INFINITELY MANY SUPERSINGULAR PRIMES FOR SOME MUMFORD'S ABELIAN FOURFOLDS

FANGU CHEN
fangu@berkeley.edu

Abstract. Elkies ([Elk87, Elk89]) proved the infinitude of supersingular primes for elliptic curves over real number fields. We generalize Elkies' result to some abelian fourfolds in Mumford's families ([Mum69, §4]), and more generally, to certain families of Kuga-Satake abelian varieties. The proof relies on the study of local deformation spaces at closed points of the integral model of a Hodge-type Shimura variety, based on [MP16], and on the analysis of real points of a Shimura curve, based on [Shi75].

1. Introduction

1.1. **Background.** Serre conjectured that an abelian variety defined over a number field K has ordinary reduction at a density one set of primes up to a finite extension of K, and proved the conjecture in the case of elliptic curves ([Ser81]). Katz and Ogus proved Serre's conjecture in the case of abelian surfaces ([DMOS82, pp. 370-372]). Recently, Hui [Hui25] proved that a non-CM abelian variety over a number field has supersingular reduction at a density zero of primes.

A natural question is whether the density zero set of supersingular primes is finite or infinite. In [Elk87, Elk89], Elkies proved that an elliptic curve defined over a number field with at least one real embedding has infinitely many primes of supersingular reduction. This result has since been generalized to various families of abelian varieties ([Jao03], [Sad04], [BG08], [LMPT]). In all previously known cases, the moduli variety is a Shimura curve of PEL type. In this paper, we extend Elkies' theorem to certain families of abelian varieties parametrized by Shimura curves of Hodge type, including families of abelian fourfolds of Mumford's type in [Mum69], which are the first examples of Shimura varieties of Hodge type but not of PEL type.

1.2. **The main result.** The main result of this paper concerns certain families of Kuga-Satake abelian varieties constructed from K3-type Hodge structures with real multiplication by F on the trace zero part of a quaternion algebra over F.

Theorem 1.1. *Let F be a totally real number field with narrow class number 1 and B be a quaternion algebra over F unramified at all finite places and exactly one of the real places of F. Let $\mathcal{O}$ be a maximal order of B and $\mathcal{O}^1$ be the group of units of $\mathcal{O}$ of reduced norm 1. Let $\mathcal{H}$ be the upper half plane, and suppose the canonical model of the Shimura curve $\mathcal{O}^1\backslash\mathcal{H}$ is isomorphic to $\mathbb{P}^1_F$. Assume*

(1) $n := [F : \mathbb{Q}]$ is odd; [1]
(2) 2 is inert in F;
(3) $F(\sqrt{-\epsilon_i})$ has class number 1, where ϵ_i is a unit of F that is negative at exactly one of the real place $\rho_i : F \hookrightarrow \mathbb{R}$;
(4) $F(\sqrt{-\epsilon_1}, \ldots, \sqrt{-\epsilon_n})$ has class number 1.

Let A be an abelian variety parametrized by the Hodge type Shimura datum (G, X) (see Section 2.1.2). Suppose the field of moduli of A is in an odd-degree extension of the field of moduli of the elliptic point of order 2,[2] *then A has supersingular reduction at infinitely many primes.*

[1] This follows immediately from our assumption on B. In the future, we may consider cases where B is ramified at some finite places.

[2] The condition that B is unramified at all finite places implies the existence of an elliptic point of order 2. When B is ramified at some finite place, analogous points may still exist based on the geometry of the corresponding Shimura curve.

Remark 1.2. The Shimura curve has good reduction everywhere. Further work is required to remove the assumption that the quaternion algebra is unramified at all finite places and $[F:\mathbb{Q}]$ is odd. The remaining assumptions are technical conditions and will be explained in section 1.4.

When $[F:\mathbb{Q}]=3$, Galluzzi [Gal00] showed that the abelian variety obtained via Kuga-Satake construction is isogenous to powers of abelian fourfold of Mumford's type.

Theorem 1.3. *Let F be a totally real cubic number field with* $\mathrm{disc}(F)\in\{49,81,169,321,361,473,785,993\}$ *and B be a quaternion algebra over F unramified at all finite places and exactly one of the real places of F. Let X be an abelian fourfold in the one-dimensional family defined in* [Mum69, §4] *by B. Suppose X has field of moduli F, then X has supersingular reduction at infinitely many primes.*

More examples satisfying all the assumptions of Theorem 1.1 can be found in Example 7.3.

1.3. **Related works and heuristics.** Elkies' result has been generalized to some families of abelian surfaces with quaternionic multiplication (see [BG08],[Jao03] for the case of discriminant 6, and [Sad04] for the case of discriminant $21, 33$), and some families of abelian fourfolds by work of Li, Mantovan, Pries and Tang. In all known cases, the coarse moduli variety is isomorphic to $\mathbb{P}^1$. Heuristically, following the philosophy of [ST18], for an abelian variety A on a Shimura variety S, the probability that A mod $\mathfrak{p}$ lies in the Hecke orbit of a codimension d subvariety $V\subset S_{\mathbb{F}_\mathfrak{p}}$ is roughly $(N\mathfrak{p})^{-d/2}$. Since

$$\sum_{p\le x} p^{-d/2}\sim\begin{cases}\sqrt{x}/\log x & d=1,\\ \log\log x & d=2,\\ 1 & d\ge 3,\end{cases}$$

we expect infinitely many supersingular primes when the Shimura variety has dimension 1 and its supersingular locus has codimension 1.

There are similar results showing that certain density zero set of primes related to the reduction of abelian varieties is infinite, as in the case of split reduction of abelian surfaces ([ST20, SSTT22, Tay25]), and geometrically isogenous reductions of non-isogenous elliptic curves ([Cha18]). The proofs of these theorems rely on the intersection of the given arithmetic 1-cycle with the reductions of divisors defined in characteristic 0. By contrast, the supersingular locus varies from prime to prime. We follow Elkies' strategy to use CM cycles, which have supersingular reduction at roughly half of the primes, and we need to detect whether the intersection occurs at the supersingular primes. For this, we work with $\mathbb{P}^1$, where the intersection theory is especially simple.

1.4. **The strategy of the proof.** Given an elliptic curve E defined over a number field, Elkies' strategy to construct a new supersingular prime $\mathfrak{p}$ for E is to find a CM cycle whose $\overline{\mathbb{Q}}$-points are elliptic curves with complex multiplication by $\mathbb{Z}[\frac{1}{2}(D+\sqrt{-D})]$ such that this CM cycle intersects E at $\mathfrak{p}$ and the CM elliptic curves on the cycle have supersingular reduction at $\mathfrak{p}$, which occurs when the residue field has characteristic p that is ramified or inert in $\mathbb{Q}(\sqrt{-D})$. With a coordinate defined by the j-invariant, the intersection is captured by the non-archimedean part of $P_D(j(E))$, where $P_D(X)$ is the monic polynomial whose roots are j-invariants of the elliptic curves on the CM cycle, and the goal is to find a prime $\mathfrak{p}$ such that $P_D(j_E)$ has positive $\mathfrak{p}$-valuation and p divides D or $-D$ is a quadratic non-residue modulo p. By quadratic reciprocity, the problem reduces to studying the reduction of the CM cycle modulo primes dividing D, as well as at the real place.

Our proof builds on the idea of Elkies. We relate the Hodge-type Shimura curve parametrizing the Kuga-Satake abelian varieties to the quaternionic Shimura curve $\mathcal{O}^1\backslash\mathcal{H}$ that is assumed to be isomorphic to $\mathbb{P}^1$. This allows us to choose a coordinate and construct CM cycles on $\mathbb{P}^1$. For each totally positive odd prime $\lambda\in F$ such that $-\lambda$ is a square modulo 8, we construct polynomials $P_\lambda(x)$ and $P_{4\lambda}(x)$ from CM cycles $\mathcal{P}_\lambda,\mathcal{P}_{4\lambda}$ defined over F. The cycles correspond to optimal embeddings $\mathcal{O}_{F(\sqrt{-\lambda})}\hookrightarrow\mathcal{O}$ and $\mathcal{O}_F[\sqrt{-\lambda}]\hookrightarrow\mathcal{O}$, respectively.[3] By computing the Newton polygon via the Shimura-Taniyama formula, if a prime $\mathfrak{p}$ of F is ramified or inert in $F(\sqrt{-\lambda})$, then the CM abelian varieties have supersingular reduction modulo primes above $\mathfrak{p}$.

[3]If we drop the simplifying assumption that 2 is inert in F, then we need to consider optimal embeddings $R\hookrightarrow\mathcal{O}$ for all $\mathcal{O}_F$-orders R satisfying $\mathcal{O}_F[\sqrt{-\lambda}]\subseteq R\subseteq\mathcal{O}_{F(\sqrt{-\lambda})}$.

1.4.1. *Reduction of the CM cycles $\mathcal{P}_\lambda, \mathcal{P}_{4\lambda}$ modulo λ.* As in the classical setting, the CM points in each cycle fall into pairs modulo λ, except possibly those that reduce to elliptic points with an even order automorphism. Instead of using Lubin-Tate deformation of formal groups typical of PEL cases (such as in [Elk89], [Jao03], [LMPT]), we follow the approach of Madapusi Pera [MP16] on integral models for GSpin Shimura varieties, applying Grothendieck–Messing theory to establish a bijection between deformations of the abelian variety $\mathcal{A}_{x_0}$ at a closed point x_0 with a special endomorphism and liftings of certain isotropic lines orthogonal to the special endomorphism. This description solves the local intersection problem and provides a clear picture of how the liftings are expected to occur in pairs given the quadratic space defined by the quaternion algebra.

In particular, our method explains how to pair the liftings in the neighborhood of the exception points. In the case of elliptic curves, the only exception point is $j = 1728$. In the case of [Jao03] and [BG08], the elliptic points have CM by orders in distinct imaginary quadratic fields, and the presence of unpaired points can be predicted explicitly by checking whether a maximal order of a known quaternion algebra contains two anticommuting CM orders of given discriminants. By contrast, we have multiple elliptic points of order 2 when $h(F(\sqrt{-1})) > 1$. To address the complication, we equip the space of special quasi-endomorphisms $V(\mathcal{A}_{x_0})$ with an F-linear structure via comparison, and use the automorphism to pair the special endomorphisms. This yields a pairing of liftings in the neighborhood of any exception point when we consider the union of all cycles corresponding to all orders containing $\mathcal{O}_F[\sqrt{-\lambda}]$.

This method for studying the deformation of mod $\mathfrak{p}$ points on Shimura curves works in general, without assuming that the Shimura curve has genus zero.

1.4.2. *Real CM points on $\mathcal{P}_\lambda, \mathcal{P}_{4\lambda}$.* At the archimedean places, we follow the work of Shimura [Shi75] to study real points of the Shimura curve and apply Hecke's equidistribution of primes (see for instance [Lan94, XV, §5]). The real points are given by geodesics of the form $Z_\alpha := \{z \in \mathcal{H} : \alpha(\overline{z}) = z\}$, where $\alpha \in \mathcal{O}^\times$ satisfies $\mathrm{trd}(\alpha) = 0$ and $\mathrm{nrd}(\alpha) = \epsilon$, with ϵ a unit negative at the real place where B is split and positive at other real places. Under the assumptions that 2 is inert in F and the class number $h(F(\sqrt{-\epsilon})) = 1$, it suffices to consider a single geodesic. The congruence condition on λ ensures that each of the CM cycles we consider has a unique real point. These real CM points correspond to solutions of the norm equation $\mathrm{Nm}_{F(\sqrt{-\epsilon})/F}(x) = \lambda$. Similar equations are obtained in [Jao03] and [BG08] by describing the real locus as the hyperbolic lines segments between two elliptic points. By Hecke's equidistribution of primes in $F(\sqrt{-\epsilon})$, we can find λ such that $P_\lambda(x)P_{4\lambda}(x)$ is negative at the coordinate of the given abelian variety.

To account for all real embeddings of F, we need to consider all conjugates of the Shimura curve, which correspond to quaternion algebra with different local invariants at infinite places. Assuming that $\mathcal{F} := F(\sqrt{-\epsilon_1}, \ldots, \sqrt{-\epsilon_n})$ has class number 1, we construct a Hecke character of $\mathbb{A}_{\mathcal{F}}^\times$ and apply the equidistribution of primes in $\mathcal{F}$.

Here we have found a good condition that simplifies the setting to a single geodesic. More generally, each $\mathcal{O}^1$-conjugacy class of embeddings $\mathcal{O}_F[\sqrt{-\epsilon}] \hookrightarrow \mathcal{O}$ gives a geodesic. The associated real CM points correspond to solutions of an equation of the form $\mathrm{nrd}(v) = \lambda$, where $v \in B^0 \cap \mathcal{O}$ is orthogonal to the image of $\sqrt{-\epsilon}$. Computations are possible with an explicit basis of maximal order, and a similar equidistribution result can be derived on each geodesic.

Following the proof of [Elk87], we combine 1.4.1 and 1.4.2 to obtain a desired supersingular prime.

1.5. **Organization of the paper.** In §2, we introduce the Shimura curves considered in this work, review the theory of integral canonical model for Shimura varieties of Hodge type, focusing on the GSpin case. The section also includes some other preliminaries that will be used in the proof. In §3, we construct the CM cycles and study their basic properties. In §4, we investigate the reduction of the CM cycles modulo a finite prime, and pair the liftings in the neighborhood of each closed point. In §5, we analyze the distribution of the CM points in the real locus of the Shimura curve. In §6, we combine the results in previous sections to prove Theorem 1.1. In §7, we compute explicit examples in which all the technical assumptions of Theorem 1.1 are satisfied.

1.6. **Notation and conventions.** Assume the following unless specified otherwise.

Suppose F is a totally real number field with narrow class number 1. Equivalently, F is a totally real number field with class number 1 and units of independent signs.

Suppose B is a quaternion algebra over F unramified at all finite places and exactly one of the real places of F. Necessarily $[F:\mathbb{Q}]$ is odd. Denote by $\rho: F \hookrightarrow \mathbb{R}$ the real place where B is split. Let ϵ be a unit of F that is negative at ρ and positive at the other real places, so that the field $F(\sqrt{-\epsilon})$ splits B.

Let $\mathcal{O} = \mathcal{O}_B$ be a maximal order of B.[4] Its normalizer $N_{B^\times}(\mathcal{O}) = F^\times \mathcal{O}^\times$.

Acknowledgments. I thank my advisor Yunqing Tang for introducing this problem to me and for the enlightening discussions and encouragement. I thank Frank Calegari for his blog post "Polymath Proposal: 4-folds of Mumford's type", which was a source of inspiration and useful references. I thank Robin Huang, Wanlin Li, and Sug Woo Shin for helpful discussions.

2. Preliminaries

2.1. The Shimura curves.

2.1.1. Let $\widetilde{G} = \mathrm{Res}_{F/\mathbb{Q}} \mathrm{GL}_{1,B}$ be the algebraic group over $\mathbb{Q}$ with $\widetilde{G}(\mathbb{Q}) = B^\times$, and $\widetilde{K} = \widehat{\mathcal{O}}^\times = \prod \mathcal{O}_v^\times \subset \widetilde{G}(\mathbb{A}_f)$. Strong approximation implies that

$$|B_{>0}^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times| = |F_{>0}^\times \backslash \widehat{F}^\times / \mathrm{nrd}(\widehat{\mathcal{O}}^\times)| = h_+(F) = 1, \tag{2.1.1}$$

and then

$$\widetilde{G}(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \widetilde{G}(\mathbb{A}_f)/\widetilde{K} = \widetilde{G}(\mathbb{Q})_+ \backslash \mathcal{H} \times \widetilde{G}(\mathbb{A}_f)/\widetilde{K} = \widetilde{\Gamma} \backslash \mathcal{H} = \widetilde{\Gamma}^1 \backslash \mathcal{H},$$

where

$$\widetilde{\Gamma} = \{\alpha \in \mathcal{O}^\times : \mathrm{nrd}(\alpha) \in \mathcal{O}_F^\times \text{ is totally positive}\},$$
$$\widetilde{\Gamma}^1 = \mathcal{O}^1 = \{\alpha \in \mathcal{O}^\times : \mathrm{nrd}(\alpha) = 1\}.$$

(Since the totally real number field F has units with independent signs, every totally positive unit in $\mathcal{O}_F^*$ is a square ([CH88, 12.2]), which implies $\widetilde{\Gamma} \backslash \mathcal{H} = \widetilde{\Gamma}^1 \backslash \mathcal{H}$.) The reflex field of this Shimura curve is $\rho(F)$.

2.1.2. Let $V = B^0 = \{\alpha \in B : \mathrm{trd}(\alpha) = 0\}$, then $(V, Q_F := \mathrm{nrd}\,|_{B^0})$ is a 3-dimensional quadratic space over F. For any field extension $\sigma: F \hookrightarrow K$, denote by $(V \otimes_{F,\sigma} K, Q_\sigma := \sigma \circ Q_F)$ the 3-dimensional quadratic space over K. Let $(V, Q := \mathrm{Tr}_{F/\mathbb{Q}} \circ Q_F)$ be the $(3[F:\mathbb{Q}])$-dimensional quadratic space over $\mathbb{Q}$. The signature of (V, Q) is $(3[F:\mathbb{Q}]-2, 2)$, since there is an orthogonal direct sum decomposition $V_\mathbb{R} = V \otimes_\mathbb{Q} \mathbb{R} \simeq \oplus_\sigma (V \otimes_{F,\sigma} \mathbb{R})$, where $V \otimes_{F,\sigma} \mathbb{R}$ has signature $(3,0)$ for $\sigma \neq \rho$ and $(1,2)$ for $\sigma = \rho$.

Let $\mathcal{D} = \{w \in V \otimes_\mathbb{Q} \mathbb{C} : [w,w]_Q = 0, [w, \bar{w}]_Q < 0\}/\mathbb{C}^\times$ be the space of oriented negative definite 2-planes in $V_\mathbb{R}$ and

$$X = \{w \in V \otimes_{F,\rho} \mathbb{C} : [w,w]_Q = 0, [w,\bar{w}]_Q < 0\}/\mathbb{C}^\times.$$

Note that $X \simeq \mathcal{H}^\pm$ is one-dimensional. Each $V \otimes_{F,\sigma} \mathbb{C}$ is an eigenspace for the F-action on $V \otimes_\mathbb{Q} \mathbb{C}$ induced by the F-linear structure on V. The weight 0 Hodge structure on V defined by $[w] \in X$ is $V^{-1,1} = \mathbb{C}w, V^{1,-1} = \mathbb{C}\bar{w}, V^{0,0} = (V^{-1,1} \oplus V^{1,-1})^\perp$, then for $a \in F^\times$, $aV^{-1,1} = V^{-1,1}, aV^{1,-1} = V^{1,-1}$, and since $[au, v]_Q = [u, av]_Q$ for all $u, v \in V$, $aV^{0,0} = V^{0,0}$. Thus, for a Hodge structure V defined by $[w] \in X$, we have $F \subseteq \mathrm{End}_{Hdg}(V)$.

Let $C(V)$ be the Clifford algebra of V over $\mathbb{Q}$. It has a $\mathbb{Z}/2\mathbb{Z}$-grading $C(V) = C^+(V) \oplus C^-(V)$, where $C^+(V)$ is the even Clifford algebra. The reductive group scheme $\mathrm{GSpin}(V, Q)$ over $\mathbb{Q}$ is defined by

$$\mathrm{GSpin}(V,Q)(R) := \{g \in C_R^+(V_R)^\times : gV_R g^{-1} = V_R\}$$

for any $\mathbb{Q}$-algebra R, where C_R (resp. C_R^+) denotes the Clifford algebra (resp. even Clifford algebra) of a quadratic space over R. There is a canonical involution $*$ on $C(V)$ given by the reversal involution on $\oplus_{d=0}^\infty V^{\otimes d}$, and the spinor norm $\nu: \mathrm{GSpin}(V,Q) \to \mathbb{G}_m$ is defined by $x \mapsto x^* x$. A choice of $\delta \in C(V)^\times$ such that $\delta^* = -\delta$ (for example, $\delta = ef$ for orthogonal vectors $e, f \in V$ with $Q(e) < 0, Q(f) < 0$) defines a symplectic form $\psi_\delta: C(V) \times C(V) \to \mathbb{Q}$, $(x,y) \mapsto \mathrm{Trd}(x\delta y^*)$. The action of $\mathrm{GSpin}(V,Q)$ on $C(V)$ by left multiplication induces an embedding $\mathrm{GSpin}(V,Q) \hookrightarrow \mathrm{GSp}(C(V), \psi_\delta)$, under which the similitude character on $\mathrm{GSp}(C(V), \psi_\delta)$ restricts to the spinor norm ν on $\mathrm{GSpin}(V,Q)$ ([MP16, 1.6, 1.7]).

[4] If F has narrow class number 1, then any two maximal orders in an indefinite quaternion algebra over F are conjugate to each other.

The action of $\mathrm{GSpin}(V,Q)$ on V by conjugation induces an exact sequence of group schemes over $\mathbb{Q}$

$$1 \to \mathbb{G}_m \to \mathrm{GSpin}(V,Q) \to \mathrm{SO}(V,Q) \to 1. \tag{2.1.2}$$

Define the algebraic groups $G \subset \mathrm{GSpin}(V,Q)$ and $G_0 \subset \mathrm{SO}(V,Q)$ by

$$\begin{aligned} G(R) &= \{g \in \mathrm{GSpin}(V,Q)(R) : \alpha(g\cdot v) = g\cdot(\alpha v)\,\forall \alpha \in F, v \in V_R\} \\ G_0(R) &= \{g \in \mathrm{SO}(V,Q)(R) : \alpha g = g\alpha\,\forall \alpha \in F\} \end{aligned}$$

for any $\mathbb{Q}$-algebra R, so that the image of G under (2.1.2) is G_0. Since $(\alpha,\beta) \mapsto \mathrm{Tr}_{F/\mathbb{Q}}(\alpha\beta)$ is a perfect pairing on the $\mathbb{Q}$-vector space F, we have $G_0(\mathbb{Q}) = \mathrm{SO}(V,Q_F)(F) = B^\times/F^\times$.

The embedding

$$(G,X) \hookrightarrow (\mathrm{GSpin}(V,Q),\mathcal{D}) \hookrightarrow (\mathrm{GSp}(C(V),\psi_\delta),\mathcal{S}^\pm)$$

realizes (G,X) as a Shimura datum of Hodge type. When F is cubic, we have $\mathrm{Cor}_{F/\mathbb{Q}}(B) \simeq M_8(\mathbb{Q})$ since B is split at all finite places, and this Kuga-Satake construction from K3 type Hodge structures with real multplication is consistent with Mumford's original construction ([vG08, 6.4]).

2.1.3. We can use the corestriction of algebras to describe the morphism $\widetilde{G} \to G$ ([Mum69, §4], [vG08, 6.2, 6.3]). Let $\tilde{F}$ be the Galois closure of F. The direct sum decomposition of quadratic spaces

$$(V \otimes_{\mathbb{Q}} \tilde{F}, Q) = \bigoplus_{\sigma: F \hookrightarrow \tilde{F}} (V \otimes_{F,\sigma} \tilde{F}, Q_\sigma)$$

gives an isomorphism of $\tilde{F}$-algebras

$$C(V) \otimes_{\mathbb{Q}} \tilde{F} = C_{\tilde{F}}(V \otimes_{\mathbb{Q}} \tilde{F}) = \widehat{\bigotimes}_{\sigma: F\hookrightarrow\tilde{F}} C_{\tilde{F}}(V \otimes_{F,\sigma} \tilde{F}) = \widehat{\bigotimes}_{\sigma: F\hookrightarrow\tilde{F}} \left(C_F(V) \otimes_{F,\sigma} \tilde{F}\right), \tag{2.1.3}$$

where $\widehat{\bigotimes}_{\sigma:F\hookrightarrow\tilde{F}}$ denotes a graded tensor product over $\tilde{F}$ indexed by embeddings $\sigma : F \hookrightarrow \tilde{F}$. On the all even part, the graded tensor product over $\tilde{F}$ is the usual tensor product over $\tilde{F}$, so $\bigotimes_{\sigma:F\hookrightarrow\tilde{F}} \left(C_F^+(V) \otimes_{F,\sigma} \tilde{F}\right)$ lies in the even part of $\widehat{\bigotimes}_{\sigma:F\hookrightarrow\tilde{F}} \left(C_F(V) \otimes_{F,\sigma} \tilde{F}\right)$. The Galois group $\mathrm{Gal}(\tilde{F}/\mathbb{Q})$ acts on $V \otimes_{\mathbb{Q}} \tilde{F}$ via the second factor of the tensor product, thus under the isomorphism $V \otimes_{\mathbb{Q}} \tilde{F} = \bigoplus_{\sigma:F\hookrightarrow\tilde{F}} V \otimes_{F,\sigma} \tilde{F}$, this action permutes the eigenspaces $V \otimes_{F,\sigma} \tilde{F}$: for $g \in \mathrm{Gal}(\tilde{F}/\mathbb{Q})$, we have $g : V \otimes_{F,\sigma} \tilde{F} \to V \otimes_{F,g\sigma} \tilde{F}$ defined by $r \otimes a \mapsto r \otimes g(a)$. Similarly, $\mathrm{Gal}(\tilde{F}/\mathbb{Q})$ acts on $C(V) \otimes_{\mathbb{Q}} \tilde{F}$ via the second factor of the tensor product. Over $\tilde{F}$, we have a group homomorphism

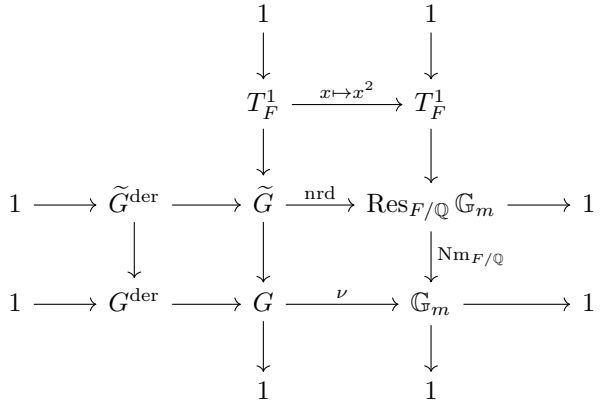
$$\left(C_F^+(V) \otimes_{\mathbb{Q}} \tilde{F}\right)^\times = \prod_{\sigma:F\hookrightarrow\tilde{F}} \left(C_F^+(V) \otimes_{F,\sigma} \tilde{F}\right)^\times \xrightarrow{\mathrm{Nm}} \bigotimes_{\sigma:F\hookrightarrow\tilde{F}} \left(C_F^+(V) \otimes_{F,\sigma} \tilde{F}\right)^\times \hookrightarrow \left(C^+(V) \otimes_{\mathbb{Q}} \tilde{F}\right)^\times,$$

where the norm map is defined by

$$\mathrm{Nm}\left((b_\sigma)_{\sigma:F\hookrightarrow\tilde{F}}\right) = \bigotimes_{\sigma:F\hookrightarrow\tilde{F}} b_\sigma.$$

The image of $(b_\sigma)_{\sigma:F\hookrightarrow\tilde{F}}$ acts as b_σ on each $V \otimes_{F,\sigma} \tilde{F}$; in particular, it preserves $V \otimes_{\mathbb{Q}} \tilde{F}$ and respects the F-linear structure on $V \otimes_{\mathbb{Q}} \tilde{F}$. Therefore, we have a group homomorphism $(C_F^+(V) \otimes_{\mathbb{Q}} \tilde{F})^\times \to G(\tilde{F})$. Taking $\mathrm{Gal}(\tilde{F}/\mathbb{Q})$-invariants gives a group homomorphism $C_F^+(V)^\times \to G(\mathbb{Q})$. Under the identification $C_F^+(V) \xrightarrow{\simeq} B$, we obtain the corresponding morphism of algebraic groups $\widetilde{G} \to G$ over $\mathbb{Q}$, whose kernel is the algebraic torus T_F^1 over $\mathbb{Q}$ defined by $T_F^1(\mathbb{Q}) = \{x \in F^\times : \mathrm{Nm}_{F/\mathbb{Q}}\, x = 1\}$. The morphism $\widetilde{G} \to G$ induces $\widetilde{G}^{\mathrm{der}} \to G^{\mathrm{der}}$

and the following diagram



commutes. Since $\widetilde{G}^{\mathrm{der}}(\mathbb{Q}) \cap T_F^1(\mathbb{Q}) = \{x \in F^\times : x^2 = 1, \mathrm{Nm}_{F/\mathbb{Q}}(x) = 1\} = \{1\}$ as $[F : \mathbb{Q}]$ is odd, we have an isomorphism $\mathrm{Res}_{F/\mathbb{Q}} \mathrm{SL}_{1,B} = \widetilde{G}^{\mathrm{der}} \xrightarrow{\simeq} G^{\mathrm{der}}$.

2.1.4. Let $L = V \cap \mathcal{O}$, then it is a rank 3 free $\mathcal{O}_F$-module and a rank $3[F : \mathbb{Q}]$ free $\mathbb{Z}$-module. By [Voi21, 22.4.15], for any quaternion $\mathcal{O}_F$ order $\mathcal{O}'$ we have $\mathcal{O}' = \mathcal{O}_F + \mathrm{discrd}(\mathcal{O}')(\mathcal{O}'^{\#})^0(\mathcal{O}'^{\#})^0 = C^+_{\mathcal{O}_F}((\mathcal{O}'^{\#})^0, N\,\mathrm{nrd})$, where $\mathrm{discrd}(\mathcal{O}') = (N)$ and $(\mathcal{O}'^{\#})^0 = \{\alpha \in B : \mathrm{trd}(\alpha\mathcal{O}') \subseteq \mathcal{O}_F, \mathrm{trd}(\alpha) = 0\}$. Here $\mathrm{discrd}(\mathcal{O}) = \mathrm{disc}(B) = (1)$ and $\mathcal{O}^{\#} = \mathcal{O}$ since $\mathcal{O}$ is maximal and B is split at all finite places. Define

$$K = \{g \in G(\mathbb{A}_f) : g(C(L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})) = C(L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})\} = G(\mathbb{A}_f) \cap C(L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times,$$
$$K_0 = \{g \in G_0(\mathbb{A}_f) : g(L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}) = L \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}\}.$$

The image of $\widetilde{K}$ under $\widetilde{G} \to G \to G_0$ is K_0 since $N_{B^\times}(\mathcal{O}) = F^\times \mathcal{O}^\times$. The image of K in $G_0(\mathbb{A}_f)$ is $\{g \in K_0 : g \text{ acts trivially on } L^\vee_{\widehat{\mathbb{Z}}}/L_{\widehat{\mathbb{Z}}}\}$ ([MP16, 2.6]). The dual lattice $L^\vee = \mathfrak{D}^{-1}_{F/\mathbb{Q}} L \subset V$, where $\mathfrak{D}_{F/\mathbb{Q}} \subset \mathcal{O}_F$ is the different of $F/\mathbb{Q}$. There are well-defined maps

$$\widetilde{G}(\mathbb{Q})\backslash \mathcal{H}^{\pm} \times \widetilde{G}(\mathbb{A}_f)/\widetilde{K} \to G_0(\mathbb{Q})\backslash X \times G_0(\mathbb{A}_f)/K_0 \tag{2.1.4}$$

and

$$G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K \to G_0(\mathbb{Q})\backslash X \times G_0(\mathbb{A}_f)/K_0. \tag{2.1.5}$$

Note that $1 \to \mathrm{Res}_{F/\mathbb{Q}} \mathbb{G}_m \to \widetilde{G} \to G_0 \to 1$ and $H^1(\mathbb{Q}_l, \mathrm{Res}_{F/\mathbb{Q}} \mathbb{G}_m) \simeq H^1(\mathbb{Q}_l, \prod_{v|l} \mathrm{Res}_{F_v/\mathbb{Q}_l} \mathbb{G}_m) \simeq \prod_{v|l} H^1(\mathbb{Q}_l, \mathrm{Res}_{F_v/\mathbb{Q}_l} \mathbb{G}_m) \simeq \prod_{v|l} H^1(F_v, \mathbb{G}_m)$ is trivial by Hilbert's 90. Therefore, the map (2.1.4) is surjective, and in particular, $G_0(\mathbb{Q})\backslash X \times G_0(\mathbb{A}_f)/K_0$ is connected. Let $\Gamma_0 := G_0(\mathbb{Q}) \cap K_0 = F^\times \mathcal{O}^\times / F^\times$, then (2.1.4) is an isomorphism

$$\widetilde{\Gamma}\backslash \mathcal{H} \xrightarrow{\simeq} \Gamma_0 \backslash X^+. \tag{2.1.6}$$

For each $g \in G(\mathbb{A}_f)$, let $\Gamma_g := G(\mathbb{Q})_+ \cap gKg^{-1}$, then $[x] \mapsto [x, g]$ defines a connected component $\Gamma_g\backslash X^+ \hookrightarrow G(\mathbb{Q})_+\backslash X^+ \times G(\mathbb{A}_f)/K$ and (2.1.5) gives a finite map

$$\Gamma_g\backslash X^+ \to \Gamma_0 \backslash X^+. \tag{2.1.7}$$

Note that

$$G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K \simeq \bigsqcup_{[g] \in G(\mathbb{Q})_+\backslash G(\mathbb{A}_f)/K} \Gamma_g\backslash X^+,$$

and if $x_1, x_2 \in G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$ maps to the same point under (2.1.5), then the corresponding abelian varieties $\mathcal{A}_{x_1}, \mathcal{A}_{x_2}$ are isogenous.

2.1.5. See [Voi09, §4] for a complete list of genus 0 Shimura curves constructed from congruence arithmetic Fuchsian group in $\mathrm{PSL}_2(\mathbb{R})$. In particular, we have $[F : \mathbb{Q}] \leq 7$.

2.2. **Integral model.** Let p be an odd prime unramified in F. Let $L_{(p)} = L \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ and $H_{(p)} = C(L_{(p)})$ be the Clifford algebra of $L_{(p)}$ over $\mathbb{Z}_{(p)}$. Since B is unramified at all finite places, $(L_{(p)}, Q)$ is non-degenerate, i.e., Q induces an isomorphism $L_{(p)} \xrightarrow{\simeq} L_{(p)}^\vee$, and $\mathrm{GSpin}(V, Q)$ extends to a reductive group scheme $\mathrm{GSpin}(L_{(p)}, Q)$ over $\mathbb{Z}_{(p)}$. Via left multiplication, the group $C^+(L_{(p)}) \subset \mathrm{GL}(H_{(p)})$ is the subgroup of automorphisms that preserves the grading and centralizes the right $C(L_{(p)})$-action on $H_{(p)}$. The pairing

$$[\varphi_1, \varphi_2] = \frac{1}{2^{3[F:\mathbb{Q}]-1}} \operatorname{Tr}(\varphi_1 \circ \varphi_2)$$

on $\mathrm{End}(H_{(p)})$ restricts to $[\cdot,\cdot]_Q$ on $L_{(p)}$ since $[v, v] = \frac{1}{2^{3[F:\mathbb{Q}]-1}} \operatorname{Tr}(Q(v)|_{H_{(p)}}) = 2Q(v)$ for all $v \in L_{(p)}$. Let $\boldsymbol{\pi} : \mathrm{End}(H_{(p)}) \to \mathrm{End}(H_{(p)})$ be the orthogonal projection onto $L_{(p)}$. Then $\mathrm{GSpin}(L_{(p)}, Q) \subset C^+(L_{(p)})$ is the stablizer of the idempotent operator $\boldsymbol{\pi}$ ([MP16, 1.4]). For $\epsilon_1, \ldots, \epsilon_m \in \mathcal{O}_F$ such that $\mathcal{O}_F = \mathbb{Z}[\epsilon_1, \ldots, \epsilon_m]$, consider the endomorphism $\boldsymbol{\pi}_{\epsilon_i} : \mathrm{End}(H_{(p)}) \to \mathrm{End}(H_{(p)})$ given by $\boldsymbol{\pi}_{\epsilon_i}(\varphi) = \epsilon_i(\boldsymbol{\pi}(\varphi))$. Let $G_{\mathbb{Z}_{(p)}} \subset \mathrm{GSpin}(L_{(p)}, Q)$ be the stablizer of all $\boldsymbol{\pi}_{\epsilon_i}$. Let $\{s_\alpha\} \subset H_{(p)}^\otimes$ denote a finite collection of tensors defining $G \subset \mathrm{GL}(H_{(p)})$ with $\boldsymbol{\pi}, \boldsymbol{\pi}_{\epsilon_i} \in \{s_\alpha\}$.

Let $K_p = G(\mathbb{Z}_p)$ and $K^p \subset G(\mathbb{A}_f^p)$ be a small enough open compact subgroup. Denote by $\mathrm{Sh}_{K_pK^p} = \mathrm{Sh}_{K_pK^p}(G, X)$ the Shimura curve attached to G and $\mathscr{S}_{K_pK^p}$ its integral canonical model. The integral model $\mathscr{S}_{K_pK^p}$ is constructed in [Kis10] as the normalization of $\mathscr{S}^-_{K_pK^p}(G, X)$, the closure of $\mathrm{Sh}_{K_pK^p}$ in the natural integral model of the Siegel modular variety. The normalization step can be removed by [Xu22]. Let $\mathcal{A} \to \mathscr{S}_{K_pK^p}$ denote the universal abelian scheme, which exists assuming that K^p sufficiently small. Let $s_{\alpha,?}$ denote the cohomological realizations of s_α, where $? = B, \mathrm{dR}, \ell, p, \mathrm{cris}$.

Let $k = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$ and $W = W(k)$ be its ring of Witt vectors. Suppose $x \in \mathscr{S}_{K_pK^p}(k)$ is a closed point. Write $\widehat{U}_x$ for the completion of $\mathscr{S}_{K_pK^p}$ at x. Suppose $\tilde{x} \in \mathscr{S}_{K_pK^p}(E)$ is a point specializing to x, where E is a finite extension of $W[p^{-1}]$.

Choose an embedding $\iota : \overline{E} \hookrightarrow \mathbb{C}$. The natural isomorphism $H_{(p)} \simeq H_B^1(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}), \mathbb{Z}_{(p)})$ takes s_α to $s_{\alpha,B,\iota(\tilde{x})}$. The comparison isomorphism

$$H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/E) \otimes_{E,\iota} \mathbb{C} \xrightarrow{\simeq} H_B^1(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \tag{2.2.1}$$

takes $s_{\alpha,\mathrm{dR},\tilde{x}} \otimes 1$ to $s_{\alpha,B,\iota(\tilde{x})} \otimes 1$, and the comparison isomorphism

$$H_B^1(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}), \mathbb{Z}_{(p)}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p \xrightarrow{\simeq} H^1_{\text{ét}}(\mathcal{A}_{\tilde{x}_{\bar{E}}}, \mathbb{Z}_p) \tag{2.2.2}$$

takes $s_{\alpha,B,\iota(\tilde{x})} \otimes 1$ to $s_{\alpha,p,\tilde{x}}$. Via the p-adic comparison isomorphism

$$H^1_{\text{ét}}(\mathcal{A}_{\tilde{x}_{\bar{E}}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} B_{\mathrm{cris}} \xrightarrow{\simeq} H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W B_{\mathrm{cris}}, \tag{2.2.3}$$

the $\mathrm{Gal}(\overline{F_v}/E)$-invariant tensors $s_{\alpha,p,\tilde{x}}$ give rise to Frobenius invariant tensors $s_{\alpha,\mathrm{cris},x} \in H^1_{\mathrm{cris}}(\mathcal{A}_x/W)^\otimes$. From the proof of [Kis10, 2.3.5], it follows that the tensors $s_{\alpha,\mathrm{cris},x}$ are independent of the choice of $\tilde{x}$. There exists a W-linear isomorphism

$$H^1_{\text{ét}}(\mathcal{A}_{\tilde{x}_{\bar{E}}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} W \to H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \tag{2.2.4}$$

taking $s_{\alpha,p,\tilde{x}}$ to $s_{\alpha,\mathrm{cris},x}$ ([Kis10, 1.4.3]). From (2.2.2) and (2.2.4), there exists a W-linear isomorphism $H_{(p)} \otimes_{\mathbb{Z}_{(p)}} W \to H^1_{\mathrm{cris}}(\mathcal{A}_x/W)$ taking s_α to $s_{\alpha,\mathrm{cris},x}$, and the tensors $s_{\alpha,\mathrm{cris},x}$ define a reductive subgroup $G_W \subset GL(H^1_{\mathrm{cris}}(\mathcal{A}_x/W))$, which is isomorphic to $G_{\mathbb{Z}_{(p)}} \times_{\mathrm{Spec}\,\mathbb{Z}_{(p)}} \mathrm{Spec}\, W$. Let $\boldsymbol{L}_{\mathrm{cris},x}$ be the image of $\boldsymbol{\pi}_{\mathrm{cris},x}$ on $\mathrm{End}(H^1_{\mathrm{cris}}(\mathcal{A}_x/W))$, then since all $\boldsymbol{\pi}_{\epsilon_i}$ and the quadratic form on $L_{(p)}$ are absolute Hodge cycles, there is an $\mathcal{O}_F$-linear isometry

$$L_{(p)} \otimes_{\mathbb{Z}_{(p)}} W \to \boldsymbol{L}_{\mathrm{cris},x}, \tag{2.2.5}$$

and $G_W \subset \mathrm{GSpin}(\boldsymbol{L}_{\mathrm{cris},x})$. Since p is unramified in F, we have an orthogonal direct sum decomposition

$$\boldsymbol{L}_{\mathrm{cris},x} \simeq L_{(p)} \otimes_{\mathbb{Z}_{(p)}} W = \bigoplus_{\sigma' : F \hookrightarrow W[p^{-1}]} L \otimes_{\mathcal{O}_F, \sigma'} W, \tag{2.2.6}$$

where orthogonality arises from the distinct scalar actions of $\mathcal{O}_F$ via the embeddings σ'. From the proof of (2.3.5) in [Kis10], $\widehat{U}_x$ is isomorphic to $\mathrm{Spf}\, R_{G_W}$, where R_{G_W} is the complete local ring at the identity section of the opposite unipotent defined by a cocharacter $\mathbb{G}_m \to G_W$ whose reduction modulo p induces the

filtration on $H^1_{\mathrm{cris}}(\mathcal{A}_x/W)\otimes k = H^1_{\mathrm{dR}}(\mathcal{A}_x/k)$. For any $\tilde{x}' \in \widehat{U}_x$ defined over a finite extension E' of $W[p^{-1}]$, the filtration on

$$H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}'}/E') \xrightarrow{\simeq} H^1_{\mathrm{cris}}(\mathcal{A}_x/W)\otimes_W E'$$

is induced by a $G_W \otimes_W E'$-valued cocharacter ([Kis10, 1.4.5]).

2.3. **Special endomorphisms.** We follow [MP16, 5.1-5.13] to define the space of special endomorphisms $L(\mathcal{A}_x)$ of a point $x \to \mathscr{S}_{K_pK^p}$.

2.3.1. Let $x \to \mathrm{Sh}_{K_pK^p}$ be a geometric point with $k(x) \subseteq \mathbb{C}$ and ℓ be a rational prime. The comparison isomorphism

$$H^1_B(\mathcal{A}_x(\mathbb{C}),\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{Q}_\ell \xrightarrow{\simeq} H^1_{\text{ét}}(\mathcal{A}_x,\mathbb{Q}_\ell) \tag{2.3.1}$$

takes $s_{\alpha,B,x}\otimes 1$ to $s_{\alpha,\ell,x}$. Let $\boldsymbol{V}_{\ell,x}$ be the image of $\boldsymbol{\pi}_{\ell,x}$, then (2.3.1) induces an F-linear isometry

$$V\otimes_{\mathbb{Q}}\mathbb{Q}_l \xrightarrow{\simeq} \boldsymbol{V}_{\ell,x}. \tag{2.3.2}$$

Let $\boldsymbol{L}_{\ell,x} = \boldsymbol{V}_{\ell,x}\cap \mathrm{End}(T_\ell(\mathcal{A}_x))$, where $T_\ell(\mathcal{A}_x) = \varprojlim \mathcal{A}_x[\ell^n]$ is the ℓ-adic Tate module of $\mathcal{A}_x$. Since the comparison isomorphism gives

$$H^1_B(\mathcal{A}_x(\mathbb{C}),\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \xrightarrow{\simeq} H^1_{\text{ét}}(\mathcal{A}_x,\mathbb{Z}_\ell) \tag{2.3.3}$$

and $L = V\cap \mathrm{End}(C(L))$, under (2.3.2) we have

$$L\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \simeq \boldsymbol{L}_{\ell,x}. \tag{2.3.4}$$

Definition 2.1 ([MP16, 5.4, 5.5])**.** An endomorphism $f\in \mathrm{End}(\mathcal{A}_x)$ is special if it satisfies any of the equivalent conditions:

(1) the Betti realization of $f_{\mathbb{C}}$ gives a section of $\boldsymbol{V}_{B,x}\subset \mathrm{End}(H^1_B(\mathcal{A}_x(\mathbb{C}),\mathbb{Q}))$;
(2) the ℓ-adic realization of f is an element of $\boldsymbol{V}_{\ell,x}\subset \mathrm{End}(H^1_{\text{ét}}(\mathcal{A}_x,\mathbb{Q}_\ell))$ for some prime ℓ;
(3) the ℓ-adic realization of f is an element of $\boldsymbol{V}_{\ell,x}\subset \mathrm{End}(H^1_{\text{ét}}(\mathcal{A}_x,\mathbb{Q}_\ell))$ for all prime ℓ.

2.3.2. Let $x\in \mathscr{S}_{K_pK^p}(\overline{\mathbb{F}}_p)$ and $\ell\neq p$.

Definition 2.2. An endomorphism $f\in\mathrm{End}(\mathcal{A}_x)$ is special if its crystalline realization lies in $\boldsymbol{L}_{\mathrm{cris},x}$.

The definition of $\boldsymbol{V}_{\ell,x}$ and $\boldsymbol{L}_{\ell,x}$ carries over since $T_\ell(\mathcal{A}_{\tilde{x}})\xrightarrow{\simeq} T_\ell(\mathcal{A}_x)$ for any lift $\mathcal{A}_{\tilde{x}}$ of $\mathcal{A}_x$. By [MP16, 5.13], if $f\in\mathrm{End}(\mathcal{A}_x)$ is special, then its ℓ-adic realization is an element of $\boldsymbol{L}_{\ell,x}$.

2.4. **Intersection number.**

Definition 2.3. Let R be a Dedekind domain and $\mathcal{X}\to \mathrm{Spec}\, R$ be an arithmetic surface. Let D and E be two effective divisors on $\mathcal{X}$ with no common irreducible component. Let $z_0\in\mathcal{X}$ be a closed point. The local intersection number $i_{z_0}(D,E)$ of D and E at z_0 is the length of the $\mathcal{O}_{\mathcal{X},z_0}$-module $\mathcal{O}_{\mathcal{X},z_0}/(\mathcal{O}_{\mathcal{X}}(-D)_{z_0}+\mathcal{O}_{\mathcal{X}}(-E)_{z_0})$.

Example 2.4. Let R be a discrete valuation ring with field of fraction K, maximal ideal $\mathfrak{p}$ and residue field k. Let $x,y\in\mathcal{X}(K)$ be distinct, then x,y extend uniquely to $\underline{x},\underline{y}\in\mathcal{X}(R)$ by properness of $\mathcal{X}\to\mathrm{Spec}\,R$, and $\underline{x},\underline{y}$ are closed immersions since they are sections to a separated map. Define

$$(\underline{x}.\underline{y}) := \sum_{z\in\mathcal{X}_k} i_z(\underline{x},\underline{y}).$$

Let $x_n,y_n\in\mathcal{X}(R/\mathfrak{p}^n)$ be the reduction of $\underline{x},\underline{y}$ modulo $\mathfrak{p}^n$ for positive integer n. Suppose $x\neq y$, then as in [Sad04, 3.13],

$$(\underline{x}.\underline{y}) = \max\{n : x_n = y_n\}.$$

In particular,

(1) if $\mathcal{X}$ is a fine moduli space with a universal object $\mathcal{A}\to\mathcal{X}$, then the complete local ring $\widehat{\mathcal{O}}_{\mathcal{X},z_0}$ is the universal deformation ring for z_0 and

$$(\underline{x}.\underline{y}) = \max\{n : \mathcal{A}_{\underline{x}}\simeq \mathcal{A}_{\underline{y}} \mod \mathfrak{p}^n\};$$

(2) if $\mathcal{X} = \mathbb{P}^1_R$ and $x_1 = y_1 = z_0 \in \mathcal{X}(k)$, then

$$(\underline{x}.\underline{y}) = i_{z_0}(\underline{x}, \underline{y}) = \begin{cases} v_{\mathfrak{p}}(x-y) & v_{\mathfrak{p}}(x) \geq 0, v_{\mathfrak{p}}(y) \geq 0, \\ v_{\mathfrak{p}}(\frac{1}{x} - \frac{1}{y}) & v_{\mathfrak{p}}(x) < 0 \text{ or } x = \infty, v_{\mathfrak{p}}(y) < 0 \text{ or } y = \infty. \end{cases}$$

Lemma 2.5. *Let R be a complete discrete valuation ring with field of fraction K, maximal ideal $\mathfrak{p}$ and algebraically closed residue field $k = \bar{k}$. Suppose $\mathcal{Y} \to \operatorname{Spec} R$ is a smooth curve over R and G is a finite group acting R-linearly on $\mathcal{Y}$. Let $\mathcal{X} = \mathcal{Y}/G$.*

(1) The complete local ring of $\mathcal{Y}$ at a closed point y_0 is R-isomorphic to $R[[T]]$. The isotropy group $G_{y_0} \subset G$ of y_0 acts R-linearly on $R[[T]]$, and the complete local ring of $\mathcal{X}$ at the image x_0 of y_0 is the ring of invariants $(R[[T]])^{G_{y_0}} = R[[\mathrm{Nm}_{\overline{G}_{y_0}}(T)]]$, where $\overline{G}_{y_0}$ is the image of G_{y_0} in $\mathrm{Aut}_R(R[[T]])$ and $\mathrm{Nm}_{\overline{G}_{y_0}}(T) = \prod_{\gamma \in \overline{G}_{y_0}} \gamma(T)$.

(2) Suppose $\underline{y}, \underline{y}' \in \mathcal{Y}(R)$ both reduce to $y_0 \in \mathcal{Y}(k)$. Suppose T, T' cut out the sections $\underline{y}, \underline{y}' : \widehat{\mathcal{O}}_{\mathcal{Y},y_0} \twoheadrightarrow R$, respectively. Let $\underline{x}, \underline{x}'$ be the images of $\underline{y}, \underline{y}'$, respectively, then

$$(\underline{x}.\underline{x}') = \sum_{\gamma \in \overline{G}_{y_0}} \mathrm{length}(\widehat{\mathcal{O}}_{\mathcal{Y},y_0}/(T, \gamma(T'))).$$

In particular, let $G_{y'} \subset G_{y_0}$ be the isotropy group of $\underline{y}'$, and $\overline{G}_{y'}$ be its image in $\overline{G}_{y_0}$, then

$$(\underline{x}.\underline{x}') = \#\overline{G}_{y'} \sum_{\gamma \in \overline{G}_{y_0}/\overline{G}_{y'}} \mathrm{length}(\widehat{\mathcal{O}}_{\mathcal{Y},y_0}/(T, \gamma(T')))$$

is divisible by $\#\overline{G}_{y'}$, and $(\underline{x}.\underline{x}') = \#\overline{G}_{y_0}(\underline{y}.\underline{y}')$ if $G_{y'} = G_{y_0}$.

Proof. (1) [KM85, pp. 508-509]
(2) [Con04, p.12]

□

2.5. **Quadratic reciprocity.**

Theorem 2.6 ([Hec81, Theorem 167])**.** *Fix a number field K with r_1 real embeddings $\rho_1, \ldots, \rho_{r_1} : K \hookrightarrow \mathbb{R}$. Let $\alpha, \beta \in \mathcal{O}_K$, where α is odd, i.e., α is relatively prime to 2. If $\beta = \mathfrak{m}\mathfrak{n}$, where $\mathfrak{m}$ is an integral ideal without odd prime factors and $\mathfrak{n}$ is an odd integral ideal, then*

$$\left(\frac{\beta}{\alpha}\right) \cdot \left(\frac{\alpha}{\mathfrak{n}}\right) = (-1)^{\sum_{i=1}^{r_1} \frac{\operatorname{sgn} \rho_i(\alpha) - 1}{2} \frac{\operatorname{sgn} \rho_i(\beta) - 1}{2}}$$

if the odd number α is a quadratic residue $\bmod 4\mathfrak{m}$ *and relatively prime to β.*

3. CM points

In this section, we construct CM cycles and describe some properties of the cycles and the abelian varieties they parametrize. An abelian variety parametrized by a Shimura variety of Hodge type is of CM type if and only if the corresponding Hodge cocharacter factors through a $\mathbb{Q}$-rational torus. The CM cycles are constructed in section 3.1 using subtori of $\widetilde{G}$. Each CM cycle on $\widetilde{G}(\mathbb{Q})\backslash\mathcal{H}^{\pm} \times \widetilde{G}(\mathbb{A}_f)/\widetilde{K} = \widetilde{\Gamma}\backslash\mathcal{H} \simeq \Gamma_0\backslash X^+$ corresponds to an $\mathcal{O}_F$-order in a CM extension of F by Lemma 3.1, and it is defined over F by Lemma 3.2. Its size equals the class number of the corresponding $\mathcal{O}_F$-order, as shown in Lemma 3.5 and computed in Lemma 3.6. The specific $\mathcal{O}_F$-orders we will consider are described in 3.7. Finally, using the Shimura-Taniyama formula, we obtain in 3.10 a sufficient condition for the primes at which the abelian varieties on the CM cycle have supersingular reduction.

3.1. **CM cycles.** Let $L = F(\sqrt{-\lambda})$ be a CM extension of F and $\phi : L \hookrightarrow B$ be an embedding.[5] Note that $\phi(L) \cap \mathcal{O} = \phi(\phi^{-1}(\mathcal{O}))$ and ϕ defines an optimal embedding $\phi^{-1}(\mathcal{O}) \hookrightarrow \mathcal{O}$. Let $\widetilde{T} = \mathrm{Res}_{L/\mathbb{Q}} \mathbb{G}_m$ and

[5]Such an embedding $\phi : L \hookrightarrow B$ exists because B is split at all finite places of F, which implies that any CM extension L of F splits B, and L is a maximal subfield of B.

$\tilde{h}: \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m \to \widetilde{G}_{\mathbb{R}}$ be the cocharacter defined by

$$\mathbb{C}^\times \to \prod_{\sigma:F\hookrightarrow\mathbb{R}} \mathbb{C}^\times = \prod_{\sigma:F\hookrightarrow\mathbb{R}} (L\otimes_{F,\sigma}\mathbb{R})^\times = L\otimes_{\mathbb{Q}}\mathbb{R} \overset{\phi}{\hookrightarrow} B\otimes_{\mathbb{Q}}\mathbb{R}, \tag{3.1.1}$$

where $\mathbb{C}^\times \to \prod_{\sigma:F\hookrightarrow\mathbb{R}}\mathbb{C}^\times$ is the inclusion on the coordinate corresponding to $\rho: F\hookrightarrow\mathbb{R}$ at which B is split. Consider the CM cycle

$$\widetilde{T}(\mathbb{Q})\backslash\{\tilde{h}\}\times\widetilde{T}(\mathbb{A}_f)/K_{\widetilde{T}} \hookrightarrow \widetilde{G}(\mathbb{Q})\backslash\mathcal{H}^\pm\times\widetilde{G}(\mathbb{A}_f)/\widetilde{K}, \tag{3.1.2}$$

where $K_{\widetilde{T}} = \widetilde{T}(\mathbb{A}_f)\cap\phi^{-1}(\widehat{\mathcal{O}})$. This is injective because if $[\tilde{h},t_1]=[\tilde{h},t_2]$ with $t_1,t_2\in\widetilde{T}(\mathbb{A}_f)$, then there exist $a\in\widetilde{G}(\mathbb{Q})$, $k\in\widetilde{K}$ such that $a\cdot\tilde{h}=\tilde{h}$ and $at_1k=t_2$. The first equality implies $a\in L^\times$ and then $k=t_1^{-1}a^{-1}t_2\in\widetilde{T}(\mathbb{A}_f)\cap\widetilde{K}=K_{\widetilde{T}}$.

This CM cycle can be described via optimal embeddings $\phi^{-1}(\mathcal{O})\hookrightarrow\mathcal{O}$ by Lemma 3.1, which is a special case of the trace formula [Voi21, 30.4.7]. Let

$$\mathcal{E} := \{\beta\in B^\times : \beta^{-1}\phi(L)\beta\cap\mathcal{O}=\beta^{-1}\phi(\phi^{-1}(\mathcal{O}))\beta\} = \{\beta\in B^\times : \phi(L)\cap\beta\mathcal{O}\beta^{-1}=\phi(\phi^{-1}(\mathcal{O}))\},$$
$$\widehat{\mathcal{E}} := \{\widehat{\beta}\in\widehat{B}^\times : \widehat{\beta}^{-1}\widehat{\phi(L)}\widehat{\beta}\cap\widehat{\mathcal{O}}=\widehat{\beta}^{-1}\widehat{\phi(\phi^{-1}(\mathcal{O}))}\widehat{\beta}\} = \{\widehat{\beta}\in\widehat{B}^\times : \widehat{\phi(L)}\cap\widehat{\beta}\widehat{\mathcal{O}}\widehat{\beta}^{-1}=\widehat{\phi(\phi^{-1}(\mathcal{O}))}\}.$$

By Skolem-Noether theorem, the map $\beta\mapsto\beta^{-1}\phi\beta$ gives a bijection from $\phi(L)^\times\backslash\mathcal{E}$ to the set of optimal embedings $\phi^{-1}(\mathcal{O})\hookrightarrow\mathcal{O}$. Given $e_1\in\widehat{\mathcal{E}}$, if $[\tilde{h},e_1]=[\tilde{h},e_2]$ in $\widetilde{G}(\mathbb{Q})\backslash\mathcal{H}^\pm\times\widetilde{G}(\mathbb{A}_f)/\widetilde{K}$ with $e_2\in\widetilde{G}(\mathbb{A}_f)$, then there exist $a\in\widetilde{G}(\mathbb{Q})$ and $k\in\widetilde{K}=\widehat{\mathcal{O}}^\times$ such that $e_2=ae_1k\in\widehat{\mathcal{E}}$. Thus, $e\mapsto[\tilde{h},e]$ defines a bijection from $\phi(L)^\times\backslash\widehat{\mathcal{E}}/\widehat{\mathcal{O}}^\times$ to a set of CM points in $\widetilde{G}(\mathbb{Q})\backslash\mathcal{H}^\pm\times\widetilde{G}(\mathbb{A}_f)/\widetilde{K}$. Note that $\widetilde{T}(\mathbb{A}_f)\hookrightarrow\widehat{\mathcal{E}}$.

Lemma 3.1. *(1) When $\widehat{B}^\times = B^\times\widehat{\mathcal{O}}^\times$, the set of CM points $\{[\tilde{h},e]: e\in\widehat{\mathcal{E}}\}$ corresponds to $\mathcal{O}^\times$-conjugacy classes of optimal embeddings $\phi^{-1}(\mathcal{O})\hookrightarrow\mathcal{O}$.*

(2) When B is split at all finite primes of F, the set of CM points $\{[\tilde{h},e]: e\in\widehat{\mathcal{E}}\}$ is the image of the CM cycle $\widetilde{T}(\mathbb{Q})\backslash\{\tilde{h}\}\times\widetilde{T}(\mathbb{A}_f)/K_{\widetilde{T}}$, which has cardinality $h(\phi^{-1}(\mathcal{O}))$.

Proof. (1) Clearly $\mathcal{E}\subset\widehat{\mathcal{E}}$ and there is a natural map $\phi(L)^\times\backslash\mathcal{E}/\mathcal{O}^\times\to\phi(L)^\times\backslash\widehat{\mathcal{E}}/\widehat{\mathcal{O}}^\times$. This is injective since $B\cap\widehat{\mathcal{O}}^\times=\mathcal{O}^\times$. For any $\widehat{\beta}\in\widehat{B}^\times$, since $\widehat{B}^\times=B^\times\widehat{\mathcal{O}}^\times$, there is $\beta\in B^\times$ such that $\widehat{\beta}\widehat{\mathcal{O}}^\times=\beta\widehat{\mathcal{O}}^\times$. Note that the class $\beta\mathcal{O}^\times$ is well-defined, and $\widehat{\beta}\in\widehat{\mathcal{E}}$ if and only if $\beta\in\mathcal{E}$. Therefore, for $[\tilde{h},\widehat{\beta}]$ where $\widehat{\beta}\in\widehat{\mathcal{E}}$, pick $\beta\in\mathcal{E}$ such that $\widehat{\beta}\mathcal{O}^\times=\beta\mathcal{O}^\times$, then $[\tilde{h},\widehat{\beta}]=[\tilde{h},\beta]=[\beta^{-1}\cdot\tilde{h},1]$, where $\beta^{-1}\cdot\tilde{h}$ is defined by an optimal embedding $z\mapsto\beta^{-1}\phi(z)\beta$ of $\phi^{-1}(\mathcal{O})\hookrightarrow\mathcal{O}$.

(2) As in the proof of [Voi21, 30.4.7], there is a natural surjective map $\phi(L)^\times\backslash\widehat{\mathcal{E}}/\widehat{\mathcal{O}}^\times\to\widehat{\phi(L)}^\times\backslash\widehat{\mathcal{E}}/\widehat{\mathcal{O}}^\times$ whose fiber over the identity element is $\phi(L)^\times\backslash\widehat{\phi(L)}^\times/(\widehat{\phi(L)}^\times\cap\widehat{\mathcal{O}}^\times)\simeq Pic(\phi^{-1}(\mathcal{O}))$. There is a bijection $\widehat{\phi(L)}^\times\backslash\widehat{\mathcal{E}}/\widehat{\mathcal{O}}^\times\xrightarrow{\simeq}\{\widehat{\mathcal{O}}^\times$-conjugacy classes of optimal $\widehat{\phi^{-1}(\mathcal{O})}\hookrightarrow\widehat{\mathcal{O}}\}$. In the case B is split at all finite primes of F, since $\#\{GL_2(\mathcal{O}_{F_v})$-conjugacy classes of optimal $S\hookrightarrow M_2(\mathcal{O}_{F_v})\}=1$ for any $\mathcal{O}_{F_v}$-order S by [Voi21, 30.5.3], we have $\#\widehat{\phi(L)}^\times\backslash\widehat{\mathcal{E}}/\widehat{\mathcal{O}}^\times=\prod_v 1=1$.

□

Lemma 3.2. *When B is split at all finite primes of F, complex conjugation defines an involution on the CM cycle $\widetilde{T}(\mathbb{Q})\backslash\{\tilde{h}\}\times\widetilde{T}(\mathbb{A}_f)/K_{\widetilde{T}}$. In particular, if $h(\phi^{-1}(\mathcal{O}))$ is odd, then there is a real point on this CM cycle.*

Proof. For a CM point $[\tilde{h},t]$ where $\tilde{h}$ is induced by $\phi: L\hookrightarrow B$ and $t\in\widetilde{T}(\mathbb{A}_f)$, its complex conjugate is $[\iota\tilde{h},t]$ ([MS81]), where $\iota\tilde{h}$ is induced by $\overline{\phi}: L\hookrightarrow B$, $\overline{\phi}(z)=\phi(\bar{z})$. By the Skolem-Noether theorem, there exists $\beta\in B^\times$ such that $\overline{\phi}(\alpha)=\beta^{-1}\phi(\alpha)\beta$, then $\iota\tilde{h}(z)=\beta^{-1}\tilde{h}(z)\beta$ and $[\iota\tilde{h},t]=[\tilde{h},\beta t]=[\tilde{h},\bar{t}\beta]$. Since $\beta^{-1}\phi(L)\beta=\overline{\phi(L)}=\phi(L)$ and $\beta^{-1}\phi(\phi^{-1}(\mathcal{O}))\beta=\overline{\phi(\phi^{-1}(\mathcal{O}))}=\phi(\phi^{-1}(\mathcal{O}))=\phi(L)\cap\mathcal{O}$, we have $\beta\in\mathcal{E}$, then $\bar{t}\beta\in\widehat{\mathcal{E}}$, and the result follows from the second part of Lemma 3.1. □

Lemma 3.3. *Suppose F is a totally real number field with narrow class number 1 and B is a quaternion algebra over F unramified at all finite places and exactly one of the real places of F. If $\phi: L\hookrightarrow B$ is an embedding with $h(\phi^{-1}(\mathcal{O}))$ odd, then there is a unique real point on the CM cycle $\widetilde{T}(\mathbb{Q})\backslash\{\tilde{h}\}\times\widetilde{T}(\mathbb{A}_f)/K_{\widetilde{T}}$ defined by ϕ.*

Proof. Existence of a real point follows from Lemma 3.2. Note that $\widehat{B}^\times = B^\times \widehat{\mathcal{O}}^\times$ by (2.1.1). Then by Lemma 3.1, replacing ϕ by $\beta^{-1}\phi\beta$ and consequently $\tilde{h}$ by $\beta^{-1}\cdot\tilde{h}$ for $\beta \in \mathcal{E}$ does not change the CM cycle. Thus, we may assume $[\tilde{h}, 1]$ is a real point on this CM cycle. There exists some $\beta \in B^\times$ such that the complex conjugation of any point $[\tilde{h}, t]$ with $t \in \widetilde{T}(\mathbb{A}_f)$ is given by $[\tilde{h}, \beta t] = [\tilde{h}, \bar{t}\beta]$. Since $[\tilde{h}, 1]$ is real, we have $[\tilde{h}, 1] = [\tilde{h}, \beta]$, which implies $\beta \in \widetilde{T}(\mathbb{Q})\widetilde{K}$, and then $[\tilde{h}, \bar{t}\beta] = [\tilde{h}, \bar{t}]$.

By Lemma 3.5, there is an isomorphism of groups $i : \widetilde{T}(\mathbb{Q})\backslash\widetilde{T}(\mathbb{A}_f)/K_{\widetilde{T}} \xrightarrow{\simeq} \mathrm{Pic}(\phi^{-1}(\mathcal{O}))$ compatible with complex conjugation. Then $[\tilde{h}, t]$ is real, i.e., $[\tilde{h}, t] = [\tilde{h}, \bar{t}]$ if and only if $i(t) = \overline{i(t)}$. The norm map defines a homomorphism $\widetilde{T}(\mathbb{Q})\backslash\widetilde{T}(\mathbb{A}_f)/K_{\widetilde{T}} \simeq \mathrm{Pic}(\phi^{-1}(\mathcal{O})) \to \mathrm{Pic}(\mathcal{O}_F) = \mathrm{Cl}(F)$. Since $h(F) = 1$ and $\mathcal{O}_F \subset \phi^{-1}(\mathcal{O})$, for I an invertible ideal of $\phi^{-1}(\mathcal{O})$ we have $I\bar{I} = \mathrm{Nm}_{L/F}(I)\phi^{-1}(\mathcal{O})$ a principal ideal in $\phi^{-1}(\mathcal{O})$. Then the real CM points in this CM cycle correspond to the 2-torsion points in $\mathrm{Pic}(\phi^{-1}(\mathcal{O}))$. Under the assumption that $h(\phi^{-1}(\mathcal{O}))$ is odd, there is a unique 2-torsion point in $\mathrm{Pic}(\phi^{-1}(\mathcal{O}))$; thus there is a unique real CM point in this cycle. □

Lemma 3.4. *Let F be a number field with class number 1 and L be a quadratic extension of F. Then the maximal order of L is of the form $\mathcal{O}_L = \mathcal{O}_F[\alpha]$ for some $\alpha \in \mathcal{O}_L$, and any order R of K containing $\mathcal{O}_F$ is of the form $R = \mathcal{O}_F + f\mathcal{O}_K = \mathcal{O}_F[f\alpha]$ for some $f \in \mathcal{O}_F$; in particular, R has conductor $f\mathcal{O}_K$ and R is stable under the action of* $\mathrm{Gal}(L/F)$.

Proof. Since $\mathcal{O}_F$ is a PID, given an order $R \subseteq \mathcal{O}_K$ containing $\mathcal{O}_F$, let ω_1, ω_2 be a basis for $\mathcal{O}_K$ over $\mathcal{O}_F$ such that $a_1\omega_1, a_2\omega_2$ form a basis for R over $\mathcal{O}_F$ for some $a_1, a_2 \in \mathcal{O}_F$. We have $1 = b_1\omega_1 + b_2\omega_2$ for some $b_1, b_2 \in \mathcal{O}_F$ relatively prime, then $b_1c_1 + b_2c_2 = 1$ for some $c_1, c_2 \in \mathcal{O}_F$, and $1, \alpha := -c_2\omega_1 + c_1\omega_2$ form another basis for $\mathcal{O}_K$ over $\mathcal{O}_F$. Let $f = a_1a_2$, then $f\mathcal{O}_K \subset R$ and $\mathrm{disc}_{L/F}(R) = f^2\,\mathrm{disc}_{L/F}(\mathcal{O}_L)$. Since $\mathcal{O}_F + f\mathcal{O}_K \subseteq R$ and $\mathcal{O}_F + f\mathcal{O}_K = \mathcal{O}_F[f\alpha]$ has discriminant f^2d, we have $R = \mathcal{O}_F + f\mathcal{O}_K$. □

Lemma 3.5. *Let L/F be an extension of number fields, and $\mathfrak{f} \subset \mathcal{O}_F$ be an ideal. Let $R = \mathcal{O}_F + \mathfrak{f}\mathcal{O}_L$, which is an order of L containing $\mathcal{O}_F$, and $R_\mathfrak{p} = R \otimes_{\mathcal{O}_F} \mathcal{O}_{F_\mathfrak{p}}$ be the completion of R at a prime $\mathfrak{p} \subset \mathcal{O}_F$. Note that $\mathcal{O}_{L,\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_{L_\mathfrak{q}}$, so that $\prod_\mathfrak{p} R_\mathfrak{p}^\times \subset \prod_\mathfrak{p}\prod_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_{L_\mathfrak{q}}^\times \subset \mathbb{A}_{L,f}^\times$. There is an isomorphism $\mathbb{A}_{L,f}^\times/(L^\times \prod_\mathfrak{p} R_\mathfrak{p}^\times) \simeq \mathrm{Pic}(R)$.*

Proof. Write $\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})}$, then $\mathfrak{f}\mathcal{O}_L = \prod_\mathfrak{p}\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})m(\mathfrak{p})}$. Let $\mathbb{I}_{\mathfrak{f},R} := \{(\alpha_\mathfrak{q}) \in \mathbb{A}_{L,f}^\times : (\alpha_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}} \in R_\mathfrak{p}^\times \text{ for all } \mathfrak{p}|\mathfrak{f}\}$ and $L_{\mathfrak{f},R} := \{x \in L^\times : x \in R_\mathfrak{p}^\times \text{ for all } \mathfrak{p}|\mathfrak{f}\} = L^\times \cap \mathbb{I}_{\mathfrak{f},R}$. Since $R_\mathfrak{p} \supseteq \mathcal{O}_{F_\mathfrak{p}} + \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{f}\mathcal{O}_{L_\mathfrak{q}}$, we have $\mathbb{I}_{\mathfrak{f},R} \supset \mathbb{I}_{\mathfrak{f},1} := \{(\alpha_\mathfrak{q}) \in \mathbb{A}_{L,f}^\times : \alpha_\mathfrak{q} - 1 \in \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})m(\mathfrak{p})}\mathcal{O}_{L_\mathfrak{q}} \text{ for all } \mathfrak{q}|\mathfrak{f}\mathcal{O}_L\}$ and $L_{\mathfrak{f},R} \supset L_{\mathfrak{f},1} := \{x \in L^\times : v_\mathfrak{q}(x-1) \geq e(\mathfrak{q}/\mathfrak{p})m(\mathfrak{p}) \text{ for all } \mathfrak{q}|\mathfrak{f}\mathcal{O}_L\}$. The inclusion $\mathbb{I}_{\mathfrak{f},R} \hookrightarrow \mathbb{A}_{L,f}^\times$ defines an isomorphism $\mathbb{I}_{\mathfrak{f},R}/((L^\times \prod_\mathfrak{p} R_\mathfrak{p}^\times) \cap \mathbb{I}_{\mathfrak{f},R})) \xrightarrow{\simeq} \mathbb{A}_{L,f}^\times/(L^\times \prod_\mathfrak{p} R_\mathfrak{p}^\times)$, where $(L^\times \prod_\mathfrak{p} R_\mathfrak{p}^\times) \cap \mathbb{I}_{\mathfrak{f},R} = L_{\mathfrak{f},R}\prod_\mathfrak{p} R_\mathfrak{p}^\times$.

Let $J(R, \mathfrak{f})$ (resp. $J(\mathcal{O}_L, \mathfrak{f})$) be the subgroup of the group $J(R)$ (resp. $J(\mathcal{O}_L)$) of invertible ideals of R (resp. $\mathcal{O}_L$) generated by prime ideals not dividing $\mathfrak{f}\mathcal{O}_L$. Then $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_L$ defines an isomorphism $J(R, \mathfrak{f}) \xrightarrow{\simeq} J(\mathcal{O}_L, \mathfrak{f})$ ([Neu99, I.12.6, I.12.10]). The natural map $\mathbb{I}_{\mathfrak{f},R} \to J(\mathcal{O}_L, \mathfrak{f})$ has kernel $\prod_\mathfrak{p} R_\mathfrak{p}^\times$ and defines an isomorphism

$$\mathbb{I}_{\mathfrak{f},R}/(L_{\mathfrak{f},R}\prod_\mathfrak{p} R_\mathfrak{p}^\times) \xrightarrow{\simeq} J(\mathcal{O}_L, \mathfrak{f})/\{x\mathcal{O}_L : x \in L_\mathfrak{f}\}.$$

The inclusion $J(\mathcal{O}_L, \mathfrak{f}) \simeq J(R, \mathfrak{f}) \hookrightarrow J(R)$ defines an injection

$$J(\mathcal{O}_L, \mathfrak{f})/\{x\mathcal{O}_L : x \in L_\mathfrak{f}\} \to \mathrm{Pic}(R), \tag{3.1.3}$$

whose composition with $\mathrm{Pic}(R) \to \mathrm{Pic}(\mathcal{O}_L) \simeq J(\mathcal{O}_L, \mathfrak{f})/\{x\mathcal{O}_L \in J(\mathcal{O}_L, \mathfrak{f}) : x \in L\}$ is surjective. Then surjectivity of (3.1.3) follows from the exact sequence $(\mathcal{O}_L/\mathfrak{f}\mathcal{O}_L)^\times/(R/\mathfrak{f}\mathcal{O}_L)^\times \to \mathrm{Pic}(R) \to \mathrm{Pic}(\mathcal{O}_L) \to 1$ ([Neu99, I.12.9, I.12.11]) and surjectivity of $\{x \in L^\times : x\mathcal{O}_L \in J(\mathcal{O}_L, \mathfrak{f})\} \to (\mathcal{O}_L/\mathfrak{f}\mathcal{O}_L)^\times$. □

Lemma 3.6. *Let F be a totally real number field with odd narrow class number, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be distinct primes of F above 2. Let λ be a large enough totally positive prime of F such that $-\lambda$ is a square modulo 4, and R be an order of $L = F(\sqrt{-\lambda})$ with conductor $\mathfrak{f}$. If $\mathfrak{f} \cap \mathcal{O}_F \mid \mathfrak{p}_1 \cdots \mathfrak{p}_r$, then the class number $h(R)$ of R is odd.*

Proof. Given that $-\lambda \equiv m^2 \pmod 4$ for some $m \in \mathcal{O}_F$, the maximal order of L is $\mathcal{O}_L = \mathcal{O}_F[\frac{m+\sqrt{-\lambda}}{2}]$, and λ is the only prime of F that ramifies in the CM extension L/F. By [CH88, 13.7], the class number $h(L)$ is odd. For an $\mathcal{O}_F$-order R of L, we have

$$h(R) = \frac{h(L)}{(\mathcal{O}_L^\times : R^\times)} \frac{\#(\mathcal{O}_L/\mathfrak{f})^\times}{\#(R/\mathfrak{f})^\times}$$

(see for instance [Neu99, I.12.12]). By [CH88, 13.3, 13.4, 13.5], we have $\mathcal{O}_L^\times = \mu_L \mathcal{O}_F^\times$, where μ_L is the group of roots of unity in $L^\times$, so $(\mathcal{O}_L^\times : R^\times) = 1$ when $\mu_L = \{\pm 1\}$, which can be guaranteed if λ is large enough. From the injections $\mathcal{O}_F/(\mathfrak{f} \cap \mathcal{O}_F) \hookrightarrow R/\mathfrak{f} \hookrightarrow \mathcal{O}_L/\mathfrak{f}$, it suffices to show $\frac{\#(\mathcal{O}_L/\mathfrak{f})^\times}{\#(\mathcal{O}_F/(\mathfrak{f}\cap\mathcal{O}_F))^\times}$ is odd. Write $\mathfrak{f} \cap \mathcal{O}_F = \prod_{i=1}^r \mathfrak{p}_i^{\varepsilon_i}$ where $\varepsilon_1, \dots, \varepsilon_r \in \{0,1\}$, then $\#(\mathcal{O}_F/(\mathfrak{f} \cap \mathcal{O}_F))^\times = \prod_{i=1}^r (2^{f(\mathfrak{p}_i/2)} - 1)^{\varepsilon_i}$. Each $\mathfrak{p}_i$ is unramified in L, then $\mathfrak{f} \mid \prod_{i=1}^r \prod_{\mathfrak{q}|\mathfrak{p}_i} \mathfrak{q}^{\varepsilon_i}$ and $\#(\mathcal{O}_L/\mathfrak{f})^\times \mid \prod_{i=1}^r \prod_{\mathfrak{q}|\mathfrak{p}_i} (2^{f(\mathfrak{q}/2)} - 1)^{\varepsilon_i}$. Since

$$\frac{\prod_{\mathfrak{q}|\mathfrak{p}_i} (2^{f(\mathfrak{q}/2)} - 1)}{2^{f(\mathfrak{p}_i/2)} - 1} = \begin{cases} 2^{f(\mathfrak{p}_i/2)} - 1 & \text{if } \mathfrak{p}_i \text{ split in } L \\ 2^{f(\mathfrak{p}_i/2)} + 1 & \text{if } \mathfrak{p}_i \text{ inert in } L \end{cases}$$

is odd, we conclude that $h(R)$ is odd. □

3.7. When F has a unique prime $\mathfrak{p}$ above 2, and λ is a totally positive prime of F such that $-\lambda$ is a square modulo 4, we will consider the CM cycles corresoponding to the optimal embeddings of the maximal order $\mathcal{O}_L$ and a nonmaximal order $\mathcal{O}_F + \mathfrak{p}\mathcal{O}_L$. By Lemma 3.6, both orders have odd class numbers, and therefore, each corresponding CM cycle has a unique real point.

3.2. **Special endomorphisms.** Given $\phi : L = F(\sqrt{-\lambda}) \hookrightarrow B$, we have $v = \phi(\sqrt{-\lambda}) \in V$ and denote by V_v its orthogonal complement in V as F-vector space. The inclusion $V \hookrightarrow B$ induces an F-algebra isomorphism $C_F^+(V) \xrightarrow{\simeq} B$, under which $C_F^+(V_v) \xrightarrow{\simeq} \phi(L)$. Thus, we have $\mathrm{Res}_{F/\mathbb{Q}} \mathrm{GSpin}(V_v, F) \hookrightarrow \mathrm{Res}_{F/\mathbb{Q}} \mathrm{GSpin}(V, F)$ that agrees with $\phi : L \hookrightarrow B$.

The quadratic space $V_v \otimes_{F,\sigma} \mathbb{R}$ has signature $(2,0)$ for $\sigma \neq \rho$ and $(0,2)$ for $\sigma = \rho$. Let $\{e_1, e_2\}$ be an $\mathbb{R}$-basis of $V_v \otimes_{F,\rho} \mathbb{R}$ such that the matrix of the bilinear form is $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. The $\mathbb{R}$-algebra homomorphism $\mathbb{C} \to C_F^+(V_v) \otimes_{F,\rho} \mathbb{R}$ defined by the oriented negative 2-plane $\langle e_1, e_2 \rangle$ (resp. $\langle e_2, e_1 \rangle$) is $a + bi \mapsto a + be_1e_2$ (resp. $a + be_2e_1$). Its restriction to $\mathbb{C}^\times$ gives a homomorphism $\mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \to (\mathrm{Res}_{F/\mathbb{Q}} \mathrm{GSpin}(V, F))_{\mathbb{R}}$. Under the isomorphism $C_F^+(V) \otimes_{F,\rho} \mathbb{R} \simeq B \otimes_{F,\rho} \mathbb{R}$, we have

$$\{e_1e_2, e_2e_1\} = \{\frac{1}{\sqrt{\lambda}} v, -\frac{1}{\sqrt{\lambda}} v\}. \tag{3.2.1}$$

Therefore, the homomorphism $\mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \to \widetilde{G}_{\mathbb{R}}$ defined by the special endomorphism v is $\tilde{h}$ or $\iota\tilde{h}$ defined above.

3.3. **Definition field.** Let $\tilde{\mu} = \mu_{\tilde{h}} : \mathbb{G}_{m,\mathbb{C}} \to \widetilde{T}_{\mathbb{C}}$ be the cocharacter defined by $\tilde{\mu}(z) = \tilde{h}_{\mathbb{C}}(z, 1)$. Let T be the image of $\widetilde{T}$ in G and μ (resp. h) be the composition $\mathbb{G}_{m,\mathbb{C}} \xrightarrow{\tilde{\mu}} \widetilde{T}_{\mathbb{C}} \to T_{\mathbb{C}}$ (resp. $\mathrm{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \xrightarrow{\tilde{h}} \widetilde{T}_{\mathbb{R}} \to T_{\mathbb{R}}$). Since $\tilde{\mu}$ corresponds to an embedding $\tilde{\rho} : L \hookrightarrow \mathbb{C}$ extending $\rho : F \hookrightarrow \mathbb{R}$, the cocharacters are defined over $\tilde{\rho}(L)$.

Suppose λ is an unramified prime of F above p and let $K' \subset \widetilde{T}(\mathbb{A}_f)$ be a compact open subgroup such that K'_p is maximal and K'^p is small enough such that $\mathrm{Sh}_{K'}(T, \{h\}) := T(\mathbb{Q}) \backslash \{h\} \times T(\mathbb{A}_f)/K'$ is a fine moduli space for abelian varieties with Hodge cycles and sufficiently high level structure away from p. By definition of canonical model, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ acts on $\mathrm{Sh}_{K'}(T, \{h\})$ by

$$\sigma[h, t] = [h, r(T, \mu)(s)t] \text{ where } s \in \mathbb{A}_L^\times \text{ with } \mathrm{art}(s) = \sigma|_{L^{ab}},$$

and the homomorphism $r(T, \mu) : \mathrm{Res}_{L/\mathbb{Q}} \mathbb{G}_m = \widetilde{T} \to T$ is the natural surjection under $T \simeq \widetilde{T}/T_F^1$. Then there exists an abelian extension L'/L, unramified at the primes above p, such that $\mathrm{Gal}(\overline{\mathbb{Q}}/L')$ fixes $\mathrm{Sh}_{K'}(T, \{h\})$. In particular, the ramification index of p in L' is 2. Since there are no nontrivial automorphisms of the abelian varieties with level structure parametrized by $\mathrm{Sh}_{K'}(T, \{h\})$, the abelian varieties are defined over L'. Moreover, since $\mathrm{Gal}(\overline{\mathbb{Q}}/L')$ fixes μ, it fixes the special endomorphism.

3.4. **Supersinigular reduction.**

Lemma 3.8. *Let E be a CM field. Suppose that A is an abelian variety of CM type (E,Φ) over a number field $K\subset\overline{\mathbb{Q}}$. Let (E^*,Φ^*) be the reflex CM type. Suppose $E\subseteq \mathrm{End}^0(A/K)$ (so that $E^*\subseteq K$). Assume that $\mathfrak{p}$ is a prime of K of with residue field k of characteristic p such that A has good reduction A_k at $\mathfrak{p}$. Let $\mathfrak{q}=\mathfrak{p}\cap E^{*+}$, where E^{*+} is the totally real subfield of E^*. If $\mathfrak{q}$ is inert or ramified in E^*, then A_k is supersingular.*

Proof. After passing to a finite extension, we may assume K contains all conjugates of E. Fix a p-adic valuation v of a normal closure $\tilde{E}$ of E. Let $\mathfrak{q}'=\mathfrak{p}\cap E^*$. By Shimura-Taniyama, there exists an element $\pi\in\mathcal{O}_E$ inducing the Frobenius endomorphism on A_k and the Newton slopes are $\frac{v(\sigma(\pi))}{v(p^{f(\mathfrak{p}/p)})}$ for $\sigma\in\mathrm{Hom}(E,\overline{\mathbb{Q}})$, where

$$(\pi)=N_{K,\Phi}(\mathfrak{p})=N_\Phi(\mathrm{Nm}_{K/E^*}\mathfrak{p})=N_\Phi(\mathfrak{q}'^{f(\mathfrak{p}/\mathfrak{q}')}).$$

For a sufficiently large integer N, there exists $\alpha\in\mathcal{O}_{E^*}$ such that $\mathfrak{q}'^N=(\alpha)$. Then

$$\frac{v(\sigma(\pi))}{v(p^{f(\mathfrak{p}/p)})}=\frac{v(\sigma(N_\Phi(\alpha^{f(\mathfrak{p}/\mathfrak{q}')})))}{v(p^{Nf(\mathfrak{p}/p)})}=\frac{v(\sigma(N_\Phi(\alpha)))}{v(p^{Nf(\mathfrak{q}'/p)})}.$$

With E a subfield of $\overline{\mathbb{Q}}$, we have $N_\Phi: E^{*\times}\to E^\times$ described by $N_\Phi(a)=\prod_{\psi\in\Phi^*}\psi(a)$. Let $\tilde{\sigma}\in\mathrm{Aut}(\tilde{E})$ such that $\tilde{\sigma}|_E=\sigma$. If $\mathfrak{q}$ is inert or ramified in E^*, then $\mathfrak{q}'^N=(\alpha)=(c\alpha)$ and $v\circ\tilde{\sigma}\circ\psi(\alpha)=v\circ\tilde{\sigma}\circ c\circ\psi(\alpha)$ for any $\psi: E^*\hookrightarrow\overline{\mathbb{Q}}$, so that $v(\sigma(N_\Phi(\alpha)))=v(\sigma(\prod_{\psi\in\Phi^*}\psi(a)))=v(\sigma(\prod_{\psi\in\Phi^*}c\psi(a)))=v(\sigma(cN_\Phi(\alpha)))$, where c denotes the unique complex conjugation on the CM fields. On the other hand, $N_\Phi(\alpha)\cdot cN_\Phi(\alpha)=\mathrm{Nm}_{E^*/\mathbb{Q}}(\alpha)$ and $v(\mathrm{Nm}_{E^*/\mathbb{Q}}(\alpha))=v(\mathrm{Nm}_{E^*/\mathbb{Q}}\mathfrak{q}'^N)=v(p^{f(\mathfrak{q}'/p)N})$. Thus, the Newton slopes are all $\frac{1}{2}$. □

Corollary 3.9. *Let $E=E_1\times\cdots\times E_m$ be a CM algebra and E^* be its reflex field. Suppose that A is a CM abelian variety over a number field $K\subset\overline{\mathbb{Q}}$ with $E\subseteq\mathrm{End}^0(A/K)$. Assume that $\mathfrak{p}$ is a prime of K with residue field k of characteristic p such that A has good reduction A_k at $\mathfrak{p}$. Let $\mathfrak{q}=\mathfrak{p}\cap E^{*+}$, where E^{*+} is the totally real subfield of E^*. Suppose $E^*\subseteq L$, where L is a CM field and $\mathfrak{P}$ a prime of its totally real subfield L^+ above $\mathfrak{q}$. If $\mathfrak{P}$ is inert or ramified in L, then A_k is supersingular.*

Proof. The abelian variety is isogenous to $A_1\times\cdots\times A_m$ where each A_i is CM by E_i, and after passing to a finite extension, we may assume each A_i is defined over K with $E_i\subseteq\mathrm{End}^0(A_i/K)$. Since $E_i^*\subseteq E^*$, we reduce to the case E is a CM field.

Note that $L=L^+E^*$ and if $\mathfrak{P}$ is inert or ramified in L, then $\mathfrak{q}$ is inert or ramified in E^*, and the result follows from the lemma. □

3.10. For a CM abelian variety A constructed from $L=F(\sqrt{-\lambda})\hookrightarrow B$, since the Hodge cocharacter factors through $\mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_m$, elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that fixes the Hodge cocharacter fixes the CM type. It follows that $L\supseteq E^*$, and if a prime $\mathfrak{P}$ of F is inert or ramified in L, then A has supersingular reduction at primes above $\mathfrak{P}$.

4. Non-Archimedean place

Recall that in [Elk87], the polynomial $P_l(x)P_{4l}(x)$ is a square modulo l and our goal is to establish a similar result by pairing the roots of the polynomials. In this section, we prove Proposition 4.6 and Proposition 4.8, which together show that CM liftings of a closed point $x\in\mathscr{S}_{K_0}(k)$ occur in pairs when we consider liftings to cycles corresponding to all orders containing $\mathcal{O}_F[\sqrt{-\lambda}]$. Proposition 4.6 is the easier case where x has no self-automorphisms of even order. The main input is the description of the local deformation space of abelian varieties parametized by a GSpin Shimura variety as the deformation space of isotropic lines in [MP16, 5.16], which we adapt to our setting in Lemma 4.2 by considering the F-linear structure on $\boldsymbol{L}_{\mathrm{cris},x}$ defined by $\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}$. In addition, we define an F-linear structure on the space of special quasi-endomorphisms $V(\mathcal{A}_x)$ in section 4.2. When $\mathcal{A}_x$ is supersingular, the structure of $V(\mathcal{A}_x)$ as a quadratic space over F is described in Lemma 4.3 and Lemma 4.4.

Extra work is required when x admits an even order automorphism, analogous to the case $j=1728$ in [Elk87, Elk89]. In this situation, Lemma 4.5 and Lemma 4.10 give a pairing of the special endomorphsims,

which in turn yields a pairing of liftings in Proposition 4.8. Moreover, Proposition 4.8 provides necessary information on the intersection number of these cycles to address the complication caused by lack of cusps.

Let p be an odd prime unramified in F. Let $k = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$ and $W = W(k)$ be its ring of Witt vectors. Denote by Art_W the category of Artinian local algebras over W. Fix an embedding $\iota : \overline{W[p^{-1}]} \hookrightarrow \mathbb{C}$ and let $\rho' : F \hookrightarrow W[p^{-1}]$ such that $\rho = \iota \circ \rho'$.

4.1. **Lifting of abelian varieties.** Let $x \in \mathscr{S}_{K_pK^p}(k)$ be a closed point and $\widehat{U}_x$ be the completion of $\mathscr{S}_{K_pK^p}$ at x. We follow [MP16, 5.15, 5.16] to relate the infinitesimal deformations of x to the liftings of certain isotropic lines in the quadratic spaces associated to $\boldsymbol{L}_{\mathrm{cris},x}$, and then apply the Grothendieck existence theorem to lift a compatible system of such deformations to a certain finite extension of W.

For $\mathscr{O}$ in Art_W, let $\boldsymbol{H}_{\mathscr{O}} \simeq H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W \mathscr{O}$ be the $\mathscr{O}$-module obtained by evaluating $H^1_{\mathrm{cris}}(\mathcal{A}_x/W)$ on $\operatorname{Spec} \mathscr{O}$, and $\boldsymbol{L}_{\mathscr{O}} \subset \mathrm{End}(\boldsymbol{H}_{\mathscr{O}})$ be the corresponding quadratic space over $\mathscr{O}$. If $\mathcal{A}_{\tilde{x}}$ is an abelian scheme over $\mathscr{O}$ lifting $\mathcal{A}_x$, then via the canonical identification $H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/\mathscr{O}) \xrightarrow{\simeq} \boldsymbol{H}_{\mathscr{O}}$, the Hodge filtration on $H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/\mathscr{O})$ corresponds to a direct summand of $\mathrm{Fil}^1 \boldsymbol{H}_{\mathscr{O}} \subset \boldsymbol{H}_{\mathscr{O}}$. If $\mathscr{O}_2 \twoheadrightarrow \mathscr{O}_1$ is a surjection in Art_W whose kernel admits nilpotent divided powers and $\mathcal{A}_{x_1}$ is an abelian scheme over $\mathscr{O}_1$ lifting x, then this gives a natural bijection

(4.1.1)
$$\left\{ \begin{array}{c} \text{Isomorphism classes of abelian schemes over } \mathscr{O}_2 \\ \text{lifting } \mathcal{A}_{x_1} \end{array} \right\} \xrightarrow{\simeq} \left\{ \begin{array}{c} \text{Direct summands } \mathrm{Fil}^1 \boldsymbol{H}_{\mathscr{O}_2} \subset \boldsymbol{H}_{\mathscr{O}_2} \\ \text{lifting } \mathrm{Fil}^1 \boldsymbol{H}_{\mathscr{O}_1} \end{array} \right\}$$

by Serre-Tate theory ([Kat81, 1.2.1]) and Grothendieck-Messing theory ([Mes72, V. 1.6])[6].

We recall Grothendieck existence theorem for the convenience of the reader.

Theorem 4.1 (Grothendieck [Con04, 3.4])**.** *Let R be a noetherian ring which is separated and complete with respect to the I-adic topology for an ideal I. Let X and Y be proper R-schemes, and R_n, X_n, Y_n the reductions modulo I^{n+1}. The natural map of sets $\mathrm{Hom}_R(X,Y) \to \varprojlim \mathrm{Hom}_{R_n}(X_n, Y_n)$ is bijective.*

Moreover, if $\{X_n\}$ is a compatible system of proper schemes over the R_n's and $\mathscr{L}_0$ is an ample line bundle on X_0 which lifts compatibly to a line bundle $\mathscr{L}_n$ on each X_n, then there exists a pair $(X, \mathscr{L})$ consisting of a proper R-scheme and ample line bundle which comaptibly reduces to each $(X_n, \mathscr{L}_n)$, and this data over R is unique up to unique isomorphism.

Lemma 4.2. *Suppose p is an odd prime unramified in F. Let $k = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$ and $x \in \mathscr{S}_{K_pK^p}(k)$. Suppose E is a finite extension of $W[p^{-1}]$ of ramification index $e \leq p-1$ with uniformizer ϖ. Let*

$$\mathrm{Iso} := \{\textit{isotropic line } \langle w \rangle \subset \boldsymbol{L}_{\mathrm{cris},x} \otimes_W E : (\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x} \otimes 1)(w) = \rho'(\epsilon_i) w\}.$$

Then there is a natural bijection

$$\left\{\tilde{x} \in \mathscr{S}_{K_pK^p}(E) \textit{ lifting } x\right\} \xrightarrow{\simeq} \left\{\mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E) \in \mathrm{Iso} \textit{ lifting } \mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},x}\right\}. \tag{4.1.2}$$

Moreover, if $v \in L(\mathcal{A}_x)$ is a special endomorphism, then there is a natural bijection

$$\left\{ \begin{array}{c} \tilde{x} \in \mathscr{S}_{K_pK^p}(E) \textit{ lifting } x, \\ \tilde{v} \in L(\mathcal{A}_{\tilde{x}}) \textit{ lifting } v \end{array} \right\}^{7} \xrightarrow{\simeq} \left\{ \begin{array}{c} \mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E) \in \mathrm{Iso} \textit{ lifting } \mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},x} \\ \textit{and orthogonal to } v \end{array} \right\}. \tag{4.1.3}$$

Proof. For any lift $\tilde{x}$ of x, via the comparison $H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/E) \xrightarrow{\simeq} H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W E$, the Hodge filtration $\mathrm{Fil}^1 H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/E) \subset H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/E)$ gives a filtration $\mathrm{Fil}^1(H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W E) \subset H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W E$ that is split by a cocharacter $\mu : \mathbb{G}_{m,E} \to G_W \otimes_W E$. Since $G_W \subset \mathrm{GSpin}(\boldsymbol{L}_{\mathrm{cris},x})$, it induces a splitting

$$\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E = \mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E) \oplus (\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E)^0 \oplus \overline{\mathrm{Fil}}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E),$$

where $\mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E)$ is an isotropic line such that

$$\mathrm{Fil}^1(H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W E) = \ker(\mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E)) = \mathrm{im}(\mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x} \otimes_W E)). \tag{4.1.4}$$

[6]Serre-Tate theory and Grothendieck-Messing theory apply to surjections $\mathscr{O} \to \overline{\mathscr{O}}$ such that p is nilpotent in $\mathscr{O}$ and the kernel I admits nilpotent divided powers. If $k = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$, $W = W(k)$, and a finite extension E of $W[p^{-1}]$ has ramification index e with uniformizaing parameter ϖ, then $(\mathcal{O}_E, (\varpi))$ has a P.D. structure iff $e \leq p-1$ ([BO78], 3.2.3). For the liftings we will consider, where p is odd and $e \leq 2$, the kernel of $\mathcal{O}_E/(\varpi^n) \twoheadrightarrow \mathcal{O}_E/(\varpi)$ always admits nilpotent divided powers.

[7]If $\tilde{v}$ exists, then it is unique, since $\tilde{v} \in L(\mathcal{A}_{\tilde{x}})$ lifts $v \in L(\mathcal{A}_x)$ and $L(\mathcal{A}_{\tilde{x}}) \hookrightarrow L(\mathcal{A}_x)$.

Note that $\mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x}\otimes_W E)$ lifts $\mathrm{Fil}^1\boldsymbol{L}_{\mathrm{dR},x}$ as $\mathrm{Fil}^1(H^1_{\mathrm{cris}}(\mathcal{A}_x/W)\otimes_W E)$ lifts $\mathrm{Fil}^1 H^1_{\mathrm{dR}}(\mathcal{A}_x/k)$. By construction, the filtration on $H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}}/E)\otimes_{E,\iota}\mathbb{C}\simeq H^1_B(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}),\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{C}$ is induced by a cocharacter $\mu_{\mathbf{h}}$ defined by a Hodge structure $\mathbf{h}\in X$ such that $\mathrm{Fil}^1 H_{\mathbb{C}}=\ker(\mathrm{Fil}^1 V_{\mathbb{C}})$. The action of $\boldsymbol{\pi}_{\epsilon_i,B,\iota(\tilde{x})}\otimes 1$ on $\mathrm{Fil}^1 V_{\mathbb{C}}$ is scalar multiplication by $\rho(\epsilon_i)$. If w is a generator of the isotropic line $\mathrm{Fil}^1 V_{\mathrm{dR},\tilde{x}}$, then since (2.2.1) takes $\boldsymbol{\pi}_{\epsilon_i,\mathrm{dR},\tilde{x}}\otimes 1$ to $\boldsymbol{\pi}_{\epsilon_i,B,\iota(\tilde{x})}\otimes 1$, we have $\boldsymbol{\pi}_{\epsilon_i,\mathrm{dR},\tilde{x}}(w)\otimes_{E,\iota}1=w\otimes_{E,\iota}\rho(\epsilon_i)$, i.e., $\boldsymbol{\pi}_{\epsilon_i,\mathrm{dR},\tilde{x}}(w)=\rho'(\epsilon_i)w$.

To show the map (4.1.2) is a bijection, we work successively with the thicknings $\mathcal{O}_E/(\varpi^n)\twoheadrightarrow\mathcal{O}_E/(\varpi^{n-1})$ following the proof of [MP16, 5.16] and then apply Grothendieck existence theorem. Let Iso_n denote the set of isotropic lines in $\boldsymbol{L}_{\mathrm{cris},x}\otimes_W(\mathcal{O}_E/(\varpi^n))$ on which each $\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}\otimes 1$ acts as $\rho'(\epsilon_i)\otimes 1$. Suppose $x_{n-1}\in\widehat{U}_x(\mathcal{O}_E/(\varpi^{n-1}))$ gives rise to $l_{n-1}\in\mathrm{Iso}_{n-1}$ that lifts $\mathrm{Fil}^1\boldsymbol{L}_{\mathrm{dR},x}$, and consider

$$\left\{x_n\in\widehat{U}_x(\mathcal{O}_E/(\varpi^n))\text{ lifting }x_{n-1}\right\}\to\{l_n\in\mathrm{Iso}_n\ \text{ lifting }l_{n-1}\}\,. \tag{4.1.5}$$

Injectivity of (4.1.5) follows from (4.1.1) and the correspondence

$$\mathrm{Fil}^1\boldsymbol{H}_{\mathcal{O}_E/(\varpi^n)}=\ker(\mathrm{Fil}^1(\boldsymbol{L}_{\mathrm{cris},x}\otimes_W(\mathcal{O}_E/(\varpi^n)))).$$

Then we can prove (4.1.5) is a bijection by showing both sides are vector spaces over $\mathcal{O}_E/(\varpi)$ of the same dimension. Since $\widehat{U}_x$ is formally smooth of relative dimension 1 over W ([Kis10, 2.3.5]), the left-hand side of (4.1.5) is a 1-dimensional vector space over $\mathcal{O}_E/(\varpi)$. On the other hand, since $\boldsymbol{L}_{\mathrm{cris},x}$ is non-degenerate modulo (ϖ), there exists $l_n=\langle w_n\rangle\in\mathrm{Iso}_n$ lifting l_{n-1} and the right-hand side of (4.1.5) is $\{\langle w_n+\varpi^{n-1}u\rangle\subset\boldsymbol{L}_{\mathrm{cris},x}\otimes_W(\mathcal{O}_E/(\varpi^n)):\varpi^{n-1}u\perp w_n,(\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}\otimes 1)(u)=\rho'(\epsilon_i)u\}\simeq\{u\in\boldsymbol{L}_{\mathrm{cris},x}\otimes_W(\mathcal{O}_E/(\varpi)):u\in l_1^{\perp},(\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}\otimes 1)(u)=\rho'(\epsilon_i)u\}/l_1$, which is a 1-dimensional $\mathcal{O}_E/(\varpi)$-vector space. Hence (4.1.5) is a bijection. Applying Theorem 4.1 to a compatible system of polarized abelian varieties associated to $\{l_n\}$, the map (4.1.2) is a bijection.

For (4.1.3), by Theorem 4.1, given a lift $\tilde{x}\in\mathscr{S}_{K_pK^p}(E)$ of x, there is $\tilde{v}\in L(\mathcal{A}_{\tilde{x}})$ lifting v if v lifts to a compatible system $\{v_n\}$, where v_n is an endomorphism of the reduction of $\mathcal{A}_{\tilde{x}}$ modulo (ϖ^n). With $x_n\in\widehat{U}_x(\mathcal{O}_E/(\varpi^n))$ lifting x, we have $v\in L(\mathcal{A}_x)$ lifts to an endomorphism of $\mathcal{A}_{x_n}$ if and only if its crystalline realization $v_{\mathrm{cris},n}\in\boldsymbol{L}_{\mathcal{O}_E/(\varpi^n)}$ preserves the Hodge filtration $\mathrm{Fil}^1\boldsymbol{H}_{\mathcal{O}_E/(\varpi^n)}$ if and only if $v_{\mathrm{cris},n}\in\mathrm{Fil}^0\boldsymbol{L}_{\mathcal{O}_E/(\varpi^n)}$ if and only if $v_{\mathrm{cris},n}$ is orthogonal to $\mathrm{Fil}^1\boldsymbol{L}_{\mathcal{O}_E/(\varpi^n)}$. □

4.2. **Structure of the space of special endomorphisms.** Let $x\in\mathscr{S}_{K_pK^p}(k)$ be a closed point and $v\in L(\mathcal{A}_x)$ be a special endomorphism. By Lemma 4.2 and its proof, there exists some lift $\tilde{x}$ of x with special endomorphism $\tilde{v}$ lifting v. The abelian variety $\mathcal{A}_{\iota(\tilde{x})}$ defines a Hodge structure $V\otimes_{\mathbb{Q}}\mathbb{C}=V^{-1,1}\oplus V^{0,0}\oplus V^{1,-1}$, where $L(\mathcal{A}_{\tilde{x}})\otimes_{\mathbb{Z}}\mathbb{Q}\simeq V\cap V^{0,0}$ has an F-linear structure defined by the absolute Hodge cycles $\boldsymbol{\pi}_{\epsilon_i}$. Therefore, there is an $\mathcal{O}_F$-linear structure on the sublattice $L(\mathcal{A}_{\tilde{x}})\hookrightarrow L(\mathcal{A}_x)$ such that $\boldsymbol{\pi}_{\epsilon_i}(\tilde{v})$ agrees with $\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}(v_{\mathrm{cris}})$ in $\boldsymbol{L}_{\mathrm{cris},x}$. Applying this process to a basis for $L(\mathcal{A}_x)$ shows that it is stable under the $\mathcal{O}_F$-action on $\boldsymbol{L}_{\mathrm{cris},x}$, thereby endowing $L(\mathcal{A}_x)$ with an $\mathcal{O}_F$-linear structure compatible with that on $\boldsymbol{L}_{cris,x}$ and $\boldsymbol{L}_{\ell,x}$ for $\ell\neq p$.

Let $V(\mathcal{A}_x)=L(\mathcal{A}_x)\otimes_{\mathbb{Z}}\mathbb{Q}$ and Q' denote the quadratic form on $V(\mathcal{A}_x)$ over $\mathbb{Q}$. Since $\mathrm{Tr}_{F/\mathbb{Q}}$ is perfect, and for $u,w\in L(\mathcal{A}_x)$, $[\epsilon_i u,w]_{Q'}=[\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}u_{\mathrm{cris}},w_{\mathrm{cris}}]_{\mathrm{cris}}=[u_{\mathrm{cris}},\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}w_{\mathrm{cris}}]_{\mathrm{cris}}=[u,\epsilon_i w]_{Q'}$, there is a quadratic form Q'_F on $V(\mathcal{A}_x)$ over F determined by $\mathrm{Tr}_{F/\mathbb{Q}}(f[u,w]_{Q'_F})=[fu,w]_{Q'}$ for all $f\in F$. In particular, $Q'=\mathrm{Tr}_{F/\mathbb{Q}}\circ Q'_F$. The orthogonal direct sum decompositions

$$(V(\mathcal{A}_x)\otimes_{\mathbb{Q}}W[p^{-1}],Q')=\bigoplus_{\sigma':F\hookrightarrow W[p^{-1}]}(V(\mathcal{A}_x)\otimes_{F,\sigma'}W[p^{-1}],\sigma'\circ Q'_F),$$

$$\boldsymbol{L}_{\mathrm{cris},x}[p^{-1}]\simeq(V\otimes_{\mathbb{Q}}W[p^{-1}],Q)=\bigoplus_{\sigma':F\hookrightarrow W[p^{-1}]}(V\otimes_{F,\sigma'}W[p^{-1}],\sigma'\circ Q_F)$$

and the F-linear isometric embedding

$$V(\mathcal{A}_x)\otimes_{\mathbb{Q}}W[p^{-1}]\hookrightarrow\boldsymbol{L}_{\mathrm{cris},x}[p^{-1}] \tag{4.2.1}$$

induce an isometric embedding

$$(V(\mathcal{A}_x)\otimes_{F,\sigma'}W[p^{-1}],\sigma'\circ Q'_F)\hookrightarrow(V\otimes_{F,\sigma'}W[p^{-1}],\sigma'\circ Q_F) \tag{4.2.2}$$

of quadratic spaces over $W[p^{-1}]$ for each $\sigma' : F \hookrightarrow W[p^{-1}]$. Moreover, $(V(\mathcal{A}_{\tilde{x}}), Q_F) \hookrightarrow (V(\mathcal{A}_x), Q'_F)$ is isometric for any lift $\tilde{x}$ of x. Similarly, for $\ell \neq p$, we have orthogonal direct sum decompositions

$$(V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell, Q') = \bigoplus_{v|\ell} (V(\mathcal{A}_x) \otimes_F F_v, \mathrm{Tr}_{F_v/\mathbb{Q}_\ell} \circ Q'_F),$$

$$\boldsymbol{V}_{\ell,x} \simeq (V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell, Q) = \bigoplus_{v|\ell} (V \otimes_F F_v, \mathrm{Tr}_{F_v/\mathbb{Q}_\ell} \circ Q_F)$$

of quadratic spaces over $\mathbb{Q}_\ell$. Since the natural embedding

$$V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \boldsymbol{V}_{\ell,x} \tag{4.2.3}$$

is $(F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$-linear by construction and $\mathrm{Tr}_{F_v/\mathbb{Q}_\ell}$ is perfect, we have an isometric embedding

$$(V(\mathcal{A}_x) \otimes_F F_v, Q'_F) \hookrightarrow (V \otimes_F F_v, Q_F) \tag{4.2.4}$$

of quadratic spaces over F_v for each $v|\ell$. The next lemma shows that (4.2.1) – (4.2.4) are isomorphisms when $\mathcal{A}_x$ is supersingular.

Lemma 4.3. *Suppose $\mathcal{A}_x$ is supersingular.*

(1) As a quadratic space over $\mathbb{Q}$, $V(\mathcal{A}_x)$ is positive definite with the same dimension ($= 3[F : \mathbb{Q}]$) and determinant as V, but with Hasse invariant

$$\epsilon(V(\mathcal{A}_x)_{\mathbb{Q}_\ell}) = \begin{cases} \epsilon(V_{\mathbb{Q}_\ell}) = 1 & \text{if } \ell \neq p \\ -\epsilon(V_{\mathbb{Q}_\ell}) = -1 & \text{if } \ell = p \end{cases}$$

for all finite rational primes ℓ.

(2) As a quadratic space over F, $V(\mathcal{A}_x)$ is positive definite at all real places with the same dimension ($= 3$) as V, and with Hasse invariant $\epsilon(V(\mathcal{A}_x)_{F_v}) = \epsilon(V_{F_v}) = 1$ for all finite primes $v \nmid p$.

Proof. Positive-definiteness follows from [MP16, 5.12]. The Tate-conjecture ([MP15, 6.4]) implies that under the natural isometric embedding $V(\mathcal{A}_x)_{\mathbb{Q}_p} = L(\mathcal{A}_x) \otimes_{\mathbb{Z}} \mathbb{Q}_p \hookrightarrow \boldsymbol{L}_{\mathrm{cris},x} \otimes_W W(\bar{k})[p^{-1}]$, the subspace $V(\mathcal{A}_x)_{\mathbb{Q}_p}$ consists of Frobenius invariant vectors in the isocrystal $\boldsymbol{L}_{\mathrm{cris},x} \otimes_W W(\bar{k})[p^{-1}]$, which is a $\mathbb{Q}_p$-quadratic space with the same dimension and determinant as $V_{\mathbb{Q}_p}$, but has Hasse invariant -1 by [HP17, 4.2.5]. For $\ell \neq p$, the natural isometric embedding $V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \boldsymbol{V}_{\ell,x} \simeq V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is an isomorphism for the dimension reason.

Since $Q' = \mathrm{Tr}_{F/\mathbb{Q}} \circ Q'_F$, we have an orthogonal direct sum decomposition

$$V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{R} = \oplus_{\sigma:F \hookrightarrow \mathbb{R}} V(\mathcal{A}_x) \otimes_{F,\sigma} \mathbb{R}$$

of quadratic space spaces over $\mathbb{R}$, then positive definiteness of Q'_F follows from positive-definiteness of Q'. Similarly, if $\ell \neq p$, then the natural map $V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \boldsymbol{V}_{\ell,x} \simeq V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is an F-linear isometry of $\mathbb{Q}_\ell$-quadratic spaces; therefore, $V(\mathcal{A}_x) \otimes_F F_v \simeq V \otimes_F F_v$ for all prime $v|\ell$. □

Lemma 4.4. *Suppose p is totally split in F. If $\mathcal{A}_x$ is supersingular, then $V(\mathcal{A}_x)$ is a quadratic space over F of dimension 3 and determinant 1. Morevoer, the Hasse invariant of $V(\mathcal{A}_x)$ is -1 at $\mathfrak{p}$ over p corresponding to $\rho' : F \hookrightarrow W[p^{-1}]$, and 1 at other finite primes of F.*

Proof. When p is totally split in F, fix a $\mathbb{Z}_p$ basis $x_1, \ldots, x_n$ ($n = 3[F : \mathbb{Q}]$) of $L \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \oplus_{\sigma':\mathcal{O}_F \to \mathbb{Z}_p} L \otimes_{\mathcal{O}_F,\sigma'} \mathbb{Z}_p$ for which $x_1, x_2, x_3 \in L \otimes_{\mathcal{O}_F,\rho'} \mathbb{Z}_p$ and the matrix of inner products has the form

$$\begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & * & & & & \\ & & & * & & & \\ & & & & \ddots & & \\ & & & & & * & \end{pmatrix}.$$

As in [HP17, 4.2.1], this defines a $G_{\mathbb{Z}_p}$-valued cocharacter μ by $\mu(t) = t^{-1}x_1x_2 + x_2x_1$ such that

$$\mu(t)\cdot x_i = \begin{cases} t^{-1}x_i & i=1,\\ tx_i & i=2,\\ x_i & 3\le i\le n.\end{cases}$$

Under the fixed isomorphism $\iota : \overline{W[p^{-1}]} \to \mathbb{C}$, the cocharacters μ and μ_h^{-1} are conjugate, where μ_h is the Hodge cocharacter.

Following [HP17, 4.2.5, 4.2.6], since the derived group of G is $G^{\mathrm{der}} \simeq \mathrm{Res}_{F/\mathbb{Q}}\mathrm{SL}_{1,B}$, which is simply connected, and the embedding $G \hookrightarrow \mathrm{GSpin}(V,Q)$ induces $G/G^{\mathrm{der}} \simeq \mathrm{GSpin}(V,Q)/\mathrm{GSpin}(V,Q)^{\mathrm{der}} \simeq \mathbb{G}_m$, if we set $b = x_3(p^{-1}x_1+x_2) \in G(\mathbb{Q}_p) \subset \mathrm{GSpin}(V,Q)(\mathbb{Q}_p)$, then the isocrystal $\boldsymbol{L}_{\mathrm{cris},x}\otimes_W K$ is isomorphic to the isocrystal structure on V_K defined by $\Phi = b\circ\sigma$, where σ is the automorphism of $K = W(\overline{\mathbb{F}}_p)[p^{-1}]$ induced by the absolute Frobenius on $\overline{\mathbb{F}}_p$. If we define $M = V\otimes_{F,\rho'}\mathbb{Q}_p = \mathbb{Q}_p x_1 + \mathbb{Q}_p x_2 + \mathbb{Q}_p x_3$, then $V_K^{\Phi} = M_K^{\Phi}\oplus M^{\perp}$, where $M^{\perp} = \oplus_{\sigma'\neq\rho'} V\otimes_{F,\sigma'}\mathbb{Q}_p$. Moreover, M_K^{Φ} and M have the same dimension and determinant, but different Hasse invariants. In particular, as a quadratic space over $F_\lambda \simeq \mathbb{Q}_p$, $V(\mathcal{A}_x)\otimes_F F_\lambda$ has dimension 3, determinant 1 and Hasse invariant -1. □

By definition, we have

$$L(\mathcal{A}_x) = \{v\in V(\mathcal{A}_x) : v_{\mathrm{cris}} \in \boldsymbol{L}_{\mathrm{cris},x},\ v_\ell \in \boldsymbol{L}_{\ell,x} \text{ for all } \ell\neq p\}. \tag{4.2.5}$$

Then we have $L(\mathcal{A}_x)\otimes_{\mathbb{Z}} W \simeq \boldsymbol{L}_{\mathrm{cris},x}$ and $L(\mathcal{A}_x)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \simeq \boldsymbol{L}_{\ell,x}$ for $\ell\neq p$.

Lemma 4.5. *Let p be a rational prime that is totally split in F. Suppose $\mathcal{A}_x$ is supersingular and there is an order 2 automorphism $\alpha\in\mathrm{SO}(V(\mathcal{A}_x),Q'_F)$ such that $\alpha(\boldsymbol{L}_{\mathrm{cris},x}) = \boldsymbol{L}_{\mathrm{cris},x}$ under the identification $L(\mathcal{A}_x)\otimes_{\mathbb{Z}} W \simeq \boldsymbol{L}_{\mathrm{cris},x}$ and $\alpha(\boldsymbol{L}_{\ell,x}) = \boldsymbol{L}_{\ell,x}$ under the identification $L(\mathcal{A}_x)\otimes_{\mathbb{Z}}\mathbb{Z}_\ell \simeq \boldsymbol{L}_{\ell,x}$ for all $\ell\neq p$, then there is $u\in L(\mathcal{A}_x)$ such that $Q'_F(u) = 1$ and $\alpha(u) = u$.*

Proof. By Lemma 4.3 and Lemma 4.4, there exists a totally definite quaternion algebra B' over F that is ramified at $\mathfrak{p}$ over p corresponding to $\rho' : F\hookrightarrow W[p^{-1}]$ and an isometry of quadratic spaces

$$f : (B'^0, \mathrm{nrd}\,|_{B'^0}) \xrightarrow{\sim} (V(\mathcal{A}_x), Q'_F).$$

Since $\mathrm{SO}(B'^0,\mathrm{nrd}\,|_{B'^0}) = B'^{\times}/F^{\times}$ with $B'^{\times}$ acts on B'^0 by conjugation, there exists $\beta\in B'$ such that $\alpha(x) = f(\beta f^{-1}(x)\beta^{-1})$ for all $x\in V(\mathcal{A}_x)$. The automorphism α has order 2, so $\beta^2\in F$ and $\beta\notin F$, which implies $\beta\in B'^0$. Let $u' = f(\beta)\in V(\mathcal{A}_x)$. Note that $\alpha(cu') = cu'$ for all $c\in F$.

For each $\sigma' : F\hookrightarrow W[p^{-1}]$, let

$$g_{\sigma'} : (V(\mathcal{A}_x)\otimes_{F,\sigma'} W[p^{-1}], \sigma'\circ Q'_F) \xrightarrow{\sim} (V\otimes_{F,\sigma'} W[p^{-1}], \sigma'\circ Q_F)$$

be the isometry (4.2.2) over $W[p^{-1}]$, and

$$u_{\sigma'} = g_{\sigma'}(u'\otimes 1)\in V\otimes_{F,\sigma'} W[p^{-1}] = (B\otimes_{F,\sigma'} W[p^{-1}])^0,$$

then $g_{\sigma'}\circ\alpha\circ g_{\sigma'}^{-1}$ acts as 1 on $\langle u_{\sigma'}\rangle$ and -1 on $\langle u_{\sigma'}\rangle^{\perp}$, so $g_{\sigma'}\circ\alpha\circ g_{\sigma'}^{-1}(x) = u_{\sigma'}xu_{\sigma'}^{-1}$ for all $x\in V\otimes_{F,\sigma'}W[p^{-1}]$. Since the automorphism preserves $\boldsymbol{L}_{\mathrm{cris},x}\simeq L\otimes_{\mathbb{Z}} W = \bigoplus_{\sigma':F\hookrightarrow W[p^{-1}]} L\otimes_{\mathcal{O}_F,\sigma'} W$, where $L = B^0\cap\mathcal{O}$, and $\mathcal{O}\otimes_{\mathcal{O}_F,\sigma'} W$ is a maximal order in $B\otimes_{F,\sigma'} W[p^{-1}]\simeq M_2(W[p^{-1}])$, we have

$$u_{\sigma'}\in N_{(B\otimes_{F,\sigma'}W[p^{-1}])^\times}(\mathcal{O}\otimes_{\mathcal{O}_F,\sigma'} W) = W[p^{-1}]^\times(\mathcal{O}\otimes_{\mathcal{O}_F,\sigma'} W)^\times.$$

In particular, $\sigma'(Q'_F(u')) = \mathrm{nrd}(u_{\sigma'})\in W[p^{-1}]^\times$ has even valuation, and $u_{\sigma'}\in L\otimes_{\mathcal{O}_F,\sigma'} W$ if and only $\mathrm{nrd}(u_{\sigma'})$ has zero valuation. Here since p splits in F, each σ' corresponds to a unique place of F above p.

For $v\nmid p$, let

$$g_v : (V(\mathcal{A}_x)\otimes_F F_v, Q'_F) \xrightarrow{\sim} (V\otimes_F F_v, Q_F)$$

be the isometry (4.2.4) over F_v, and

$$u_v = g_v(u'\otimes 1)\in V\otimes_F F_v = B_v^0,$$

then $g_v\circ\alpha\circ g_v^{-1}(x) = u_v x u_v^{-1}$ for all $x\in V\otimes_F F_v$. Similarly as before, since the automorphism preserves $\boldsymbol{L}_{\ell,x}\simeq L\otimes_{\mathbb{Z}}\mathbb{Z}_\ell = \oplus_{v|\ell} L\otimes_{\mathcal{O}_F}\mathcal{O}_{F_v}$, we have

$$u_v\in N_{B_v^\times}(\mathcal{O}_v) = F_v^\times\mathcal{O}_v^\times.$$

In particular, $Q'_F(u') = \mathrm{nrd}(u_v) \in F_v^\times$ has even valuation, and $u_v \in L \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$ if and only if $\mathrm{nrd}(u_v)$ has zero valuation.

Since $h(F) = 1$ and $Q'_F(u')$ has even valuations at all finite places of F, there exists $c_1 \in F^\times$ such that $Q'_F(c_1 u') = c_1^2 Q'_F(u) \in \mathcal{O}_F^\times$. Moreover, since Q'_F is positively definite, and every totally positive unit in F is a square (F has units of independent signs), there exists $c_2 \in \mathcal{O}_F^\times$ such that $Q'_F(c_1 c_2 u') = 1$. Let $u = c_1 c_2 u'$, then $u \in L(\mathcal{A}_x)$ since $\sum_{\sigma': F \hookrightarrow W[p^{-1}]} c_1 c_2 u_{\sigma'} \in \boldsymbol{L}_{\mathrm{cris},x}$ and $\sum_{v|\ell} c_1 c_2 u_v \in \boldsymbol{L}_{\ell,x}$ for all $\ell \neq p$. □

4.3. **Pairing at points without even order automorphisms.** Let T be an $\mathscr{S}_{K_p K^p}$-scheme, then $x \in \mathscr{S}_{K_p K^p}(T)$ gives a triple $(\mathcal{A}_x, \lambda_x, \bar{\eta}_x)$, where $(\mathcal{A}_x, \lambda_x : \mathcal{A}_x \to \mathcal{A}_x^\vee)$ is a polarized abelian scheme over T up to isomorphism and the level structure $\eta \in \Gamma(T, \underline{\mathrm{Isom}}_G(H_{\widehat{\mathbb{Z}}^p}, \varprojlim_{p\nmid n} \mathcal{A}_x[n])/K^p)$. An integral model $\mathscr{S}_{K_0}$ of $\Gamma_0 \backslash X^+$ is constructed from $\mathscr{S}_{K_p K^p}$ by action of a finite group. Two points $x_1, x_2 \in \mathscr{S}_{K_p K^p}(\mathbb{C})$, corresponding to $(\mathcal{A}_{x_1}, \lambda_1, \bar{\eta}_1), (\mathcal{A}_{x_2}, \lambda_2, \bar{\eta}_2)$, are identified in $\mathscr{S}_{K_0}$ if there is a prime-to-p quasi-isogeny $\mathcal{A}_{x_1} \to \mathcal{A}_{x_2}$ that preserves polarization up to $\mathbb{Z}_{(p)}^\times$, sends s_{α,B,x_1} to s_{α,B,x_2} and takes $\boldsymbol{L}_{\ell,x_1}$ to $\boldsymbol{L}_{\ell,x_2}$ for all $\ell \neq p$.

Proposition 4.6. *Let $\lambda \in \mathcal{O}_F$ be a totally positive prime of F above p and $\phi : F(\sqrt{-\lambda}) \hookrightarrow B$ defining a CM cycle* (3.1.2)*. For $x \in \mathscr{S}_{K_0}(k)$ without even order automorphisms,* [8] *points in the CM cycle lifting x are paired, i.e., there is a map*

$$\{\textit{lifts of } x \textit{ in } (3.1.2)\} \longrightarrow \{\langle v\rangle : v \in L(\mathcal{A}_x), Q'_F(v) = \lambda\}/\operatorname{Aut}(x)$$

such that the fiber of every element in the image has size 2*.*

Proof. Suppose $\tilde{x}$ is a point in the CM cycle lifting x, then $\tilde{x}$ corresponds to an embedding $F(\sqrt{-\lambda}) \hookrightarrow B$. As in section 3.2, the image of $\sqrt{-\lambda}$ has reduced trace zero and reduced norm λ, and it gives a special endomorphism $\tilde{v} \in L(\mathcal{A}_{\tilde{x}})$ such that $Q_F(\tilde{v}) = \lambda$. Then $\mathcal{A}_x$ is supersingular by 3.10. Let v be the image of $\tilde{v}$ under the $\mathcal{O}_F$-linear isometric map $L(\mathcal{A}_{\tilde{x}}) \hookrightarrow L(\mathcal{A}_x)$ and v_{cris} be the image of v under the $\mathcal{O}_F$-linear isometric map $L(\mathcal{A}_x) \hookrightarrow \boldsymbol{L}_{\mathrm{cris},x}$, then $\mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},x} \in v_{\mathrm{cris}}^\perp$ over k. By (2.2.6), we have an orthogonal direct sum decomposition $v_{\mathrm{cris}} = \sum_{\sigma': F \hookrightarrow W[p^{-1}]} v_{\mathrm{cris},\sigma'}$ and $Q_{\mathrm{cris},x}(v_{\mathrm{cris},\sigma'}) = \sigma'(Q_F(\tilde{v})) = \sigma'(\lambda)$, where $Q_{\mathrm{cris},x}$ denotes the quadratic form on $\boldsymbol{L}_{\mathrm{cris},x}$. By section 3.3, the abelian varieties on the CM cycle are defined over a field whose ramification index over p is at most 2, so we can apply Lemma 4.2. There are exactly two lifts $\mathcal{A}_{\tilde{x}_1}, \mathcal{A}_{\tilde{x}_2}$ with $\tilde{v}_1 \in L(\mathcal{A}_{\tilde{x}_1}), \tilde{v}_2 \in L(\mathcal{A}_{\tilde{x}_2})$ lifting v, corresponding to the two isotropic lines lifting $\boldsymbol{L}_{\mathrm{dR},x}$ that are orthogonal to $(v_{\mathrm{cris},\rho'} \otimes 1)$ in the subspace of $\boldsymbol{L}_{\mathrm{cris},x} \otimes_W \mathcal{O}_E$ where each $\boldsymbol{\pi}_{\epsilon_i,\mathrm{cris},x}$ acts as $\rho'(\epsilon_i) \otimes 1$, by the linear algebra computation Lemma 4.7.

If $\mathcal{A}_{\tilde{x}_1}$ and $\mathcal{A}_{\tilde{x}_2}$ give the same point in $\Gamma_0 \backslash X^+$, then there is a quasi-isogeney $f : \mathcal{A}_{\tilde{x}_1} \to \mathcal{A}_{\tilde{x}_2}$ that sends $s_{\alpha,?,\tilde{x}_1}$ to $s_{\alpha,?,\tilde{x}_2}$, where $? = \ell, p, \mathrm{dR}$, and takes $\boldsymbol{L}_{\ell,\tilde{x}_1}$ to $\boldsymbol{L}_{\ell,\tilde{x}_1}$ and $\boldsymbol{L}_{p,\tilde{x}_1}$ to $\boldsymbol{L}_{p,\tilde{x}_1}$. In particular, $f(v_1) = f \circ v_1 \circ f^{-1} \in V(\mathcal{A}_{\tilde{x}_2}) \cap (\prod_{\ell \text{ prime}} \boldsymbol{L}_{\ell,\tilde{x}_2}) = L(\mathcal{A}_{\tilde{x}_2})$. Then f induces a quasi-isogeny of $\mathcal{A}_x$ such that $f : H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W E \to H^1_{\mathrm{cris}}(\mathcal{A}_x/W) \otimes_W E$ preserves all $s_{\alpha,\mathrm{cris},x}$, and $f(\mathrm{Fil}^1 H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}_1}/E)) = \mathrm{Fil}^1 H^1_{\mathrm{dR}}(\mathcal{A}_{\tilde{x}_2}/E)$, which gives a $\mathcal{O}_F$-linear isometry of $\boldsymbol{L}_{\mathrm{cris},x} \otimes_W \mathcal{O}_E$ taking $\mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},\tilde{x}_1}$ to $\mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},\tilde{x}_2}$. The isotropic line $\mathrm{Fil}^1 \boldsymbol{L}_{dR,\tilde{x}_2} \in (v_{\mathrm{cris}} \otimes 1)^\perp \cap f(v_{\mathrm{cris}} \otimes 1)^\perp$ and it lies in the 3-dimensional ρ'-eigenspace of $\boldsymbol{L}_{\mathrm{cris},x}$. There is an isometry from $L(\mathcal{A}_x) \otimes_{\mathcal{O}_F,\rho'} W$ to the ρ'-eigenspace of $\boldsymbol{L}_{\mathrm{cris},x}$, where $v \otimes 1$ (resp. $f(v) \otimes 1$) maps to $v_{\mathrm{cris},\rho'}$ (resp. $f(v)_{\mathrm{cris},\rho'}$). Then $v \otimes 1$ and $f(v) \otimes 1$ must span the same line in $L(\mathcal{A}_x) \otimes_{\mathcal{O}_F,\rho'} W$ since otherwise $(v \otimes 1)^\perp \cap (f(v) \otimes 1)^\perp \subset L(\mathcal{A}_x) \otimes_{\mathcal{O}_F,\rho'} W$ is a one-dimensional subspace defined in $L(\mathcal{A}_x)$, which cannot be isotropic. Then $f(\mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},\tilde{x}_2}) \in f(v_{\mathrm{cris},\rho'} \otimes 1)^\perp = (v_{\mathrm{cris},\rho'} \otimes 1)^\perp$ implies $f(F^1 \boldsymbol{L}_{dR,\tilde{x}_2}) = F^1 \boldsymbol{L}_{dR,\tilde{x}_1}$. Therefore, f fixes the line spanned by $v_{\mathrm{cris},\rho'} \otimes 1$ and switches the two isotropic lines $\mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},\tilde{x}_1}, \mathrm{Fil}^1 \boldsymbol{L}_{\mathrm{dR},\tilde{x}_2}$. In particular, f has even order as an automorphism of x.

If $\mathcal{A}_{\tilde{x}_1}, \mathcal{A}_{\tilde{x}_2}$ (resp. $\mathcal{A}_{\tilde{x}'_1}, \mathcal{A}_{\tilde{x}'_2}$) correspond to lifting v (resp. v') in $L(\mathcal{A}_x)$, and $\mathcal{A}_{\tilde{x}_1}$ and $\mathcal{A}_{\tilde{x}'_1}$ give the same point in $\Gamma_0 \backslash X^+$, then there is a quasi-isogeney $f : \mathcal{A}_{\tilde{x}_1} \to \mathcal{A}_{\tilde{x}'_1}$ that sends $s_{\alpha,?,\tilde{x}_1}$ to $s_{\alpha,?,\tilde{x}'_1}$, where $? = \ell, p, \mathrm{dR}$, and takes $\boldsymbol{L}_{\ell,\tilde{x}_1}$ to $\boldsymbol{L}_{\ell,\tilde{x}_1'}$ and $\boldsymbol{L}_{p,\tilde{x}_1}$ to $\boldsymbol{L}_{p,\tilde{x}_1'}$. By the same argument, $v' \otimes 1$ and $f(v) \otimes 1$ must span the same line in $L(\mathcal{A}_x) \otimes_{\mathcal{O}_F,\rho'} W$, and then f takes $\mathrm{Fil}\, \boldsymbol{L}_{\mathrm{dR},\tilde{x}_2}$ to $\mathrm{Fil}\, \boldsymbol{L}_{\mathrm{dR},\tilde{x}'_2}$, which implies that $\mathcal{A}_{\tilde{x}_2}$ and $\mathcal{A}_{\tilde{x}'_2}$ give the same point in $\Gamma_0 \backslash X^+$. □

Lemma 4.7. *Let $k \subset \overline{\mathbb{F}}_p$ be a field of odd characteristic p. Let $W = W(k)$ and (L, Q) be a rank* 3 *quadratic space over W such that $L \otimes_W k$ is nondegenerate. If $v \in L$ such that $Q(v) = t$ is a uniformizer of W,*

[8] The automorphisms are defined over $\bar{k}$.

then there are exactly two isotropic lines in the 2-dimensional subspace $(v \otimes 1)^\perp \subset L \otimes_W \overline{W[p^{-1}]}$. The two isotropic lines can be defined in $L \otimes_W \mathcal{O}_E$ where E is a finite extension of $W[p^{-1}]$ of ramification index 2, and reduce to the same line modulo $\mathfrak{p}$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_E$.

Proof. Since W is a local PID and $2 \in W^\times$, the quadratic form Q over W is diagonalizable. Let e_1, e_2, e_3 be an orthogonal basis of L with $Q(e_i) = a_i$, $i = 1, 2, 3$. By assumption that $L \otimes_W k$ is nondegenerate, each $a_i \in W^\times$. Suppose $xe_1 + ye_2 + ze_3$ is a generator of an isotropic line orthogonal to $v = \sum_{i=1}^3 c_i e_i$, $c_i \in W$, then we have $a_1x^2 + a_2y^2 + a_3z^2 = 0$ and $a_1c_1x + a_2c_2y + a_3c_3z = 0$ with $\sum_{i=1}^3 a_i c_i^2 = t$. Note that at least two $c_i \in W^\times$ since t is a uniformizer and $a_i \in W^\times$. Without loss of generality, assume $c_1, c_2 \in W^\times$. Solving the equation gives two lines generated by $(-a_1a_2a_3c_1c_2 \pm a_3c_3\sqrt{-a_1a_2a_3t})e_1 + a_1a_3(t - a_2c_2^2)e_2 + (\mp a_1c_1\sqrt{-a_1a_2a_3t} - a_1a_2a_3c_2c_3)e_3$ defined over $E := W[p^{-1}](\sqrt{-a_1a_2a_3t})$ where $-a_1a_2a_3t$ is a uniformizer of W. Note that $a_1a_3(t - a_2c_2^2) \in W^\times$, and modulo the maximal ideal of $\mathcal{O}_E$, both lines reduce to $\langle c_1e_1 + c_2e_2 + c_3e_3 \rangle = \langle v \rangle$. □

4.4. **Pairing at points with an even order automorphism.**

Proposition 4.8. *Let p be a rational prime that is totally split in F and λ be the totally positive prime of F above p corresponding to $\rho' : F \hookrightarrow W[p^{-1}]$.*

(1) For $x \in \mathscr{S}_{K_0}(k)$ with an even order automorphism, there is a bijection

$$\{\textit{lifts of } x \textit{ admitting a special endomorphism } \sqrt{-\lambda}\} \longrightarrow \{\langle v \rangle : v \in L(\mathcal{A}_x),\, Q'_F(v) = \lambda\}/\operatorname{Aut}(x)$$

where the elements on the right-hand side are paired such that $\langle v \rangle$ and $\langle w \rangle$ are paired if and only if $v \perp w$. In particular, all CM lifts of x arising from all optimal embeddings $S \hookrightarrow \mathcal{O}$, where $S \subset F(\sqrt{-\lambda})$ is an order containing $\sqrt{-\lambda}$, are paired.

(2) Moreover, such CM lifts are defined over an extension E of $W(k)[p^{-1}]$ of ramification index 2 and the two lifts in a pair are isomorphic modulo $\mathfrak{p}^2$, but they are not isomorphic to the lift with special endomorphism $\sqrt{-1}$ modulo $\mathfrak{p}^2$, where $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}_E$.

The proof of Proposition 4.8 uses Lemma 4.10 and the linear algebra computation Lemma 4.11. The proof of Lemma 4.10 uses the linear algebra computation Lemma 4.9.

Lemma 4.9. *Let F be a totally real number field and $\mathcal{O}_F$ be its ring of integers. Let λ be a large enough totally positive prime of F ($\lambda > 4$ at all real places of F).*[9] *Suppose $Q : L \to \mathcal{O}_F$ is a quadratic module over $\mathcal{O}_F$ such that the extension $Q : L \otimes_{\mathcal{O}_F} F \to F$ is a quadratic form anisotropic at λ and at all real places of F.*

(1) If $Q(e_1) = 1$ and $Q(e_2) = \lambda$ where $e_1, e_2 \in L$, then $e_1 \perp e_2$.

(2) Suppose L has rank 3. If $Q(e_1) = 1, Q(e_2) = Q(e_3) = \lambda$, where $e_1, e_2, e_3 \in L$ and e_2, e_3 are linearly independent, and $\alpha \in \mathrm{SO}(L, Q)$, then $\alpha(e_1) = \pm e_1$.

Proof. (1) Let $n = Q(e_1 + e_2) - Q(e_1) - Q(e_2)$. Consider $f(x) = Q(e_2 - xe_1) = x^2 - nx + \lambda \in \mathcal{O}_F[x]$. Note that e_1, e_2 are linearly independent. By Hensel's lemma, since $f(0) = \lambda$ and $f'(0) = -n$, f has no roots in F_λ implies $n = a\lambda$ for some $a \in \mathcal{O}_F$. On the other hand, f has no roots at all real places of F implies that $n^2 - 4\lambda$ is totally negative. Then $a^2 < \frac{4}{\lambda} < 1$ at all real places of F, which gives $a = 0$.

(2) Since $Q(\alpha(e_1)) = 1$, we have $\alpha(e_1) \perp e_2, \alpha(e_1) \perp e_3$, which implies $\alpha(e_1) \in \mathrm{Span}(e_1)$.

□

[9] Given a totally positive number $\lambda \in F$ such that $\mathrm{Nm}_{F/\mathbb{Q}}(\lambda)$ is large enough, there exists $u \in \mathcal{O}_F^\times$ such that $\rho_i(u^2) > \frac{4}{\rho_i(\lambda)}$ for each $\rho_i : F \hookrightarrow \mathbb{R}$; thus, after replacing λ by $u^2\lambda$, $\rho_i(\lambda) > 4$ is not an extra condition for us. The existence of such u follows from Dirichlet's unit theorem. Indeed, since the image Γ of $\mathcal{O}_F^\times \to \mathbb{R}^r$, $x \mapsto (-\log|\rho_i(x)|)_{\rho_i : F \hookrightarrow \mathbb{R}}$ is a complete lattice in the trace zero hyperplane $H = \{(x_{\rho_i}) : \sum_{i=1}^r x_{\rho_i} = 0\}$, where $r = [F : \mathbb{Q}]$ for F totally real, we pick a basis $\gamma_1 = (\gamma_{1,1}, \ldots, \gamma_{1,r-1}, -\sum_{i=1}^{r-1} \gamma_{1,i}), \ldots, \gamma_{r-1} = (\gamma_{r-1,1}, \ldots, \gamma_{r-1,r-1}, -\sum_{i=1}^{r-1} \gamma_{r-1,i})$ for the rank $(r-1)$ lattice $2\Gamma \subset H$. Write $a_i = \log(\rho_i(\lambda)) - \log(4)$ for each $i = 1, \ldots, r$ and $a = \sum_{i=1}^r a_i = \log \mathrm{Nm}_{F/\mathbb{Q}}(\lambda) - r\log(4)$. Consider $\sum_{i=1}^{r-1} c_i\gamma_i = (a_1 - \frac{a}{2(r-1)}, \ldots, a_{r-1} - \frac{a}{2(r-1)}, a_r - \frac{a}{2}) \in H$ with $c_1, \ldots, c_{r-1} \in \mathbb{R}$, and $\gamma = \sum_{i=1}^{r-1} [c_i]\gamma_i$ where each $[c_i] \in \mathbb{Z}$ with $|[c_i] - c_i| \le \frac{1}{2}$. If $a > (r-1)\max_{1 \le j \le r-1} \sum_{i=1}^{r-1} |\gamma_{i,j}|$, then the cube $C = \{(x_{\rho_i}) : \sum_{i=1}^r x_{\rho_i} = 0,\, a_j - \frac{a}{r-1} < x_{\rho_j} < a_j \text{ for each } j = 1, \ldots, r-1\} \subset H$ contains $\gamma \in 2\Gamma$.

Lemma 4.10. *Let p be a large enough rational prime that is totally split in F and λ be a totally positive prime of F above p corresponding to $\rho' : F \hookrightarrow W[p^{-1}]$. Let $x \in \mathscr{S}_{K_0}(k)$. Suppose $\mathcal{A}_x$ is supersingular, and x has an even order automorphism, then there exists $e_1 \in L(\mathcal{A}_x)$ such that $Q'_F(e_1) = 1$ by Lemma 4.5. If there is $e_2 \in L(\mathcal{A}_x)$ with $Q'_F(e_2) = \lambda$, then there is $e_3 \in L(\mathcal{A}_x)$ orthogonal to both e_1 and e_2 such that $Q'_F(e_3) = \lambda$. Moreover, there is no $\alpha \in \mathrm{SO}(L(\mathcal{A}_x), Q'_F)$ such that $\alpha(e_2) = \pm e_3$.*

Proof. Note that $e_2 \perp e_1$ by Lemma 4.9. Since Q'_F is a ternary quadratic form over F with determinant $1 \in F^\times/F^{\times 2}$, there exists a quaternion algebra B' over F with an isometry $(B'^0, \mathrm{nrd}\,|_{B'^0}) \simeq (V(\mathcal{A}_x), Q'_F)$. Under this identification, let $e_3 = e_1e_2$ where multiplication is taken in the quaternion algebra B'. Since $e_1 \perp e_2$ and $Q'_F(e_1) = 1, Q'_F(e_2) = \lambda$, we have $e_3 \in V(\mathcal{A}_x)$ and $Q'_F(e_3) = \lambda$.

For each $\sigma' : F \hookrightarrow W[p^{-1}]$, let

$$g_{\sigma'} : (V(\mathcal{A}_x) \otimes_{F,\sigma'} W[p^{-1}], \sigma' \circ Q'_F) \xrightarrow{\sim} (V \otimes_{F,\sigma'} W[p^{-1}], \sigma' \circ Q_F) = ((B \otimes_{F,\sigma'} W[p^{-1}])^0, \mathrm{nrd})$$

be the isometry (4.2.2) over $W[p^{-1}]$, and for $v \nmid p$, let

$$g_v : (V(\mathcal{A}_x) \otimes_F F_v, Q'_F) \xrightarrow{\sim} (V \otimes_F F_v, Q_F) = (B_v^0, \mathrm{nrd})$$

be the isometry (4.2.4) over F_v. Each isometry $g_{\sigma'}$ extends to a $W[p^{-1}]$-algebra isomorphism or anti-isomorphism $B' \otimes_{F,\sigma'} W[p^{-1}] \xrightarrow{\sim} B \otimes_{F,\sigma'} W[p^{-1}]$. Under this isomorphism, since $e_1, e_2 \in L(\mathcal{A}_x)$, we have $g_{\sigma'}(e_1 \otimes 1), g_{\sigma'}(e_2 \otimes 1) \in \mathcal{O} \otimes_{\mathcal{O}_F,\sigma'} W$, and then $g_{\sigma'}(e_3 \otimes 1) = \pm g_{\sigma'}(e_1 \otimes 1)g_{\sigma'}(e_2 \otimes 1) \in \mathcal{O} \otimes_{\mathcal{O}_F,\sigma'} W \cap (B \otimes_{F,\sigma'} W[p^{-1}])^0 = L \otimes_{\mathcal{O}_F,\sigma'} W$. Thus, $\sum_{\sigma'} g_{\sigma'}(e_3 \otimes 1) \in \boldsymbol{L}_{cris,x}$. Similarly, for every $v \nmid p$, the isometry g_v extends uniquely to an F_v-algebra isomorphism or anti-isomorphism $B'_v \xrightarrow{\sim} B_v$. Under this isomorphsim, since $e_1, e_2 \in L(\mathcal{A}_x)$, we have $g_v(e_1 \otimes 1), g_v(e_2 \otimes 1) \in \mathcal{O}_v$ and then $g_v(e_3 \otimes 1) = \pm g_v(e_1 \otimes 1)g_v(e_2 \otimes 1) \in \mathcal{O}_v \cap B_v^0 = L \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$. Therefore, we have $e_3 \in L(\mathcal{A}_x)$.

Suppose $\alpha \in \mathrm{SO}(L(\mathcal{A}_x))$, then $\alpha(e_1) = \pm e_1$ by Lemma 4.9. If $\alpha(e_1) = e_1$, $\alpha(e_2) = \pm e_3$, then $\alpha(e_3) = \mp e_2$, and α is conjugation by $1 \pm e_1 \in B'$. For $v|2$, since under the extended isomorphism or anti-isomorphism $g_v : B'_v \to B_v$, the automorphism $g_v \circ \alpha \circ g_v^{-1} : B_v \to B_v$ corresponding to α, which is conjugation by $g_v(1 + e_1)$ or $g_v(1 - e_1)$, preserves $\mathcal{O}_v$, we have $g_v(1 + e_1) \in F_v^\times \mathcal{O}_v^\times$ or $g_v(1 - e_1) \in F_v^\times \mathcal{O}_v^\times$, which implies particular $v(\mathrm{nrd}(1 + e_1)) = v(\mathrm{nrd}(1 - e_1)) = v(2)$ is even. However, $[F : \mathbb{Q}]$ is odd, so there is some $v|2$ with odd ramification index, i.e., $v(2)$ is odd. If $\alpha(e_1) = -e_1, \alpha(e_2) = \pm e_3$, then $\alpha(e_3) = \pm e_2$, then $\alpha^2 = 1$. By Lemma 4.5, there is $u \in L(\mathcal{A}_x)$ with $Q'_F(u) = 1$ and $\alpha(u) = u$. By Lemma 4.9, we have $u \perp e_2$ and $u \perp e_3$, which implies $u \in \mathrm{Span}(e_1)$ and $\alpha(u) = -u$, leading to contradiction. □

Lemma 4.11. *Let K be a local field with valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{p}$, residue field k, and a uniformizer ϖ. Suppose $Q : L \to \mathcal{O}$ is a rank 3 quadratic module over $\mathcal{O}$ such that the reduction $L \otimes_{\mathcal{O}} k \to k$ is nondegenerate over k. Suppose $e_1, e_2, e_3 \in L$ satisfy $v_\mathfrak{p}(Q(e_1)) = 0$, $v_\mathfrak{p}(Q(e_2)) = v_\mathfrak{p}(Q(e_3)) = 1$, and $v_\mathfrak{p}([e_i, e_j]) > 0$ for $i \neq j$. Then*

(1) e_1, e_2, e_3 are nonzero modulo $\mathfrak{p}$;
(2) e_1, e_i are linearly independent modulo $\mathfrak{p}$ for $i = 2, 3$;
(3) e_1, e_2, e_3 are linearly dependent modulo $\mathfrak{p}$;
(4) e_2 and e_3 span the same line in $L \otimes_{\mathcal{O}} k$.

Proof. (1) $\mathfrak{p}^2 \nmid Q(e_i), i = 1, 2, 3$.

(2) For $i = 2, 3$, if $e_i = ce_1 + \varpi v$ for some $c \in \mathcal{O}, v \in L$, then $0 \equiv [e_1, e_i] \equiv c[e_1, e_1] \pmod{\mathfrak{p}}$ implies $c \equiv 0 \pmod{\mathfrak{p}}$, contradicting e_i being nonzero modulo $\mathfrak{p}$.

(3) $[e_3, e_i] \equiv 0 \pmod{\mathfrak{p}}, i = 1, 2, 3$.

(4) Write $e_3 = c_1e_1 + c_2e_2 + \varpi v$ for some $c_1, c_2 \in \mathcal{O}, v \in L$, then $0 \equiv [e_1, e_3] \equiv c_1[e_1, e_1] \pmod{\mathfrak{p}}$ implies $c_1 \equiv 0 \pmod{\mathfrak{p}}$.

□

Proof of Proposition 4.8. Suppose $\tilde{x}$ is a point in the CM cycle lifting x with $\tilde{v} \in L(\mathcal{A}_{\tilde{x}})$ such that $Q_F(\tilde{v}) = \lambda$, then $\mathcal{A}_x$ is supersingular by 3.10. Let $e_1 \in L(\mathcal{A}_x)$ such that $Q'_F(e_1) = 1$ by Lemma 4.5. Let e_2 be the image of $\tilde{v}$ under the $\mathcal{O}_F$-linear isometric map $L(\mathcal{A}_{\tilde{x}}) \hookrightarrow L(\mathcal{A}_x)$, then $Q'_F(e_2) = \lambda$, and let $e_3 \in L(\mathcal{A}_x)$ with $Q'_F(e_3) = \lambda$ be constructed as in Lemma 4.10.

By Lemma 4.11, the pairwise orthogonal elements $e_1, e_2, e_3 \in L(\mathcal{A}_x)$ form a basis of $V(\mathcal{A}_x) \otimes_{F,\rho'} W[p^{-1}] \simeq V \otimes_{F,\rho'} W[p^{-1}]$ such that e_1, e_2 (resp. e_1, e_3) are linearly independent modulo p, while e_2, e_3 span the same

line modulo p. Let $E = (W[p^{-1}])(\sqrt{-\rho'(\lambda)})$ and $\mathfrak{p} = (\sqrt{-\rho'(\lambda)})$ be the maximal ideal in $\mathcal{O}_E$. Over E, the two isotropic lines in $\langle e_2\rangle^\perp$ (resp. $\langle e_3\rangle^\perp$) are $l_2 = \langle\sqrt{-\rho'(\lambda)}e_1 + e_3\rangle$ and $l_2' = \langle-\sqrt{-\rho'(\lambda)}e_1 + e_3\rangle$ (resp. $l_3 = \langle\sqrt{-\rho'(\lambda)}e_1 + e_2\rangle$ and $l_3' = \langle-\sqrt{-\rho'(\lambda)}e_1 + e_2\rangle$). The automorphism e_1 acts as 1 on $\langle e_1\rangle$ and -1 on $\langle e_1\rangle^\perp$. Therefore, the two liftings corresponding to l_2 and l_2' (resp. l_3 and l_3') are isomorphic. Over $\mathcal{O}_E/\mathfrak{p} = k$, the isotropic lines l_2, l_2', l_3, l_3' are all spanned by e_2. Over $\mathcal{O}_E/\mathfrak{p}^2$ both l_2 and l_3 are spanned by $\sqrt{-\rho'(\lambda)}e_1 + e_2$, where e_1, e_2 are linearly independent. Therefore, by [MP16, 5.16] or the proof of Lemma 4.2, the liftings corresponding to e_2 and e_3 are isomorphic modulo $\mathfrak{p}^2$. If the liftings $\tilde{x}_2$ and $\tilde{x}_3$ corresponding to l_2 and l_3, respectively, are isomorphic, then by the same argument as in Proposition 4.6, there exists a quasi-isogeny $\mathcal{A}_{\tilde{x}_2} \to \mathcal{A}_{\tilde{x}_3}$ inducing an automorphism $\alpha \in \mathrm{SO}(L(\mathcal{A}_x), Q_F')$ with $\alpha(e_2) = \pm(e_3)$, which contradicts Lemma 4.10.

After possibly extending k, we may assume $\sqrt{-1} \in W$. Over $W[p^{-1}]$, the two isotropic lines in $\langle e_1\rangle^\perp$ are $l_1 = \langle e_2 + \sqrt{-1}e_3\rangle$ and $l_1' = \langle e_2 - \sqrt{-1}e_3\rangle$. Since e_2, e_3 are nonzero modulo p, at least one of $e_2 \pm \sqrt{-1}e_3$ is nonzero modulo p, then at least one of l_1, l_1' reduces modulo p to a line spanned by e_2, in which case it corresponds to a lift with special endomorphism $\sqrt{-1}$. Over $\mathcal{O}_E/\mathfrak{p}^2$, l_1 (or l_1') is spanned by e_2, while l_2, l_3 are spanned by $\sqrt{-\sigma(\lambda)}e_1 + e_2$, with e_1, e_2 are linearly independent. Therefore, over $\mathcal{O}_K/\mathfrak{p}^2$, the lifts corresponding to e_2 and e_3 are isomorphic to each other, but not to the lift(s) correspoinding to l_1 or l_1'. □

5. Archimedean place

In this section, we prove Proposition 5.5 and its slightly more general form, Proposition 5.6, which give an equidistribution result used to control the archimedean contribution, i.e., the sign of the polynomial $P_\lambda(x)P_{4\lambda}(x)$ evaluated at the coordinate corresponding to a given abelian variety. In section 5.1, we recall Shimura's work on the real points of Shimura varieties, specializing to the one-dimensional case, where the set of real points is the image of a finite collection of geodesics in the upper half plane. Under the additional assumptions on F, we focus on the case where it suffices to consider a single geodesic. In section 5.2, we study the CM points on this geodesic, and in section 5.3, we use equidistribution of primes to show the density of the CM points on it.

5.1. **Real points on the Shimura curve.** Let $\varphi : \mathcal{H} \to \widetilde{\Gamma}\backslash\mathcal{H}$ be the natural map. According to Shimura [Shi75, 4.2], the action of complex conjugation on the Shimura curve $\widetilde{\Gamma}\backslash\mathcal{H}$ satisfies

$$\overline{\varphi(z)} = \varphi(\alpha(\bar{z})),$$

for any $\alpha \in F^\times\mathcal{O}^\times$ with $\rho(\mathrm{nrd}(\alpha)) < 0$. Recall that ϵ denotes a unit of F that is negative at ρ and positive at the other real places. The field $F(\sqrt{-\epsilon})$ embeds into B, since B is split at all finite places and $F(\sqrt{-\epsilon})$ splits B at all real ramified places of B. Moreover, there exists $\alpha \in \mathcal{O}$ such that $\mathrm{trd}(\alpha) = 0$ and $\mathrm{nrd}(\alpha) = -\alpha^2 = \epsilon$, as any two maximal orders in B are conjugate to each other. Let

$$U(\epsilon) := \{\alpha \in \mathcal{O}^\times : \mathrm{trd}(\alpha) = 0, \mathrm{nrd}(\alpha) = \epsilon\} = \{\alpha \in \mathcal{O}^\times : \alpha^2 = -\epsilon\},$$

and for each $\alpha \in U(\epsilon)$, put

$$Z_\alpha := \{z \in \mathcal{H} : \alpha(\overline{z}) = z\}.$$

Since every totally poistive unit in $\mathcal{O}_F^\times$ is a square, by [Shi75, 7.4], the real points of $\widetilde{\Gamma}\backslash\mathcal{H}$ are given by

$$\bigcup_{\alpha\in U(\epsilon)} \varphi(Z_\alpha).$$

The union might be taken over a set of representatives for $U(\epsilon)$ modulo inner automorphisms given by the elements of $\widetilde{\Gamma}$. This set is in bijection with the set of $\widetilde{\Gamma}$-conjugacy classes of embeddings $\mathcal{O}_F[\sqrt{-\epsilon}] \hookrightarrow \mathcal{O}$, where $\mathcal{O}_F[\sqrt{-\epsilon}]$ is an order in $F(\sqrt{-\epsilon})$.

5.1.1. *One geodesic case.* Assume $[F : \mathbb{Q}] > 1$, $\mathcal{O}_F[\sqrt{-\epsilon}]$ is the maximal order of $F(\sqrt{-\epsilon})$ [10] and $F(\sqrt{-\epsilon})$ has class number $h(F(\sqrt{-\epsilon})) = 1$, then the real points of $\widetilde{\Gamma}\backslash\mathcal{H}$ is $\varphi(Z_\alpha)$ for any $\alpha \in U(\epsilon)$ by Lemma 5.1.

[10]Since F has narrow class number 1, if 2 is inert in F, then $2\mathcal{O}_F$ ramifies in $F(\sqrt{-\epsilon})$ and $\mathcal{O}_F[\sqrt{-\epsilon}]$ is the maximal order of $F(\sqrt{-\epsilon})$.

Lemma 5.1. *For any quadratic $\mathcal{O}_F$-order $S \subset F[\sqrt{-\epsilon}]$, the number of $\widetilde{\Gamma}$-conjugacy classes of optimal $S \hookrightarrow \mathcal{O}$ is equal to the class number $h(S)$.*

Proof. For $\mathcal{O}^1 \subseteq \Gamma \subseteq N_{B^\times}(\mathcal{O})$, let $m(S, \mathcal{O}; \Gamma)$ denote the number of Γ-conjugacy classes of optimal $S \hookrightarrow \mathcal{O}$. Then $m(S, \mathcal{O}; \widetilde{\Gamma}) = m(S, \mathcal{O}; \mathcal{O}^\times)[\mathrm{nrd}(\mathcal{O}^\times) : \mathrm{nrd}(\widetilde{\Gamma})\,\mathrm{nrd}(S^\times)]$ by [Voi21, 30.3.14], where $[\mathrm{nrd}(\mathcal{O}^\times) : \mathrm{nrd}(\widetilde{\Gamma})\,\mathrm{nrd}(S^\times)] = 1$ since $\rho(\mathrm{Nm}_{F(\sqrt{-\epsilon})/F}(S)) \cap \mathbb{R}_{<0} \neq \emptyset$. Since F has narrow class number 1, the maximal order $\mathcal{O}$ of B has class number 1 and then $m(S, \mathcal{O}; \mathcal{O}^\times) = h(S) m(\widehat{S}, \widehat{\mathcal{O}}; \widehat{\mathcal{O}}^\times)$ by [Voi21, 30.4.17]. Finally, as B is split at all finite places, we have $m(\widehat{S}, \widehat{\mathcal{O}}; \widehat{\mathcal{O}}^\times) = \prod_{v \text{ finite}} m(S_v, \mathcal{O}_v; \mathcal{O}_v^\times) = 1$. □

We assume F has only one prime $\mathfrak{p}_2$ above 2, then the quaternion algebra $B \simeq \left(\frac{-\epsilon,-1}{F}\right)$ [11] and can be realized as

$$B \simeq \left\{ \begin{pmatrix} a & b \\ -b' & a' \end{pmatrix} : a, b \in F(\sqrt{-\epsilon}) \right\},$$

where $'$ denotes the nontrivial involution of $F(\sqrt{-\epsilon})/F$. Let

$$\mu = \begin{pmatrix} \sqrt{-\epsilon} & 0 \\ 0 & -\sqrt{-\epsilon} \end{pmatrix}, \nu = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mu\nu = \begin{pmatrix} 0 & \sqrt{-\epsilon} \\ \sqrt{-\epsilon} & 0 \end{pmatrix}.$$

Lemma 5.2. *The quaternion algebra $\left(\frac{-\epsilon,-1}{F}\right)$ has a maximal order of the form*

$$\mathcal{O} = \mathcal{O}_F[\mu, \frac{a + b\mu + \nu}{2}] = \mathcal{O}_F + \mathcal{O}_F\mu + \mathcal{O}_F\frac{a + b\mu + \nu}{2} + \mathcal{O}_F\frac{-\epsilon b + a\mu + \mu\nu}{2} \tag{5.1.1}$$

for some nonzero $a, b \in \mathcal{O}_F$.

Proof. Let π be a generator of the prime $\mathfrak{p}_2$ of F above 2. By [Voi21, 5.4.4], since $\left(\frac{-\epsilon,-1}{F_\pi}\right)$ is split, there exists $a', b' \in F_\pi$ such that $a'^2 + b'^2\epsilon + 1 = 0$.

We must have $a', b' \in \mathcal{O}_{F_\pi}$. Otherwise, $v_\pi(a') = v_\pi(b') = -m < 0$ and then $c'^2 + d'^2\epsilon \equiv 0 \pmod{\pi^{2m}}$ where $c' = \pi^m a'$, $d' = \pi^m b' \in \mathcal{O}_{F_\pi}^\times$. If $m > e$, then $-\epsilon$ is a square in F_π by Hensel's lemma, which contradicts (π) being ramified in $F(\sqrt{-\epsilon})$. If $m \leq e$, then pick $c, d \in \mathcal{O}_F$ with $c \equiv c' \pmod{\pi^{2m}}, d \equiv d' \pmod{\pi^{2m}}$, then $\mathcal{O}_F[\frac{c+d\sqrt{-\epsilon}}{\pi^m}]$ is an order in $F(\sqrt{-\epsilon})$, which contradicts $F(\sqrt{-\epsilon})$ having maximal order $\mathcal{O}_F[\sqrt{-\epsilon}]$.

Choose $a, b \in \mathcal{O}_F$ with $a \equiv a' \pmod 4$, $b \equiv b' \pmod 4$, then $\frac{a+b\mu+\nu}{2}$ is integral and $\mathcal{O} = \mathcal{O}_F[\mu, \frac{a+b\mu+\nu}{2}] = \mathcal{O}_F + \mathcal{O}_F\mu + \mathcal{O}_F\frac{a+b\mu+\nu}{2} + \mathcal{O}_F\mu\frac{a+b\mu+\nu}{2}$ is an order in B. Moreover, $\mathcal{O} \supset \mathcal{O}_F[\mu, \nu]$ and its discriminant $\mathrm{disc}(\mathcal{O}) = (\frac{1}{4})^2 \mathrm{disc}(\mathcal{O}_F[\mu, \nu]) = (\frac{1}{4})^2(-4\epsilon)^2 = \epsilon^2$ is a unit in F. □

We may assume $\mathcal{O}$ is the maximal order as defined by (5.1.1) and $\alpha = \mu \in U(\epsilon)$. Then the geodesic

$$Z_\alpha = \{iy : y > 0\} \tag{5.1.2}$$

is the positive imaginary axis and its stablizer in $\widetilde{\Gamma}$ is

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix} : a \in \mathcal{O}_F[\sqrt{-\epsilon}]^\times,\ \rho(aa') > 0 \right\} \bigcup \left\{ \begin{pmatrix} 0 & b \\ -b' & 0 \end{pmatrix} : b \in \mathcal{O}_F[\sqrt{-\epsilon}]^\times,\ \rho(bb') > 0 \right\}.$$

By assumption, the Shimura curve $\widetilde{\Gamma}\backslash\mathcal{H}$ is isomorphic to $\mathbb{P}^1(\mathbb{C})$. Hence, its real points form a circle. Fix an extension of ρ to $F(\sqrt{-\epsilon})$ and let u be the generator of $\ker(\mathcal{O}_F[\sqrt{-\epsilon}]^\times \xrightarrow{\mathrm{Nm}} \mathcal{O}_F^\times)$ with $\rho(u) > 1$.[12] Then $\pm u^2 = \pm\frac{u}{u'}$ generates $\{\frac{a'}{a} : a \in \mathcal{O}_F[\sqrt{-\epsilon}]^\times\}$,[13] and $[i, i\rho(u^2)]$ is a fundamental domain for $\varphi(Z_\alpha)$.

---

[11] This is the quaternion algebra unramified at all odd primes and exactly one of the real places ρ of F.

[12] The rank of $\ker(\mathcal{O}_F[\sqrt{-\epsilon}]^\times \xrightarrow{\mathrm{Nm}} \mathcal{O}_F^\times)$ is $\mathrm{rank}(\mathcal{O}_F[\sqrt{-\epsilon}]^\times) - \mathrm{rank}(\mathcal{O}_F^\times) = (2 + ([F : \mathbb{Q}] - 1) - 1) - ([F : \mathbb{Q}] - 1) = 1$. Thus, $\ker(\mathcal{O}_F[\sqrt{-\epsilon}]^\times \xrightarrow{\mathrm{Nm}} \mathcal{O}_F^\times) = \{\pm u^m : m \in \mathbb{Z}\}$.

[13] The 2-rank of $H^1(\mathrm{Gal}(F(\sqrt{-\epsilon})/F), \mathcal{O}_F[\sqrt{-\epsilon}]^\times)$ is 1 by [CH88, 5.1, 9.1] and $-1 = \frac{\sqrt{-\epsilon}}{-\sqrt{-\epsilon}}$. Thus, the class of u generates the size 2 group $H^1(\mathrm{Gal}(F(\sqrt{-\epsilon})/F), \mathcal{O}_F[\sqrt{-\epsilon}]^\times)$.

5.2. **CM points on the geodesic.** For a CM point $x+iy \in \mathcal{H}$ corresponding to an embedding $L = F(\sqrt{-\lambda}) \hookrightarrow B$, the element $\sqrt{-\lambda}$ maps to $\begin{pmatrix} a\sqrt{-\epsilon} & b \\ -b' & -a\sqrt{-\epsilon} \end{pmatrix}$ with $a \in F, b \in F(\sqrt{-\epsilon})$, and the matrix stabilizes $x+iy$. There exists $y>0$ such that $\rho\left(\begin{pmatrix} a\sqrt{-\epsilon} & b \\ -b' & -a\sqrt{-\epsilon} \end{pmatrix}\right) iy = iy$ if and only if $a=0$ and $\lambda = bb' \in \mathrm{Nm}_{F(\sqrt{-\epsilon})/F}(F(\sqrt{-\epsilon})^\times)$. In this case,

$$y = \sqrt{\rho\left(\frac{b}{b'}\right)}.$$

Suppose $\sqrt{-\lambda} \in \mathcal{O}$, then $2b \in \mathcal{O}_F[\sqrt{-\epsilon}]$, and since $\lambda = bb'$ and $F(\sqrt{-\epsilon})$ has only one prime above 2 by assumption, it follows that $b \in \mathcal{O}_F[\sqrt{-\epsilon}]$ is a prime above λ.

Lemma 5.3. *Assume $F(\sqrt{-\epsilon})$ has class number $h(F(\sqrt{-\epsilon})) = 1$. For a totally positive prime λ of F such that $-\lambda$ is a square modulo 4, there exists $x \in \mathcal{O}_{F(\sqrt{-\epsilon})}$ such that $\lambda = \mathrm{Nm}_{F(\sqrt{-\epsilon})/F}(x)$; moreover, if $x_1, x_2 \in \mathcal{O}_{F(\sqrt{-\epsilon})}$ both satisfy the norm equation, then one of $\frac{x_1}{x_2}$, $\frac{x_1}{x_2'}$ is a unit in $\ker(\mathcal{O}_{F(\sqrt{-\epsilon})}^\times \xrightarrow{\mathrm{Nm}} \mathcal{O}_F^\times)$.*

Proof. Since the totally negative $-\lambda$ is square modulo 4, the quadratic reciprocity law gives

$$\left(\frac{-\epsilon}{-\lambda}\right) = \left(\frac{-\lambda}{-\epsilon}\right)\left(\frac{-\epsilon}{-\lambda}\right) = (-1)^{\sum_{\sigma: F \hookrightarrow \mathbb{R}} \frac{\mathrm{sign}(\sigma(-\epsilon))-1}{2}} = (-1)^{[F:\mathbb{Q}]-1} = 1,$$

which implies (λ) splits in $F(\sqrt{-\epsilon})$. Let $x \in \mathcal{O}_{F(\sqrt{-\lambda})}$ be a prime above λ, then $xx' = z\lambda$ for some $z \in \mathcal{O}_F^\times$ such that $\sigma(z) > 0$ for all embeddings $\sigma: F \hookrightarrow \mathbb{R}$ with $\sigma \neq \rho$. If $\rho(z) > 0$, then $z \in (\mathcal{O}_F^\times)^2 \subset \mathrm{Nm}_{F(\sqrt{-\epsilon})/F}(\mathcal{O}_{F(\sqrt{-\epsilon})}^\times)$; if $\rho(z) < 0$, then $z \in \epsilon(\mathcal{O}_F^\times)^2$, where $\epsilon = -\sqrt{-\epsilon}\sqrt{-\epsilon}$. Therefore, λ is always a norm from $\mathcal{O}_{F(\sqrt{-\epsilon})}$. □

By Lemma 5.3, the norm equation $\lambda = bb'$ with $b \in \mathcal{O}_F[\sqrt{-\epsilon}]$ gives two points $\varphi\left(i\sqrt{\rho\left(\frac{b}{b'}\right)}\right)$ and $\varphi\left(i\rho(u)\sqrt{\rho\left(\frac{b}{b'}\right)}\right)$ on $\varphi(Z_\alpha)$. Recall in 3.7 that each of the two CM cycles defined by optimal embeddings of $\mathcal{O}_{F(\sqrt{-\lambda})}$ and $\mathcal{O}_F + \mathfrak{p}_2\mathcal{O}_{F(\sqrt{-\lambda})}$ has a unique real point. The two real CM points are precisely the two points obtained from the norm equation.

5.3. **Equidistribution.** Given a CM cycle on the Shimura curve defined by $\widetilde{T} \subset \widetilde{G}$ and $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, by [DMOS82, V], the conjugate of the CM cycle on the conjugate Shimura curve is defined by $\widetilde{T} = {}^{\tau,\mu}\widetilde{T} \subset {}^{\tau,\mu}\widetilde{G}$, where μ is the Hodge cocharacter and ${}^{\tau,\mu}\widetilde{G}$ is a twist of $\widetilde{G}$. Explicitly, as in [MS10, 1.4], ${}^{\tau,\mu}\widetilde{G}$ arises from a quaternion algebra ${}^\tau B$ such that $\mathrm{inv}_v({}^\tau B) = \mathrm{inv}_{\tau\circ v}(B)$ for all infinite places v of F and $\mathrm{inv}_v({}^\tau B) = \mathrm{inv}_v(B)$ for all finite places v of F. Moreover, the isomorphism $\widetilde{G}(\mathbb{A}_f) \simeq {}^{\tau,\mu}\widetilde{G}(\mathbb{A}_f)$ induced by $B_v \simeq {}^\tau B_v$ maps $\widetilde{K} = \prod \mathcal{O}_v^\times$ to ${}^{\tau,\mu}\widetilde{K} = \prod {\mathcal{O}'_v}^\times$, where each $\mathcal{O}'_v$ is a maximal order of ${}^\tau B_v$. For a CM cycle corresponding to optimal embeddings $R \hookrightarrow \mathcal{O}_B$, where R is an $\mathcal{O}_F$-order in a CM extension of F, its conjugate on the conjugate Shimura curve corresponds to optimal embeddings $R \hookrightarrow \mathcal{O}_{{}^\tau B}$, where $\mathcal{O}_{{}^\tau B}$ is a maximal order of ${}^\tau B$.

Let $n = [F:\mathbb{Q}]$ and $\rho_1, \dots, \rho_n : F \hookrightarrow \mathbb{R}$ be distinct embeddings of F into $\mathbb{R}$. For each $i = 1, \dots, n$, let $F_i = F(\sqrt{-\epsilon_i})$, where ϵ_i is a unit of F that is negative at ρ_i, and denote by B_i the quaternion algebra over F unramified at all finite places and exactly one of the real places ρ_i. Under the assumption that F has only one prime above 2, we have $B_i \simeq \left(\frac{-\epsilon_i, -1}{F}\right)$.

Assume $\mathcal{O}_F[\sqrt{-\epsilon_i}]$ is the maximal order of $F(\sqrt{-\epsilon_i})$ and $F(\sqrt{-\epsilon_i})$ has class number $h(F(\sqrt{-\epsilon_i})) = 1$ for all $i = 1, \dots, n$.[14] Then the real points of each conjugate Shimura curve is the image of one geodesic Z_{α_i} and we may assume $Z_{\alpha_i} = \{iy : y > 0\}$ by choosing appropriate embeddings $B_i \hookrightarrow M_2(\mathbb{R})$. Let φ_i denote the natrual map from the upper half plane to the Shimura curve defined by B_i. The real CM points on the geodesic $\{iy : y > 0\}$ are $i\sqrt{\frac{\rho_{i,1}(b_i)}{\rho_{i,1}(b_i')}}$ for some $b_i \in F_i$ satisfying $\lambda = \mathrm{Nm}_{F_i/F}(b_i)$, where $\rho_{i,1}$ is a real place of F_i above ρ_i and $\lambda \in F$ totally positive.

[14] If $F/\mathbb{Q}$ is Galois, this is true if and only if one of the ϵ_i satisfies the assumption.

Let $\mathcal{F} = F_1 \cdots F_n$ be the compositum. Assume $\mathcal{F}$ has class number $h(\mathcal{F}) = 1$. The image of $\mathrm{Nm}_{\mathcal{F}/F} = \mathrm{Nm}_{F_i/F} \circ \mathrm{Nm}_{\mathcal{F}/F_i} : \mathcal{F}^\times \to F^\times$ is totally positive. Suppose λ is a totally positve prime of F such that $-\lambda$ is a square modulo 4. Then by Lemma 5.3, (λ) splits in each F_i, and thus splits completely in the compositum $\tilde{F}$.

Lemma 5.4. *Let P be the set of prime ideals of $\mathcal{F}$. Assume $\mathcal{F}$ has class number $h(\mathcal{F}) = 1$. Then the set*

$$\left\{ \left(\frac{1}{2} \log \frac{\rho_{i,1}(\mathrm{Nm}_{\mathcal{F}/F_i}(\alpha))}{\rho_{i,1}(\mathrm{Nm}_{\mathcal{F}/F_i}(\alpha)')} \right)_{i=1,\dots,n} : (\alpha) \in P \right\}$$

is equidistributed in $\prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$, where each $\rho_{i,1}$ is a real place of F_i above ρ_i, and u_i is the generator of $\ker(\mathcal{O}_{F(\sqrt{-\epsilon_i})}^\times \to \mathcal{O}_F^\times)$ with $\rho_{i,1}(u_i) > 1$.

Proof. Since $h(\mathcal{F}) = 1$, we have $\mathbb{A}_{\mathcal{F}}^\times = \mathcal{F}^\times (\prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathcal{F}_\mathfrak{p}}^\times \prod_{w \mid \infty} \mathbb{C}^\times)$. The injection $\prod_{w \mid \infty} \mathbb{C}^\times \hookrightarrow \mathbb{A}_{\mathcal{F}}^\times$ induces an isomorphism $(\prod_{w \mid \infty} \mathbb{C}^\times)/\mathcal{O}_{\mathcal{F}}^\times \xrightarrow{\sim} \mathbb{A}_{\mathcal{F}}^\times / (\mathcal{F}^\times (\prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathcal{F}_\mathfrak{p}}^\times))$. For each $i = 1, \dots, n$, let $N_i : \prod_{w \mid \rho_i} \mathbb{C}^\times \to \mathbb{R}_{>0}$ be the composition

$$\prod_{w \mid \rho_i} \mathbb{C}^\times = \prod_{v \mid \rho_i} \prod_{w \mid v} \mathbb{C}^\times \xrightarrow{(\mathrm{Nm}_{\mathcal{F}/F_i}, \mathrm{Nm}_{\mathcal{F}/F_i})} \prod_{v \mid \rho_i} \mathbb{R}_{>0} \xrightarrow{(x,y) \mapsto \sqrt{\frac{x}{y}}} \mathbb{R}_{>0} \xrightarrow{\log} \mathbb{R}, \tag{5.3.1}$$

where v denotes infinite places of F_i, w denotes infinite places of $\mathcal{F}$, and $\mathrm{Nm}_{\mathcal{F}/F_i}$ is the local norm. For $\alpha \in \mathcal{F}^\times \hookrightarrow \prod_{w \mid \rho_i} \mathbb{C}^\times$, we have $N_i(\alpha) = \frac{1}{2} \log \frac{\rho_{i,1}(\mathrm{Nm}_{\mathcal{F}/F_i}(\alpha))}{\rho_{i,1}(\mathrm{Nm}_{\mathcal{F}/F_i}(\alpha)')}$. Note that (5.3.1) induces a surjection $\{(z_w)_{w \mid \rho_i} : \prod_{w \mid \rho_i} \|z_w\| = 1\}/\mathcal{O}_{\mathcal{F}}^\times \twoheadrightarrow \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$. Then $\prod_{i=1}^n N_i : \prod_{w \mid \infty} \mathbb{C}^\times = \prod_{i=1}^n \prod_{w \mid \rho_i} \mathbb{C}^\times \to \prod_{i=1}^n \mathbb{R}$ induces a Hecke character $\chi : \mathbb{A}_{\mathcal{F}}^\times \to \prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ such that $\chi(\mathbb{A}_{\mathcal{F}}^1) = \prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$, where $\mathbb{A}_{\mathcal{F}}^1 := \{(a_v) \in \mathbb{A}_{\mathcal{F}} : \prod_v \|a_v\| = 1\}$, and the result follows from Hecke's equidistribution [Lan94, XV, §5]. □

Recall that $iy \mapsto \log y$ gives an isomorphism $\varphi_i(Z_{\alpha_i}) \to \mathbb{R}/(2 \log \rho_{i,1}(u_i))\mathbb{Z}$, and two real CM points $\varphi_i(z_{i,1}), \varphi_i(z_{i,2}) \in \varphi_i(Z_{\alpha_i})$ defined by the two orders in $L = F(\sqrt{-\lambda})$ are related by $\varphi(z_{i,2}) = \varphi(\rho_{i,1}(u_i) z_{i,1})$.

Proposition 5.5. *Let $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ be a finite set of odd prime ideals of F. For each $i = 1, \dots, n$, let $t_{i,0}$ and $t_{i,\infty}$ be distinct points on the circle $\varphi(Z_{\alpha_i}) \simeq \mathbb{R}/(2 \log \rho_{i,1}(u_i))\mathbb{Z}$. There exists a prime ideal $\mathfrak{q}$ of F generated by some totally positive $\lambda \in \mathcal{O}_F$ satisfying the following:*

(1) $-\lambda$ is a nonzero square modulo $8\mathfrak{q}_1 \dots \mathfrak{q}_r$;
(2) $\varphi_i(z_{i,1}), \varphi_i(z_{i,2})$ lie on different open segments defined by $t_{i,0}, t_{i,\infty}$ for each $i = 1, \dots, n$;
(3) $\mathfrak{q}$ lies above a rational prime that is totally split in $\mathcal{F}$.

Proof. Consider the modulus $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty = 8\mathfrak{q}_1 \dots \mathfrak{q}_r \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}$ and the canonical homomorphism $\pi_\mathfrak{m} : \mathbb{A}_F^\times \to C_\mathfrak{m}$ realizing the ray class group $C_\mathfrak{m}$ as a quotient of $\mathbb{A}_F^\times$. For $(a_\mathfrak{p})_\mathfrak{p} \in \mathbb{A}_F^\times$ with $v_\mathfrak{p}(a_\mathfrak{p} - 1) \geq m(\mathfrak{p})$ for all $\mathfrak{p} \mid \mathfrak{m}_0$ and $a_\mathfrak{p} > 0$ for all real $\mathfrak{p}$, $\pi_\mathfrak{m}((a_\mathfrak{p})_\mathfrak{p})$ is the class of $\prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$. Note that $\pi_\mathfrak{m}(F^\times) = 1$ and $\pi_\mathfrak{m}(\mathbb{A}_F^1) = C_\mathfrak{m}$. Let $V_\mathfrak{m}$ be the image of $\{(x) : x \in F^\times, v_\mathfrak{p}(x+1) \geq m(\mathfrak{p}) \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0 \text{ and } x_\mathfrak{p} > 0 \text{ for all real } \mathfrak{p}\}$ in $C_\mathfrak{m}$, which is nonempty by weak approximation. By equidistribution there exists some prime ideal of F that can be generated by some totally negative $-\lambda$ satisfying $-\lambda \equiv 1$ modulo $\mathfrak{m}_0$. Let $\chi_0 = \pi_\mathfrak{m} \circ \mathrm{Nm}_{\mathcal{F}/F}$, then $\chi_0(\mathbb{A}_{\mathcal{F}}^1) \cap V_\mathfrak{m} \neq \emptyset$ since (λ) splits in $\mathcal{F}$.

Define a Hecke character $\chi = (\chi_0, \chi_\infty) : \mathbb{A}_{\mathcal{F}}^\times \to C_\mathfrak{m} \times (\prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z})$, where χ_∞ is defined in the proof of Lemma 5.4 by (5.3.1). Note that $\chi_0(\prod_{w \mid \infty} \mathbb{C}^\times) = 1$, so we have $\chi_0(\mathbb{A}_{\mathcal{F}}^\times) = \chi_0(\ker(\chi_\infty))$, and $\chi(\mathbb{A}_{\mathcal{F}}^1) = \chi_0(\mathbb{A}_{\mathcal{F}}^1) \times \chi_\infty(\mathbb{A}_{\mathcal{F}}^1)$. For each $i = 1, \dots, r$, let V_i be the image in $\mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ of the open segment on the circle $\varphi(Z_{\alpha_i}) \simeq \mathbb{R}/(2 \log \rho_{i,1}(u_i))\mathbb{Z}$ defined by $t_{i,0}, t_{i,\infty}$ of smaller measure. Note that a point in $V_i \subset \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ has two preimages lie on different open segments of $\mathbb{R}/(2 \log \rho_{i,1}(u_i))\mathbb{Z}$. Since $V := V_\mathfrak{m} \times (\prod_{i=1}^n V_i)$ is a nonempty open subspace of the compact space $C_\mathfrak{m} \times (\prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z})$, and $\chi(\mathbb{A}_{\mathcal{F}}^1) \cap V \neq \emptyset$, it follows from Hecke's equidistribution [Lan94, XV, §5] that there exists a prime ideal (α) of $\mathcal{F}$ such that $\chi((\alpha)) \in V$. Note that $\mathrm{Nm}_{\mathcal{F}/F}(\alpha)$ is totally positive since (5.3.1) always gives positive terms in the middle. Let $\mathfrak{q} = \mathrm{Nm}_{\mathcal{F}/F}((\alpha))$, where we may assume (α) lies above a totally split rational prime, as such primes have density one in $\mathcal{F}$. □

Proposition 5.6. *Let $S = \{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ be a finite set of odd prime ideals of F. For each $i = 1, \dots, n$, let d_i be an odd positive integer, and $t_i, s_{i,1}, \dots, s_{i,d_i} \in \varphi(Z_{\alpha_i}) \simeq \mathbb{R}/(2\log \rho_{i,1}(u_i))\mathbb{Z}$ such that their images in $\mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ are distinct. There exists a prime ideal $\mathfrak{q}$ of F generated by some totally positive $\lambda \in \mathcal{O}_F$ satisfying the following:*

(1) $-\lambda$ is a nonzero square modulo $8\mathfrak{q}_1 \dots \mathfrak{q}_r$;
(2) for each $i = 1, \dots, n$, the two real CM points $\varphi_i(z_{i,1}), \varphi_i(z_{i,2})$ lie on different open segments defined by $t_i, s_{i,j}$ for an odd number of $j \in \{1, \dots, d_i\}$;
(3) $\mathfrak{q}$ lies above a rational prime that is totally split in $\mathcal{F}$.

Proof. The proof follows that of Proposition 5.5, with the only modification being the definition of V_i. For each $i = 1, \dots, r$ and $j = 1, \dots, d_i$, the two distinct points $t_i, s_{i,j}$ define two open segments in $\mathbb{R}/(2\log \rho_{i,1}(u_i))\mathbb{Z}$, and let $V_{i,j} \subset \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ be the image of the one of smaller measure. Note that a point in $\mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ has two preimages on different open segments of $\mathbb{R}/(2\log \rho_{i,1}(u_i))\mathbb{Z}$ if and only if it is in $V_{i,j}$. There exists $J_i \subset \{1, \dots, d_i\}$ such that $\#J_i$ is odd and $V_i := (\bigcap_{j \in J_i} V_{i,j}) \backslash (\bigcup_{j \notin J_i} V_{i,j}) \neq \emptyset$ is a non empty open subspace of the compact space $\mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$. □

6. Proof of main theorem

In this section, we prove Theorem 1.1. We begin by defining the polynomials associated to the CM cycles constructed in §3. In section 6.2 we use the input from §4 to study the polynomials modulo λ after clearing denominators, and in section 6.3 we use the input from §5 to analyze the sign of the polynomials evaluated at the coordinate of the given abelian variety and at the elliptic points with even order automorphisms. In section 6.4 we combine all of the ingredients and apply quadratic reciprocity to complete the proof.

Suppose the Shimura curve $\widetilde{\Gamma}\backslash\mathcal{H} \simeq \Gamma_0\backslash X^+$ has genus 0. Its canonical model is defined over the reflex field $\rho(F) \subset \mathbb{C}$. Assume the canonical model is isomorphic to $\mathbb{P}^1_{F'}$. Since the quaternion algebra B is unramified at all finite primes, by [KM85, pp. 508-509], the coarse moduli space of the integral canonical model is smooth, and thus isomorphic to $\mathbb{P}^1_{\mathcal{O}_F}$. Choose a coordinate j compatible with the model over $\mathcal{O}_F$.

Fix $\overline{F} \hookrightarrow \mathbb{C}$, and let $\tau_1, \dots, \tau_{[F:\mathbb{Q}]} \in \mathrm{Gal}(\overline{F}/\mathbb{Q})$ correspond to the embeddings $\rho_1, \dots, \rho_{[F:\mathbb{Q}]} : F \hookrightarrow \mathbb{R}$ and c denote complex conjugation.

Assume 2 is inert in F and F satisfies all the additional assumptions in §5. Since $h(F(\sqrt{-1}))$ is odd by [CH88, 13.7], there is an elliptic point of order 2 with coordinate j_∞ such that $[F(j_\infty) : F]$ is odd. Let $j_0 \in F$ be the coordinate of the given point on the Shimura curve such that $F' := F(j_\infty, j_0)$ is an odd-degree extension of F. Let $\sigma_1, \dots, \sigma_{[F':F]} \in \mathrm{Gal}(\overline{F}/F)$ such that $\mathrm{Hom}_F(F', \overline{F}) = \{\sigma_1|_{F'}, \dots, \sigma_{[F':F]}|_{F'}\}$. To get the main idea of the proof, the reader may focus on the case when $F' = F$.

Let S' be a finite set of rational primes such that $S' \supset \{p : p \text{ is ramified in } F'\} \cup \{p : v_\mathfrak{p}(j_0) \neq 0 \text{ for some prime } \mathfrak{p} \text{ of } F' \text{ above } p\} \cup \{p : v_\mathfrak{p}(j_\infty) \neq 0 \text{ for some prime } \mathfrak{p} \text{ of } F' \text{ above } p\}$. Let S be the set of prime ideals of F above the primes in S'. Then there exist $d_0, d_\infty \in \mathcal{O}_F$ such that $d_0 j_0 \in \mathcal{O}_{F'}, d_\infty j_\infty \in \mathcal{O}_{F'}$ and all primes dividing $d_0 d_\infty$ lie in S.

6.1. For a large enough totally positive prime $\lambda \in F$ with $-\lambda$ square modulo 4, let $\alpha_1, \dots, \alpha_{h_1}$ (resp. $\beta_1, \dots, \beta_{h_2}$) be the j-coordinates of the CM points in the CM cycle corresponding to optimal embeddings $\mathcal{O}_{F(\sqrt{-\lambda})} \hookrightarrow \mathcal{O}$ (resp. $\mathcal{O}_F[\sqrt{-\lambda}] \hookrightarrow \mathcal{O}$), where $h_1 = h(F(\sqrt{-\lambda}))$ (resp. $h_2 = h(\mathcal{O}_F[\sqrt{-\lambda}])$) is odd, and define the polynomials

$$P_\lambda(x) := \prod_{l=1}^{h_1}(x - \alpha_l),$$

$$P_{4\lambda}(x) := \prod_{l=1}^{h_2}(x - \beta_l).$$

By construction, $\mathrm{Gal}(\overline{F}/F)$ permutes $\alpha_1, \dots, \alpha_{h_1}$ (resp. $\beta_1, \dots, \beta_{h_2}$), so that $P_\lambda(x)$, $P_{4\lambda}(x) \in F[x]$. Moreover, we have $\alpha_1, \dots, \alpha_{h_1} \in H_{F(\sqrt{-\lambda})}$ and $\beta_1, \dots, \beta_{h_2} \in H_{\mathcal{O}_F[\sqrt{-\lambda}]}$, where $H_{F(\sqrt{-\lambda})}$ is the Hilbert class field of $F(\sqrt{-\lambda})$ and $H_{\mathcal{O}_F[\sqrt{-\lambda}]}$ is the ring class field corresponding to the order $\mathcal{O}_F[\sqrt{-\lambda}]$. Note that $H_{F(\sqrt{-\lambda})} \subset H_{\mathcal{O}_F[\sqrt{-\lambda}]}$ and the extension $H_{\mathcal{O}_F[\sqrt{-\lambda}]}/H_{F(\sqrt{-\lambda})}$ is ramified at a subset of the primes dividing

the conductor 2. Since $(\sqrt{-\lambda})$ is a principal prime ideal of $\mathcal{O}_F[\sqrt{-\lambda}]$, it splits completely in $H_{\mathcal{O}_F[\sqrt{-\lambda}]}$. Let $H := H_{\mathcal{O}_F[\sqrt{-\lambda}]}$ and $\mathfrak{l}$ be a prime of H above λ.

Let $b_\lambda \in \mathcal{O}_F$ (resp. $b_{4\lambda} \in \mathcal{O}_F$) be the denominator of $P_\lambda(x)$ (resp. $P_{4\lambda}(x)$) such that $b_\lambda P_\lambda(x)$ (resp. $b_{4\lambda}P_{4\lambda}(x)$) is primitive, then

$$b_\lambda P_\lambda(x) = \left(b_\lambda \prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)<0}}^{h_1} (x-\alpha_k) \right) \prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)\geq 0}}^{h_1} (x-\alpha_k) \in \mathcal{O}_{H_\mathfrak{l}}[x],$$

$$b_{4\lambda} P_{4\lambda}(x) = \left(b_{4\lambda} \prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)<0}}^{h_2} (x-\beta_k) \right) \prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)\geq 0}}^{h_2} (x-\beta_k) \in \mathcal{O}_{H_\mathfrak{l}}[x],$$

where

$$b_\lambda \prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)<0}}^{h_1} (x-\alpha_k) \equiv \tilde{b}_\lambda \not\equiv 0 \pmod{\mathfrak{l}}, \qquad \tilde{b}_\lambda := b_\lambda \prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)<0}}^{h_1} (-\alpha_k),$$

$$b_{4\lambda} \prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)<0}}^{h_2} (x-\beta_k) \equiv \tilde{b}_{4\lambda} \not\equiv 0 \pmod{\mathfrak{l}}, \qquad \tilde{b}_{4\lambda} := b_{4\lambda} \prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)<0}}^{h_2} (-\beta_k).$$

6.2. By Proposition 4.6 and the first part of Proposition 4.8, roots of $P_\lambda(x)P_{4\lambda}(x)$ are paired modulo $\mathfrak{l}$. Then Lemma 6.1 shows that $\mathrm{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty) d_0^{h_1+h_2} b_\lambda P_\lambda(j_0) b_{4\lambda} P_{4\lambda}(j_0)) \in \mathcal{O}_F$ is a square in $\mathcal{O}_F/\lambda\mathcal{O}_F = \mathcal{O}_{H_\mathfrak{l}}/\mathfrak{l}\mathcal{O}_{H_\mathfrak{l}}$.

Lemma 6.1. *Modulo $\mathfrak{l}$, we have*

$$\mathrm{Nm}_{F'/F}(d_0^{h_1+h_2} b_\lambda P_\lambda(j_0) b_{4\lambda} P_{4\lambda}(j_0)) \equiv (\tilde{b}_\lambda \tilde{b}_{4\lambda})^{[F':F]} \cdot \textit{square}, \tag{6.2.1}$$

$$\mathrm{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)) \equiv (\tilde{b}_\lambda \tilde{b}_{4\lambda})^{[F':F]} \cdot \textit{square}. \tag{6.2.2}$$

Proof. We prove (6.2.2), and (6.2.1) follows by the same argument. Let $\sigma_1, \dots, \sigma_{[F':F]} \in \mathrm{Gal}(\overline{F}/F)$ such that $\mathrm{Hom}_F(F', \overline{F}) = \{\sigma_1|_{F'}, \dots, \sigma_{[F':F]}|_{F'}\}$. Then

$$\mathrm{Nm}_{F'/F}(P_\lambda(j_\infty)) = \prod_{i=1}^{[F':F]} \sigma_i(P_\lambda(j_\infty)) = \prod_{i=1}^{[F':F]} P_\lambda(\sigma_i j_\infty) = \prod_{k=1}^{h_1} \prod_{i=1}^{[F':F]} (\sigma_i j_\infty - \alpha_k)$$

where $\prod_{i=1}^{[F':F]} (\sigma_i j_\infty - \alpha_k) \in H$ for each $k = 1, \dots, h_1$. Similarly,

$$\mathrm{Nm}_{F'/F}(P_{4\lambda}(j_\infty)) = \prod_{k=1}^{h_2} \prod_{i=1}^{[F':F]} (\sigma_i j_\infty - \beta_k)$$

where $\prod_{i=1}^{[F':F]} (\sigma_i j_\infty - \beta_k) \in H$ for each $k = 1, \dots, h_2$. Then we have

$$\mathrm{Nm}_{F'/F}(d_\infty^{h_1} b_\lambda P_\lambda(j_\infty)) = \left(b_\lambda^{[F':F]} \prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)<0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \right) \left(\prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)\geq 0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \right) \in \mathcal{O}_{H_\mathfrak{l}},$$

$$\mathrm{Nm}_{F'/F}(d_\infty^{h_2} b_{4\lambda} P_{4\lambda}(j_\infty)) = \left(b_{4\lambda}^{[F':F]} \prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)<0}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \right) \left(\prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)\geq 0}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \right) \in \mathcal{O}_{H_\mathfrak{l}}.$$

From the assumption that $\lambda \notin S$, we have $v_{\mathfrak{l}}(d_\infty) = 0$ and $v_{\mathfrak{l}'}(\sigma_i j_\infty) = 0$ for any prime $\mathfrak{l}'$ above $\mathfrak{l}$, then

$$b_\lambda^{[F':F]} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\alpha_k)<0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \equiv \tilde{b}_\lambda^{[F':F]} \not\equiv 0 \pmod{\mathfrak{l}},$$

$$b_{4\lambda}^{[F':F]} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\beta_k)<0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \equiv \tilde{b}_{4\lambda}^{[F':F]} \not\equiv 0 \pmod{\mathfrak{l}}.$$

Let $\mathfrak{l}'$ be a prime above $\mathfrak{l}$ in the Galois closure of $F'H$. Since $\lambda \notin S$, it is unramified in F', and $\mathfrak{l}'$ over λ has ramification index 2. For each point on the Shimura curve with coordinate $j \in F'H$, if it reduces to a point without even order automorphisms, then the sets $\{\alpha_k : v_{\mathfrak{l}'}(\alpha_k - j) > 0\}$ and $\{\beta_k : v_{\mathfrak{l}'}(\beta_k - j) > 0\}$ both have even cardinality from the pairing as described in Proposition 4.6; if it reduces to a point with even order automorphisms, then the set $\{\alpha_k : v_{\mathfrak{l}'}(\alpha_k - j) > 0\} \cup \{\beta_k : v_{\mathfrak{l}'}(\beta_k - j) > 0\}$ has even cardinality from the pairing as described in Proposition 4.8.[15] Therefore, for any $\bar{j} \in \mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$,

$$\left(\prod_{\substack{k=1 \\ \overline{\alpha_k}=\bar{j}}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \right) \left(\prod_{\substack{k=1 \\ \overline{\beta_k}=\bar{j}}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \right) \tag{6.2.3}$$

is a square in $\mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$, where $\overline{\alpha_k}$ (resp. $\overline{\beta_k}$) denotes the image of α_k (resp. β_k) in $\mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$. □

We consider the product of $b_\lambda P_\lambda(j_0) b_{4\lambda} P_{4\lambda}(j_0)$ and $b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)$ to cancel the effect of the leading coefficient $\tilde{b}_\lambda \tilde{b}_{4\lambda}$ of $b_\lambda P_\lambda(x) b_{4\lambda} P_{4\lambda}(x)$ modulo λ. In order to analyze $\mathrm{Nm}_{F'/F}(d_0^{h_1+h_2} b_\lambda P_\lambda(j_0) b_{4\lambda} P_{4\lambda}(j_0))$ modulo λ, we need to divide appropriate power of λ from $\mathrm{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty))$ to get a nonzero square, so we use Proposition 4.8 to prove Lemma 6.2.

Each $\sigma_i(j_\infty)$ is a point with an even order automorphism, and let

$$A_i := \{\alpha_k : v_{\mathfrak{l}'}(\sigma_i(j_\infty) - \alpha_k) > 0\} \cup \{\beta_k : v_{\mathfrak{l}'}(\sigma_i(j_\infty) - \beta_k) > 0\}.$$

For λ large enough, we may assume $A_i \cap A_{i'} = \emptyset$ whenever $\sigma_i(j_\infty) \neq \sigma_{i'}(j_\infty)$, and $\#\operatorname{Aut}(\sigma_i(j_\infty)_{\overline{\mathbb{F}}_{\mathfrak{l}'}}) = \#\operatorname{Aut}(\sigma_i(j_\infty)) = 2$.

Lemma 6.2. *Each $\#A_i$ is even, and we have*

$$\lambda^{-\sum_{i=1}^{[F':F]} \#A_i} \mathrm{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)) \equiv (\tilde{b}_\lambda \tilde{b}_{4\lambda})^{[F':F]} \cdot \textit{nonzero square} \tag{6.2.4}$$

modulo $\mathfrak{l}$.

Proof. For $\bar{j} \in \mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$ such that $\bar{j} \neq \overline{\sigma_i(j_\infty)}$ for any i, (6.2.3) is a nonzero square in $\mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$ as in the proof of Lemma 6.1. From the pairing in the neighborhood of $\sigma_i(j_\infty)_{\overline{\mathbb{F}}_{\mathfrak{l}'}}$ as described in Proposition 4.8, elements in A_i are paired and for each pair $\{\gamma_1, \gamma_2\}$, by Lemma 2.5, we have

$$v_{\mathfrak{l}}(\gamma_1 - \gamma_2) = v_{\mathfrak{l}'}(\gamma_1 - \gamma_2) \geq \#\operatorname{Aut}(\sigma_i(j_\infty)_{\overline{\mathbb{F}}_{\mathfrak{l}'}}) \cdot 2 > \#\operatorname{Aut}(\sigma_i(j_\infty)_{\overline{\mathbb{F}}_{\mathfrak{l}'}}) \cdot 1 = v_{\mathfrak{l}'}(\sigma_i(j_\infty) - \gamma_1) = v_{\mathfrak{l}'}(\sigma_i(j_\infty) - \gamma_2),$$

where $\#\operatorname{Aut}(\sigma_i(j_\infty)_{\overline{\mathbb{F}}_{\mathfrak{l}'}}) = 2 = v_{\mathfrak{l}'}(\lambda)$ and $\mathfrak{l}'$ is a prime above $\mathfrak{l}$ in the Galois closure of $F'H$. Then

$$v_{\mathfrak{l}} \left(\prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_1)) \right) = v_{\mathfrak{l}} \left(\prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_2)) \right) = 2[F' : F(j_\infty)],$$

$$\lambda^{-[F':F(j_\infty)]} \left(\prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_1)) - \prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_2)) \right) \in \lambda \mathcal{O}_{H_{\mathfrak{l}}}.$$

[15] Here we need the assumption 2 inert in F.

Therefore,

$$\lambda^{-\sum_{i=1}^{[F':F]}\#A_i}\left(\prod_{\substack{k=1\\ v_\mathfrak{l}(\alpha_k)\geq 0}}^{h_1}\prod_{i=1}^{[F':F]}(d_\infty(\sigma_i(j_\infty)-\alpha_k))\right)\left(\prod_{\substack{k=1\\ v_\mathfrak{l}(\beta_k)\geq 0}}^{h_2}\prod_{i=1}^{[F':F]}(d_\infty(\sigma_i(j_\infty)-\beta_k))\right)$$

is a square in $(\mathcal{O}_{H_\mathfrak{l}}/\mathfrak{l}\mathcal{O}_{H_\mathfrak{l}})^\times \simeq (\mathcal{O}_F/\lambda\mathcal{O}_F)^\times$, where each $\#A_i$ is even. □

6.3. As explained in Section 5.3, for each $\tau_i \in \mathrm{Gal}(\overline{F}/\mathbb{Q})$, $\tau_i(\alpha_1),\dots,\tau_i(\alpha_{h_1})$ (resp. $\tau_i(\beta_1),\dots,\tau_i(\beta_{h_2})$) correspond to the points in the conjugate CM cycle on the conjugate Shimura variety $\mathbb{P}^1_{\tau_i(F)}$. The conjugate CM cycle is defined over $\tau_i(F)\subset\mathbb{R}$, then $\{\tau_i(\alpha_1),\dots,\tau_i(\alpha_{h_1})\}$ (resp. $\{\tau_i(\beta_1),\dots,\tau_i(\beta_{h_2})\}$) is invariant under complex conjugation, and let $\alpha_i^*\in\{\tau_i(\alpha_1),\dots,\tau_i(\alpha_{h_1})\}$ (resp. $\beta_i^*\in\{\tau_i(\beta_1),\dots,\tau_i(\beta_{h_2})\}$) be the unique real point (Lemma 3.3).

Lemma 6.3. *For each $\tau_i\in\mathrm{Gal}(\overline{F}/\mathbb{Q})$, the sign of $\tau_i(\mathrm{Nm}_{F'/F}(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty)))$ is determined by the sign of*

$$\prod_{\substack{\sigma:F(j_0)\hookrightarrow\mathbb{R}\\ \sigma|_F=\rho_i}}(\sigma(j_0)-\alpha_i^*)(\sigma(j_0)-\beta_i^*)(\sigma_{\infty,i}(j_\infty)-\alpha_i^*)(\sigma_{\infty,i}(j_\infty)-\beta_i^*),$$

where $\sigma_{\infty,i}$ is the unique embedding $F(j_\infty)\hookrightarrow\mathbb{R}$ satisfying $\sigma_{\infty,i}|_F=\rho_i$.

Proof. When $\sigma\in\mathrm{Gal}(\overline{F}/F)$ with $\tau_i\sigma(F')\subset\mathbb{R}$, we have

$$\prod_{\substack{l=1\\ \tau_i(\alpha_l)\neq\alpha_i^*}}^{h_1}(\tau_i\sigma(j_\infty)-\tau_i(\alpha_l))>0,\qquad \prod_{\substack{l=1\\ \tau_i(\beta_l)\neq\beta_i^*}}^{h_2}(\tau_i\sigma(j_\infty)-\tau_i(\beta_l))>0,$$

$$\prod_{\substack{l=1\\ \tau_i(\alpha_l)\neq\alpha_i^*}}^{h_1}(\tau_i\sigma(j_0)-\tau_i(\alpha_l))>0,\qquad \prod_{\substack{l=1\\ \tau_i(\beta_l)\neq\beta_i^*}}^{h_2}(\tau_i\sigma(j_0)-\tau_i(\beta_l))>0,$$

then

$$\begin{aligned}\mathrm{sgn}(\tau_i\sigma(P_\lambda(j_\infty)P_{4\lambda}(j_\infty)))&=\mathrm{sgn}\left((\tau_i\sigma(j_\infty)-\alpha_i^*)(\tau_i\sigma(j_\infty)-\beta_i^*)\right),\\ \mathrm{sgn}(\tau_i\sigma(P_\lambda(j_0)P_{4\lambda}(j_0)))&=\mathrm{sgn}\left((\tau_i\sigma(j_0)-\alpha_i^*)(\tau_i\sigma(j_0)-\beta_i^*)\right).\end{aligned}$$

Since F is totally real, we have $c\circ\tau_i\circ\sigma_k|_F=\tau_i|_F$, and $c\circ\tau_i\circ\sigma_k|_{F'}=\tau_i\circ\sigma_{k'}|_{F'}$ for a unique $k'\in\sigma_1,\dots,\sigma_{[F':F]}\in\mathrm{Gal}(\overline{F}/F)$, where $k'=k$ if and only if $\tau_i(\sigma_k(F'))\subset\mathbb{R}$, then

$$\begin{aligned}&\mathrm{sgn}(\tau_i(\mathrm{Nm}_{F'/F}(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty))))\\ =&\,\mathrm{sgn}\left(\tau_i\prod_{k=1}^{[F':F]}(\sigma_k(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty)))\right)\\ =&\,\mathrm{sgn}\left(\tau_i\prod_{\substack{k=1\\ \tau_i\sigma_k(F')\subset\mathbb{R}}}^{[F':F]}(\sigma_k(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty))\right)\\ =&\,\mathrm{sgn}\left(\prod_{\substack{k=1\\ \tau_i\sigma_k(F')\subset\mathbb{R}}}^{[F':F]}((\tau_i\sigma_k(j_0)-\alpha_i^*)(\tau_i\sigma_k(j_0)-\beta_i^*)(\tau_i\sigma_k(j_\infty)-\alpha_i^*)(\tau_i\sigma_k(j_\infty)-\beta_i^*))\right)\\ =&\,\mathrm{sgn}\left(\prod_{\substack{\sigma:F(j_0)\hookrightarrow\mathbb{R}\\ \sigma|_F=\rho_i}}((\sigma(j_0)-\alpha_i^*)(\sigma(j_0)-\beta_i^*))\prod_{\substack{\sigma:F(j_\infty)\hookrightarrow\mathbb{R}\\ \sigma|_F=\rho_i}}((\sigma(j_\infty)-\alpha_i^*)(\sigma(j_\infty)-\beta_i^*))\right),\end{aligned}$$

where the last equality follows from $[F' : F]$ being odd. Since the CM cycle corresponding to optimal embedding $\mathcal{O}_{F(\sqrt{-1})}$ has a unique real point, there is a unique $\sigma_{\infty,i} : F(j_\infty) \hookrightarrow \mathbb{R}$ with $\sigma_{\infty,i}|_F = \rho_i$. □

6.4. By Proposition 5.6, there exists a totally positive prime $\lambda \notin S$ of F such that

(1) $-\lambda$ is a square modulo 8 and all primes in S;
(2) for each $i = 1, \dots, [F : \mathbb{Q}]$, $(\sigma(j_0) - \alpha_i^*)(\sigma(j_0) - \beta_i^*)(\sigma_{\infty,i}(j_\infty) - \alpha_i^*)(\sigma_{\infty,i}(j_\infty) - \beta_i^*) < 0$ for an odd number of $\sigma : F(j_0) \hookrightarrow \mathbb{R}$ with $\sigma|_F = \rho_i$.

The first condition implies that

$$\left(\frac{q}{-\lambda}\right) = \left(\frac{-\lambda}{q}\right) = 1 \text{ for any totally positive odd prime } q \in \mathcal{O}_F \text{ with } (q) \in S \tag{6.4.1}$$

by Theorem 2.6. The second condition implies that $\mathrm{Nm}_{F'/F}(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty))$ is totally negative. Let

$$N := \lambda^{-\sum_{i=1}^{[F':F]} \#A_i} \mathrm{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty) d_0^{h_1+h_2} b_\lambda P_\lambda(j_0) b_{4\lambda} P_{4\lambda}(j_0)) \in \mathcal{O}_F.$$

Then N is a square in $\mathcal{O}_{H_\mathfrak{l}}/\mathfrak{l}\mathcal{O}_{H_\mathfrak{l}} = \mathcal{O}_F/\lambda\mathcal{O}_F$ and N is totally negative. If $\lambda | N$, then

$$v_\mathfrak{l}\left(\left(\prod_{\substack{k=1 \\ v_\mathfrak{l}(\alpha_k)\geq 0}}^{h_1} \prod_{i=1}^{[F':F]} (\sigma_i(j_0) - \alpha_k)\right)\left(\prod_{\substack{k=1 \\ v_\mathfrak{l}(\beta_k)\geq 0}}^{h_2} \prod_{i=1}^{[F':F]} (\sigma_i(j_0) - \beta_k)\right)\right) > 0,$$

which implies j_0 is a root of $b_\lambda b_{4\lambda} P_\lambda(x) P_{4\lambda}(x)$ modulo some prime above λ, where λ is ramified in $F(\sqrt{-\lambda})$. Assume $\lambda \nmid N$ and write $(N) = \mathfrak{m}\mathfrak{n}$, where $\mathfrak{m}$ is an integral ideal without odd prime factors and $\mathfrak{n}$ is an odd integral ideal. By Theorem 2.6, we have

$$\left(\frac{-\lambda}{\mathfrak{n}}\right) = (-1)^{[F:\mathbb{Q}]}\left(\frac{N}{-\lambda}\right) = -1 \cdot 1 = -1,$$

and therefore, there is an odd prime $\mathfrak{p}|\mathfrak{n}$ with $v_\mathfrak{p}(N)$ odd such that $\left(\frac{-\lambda}{\mathfrak{p}}\right) = -1$. In particular, $\mathfrak{p} \notin S$ by (6.4.1), so that $\mathfrak{p}$ is a good reduction prime and $\mathfrak{p}$ is unramified in F'.

If $v_\mathfrak{p}(\mathrm{Nm}_{F'/F}(b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)) > 0$, then $v_\mathfrak{p}(\mathrm{Nm}_{F'/F}(b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)))$ is even by Lemma 2.5.[16] Therefore, j_0 is a root of $b_\lambda P_\lambda(x) b_{4\lambda} P_{4\lambda}(x)$ modulo some prime above $\mathfrak{p}$.

7. Examples

In this section, we provide sufficient conditions for verifying some of the assumptions in Theorem 1.1. In particular, all the assumptions in Theorem 1.1 hold for the cases in Theorem 1.3, and hence we prove Theorem 1.3.

Lemma 7.1. *Let C be a smooth projective geometrically connected curve over a field k. If C has genus 0 and there exists a divisor D of degree 1, then $C \simeq \mathbb{P}^1_k$. In particular, if there are divisors D_1 and D_2 such that $\deg D_1$ and $\deg D_2$ are relatively prime, then $C \simeq \mathbb{P}^1_k$.*

Proof. By Riemann-Roch, we have

$$\dim_k H^0(C, \mathcal{O}_C(D)) \geq \deg D + 1 - g(C) = 2,$$

then $\mathcal{O}_C(D)$ is very ample and induces an isomorphism $C \simeq \mathbb{P}^1_k$ ([Liu02, 7.3.24]). □

By Lemma 3.1 and Lemma 3.2, a CM cycle defined by $\phi : L \hookrightarrow B$ defines a divisor of degree $h(\phi^{-1}(\mathcal{O}))$. If there exist CM extensions L_1, L_2 of F such that $h(L_1)$ and $h(L_2)$ are relatively prime, then the canonical model of the Shimura curve $\mathcal{O}^1\backslash\mathcal{H}$ is isomorphic to $\mathbb{P}^1_F$.

Lemma 7.2. *Let F be a totally real number field with narrow class number 1, and suppose there is a unique prime $\mathfrak{p}_2$ of F lying above 2. Suppose $F(\sqrt{u})$ has odd class number for all unit $u \in \mathcal{O}_F^\times$. Let M denote the compositum of $F(\sqrt{u})$ as u ranges over $\mathcal{O}_F^\times$. Then every intermediate field K with $F \subseteq K \subseteq M$ has class number $\prod_{F(\sqrt{u})\subseteq M} h(F(\sqrt{u}))$.*

[16] This treatment follows the idea of [LMPT].

Proof. Let $r = [F : \mathbb{Q}]$ and $u_1, \dots, u_{r-1}$ be fundamental units of F, then $M = F(\sqrt{-1}, \sqrt{u_1}, \dots, \sqrt{u_{r-1}})$ is a multiquadratic extension of F with $[M : F] = 2^r$, and any quadratic subextension of M/F is of the form $F(\sqrt{u})$ for some $u \in \mathcal{O}_F^\times \backslash \mathcal{O}_F^{\times 2}$. Any intermediate field K with $F \subsetneq K \subseteq M$ is a multiquadratic extension of F. As a special case of the example in [Neh33, pp. 329-330], we have $h(K) = 2^{\mu(K)} \prod_{F(\sqrt{u}) \subseteq M} h(F(\sqrt{u}))$ for some nonnegative integer $\mu(K)$.

Let $L_0 := F(\sqrt{-1})$, and $L_i := L_{i-1}(\sqrt{u_i})$. Inductively, for each $i = 1, \dots, r-1$, under the assumption that $h(L_{i-1})$ is odd, there is exactly one prime (both finite and infinite), namely the unique prime lying above 2, of L_{i-1} ramifying in the quadratic extension L_i, then $2 \nmid h(L_i)$ by [CH88, 9.2]. In particular, we have $2 \nmid h(M)$ and $\mathfrak{p}_2$ is totally ramified in M.

Let $K_0 = K$ and $K_i = KL_{i-1}$ for each $i = 1, \dots, r$, then $K_i = K_{i-1}$ or K_i/K_{i-1} is a ramified quadratic extension, which implies $h(K_{i-1})$ divides $h(K_i)$ by [CH88, 5.4]. Therefore, we have $h(K)$ odd. □

When the totally real field F has narrow class number 1 and there is a unique prime of F lying above 2, given units $\epsilon_1, \dots, \epsilon_n$ that are negative at exactly one of the distinct real embeddings $F \hookrightarrow \mathbb{R}$, if we can verify that $F\left(\sqrt{(-\epsilon_1)^{\delta_1} \cdots (-\epsilon_n)^{\delta_n}}\right)$ has class number 1 for all $\delta_1, \dots, \delta_n \in \{0, 1\}$, then $F(\sqrt{-\epsilon_1}, \dots, \sqrt{-\epsilon_n})$ has class number 1.

Example 7.3. The following examples from [Voi09, §4] satisfy all the assumptions.

- $[F : \mathbb{Q}] = 3$, $\operatorname{disc}(F) = 49, 81, 169, 321, 361, 473, 785, 993$
- $[F : \mathbb{Q}] = 5$, $\operatorname{disc}(F) = 14641, 24217, 65657, 70601, 124817, 149169, 157457, 160801, 161121, 173513, 176281, 202817, 240881$
- $[F : \mathbb{Q}] = 7$, $\operatorname{disc}(F) = 20134393, 25367689, 28118369, 31056073, 32567681, 35269513$

We used Magma [BCP97] to perform the computations.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478

[BG08] Srinath Baba and Hå kan Granath, *Primes of superspecial reduction for QM abelian surfaces*, Bull. Lond. Math. Soc. **40** (2008), no. 2, 311–318. MR2414789

[BO78] Pierre Berthelot and Arthur Ogus, *Notes on crystalline cohomology*, Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1978. MR491705

[CH88] P. E. Conner and J. Hurrelbrink, *Class number parity*, Series in Pure Mathematics, vol. 8, World Scientific Publishing Co., Singapore, 1988. MR963648

[Cha18] François Charles, *Exceptional isogenies between reductions of pairs of elliptic curves*, Duke Math. J. **167** (2018), no. 11, 2039–2072. MR3843371

[Con04] Brian Conrad, *Gross-Zagier revisited*, Heegner points and Rankin L-series, 2004, pp. 67–163. With an appendix by W. R. Mann. MR2083211

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982. MR654325

[Elk87] Noam D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbf{Q}$, Invent. Math. **89** (1987), no. 3, 561–567. MR903384

[Elk89] ———, *Supersingular primes for elliptic curves over real number fields*, Compositio Math. **72** (1989), no. 2, 165–172. MR1030140

[Gal00] Federica Galluzzi, *Abelian fourfold of Mumford-type and Kuga-Satake varieties*, Indag. Math. (N.S.) **11** (2000), no. 4, 547–560. MR1909819

[Hec81] Erich Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. MR638719

[HP17] Benjamin Howard and Georgios Pappas, *Rapoport-Zink spaces for spinor groups*, Compos. Math. **153** (2017), no. 5, 1050–1118. MR3705249

[Hui25] Chun-Yin Hui, *On distribution of supersingular primes of abelian varieties and k3 surfaces*, 2025.

[Jao03] David Yen Jao, *Supersingular primes for rational points on modular curves*, ProQuest LLC, Ann Arbor, MI, 2003. Thesis (Ph.D.)–Harvard University. MR2704678

[Kat81] N. Katz, *Serre-Tate local moduli*, Algebraic surfaces (Orsay, 1976–78), 1981, pp. 138–202. MR638600

[Kis10] Mark Kisin, *Integral models for Shimura varieties of abelian type*, J. Amer. Math. Soc. **23** (2010), no. 4, 967–1012. MR2669706

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569

[Lan94] Serge Lang, *Algebraic number theory*, Second, Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994. MR1282723

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications. MR1917232

[LMPT] Wanlin Li, Elena Mantovan, Rachel Pries, and Yunqing Tang, *Infinitely many primes of basic reduction for some abelian fourfolds*.

[Mes72] William Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Mathematics, vol. Vol. 264, Springer-Verlag, Berlin-New York, 1972. MR347836

[MP15] Keerthi Madapusi Pera, *The Tate conjecture for K3 surfaces in odd characteristic*, Invent. Math. **201** (2015), no. 2, 625–668. MR3370622

[MP16] ———, *Integral canonical models for spin Shimura varieties*, Compos. Math. **152** (2016), no. 4, 769–824. MR3484114

[MS10] James S. Milne and Junecue Suh, *Nonhomeomorphic conjugates of connected Shimura varieties*, Amer. J. Math. **132** (2010), no. 3, 731–750. MR2666906

[MS81] J. S. Milne and Kuang-yen Shih, *The action of complex conjugation on a Shimura variety*, Ann. of Math. (2) **113** (1981), no. 3, 569–599. MR621017

[Mum69] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*, Math. Ann. **181** (1969), 345–351. MR248146

[Neh33] Harald Nehrkorn, *über absolute idealklassengruppen und einheiten in algebraischen zahlkörpern*, Abh. Math. Sem. Univ. Hamburg **9** (1933), no. 1, 318–334. MR3069610

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR1697859

[Sad04] Marat Sadykov, *Two results in the arithmetic of Shimura curves*, ProQuest LLC, Ann Arbor, MI, 2004. Thesis (Ph.D.)–Columbia University. MR2705896

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR644559

[Shi75] Goro Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164. MR572971

[SSTT22] Ananth N. Shankar, Arul Shankar, Yunqing Tang, and Salim Tayou, *Exceptional jumps of Picard ranks of reductions of K3 surfaces over number fields*, Forum Math. Pi **10** (2022), Paper No. e21, 49. MR4490194

[ST18] Ananth N. Shankar and Jacob Tsimerman, *Unlikely intersections in finite characteristic*, Forum Math. Sigma **6** (2018), Paper No. e13, 17. MR3841493

[ST20] Ananth N. Shankar and Yunqing Tang, *Exceptional splitting of reductions of abelian surfaces*, Duke Math. J. **169** (2020), no. 3, 397–434. MR4065146

[Tay25] Salim Tayou, *Picard rank jumps for K3 surfaces with bad reduction*, Algebra Number Theory **19** (2025), no. 1, 77–112. MR4836458

[vG08] Bert van Geemen, *Real multiplication on $K3$ surfaces and Kuga-Satake varieties*, Michigan Math. J. **56** (2008), no. 2, 375–399. MR2492400

[Voi09] John Voight, *Shimura curves of genus at most two*, Math. Comp. **78** (2009), no. 266, 1155–1172. MR2476577

[Voi21] ———, *Quaternion algebras*, Graduate Texts in Mathematics, vol. 288, Springer, Cham, 2021. MR4279905

[Xu22] Yujie Xu, *Normalization in the Integral Models of Shimura Varieties of Abelian Type*, ProQuest LLC, Ann Arbor, MI, 2022. Thesis (Ph.D.)–Harvard University. MR4464238