb{C}$, and

$$L_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s) \quad \text{where} \quad \Gamma(s) = \int_0^\infty e^{-y} y^{s-1} dy$$

denote the L -function of $\mathbb{C}$ and the Γ -function, respectively.

We specialize the above functional equation to a real quadratic field and $s = 2$ for our application:

Corollary B.14. *Let K be a real quadratic field. Then we have*

$$\zeta_K(-1) = \frac{1}{4\pi^4} d_K^{3/2} \cdot \zeta_K(2).$$

Proof. For the real quadratic field K we have $r_1 = n = 2$ and $r_2 = 0$, and integration by parts gives $\Gamma(2) = \int_0^\infty e^{-y} y \, dy = 1$. Thus we further obtain $L_{\mathbb{C}}(2) = \frac{1}{2\pi^2} \cdot \Gamma(2) = \frac{1}{2\pi^2}$, and the claim follows from Proposition B.13. $\square$

Arguably the most important example of a Dedekind zeta function is the *Riemann zeta function* $\zeta = \zeta_{\mathbb{Q}}$, which admits the infinite product expansion

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}} \quad (\operatorname{Re}(s) > 1).$$

Furthermore, it is well-known that

$$\zeta(2) = \sum_{n \geq 1} n^{-2} = \frac{\pi^2}{6},$$

which can easily be verified via contour integration and Cauchy's residue theorem (applied to the meromorphic function $f(z) = \pi \cot(\pi z) \cdot z^{-2}$), for example.

Having reduced the analysis of $\zeta_K(-1)$ to $\zeta_K(2)$, we can now work with the infinite series and product representations to obtain the desired asymptotic given in Lemma B.1:

Corollary B.15. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field (with $d \in \mathbb{N}$ square-free). Then $1 \leq \zeta_K(2) \leq \pi^4/36$ and*

$$\frac{1}{4\pi^4} d^{3/2} \leq \zeta_K(-1) \leq \frac{1}{18} d^{3/2}.$$

Proof. For the lower bound we use the power series expression to immediately get

$$\zeta_K(2) = \sum_{\mathfrak{a}} [R_K : \mathfrak{a}]^{-2} \geq [R_K : R_K]^{-2} = 1.$$

For the upper bound we make use of the absolute convergence of the infinite product representation of $\zeta_K(2)$: We write

$$\zeta_K(2) = \prod_p \prod_{\mathfrak{p} : \mathfrak{p}|p} \frac{1}{1 - [R_K : \mathfrak{p}]^{-2}}$$

by grouping for each prime $p \in \mathbb{N}$ the prime ideals $\mathfrak{p}$ of R_K that lie above p . Now, for each such prime ideal $\mathfrak{p} \mid p$, we have $[R_K : \mathfrak{p}] \geq p$, so $1 - [R_K : \mathfrak{p}]^{-2} \geq 1 - p^{-2}$. As there are at most two prime ideals lying above p , we obtain

$$\zeta_K(2) \leq \prod_p \left(\frac{1}{1 - p^{-2}} \right)^2 = \zeta(2)^2 = \pi^4/36.$$

Lastly, the bounds on $\zeta_K(-1)$ follow immediately from Corollary B.14 in view of $d \leq d_K \leq 4d$. $\square$

C RM graph traversal implementations

We describe a proof-of-concept implementation of the RM-CGL hash function and, more generally, traversal of the graph $\mathcal{G}_K(p, \ell)$ for $K = \mathbb{Q}(\sqrt{5})$ and $\ell = 2$. As described in Section 6, graph edges are computed with $(2, 2)$ -isogenies, while RM-data is represented by $(5, 5)$ -isogenies. Our implementation represents PPASs using level-two theta coordinates. We recall the necessary features as they arise and refer the reader to [Dar+25b; LR22] for details.

C.1 Vertex representation

Throughout the appendix, we write A for a principally polarized abelian surface, leaving its principal polarization implicit. Recall from Proposition 6.4 that, after writing

$$\tau = \iota(\sqrt{5}) = 2\sigma - 1, \quad \sigma = \iota\left(\frac{1 + \sqrt{5}}{2}\right),$$

a representative of an RM vertex may be encoded by $(A, \ker \tau, \tau|_{A[3]})$. We represent the three components of this tuple as follows:

- We represent A by its theta null point $O_A = \theta(0)$, where

$$\theta: A(\mathbb{F}_{p^2}) \longrightarrow \mathbb{P}^3(\mathbb{F}_{p^2})$$

is a level-two theta coordinate map, so that $\theta(P) = \theta(-P)$. When A is a Jacobian of a genus-2 curve, these coordinates determine any point up to sign. When A splits as a product $E_1 \times E_2$, the coordinates identify a pair (P, Q) with $(\pm P, \pm Q)$, with the signs chosen independently. To resolve this additional sign ambiguity, we also retain the elliptic factors and lift theta coordinates to pairs of elliptic points.

- We represent $\ker \tau = \langle P, Q \rangle \subseteq A[5]$ with $(\theta(P), \theta(Q), \theta(P + Q))$. Since theta coordinates do not distinguish a point from its negative, $\theta(P)$ and $\theta(Q)$ alone cannot distinguish $P + Q$ from $P - Q$. The auxiliary point $\theta(P + Q)$ records the relative signs of the generators and allows us to efficiently compute for any $a, b \in \mathbb{Z}$ the point $\theta(aP + bQ)$ using the differential-addition algorithms of [Dar+25b].
- We represent $\tau|_{A[3]}$ by an ordered basis (P_1, P_2, P_3, P_4) of $A[3]$ for which τ acts by the matrix introduced below in Equation (8). To use the same differential-addition algorithms, we store the theta coordinates of the four basis points and their six pairwise sums:

$$(\theta(P_i))_{1 \leq i \leq 4} \quad \text{and} \quad (\theta(P_i + P_j))_{1 \leq i < j \leq 4}.$$

Our implementation never has to check whether an arbitrary PPAS A admits RM by K . Instead, we begin at a vertex with known RM and push it through K -linear (ℓ, ℓ) -isogenies. We take our initial PPAS to be $A_0 = E_0^2$, where E_0 is any supersingular elliptic curve.

Under the identification $\text{End}(A_0) = M_2(\text{End}(E_0))$, specifying RM by a Rosati-symmetric endomorphism σ_0 with minimal polynomial $x^2 - x - 1$ amounts to finding a Hermitian 2×2 matrix over $\text{End}(E_0)$ with the same minimal polynomial. We take

$$\sigma_0 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \text{and thus} \quad \tau_0 = 2\sigma_0 - 1 = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Interestingly, because both matrices have integer entries, they can be represented using only multiplication maps on E_0 , without knowing $\text{End}(E_0)$.

In our chosen representation, the initial kernel is

$$\ker \tau_0 = \{(2P, P) : P \in E_0[5]\},$$

so it can be constructed directly from the 5-torsion of E_0 . To specify the action on 3-torsion, choose a symplectic basis (P_3, Q_3) of $E_0[3]$. With respect to the resulting symplectic basis $((P_3, 0), (0, P_3), (Q_3, 0), (0, Q_3))$ of $A_0[3]$, the action $\tau_0|_{A_0[3]}$ is given by

$$\begin{pmatrix} -1 & 2 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 2 & 1 \end{pmatrix}. \quad (8)$$

C.2 Recovering and evaluating RM

To compute the outgoing edges at a given vertex $(A, \ker \tau, \tau|_{A[3]})$, we enumerate all $(2, 2)$ -isogeny kernels $H \subseteq A[2]$ and retain those stable under σ . Although the vertex representation stores τ rather than σ , we compute the action of σ on $A[2]$ from τ as follows. For each generator $P \in H$, choose $Q \in A[4]$ such that $2Q = P$. Since $1 + \tau = 2\sigma$, we have

$$\sigma(P) = 2\sigma(Q) = Q + \tau(Q),$$

so H is stable under σ if and only if $Q + \tau(Q)$ lies in H for each generator P .

This test requires evaluating $\tau(Q)$, but our vertex representation stores the kernel of τ and its action on $A[3]$, rather than an explicit map. We begin by constructing the quotient $q: A \rightarrow B = A/G$ by the stored kernel $G = \ker \tau$; we then compute an isomorphism $u: B \rightarrow A$ to recover the endomorphism.

To compute this quotient, we use the kernel-sum formula of Lubicz and Robert [LR22, Corollary 4.5, Equation (9)] with $5 = 1 + 1 + 1 + 1 + 1$. We fix an affine lift $\tilde{O}_A \in \mathbb{F}_{p^2}^4$ of O_A . In our notation, the formula becomes

$$O_B \sim \tilde{O}_A^5 + 2 \sum_{T \in (G \setminus \{0\})/\{\pm 1\}} \tilde{R}_T^5,$$

where powers are taken coordinate-wise. In the terminology of Lubicz and Robert, $\tilde{R}_T$ is an *excellent lift* of $\theta(T)$ relative to $\tilde{O}_A$.

To compute the summands, choose arbitrary affine lifts $R_T \in \mathbb{F}_{p^2}^4$ and write $\tilde{R}_T = \lambda_T R_T$. Although λ_T may lie in an extension field, the formula only requires $c_T = \lambda_T^5$. Starting from R_T , we use differential addition to compute lifts R_{2T} and R_{3T} . Replacing R_T by $\lambda_T R_T$ scales these lifts by λ_T^4 and λ_T^9 , respectively. The excellent-lift condition requires the resulting lifts to agree, since $3T = -2T$ for $T \in A[5]$. Thus

$$\lambda_T^4 R_{2T} = \lambda_T^9 R_{3T}, \quad \text{so} \quad R_{2T} = c_T R_{3T}.$$

Thus, we obtain $\tilde{R}_T^5 = c_T R_T^5$ by computing c_T from the ratio of any non-zero coordinate of R_{2T} and R_{3T} . This avoids the need to compute λ_T , which would naively require taking fifth roots. We evaluate $q(X)$ similarly, using excellent lifts of the points $X + T$ for $T \in G$, compatible with the chosen lift of X and the kernel lifts.

Having constructed q , we now find a polarized isomorphism $u: B \rightarrow A$ such that $\tau = u \circ q$. The level-two theta structure identifies $A[2]$ with $\mathbb{F}_2^2 \times \mathbb{F}_2^2$; write $T_{a,b}^A$ for the point corresponding to (a, b) . The construction gives B a compatible theta structure, with $q(T_{a,b}^A) = T_{a,b}^B$. Since τ acts as the identity on $A[2]$, we require $u(T_{a,b}^B) = T_{a,b}^A$. With these labels fixed, the remaining ambiguity in the theta coordinates consists of coordinate permutations and sign changes arising from the choice of theta structure [LR22, Section 2.3]. Indexing the four theta coordinates by $k \in \mathbb{F}_2^2$, this leaves the sixteen coordinate transformations

$$(x_k)_k \mapsto ((-1)^{a \cdot k} x_{k+b})_k, \quad a, b \in \mathbb{F}_2^2.$$

We enumerate these transformations and select one sending O_B to O_A projectively. This determines the action of u in theta coordinates and allows us to evaluate $\theta(\tau(P))$ in the original theta coordinates.

C.3 Identifying outgoing RM-preserving isogenies

The recovered images $\theta(\tau(P))$, together with the kernel of τ , determine τ only up to sign. Distinguishing the two conjugate RM embeddings requires the stored action $\tau|_{A[3]}$, as discussed before Proposition 6.4. For identifying the σ -stable maximal isotropic subgroups of $A[2]$, however, either sign suffices: replacing τ by $-\tau$ replaces σ by $1 - \sigma$, and a subgroup is stable under one exactly when it is stable under the other.

To test whether $\sigma(P) \in H$, choose $Q \in A[4]$ such that $2Q = P$ and compute $\theta(Q + \tau(Q))$. Differential addition requires the auxiliary image $\theta(Q - \tau(Q))$, which is not stored. Instead, we use normal addition on the Kummer surface, based on the Riemann relations of Lubicz and Robert [LR22, Theorem 3.3], to recover the unordered pair

$$\{\theta(Q + \tau(Q)), \theta(Q - \tau(Q))\}.$$

Either image suffices for the membership test: since $\tau = 2\sigma - 1$ acts as the identity on $A[2]$, the two points differ by

$$(Q + \tau(Q)) - (Q - \tau(Q)) = 2\tau(Q) = \tau(P) = P \in H.$$

Thus, either both lie in H or neither does.

After selecting an outgoing isogeny $\varphi: A \rightarrow A'$, we evaluate it on the stored kernel generators, the 3-torsion basis, and their auxiliary sums. By Proposition 6.2, the induced endomorphism τ' satisfies $\tau' \circ \varphi = \varphi \circ \tau$, so

$$\ker \tau' = \varphi(\ker \tau), \quad P'_i = \varphi(P_i).$$

Since $\deg_K \varphi$ is coprime to 3 and 5, these images retain all the stored RM data, and the matrix of τ' with respect to the induced basis of $A'[3]$ again takes the shape given in Equation (8).

C.4 Unique K -equivalence representative

To obtain a unique representative of $(A, \ker \tau, \tau|_{A[3]})$, we enumerate all changes of level-two theta structure on A , giving polarized isomorphisms $u: A \rightarrow B$ in theta coordinates. After normalizing the first non-zero coordinate to be 1, we choose the lexicographically smallest resulting theta null point to define our canonical PPAS A_{can} . For every $u: A \rightarrow A_{\text{can}}$, we store $\theta(u(T))$ for all 25 points $T \in \ker \tau$, as well as

$$(\theta(u(T)), \theta(u(\tau(T))), \theta(u(T + \tau(T))))$$

for all 81 points $T \in A[3]$. Encoding these sets rather than their generators removes dependence on the chosen kernel generators and torsion basis; taking the lexicographically smallest encoding over these u removes the remaining choice of isomorphism. Together with A_{can} , this data determines the RM vertex by Proposition 6.4, and it is invariant under K -isomorphisms (and hence under K -equivalences, cf. Remark 3.9).

D Enumerating RM

In this section we show how to enumerate all vertices in the RM graph $\mathcal{G}_K(p, \ell)$ that correspond to a given PPAS (A, λ) . We assume the setup of Section 4, with $\mathcal{O}_0 = \text{End}(E_0)$ known and (A, λ) represented by its g -matrix $g \in \text{GL}_2(\mathcal{O}_0)$, which defines the Rosati involution $\cdot^\dagger$. In this section, we do not assume that $K = \mathbb{Q}(\sqrt{d})$ has strict class number 1.

Given the minimal polynomial $m(x) = x^2 - tx + n$ of the standard generator $\alpha_K \in \{\sqrt{d}, \frac{1+\sqrt{d}}{2}\}$ of R_K , our goal is to find all $a \in \text{Sym}^\dagger(M_2(\mathcal{O}_0))$ such that $m(a) = 0$. A matrix a satisfying these conditions exactly satisfies the definition for (g, a) to be an RM pair. In what follows, we explain in detail how to do this efficiently, and we provide an implementation¹⁸ in SageMath [Sage].

First, we compute a basis $\mathcal{O}_0 = \langle b_1, b_2, b_3, b_4 \rangle$, which yields a natural basis for the lattice of Hermitian matrices $\text{Sym}^*(M_2(\mathcal{O}_0))$:

$$B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad B_{i+2} = \begin{pmatrix} 0 & b_i \\ \overline{b_i} & 0 \end{pmatrix}, \quad i \in \{1, 2, 3, 4\}.$$

¹⁸ Available under <https://github.com/NicSwansonwaterloo/RMIsogenies>.

On this lattice, we define the inner product *twisted by g* by

$$\langle X, Y \rangle_g := \text{Trd}(\text{tr}(g^{-1}Xg^{-1}Y)) \in \mathbb{Q},$$

where Trd denotes the reduced trace in $\mathcal{B}_{p,\infty}$ and tr the matrix trace in $M_2(\mathcal{B}_{p,\infty})$. We also denote the associated norm as $\|X\|_g^2 = \langle X, X \rangle_g$. When $g = \text{Id}_2$, we drop the subscript notation and simply write $\|X\|$ and $\langle X, Y \rangle$, also using $\langle X, Y \rangle = \text{Trd}(\text{tr}(XY))$ as a bilinear form on all of $M_2(\mathcal{O}_0)$. We now show that we can work in the lattice $\text{Sym}^*(M_2(\mathcal{O}_0))$ with the twisted norm instead of working in $\text{Sym}^\dagger(M_2(\mathcal{O}_0))$:

Lemma D.1. The matrix g induces an inner-product-preserving isomorphism of lattices

$$(\text{Sym}^\dagger(M_2(\mathcal{O}_0)), \langle \cdot, \cdot \rangle) \rightarrow (\text{Sym}^*(M_2(\mathcal{O}_0)), \langle \cdot, \cdot \rangle_g), \quad X \mapsto gX.$$

Moreover, if $a \in \text{Sym}^\dagger(M_2(\mathcal{O}_0))$ has minimal polynomial $x^2 - tx + n$, then $b = ga \in \text{Sym}^*(M_2(\mathcal{O}_0))$ satisfies

$$\|b\|_g^2 = 2t^2 - 4n.$$

Proof. Since $g \in \text{GL}_2(\mathcal{O}_0)$ is invertible, we see that $X \mapsto gX$ defines a group automorphism of $(M_2(\mathcal{O}_0), +)$. Furthermore, for any matrix $X \in M_2(\mathcal{O}_0)$ we have

$$X^\dagger = g^{-1}X^*g = g^{-1}X^*g^* = g^{-1}(gX)^*$$

as g is Hermitian, so $X^\dagger = X$ happens if and only if $gX = (gX)^*$. We thus see that $X \mapsto gX$ induces the desired the group isomorphism, and from the definition of the inner products we directly see $\langle gX, gY \rangle_g = \langle X, Y \rangle$.

Finally, we can rearrange $a^2 - ta + nI = 0$ to $a^2 = ta - nI$, and thus obtain

$$\|b\|_g^2 = \|a\|^2 = \text{Trd}(\text{tr}(a^2)) = \text{Trd}(\text{tr}(ta - nI)) = \text{Trd}(t \text{tr}(a) - 2n) = 2t^2 - 4n$$

since $\text{Trd}(s) = 2s$ for $s \in \mathbb{Q}$ and $\text{Trd}(\text{tr}(a)) = 2t$, the latter following from the characteristic polynomial $(x^2 - tx + n)^2$ of a in $M_2(\mathcal{B}_{p,\infty})$. $\square$

This gives a computable norm form, Hermitian matrix, and target norm $N = 2t^2 - 4n$ for our lattice search, which can be computed solely from g and our real quadratic field $K = \mathbb{Q}(\sqrt{d})$. Since this is a 6-dimensional lattice, we can efficiently enumerate all short vectors using a reduced lattice basis. This approach requires $N = 2t^2 - 4n$ to be small, which is somewhat unavoidable since the number of RM any algorithm would need to return grows with d (cf. Proposition B.2).

Algorithm 6: Enumerate_{RM}

Input: $K = \mathbb{Q}(\sqrt{d})$ given by $d > 1$ square-free, a g -matrix in $M_2(\mathcal{O}_0)$,
and a basis $\{B_1, \dots, B_6\}$ of $\text{Sym}^*(M_2(\mathcal{O}_0))$.
Output: A list of all $a \in \text{Sym}^\dagger(M_2(\mathcal{O}_0))$ satisfying $a^2 - ta + nI = 0$.

- 1 Compute (t, n) from $d \bmod 4$ and set $N = 2t^2 - 4n$;
- 2 Turn $\{B_1, \dots, B_6\}$ into an LLL-reduced basis with respect to the
twisted inner product $\langle \cdot, \cdot \rangle_g$;
- 3 Enumerate all short vectors $v \in L$ with $\langle v, v \rangle_g \leq N + 1$ using the
LLL-reduced basis; retain those with $\langle v, v \rangle_g = N$;
- 4 Convert each retained $v = (c_1, \dots, c_6)$ back to a matrix
 $A = g^{-1} \sum_k c_k B_k$;
- 5 Filter out A with $A^2 - tA + nI \neq 0$;
- 6 **return** $\{A\}$.

The last step in our algorithm is to filter out equivalent RM endomorphisms so that we effectively return all vertices in the RM graph that correspond to g . Recall that two RM pairs (g, a_1) and (g, a_2) are isomorphic if and only if there exists $u \in \text{GL}_2(\mathcal{O}_0)$ such that

$$u^* g u = g, \quad u a_1 = a_2 u.$$

The first condition is equivalent to $u^\dagger u = I$, i.e. u is unitary with respect to $\cdot^\dagger$. Similarly, we enumerate unitary matrices by searching the full lattice $M_2(\mathcal{O}_0)$ for vectors satisfying $\text{Trd}(\text{tr}(u^\dagger u)) = 4$ and retaining those with $u^\dagger u = I$. We then take conjugacy orbits of the output of Algorithm 6 under these matrices.

Example D.2. For any $p \equiv 3 \bmod 4$, and $E_0 : y^2 = x^3 + x$, the following table represents all possible RM by $K = \mathbb{Q}(\sqrt{d})$ that (E_0^2, λ_0) admits up to K -equivalence. As is standard, we let $\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ denote the non-trivial automorphism and $\pi : (x, y) \mapsto (x^p, y^p)$ the Frobenius endomorphism of E_0 .

– $d = 3 :$

$$\begin{bmatrix} 1 & -1 - \iota \\ -1 + \iota & -1 \end{bmatrix}$$

– $d = 5 :$

$$\begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$$

– $d = 29 :$

$$\begin{bmatrix} -1 & 1 + 2\iota \\ 1 - 2\iota & 2 \end{bmatrix}, \begin{bmatrix} 2 & -1 - 2\iota \\ -1 + 2\iota & -1 \end{bmatrix}, \begin{bmatrix} 2 & \iota \\ -\iota & 3 \end{bmatrix}.$$